

S-60 E

Firmware Version 4.22

H.264/MPEG-4/MJPEG Video encoder

User Manual



SECURITY
SOLUTIONS

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

Copyright © 2017 Siquira B.V.

All rights reserved.

S-60 E v4.22

User Manual v10 (092606-10)

AIT55

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

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

Brand names

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

Liability

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

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

How to contact us

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

Siquira B.V.
Zuidelijk Halfroond 4
2801 DD Gouda
The Netherlands

General : +31 182 592 333

Fax : +31 182 592 123

E-mail : sales.nl@tkhsecurity.com

WWW : <http://www.tkhsecurity.com>

Contents

1	About this manual	8
2	Safety and compliance	9
2.1	Safety	9
2.2	Declaration of Conformity	11
3	Product overview	12
3.1	Features	12
3.2	Models	12
3.3	Description	13
3.4	Front Panel	14
4	Install the unit	15
4.1	Power the unit	15
4.2	Connect cables	15
4.3	Startup	16
4.4	Connector pin assignments	16
4.5	Update device definitions	17
5	Connect the unit	18
5.1	Establish a network connection	18
5.2	Establish video and other signal connections	20
5.2.1	Port numbers	21
6	Interfaces	22
6.1	ONVIF	22
6.2	OSA	22
6.3	Web UI	22
6.4	MX/IP	23
6.5	SNMP	23
6.6	SAP	23
6.7	NTCIP	23
7	Stream media via RTSP	25
7.1	RTSP and RTP	25
7.2	Transfer via UDP or TCP	26
8	Access the webpages	27
8.1	System requirements	27
8.2	Connect via web browser	27
8.3	Find the unit with Device Manager	28
8.4	Connect via UPnP	29
8.5	Log on to the unit	29
9	Navigate the webpages	31
9.1	Menu	31
9.2	Access control	31
9.3	Webpage elements	32
10	View live video via browser	33
10.1	Activate Live View	33

10.2	View live video	34
10.3	Use your browser for PTZ control	35
11	Status	37
11.1	View status information	37
11.1.1	Stream states	37
11.2	View measurements data	38
11.2.1	General, network, and stream measurements	38
11.2.2	FTP Push	38
12	Network	39
12.1	Network settings	39
12.2	Advanced	40
12.2.1	Services	40
12.2.2	Network	40
13	Video	41
13.1	Video encoding overview	41
13.2	General	42
13.2.1	Video Settings	43
13.2.2	Encoder Priorities	44
13.3	Encoder #	44
13.3.1	Encoder Settings	45
13.3.2	Combinations of settings	47
13.3.3	Notes	47
13.3.4	Make a video connection	47
13.3.5	Advanced	48
13.3.5.1	Encoder	49
13.3.5.2	Stream Manager	50
13.3.5.3	Transmitter #	51
13.3.5.4	RTSP Transmitter	52
13.3.5.5	SAP Settings	53
13.3.6	Meta data insertion	55
13.3.7	Notes	58
13.4	H.264 - 1	60
13.4.1	Encoder Settings	61
13.4.2	Constant Quality Mode configuration	62
13.4.3	Profiles	63
13.4.4	Parameter value combinations	65
13.4.5	MX Transmitter Settings and making video connections	65
13.4.6	Advanced	65
13.4.6.1	Encoder	66
13.4.6.2	Stream Manager, Transmitter #, RTSP Transmitter, and SAP	68
13.5	Live View	68
13.5.1	(M)JPEG output	68
13.5.2	Encoder Settings	69
13.5.3	Advanced	69
13.6	OSD	70
13.6.1	OSD facilities	70
13.6.2	Text Settings	71
13.6.3	Text #	71
13.6.3.1	Advanced	72
13.6.4	Graphics	73
13.6.4.1	Advanced	74
13.7	VMD	75
13.7.1	VMD startup	75

13.7.2	Configure detection parameters	76
13.7.3	Set the mask	76
13.7.4	VMD detection window	78
13.7.5	VMD alarm	78
13.7.6	Advanced	78
13.8	FTP Push	80
13.8.1	Post JPEG images	81
13.8.2	General	81
13.8.3	FTP server	81
13.8.4	Event management	82
13.8.5	Monitor and troubleshoot FTP Push	83
13.9	Image Monitor	84
13.9.1	Image quality check	84
13.9.2	Enable the Image Monitor	84
13.9.3	Dial legend	86
13.9.4	Measurements configuration	88
13.9.5	Region of Interest (ROI)	89
13.10	Tamper Detect	90
13.10.1	Camera movement and scene changes	91
13.10.2	Enable Tamper Detect	91
13.10.3	Reference images	91
13.10.3.1	Create a reference image	91
13.10.3.2	Mask the ROI	92
13.10.3.3	Compare images	92
13.10.3.4	Delete a reference image	93
13.10.4	Position measurement	94
13.10.5	Alarms	95
13.10.5.1	Alarm examples	96
13.11	Privacy Mask	97
14	Audio	98
14.1	Enable audio	98
14.1.1	Input Settings	99
14.1.2	Output Settings	99
14.2	Make audio connections	100
14.2.1	MX Transmitter Settings	100
14.2.2	MX Receiver Settings	101
14.3	Advanced	101
14.3.1	Audio Input	101
14.3.2	Audio Output	102
14.3.3	Audio Encoder	102
14.3.4	Audio Decoder	102
14.3.5	Transmitter #	103
14.3.6	Receiver 1	104
14.3.7	RTSP Transmitter	105
14.3.8	SAP Settings	106
15	Data RS-422/485	108
15.1	General Settings	108
15.2	UART Settings	109
15.3	Make data connections	109
15.4	TCP Server Settings	110
15.5	Advanced	110
15.5.1	RS-4xx Settings	110
15.5.2	Transmitter #	112
15.5.3	Receiver 1	112

16	Data RS-232	114
16.1	Configure RS-232 settings	114
17	CC Streams	115
17.1	CC channels, CC status, and alarms	115
17.2	Input # Settings	116
17.3	Make contact closure connections	116
17.4	Advanced	117
17.4.1	Transmitter #	117
17.4.2	Receiver 1	117
18	PTZ	119
18.1	Enable PTZ control	119
18.2	Upload/Remove PTZ drivers	120
18.3	Data Settings	120
19	Security	121
19.1	HTTPS	121
19.2	Certificate/Request information	122
19.3	CA-Issued certificate	122
19.4	Self-signed certificate	123
19.5	Open a secure connection	123
20	Event management	124
20.1	Associate events with output facilities	124
20.1.1	CC Output #	124
20.1.2	CC Stream #	125
20.1.3	FTP Push	125
21	Device management	127
21.1	General	127
21.1.1	Identification	127
21.1.2	Device Name	128
21.1.3	Advanced	128
21.1.3.1	Alarm Settings	128
21.1.3.2	LED control	128
21.2	Logging	129
21.2.1	Log file	129
21.2.2	Syslog settings	129
21.3	SNMP	129
21.3.1	SNMP System Information	130
21.3.2	SNMP Communities	130
21.3.3	SNMP Agent	130
21.3.4	SNMP Traps	130
21.3.5	Polling	130
21.4	MX	131
21.4.1	MX/IP	131
21.4.2	MX Notifications	131
21.5	Auto Discovery	132
21.5.1	Advertise the S-60 E	132
21.5.1.1	Note	132
21.6	ONVIF	133
21.6.1	Note	133
21.7	FTP/Telnet	133
21.8	Firmware	134
21.8.1	Firmware images	134

21.8.2	Current Version	134
21.8.3	Upgrade	134
21.8.4	Troubleshoot upgrade issues	135
21.8.5	Advanced	136
21.9	Backup/Restore	137
21.9.1	Backup	137
21.9.2	Restore	137
21.10	Reboot	137
22	User Management	139
22.1	Web Access	139
22.1.1	Access control	139
22.1.2	Manage user accounts	139
22.2	Linux	140
23	Date and Time	142
23.1	Date and time	142
23.2	SNTP Settings	143
23.3	Advanced	144
24	Multicasting	145
24.1	Multicast	145
24.2	Multi-unicasting	146
	Appendix: Enable JavaScript	147
	Appendix: Enable UPnP in Windows	148
	Appendix: Install a video player	149
	Download video player software	149
	Install QuickTime	149
	Install VLC	149
	Appendix: NTCIP Configuration	151
	Supported conformance groups	151
	Configuration	151
	CCTV configuration	152
	Motion control	152
	SNMP MIB	153

1 About this manual

What this manual covers

This manual applies to the S-60 E v4.22, TKH Security's H.264/MPEG-4/MJPEG video encoder.

It explains:

- How to install the unit
- How to establish connections
- How to communicate with the unit
- How to configure the device settings
- How to operate the unit

Who should read this manual

This manual is intended for installers and users of the S-60 E.

What you should already know

To be able to install and use the S-60 E properly, you should have adequate knowledge and skills in the following fields.

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

Before you start

We advise you to read and observe all instructions and warnings in this manual before you continue. Keep this manual with the original bill of sale for future reference and warranty service. When you unpack 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.

Why specifications may change

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

We like to hear from you!

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

Acknowledgement

This product uses the open-source Free Type font-rendering library. The *Open Source Libraries and Licenses* document, available at www.tkhsecurity.com/support-files, gives a complete overview of open source libraries used by our video encoders and IP cameras.

2 Safety and compliance

This chapter gives the S-60 E safety instructions and compliance information.

In This Chapter

2.1 Safety..... 9
 2.2 Declaration of Conformity.....11

2.1 Safety

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

Trained personnel

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

Safety requirements

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

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

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

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

The equipment must be powered by a SELV¹ power supply. This is equivalent to a Limited Power source (LPS, see UL/IEC/EN 60950-1 clause 2.5) or a "NEC Class 2" power supply. When this module is operated in extremely elevated temperature conditions, it is possible for internal and external metal surfaces to become extremely hot.

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

Power source and temperature ratings

Verify that the power source is appropriate before you plug in and operate the unit. Use the unit under conditions where the temperature remains within the range given in the Technical Specifications of this product. You can download the S-60 E datasheet at www.tkhsecurity.com/support-files.

Optical safety

The following optical safety information applies to S-60 E models with SFP interface.

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

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

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

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

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



EMC

Warning: Operation of this equipment in a residential environment could cause radio interference.

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

Note that the warning above does not apply to TKH Security products which comply with the limits for a Class B device. For product-specific details, refer to the EU Declaration of Conformity.

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

To ensure EMC compliance of the equipment, use shielded cables for all signal cables including Ethernet, such as CAT5E SF/UTP or better, as defined in ISO IEC 11801. For power cables, unshielded three wire cable (2p + PE) is acceptable. Ensure that *all* electrically connected components are carefully earthed and protected against surges (high voltage transients caused by switching or lightning).

ESD

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

Care and maintenance

The unit will normally need no maintenance. To keep it operating reliably:

- Prevent dust from collecting on the unit.
- Do not expose the equipment to moisture.

RoHS



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) (2011/65/EU). TKH Security offers products that comply with the EU's RoHS Directive.

Product disposal



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



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

2.2 Declaration of Conformity

The EU Declaration of Conformity for this product is available for download at www.tkhsecurity.com/support-files.

3 Product overview

This chapter introduces the S-60 E and its features.

In This Chapter

3.1 Features.....	12
3.2 Models.....	12
3.3 Description.....	13
3.4 Front Panel.....	14

3.1 Features

S-60 E



- 1x H.264 and 2x MPEG-4/MJPEG encoding
- Image quality monitor
- Tamper detection
- ONVIF Profile S
- Open Streaming Architecture
- Fiber and Ethernet over Coax (EoC) option
- Motion Adaptive Deinterlacing (M.A.D.™)
- Video motion detection
- Stereo audio
- Duplex serial data

3.2 Models

The S-60 E series includes the following models.

S-60 E	H.264/MPEG-4/MJPEG video encoder with audio, data, and CC
S-60 E -SFP	Model with empty SFP slot
S-60 E /SA	Stand-alone version of rack-mount models

Rack-mount S-60 E units are designed to be slotted into MC 10 or MC 11 power supply cabinets. Front panel LEDs indicate network status, stream status (sync), and DC power. All models have backup battery power for their clocks.

3.3 Description

The S-60 E combines H.264 video encoding with MPEG-4 and MJPEG. It offers an open solution for IP video CCTV applications. The video server features H.264 streaming with dual-streaming MPEG-4 or MJPEG, low bandwidth, low latency, and interoperability with most other systems.

Multistreaming

The S-60 E is capable of streaming H.264, and 2x MPEG-4 or MJPEG simultaneously. Each stream is optimised for its purpose: high-quality H.264 for live viewing, low-bandwidth MPEG-4 for storage, or easy-to-decode MJPEG for web applications and remote devices.

Picture enhancement

Almost every analogue camera offers an interlaced signal (PAL or NTSC). On digital computer monitors, this causes severe artefacts, such as comb edges on moving objects. To remove these artefacts the video signal has to be deinterlaced. This can be done in the monitor, but also at the beginning – at the encoder side. The S-60 E is fitted with a motion adaptive deinterlacer (M.A.D.). TKH Security's M.A.D removes the interlacing artefacts on the moving objects only to preserve the vertical resolution of the image. In addition, the deinterlaced image is much easier to encode, saving bits for streaming and storage.

ONVIF and Open Streaming Architecture (OSA)

The S-60 E supports both the international ONVIF standard and TKH Security OSA for remote control, configuration, video switching, and streaming. The S-60 E has been approved for ONVIF Profile S for streaming, PTZ, and I/O. OSA is a comprehensive HTTP RTSP based API, which gives access (next to ONVIF) to all controls and makes full integration easy.

Image quality monitor and tampering alarm

When the image from the camera becomes too poor, an image quality alert is raised. The built-in Image Quality Monitor continuously monitors the camera image on contrast, exposure, sharpness, and noise. In addition, the built-in Tamper Detector monitors changes in the camera's position or field of view. The instant a camera's position is changed a tamper detect alert is raised.

Audio, data, and I/O contacts

By combining audio, programmable I/O contacts, and data with streaming video, the S-60 E provides all the interfaces necessary for any IP CCTV application. On the encoder module, you will find two bidirectional audio channels (lip-synchronised), two digital inputs and outputs, and two serial data ports (RS-232 and RS-422/482). The RS-422/482 data port is combined with a built-in PTZ controller supporting a number of PTZ protocols.

Fiber and EoC options

The S-60 E is available with an optional, pluggable SFP slot. This offers unparalleled flexibility in connectivity. With fiber SFPs you can connect over multimode or single-mode optical fiber cable and cover distances from 100 m to 120 km or more. To connect over (existing) coax, you can use TKH Security's ECO-plug for Ethernet over Coax.

FTP push

Upon an event, the S-60 E can push a JPG image to one or two FTP servers. The event can be triggered externally by VMD, the Image Monitor, or Tamper Detect. The S-60 E can also periodically upload images to the remote server(s).

Web interface



Configuration, management, and live viewing are simplified by the access-controlled web interface. Full in-band control is available through Device Manager and the HTTP API. The S-60 E is field-upgradeable.

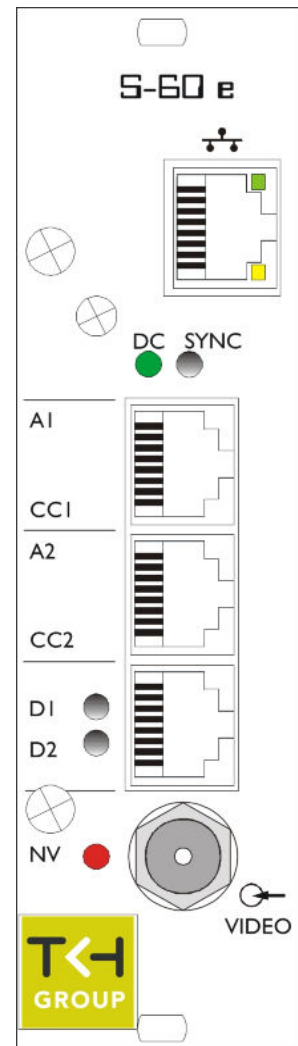
3.4 Front Panel

Features and indications

The front panel of the S-60 E has the following features.

S-60 E

 VIDEO	BNC connector	video input
	RJ-45 socket or SFP	Ethernet I/O, electrical or fiber
A1, CC1	RJ-45 socket	audio 1, contact closure 1
A2, CC2	RJ-45 socket	audio 2, contact closure 2
D1, D2	RJ-45 socket	RS-485/422, RS-232
Status indicator LEDs		
*DC	green	DC power OK; blinks on identification and errors
*NV	red	no video on input
*SYNC	off	all streams disabled
	green	all enabled streams OK
	red	a transmitted stream fails
	yellow	a received stream fails
	red/yellow blink	at least one transmitted and at least one received stream fail
*D1	green/red	RS-4xx 0/1 data input
*D2	green/off	RS-232 0/1 data input
Ethernet socket LEDs	green/yellow	Green on/off: 100/10 Mbit Yellow on/blink: link OK, active Yellow off/flash: link down, TX attempt



S-60 E front panel features and indications

Pin assignments are given in section *Connector Pin Assignments*.

4 Install the unit

This chapter describes how to install your S-60 E unit and connect power, network, and signal cables.

In This Chapter

4.1 Power the unit.....	15
4.2 Connect cables.....	15
4.3 Startup.....	16
4.4 Connector pin assignments.....	16
4.5 Update device definitions.....	17

4.1 Power the unit

» To power a rack-mount unit

- 1 Insert the S-60 E into an MC 10 or MC 11 power supply cabinet.
- 2 Plug the cabinet power cord into a grounded mains socket.

» To power a stand-alone unit

A stand-alone (/SA) S-60 E requires an external power supply adapter (12 Vdc).

- 1 Connect the power adapter to the power connector on the metal SA housing.
- 2 Plug the power adapter into a grounded mains socket.

4.2 Connect cables

Use the appropriate connectors on the S-60 E front panel to connect the network and signal cables.

» To connect the S-60 E to your 100/10Mbit IP/Ethernet network

- Plug the network cable into the RJ-45 Ethernet socket on the front panel.

Important: Use appropriate cabling (Cat 5 or Cat 6) for network links.

» To connect a video source

- Connect the coaxial cable from your video source (a camera, for example) to the video input BNC connector on the front panel.

» To connect audio, data, and/or contact closure sources/destinations

- Plug the cables carrying audio, data, and/or contact closure signals into the corresponding RJ-45 sockets on the S-60 E front panel.

Important: Through-connecting the signal ground lines of RS-data interfaces is mandatory, as is proper grounding. See also the section on pin assignments later in this chapter.

4.3 Startup

After startup, the DC LED will light and the network indicator lights go through an on/off sequence.

The power DC LED should always be lit. The link and No Video lights eventually glow upon establishing of a good network link and the absence of an input video signal, respectively.

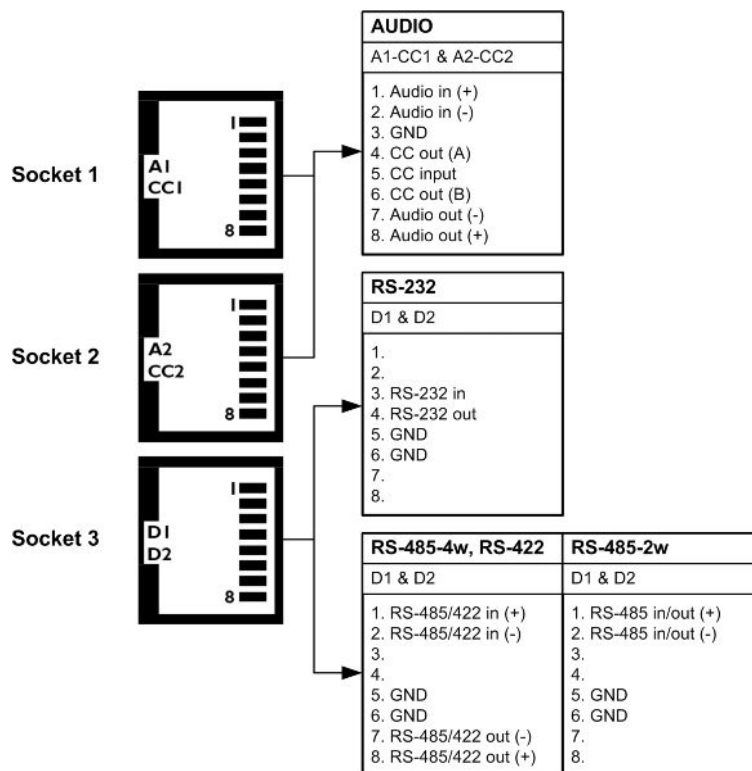
The sync LED displays as described in the *Front Panel* section.

Important: Before you can make any signal connection, you must assign at least a valid IP address (the unit's identity for the network) and a subnet mask to the unit. The *Connect the unit* chapter explains how to do this.

4.4 Connector pin assignments

Modular socket pin assignments

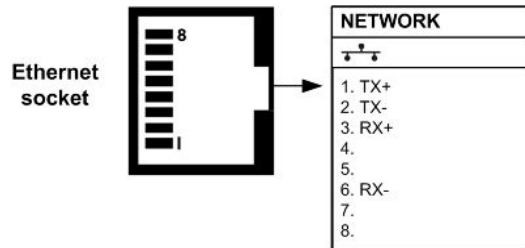
The modular socket pin assignments are such that similar sockets of different modules may be connected back to back with reversed cable (RS-232 interfaces excepted). See the figure below for the socket pin numbering convention used. For 2-wire RS-485 links, I/O is through pins 1 and 2 of socket 3.



Pin assignments of the three modular sockets. For 2-wire RS-485 use pins 1 and 2 of socket 3.

Note: Polarity indications for RS-422/485 are based on a convention used by BT, which may conflict with other implementations. Pelco systems, for example, use an implementation for which you have to connect TKH Security (+) to Pelco (-) and vice versa.

Ethernet connector pin assignment



Ethernet connector socket pinning

4.5 Update device definitions

If the S-60 E is not supported by the TKH Security application software on your host PC you can download EMX updates and MX Plug-in updates at www.tkhsecurity.com/support-files. Install the EMX update first if you are performing both update types.

Note: There is no need to install these updates if you do not use MX applications.

- **EMX updates**
Install the EMX update. The Embedded MX network driver will be updated with the latest changes.
- **MX Plug-in updates**
The updater will update the shared copy of device definitions used by Ethernet-based MX applications. An existing installation of the SNM Configuration and Service Tool will also be updated.

5 Connect the unit

With your S-60 E installed, the next step is to establish an IP connection and set up video and (if applicable) other signal links. This chapter describes how you can change the factory-set IP address and subnet mask of the S-60 E to make them compatible with the network segment in which the unit will be used. It also discusses how to configure signal streaming.

