S-60 D-MC

Firmware Version 3.10.3

Digital multicodec video decoder

User Manual

TKH GROUP 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 Siqura B.V.

S-60 D-MC v3.10.3
User Manual v7 (090405-7)
AIT55

Brand names

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

Liability

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

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

How to contact us

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

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

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

Contents

1 Introduction

Document scope

This manual applies to TKH Security's multicodec video decoder, S-60 D-MC v3.10.3.
It offers detailed information on:

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

Intended audience

This manual is aimed at network engineers, technicians, and operators involved in the installation and operation of network devices, such as the S-60 D-MC.

Assumed skills and know-how

To work with a S-60 D-MC unit, a technician or operator must have adequate knowledge and skills in the fields of:

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

Specifications

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

Important information

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

Acknowledgement

S-60 D-MC units use the open-source Free Type font-rendering library.

2 Safety and compliance

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

In This Chapter

2.1 Safety

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

Trained personnel

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

Safety requirements

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

Optical safety

The following optical safety information applies to S-60 D-MC 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 Compliance

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

3 Product Description

The unique S-60 D-MC multicodec video decoder decodes most streams effortlessly. With its automatic format detection, it can handle most H.264, MPEG-2, and MPEG-4 streams. It is an open, low-latency, and cost-effective decoder solution for IP video CCTV applications producing crystal clear and highly detailed images. This chapter introduces the unit to you by presenting its main features.

In This Chapter

3.1 Product Overview

General

The S-60 D-MC is a single-channel, multicodec video decoder, capable of handling H.264, MPEG-2, and MPEG-4 compressed video. In addition to unidirectional video, the S-60 D-MC offers independent bidirectional stereo audio, data, and contact closure channels.

Models

The S-60 D-MC is to be used in MC 11 or similar power supply cabinets, but it is also available as a stand-alone module (/SA version). The S-60 D-MC is optionally available with a pluggable SFP slot for connections via a fiber optic cable (/SFP). A range of multimode or single-mode XSNet™ SFP devices fit the empty SFP slot. Front panel LEDs indicate network status, stream status (sync), data activity, and DC power. All models have backup battery power for their clocks.

Multidecoding

The S-60 D-MC is capable of taking an H.264, MPEG-2, or MPEG-4 video stream and decompress it to an analog video output signal. The type of compression of the video stream is automatically detected. Resolution and frame rate will follow encoder settings.

Live View encoder

The decoded video can also be made available in MJPEG format. The received images can be viewed remotely using the S-60 D-MC's web interface and streamed to web applications or remote devices by using the HTTP protocol.

FTP push

On the occurrence of an event, JPG images generated by the Live View encoder can be posted on a remote server. The unit pushes the images to one or two FTP servers. The S-60 D-MC can also be configured to periodically upload images to the remote server(s).

Audio, data, and I/O contacts

Combining streaming video with duplex audio, serial data, and I/O contacts over IP, the S-60 D-MC provides all the interfaces necessary for any CCTV application (CD-quality stereo audio, alarm contacts, access control, etc.). The balanced audio inputs/outputs are suitable for all industrial audio systems.

Web interface

Configuration, management, and live viewing are simplified by the access-controlled web interface. Full in-band control is available through the MX™ Configuration Tool Kit or the HTTP API. The S-60 D-MC is field-upgradeable.

Compatibility

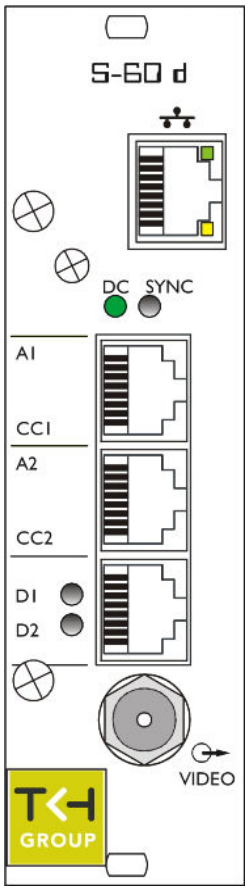
The S-60 D-MC is part of a complete offering of video surveillance equipment and solutions. TKH Security offers video codecs/servers, IP cameras, video management, network storage, and configuration software. The S-60 D-MC is designed to comply with the worldwide adopted standards for streaming video. Its Open Streaming Architecture (OSA) offers standardised streaming video and remote control. All streaming protocols are based on approved standards and tested with different vendors. A comprehensive HTTP API gives access to all controls and makes integration with third-party VMS easy. The API is available at www.tkhsecurity.com/support-files. In addition, the S-60 D-MC supports TKH Security's unique MX™ protocol.

Note: The S-60 D-MC supports the TKH Security C-, S-, and V-series codecs, and the HD-, MD-, HSD-, and MSD-series dome cameras, based on the v2.5.x up to v3.10.x firmware range. Third-party IP cameras, 1080p and 720p HD are not supported.

3.2 Front Panel

Features and indications

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



S-60 D-MC

VIDEO	BNC connector	video output
	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 (see "Advanced Settings" on page 62) and errors
***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 D-MC front panel features and indications

Pin assignments are given in section Connector Pin Assignments (on page 13).

4 Installation

This chapter describes how to power your S-60 D-MC unit and connect network and signal cables.

In This Chapter

4.1 Powering the Unit

To power a rack-mount unit

1 Insert the S-60 D-MC 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 D-MC 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 Connecting Cables

Use the appropriate connectors on the S-60 D-MC front panel (see "Front Panel" on page 10) to connect network and signal cables.

To connect the S-60 D-MC 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 monitor

- Connect the coaxial cable from your video monitor to the video output BNC connector on the S-60 D-MC 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 D-MC 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 will go through an on/off sequence.

The power DC LED should always be lit; the link lights will eventually glow upon establishing of a good network link.

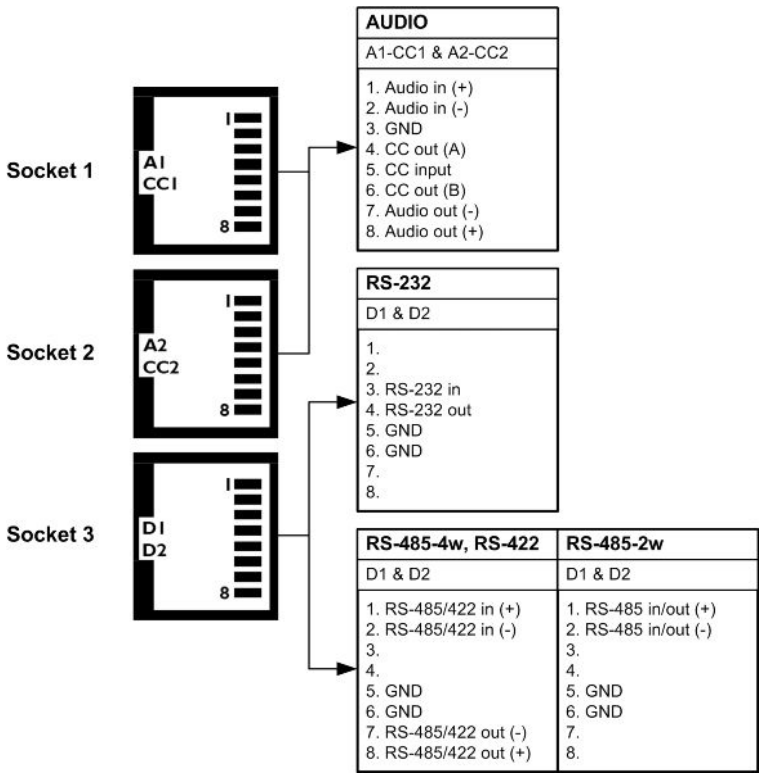
The sync LED displays as described in Front Panel (on page 10).

Important: Before any signal connection can be made, at least a valid IP address (the unit's identity for the network) and a subnet mask must be assigned to the unit. Refer to Connections (on page 15) for details on how this can be done.

4.4 Connector Pin Assignments

Modular socket pin assignments

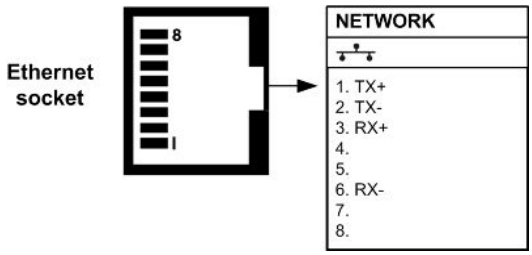
The modular socket pin assignments are such that similar sockets of different modules may be connected back to back with reversed cable (RS-232 interfaces excepted). See the figure below for the socket pin numbering convention used. For 2-wire RS-485 links, I/O is through pins 1 and 2 of socket 3.



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 Updating Device Definitions

If the S-60 D-MC 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 TKH Security MX applications. An existing installation of the SNM Configuration and Service Tool will also be updated.

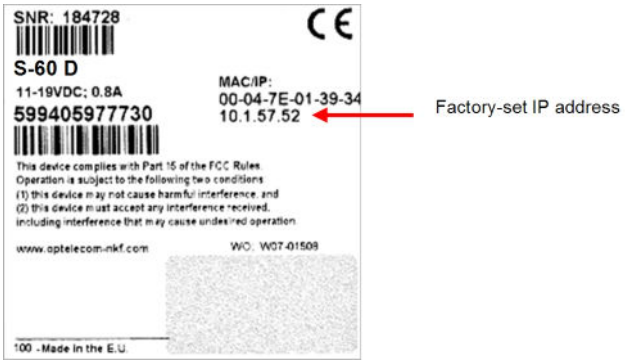
5 Connections

With your TKH Security unit installed, the next step is to establish an IP connection and set up video and (if applicable) other signal links. This chapter describes how to change the factory-set IP address and subnet mask of the S-60 D-MC to be compatible with the network segment in which the unit will be used. Additionally, it discusses how to configure signal streaming.

In This Chapter

5.1 Establishing a Network Connection

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



S-60 D-MC product sticker

Note: This is the address the unit will revert to if you issue a Reset to factory settings; incl. network settings (see "" on page 69) command and reboot the unit.

To open communication with the S-60 D-MC from a host PC and change the unit's network settings, perform the following steps.

Step 1:	Set the PC's network adapter to the unit's factory default subnet and connect the two devices.
Step 2:	Access the unit from a web browser or other tool installed on the PC.
Step 3:	Set the unit's IP address and subnet mask to the subnet it will be used in and reboot the unit.

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

Step 1: Setting the host PC to the factory default subnet of the unit

⏩ To configure the network adapter on the host PC

1 In the Control Panel, open **Network Connections**.

2 Right-click the connection to be configured, and select **Properties**.

3 In the items list, select **Internet Protocol (TCP/IP)**.

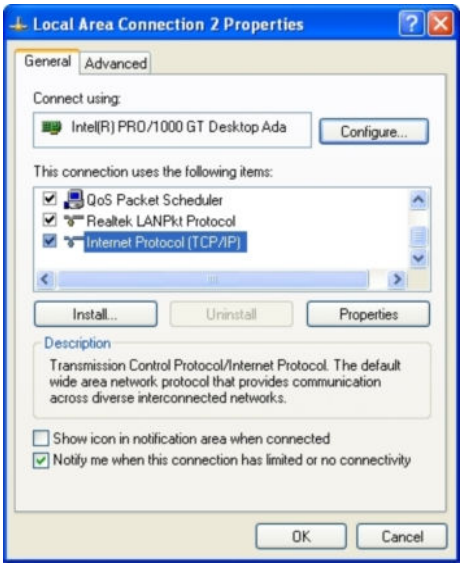
4 Click **Properties**.

5 In the Internet Protocol (TCP/IP) Properties dialog, click **Use the following IP address**.

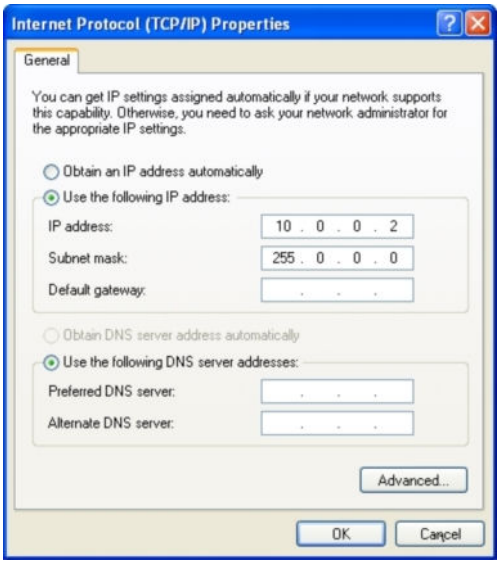
6 Enter an IP address that will assign your PC to the same subnet as the unit (i.e., within the 10.x.x.x range). Use 255.0.0.0 as a subnet mask.