In This Chapter

- 5.1 Establish a network connection..... 18
- 5.2 Establish video and other signal connections.....20

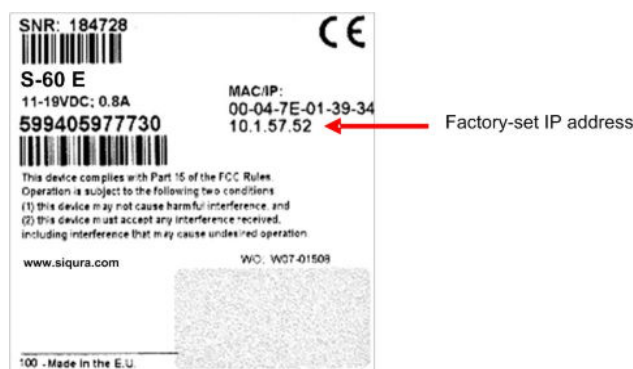
5.1 Establish a network connection

The webpages of the S-60 E provide a convenient way of accessing its settings. You can log on to the web interface of the S-60 E from a PC which is on the same subnet as the unit. Follow the steps below to open communication with the S-60 E and configure its network settings.

- Step 1: Set the network adapter of the PC to the factory-set subnet of the S-60 E and then connect the two devices to the network.
- Step 2: Access the unit from a web browser or other tool installed on the PC.
- Step 3: Set the IP address and subnet mask of the S-60 E to the subnet that it is going to be used in and reboot the unit.

To address the unit from the same PC again, configure the network adapter of the PC once more to assign the PC to the same subnet as the unit.

The factory-set IP address of the S-60 E is in the 10.x.x.x range. You will find it printed on a sticker on the unit.



S-60 E product sticker

Note: This is the address the unit reverts to if you issue a "Reset to factory settings; incl. network settings" command and reboot the unit (see chapter *Device Management*).

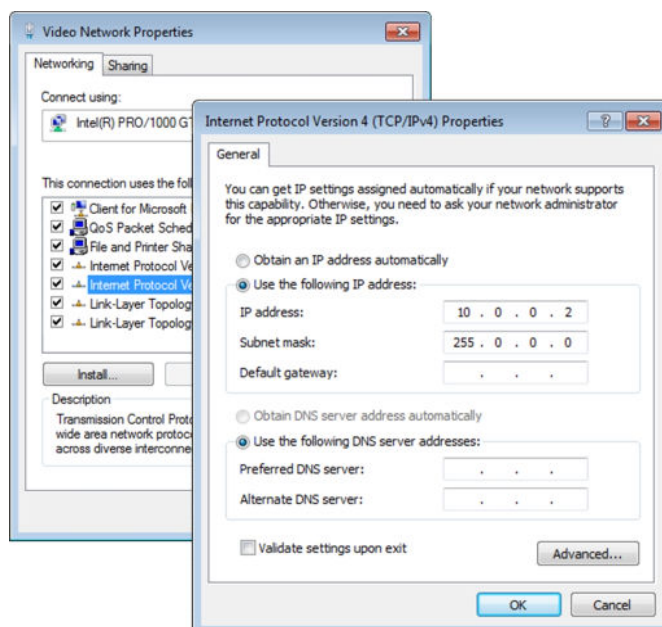
Step 1: Set the PC to the factory-set subnet of the unit

» To configure the network adapter on the PC

- 1 In Control Panel, open **Network and Sharing Center**.
- 2 Select the connection to be configured, and then click **Properties**.
- 3 On the items list, select **Internet Protocol Version 4 (TCP/IPv4)**.
- 4 Click **Properties**.
- 5 In the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box, click **Use the following IP address**.
- 6 Enter an IP address which assigns your PC to the same subnet as the S-60 E - that is, within the 10.x.x.x range. Use 255.0.0.0 as a subnet mask.

Important: To prevent conflicts, be sure to choose a unique IP address. No two devices on a network can have the same IP address.

- 7 To apply the new settings, click **OK**.



Setting the IP settings of the PC to the factory-set IP settings of the unit

At this point, connect your PC to the S-60 E. You can connect them directly using a crossover cable, or connect both to a switch.

Step 2: Access the unit

Using a standard web browser you can now log on to the web server of the S-60 E.

Step 3: Change the network settings of the unit

The Network page enables you to make the network addressing of the unit compatible with the network it will be added to. You can set a fixed IP address or have the IP address assigned by a DHCP server. In the latter case, open the Advanced Settings and enable DHCP. Do not forget to save and reboot the unit after changing the settings.

5.2 Establish video and other signal connections

Connection methods

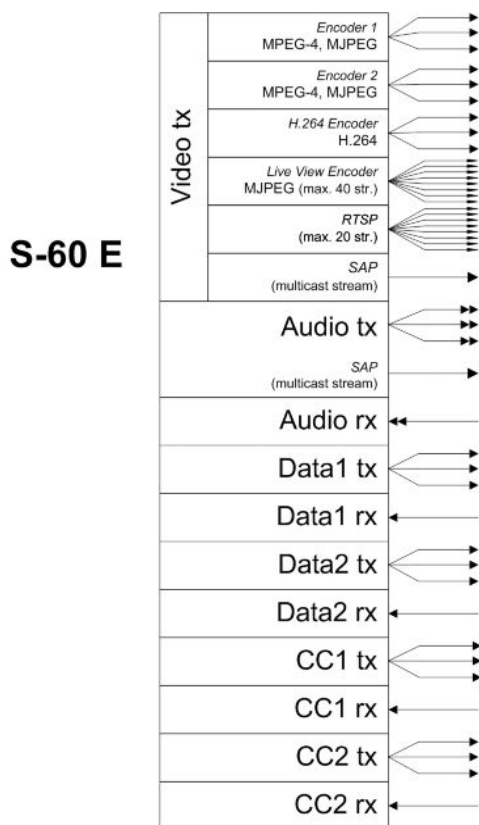
With the IP connection established, video and other signal connections can be made. The easiest way to connect with video and audio is by using RTSP or SAP. For more information, see the *Interfaces* chapter.

An alternative, convenient method to establish video, audio, data, and contact closure (I/O contacts) connections is to use the webpages of the S-60 E. For detailed information, see the chapters which describe these pages.

Separate application software, such as MX Configuration Tool, can be used as well.

Streams and connectors

Each signal stream transmitted and received by the S-60 E (see the figure below) can be conceived of as using virtual connectors (transmitters and receivers) on the network side. Each of the virtual connectors has a name. Through the internal webpages, the receivers can be assigned a port number which must be used only once for that particular device. Depending on context, the assignment is automatic or manual. Note that port numbers must be even.



Link facilities of the S-60 E.

All arrows represent separate and independent connections over Ethernet.

The abbreviations 'tx' and 'rx' refer to the network side of the module.

- tx: the stream is transmitted to the network

- rx: the stream is received from the network

General procedure for making links

In both connection methods mentioned above, perform the following steps to make a unicast one-way link (video, audio, data, contact closure) from source to destination.

- In the transmitter, specify a destination IP address and a destination port number.
- In a compatible receiver, specify the transmitter IP address (source) and the local input port number (= the destination port number mentioned above).
- Do not forget to enable both the transmitter and the receiver.

It is possible for external software to configure a stream, for instance a video stream or a contact closure stream to transmit a contact closure alarm. In such cases, port numbers are assigned automatically from a range of unused values.

For more information on port number assignment, see *Port Numbers*.

5.2.1 Port numbers

A valid UDP port number in a TKH Security A-, C-, and S-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

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

6 Interfaces

A variety of methods can be employed to communicate with the S-60 E. This chapter outlines the interfaces you can use to control the unit and manage the media streams it is handling.

In This Chapter

6.1 ONVIF.....	22
6.2 OSA.....	22
6.3 Web UI.....	22
6.4 MX/IP.....	23
6.5 SNMP.....	23
6.6 SAP.....	23
6.7 NTCIP.....	23

6.1 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 S-60 E fully supports ONVIF. It has been tested to support ONVIF Profile S.

6.2 OSA

TKH Security'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. OSA enables easy integration of the S-60 E with third-party products. The protocol consists mainly of different CGI (Common Gateway Interface) program calls for listing and configuring parameters. A detailed description of the HTTP API is given in the *SPI* specification which can be downloaded at www.tkhsecurity.com/support-files.

6.3 Web UI

Using the S-60 E's web server is the most straightforward way to access the unit. The webpages enable you to configure the settings of the S-60 E and view live video images from a standard web browser.

6.4 MX/IP

MX/IP is a proprietary TKH Security protocol which gives direct access to the settings of the S-60 E. Using special MX software, such as *MX Configuration Tool*, S-60 E settings can be read from and written to the *Management Information Base (MIB)*, a list of variables stored inside the unit. Offering full control of the S-60 E, the MIB enables you to remotely configure device settings and manage media streams. Additional MX viewing and control software offers real-time monitoring of video streams and playback of recorded images. For more information about MX/IP, the MIB, and the EMX network service, refer to the manuals which document the MX SDK and the MX applications.

Note: If you prefer using open standards, you can disable the MX/IP protocol. This is done on the MX tab of the Device Management page. Be aware that doing so prevents you from upgrading the S-60 E firmware through *MX Firmware Upgrade Tool*.

6.5 SNMP

The Simple Network Management Protocol (SNMP), part of the internet protocol suite, can be used to monitor network devices such as the S-60 E for conditions or events that require administrative attention. For more information, refer to appropriate literature on SNMP.

The S-60 E supports in-band SNMP. Via SNMP, several status variables can be read and traps can be generated on events. You can configure S-60 E SNMP settings on the SNMP tab of the Device Management page.

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

Note: The S-60 E 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.tkhsecurity.com/support-files.

6.6 SAP

The S-60 E supports the Session Announcement Protocol (SAP), a protocol used for broadcasting multicast session information. A SAP listening application can listen to the announcements advertised by the S-60 E SAP announcer. The application can use this information to receive a video or audio stream that the S-60 E is transmitting to the advertised multicast address. For more information, see the description of the Video and Audio pages.

6.7 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 S-60 E 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 S-60 E, see *Appendix: NTCIP Configuration*.

The S-60 E 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.

7 Stream media via RTSP

The easiest way to extract a video or audio stream from the S-60 E is to use the Real-Time Streaming Protocol (RTSP). This chapter explains the role of the S-60 E in RTSP media sessions and describes how to open a media stream from the unit in a video player plug-in.

In This Chapter

7.1 RTSP and RTP.....	25
7.2 Transfer via UDP or TCP.....	26

7.1 RTSP and RTP

The S-60 E 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 S-60 E 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>

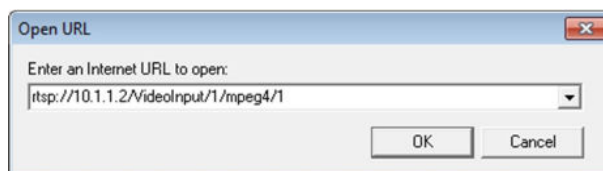
where:

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

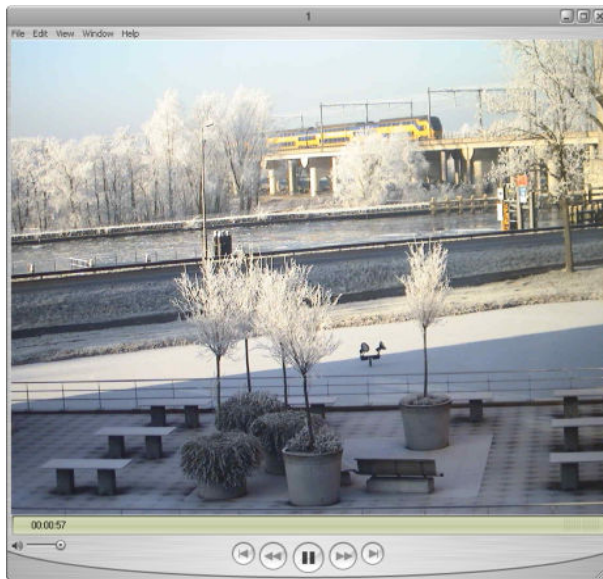
Note: The <RTSP Port> is optional. If not entered, port 554 is used by default.

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 S-60 E video stream viewed in QuickTime

7.2 Transfer via UDP or TCP

The S-60 E supports the following types of streaming.

- UDP/IP (multicast and/or unicast)
- TCP/IP (RTP, RTP over RTSP, RTP over RTSP over HTTP)

The S-60 E 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 S-60 E media streams through HTTP and RTSP, refer to the *SPI* specification. You can download this HTTP API specification at www.tkhsecurity.com/support-files.

8 Access the webpages

The webpages of the S-60 E offer a user-friendly interface for configuring its settings and viewing live video over the network. This chapter explains how to connect to the web interface of the unit.

In This Chapter

- 8.1 System requirements..... 27
- 8.2 Connect via web browser..... 27
- 8.3 Find the unit with Device Manager.....28
- 8.4 Connect via UPnP.....29
- 8.5 Log on to the unit..... 29

8.1 System requirements

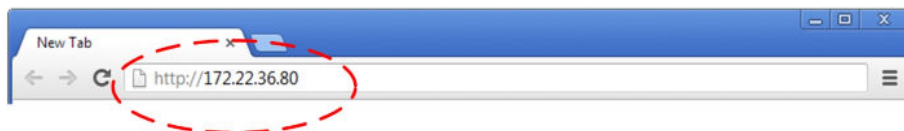
To access the webpages of the S-60 E you need the following.

- A PC with a web browser installed.
- An IP connection between the PC and the S-60 E.

8.2 Connect via web browser

» To connect to the unit via your web browser

- 1 Open your web browser.
- 2 Type the IP address of the S-60 E in the address bar, and then press ENTER.
 If your network configuration is correct you are directed to the login page of the unit.
 If the page is not displayed correctly, make sure that JavaScript is enabled in your web browser (see *Appendix: Enable JavaScript*).



Type the IP address of the S-60 E in the address bar of the browser

8.3 Find the unit with Device Manager

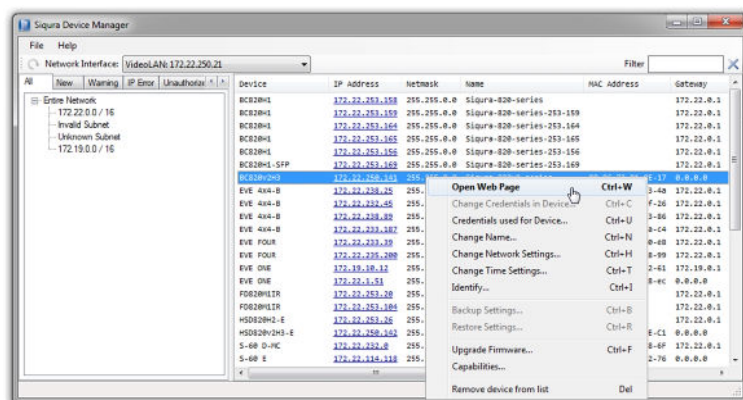
Device Manager is a Windows-based software tool that you can use to manage and configure TKH Security IP cameras and video encoders. The tool automatically locates these devices and offers you an intuitive interface to set and manage network settings, configure devices, show device status, and perform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

►► To install Device Manager

- 1 Download the latest version of Device Manager at www.tkhsecurity.com/support-files.
- 2 Double-click the setup file.
- 3 Follow the installation steps to install the software.

►► To connect to the unit via Device Manager

- 1 Start Device Manager
The network is scanned and detected devices appear in the *List View* pane.
- 2 If multiple network adapters exist, select the appropriate adapter to scan the network that you wish to connect to.
- 3 To refresh the *List view* pane, click the **Rescan now** button.
- 4 Use the tabs in the *Tree View* pane to define the scope of your search.
- 5 Click the column headings in the *List View* pane to sort devices by type, IP address, or name.
- 6 Use the *Filter* box, to search for a specific series or model.
- 7 To connect to the webpages of the S-60 E, double-click its entry in the device list, - or -
Right-click the entry, and then click **Open Web Page**.
The login page of the S-60 E is opened in your web browser.



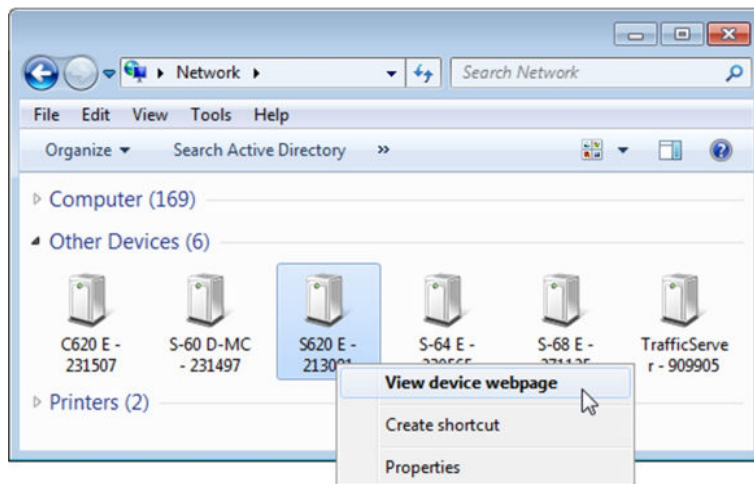
Connect to a device via Device Manager

8.4 Connect via UPnP

Universal Plug and Play (UPnP) support is enabled by default on the S-60 E. With the UPnP service enabled in Windows (see *Appendix: Enable UPnP in Windows*), you can access the unit from Windows Explorer.

» To connect to the unit via UPnP

- 1 In Windows Explorer, open the **Network** folder.
Detected devices in the same subnet as the computer are displayed, including TKH Security codecs and cameras with UPnP support.
- 2 Double-click the S-60 E,
- or -
Right-click the unit, and then click **View device webpage**.
The login page of the S-60 E is opened in your web browser.



Connect to a device via Windows Explorer

For more information about UPnP, see *Auto Discovery (Device Management chapter)*.

8.5 Log on to the unit

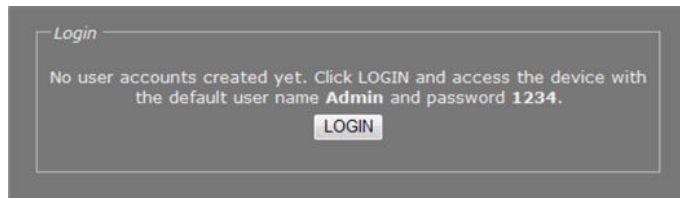
Users with a valid account for the S-60 E can log on to the unit.

» To log on to the S-60 E

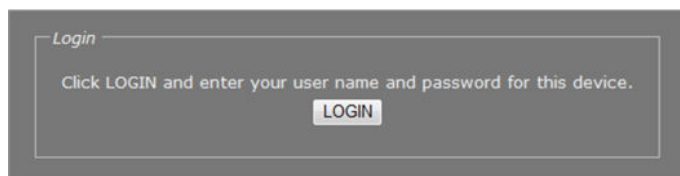
- 1 On the Login page, click **LOGIN**.
- 2 Log on with the account that was created for you.
User name and password are case sensitive.
The default user name set at the factory for the S-60 E is "Admin" with password "1234".

Note: To prevent unauthorised access from people using the default account, we recommend that the administrator changes the default password after first login and creates separate user accounts as needed. This also removes the default account details from the login screen.

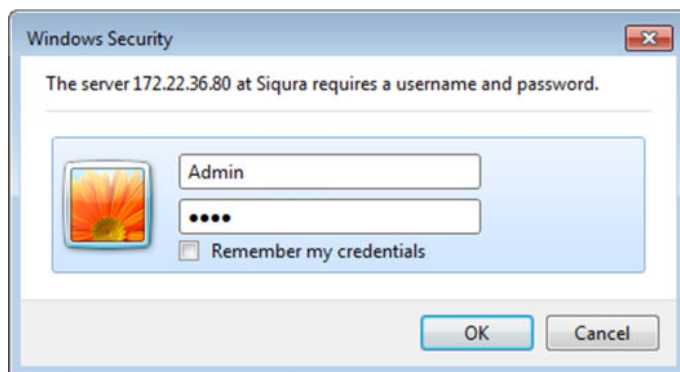
- 3 Click **OK** or press ENTER.
On successful login, the Live Video page appears.



Access possible with default Admin account only (default Admin password unchanged)



Access possible with the user account created for you (default Admin password has been changed)



Connect dialogue box

Note: The appearance of the S-60 E webpages and dialogue boxes is determined by the operating system and web browser used on the host PC. Therefore, some of the screenshots in this manual may slightly differ from what you actually see on your screen.

9 Navigate the webpages

This chapter introduces the webpages and common elements found on them. It also discusses user account types and associated access levels.

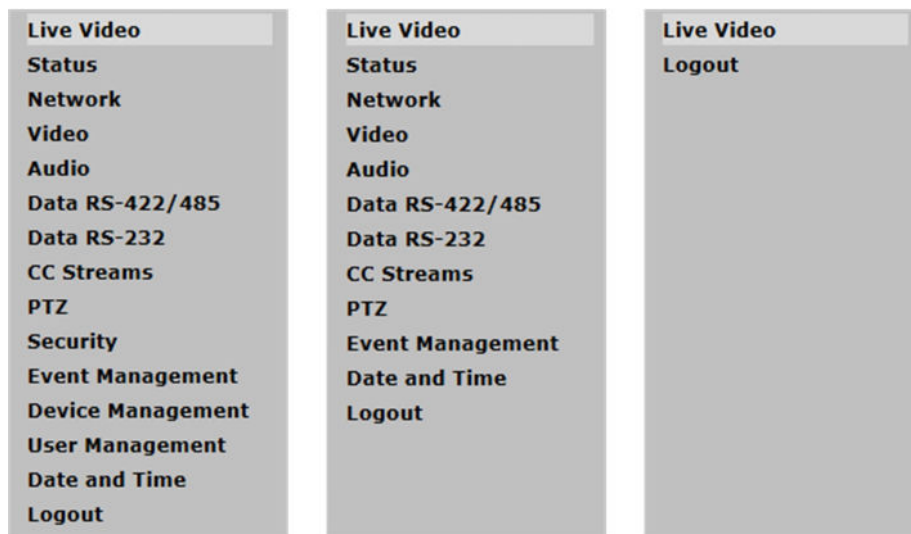
In This Chapter

9.1 Menu.....	31
9.2 Access control.....	31
9.3 Webpage elements.....	32

9.1 Menu

Use the menu on the left of each webpage to go to the other pages.

- Click the option associated with the user or device settings you want to view or configure.
- Click **Live Video** to reopen the home page of the S-60 E.
- Click **Logout** to log out the current user and display the Login box.



S-60 E menus available to (from left to right) Admin, Operator, and Viewer accounts

9.2 Access control



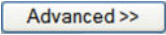
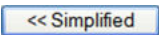
Whether a specific S-60 E webpage is available to you on the navigation menu depends on the user account you logged in with. The unit supports three account types with associated access levels.

Account	User rights
Admin	Full access to all pages. Create, edit, and delete user accounts on User Management page.
Operator	Access to device configuration pages. No access to Device Management, User Management, and Security.
Viewer	Home page only. View live video.

9.3 Webpage elements

Apart from the menu, the webpages share the following features.

- **Sections** are used to organise parameters and their values.
- **Buttons** (see below) appear in sections with editable fields.
- **Tabs** are used to organise page content.
- **Check boxes** enable you to select features.