> **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**, and then click **Close**.



Opening IP settings on the host PC



Changing host PC IP settings to the factory-default settings of the unit

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

Step 2: Accessing the unit

Using a standard web browser you can now log on to the S-60 D-MC's internal web server.

Step 3: Changing the unit's network settings

The Network web page enables you to make the unit's network addressing compatible with the network it will be hooked into. 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.

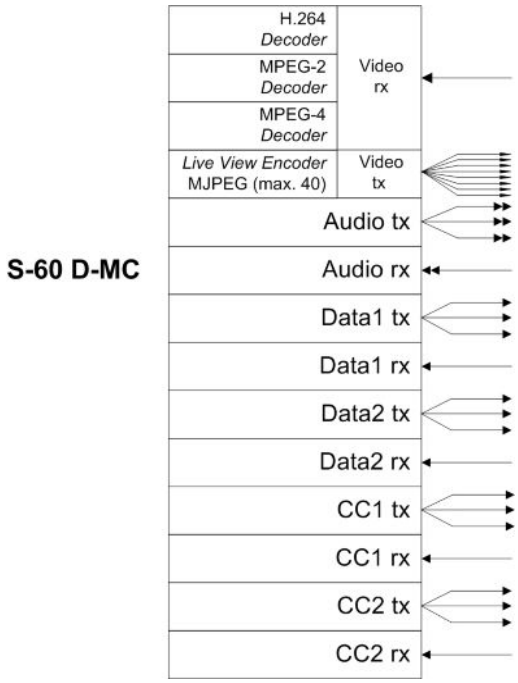
5.2 Making Video, Audio, Data, and Contact Closure Connections

Connection methods

With the S-60 D-MC's IP connection established, video and other signal connections can be made. The most convenient way to do so is using the module's internal web pages. For an elaborate description, see the Working with the Web Pages (on page 24) chapter. Separate application software, such as MX Configuration Tool, can be used as well.

Streams and connectors

Each signal stream received and transmitted by the S-60 D-MC can be conceived of as using virtual connectors. Each of the decoder's virtual connectors has a name; through the internal web pages, the receivers can be assigned a port number that 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 an S-60 D-MC.

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

The S-60 D-MC automatically detects the format of the received video stream and activates the corresponding decoder.

General procedure for making links

In both connection methods mentioned above, making a unicast one-way link (video, audio, data, contact closure) from source to destination entails at least the following steps:

- 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 numbers, consult Multicasting, Multi-Unicasting, and Port Numbers (on page 74).

6 Interfaces

A variety of methods can be employed to communicate with the S-60 D-MC. 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 Open Streaming Architecture (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. The *SPI API* enables easy integration of the S-60 D-MC with third-party products. The protocol consists mainly of different CGI (Common Gateway Interface) program calls for listing and configuring parameters. For detailed information, refer to the *SPI* specification. You can download this HTTP API specification at www.tkhsecurity.com/support-files.

Note: The S-60 D-MC supports the TKH Security C-, S-, and V-series codecs, and the HD-, MD-, HSD-, and MSD-series dome cameras, based on the v2.5.x up to v3.10.x firmware range. Third-party IP cameras, 1080p and 720p HD are not supported.

6.2 Web User Interface

Using the S-60 D-MC's internal web server is the most straightforward way to access the unit. The S-60 D-MC's web pages enable you to configure the unit's settings and view live video images from a standard web browser, eliminating the need for a separate application program.

6.3 MX/IP

MX/IP, a proprietary TKH Security protocol, offers direct access to the unit's settings contained in the *Management Information Base* (MIB), a list of variables stored inside the unit. The MIB can be read and/or written with special MX software. *MX Configuration Tool*, for example, offers full control of the S-60 D-MC through the MIB, enabling you to remotely configure device settings and manage media streams. For more details on the MX/IP protocol, the MIB and TKH Security's EMX network service, refer to the manuals documenting the MX Software Development Kit and MX Configuration Tool..

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

6.4 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 D-MC for conditions or events that require administrative attention. For more details, refer to appropriate literature on SNMP.

The S-60 D-MC supports in-band SNMP. Via SNMP several status variables can be read and traps can be generated on events. S-60 D-MC SNMP settings can be configured on the SNMP tab of the unit's Device Management web page.

The SNMP Agent is MIB-2 compliant and supports versions 1 and 2c of the SNMP protocol. The MIB database can be downloaded at www.tkhsecurity.com/support-files.

7 Accessing the Internal Web Server

The web pages of the S-60 D-MC offer a user-friendly interface for configuring the unit's settings and viewing live video images over the network. This chapter explains how to connect to the S-60 D-MC's built-in web server.

In This Chapter

7.1 System Requirements

To access the S-60 D-MC's web pages you need the following:

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

7.2 Login Procedure

To log on to the unit's internal web server

1 Open your web browser.

2 Enter the S-60 D-MC 's IP address in the address bar of the web browser.

If your network configuration is correct you are directed to the unit's login page.

If the login page does not display correctly you may need to enable JavaScript in your web browser (see Appendix: Enabling JavaScript).

3 In the Login section, click **LOGIN**.

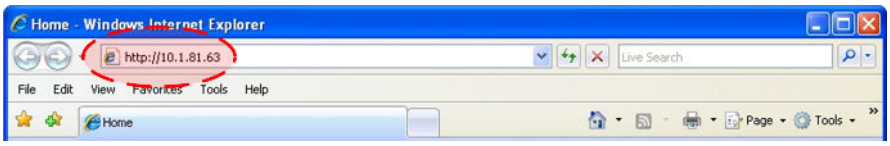
4 In the Connect box, log in as either "admin" or "root".

The default login is "admin" with an empty password.

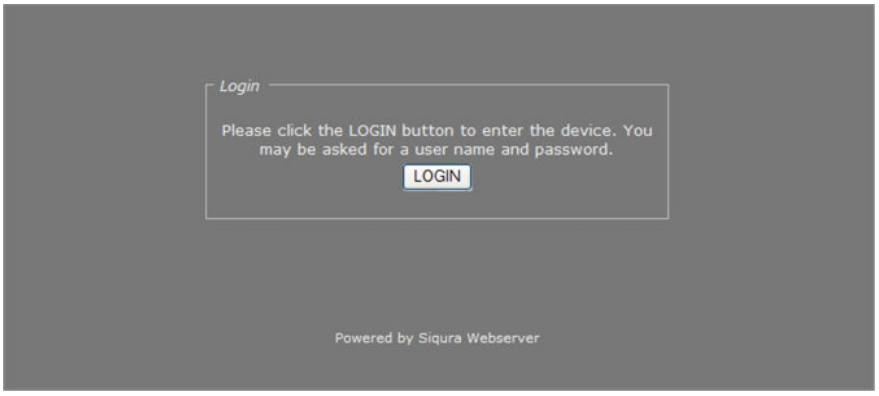
5 Click **OK** or press ENTER.

Upon successful login, the Live Video page, the home page of the unit, displays.

Important: Logging in as "root" confers admin rights plus additional rights associated with the root account. Therefore, this account should *always* be password protected.



Entering the unit's IP address in the browser's address bar



S-60 D-MC login page

Connect box

8 Web Page Features

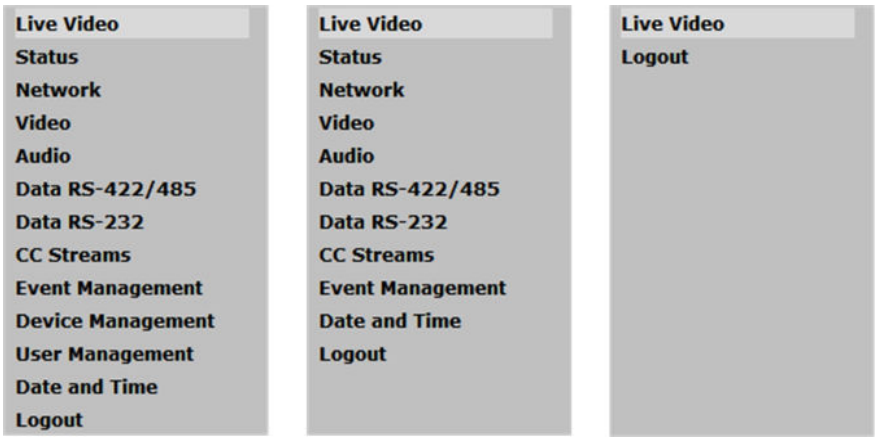
Navigation Menu

Using the menu on the left of each web page you can navigate to the other web pages. The first option in the menu is the home page of the S-60 D-MC. The pages listed below the home page enable you to view and configure the device settings of the unit.

Three-level access control

Whether a specific S-60 D-MC web page is visible and available to you on the navigation menu depends on the user account you logged in with. The unit has three access levels: *Admin*, *Operator*, and *Viewer*. Admins have full access to the web pages. They can create, edit, and delete user accounts on the User Management page. The Operator level grants access to the device configuration pages, but not to user management or device management. Viewer access is restricted to the home page.

A special account is the 'root' account. Logging in with this account (user name = root) confers Admin rights plus additional rights associated with the root account. The root account should *always* be password protected. For more information, refer to the description of the User Management page.



S-60 D-MC menu options available to (from left to right) Admin, Operator, and Viewer accounts

Logging out

Selecting the Logout option on the navigation menu logs out the current user and displays the Login box.

Sections, buttons, and tabs

Apart from the menu, the web pages share the following features.

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

After editing, press **Save** to write changes to the unit.
Press **Cancel** to undo unsaved changes and show the values as they were prior to editing.

Note: Some sections do not have *Save* and *Cancel* buttons. Changes you make in these sections are immediately written to the unit.

Some of the web pages/tabs have an *Advanced Settings* section which is displayed by clicking **Advanced >>**. Click **<< Simplified** to hide the Advanced Settings.

Important: Please be aware that configuring advanced settings requires in-depth understanding of the impact of your changes on the workings of your S-60 D-MC unit. If in doubt, do not change the default values.

9 Working with the Web Pages

A standard browser on a desktop or laptop PC with a connection to your video network is all it takes to view live video decoded by the S-60 D-MC. Working with the web pages you can also configure the S-60 D-MC's device settings and remotely upgrade the embedded software. This chapter provides a detailed description of the individual web pages.

In This Chapter

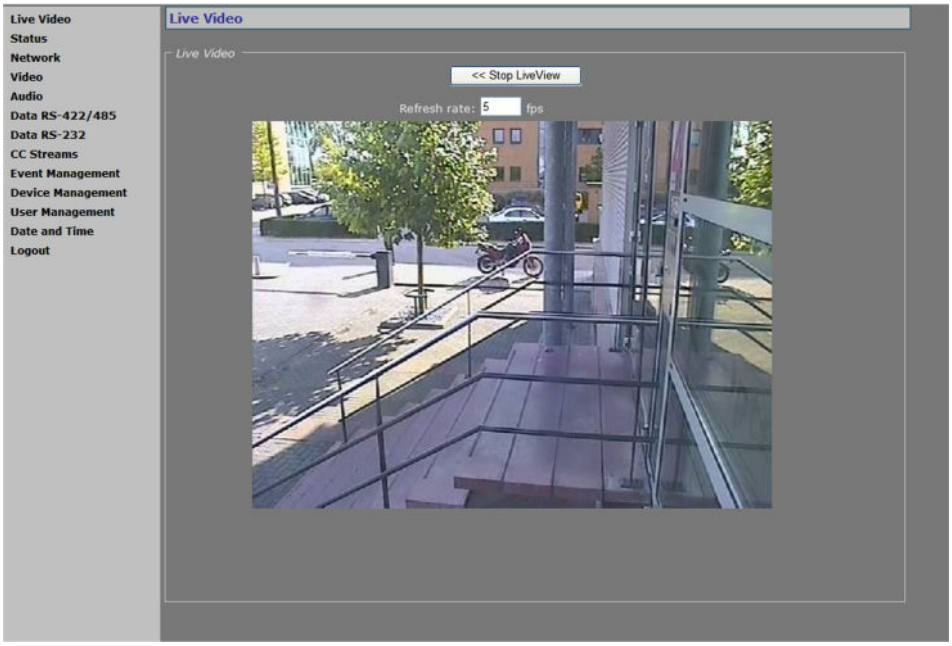
9.1 Live Video

Live Video page, LiveView inactive

Home page

After a successful login, the home page of the S-60 D-MC displays. On this page, named Live Video, you can view live images decoded by the unit. The Live View function is inactive when the page opens.

9.1.1 Viewing live video



Live Video page, LiveView activated

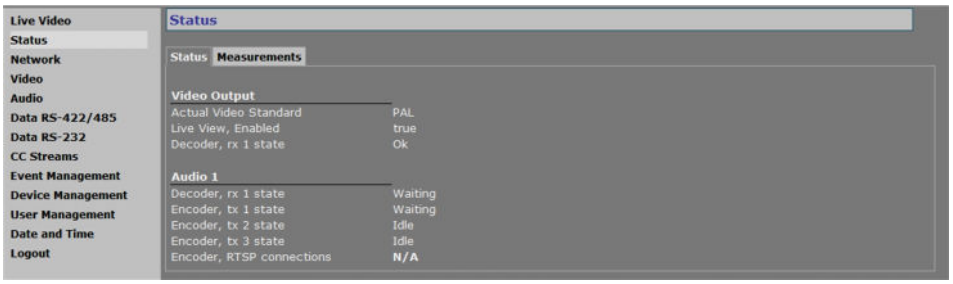
Activating live view

Pressing the *Play LiveView* >> button opens a preview showing the received video stream. As the images in the preview are generated by the Live View Encoder (on page 34), this encoder must be enabled. The video source can be defined on the Decoder tab (on page 30) of the Video page.

Live Video

<<Stop Live View	Closes the preview.
Refresh rate	Indicates the current refresh rate of the web page (Internet Explorer only). For Mozilla Firefox and Google Chrome, multipart streaming MJPEG (max 24 fps) is used.

9.2 Status



Status page: a snapshot with automatic page updating

Tabs

The Status page has two tabs: *Status*, and *Measurements*.

9.2.1 Status

Stream states

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

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

Troubleshooting connection or decoding issues

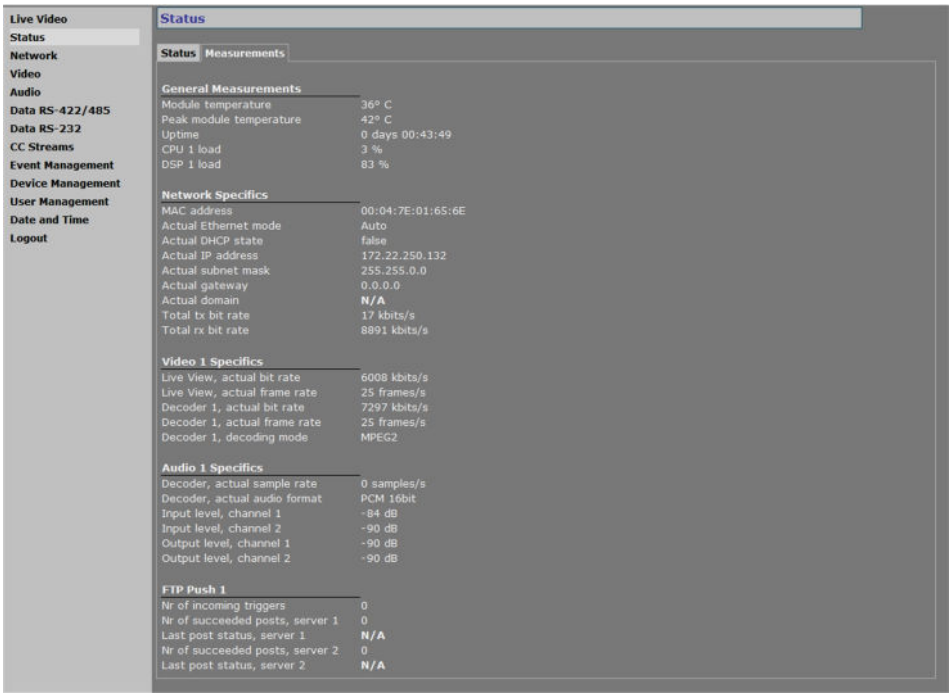
In addition to the stream states reported on the Status page, on-screen status messages appearing on a connected external display or in the web page previews can point you to problem causes.

Status OSD	
No Stream	Possible causes: With enabled receiver, • the transmitter is not enabled. • an incorrect IP address is configured. • an incorrect port number is configured.
Decode Error	With properly configured network settings and a correctly received network stream, specific decoder settings or capabilities do not match the corresponding encoder equivalents. They may hold different values for the RTP type, for example, or the stream contents are in the wrong format. For more information, see the description of the Advanced Settings of the Decoder tab on the Video page.

These messages may also appear when working with frame rates below 1 fps.

Note: When the receiver is disabled, a black screen without status OSD message displays.

9.2.2 Measurements



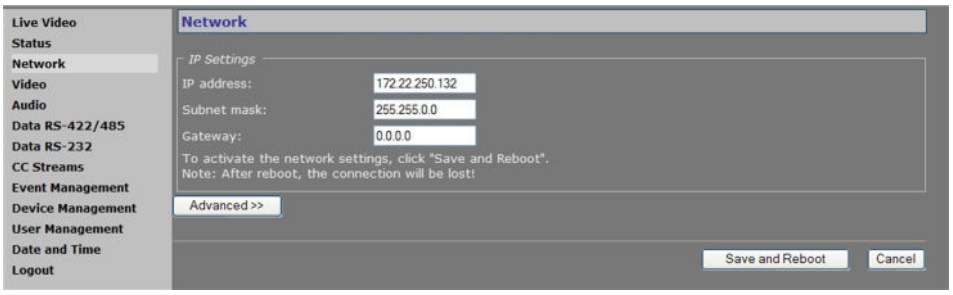
Measurements tab: a snapshot with automatic page updating

Measurements

The Measurements tab shows module temperatures (current and peak), module uptime, network specifics, such as the MAC address and the actual IP address, the network load from this module, the load information per processor, and signal stream-specific details.

The FTP Push 1 section can be used to monitor the FTP push process. See also FTP Push tab (on page 40).

9.3 Network



Network page

IP Settings

On the Network page, you can set the unit's IP address, subnet mask and gateway IP address.
For correct functioning of the S-60 D-MC, 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 D-MC; for details, see Establishing a Network Connection (on page 15). Having made the internal web pages accessible in this way, you can use the Network page to change the default network settings to the desired settings.

For IP address input to be valid, the unit's IP address:

- must be within the 1.0.0.1 – 223.255.255.254 range
- cannot start with 127 (reserved for loopback on local host)

Do not forget to *Save and Reboot* after changing IP settings.

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

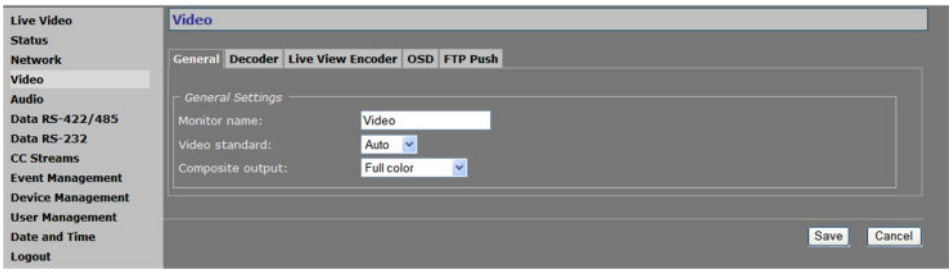
9.3.1 Advanced Settings

Network page, Advanced Settings

Pressing the **Advanced>>** button on the Network page gives you access to the following settings.

Network	
DHCP enable	Allows assigning of the IP address by a DHCP server instead of using static IP addressing.
Ethernet mode	Transmission mode and speed. • *Auto* - Autonegotiation (default) • *10 HDX* - Half duplex, 10 Mbit. • *10 FDX* - Full duplex, 10 Mbit. • *100 HDX* - Half duplex, 100 Mbit. • *100 FDX* - Full duplex, 100 Mbit
IGMP unsolicited reports enable	Enables sending of unsolicited messages, such as requests to join a multicast group, for example, without having to wait for a query message from a management PC, multicast router or switch.

9.4 Video



Video page

Note: The first time you access the Video page, you may encounter a security alert concerning the installation of a Java update. This add-on, required for web pages to be displayed properly, does not give rise to any security risks. You can install it safely.

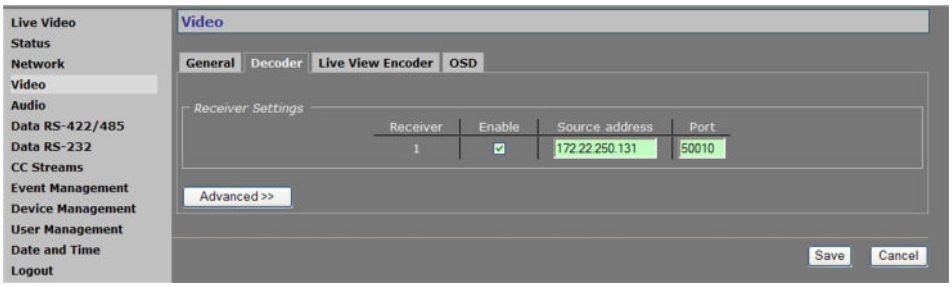
Tabs

The Video page has five tabs: *General*, *Decoder*, *Live View Encoder*, *OSD* and FTP Push .

9.4.1 General tab

General Settings	
Monitor name	Enter a name to identify the video output. The following characters are not allowed in monitor names: **! , ? ~ &**
Video standard	*PAL*, *NTSC*, or *Auto*. The video display standard.
Composite output	*Full color* (default) or *Black and White.*

9.4.2 Decoder tab



Video page, Decoder tab

9.4.2.1 Making a Video Connection

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

- configuring the encoder's settings
- configuring the decoder's settings

To configure the encoder's settings

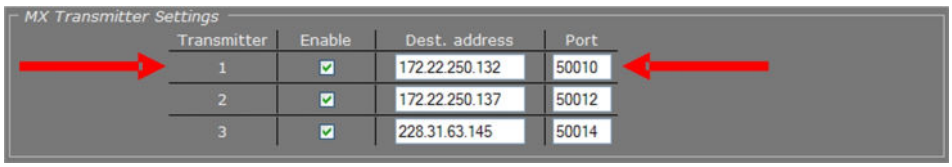
1 Open the encoder's web pages, go to the Video page, and select the appropriate Encoder tab.

2 In the Transmitter Settings section, specify the destination IP address.
This is the address of the video decoder that will be receiving the video stream.

3 Enter the decoder's port number.
For more information, see Port Numbers (see "" on page 75).

4 Select **Enable**.

5 Press **Save**.



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

To configure the decoder's settings

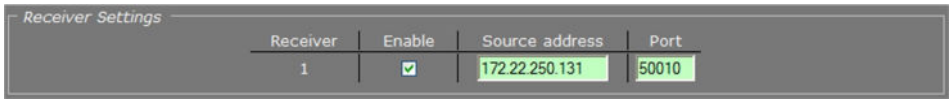
1 Open the decoder's web pages, go to the Video page, and select the Decoder tab.

2 In the Receiver Settings section, specify the source IP address.
This is the address of the video encoder that will be transmitting the video stream.

3 Enter the decoder's own port number.
For more information, see Port Numbers (see "" on page 75).

4 Select **Enable**.

5 Press **Save**.



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

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

Note: Source and destination IP addresses can be unicast or multicast. For more information, see Multicasting (see "" on page 74).

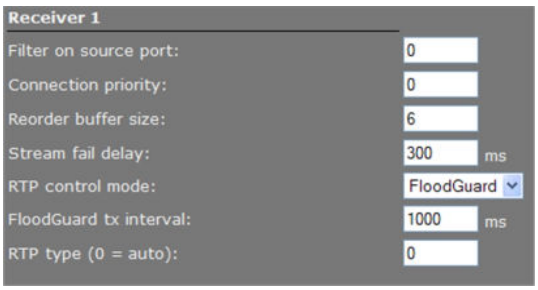
Highlighted fields

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.