This Button	Does This	Note
	Writes changes to the unit.	Some sections (for example, those on the VMD tab of the Video page) do not have <i>Save</i> and <i>Cancel</i> buttons. Changes you make here are immediately written to the device.
	Undoes unsaved changes and shows values as they were before editing.	
	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 S-60 E. If in doubt, do <i>not</i> change the default values.
	Closes the Advanced Settings section.	

10 View live video via browser

On the Live Video page, you can view live video from a video source which is connected to the S-60 E. From this page, you can also control a connected PTZ camera if the camera supports the PTZ driver selected on the PTZ page of the S-60 E.

In This Chapter

10.1 Activate Live View.....	33
10.2 View live video.....	34
10.3 Use your browser for PTZ control.....	35

10.1 Activate Live View



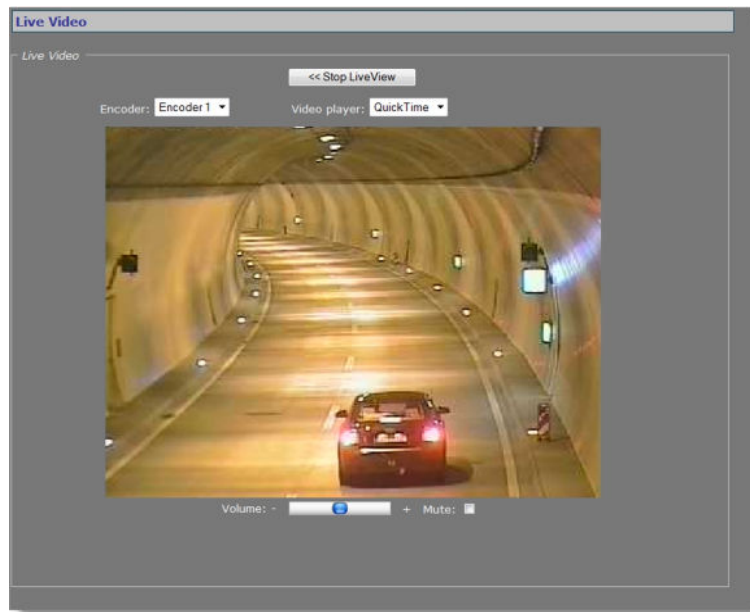
Live View inactive

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

» To activate Live View

- Click **Play LiveView>>**.

10.2 View live video



Live View activated

With Live View enabled, the Live Video page has the following items.

Item	Description
<<Stop Live View	Closes the preview.
Encoder	<p><i>Encoder 1</i></p> <hr/> <p><i>Encoder 2</i></p> <hr/> <p><i>H.264 - 1</i></p> <hr/> <p><i>Live View</i></p>
Video player	<p><i>QuickTime</i></p> <hr/> <p><i>VLC</i></p> <hr/> <p><i>No Player</i></p>
Refresh rate	Available in Live View encoder mode. Indicates the current refresh rate of the webpage.
Preview	Shows live images from the video source as encoded by the selected encoder. MPEG-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 1/2 and H.264 - 1 mode. Move the slider to control audio volume.
Mute	Available in Encoder 1/2 and H.264 - 1 mode. Select/clear this box to mute/unmute audio.

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.

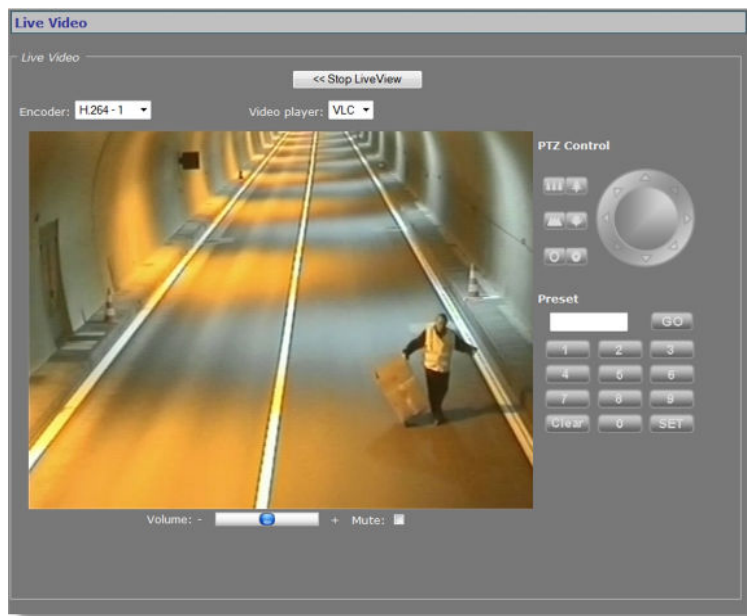
Enable audio

If the audio controls are not available in Encoder 1/2 or H.264 - 1 mode, go to the Audio page and make sure that audio is enabled and properly configured.



Audio Disabled warning

10.3 Use your browser for PTZ control



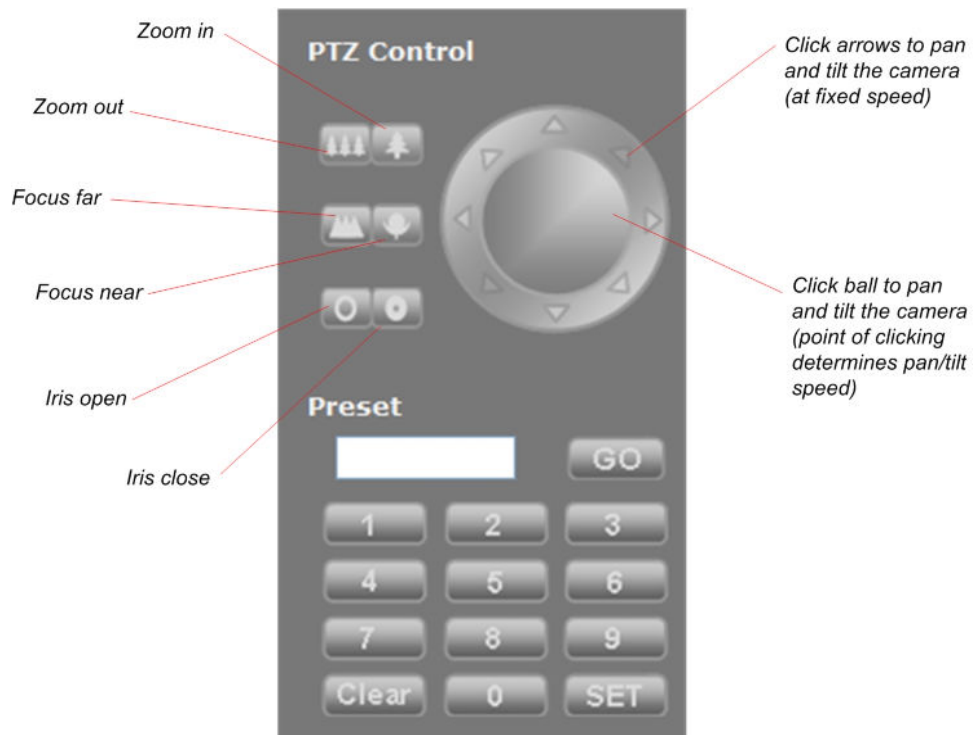
Live Video page with PTZ Control panel

Display the PTZ Control panel

With a PTZ driver selected on the PTZ page, the PTZ Control panel is visible to the right of the preview on the Live Video page. If the PTZ camera connected to the S-60 E supports the selected driver you can use the panel to control the camera and manage its presets. PTZ drivers not included in the driver list on the PTZ page can be uploaded to the S-60 E 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.

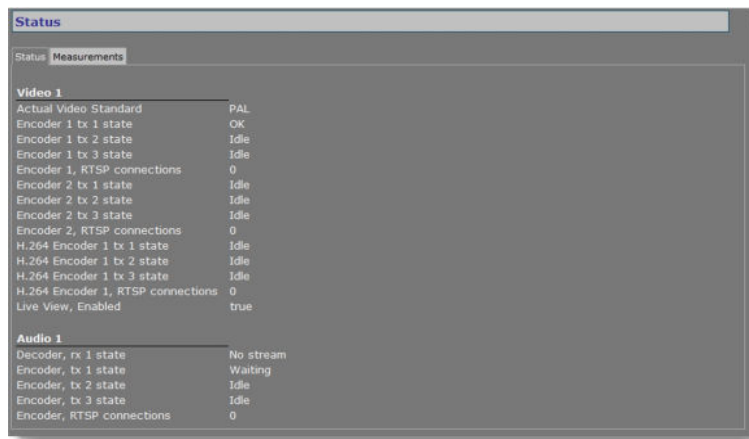
11 Status

The status information and measurements on the Status page may provide helpful clues to identify and troubleshoot technical issues.

In This Chapter

11.1 View status information.....	37
11.2 View measurements data.....	38

11.1 View status information



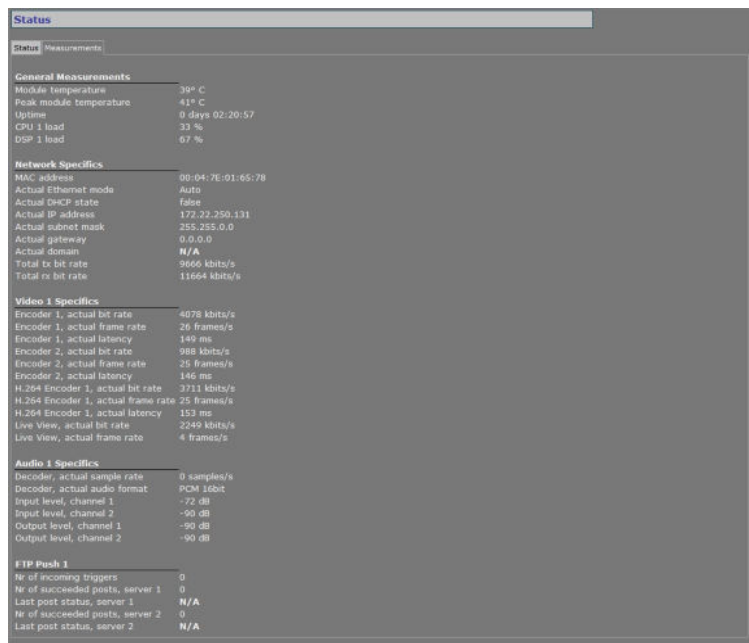
Status: a snapshot of the system state with automatic updating

11.1.1 Stream states

The Status tab provides information on the stream states of video and audio streams.

Stream state	Description
OK	There is nothing wrong with the stream. Note that if the video signal is removed from the video input on the encoder side, the Decoder rx state is still reported as <i>OK</i> , since the video transmitter is sending a stream - that is, a <i>No Video</i> image - to the decoder.
Idle	The transmitter/receiver is not enabled.
Waiting	The transmitter/receiver has lost its stream connection. Possible causes: <ul style="list-style-type: none"> • An incorrect port number. • The transmitter on the encoder side is not enabled. • No FloodGuard packets have been received for more than three seconds. For details on the FloodGuard flooding prevention mechanism, see the note on FloodGuard in the Video chapter.

11.2 View measurements data



Status > Measurements

11.2.1 General, network, and stream 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.

11.2.2 FTP Push

You can use the FTP Push data to monitor the FTP Push process.

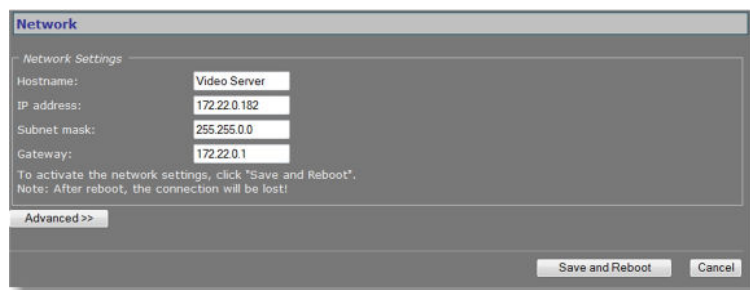
12 Network

On the Network page, you can change the network settings of the S-60 E. In this chapter, you 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

12.1 Network settings.....	39
12.2 Advanced.....	40

12.1 Network settings



Network page

In the Network Settings section, you can set the name of the unit, the IP address, the subnet mask, and the gateway IP address. For correct functioning of the S-60 E, 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 S-60 E; for details, see chapter Connections. 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 IP address of the unit:

- 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 values on record, otherwise management of the unit will require special software.

12.2 Advanced



Network > Advanced

12.2.1 Services

Item	Description
RTSP server enable	Select this check box to enable the S-60 E 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.

12.2.2 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.	
	<i>Auto</i>	Autonegotiation (default).
	<i>10 HDX</i>	Half duplex, 10 Mbit.
	<i>10 FDX</i>	Full duplex, 10 Mbit.
	<i>100 HDX</i>	Half duplex, 100 Mbit.
<i>100 FDX</i>	Full duplex, 100 Mbit.	
MTU size	Set to Ethernet (1500) by default. Maximum Transmission Unit (MTU) is the maximum size (in bytes) of an 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.	

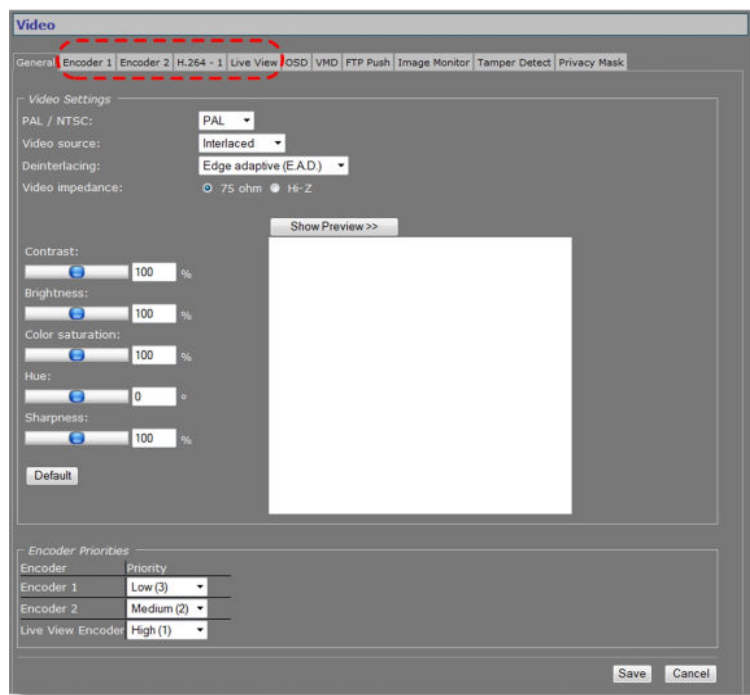
13 Video

On the Video page, you can configure settings for video encoding, on-screen display, video motion detection, FTP push, image quality, tamper detect, and privacy masks.

In This Chapter

- 13.1 Video encoding overview..... 41
- 13.2 General.....42
- 13.3 Encoder #..... 44
- 13.4 H.264 - 1..... 60
- 13.5 Live View..... 68
- 13.6 OSD..... 70
- 13.7 VMD..... 75
- 13.8 FTP Push..... 80
- 13.9 Image Monitor..... 84
- 13.10 Tamper Detect..... 90
- 13.11 Privacy Mask.....97

13.1 Video encoding overview



Video encoder tabs on the Video page

Video encoding

The S-60 E's separate video encoders - that is, Encoder 1, Encoder 2, and H.264 - 1, can convert the analogue video input signal into independent digital video streams with different resolutions and frame rates. Encoders 1 and 2 can both handle MPEG-4 and MJPEG encoding.

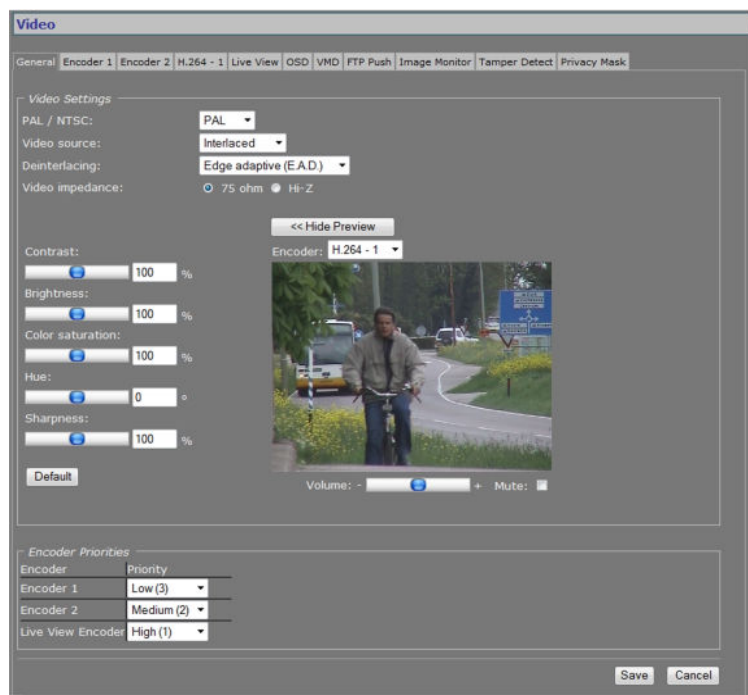
Multistreaming

Up to twenty streams can be retrieved using RTSP. A total of nine copies – three per independent MPEG-4, MJPEG, or H.264 video stream – can be transmitted to different unicast and/or multicast destinations using TKH Security's proprietary MX protocol. The S-60 E supports source-specific multicast (SSM) and it is also possible to use the Session Announcement Protocol (SAP) to transmit MPEG-2/-4/MJPEG and H.264 streams to multicast destinations.

Live View encoder

The Live View encoder can convert the analogue video input signal to (M)JPEG 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.

13.2 General



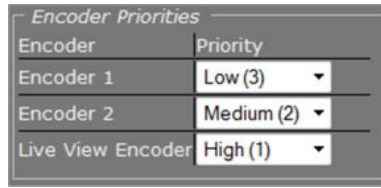
Video > General

Settings on the General tab apply to all encoders.

13.2.1 Video Settings

Item	Description	
PAL / NTSC	<i>Auto, PAL, or NTSC.</i> The video display standard.	
Video source	<i>Interlaced</i>	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. It is recommended to deinterlace (see below) interlaced video if you are planning to watch it on a progressive display, such as a computer monitor.
	<i>Progressive</i>	Progressive scan captures the entire image in one go. Images from progressive sources do not need deinterlacing, therefore. Selecting <i>Progressive</i> dims the <i>Deinterlacing</i> list.
Deinterlacing	<i>Off</i>	No deinterlacing performed.
	<i>Motion adaptive (M.A.D.)</i>	This technology creates new pixels through interpolation in areas of motion and uses pixels from the next field where there is no motion. This is generally the best setting for reducing artefacts in images with moving objects.
	<i>Edge adaptive (E.A.D.)</i>	Pixels are interpolated along edges to remove the appearance of jagged edges. This is the recommended setting for making snapshots for face recognition purposes, for example.
Note: The best option is to experiment with the two deinterlacing methods to achieve the highest quality image possible for your application.		
Video impedance	<i>75 Ohm or Hi-Z.</i> Resistance to flow of signal current. With one video source on one video input, select <i>75 Ohm</i> . With a number of video inputs in parallel using one video source, use <i>Hi-Z</i> on all inputs except the last.	
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	<i>Encoder 1, Encoder 2, or H.264 - 1.</i> List displayed on clicking Show Preview>>. Allows to select a video encoder to handle the images seen in the preview.	
Volume	Available in Encoder 1/2 and H.264 - 1 mode. Move the slider to control audio volume.	
Mute	Available in Encoder 1/2 and H.264 - 1 mode. Select/clear this box to mute/unmute audio.	
Contrast, Brightness, Color saturation, Hue, Sharpness	Move the slider or type a value to adjust the setting aided by the visual feedback from the preview. A setting entered here applies to all video encoders.	
Default	Restores the original values.	

13.2.2 Encoder Priorities

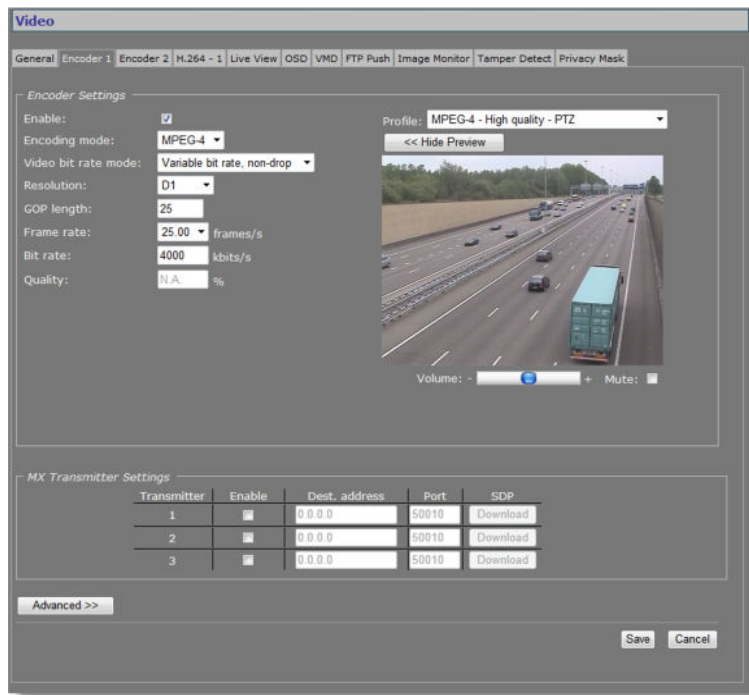


Priority list

Using the Encoder Priorities list, you can assign a priority to Encoders 1 and 2, and the Live View encoder. H.264 encoding uses a dedicated digital chip and is therefore not included in the list. Each priority can be assigned once. The encoder with high priority consumes all CPU power it needs, leaving the remainder, if any, to the next in line. The encoder with medium priority will show the same behaviour, possibly leaving little or no CPU power to the low-priority encoder.

Important: The highest priority is best assigned to the Live View encoder, because this is a relatively light task compared to the encoding tasks of Encoder 1 and Encoder 2.