9.4.2.2 Advanced Settings

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

Receiver 1



Advanced Section, Receiver 1 settings

Receiver 1

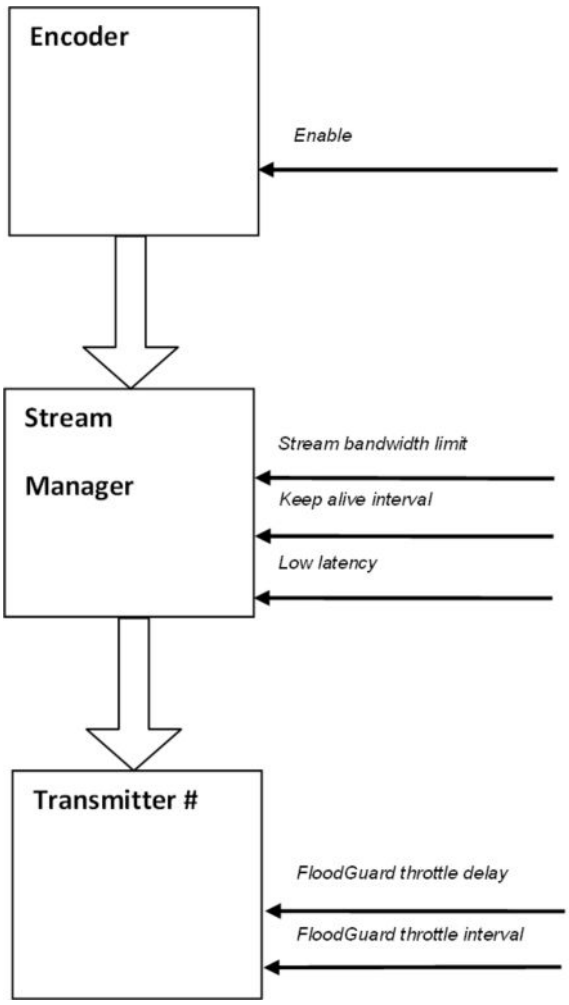
Filter on source port	Can be used to filter incoming signals. With multiple signals sent to the same IP address and destination port number, *Filter on source port* can be used to filter the input, i.e. to accept only signals from the transmitting port specified here. The filter will not be active if set to 0 (the default and recommended setting).	
Connection priority	Parameter intended for use with MX Software Development Kit.	
Reorder buffer size	Used to reorder incoming packets. Default: 6.	
Stream fail delay	Range: [0...10000] ms. Default: 300 ms. Timeout in ms before going to NoStream state.	
RTP control mode	Select the transport protocol to control the stream.	
	None	No transport protocol selected.
	FloodGuard	Flooding prevention mechanism. For more information, see the note on FloodGuard later in this chapter.
	RTCP	Real-Time Control Protocol, a network control protocol for use in communications systems to control streaming media servers.
FloodGuard tx interval	Interval at which the receiver sends control messages to the transmitter (see the section on FloodGuard).	
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.	

9.4.2.3 RTP and RTCP

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.

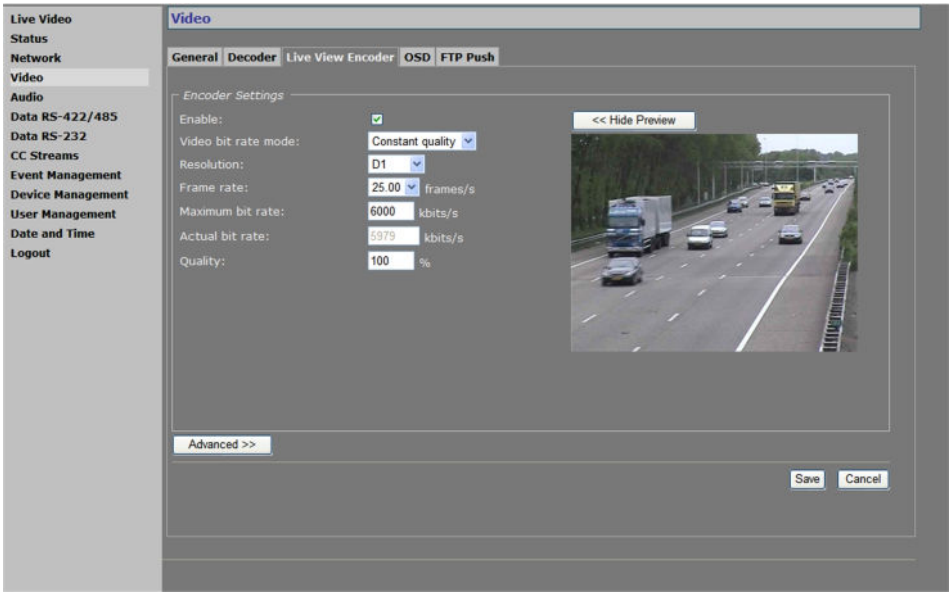
9.4.2.4 FloodGuard

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

9.4.3 Live View Encoder



Video page, Live View Encoder tab

Encoder Settings

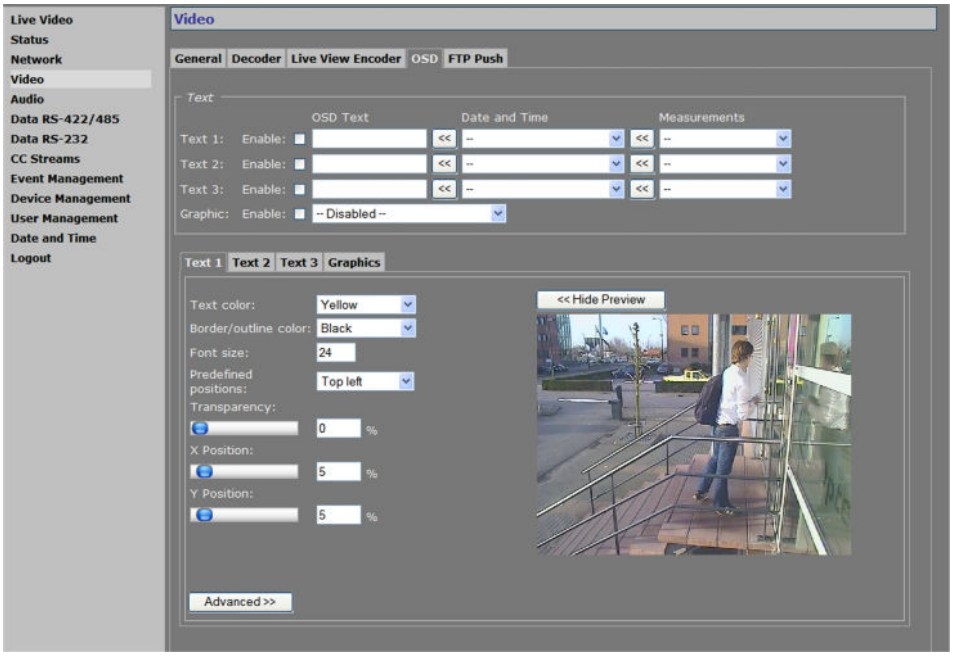
Enable	Enable the Live View Encoder to convert the input signal to MJPEG format and transport it over HTTP, to upload images to an FTP server using FTP Push (see "FTP Push tab" on page 40), and/or to use the previews on this page and the Live Video page.	
Video bit rate mode	*Constant quality*	Keeps the image quality constant, with varying network load. The quality is determined by the value set for the *Quality* parameter (see below).
	Constant bit rate	Keeps network load constant at the cost of varying image quality. Frames may be skipped.
Resolution, Frame rate, Maximum bit rate	Set sensible combinations of mode, resolution, frame rate and maximum bit rate.	
Actual bit rate	Available in Constant quality mode (CQM). This field is dynamically updated with the current bit rate to provide feedback on the bit rate that is used on average with the current Quality setting (see below).	
Quality	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 see live images and the effect of your settings.	
<< Hide Preview	Closes the preview. This may improve webpage responsiveness.	

9.4.3.1 Advanced Settings

Live View Encoder, Advanced Settings

Advanced Settings	
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	

9.4.4 On-Screen Display (OSD)



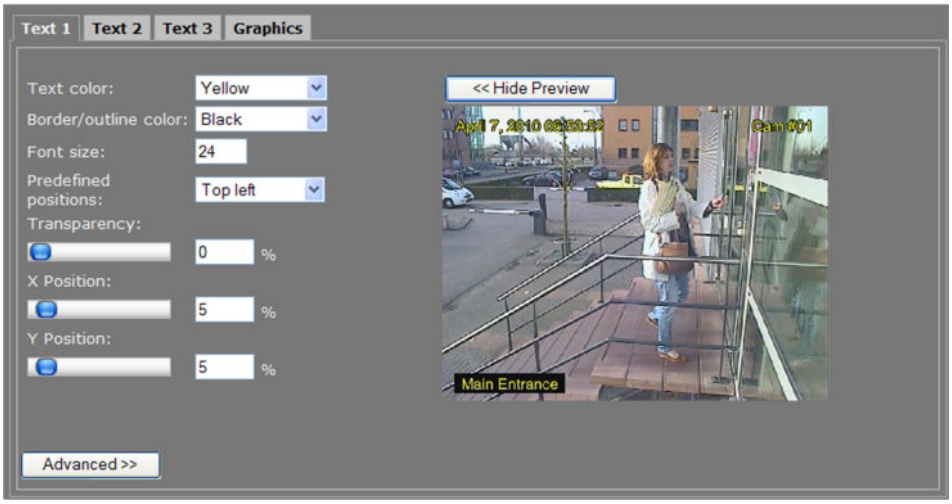
Video page, OSD tab

OSD facilities

The S-60 D-MC features programmable on-screen display 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.

Text	
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 the Advanced Settings on the Graphics tab (on page 38) - can be selected from the list and enabled.

9.4.4.1 Text # tab



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

Text

Text color/ Border/ outline color	Changes you make here (and in the other fields in this section) are immediately written into the device and reflected in the preview.
Font size	Range: [1...256].
Predefined positions	Presets for positioning the OSD bar.
Transparency	Drag the sliding button or enter a percentage.
X Position	Variables that enable you to freely position the object, instead of using the presets. Drag the sliding buttons or enter a percentage. When a preset has been selected, changing one of its defined parameters sets the *Predefined positions* box to '--', indicating that a custom position has been configured.
Y Position	
Show Preview>>	Click to view live images and see the effect of the current settings.
<< Hide Preview	Closes the preview. This may improve webpage responsiveness.

Advanced Settings

Advanced OSD Bar # Settings

Advanced OSD Bar # Settings

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

Font Management

Text # tab: Font Management settings

For OSD texts, you can use the S-60 D-MC's default fonts or fonts you upload to the unit.

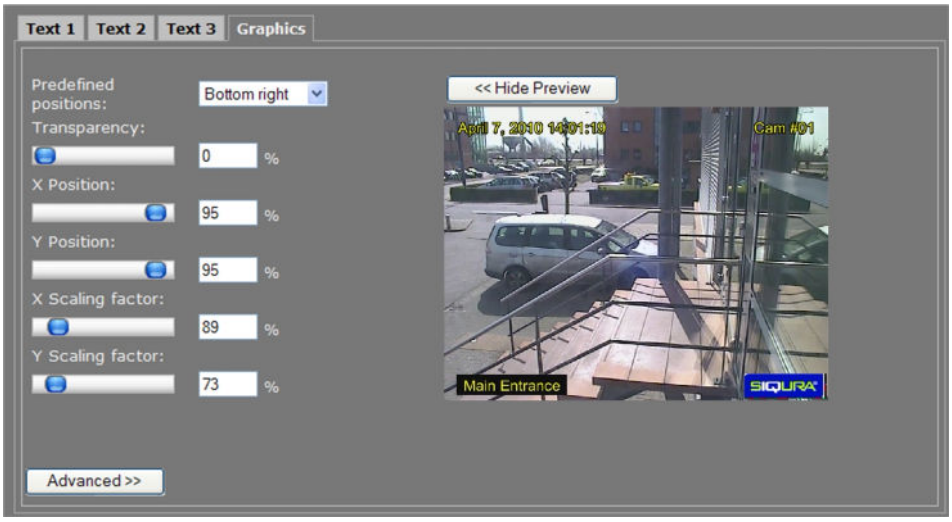
To upload a font

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.

9.4.4.2 Graphics tab



Graphics tab with 3 OSD bars and a graphic (bottom right) in the preview

The Graphics tab enables you to upload graphics (see Graphic management), and scale and position a selected graphic on your screen.

Graphics

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

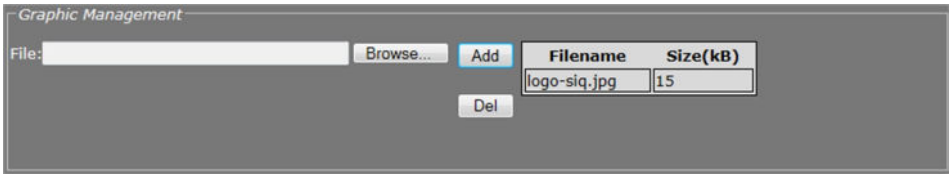
Advanced Settings

Graphics tab: Advanced Picture Settings

Advanced Picture Settings

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.

Graphic Management



Graphics tab: Graphic Management

To upload a graphic

1 In the *Graphic Management* section, click **Browse**.
The *Open* dialog box displays.
2 Browse to the folder containing the graphic to be uploaded.
3 Select a file with the correct file extension (.bmp, .gif, .jpg, jpeg), and then click **Open**.

The file appears in the *File* textbox.

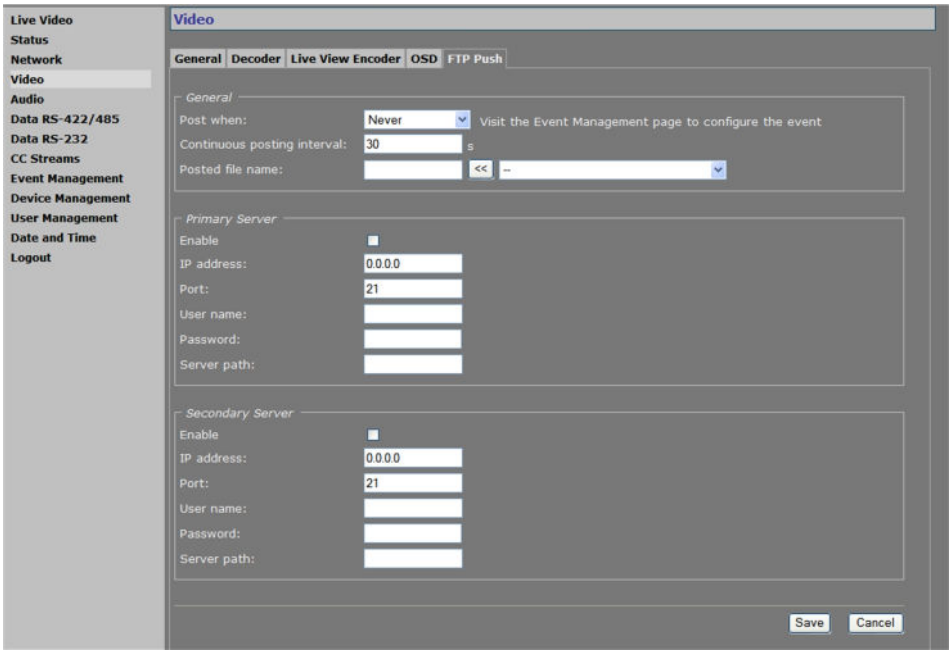
4 To start the upload, click **Add**.

The graphic is added to the graphics list and to the *Graphic* drop-down list in the *Text* section.To remove a graphic

1 In the *Graphic Management* section, select the graphic.

2 Click **Del**.

9.4.5 FTP Push tab



Video page, FTP Push tab

JPEG image posting

The S-60 D-MC 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.

General

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

FTP server

A target FTP server must hold a user account associated with the S-60 D-MC. You can assign a primary server and a secondary server. Images are posted simultaneously to both the primary server and secondary server.

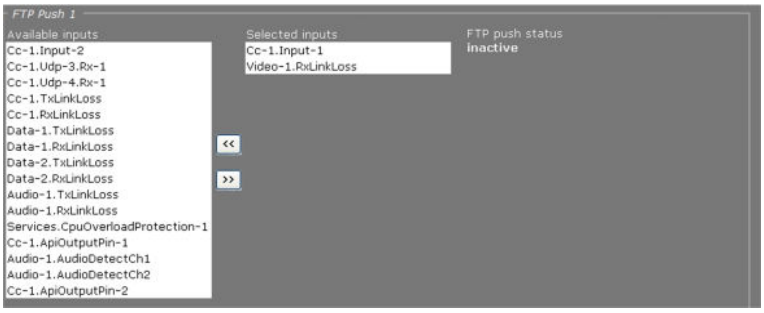
FTP Push, Primary Server, example settings

Primary/Secondary Server

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.

Event Management

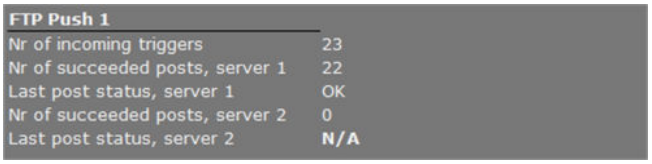
Having selected *Event On*, *Event Off*, or *Event Changed* as a trigger, do not forget to go to the Event Management page to associate one or more events with the FTP push.



Event Management page: FTP Push 1 section. Two inputs associated with FTP push.

Monitoring and troubleshooting 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.

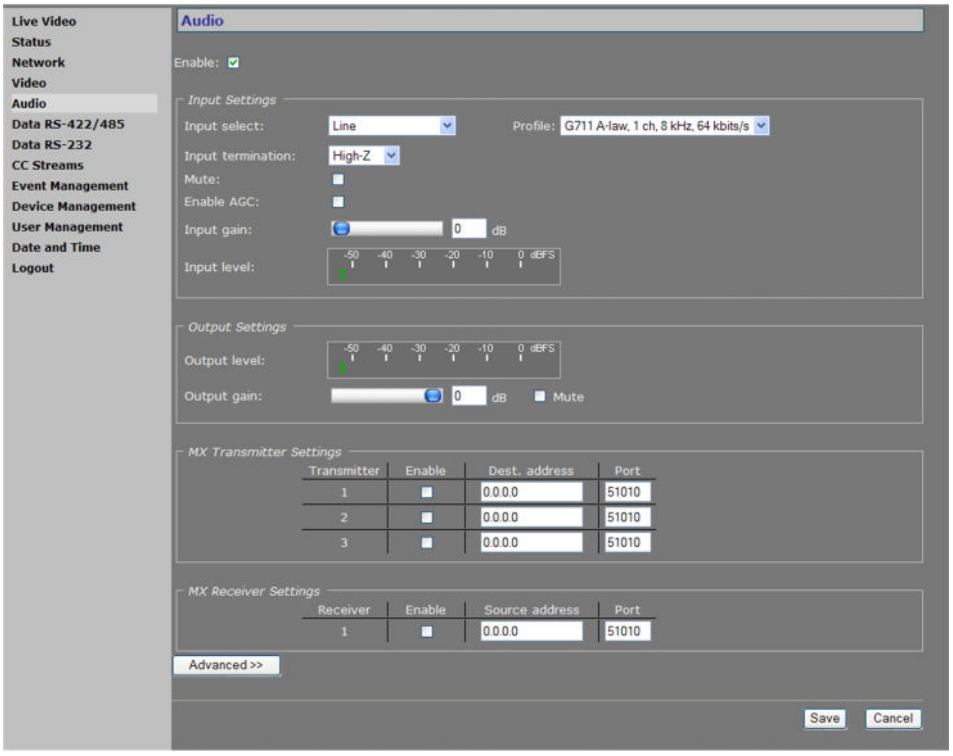


Status page, Measurements tab: FTP Push 1 section

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.

Last post status: example of error message

9.5 Audio



Audio page

Enabling/Disabling audio

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.

Input Settings

Input select	*Line*, *Microphone*, or *Microphone + bias*.
Input termination	Can be set to *High-Z* or *600 ohms*, 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 *Save*.
Input level	VU meter to display audio input level.
Profile	Preset combinations of settings. A non-standard setting configured through the Advanced Settings gives '--' in the Profile selector.
	G711 A-law. 1 ch. 8 kHz 64 kbit/s • default setting • mainly used in Europe • mono, low quality • used for QuickTime
	G711 µ-law. 1 ch. 8kHz. 64 kbit/s • mainly used in USA • mono, low quality • used for Genetec's Omnicast
	Legacy PCM • 2 channels (stereo) • high quality, 15.7 kHz • compatible with all TKH Security products

Output Settings

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

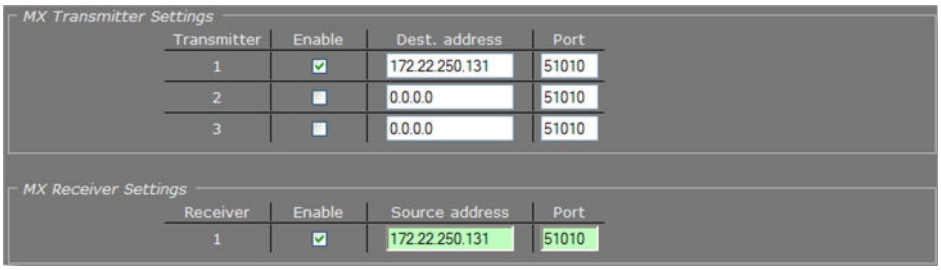
MX Transmitter Settings

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.

MX Receiver Settings

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 D-MC.

9.5.1 Making Audio Connections



Transmitter and Receiver sections, two-way audio

Audio streams

The S-60 D-MC provides bidirectional audio. The S-60 D-MC 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

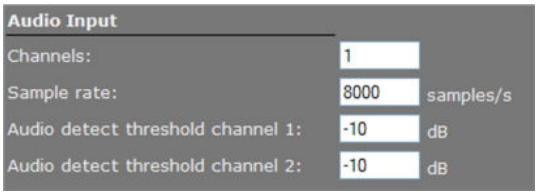
The source address and port number fields are highlighted in green when the enabled receiver receives a stream from the specified source. The two fields are marked in red when no stream is received with the receiver enabled and correctly configured.

Two-way audio

The figure above shows the setup for two-way audio on the side of the S-60 D-MC. 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 D-MC 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.

9.5.2 Advanced Settings

Audio Input



Advanced Settings, Audio Input

Audio Input

Channels	Range: [1…2]. When selecting 1 channel, only the signal on the 'A1' input is used (either line or microphone).
Sample rate	Range: [7500…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: • 7845 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	

Audio Output

Advanced Settings, Audio Output

Audio Output

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

Audio Encoder

Advanced Settings, Audio Encoder

Audio Encoder

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

Audio Decoder

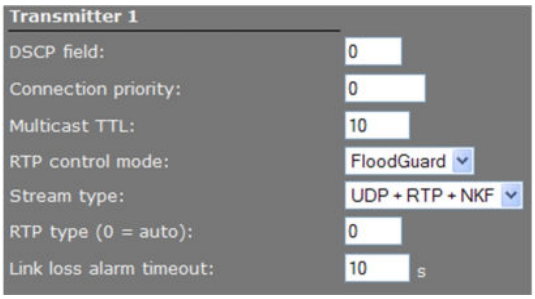
Advanced Settings, Audio Decoder

Generally speaking, Audio Decoder settings will follow the settings of the source, i.e. 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.

Audio Decoder

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: [7500…48000]. Examples (for 1 and 2 channels): • *7845 Hz* A-law • *15710 Hz* A-law • *15710 Hz* PCM • *43200 Hz* PCM
Audio format	*PCM 16bit*, *A-law 8bit*, *μ-law 8bit*.

Transmitter

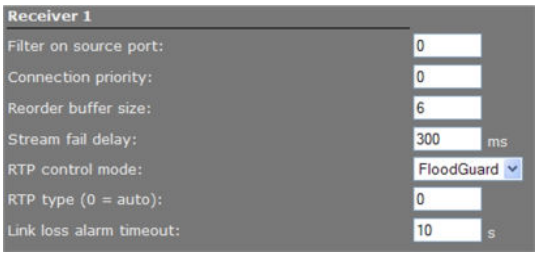


Advanced Settings, Transmitter #

Transmitter

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]. Range: [0...127]. Specify the number of routers (hops) that multicast traffic is permitted to pass through before expiring on the network.	
RTP control mode	Select the transport protocol to control the stream.	
	None	No transport protocol selected.
	FloodGuard	Flooding prevention mechanism. For more information, see the note on FloodGuard later in this chapter.
	RTCP	Real-Time Control Protocol, a network control protocol for use in communications systems to control streaming media servers.
Stream type	*UDP + RTP*	Default setting. Plain RTP stream over UDP.
	UDP + RTP + NKF	Adds an extended RTP header for 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.	