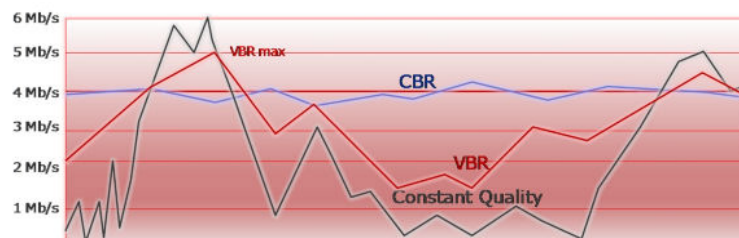
13.3 Encoder



Video > Encoder 1

13.3.1 Encoder Settings

Item	Description
Enable	All encoders are enabled by default. Use this check box to disable/re-enable this specific encoder.
Encoding mode	<p><i>MPEG-4</i> or <i>MJPEG</i></p> <p>The method used to compress the analog video input signal.</p> <p>The S-60 E can stream (M)JPEG over UDP and HTTP.</p> <ul style="list-style-type: none"> To enable and configure UDP/MJPEG streaming, select MJPEG from the Encoding mode list and configure settings. To transport JPEG over HTTP and/or to 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	<p>Controls variations in bit rates. For more information, see "Notes" later in this chapter.</p> <p>MPEG-4 encoding mode supports the following bit rate modes.</p> <p><i>Constant quality</i> 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.</p> <p><i>Variable bit rate</i> Variable network load, but limited to value set for the <i>VBR maximum bit rate</i> parameter in the Advanced Settings section. The frame rate will suffer when the <i>VBR maximum bit rate</i> is reached.</p> <p><i>Variable bit rate, non-drop</i> Variable network load, but limited to value set for the <i>VBR maximum bit rate</i> parameter in the Advanced Settings section. The quality will decrease when the <i>VBR maximum bit rate</i> is reached. The frame rate will be constant.</p> <p><i>Constant bit rate</i> Keeps network load constant at the cost of varying image quality. Frames may be skipped.</p> <p><i>Constant bit rate, non-drop</i> Keeps network load constant at the cost of varying image quality. Frames are never skipped.</p>



MJPEG encoding mode supports the following bit rate modes.

Item	Description																								
	<p><i>Constant quality</i> Keeps the image quality constant, with varying network load (from a few kb/s to 10 Mb/s or higher). The quality is determined by the value set for the <i>Quality</i> parameter (see below).</p> <p><i>Constant bit rate</i> Keeps network load constant at the cost of varying image quality. Frames may be skipped.</p>																								
Resolution	<p>The following resolutions are supported.</p> <table border="1"> <thead> <tr> <th>resolution (h x v)</th> <th>PAL</th> <th>NTSC</th> </tr> </thead> <tbody> <tr> <td>D1</td> <td>720x576</td> <td>720x480</td> </tr> <tr> <td>2/3 D1</td> <td>480x576</td> <td>480x480</td> </tr> <tr> <td>1/2 D1</td> <td>352x576</td> <td>352x480</td> </tr> <tr> <td>4CIF</td> <td>704x576</td> <td>704x480</td> </tr> <tr> <td>2CIF</td> <td>720x288</td> <td>720x240</td> </tr> <tr> <td>CIF (top field only)</td> <td>352x288</td> <td>352x240</td> </tr> <tr> <td>QCIF</td> <td>176x144</td> <td>176x120</td> </tr> </tbody> </table> <p>VGA (640x480) and QVGA (320x240) are also supported.</p> <p>For more information about CIF resolutions, see "Notes" later in this chapter.</p> <div style="border: 1px solid black; padding: 5px;"> <p>Note: The S-60 E will simultaneously H.264 encoding and dual MPEG-4 encoding at full frame rate, and Live View encoding at 5 frames per second. Setting Encoders 1 and 2 to perform MPEG-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.</p> </div>	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
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																							
GOP length	Available in MPEG-4 mode. Distance in frames between two I-frames.																								
Frame rate	Selectable rates are determined by the video mode (PAL, NTSC) set on the General tab. PAL: 1-25 fps; NTSC: 1-30 fps.																								
Bit rate	Range: [10...15000]. Selecting a profile (see below), automatically sets the bit rate associated with the profile.																								
Quality	Available in MJPEG mode. 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	Move the slider to control audio volume.																								
Mute	Select/clear this box to mute/unmute audio.																								

13.3.2 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.

13.3.3 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.

13.3.4 Make a video connection

Creating a video link between a video encoder and a video decoder involves two steps:

- Configuring settings of the encoder
- Configuring settings of the decoder

» To configure the encoder settings

- 1 Open the webpages of the encoder, go to the Video page, and then open the appropriate Encoder tab.
- 2 In the MX Transmitter Settings section, specify the destination IP address.
This is the address of the video decoder which will receive the video stream.
- 3 Enter the port number of the decoder.
For more information about port numbers, see the *Port Numbers* section.
- 4 Select **Enable**, and then click **Save**.

MX Transmitter Settings				
Transmitter	Enable	Dest. address	Port	SDP
1	<input checked="" type="checkbox"/>	172.22.250.132	50010	Download
2	<input type="checkbox"/>	0.0.0.0	50010	Download
3	<input type="checkbox"/>	0.0.0.0	50010	Download

*Video Transmitter Settings (encoder side).
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 settings

- 1 Open the webpages of the decoder, go to the Video page, and select the Decoder tab.
- 2 In the MX Receiver Settings section, specify the source IP address.
This is the address of the video encoder which will transmit the video stream.
- 3 Enter the port number of the decoder.
For more information on port numbers, see the *Port Numbers* section.
- 4 Select **Enable**, and then click **Save**.

Receiver Settings			
Receiver	Enable	Source address	Port
1	<input checked="" type="checkbox"/>	172.22.250.131	50010

*Video Receiver Settings (decoder side).
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 is 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 analogue output signal.

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

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.

SDP download

Use the SDP Download button to download a Session Description Protocol (SDP) file from the encoder. SDP files contain streaming media initialisation parameters and properties. An SDP file does not deliver media itself but through file association the media stream can be opened in media players such as QuickTime and VLC. You can also use the SDP file to specify the URI in your web browser.

13.3.5

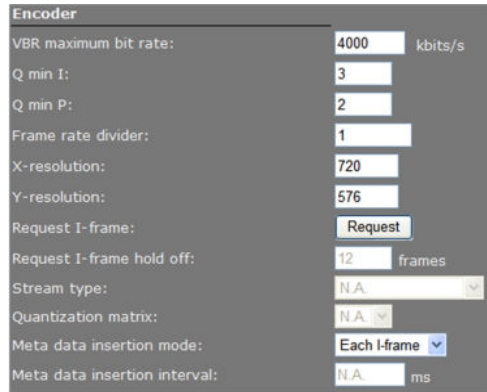
Advanced

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

13.3.5.1 Encoder

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

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.
	<i>Disabled</i> No meta data added to stream.
	<i>Fixed interval</i> Not supported for MPEG-4 streams. If a fixed interval is set, the nearest I-frame will be used.
	<i>Each I-frame</i> 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 <i>Meta data insertion mode</i> (above) to <i>Fixed interval</i> .

MJPEG mode

Encoder	
VBR maximum bit rate:	7200 kbits/s
Q min I:	N.A.
Q min P:	N.A.
Frame rate divider:	1
X-resolution:	720
Y-resolution:	576
Request I-frame:	Request
Request I-frame hold off:	12 frames
Stream type:	N.A.
Quantization matrix:	N.A.
Meta data insertion mode:	N.A.
Meta data insertion interval:	N.A. ms

Video > Encoder # > Advanced > Encoder (MJPEG mode)

Item	Description
VBR maximum bit rate	Range: [0...15000]. Sets a limit for variable bit rate.
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	

13.3.5.2 Stream Manager

Stream Manager	
Stream bandwidth limit:	4692 kbit/s
Keep-alive interval:	100 ms
Low latency:	<input type="checkbox"/>

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	<p>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.</p> <p>You are advised to limit the outgoing bit rate per encoder to a maximum of 15 Mbit/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.</p> <p>The Stream bandwidth limit mechanism is disabled when Low latency (see below) is selected. See also the graphic in the Note on FloodGuard.</p>
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 <i>Low latency</i> disables the <i>Stream bandwidth limit</i> 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).

13.3.5.3 Transmitter

The screenshot shows the configuration for Transmitter 1 with the following settings:

- DSCP field: 0
- Connection priority: 0
- Multicast TTL: 10
- RTP control mode: FloodGuard
- Stream type: UDP + RTP + NKF
- RTP type: 0
- Link loss alarm timeout: 10 s

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 (see - 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.	
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.	
	<i>None</i>	No transport protocol selected.
	<i>FloodGuard</i>	Flooding prevention mechanism. For more information, see the note on FloodGuard later in this chapter.
Stream type	<i>UDP + RTP</i>	Default setting. Plain RTP stream over UDP.
	<i>UDP + RTP + NKF</i>	Adds an extended RTP header for TKH Security 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.	

13.3.5.4 RTSP Transmitter

RTSP Transmitter

DSCP field:

Enable multicast:

Default multicast IP address: Invalid multicast address

Default multicast port:

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 (see - 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 <i>Default multicast IP address</i> text box. The RTSP transmitter itself does not require enabling.
Default multicast IP address	Select <i>Enable multicast</i> (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.

13.3.5.5 SAP Settings

Video > Encoder # > Advanced > SAP Settings

SAP announcer

The S-60 E includes a SAP announcer. The Session Announcement Protocol is used to advertise that a media stream generated by the S-60 E is available at a specific multicast address and port.

The S-60 E can send SAP multicast streams for its H.264, MPEG-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.

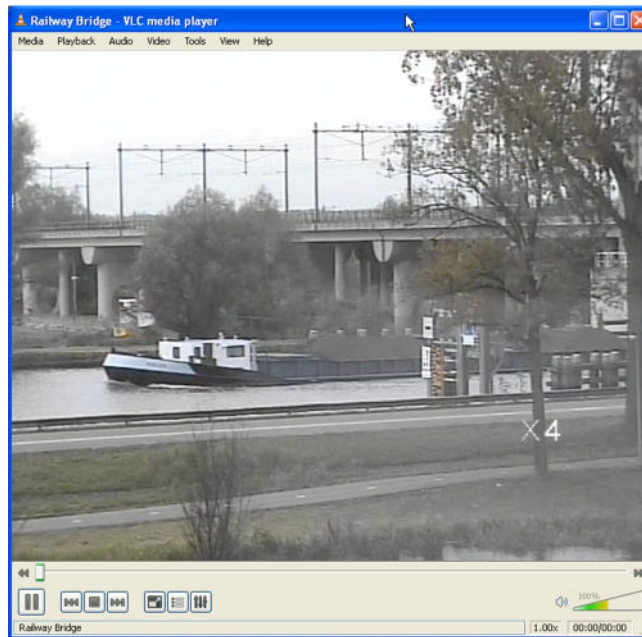
Item	Description
Enable SAP	When selected, session announcements are sent at the frequency determined by the Announcement interval parameter and the media stream is transmitted to the multicast IP address specified in the Stream dest. IP address box.
Stream name	Enter a descriptive name to identify the 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	<i>Global</i> , the default session scope, sets the <i>Multicast IP range</i> 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 <i>Administrative</i> 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 Settings	
Enable SAP:	<input checked="" type="checkbox"/>
Stream name:	Railway Bridge
Stream dest. IP:	224.2.255.249
Stream dest. port:	1024
Stream DSCP field:	0
Multicast TTL:	255
Announcement interval:	10 s
Session scope:	Global
Multicast IP range:	224.2.128.0 - 224.2.255.255

SAP example settings



S-60 E SAP network stream opened via VLC Playlist

13.3.6 Meta data insertion

Enabling

All S-60 E 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 TKH Security 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	Reserved for 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	Reserved for 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 the SPI 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.

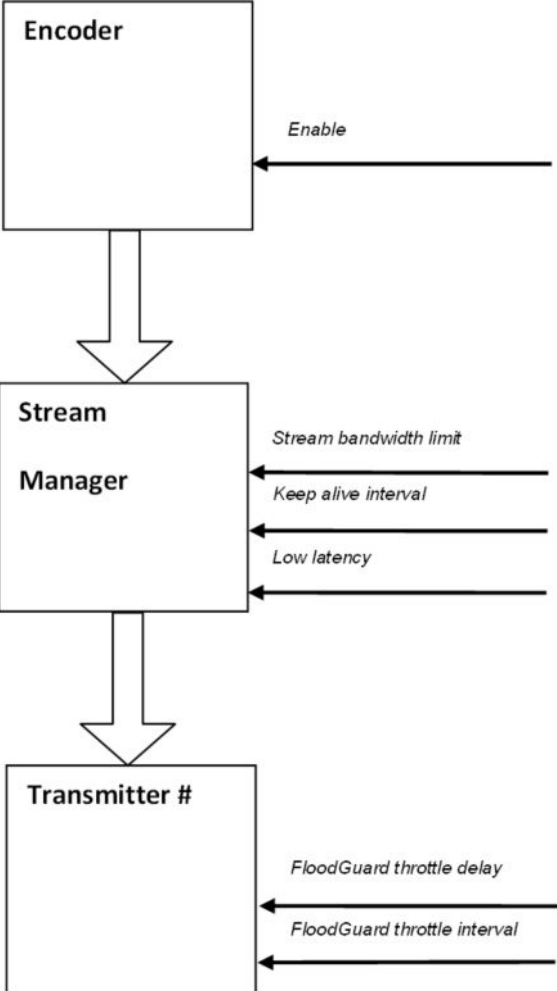
13.3.7 Notes

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.

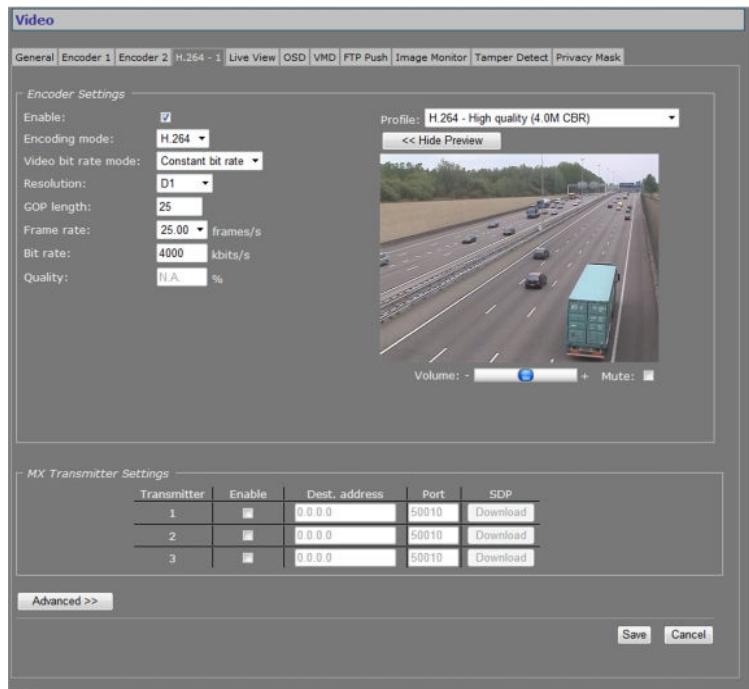
Note on the Session Announcement Protocol (SAP): SAP, defined in RFC 2974 (see RFC 2974 - <http://www.ietf.org/rfc/rfc2974.txt>), is a protocol for advertising multicast session information. A SAP announcer periodically broadcasts announcement packets which include the session description information 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 TKH Security 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

13.4 H.264 - 1



Video > H.264 - 1

13.4.1 Encoder Settings

Item	Description	
Enable	All encoders are enabled by default. Use this check box to disable/re-enable this specific encoder.	
Encoding mode	<i>H.264.</i>	
Video bit rate mode	Controls variations in bit rates. For a concise explanation, see "Note on Encoder Settings".	
	H.264 encoding mode supports the following bit rate modes.	
	<i>Constant quality</i>	Keeps the image quality constant, with varying network load. See <i>Constant Quality Mode (CQM) configuration</i> (below) for TKH Security's recommended strategy for controlling image quality.
	<i>Constant bit rate</i>	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
	<i>D1</i>	720x576 720x480
	<i>2/3 D1</i>	480x576 480x480
	<i>1/2 D1</i>	352x576 352x480
	<i>2CIF</i>	720x288 720x240
	<i>4CIF</i>	704x576 704x480
	<i>CIF (top field only)</i>	352x288 352x240
	<i>QCIF</i>	176x144 176x120
	VGA (640x480) and QVGA (320x240) are also supported. For more information on CIF resolutions, see below.	
	Note: The S-60 E will simultaneously handle H.264 encoding and dual MPEG-4 encoding at full frame rate, and Live View encoding at 5 frames per second. Setting Encoders 1 and 2 to perform MPEG-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.	
GOP length	Distance in frames between two I-frames.	
Frame rate	Selectable rates are determined by the video mode (PAL, NTSC) set on the General tab. PAL: 1-25 fps; NTSC: 1-30 fps.	
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 <i>Quality</i> setting.

Item	Description
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	Move the slider to control audio volume.
Mute	Select/clear this box to mute/unmute audio.

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.

13.4.2 Constant Quality Mode configuration

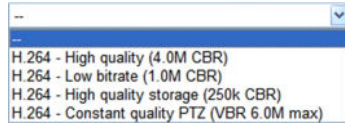
Constant Quality mode (CQM) can be used in situations with intermittent increases of movement in camera images. This mode provides better pictures when quickly panning a PTZ camera, for example. TKH Security recommends the following strategy for Constant Quality mode configuration.

» 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.

13.4.3 Profiles

To facilitate the configuration of H.264 encoding settings, the Profile list offers a number of profiles - that is, combinations of settings for specific purposes.



H.264 Profile list

The following table lists parameter settings for each profile.

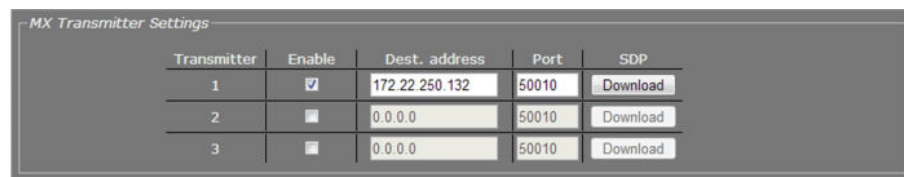
Profile	Settings
H.264 - High quality - Camera (4.0M CBR)	Max bit rate: n/a Bit rate: 4000 kbit/s Mode: Constant bit rate Quality: n/a Resolution: D1 GOP: 25 Frame rate divider: 1 Stream bandwidth limit: 20000 kbit/s
H.264 - Low bit rate - Camera (1.0M CBR)	Max bit rate: n/a Bit rate: 1000 kbit/s Mode: Constant bit rate Quality: n/a Resolution: D1 GOP: 25 Frame rate divider: 1 Stream bandwidth limit: 20000 kbit/s
H.264 - High quality - Storage (250K CBR)	Max bit rate: n/a Bit rate: 250 kbit/s Mode: Constant bit rate Quality: n/a Resolution: 2 CIF GOP: 25 Frame rate divider: 2 Stream bandwidth limit: 20000 kbit/s
H.264 - High quality - PTZ (VBR 6.0M max)	Max bit rate: 6000 kbit/s Bit rate: n/a Mode: Constant quality Quality: 70 Resolution: D1 GOP: 25 Frame rate divider: 1 Stream bandwidth limit: 20000 kbit/s

13.4.4 Parameter value combinations

Set sensible combinations of video bit rate mode, resolution, GOP length, and frame and bit rates. When you set and save these values, 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.

13.4.5 MX Transmitter Settings and making video connections



Transmitter	Enable	Dest. address	Port	SDP
1	<input checked="" type="checkbox"/>	172.22.250.132	50010	Download
2	<input type="checkbox"/>	0.0.0.0	50010	Download
3	<input type="checkbox"/>	0.0.0.0	50010	Download

MX Transmitter Settings: destination address can be unicast or multicast

» To make a video connection

- 1 Per stream, set the destination IP addresses and port numbers (even).
- 2 Enable the stream, as shown in the figure above.
These settings, in combination with decoder settings, can serve to make links. If in an H.264 video decoder a source IP address and port number corresponding to a multicast address have been set, or if it holds the encoder IP address and the destination port number, a video link is established if the stream for that destination is enabled - that is, the box in the 'Enable' column is selected.
- 3 To save the changes, click **Save**.

SDP download

Use the SDP Download button to download a Session Description Protocol (SDP) file from the encoder. SDP files contain streaming media initialisation parameters and properties. An SDP file does not deliver media itself but through file association the media stream can be opened in media players such as QuickTime and VLC. You can also use the SDP file to specify the URI in your web browser.

13.4.6 Advanced

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

13.4.6.1 Encoder

Encoder	
CQM max bit rate:	6000 kbits/s
Frame rate divider:	1
X-resolution:	720
Y-resolution:	576
Request I-frame:	Request
Request I-frame hold off:	12 frames
Scene change detect:	<input type="checkbox"/>
Scene change detect period:	N.A. ms
Force frame mode:	<input type="checkbox"/>
Deblocking filter:	<input checked="" type="checkbox"/>
Deblocking filter alpha coefficient:	0
Deblocking filter beta coefficient:	0
Meta data insertion mode:	Each I-frame
Meta data insertion interval:	N.A. ms

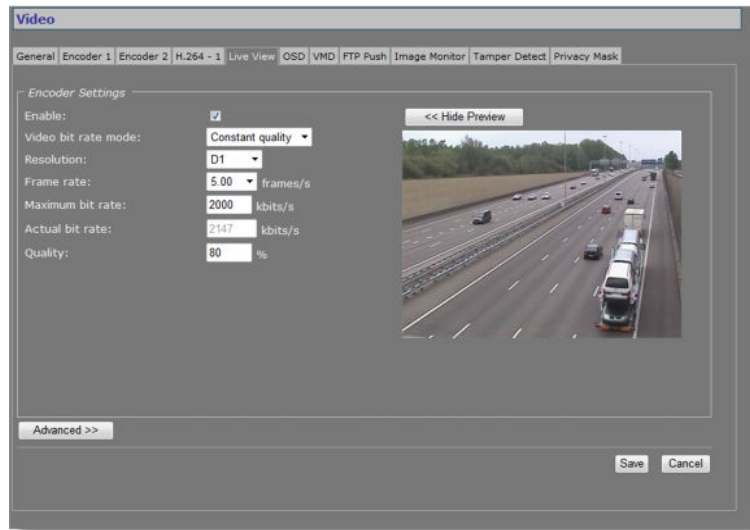
Video > H.264 > Advanced > Encoder

Item	Description						
CQM max bit rate	Available in <i>Constant quality</i> 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 Y-resolution	Variables that enable you to freely set picture resolution instead of using the resolution presets in the Encoder Settings section.						
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 <i>Force frame mode</i> 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							
Meta data insertion mode	Determines the method used to add meta data to the stream. For details, see the section on Meta Data Insertion. <table border="1" data-bbox="566 1630 1401 1854"> <tbody> <tr> <td><i>Disabled</i></td> <td>No meta data added to the stream.</td> </tr> <tr> <td><i>Fixed interval</i></td> <td>Activates <i>Meta data insertion interval</i> parameter.</td> </tr> <tr> <td><i>Each I-frame</i></td> <td>Data block is added after each I-frame. The interval is determined by the GOP length, therefore.</td> </tr> </tbody> </table>	<i>Disabled</i>	No meta data added to the stream.	<i>Fixed interval</i>	Activates <i>Meta data insertion interval</i> parameter.	<i>Each I-frame</i>	Data block is added after each I-frame. The interval is determined by the GOP length, therefore.
<i>Disabled</i>	No meta data added to the stream.						
<i>Fixed interval</i>	Activates <i>Meta data insertion interval</i> parameter.						
<i>Each I-frame</i>	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 <i>Meta data insertion mode</i> (see above) to <i>Fixed interval</i> .						