Receiver 1

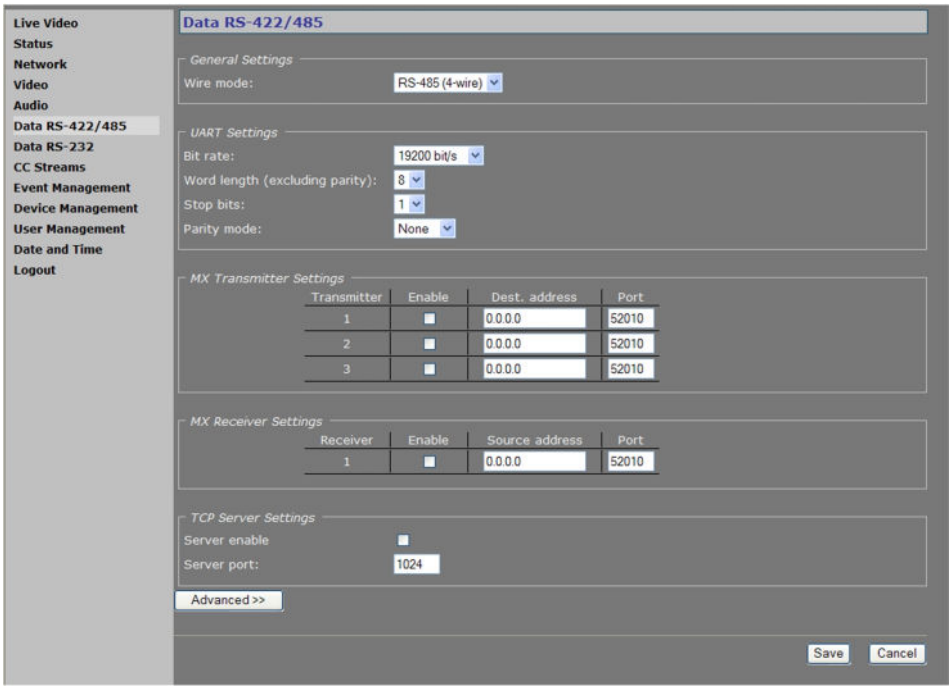


Advanced Settings, Receiver 1

Receiver 1

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

9.6 Data RS-422/485



Data RS-422/485. Transmitter and receiver can be configured in the usual manner.

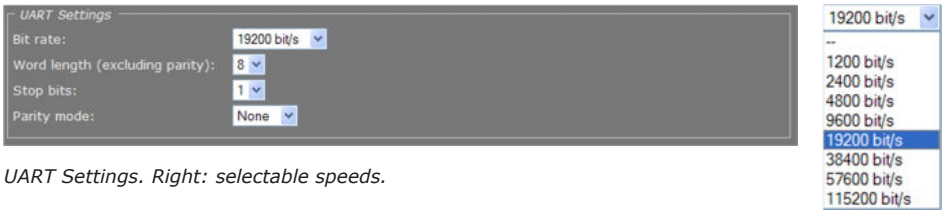
General Settings

Wire mode selection

General Settings

Wire mode	*RS-422*, *RS-485 (2-wire)*, or *RS-485 (4-wire)*. The RS-4xx interface type on the RJ-45 DATA socket is set in software. Select the type of RS-4xx interface from the Wire mode list.

UART Settings



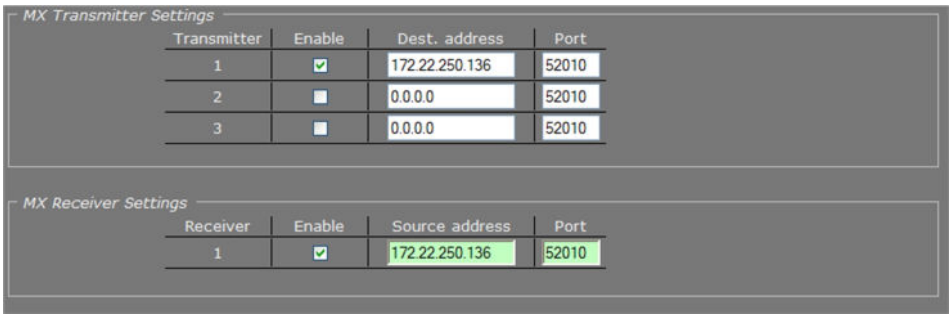
UART Settings. Right: selectable speeds.

UART

The S-60 D-MC uses a Universal Asynchronous Transmitter/Receiver (UART) for data transmission. The UART will recognize and reproduce the words in the data stream. This is only possible if the UART is programmed to understand the serial data format.

UART Settings	
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*.
Stop bits	*1*, *2*.
Parity mode	*None*, *Odd*, *Even*, *Mark*, *Space*. This setting should be the same as in the connected device (e.g., a PTZ camera).

Making data connections



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 codec. 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.

TCP Server Settings

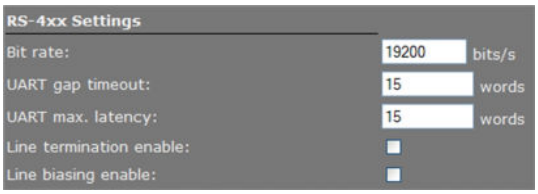
TCP Server Settings

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

TCP Server Settings	
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].

9.6.1 Advanced Settings

RS-4xx Settings



Advanced Settings, RS-4xx

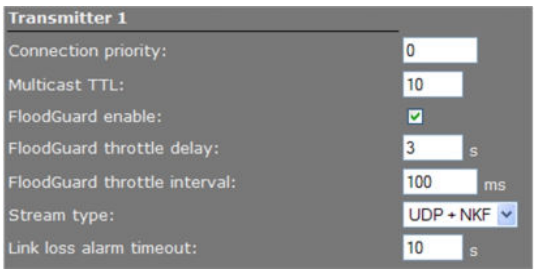
For details about 'data words' and data transfer optimization, see the note below.

RS-4xx Settings

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 timeou*t 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.

Transmitter

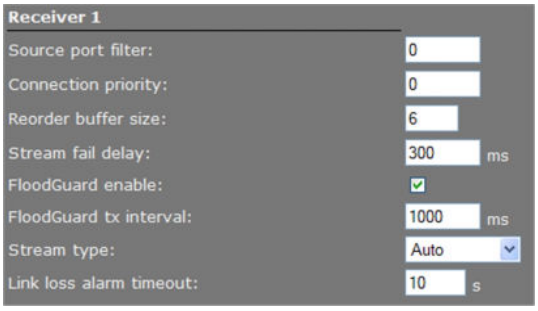


Advanced Settings, Transmitter 1

Transmitter

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.

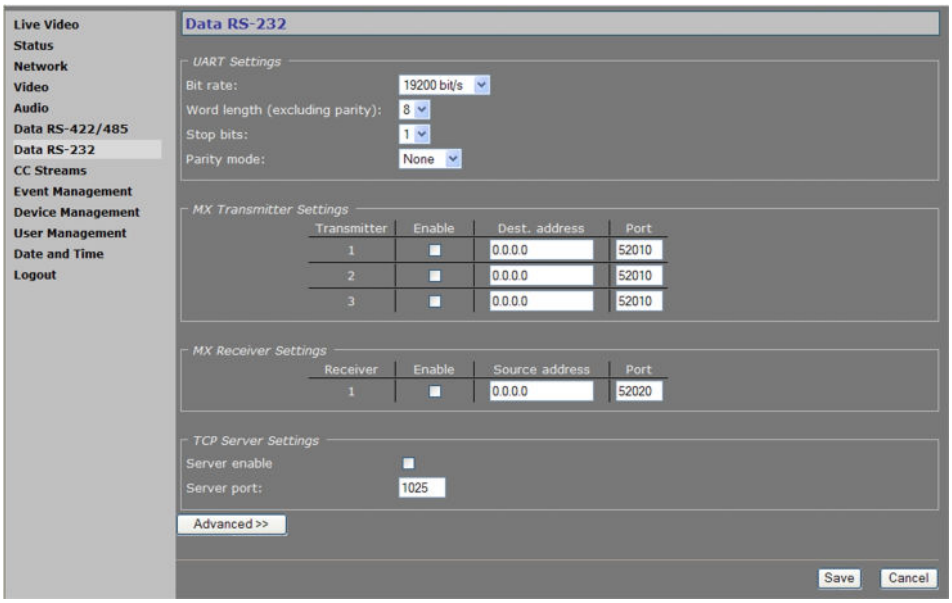
Receiver



Advanced Settings, Receiver 1

Receiver #	
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.

9.7 Data RS-232



Data RS-232 page

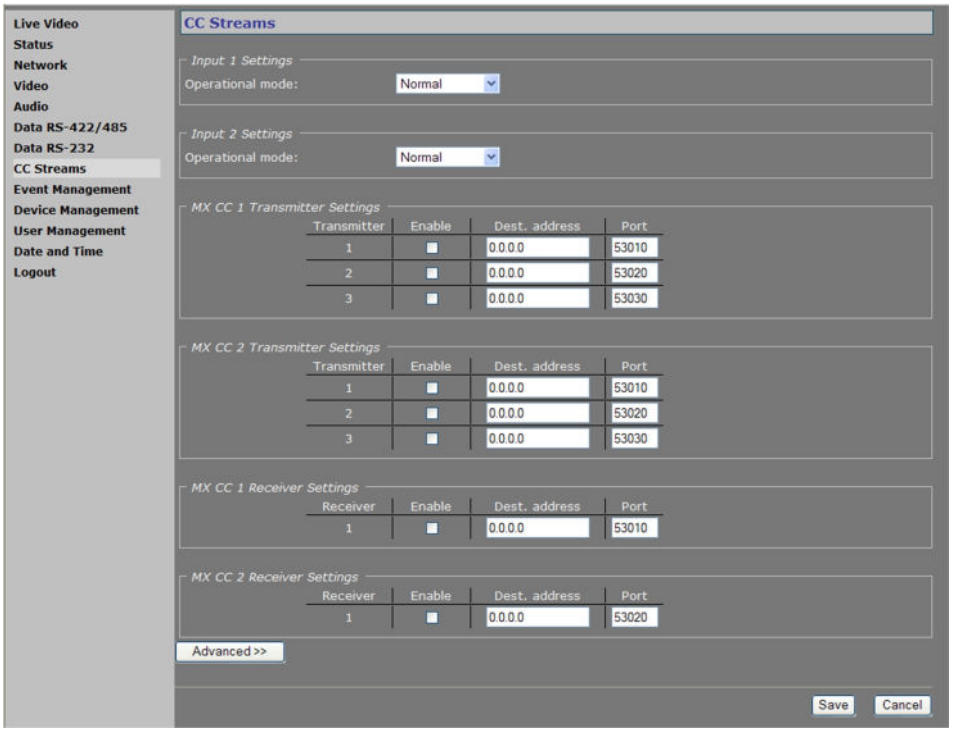
Configuring RS-232 settings

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, refer to 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.

9.8 CC Streams



CC Streams page

CC channels

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

Note: You can also control CC Outputs directly from the Event Management page.

Input # Settings

Contact Closure Input 1 Settings

Input # Settings

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

9.8.1 Making Contact Closure Connections

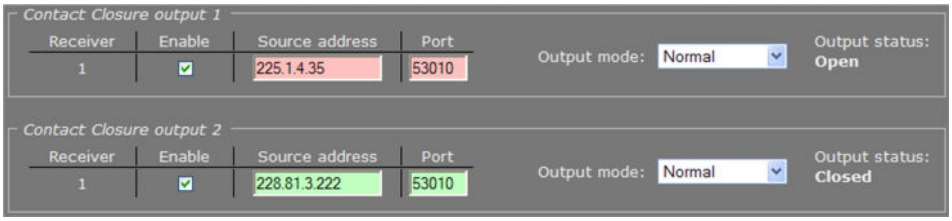
To make a contact closure connection

- 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.

Highlighted fields

The destination address and port number fields are highlighted in green (as shown below) when the enabled receiver receives the contact closure stream over the network. The two fields are marked in red when no stream is received with the receiver enabled and correctly configured.



CC Output 2 receiving a stream. CC Output 1 not receiving.

9.8.2 Advanced Settings

CC # Settings, Transmitter

Advanced Settings, CC 1, Transmitter 1

Transmitter

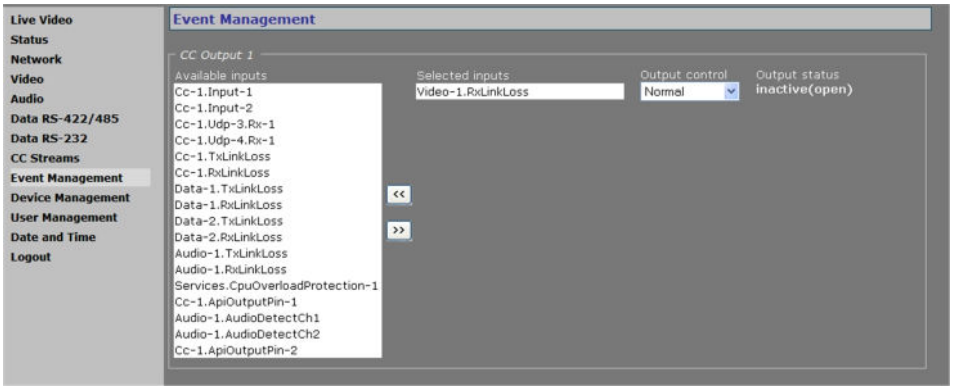
Connection priority	Parameter intended for use with MX Software Development Kit.
Multicast TTL	Range: [0...127]. Specify the number of routers (hops) that multicast traffic is permitted to pass through before expiring on the network.
Link loss alarm timeout	Range: [1...1000] s. Default: 10 s. Time in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

CC # Settings, Receiver 1

Advanced Settings, CC #, Receiver 1

Receiver	
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.

9.9 Event Management



Event Management page

Associating events with output facilities

You can use the Event Management page to configure how the S-60 D-MC 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.

CC Output

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

CC Streams

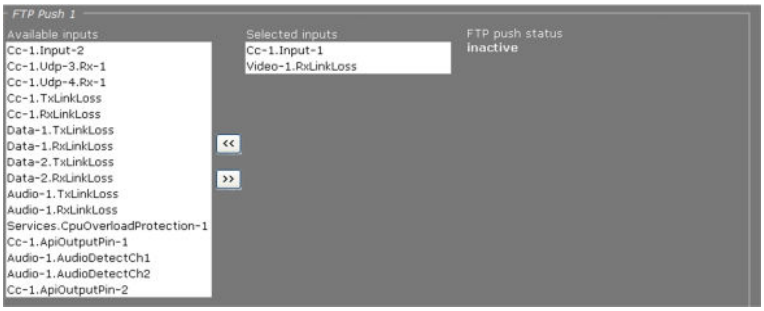
CC Streams 1

CC Streams

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

FTP push

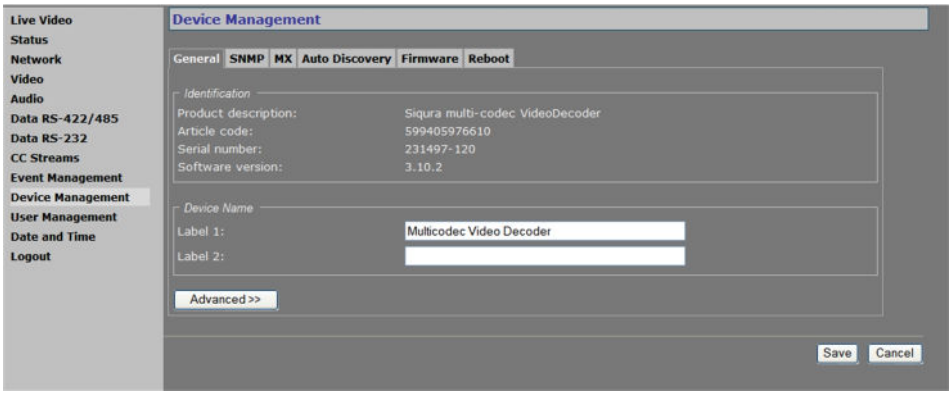
If FTP push is configured to be event-triggered (see the FTP Push tab of the Video page), you need to select one or more sources from the Available inputs list that will activate an image upload to the FTP server(s).



FTP Push 1 section. Two inputs associated with FTP push.

FTP Push 1	
Available inputs	List of sources that can be selected as triggers for an FTP push.
Selected inputs	On selection of multiple inputs, the inputs are connected with a logical OR. Any one will cause an image upload to the FTP server.
FTP push status	*Inactive (open)* or *active (closed).* Active: one or more of the selected inputs is true. Inactive: none of the selected inputs is true.

9.10 Device Management



Device Management, General tab

Tabs

The Device Management page has six tabs: *General*, *SNMP*, *MX*, *Auto Discovery*, *Firmware*, and *Reboot*.

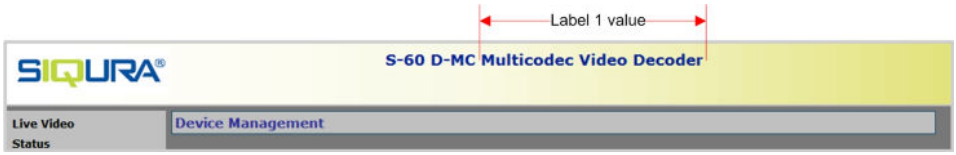
9.10.1 General tab

Identification

This section offers administrative module information.

Device name

Label 1 Label 2	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 1 value in Title pane

9.10.1.1 Advanced Settings

Device Management: Advanced Settings

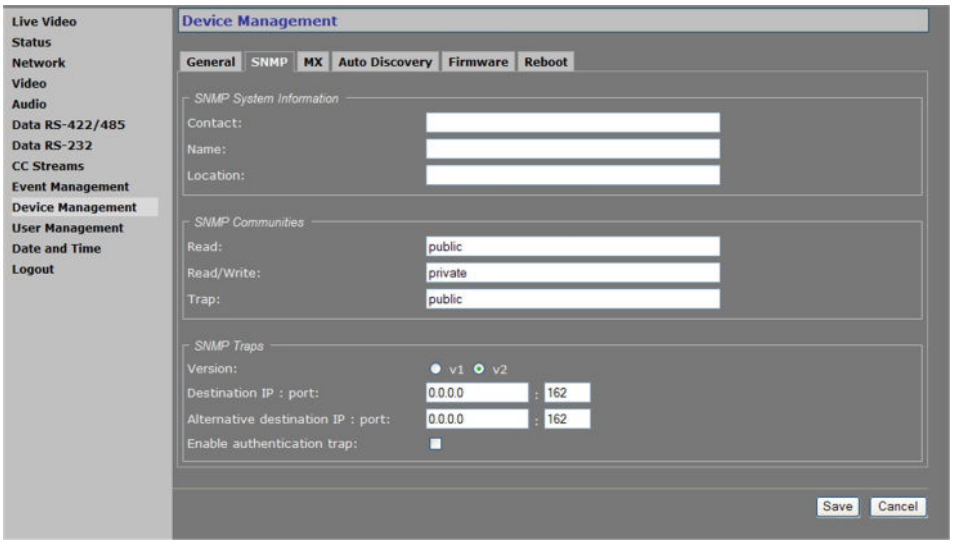
Alarm Settings

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).

Identify

Flashing DC LED	Range: [0 …1000]. To identify a S-60 D-MC, when housed in a rack among other units, for instance, enter a value and click **Save**. The DC LED on this particular unit will blink for the number of seconds you set.

9.10.2 SNMP



Device Management, SNMP tab

SNMP MIB

To prepare a S-60 D-MC for SNMP management, the database documenting the S-60 D-MC variables that can be read or modified must be registered with the program; such SNMP MIB documents (indicated OPTC) are available from TKH Security or from its website.

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. The module has an SNMP Agent running which listens on port 161.

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.

SNMP Traps

A S-60 D-MC alarm status change will generate a trap which can be caught by any SNMP manager. *Version* and *Destination IP : port* are required fields.

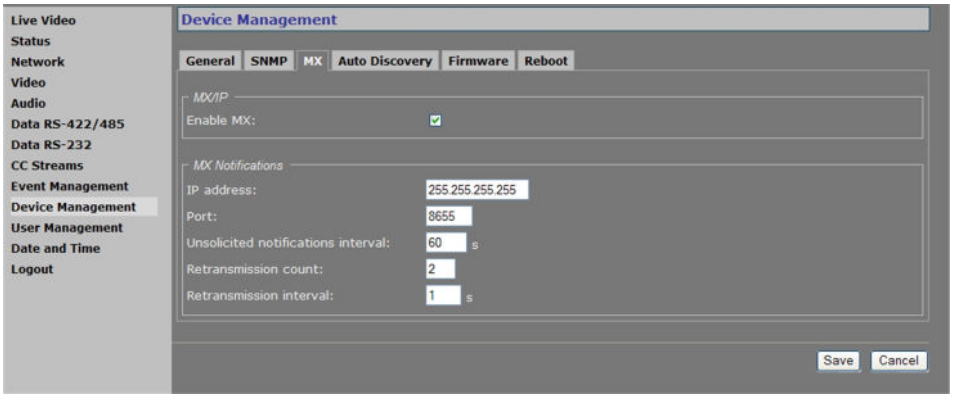
SNMP Traps

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.

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 (see - http://www.ietf.org/rfc/rfc1213.txt?number=1213).

9.10.3 MX



Device Management, MX tab

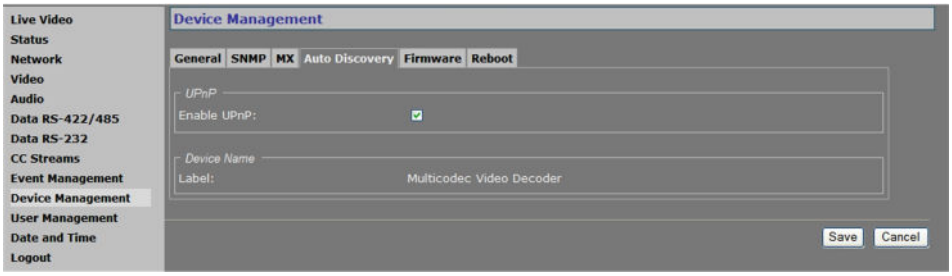
MX/IP

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.

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

MX Notifications	
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.

9.10.4 Auto Discovery



Device Management, Auto Discovery

Advertising the S-60 D-MC on the network

On the Auto Discovery tab you can enable UPnP (Universal Plug and Play). If enabled, UPnP will allow the S-60 D-MC 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 (for example, Device Spy).

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 D-MC supports the following Universal Plug and Play (UpnP) functionality: Discovery, Description (partly supported), and Presentation.

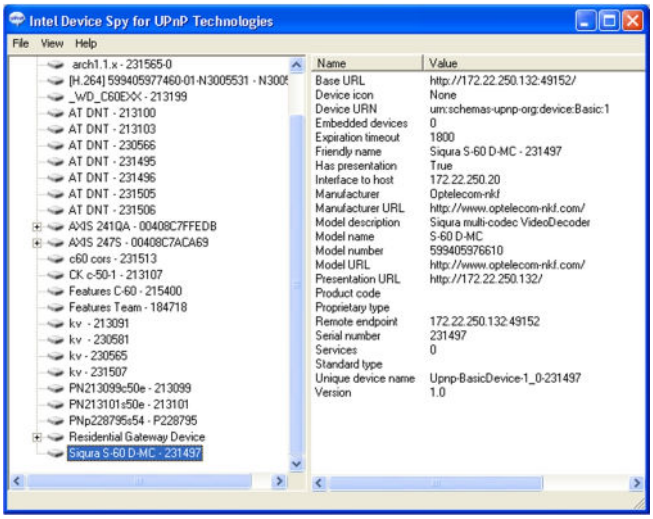
Testing the S-60 D-MC's UPnP functionality

After enabling UPnP, you can use a tool, such as Device Spy (included in the 'Developer Tools for UPnP Technologies'), to check if the S-60 D-MC correctly advertizes its presence and device description on the network.

⏩ To view the S-60 D-MC device description in Device Spy

1 Start Device Spy.
The network is scanned.
A list of detected UPnP devices displays in the left-hand panel.
2 Select your S-60 D-MC in the left-hand-panel.

The device description is shown in the right-hand panel.



S-60 D-MC device description in Device Spy

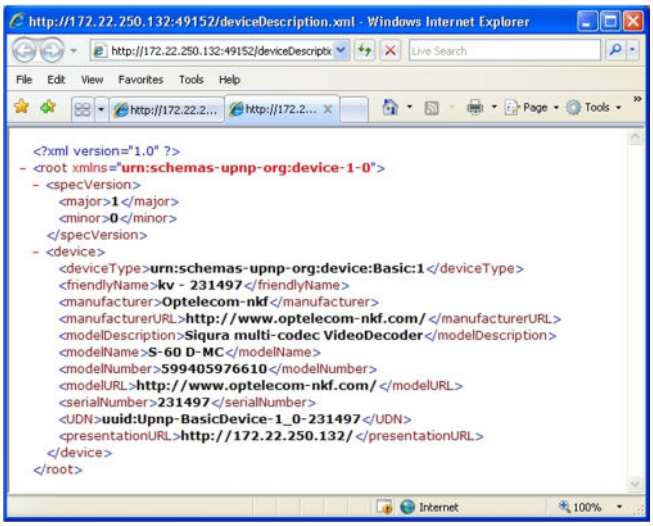
To view the S-60 D-MC device description in XML (using Device Spy)

1 Start Device Spy.

2 In the left-hand panel, right-click the S-60 D-MC entry.

3 Select **Get Device XML**.

The XML device description opens in your web browser.