13.4.6.2 Stream Manager, Transmitter #, RTSP Transmitter, and SAP

Configuring Stream Manager, Transmitter #, RTSP Transmitter, and SAP settings for H.264 encoding is done in the same way as for Encoders 1 and 2. For more information, see the description of the Advanced Settings for these encoders.

13.5 Live View



Video > Live View

13.5.1 (M)JPEG output

The S-60 E provides multiple (M)JPEG output methods.

- To transport JPEG over **HTTP** and/or to use the Live View previews in the webpages, 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.

13.5.2 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	<i>Constant quality</i>	Keeps the image quality constant, with varying network load. The quality is determined by the value set for the <i>Quality</i> parameter (see below).
	<i>Constant bit rate</i>	Keeps network load constant at the cost of varying image quality. Frames may be skipped.
Resolution Frame rate (Maximum) bit rate	Set sensible combinations of mode, resolution, frame rate and (maximum) bit rate. It is advised to limit MJPEG encoding to 5 fps when the S-60 E is also handling MPEG-4 encoding with 1xD1 and 1xCIF or 2CIF at full frame rate.	
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 <i>Quality</i> 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.	

13.5.3 Advanced

Advanced Settings

Frame rate divider:

X-resolution:

Y-resolution:

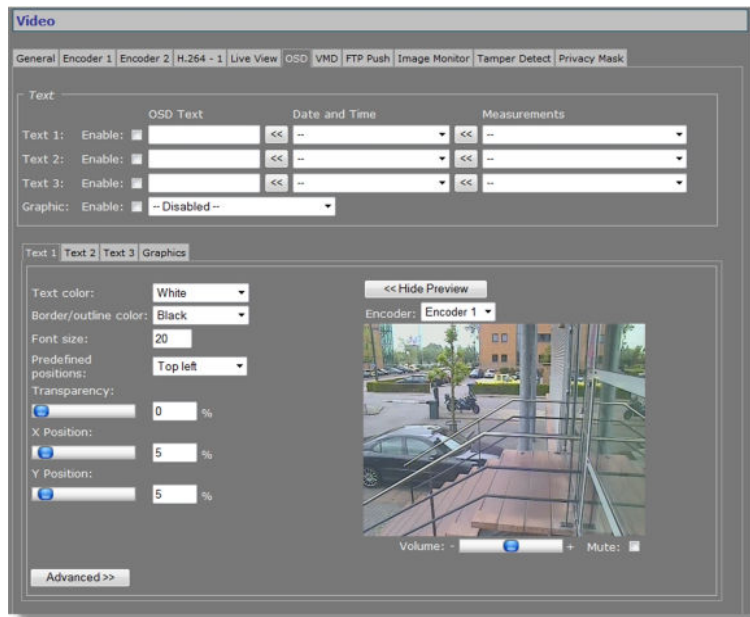
Meta data insertion mode: ▾

Meta data insertion interval: ms

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.	
	<i>Disabled</i>	No meta data added to the stream.
	<i>Fixed interval</i>	Activates <i>Meta data insertion interval</i> parameter.
	<i>Each frame</i>	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 <i>Meta data insertion mode</i> (see above) to <i>Fixed interval</i> .	

13.6 OSD



Video > OSD

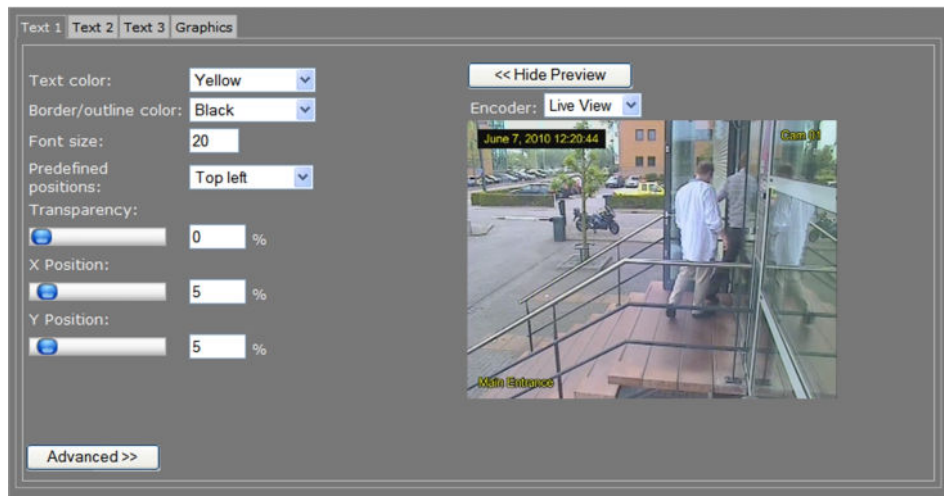
13.6.1 OSD facilities

The S-60 E 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.

13.6.2 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.

13.6.3 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	Move the slider or type 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 <i>Predefined positions</i> 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.

13.6.3.1 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	<i>Outline</i> or <i>Border</i> .
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

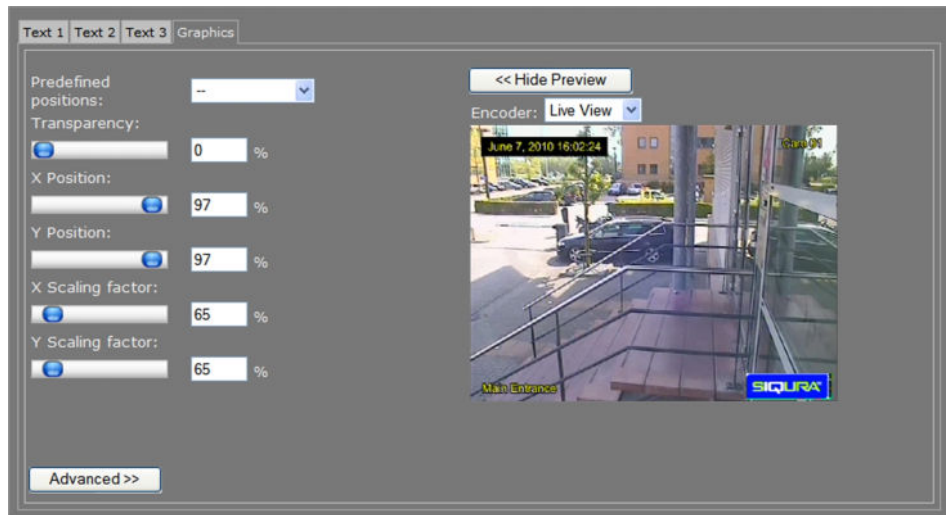
» To upload a font

- 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.

13.6.4 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.

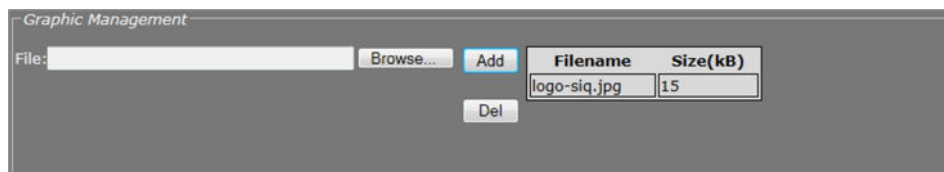
Item	Description
Predefined positions	Presets for positioning the OSD object.
Transparency	Move the slider or type a percentage.
X-Position	Variables that enable you to freely position the object, instead of using the presets. Drag the sliding buttons or enter a percentage. When a preset has been selected, changing one of its defined parameters sets the <i>Predefined positions</i> 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.

13.6.4.1 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

You can upload your own graphics with a maximum file size of 100 kB to the S-60 E. If necessary, use a picture resize tool to reduce the file size.

» To upload a graphic

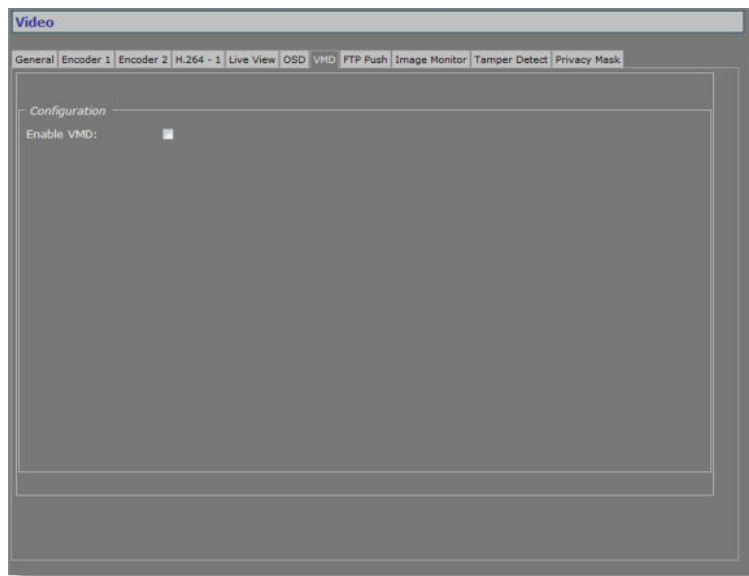
- 1 In the *Graphic Management* section, click **Browse**.
The *Open* dialog box displays.

- 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**.

13.7 VMD



Video > VMD (disabled)

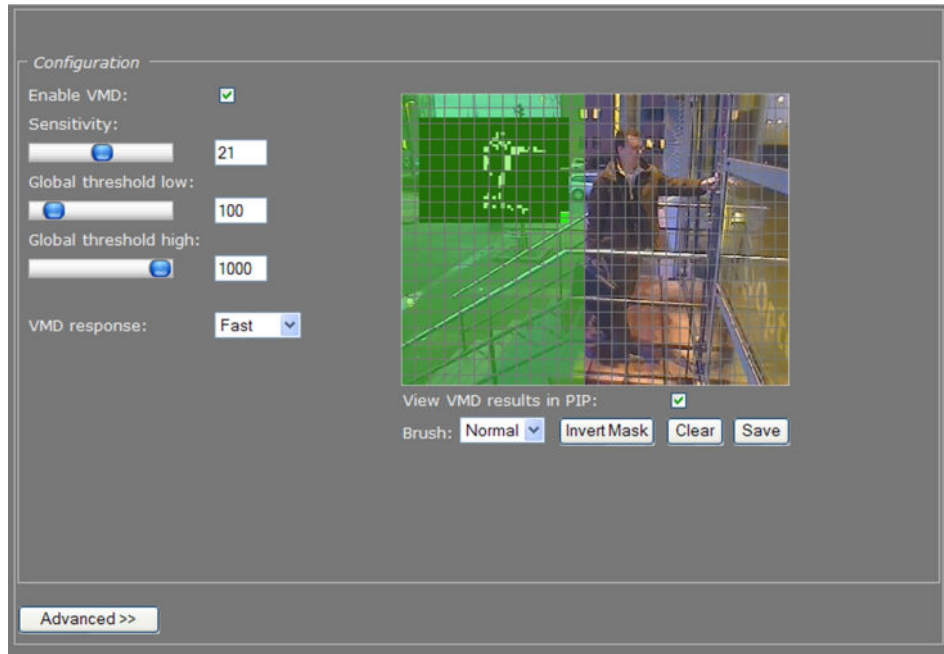
Video Motion Detection (VMD) enables the user to define a portion or portions of the screen and to detect picture changes there. These changes could be caused by motion or varying lighting, for example. Regions of less interest can be masked.

13.7.1 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.

13.7.2 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	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 TKH Security software.
Global threshold high	
VMD response	<i>Fast</i> or <i>Filtered</i> . Filtering is used to suppress a single peak as false triggering.

13.7.3 Set the mask

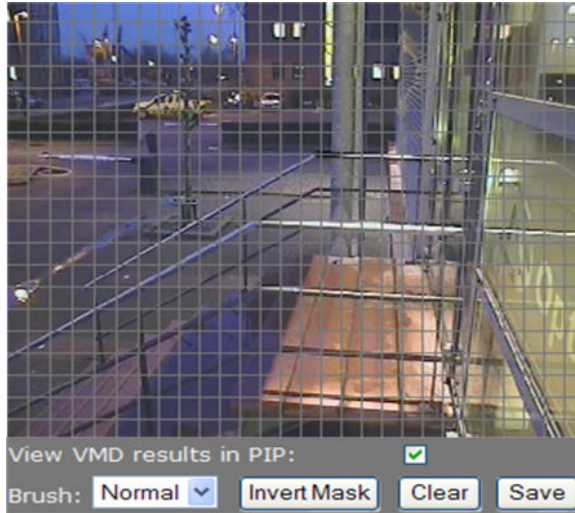
» To set a mask

- 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.

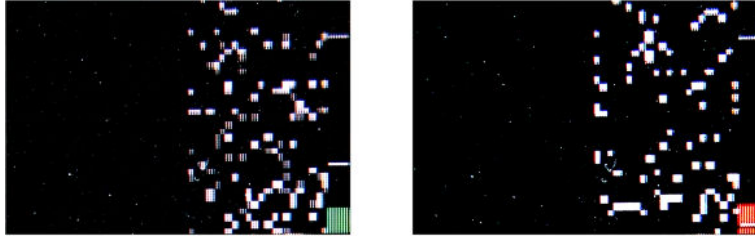


Masking grid

Item	Description	
Brush	<i>Normal</i>	Allows grid elements to be accessed in 4-element groups.
	<i>Large</i>	Allows grid elements to be accessed in 16-element groups.
	<i>Small</i>	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 <i>do</i> 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.	

13.7.4 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.

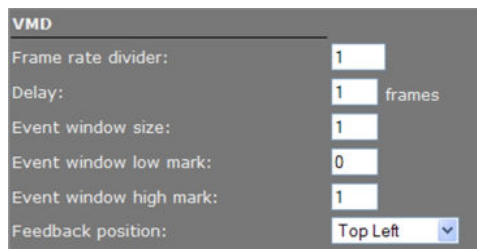


VMD detection windows, with mask applied to the left half of the window. The small white blocks indicate grid elements where change occurred above the sensitivity level. The summed change is reflected in the bars on the right, the green one (left) not reaching the lower threshold. The red one (right picture) extending past it, since this threshold is set much lower.

13.7.5 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.

13.7.6 Advanced

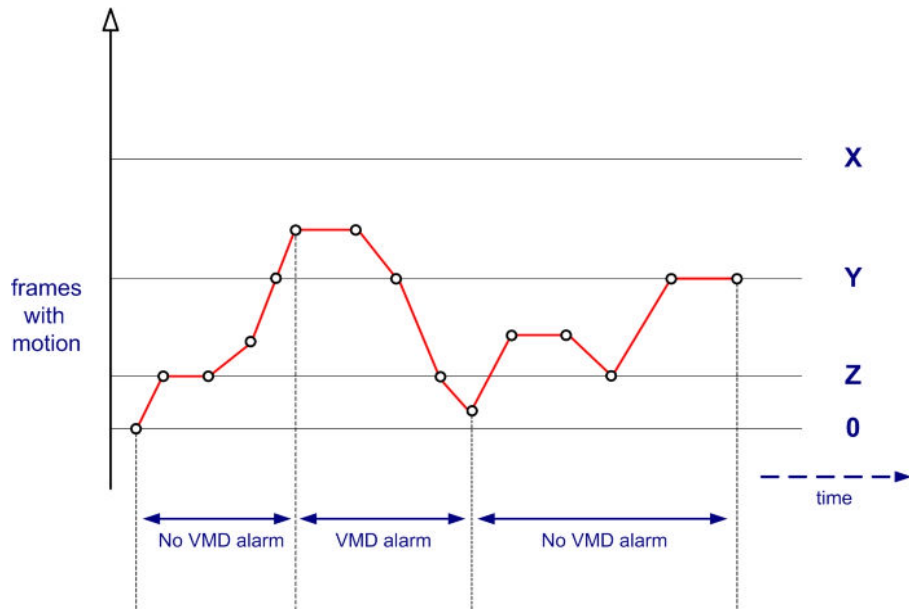


Video > VMD > Advanced > VMD

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

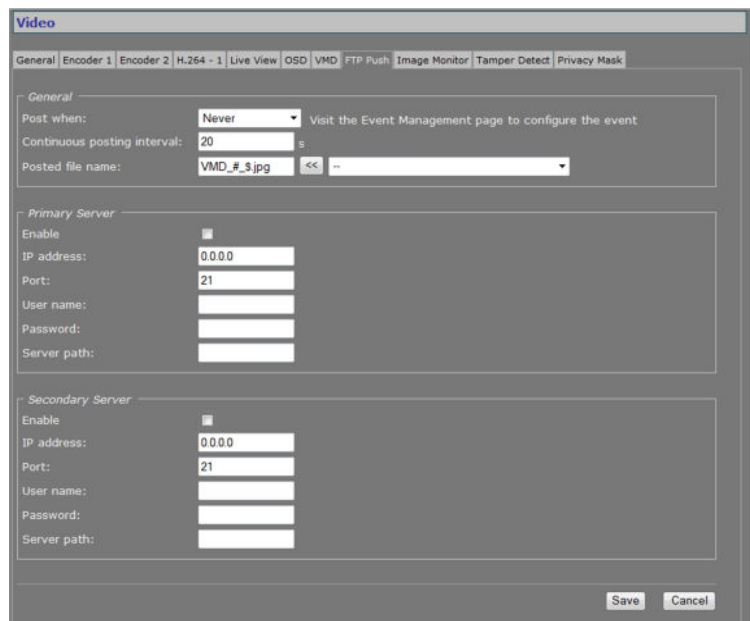
Y = Event window high mark

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.

13.8 FTP Push



Video > FTP Push

13.8.1 Post JPEG images

The S-60 E 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.

13.8.2 General

Item	Description	
Post when	<i>Never</i>	No image posting
	<i>Event On</i>	Image is posted when configured event occurs.
	<i>Event Off</i>	Image is posted when configured event ceases.
	<i>Event Changed</i>	Images are posted when configured event occurs or ceases.
	<i>Continuous</i>	Posting not associated with any event. Images are sent continuously at the frequency set for the <i>Continuous posting interval</i> 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".

13.8.3 FTP server

A target FTP server must hold a user account associated with the S-60 E. 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.

13.8.4 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.

13.8.5 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

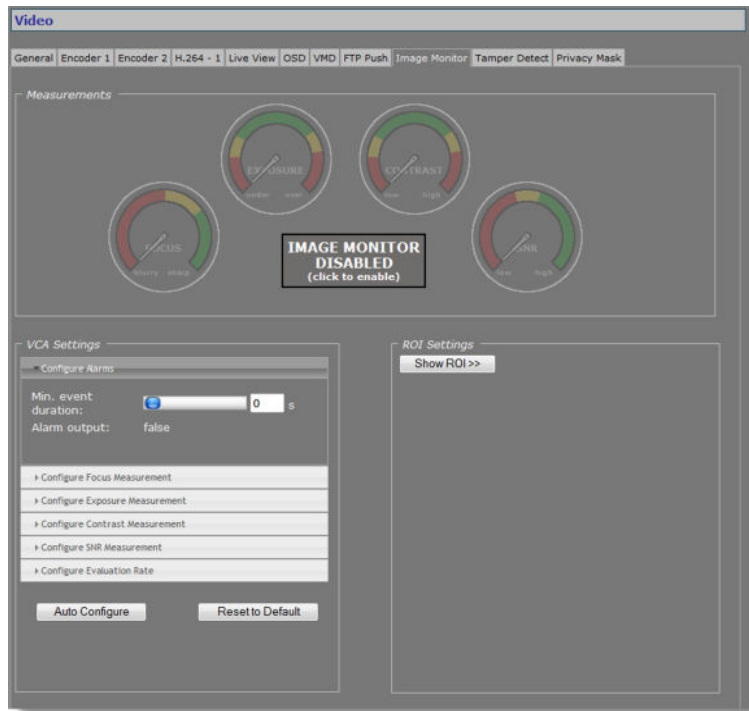
Status > Measurements > FTP Push 1

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
Last post status, server 1	ftpput: unexpected server 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

13.9 Image Monitor



Video > Image Monitor

13.9.1 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.

13.9.2 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.

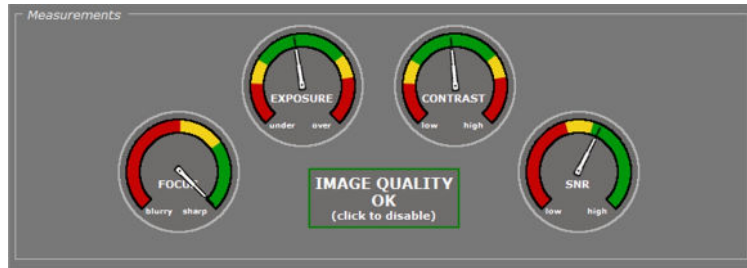


Image Monitor: all measurements enabled

» 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.

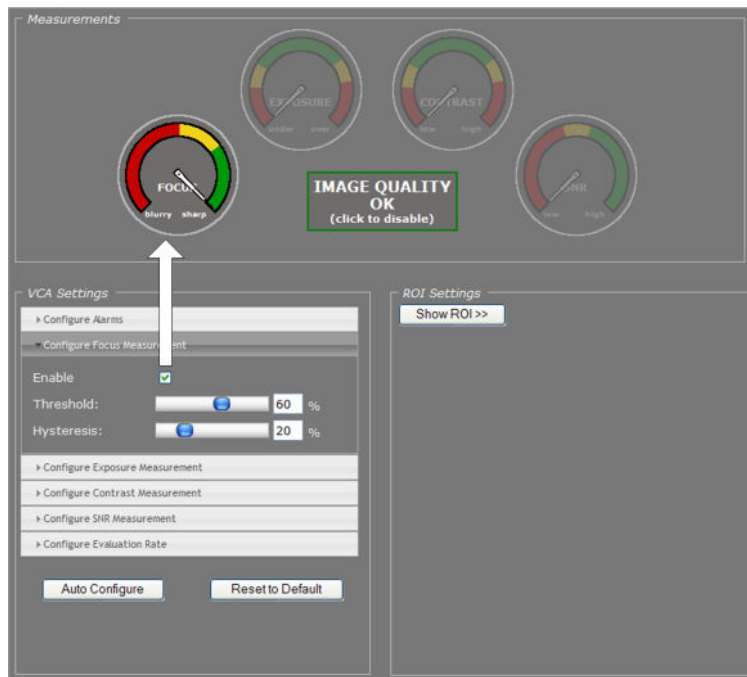


Image Monitor: FOCUS measurement enabled only

13.9.3 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



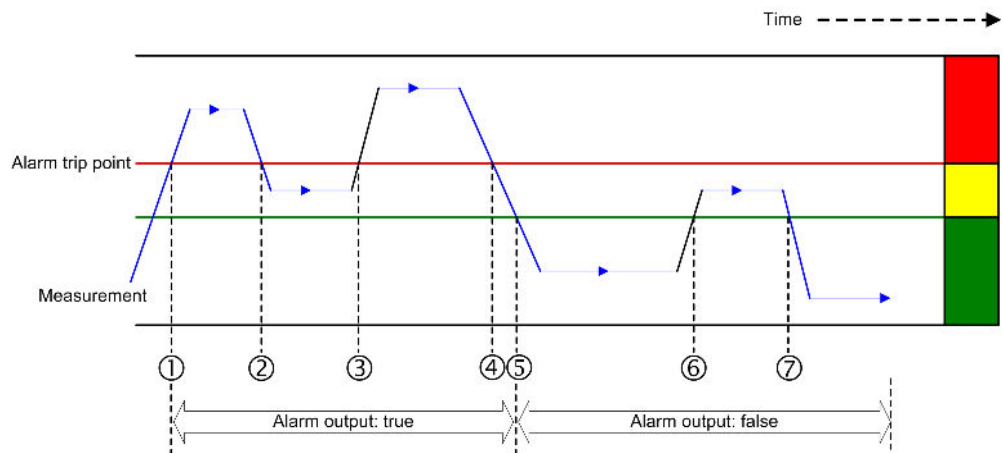
Error state.



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".

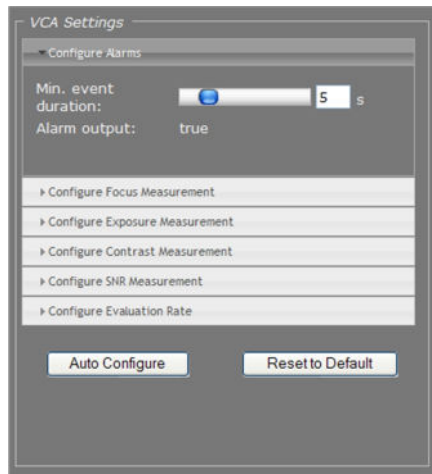


Image Quality not OK: Alarm output = true

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 S-60 E 's internal Management Information Base (MIB) using appropriate software, or through TKH Security's Open Streaming Architecture (OSA) - that is, the "SPI API". The S-60 E 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.tkhsecurity.com/support-files.

13.9.4 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.

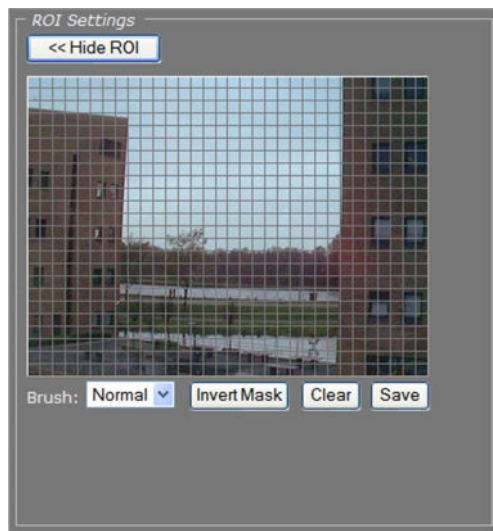
Item	Description
Configure Alarms	<i>Min. event duration</i> Alarm output delay time: the time span that is to elapse before a continued change in conditions actually activates/deactivates the alarm output.
	<i>Alarm output</i> <i>True</i> or <i>False</i> . Indication of current status.
Configure Focus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

13.9.5 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

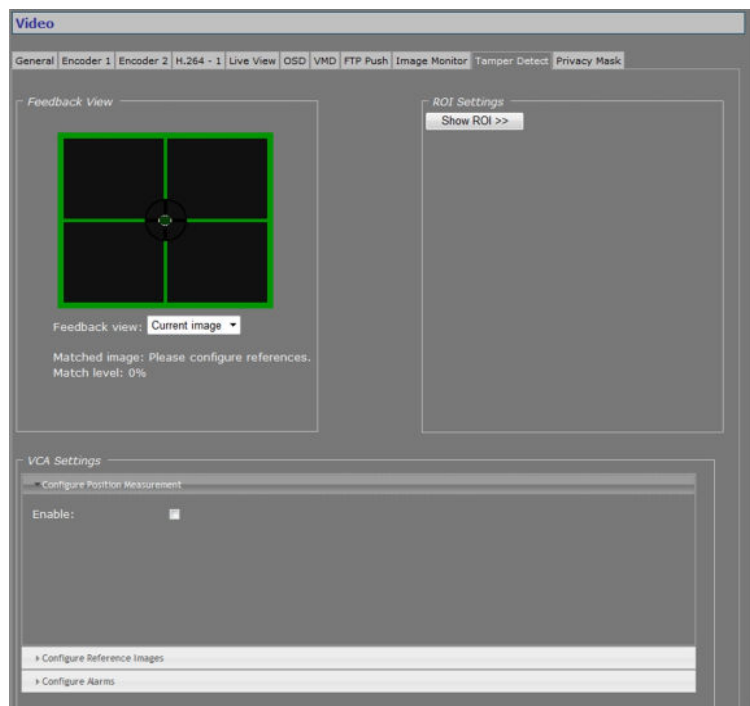
- To edit the mask, click on the grid that is put over the image.
One or more mask elements at, and possibly around, that position, are produced.
- Hold the standard mouse button and drag, to 'brush' (i.e. mask) larger areas, with a 'Normal', 'Small', or 'Large' brush.
- Use the 'Invert Mask' button 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	<i>Normal</i>	Allows grid elements to be accessed in 4-element groups.
	<i>Large</i>	Allows grid elements to be accessed in 16-element groups.
	<i>Small</i>	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 <i>do</i> 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.	

13.10 Tamper Detect



Video > Tamper Detect (disabled)

13.10.1 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.

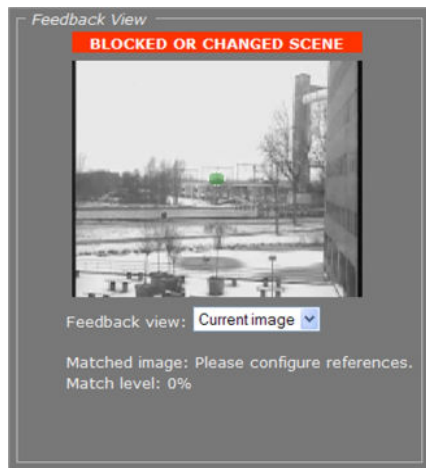
13.10.2 Enable Tamper Detect

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

13.10.3 Reference images

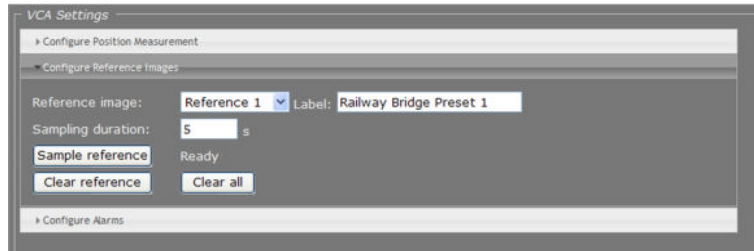
You can create up to 16 reference images. This enables you to store images captured in different day/night situations and/or from multiple PTZ preset positions. When the camera moves to a different preset Tamper Detect tries to match the new scene to the available reference images.

13.10.3.1 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

13.10.3.2 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.



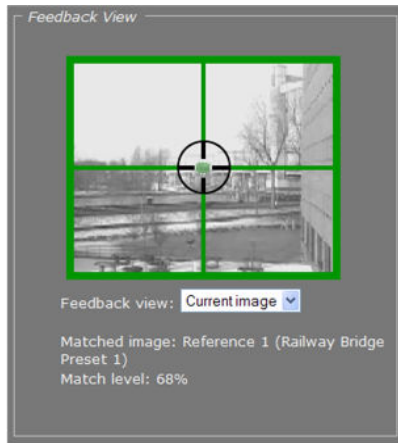
Region of less interest masked

13.10.3.3 Compare images

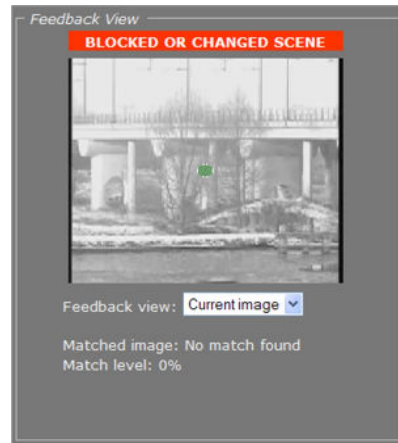
Tamper Detect compares the current scene with all available reference images. If a match is found a green crosshair is superimposed on the image in the Feedback view. Information about the matched image and the match level is displayed under the Feedback view.

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.

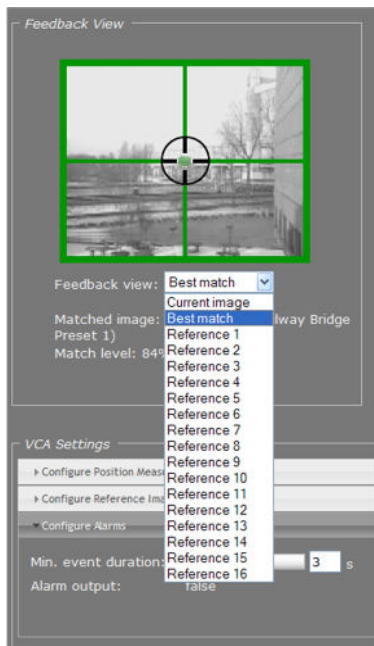


Current image matches Reference 1



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

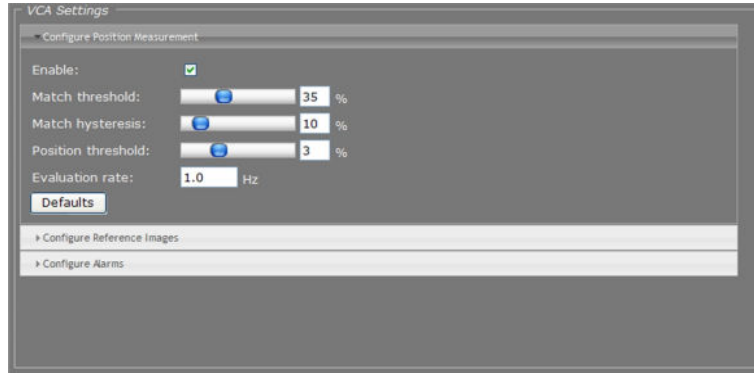
13.10.3.4 Delete a reference image

» 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.

13.10.4 Position measurement

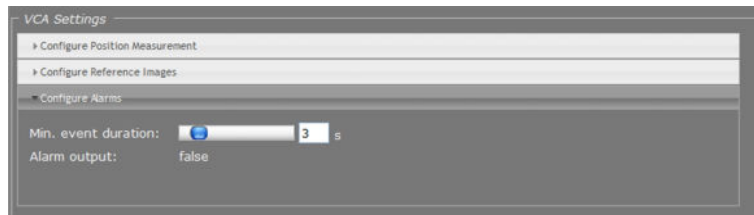


Video > Tamper Detect > Position Measurement

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.
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.

13.10.5 Alarms



Video > Tamper Detect > Configure Alarms

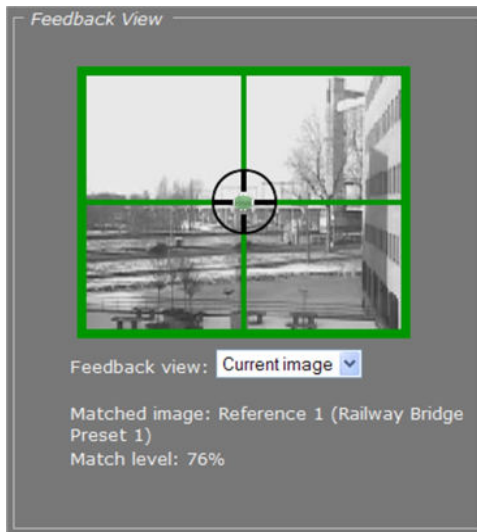
The Configure Alarms section enables you to view the current status of the alarm output and to set a delay for the activation/deactivation of alarm outputs.

Note: In addition to the status indication in this section, alarms can also be read from the S-60 E 's internal Management Information Base (MIB) using appropriate software, or through TKH Security's Open Streaming Architecture (OSA) - that is, the "SPI API". The S-60 E 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.tkhsecurity.com/support-files.

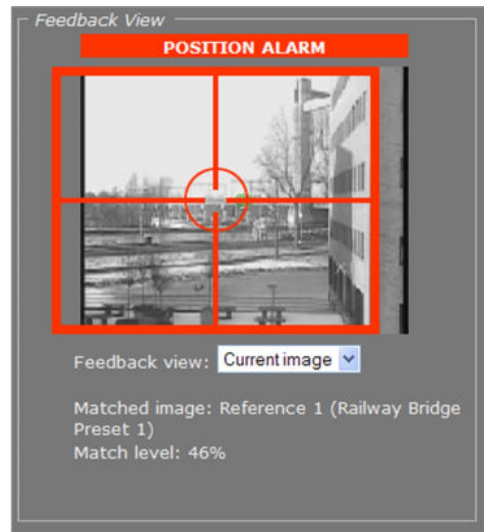
Item	Description
Min. event duration	Alarm output delay time: the time span that is to elapse before a continued change in conditions actually activates/deactivates the alarm output.
Alarm output	<i>True or False</i> . Indication of current status.

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.

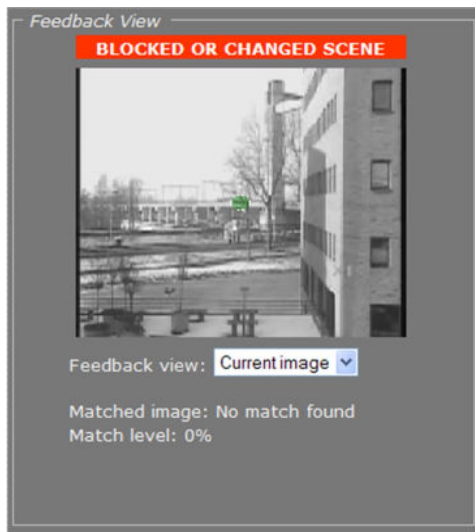
13.10.5.1 Alarm examples



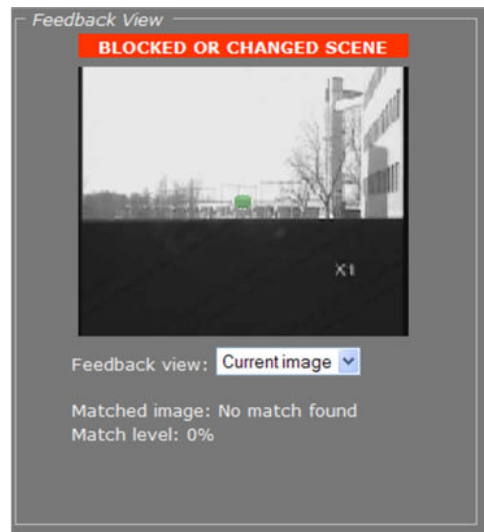
Original camera position



Camera has moved to the right. Although the current image still matches Reference 1, the changed camera position results in a position alarm.

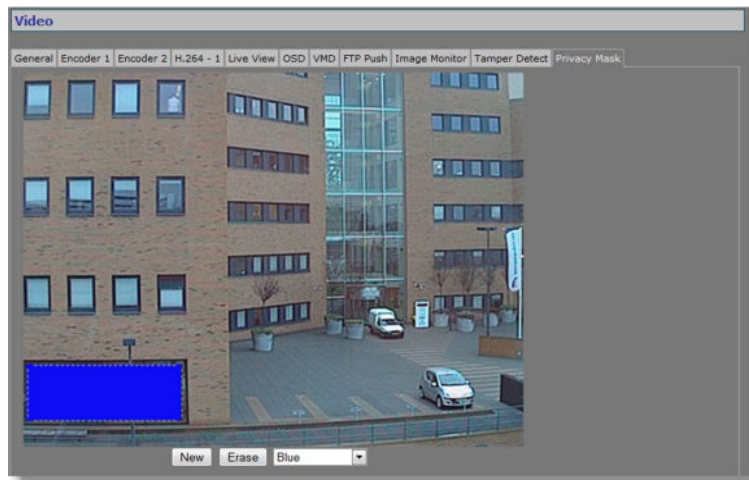


Camera has moved further to the right. Current image no longer matches any reference image, resulting in a changed scene alarm.



Blocked scene alarm

13.11 Privacy Mask



Video > Privacy Mask

The privacy mask function aims to avoid intrusive monitoring. The S-60 E 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**.

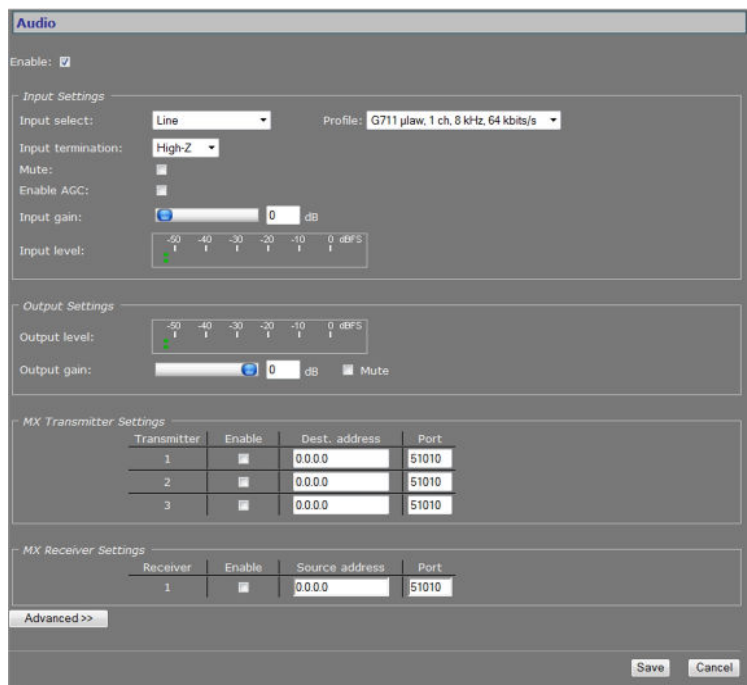
14 Audio

This chapter describes the functionality and settings found on the Audio page of the S-60 E.

In This Chapter

- 14.1 Enable audio.....98
- 14.2 Make audio connections.....100
- 14.3 Advanced..... 101

14.1 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.

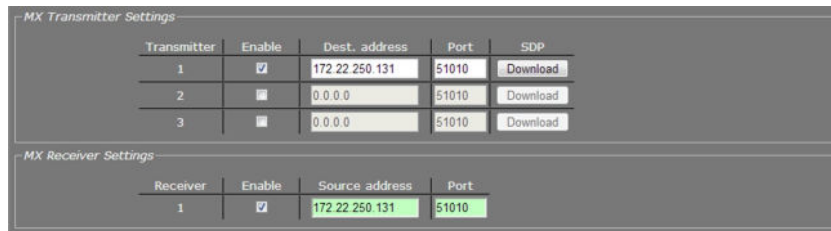
14.1.1 Input Settings

Item	Description						
Input select	<i>Line, Microphone, or Microphone + bias.</i>						
Input termination	Can be set to <i>High-Z</i> or <i>600 ohms</i> , to match audio source.						
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 <i>Save</i> .						
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.						
	<table border="0"> <tr> <td style="vertical-align: top;"><i>G711 A-law. 1 ch. 8 kHz 64 kbit/s</i></td> <td> <ul style="list-style-type: none"> • default setting • mainly used in Europe • mono, low quality • used for QuickTime </td> </tr> <tr> <td style="vertical-align: top;"><i>G711 μ-law. 1 ch. 8kHz. 64 kbit/s</i></td> <td> <ul style="list-style-type: none"> • mainly used in USA • mono, low quality • used for Genetec's Omnicast </td> </tr> <tr> <td style="vertical-align: top;"><i>Legacy PCM</i></td> <td> <ul style="list-style-type: none"> • 2 channels (stereo) • high quality, 15.7 kHz • compatible with all TKH Security products </td> </tr> </table>	<i>G711 A-law. 1 ch. 8 kHz 64 kbit/s</i>	<ul style="list-style-type: none"> • default setting • mainly used in Europe • mono, low quality • used for QuickTime 	<i>G711 μ-law. 1 ch. 8kHz. 64 kbit/s</i>	<ul style="list-style-type: none"> • mainly used in USA • mono, low quality • used for Genetec's Omnicast 	<i>Legacy PCM</i>	<ul style="list-style-type: none"> • 2 channels (stereo) • high quality, 15.7 kHz • compatible with all TKH Security products
<i>G711 A-law. 1 ch. 8 kHz 64 kbit/s</i>	<ul style="list-style-type: none"> • default setting • mainly used in Europe • mono, low quality • used for QuickTime 						
<i>G711 μ-law. 1 ch. 8kHz. 64 kbit/s</i>	<ul style="list-style-type: none"> • mainly used in USA • mono, low quality • used for Genetec's Omnicast 						
<i>Legacy PCM</i>	<ul style="list-style-type: none"> • 2 channels (stereo) • high quality, 15.7 kHz • compatible with all TKH Security products 						

14.1.2 Output Settings

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

14.2 Make audio connections



MX Transmitter Settings				
Transmitter	Enable	Dest. address	Port	SDP
1	<input checked="" type="checkbox"/>	172.22.250.131	51010	Download
2	<input type="checkbox"/>	0.0.0.0	51010	Download
3	<input type="checkbox"/>	0.0.0.0	51010	Download

MX Receiver Settings			
Receiver	Enable	Source address	Port
1	<input checked="" type="checkbox"/>	172.22.250.131	51010

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

Audio streams

The S-60 E provides bidirectional audio. The S-60 E 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 S-60 E. 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 S-60 E 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.

SDP download

Use the SDP Download button to download a Session Description Protocol (SDP) file from the encoder. SDP files contain streaming media initialisation parameters and properties. An SDP file does not deliver media itself but through file association the media stream can be opened in media players such as QuickTime and VLC. You can also use the SDP file to specify the URI in your web browser.

14.2.1 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.
SDP	To download a Session Description Protocol (SDP) file from the encoder, click the Download button.

14.2.2 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 S-60 E.

14.3 Advanced

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

14.3.1 Audio Input

Audio Input

Channels:

Sample rate: samples/s

Audio detect threshold channel 1: dB

Audio detect threshold channel 2: 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: <ul style="list-style-type: none"> • 7850 Hz A-law • 15710 Hz A-law • 15710 Hz PCM • 43200 Hz PCM
Auto detect threshold channel 1	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.
Auto detect threshold channel 2	

14.3.2 Audio Output

Audio Output

Bass: dB

Treble: dB

Audio > Advanced > Audio Output

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

14.3.3 Audio Encoder

Audio Encoder

Audio format:

Audio > Advanced > Audio Encoder

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

14.3.4 Audio Decoder

Audio Decoder

Channels:

Sample rate: samples/s

Audio format:

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): <ul style="list-style-type: none"> • 7850 Hz A-law • 15710 Hz A-law • 15710 Hz PCM • 43200 Hz PCM
Audio format	PCM 16bit, A-law 8bit, μ -law 8bit.

14.3.5 Transmitter

Transmitter 1

DSCP field:

Connection priority:

Multicast TTL:

RTP control mode: FloodGuard ▾

Stream type: UDP + RTP + NKF ▾

RTP type (0 = auto):

Link loss alarm timeout: s

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 (see - 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.	
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.	
	<i>None</i>	No transport protocol selected.
	<i>FloodGuard</i>	Flooding prevention mechanism. For more information, see the note on FloodGuard later in this chapter.
Stream type	<i>RTCP</i>	Real-Time Control Protocol, a network control protocol for use in communications systems to control streaming media servers.
	<i>UDP + RTP</i>	Default setting. Plain RTP stream over UDP.
	<i>UDP + RTP + NKF</i>	Adds an extended RTP header for TKH Security 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.	

14.3.6

Receiver 1

The screenshot shows the configuration for Receiver 1 with the following settings:

- Filter on source port: 0
- Connection priority: 0
- Reorder buffer size: 6
- Stream fail delay: 300 ms
- RTP control mode: FloodGuard (selected from a dropdown menu)
- RTP type (0 = auto): 0
- Link loss alarm timeout: 10 s

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, <i>Filter on source port</i> 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.						
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. <table border="1" data-bbox="571 734 1402 1025"> <tbody> <tr> <td><i>None</i></td> <td>No transport protocol selected.</td> </tr> <tr> <td><i>FloodGuard</i></td> <td>Flooding prevention mechanism. For more information, see the note on FloodGuard later in this chapter.</td> </tr> <tr> <td><i>RTCP</i></td> <td>Real-Time Control Protocol, a network control protocol for use in communications systems to control streaming media servers.</td> </tr> </tbody> </table>	<i>None</i>	No transport protocol selected.	<i>FloodGuard</i>	Flooding prevention mechanism. For more information, see the note on FloodGuard later in this chapter.	<i>RTCP</i>	Real-Time Control Protocol, a network control protocol for use in communications systems to control streaming media servers.
<i>None</i>	No transport protocol selected.						
<i>FloodGuard</i>	Flooding prevention mechanism. For more information, see the note on FloodGuard later in this chapter.						
<i>RTCP</i>	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.						

14.3.7 RTSP Transmitter

RTSP Transmitter

DSCP field:

Default multicast IP address:

Default multicast port:

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 (see - 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.

14.3.8 SAP Settings

Audio > Advanced > SAP Settings

The S-60 E includes a SAP announcer. The Session Announcement Protocol is used to advertise that a media stream generated by the S-60 E 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	<i>Global</i> , the default session scope, sets the <i>Multicast IP range</i> 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 <i>Administrative</i> 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.

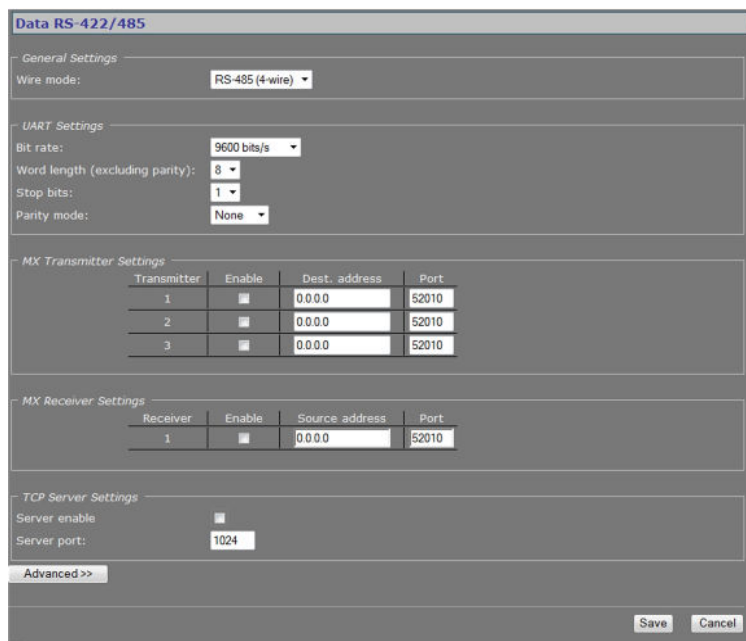
15 Data RS-422/485

This chapter describes the Data RS-422/485 page of the S-60 E.

In This Chapter

15.1 General Settings.....	108
15.2 UART Settings.....	109
15.3 Make data connections.....	109
15.4 TCP Server Settings.....	110
15.5 Advanced.....	110

15.1 General Settings



Data RS-422/485 page

Item	Description
Wire mode	<p><i>RS-422</i></p> <p><i>RS-485 (2-wire)</i></p> <p><i>RS-485 (4-wire)</i></p>

The RX-4xx interface type on the RJ-45 socket is set in software. Select the appropriate type from this list.

15.2 UART Settings

The S-60 E 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.

15.3 Make data connections

MX Transmitter Settings			
Transmitter	Enable	Dest. address	Port
1	<input checked="" type="checkbox"/>	172.22.250.136	52010
2	<input type="checkbox"/>	0.0.0.0	52010
3	<input type="checkbox"/>	0.0.0.0	52010

MX Receiver Settings			
Receiver	Enable	Source address	Port
1	<input checked="" type="checkbox"/>	172.22.250.136	52010

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.

15.4 TCP Server Settings



TCP Server Settings

Server enable

Server port:

Data RS-422/485 > TCP Server Settings

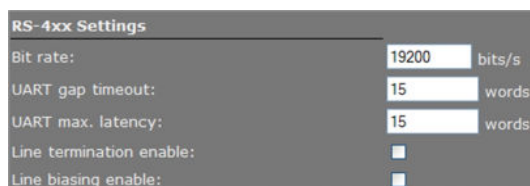
TCP connections are always bidirectional, so no separate transmitter and receiver settings are needed.

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].

15.5 Advanced

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

15.5.1 RS-4xx Settings



RS-4xx Settings

Bit rate: bits/s

UART gap timeout: words

UART max. latency: words

Line termination enable:

Line biasing enable:

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.

15.5.2 Transmitter

Transmitter 1

Connection priority: 0

Multicast TTL: 10

FloodGuard enable:

FloodGuard throttle delay: 3 s

FloodGuard throttle interval: 100 ms

Stream type: UDP + NKF

Link loss alarm timeout: 10 s

Data RS-422/485 > Advanced > Transmitter 1

Item	Description
Connection priority	Parameter intended for use with MX Software Development Kit.
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 TKH Security applications requiring extra information.
Link loss alarm timeout	Range: [1...1000] s. Default: 10 s. Time in seconds before alarm sent.

15.5.3 Receiver 1

Receiver 1

Source port filter: 0

Connection priority: 0

Reorder buffer size: 6

Stream fail delay: 300 ms

FloodGuard enable:

FloodGuard tx interval: 1000 ms

Stream type: Auto

Link loss alarm timeout: 10 s

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.
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 TKH Security applications requiring extra information.
Link loss alarm timeout	Range: [1...1000] s. Default: 10 s. Time in seconds before alarm sent.

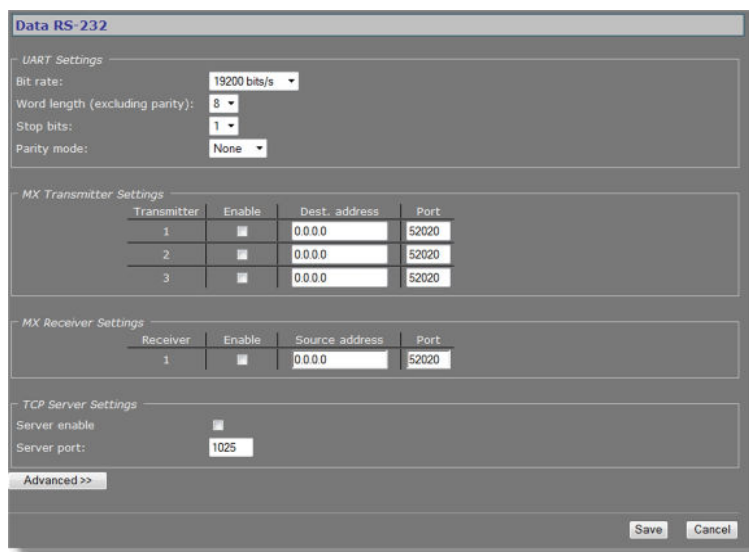
16 Data RS-232

This chapter describes the Data RS-232 page of the S-60 E.

In This Chapter

16.1 Configure RS-232 settings..... 114

16.1 Configure RS-232 settings



Data RS-232 page

Configuration of the RS-232 interface is almost identical to configuring RS-422/485 settings (with the exception that there is no line termination or biasing with RS-232). For a detailed description, see the section covering RS-422/485.

» To set up an RS-232 data link

- 1 Assign a destination IP address (a specific host or a multicast group) to a serial transmitter output stream (1, 2 or 3).
- 2 Assign a suitable destination port (even number) to the transmitter output stream.
- 3 Enable the stream.
- 4 Save the settings.
- 5 At the receiver end, fill in the source IP address.
- 6 At the receiver end, fill in the local port number (the same as the destination in the transmitter).
- 7 Enable reception.
- 8 Save the settings.

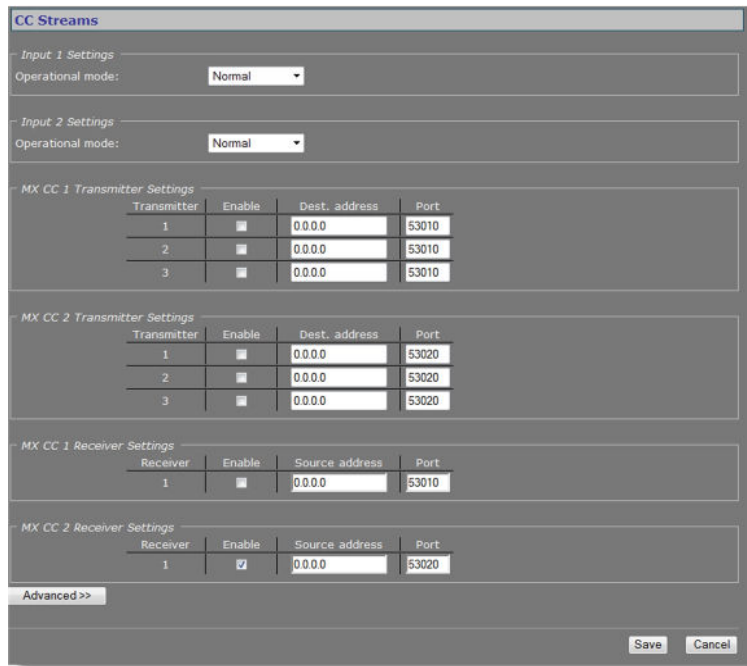
17 CC Streams

This chapter provides information about the S-60 E's contact closure (CC) channels, CC status, and alarms.

In This Chapter

- 17.1 CC channels, CC status, and alarms..... 115
- 17.2 Input # Settings.....116
- 17.3 Make contact closure connections..... 116
- 17.4 Advanced..... 117

17.1 CC channels, CC status, and alarms



CC Streams page

CC channels

The contact closure channels of the S-60 E, 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 S-60 E, 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 S-60 E and check for the module alarm. Stream alarms (link alarms in the modules, at both link ends) become active if the link fails.

17.2 Input # Settings



CC Streams > Input 1 Settings

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

17.3 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.

17.4 Advanced

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

17.4.1 Transmitter

CC 1 Settings

Transmitter 1

Connection priority:

Multicast TTL:

Link loss alarm timeout: s

CC Streams > Advanced > Transmitter 1

Item	Description
Connection priority	Parameter intended for use with MX Software Development Kit.
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.

17.4.2 Receiver 1

Receiver 1

Source port filter:

Connection priority:

Reorder buffer size:

Stream fail delay: ms

Link loss alarm timeout: s

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.
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.

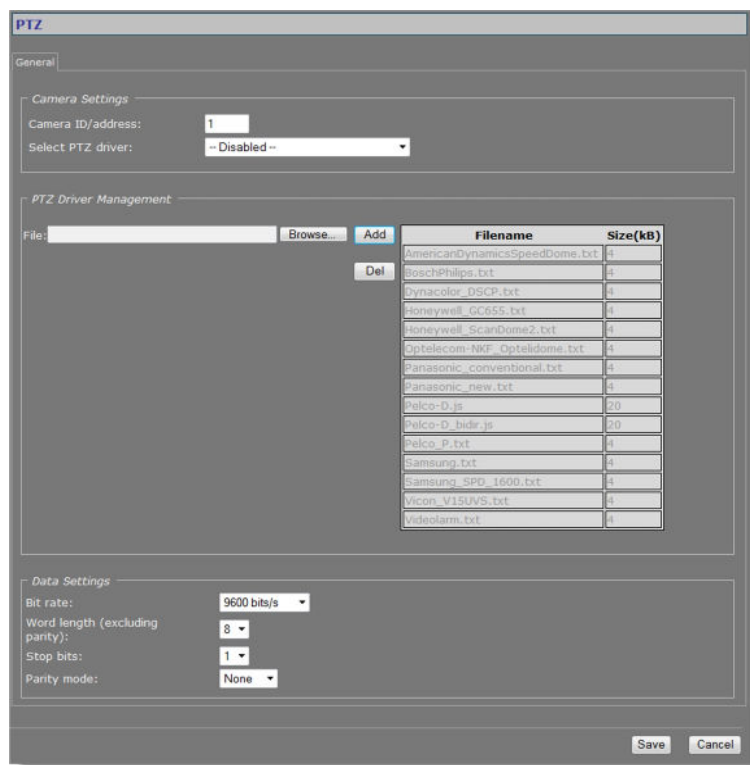
18 PTZ

A PTZ camera connected to the S-60 E can be controlled with the PTZ Control panel on the Live Video page. This chapter describes how to enable PTZ camera control. You will also see how you can upload PTZ drivers to the S-60 E and how you can remove drivers.

In This Chapter

- 18.1 Enable PTZ control.....119
- 18.2 Upload/Remove PTZ drivers..... 120
- 18.3 Data Settings.....120

18.1 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 S-60 E.

►► 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.

18.2 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.

18.3 Data Settings



The screenshot shows a 'Data Settings' dialog box with the following configuration:

- Bit rate: 19200 bit/s
- Word length (excluding parity): 8
- Stop bits: 1
- Parity mode: None

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.

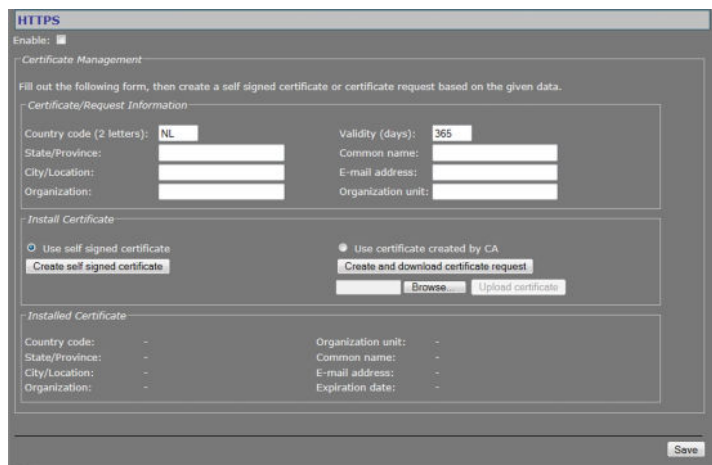
19 Security

From the Security page, Administrators can install security certificates to enable secure connections between the S-60 E and web browsers. Certificates can be self-signed or obtained from a Certificate Authority.

In This Chapter

19.1 HTTPS.....	121
19.2 Certificate/Request information.....	122
19.3 CA-Issued certificate.....	122
19.4 Self-signed certificate.....	123
19.5 Open a secure connection.....	123

19.1 HTTPS



Security page

Secure connections

An HTTPS connection is a standard HTTP connection on top of an SSL/TLS connection, adding the security capabilities of SSL/TLS to standard HTTP communication. With HTTPS implemented and used on the S-60 E, a safe exchange of data between the unit and a web browser is ensured. Information transported over the network, such as device settings and credentials, is encrypted to protect it against eavesdropping.

Certificates

To implement HTTPS on the S-60 E, you need to install an HTTPS certificate. You can use a self-signed certificate or one created by a Certificate Authority (CA). CA-issued certificates provide a higher level of security and inspire more trust than self-signed certificates. Self-signed certificates are often installed for test purposes or as a temporary solution until a CA-issued certificate has been obtained.

19.2 Certificate/Request information

In the Certificate/Request Information section, you can provide the information required for a self-signed certificate or a CA-issued certificate.

Item	Description
Country code (2 letters)	The country where the certificate is to be used. Default: "NL".
State/Province	The administrative region in which the organisation is located.
City/Location	City/Location where the organisation is based.
Organisation	The name of the organisation which owns the entity specified in the "Common name" text box.
Validity (days)	The valid period (in days) of the certificate. Default: 365.
Common name	The name of the entity to be certified by the certificate.
E-mail address	The contact e-mail address
Organisation unit	The name of the organisational unit which owns the entity specified in the "Common name" text box.

Important: Make sure that the *Common name* you specify when you generate a security certificate matches the URL that is used to access the webpages of the S-60 E. Generally, this is the IP address of the unit, followed by "/frame.html". For example: 10.50.3.72/frame.html

19.3 CA-Issued certificate

Steps towards implementing a certificate created by a CA

- Create the certificate request
- Send the request to a CA
- Upload the CA-signed certificate to the unit

Note: When you implement a certificate you may need to modify your browser settings to allow pop-ups.

» To generate a certificate request

- 1 In the *Certificate/Request Information* section, enter the required information as described above.
- 2 Click **Create and download certificate request**.
A pop-up displays.
- 3 In the pop-up, click **Save**.
You can copy the request from your download folder now and then send it to a CA.

» To install a signed certificate from a CA

- 1 Click **Browse**.
- 2 Browse and select the certificate file.
- 3 Click **Upload Certificate**.

- A warning displays.
- 4 Click **Yes** to continue.

19.4 Self-signed certificate

» To create a self-signed certificate

- 1 In the *Certificate/Request Information* section, enter the required information as described above.
- 2 Click **Create self-signed certificate**.

19.5 Open a secure connection

With a security certificate installed, you can establish a secure connection.

» To enable HTTPS and open a secure connection

- 1 On the *Security* page, select **Use self-signed certificate** or **Use certificate created by CA** (depending on the type of certificate you want to use).
- 2 At the top of the page, select **Enable**.
- 3 Click **Save**.
- 4 Refresh the page.
- 5 Log on to the S-60 E again.
Your browser is now using a secure connection to communicate with the unit.

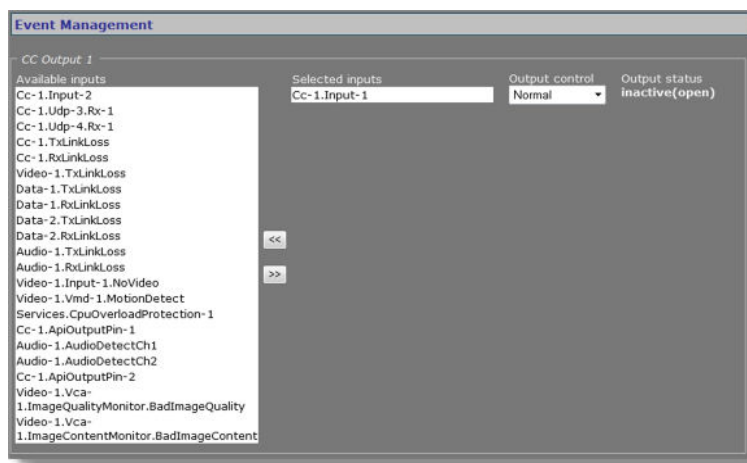
20 Event management

This chapter describes the Event Management page.

In This Chapter

20.1 Associate events with output facilities..... 124

20.1 Associate events with output facilities



Event Management page

On the Event Management page, you can configure how the S-60 E 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.

20.1.1 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	<i>Normal</i> Direction. <i>Invert</i> <i>Force active</i> Always on (for testing purposes, for example). <i>Force inactive</i> Always off.
Output status	<i>Inactive (open)</i> or <i>active (closed)</i> . Active: one or more of the selected inputs is true. Inactive: none of the selected inputs is true.

20.1.2 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	<i>Inactive (open)</i> or <i>active (closed)</i> . Active: one or more of the selected inputs is true. Inactive: none of the selected inputs is true.

20.1.3 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	<i>Inactive (open)</i> or <i>active (closed)</i> . Active: one or more of the selected inputs is true. Inactive: none of the selected inputs is true.

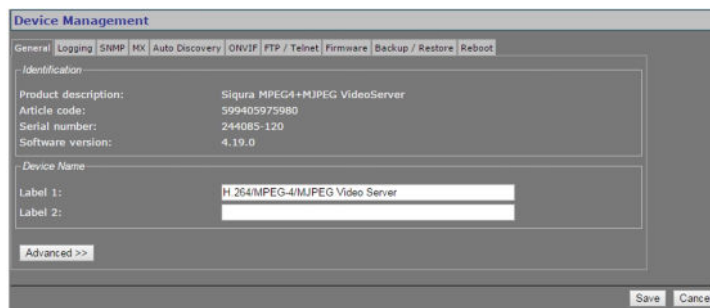
21 Device management

You can use the Device Management page to configure management settings for the S-60 E, upgrade or downgrade the embedded firmware, and reboot the unit.

In This Chapter

21.1 General.....	127
21.2 Logging.....	129
21.3 SNMP.....	129
21.4 MX.....	131
21.5 Auto Discovery.....	132
21.6 ONVIF.....	133
21.7 FTP/Telnet.....	133
21.8 Firmware.....	134
21.9 Backup/Restore.....	137
21.10 Reboot.....	137

21.1 General



Device Management > General

21.1.1 Identification

This section offers administrative module information.

21.1.2 Device Name

Item	Description
Label 1	The Device name section contains label settings, which can be edited and saved. 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.
Label 2	



Title pane with Label 1 value

21.1.3 Advanced



Device Management > General > Advanced

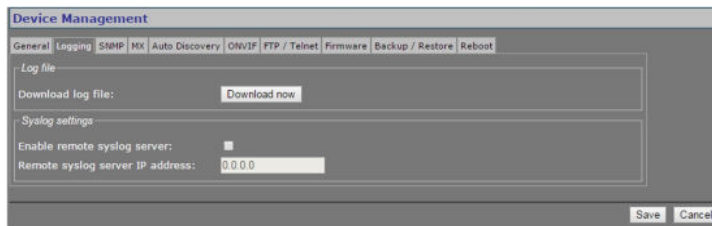
21.1.3.1 Alarm Settings

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 TKH Security software (which will also enable you to configure alarm levels and destinations).

21.1.3.2 LED control

Item	Description
Disable LEDs	For security reasons or energy efficiency you can deactivate all LEDs on the unit here.
Flash DC LED	Range: [0 ...1000]. To identify a S-60 E among other units, enter a value and click Save . The power LED on this particular unit will blink for the number of seconds you set.

21.2 Logging



Device Management > Logging

21.2.1 Log file

Press the *Download now* button to download a log file from the S-60 E to your computer. The 'system.log' file which opens in Notepad may prove useful when you are troubleshooting issues.

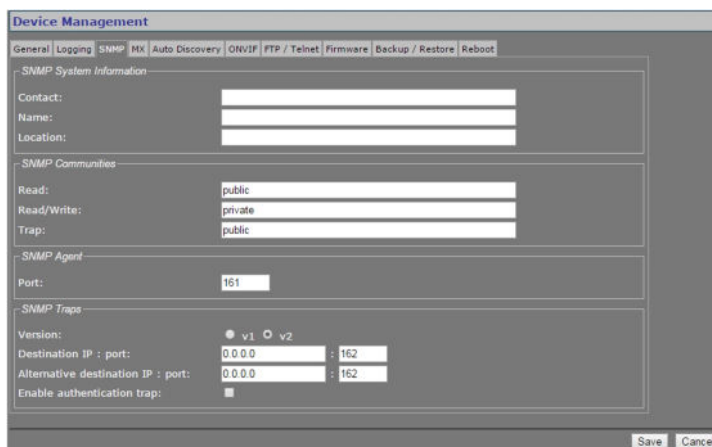
21.2.2 Syslog settings

Syslog is a standard which allows devices to send event notification messages over IP networks to event message collectors, also known as syslog servers.

» To enable a remote syslog server

- 1 In *Syslog settings*, select **Enable remote syslog server**.
- 2 Specify the IP address of the remote syslog server.
- 3 Click **Save**.

21.3 SNMP



Device Management > SNMP

21.3.1 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.

21.3.2 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.

21.3.3 SNMP Agent

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

21.3.4 SNMP Traps

A S-60 E alarm status change generates a trap which can be caught by any SNMP manager. The S-60 E can, for example, send traps on the occurrence of Image Quality and Camera Tampering events. Variables, which can be read from the S-60 E'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 S-60 E MIBs, at www.tkhsecurity.com/support-files.

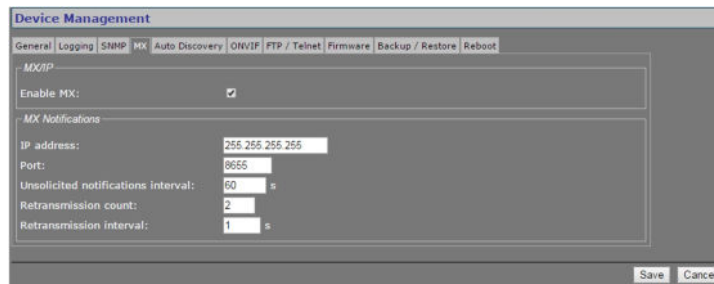
Note that *Version* and *Destination IP : port* are required fields.

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.

21.3.5 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.

21.4 MX



Device Management > MX

21.4.1 MX/IP

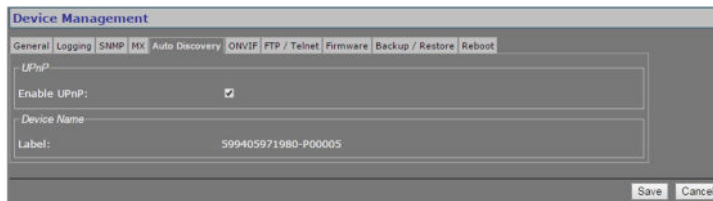
MX/IP is a UDP protocol used to communicate with TKH Security equipment over a network connection. TKH Security applications use the MX/IP protocol to access, configure, and control TKH Security network devices.

Item	Description
Enable MX	In addition to the proprietary MX/IP protocol, a S-60 E 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 S-60 E firmware through the MX Firmware Upgrade Tool application.

21.4.2 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.

21.5 Auto Discovery



Device Management > Auto Discovery

21.5.1 Advertise the S-60 E

On the Auto Discovery tab, you can enable UPnP (Universal Plug and Play). If enabled, UPnP allows the S-60 E 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. With the UPnP service enabled in Windows (see *Appendix: Enable UPnP in Windows 7*), you can connect to the S-60 E from Windows Explorer.

21.5.1.1 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.

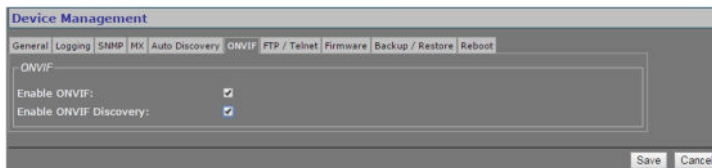
Step 3: Control. The control point can send actions to a device's service.

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 S-60 E supports the following Universal Plug and Play (UPnP) functionality: *Discovery*, *Description* (partly supported), and *Presentation*.

21.6 ONVIF



Device Management > ONVIF

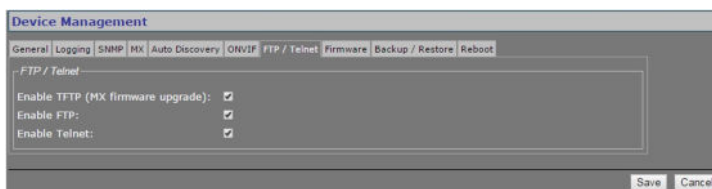
The S-60 E supports the ONVIF standard. On the ONVIF tab, you can enable ONVIF compatibility and ONVIF discovery.

Item	Description
Enable ONVIF	Enables the ONVIF interface on the S-60 E.
Enable ONVIF Discovery	Makes the S-60 E discoverable for ONVIF clients. Clear this check box if you prefer to disable discovery. In that case, the S-60 E can still be controlled from ONVIF clients that "know" of its existence.

21.6.1 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.

21.7 FTP/Telnet

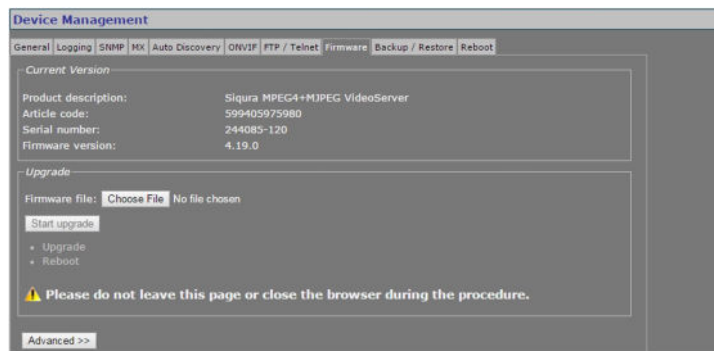


Device Management > FTP/Telnet

The TFTP, FTP, and Telnet services are enabled by default. For security reasons, you may wish to disable these services.

Item	Description
Enable TFTP (MX firmware upgrade)	Activates the TFTP service. Note that this service is required if you want to upload ".nkffw" firmware files to the unit.
Enable FTP	Activates the FTP service. Clear this check box to disable file upload to the unit via FTP. Note that this setting does not affect the unit's FTP Push feature.
Enable Telnet	Activates the Telnet service. Clear this check box to disable access via Telnet (including root account access).

21.8 Firmware



Device Management > Firmware

21.8.1 Firmware images

The S-60 E 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 S-60 E 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 S-60 E.

21.8.2 Current Version

This section offers information on the currently active firmware version.

21.8.3 Upgrade

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

Important: On upgrading a S-60 E 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 S-60 E 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 S-60 E via the webpage. You can use them to upgrade the unit through MX Firmware Upgrade Wizard. This software is embedded in 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.

21.8.4 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.

21.8.5 Advanced

For various reasons you may want to downgrade the S-60 E 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.

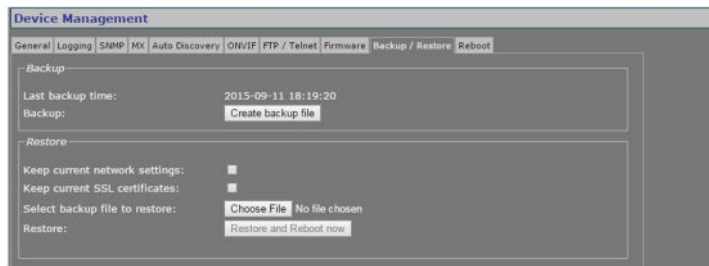
» To revert to the S-60 E's fixed image

- 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.

- 5 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.

21.9 Backup/Restore



Device Management > Backup/Restore

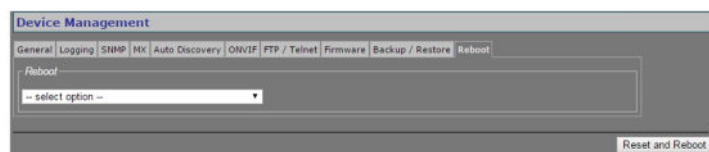
21.9.1 Backup

Item	Description
Last backup time	Date and time of the most recent backup.
Backup	Saves the current configuration of the S-60 E to the designated download folder.

21.9.2 Restore

Item	Description
Keep current network settings	Select to preserve the current network settings when you restore a backed-up S-60 E configuration.
Keep current SSL certificates	Select to preserve currently installed SSL certificates, if any, when you restore a backed-up S-60 E configuration.
Select backup file to restore	Browse for and select the backed-up S-60 E configuration you wish to restore.
Restore	Starts the restore process using the selected backup file.

21.10 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 S-60 E.

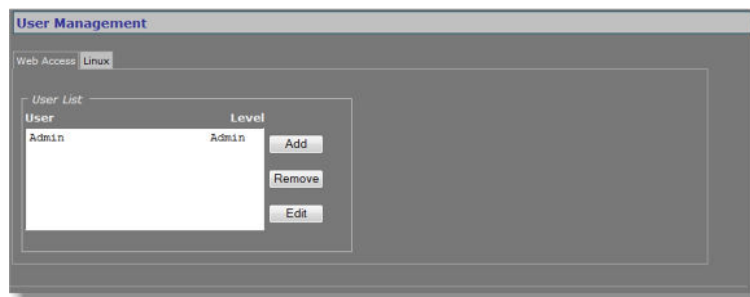
22 User Management

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

22.1 Web Access.....	139
22.2 Linux.....	140

22.1 Web Access



User Management > Web Access

22.1.1 Access control

The S-60 E 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 S-60 E supports up to 20 users at a time.

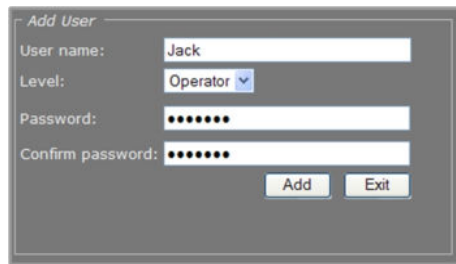
Important: On upgrading a S-60 E to firmware version 4.0 and higher, all existing users are deleted. After a successful upgrade, you can access the webpages with the default Admin account (user name = Admin; password = 1234).

22.1.2 Manage user accounts

» To add a user

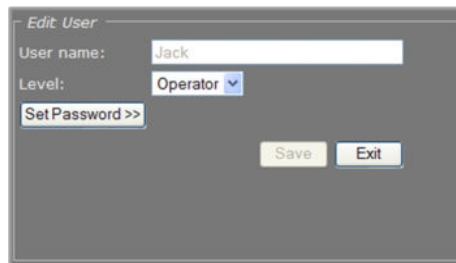
- 1 On the *User Management* page, open the **Web Access** tab.
- 2 In the *User List* section, click **Add**.
The Add User section displays.
- 3 Enter the new user name (alphanumeric and underscore only) and password. Confirm the password to prevent errors.
- 4 Select the appropriate access level.
-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

The user is added to the User List.



Adding a user

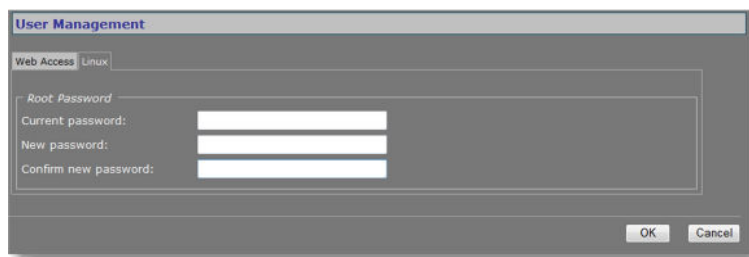
- 1 On the *User Management* page, open the **Web Access** tab.
- 2 Select the user name from the *User List*, and then click **Edit**.
The Edit User section displays.
- 3 Modify the user name, permission level, and/or password.
- 4 To write the settings into the module, click **Save**.



Editing a user

- 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**.

22.2 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.

Note: Root account access requires that the Telnet service is enabled on the unit. For more information, see *Device Management > FTP/Telnet*.

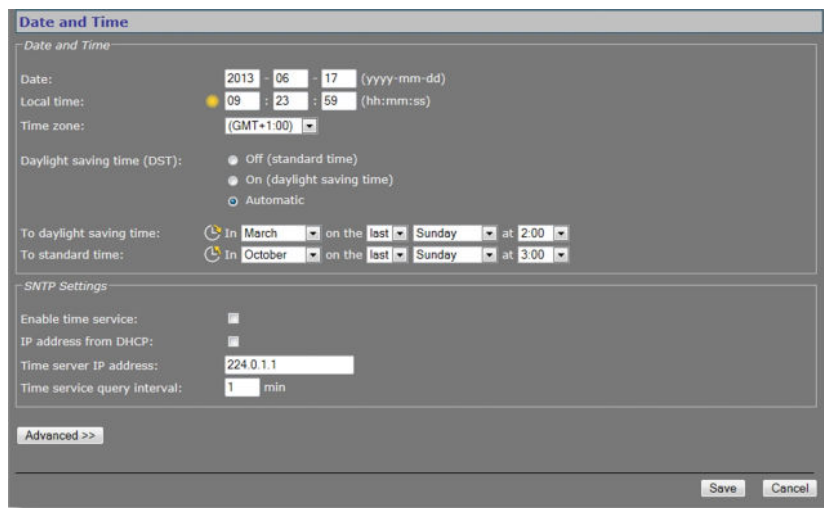
23 Date and Time

The S-60 E has a battery-supported real-time clock. This chapter explains how to adjust the date and time.

In This Chapter

- 23.1 Date and time..... 142
- 23.2 SNTP Settings..... 143
- 23.3 Advanced..... 144

23.1 Date and time



Date and Time

You can set the date and time manually in the Date and Time section. Press **Save** to make your changes permanent.

On-screen date/time display can be activated on the OSD tab of the Video page. The on-screen position and colour of the text are governed by the relevant OSD settings.

» To set the date and time manually

- 1 In the SNTP Settings section, clear **Enable time service**.
This activates the Date and Local time text boxes.
- 2 Set the date and local time.
- 3 On the *Time zone* list, select your local zone.

» To disable Daylight saving time

- Select **Off (standard time)**.
Standard time will be used throughout the year.

» To activate Daylight saving time manually

- Select **On (daylight saving time)**.
This adds one hour to the currently configured local time. The unit will not automatically switch between summer and winter time.

» To activate automatic Daylight saving time switchover

- 1 Select **Automatic**.
- 2 Use the *To daylight saving time* and *To standard time* lists to enter the appropriate start and end details.
The unit will automatically adjust at the given dates and times.

	DST begins	DST ends
Australia	2:00 AM local time on first Sunday in October	3:00 AM local time on first Sunday in April
China	N/A	N/A
Europe	2:00 AM local time on last Sunday in March	3:00 AM local time on last Sunday in October
Russia	N/A	N/A
USA	2:00 AM local time on second Sunday in March	2:00 AM local time on first Sunday in November

23.2 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 S-60 E for use with an SNTP server

- 1 In *SNTP Settings*, clear **Enable time service**, and then click **Save**.
- 2 In *Date and Time*, open the **Time zone** list, and then select your local zone.
- 3 Select the *Daylight saving time (DST)* option to be applied.
- 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 *SNTP Settings*, select **Enable time service**.
- 8 Select **IP address from DHCP** 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.

Note: (S)NTP synchronisation is mandatory for ONVIF.

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.

23.3 Advanced



Date and Time > Advanced

As an alternative to using the the Date and Time section values to configure time zone and DST settings, you can go to Advanced Settings and enter custom settings there. You may, for example, need to set a time zone which is not included in the list. Once you have saved a custom value, the Time zone list in the Date and Time section indicates "User defined".

Custom time zones can have the Time zone list format or the POSIX 1003.1 time zone strings format as defined in *Standard for Information Technology - Portable Operating System Interface (POSIX) - Base Definitions, IEEE Std 1003.1-2004, December 2004*. The benefit of the POSIX format is that time zone and DST details can be specified more explicitly than through the Date and Time section.

Note: Adjusting time zone and DST settings through POSIX is recommended only for advanced users who are familiar with the intricacies of POSIX.

►► To adjust the time zone and DST through POSIX

- 1 Select **Time zone in POSIX**.
- 2 In the *User defined time zone* text box, enter a valid POSIX time zone string.
If the string is recognised, the Date and Local time values in the Date and Time section are adjusted accordingly.

24 Multicasting

The S-60 E can be used in a multicast setting. This chapter outlines IP multicast and one of its methods in particular: source-specific multicast. It also describes the concept of multi-unicast.

In This Chapter

24.1 Multicast.....	145
24.2 Multi-unicasting.....	146

24.1 Multicast

IP multicast

The S-60 E 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 S-60 E 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 S-60 E 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 S-60 E, 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 S-60 E 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](#)

[rfc4570](#)

[rfc3569](#)

[rfc5760](#)

24.2 Multi-unicasting

As an alternative to multicasting, the S-60 E features 'multi-unicasting', that is - sending out up to 3x3 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.

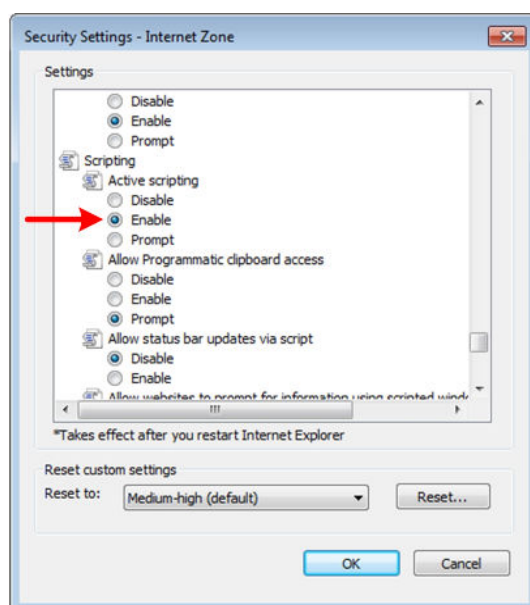
When such a destination is removed, the source also stops sending the corresponding stream. If the input channel of a destination is disabled without disabling the source, source transmission will be throttled, but not disabled (this behavior is selectable through the FloodGuard settings). The source 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.

Appendix: Enable JavaScript

To have the S-60 E webpages displayed correctly, JavaScript must be enabled in your web browser.

» **To enable JavaScript in Internet Explorer**

- 1 On the *Tools* menu, 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

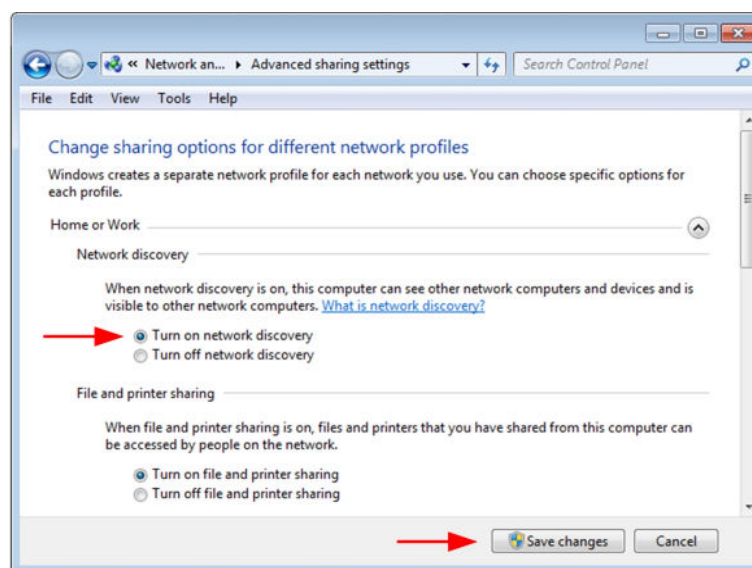
Appendix: Enable UPnP in Windows

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

» To enable UPnP

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

UPnP will automatically start when you turn on your computer.



Enable network discovery

Appendix: Install a video player

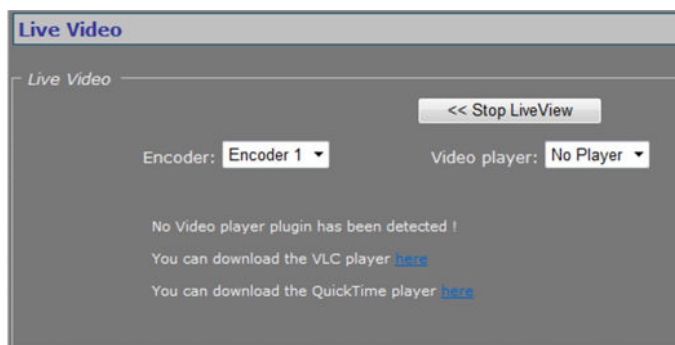
Viewing video streams on the webpages of the S-60 E requires a video player installation on the machine running the web browser. This appendix provides instructions for installing QuickTime and VLC, the video plug-ins supported by the S-60 E.

In This Chapter

Download video player software.....	149
Install QuickTime.....	149
Install VLC.....	149

Download video player software

The S-60 E 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.



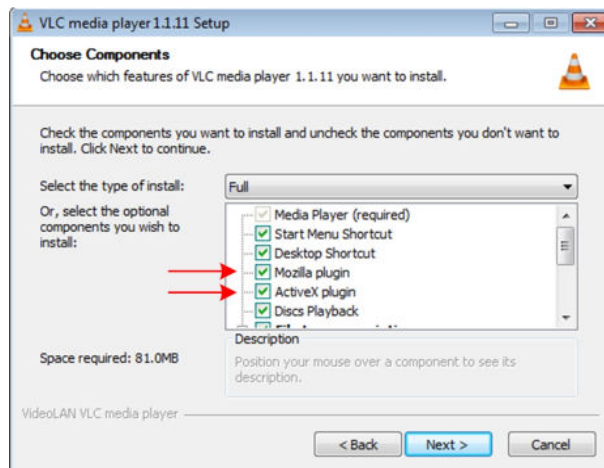
Live Video page with video player download links

Install QuickTime

QuickTime installation is straightforward and self-explanatory.

Install 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 S-60 E has been successfully tested with VLC v2.1.0.

VLC and Windows 7

» To configure VLC media player settings when running this plug-in on a 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 S-60 E.

In This Chapter

Supported conformance groups.....	151
SNMP MIB.....	153

Supported conformance groups

The S-60 E 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 TKH Security 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.