S-60 D-MC XML device description

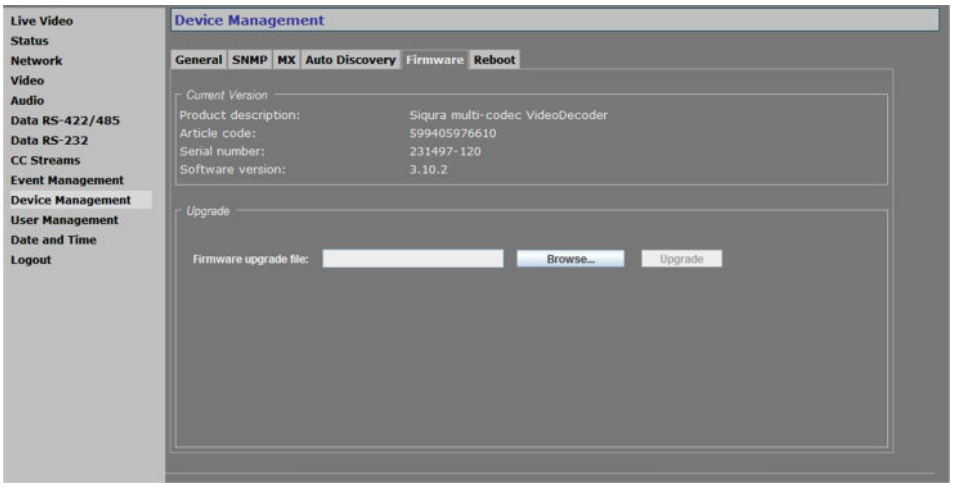
To access the S-60 D-MC's web pages via Device Spy

1 Start Device Spy.

2 In the right-hand panel, double-click the **Presentation URL** entry.
-or-
In the left-hand panel, right-click the S-60 D-MC entry, and then select **Display Presentation Page**.
The login page of the S-60 D-MC displays in your browser.

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

9.10.5 Firmware



Device Management, Firmware tab

Note: The first time you access the Firmware tab after opening your web browser, you are asked to authenticate. Next, a security alert displays. Using the S-60 D-MC firmware upgrade feature requires Java Runtime Environment 1.6 or higher. The TKH Security application does not give rise to any security risks. You can run it safely.

Firmware images

The S-60 D-MC 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 D-MC 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 D-MC.

Important: If an error should occur during the upgrade procedure, the S-60 D-MC will not revert to a former upgrade image. Instead, it will be downgraded to the fixed image.

Current version

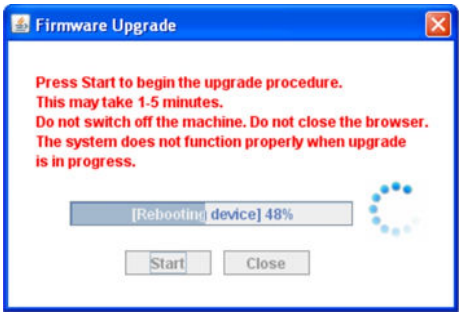
This section offers information on the currently active firmware version.

Upgrade

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

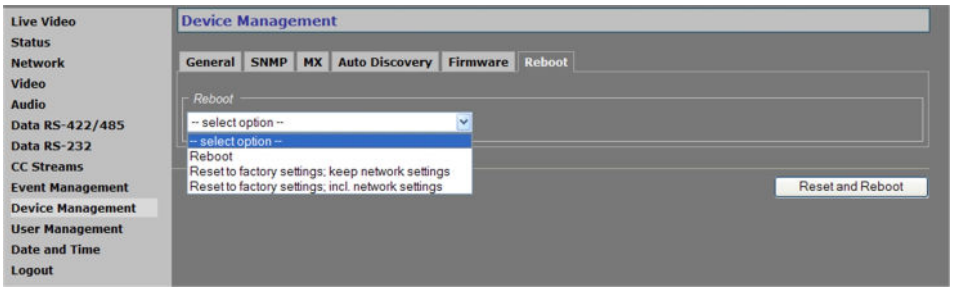
To upgrade the S-60 D-MC firmware

1 On the *Device Management* web page, open the **Firmware** tab.
2 In the *Upgrade* section, click **Browse**.
The *Open* dialog box displays.
3 Browse to the folder containing the firmware image.
4 Select the appropriate file (`.nkffw` extension), and then click **Open**.
The Article code and Software version appear in the *Upgrade* section.
5 Click **Upgrade**.
6 In the *Firmware Upgrade* dialog box, click **Start**.
A progress bar informs you on the task's completion percentage.
7 Upon completion, click **Close**.



Firmware upgrade progress

9.10.6 Reboot

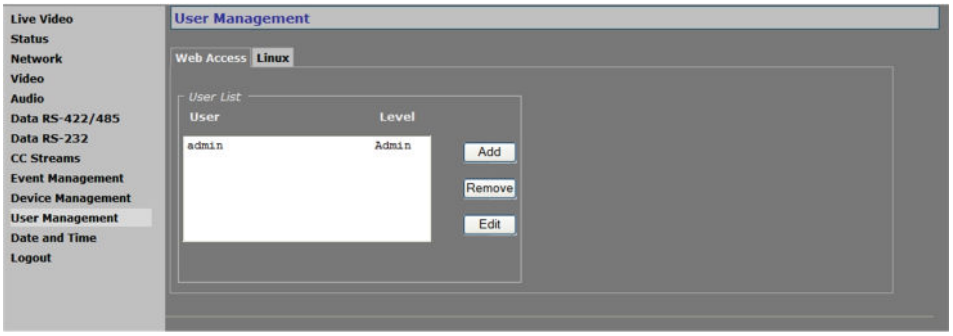


Device Management, Reboot options

Reboot

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 D-MC.

9.11 User Management



User Management, Web Access tab

Tabs

The User Management page is available to users with an Admin account. It has two tabs: *Web Access* and *Linux*.

9.11.1 Web Access tab

Three-level access control

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

Managing user accounts

To add a user

1 On the *User Management* page, open the **Web Access** tab.

2 In the *User List* section, click **Add**.

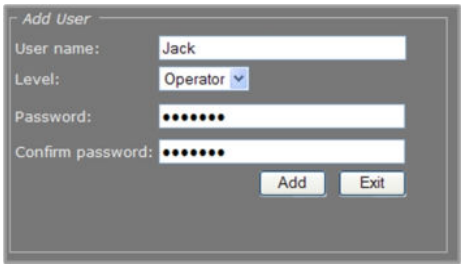
The Add User section displays.

3 Enter the new user name (alphanumeric and underscore only) and password. Confirm the password to prevent errors.

4 Select the appropriate access level.

5 To write the settings into the unit, click **Add**.

The user is added to the User List.



Adding a user

To edit a user

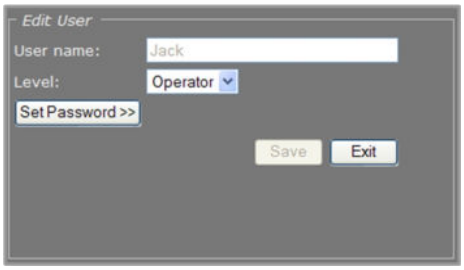
1 On the *User Management* page, open the **Web Access** tab.

2 Select the user name from the *User List*, and then click **Edit**.

The Edit User section displays.

3 Modify the user name, permission level, and/or password.

4 To write the settings into the module, click **Save**.



Editing a user

To delete a user

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

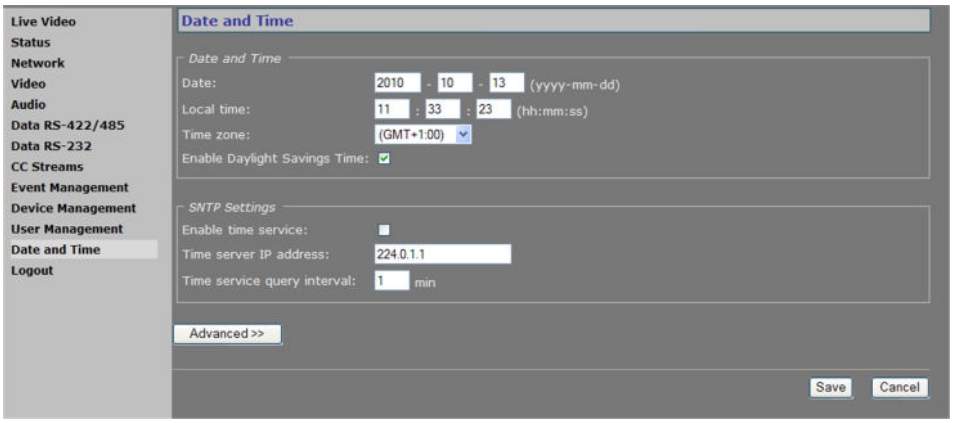
9.11.2 Linux tab

Linux root password

Root password

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 empty 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.

9.12 Date and Time



Date and Time settings

Date and Time

The S-60 D-MC has a battery-supported real-time clock that can be adjusted either manually (as shown above), or automatically with the aid of an SNTP (Simple Network Time Protocol) server. After entering changes, press Save to make them permanent.

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

The S-60 D-MC adds 1 hour to the local time when Daylight Savings Time is enabled. The unit does *not* automatically change between summer and winter time. The user has to set the proper state in the Date and Time section of the web page (or use an MX/IP command).

SNTP Settings

If enabled, the SNTP server is queried automatically by the internal clocks, with a configurable time interval.

⏩ To set up the S-60 D-MC for use with an SNTP server

1 In the *SNTP Settings* section, clear the **Enable time service** check box, and then click **Save**.

2 On the *Time zone* list, select your local zone.

3 Select **Enable Daylight Savings Time**, if required.

4 Click **Save**, and then wait for 2 seconds.

5 Set the **Date** and **Local time** values.

A maximum error of 5 minutes is allowed for these settings.

6 Click **Save**.

7 In the *SNTP Settings* section, select the **Enable time service** check box, and then click **Save**.

The unit will now synchronize (within the interval set in the SNTP Settings section) to the time server and remain synchronized, also after reboots.

Notes for advanced users

- Far off (more than a few minutes) or jumping time server values may be rejected by the unit.

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

9.12.1 Advanced Settings

Date and Time: Advanced settings

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

10 Multicasting, Multi-Unicasting, and Port Numbers

The S-60 D-MC can be used in a multicast setting. This chapter outlines IP multicasting and additionally describes the concept of multi-unicasting. You also learn about assigning valid port numbers.

In This Chapter

10.1 Multicasting

IP multicast

The S-60 D-MC 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 D-MC 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 D-MC 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 D-MC, 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.

10.2 Multi-Unicasting

Multi-unicasting

Alternatively, an S-60 D features 'multi-unicasting', i.e. sending out up to three copies of audio, data and contact closure streams. If the bit rates selected are moderate, it may be more convenient to use this mechanism instead of multicasting, even though the network gets more signal to carry from the encoder.

When such a destination is removed, the source also stops sending the corresponding stream. If the input channel of a destination is disabled without disabling the source, source transmission will be throttled, but not disabled (this behaviour is selectable through the FloodGuard settings discussed in the Note on FloodGuard (on page 33). 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.

10.3 Port Numbers

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

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

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

Default port numbers

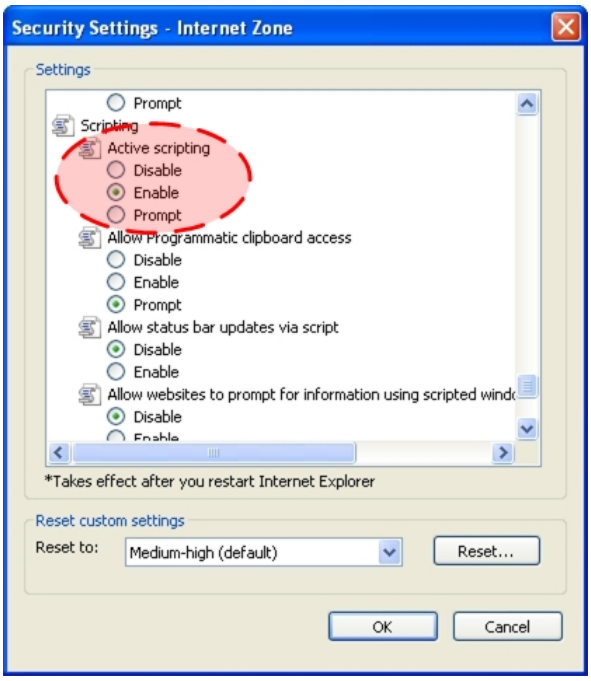
TKH Security MX applications using automatic port number allocation may use 55000 and up.

11 Appendix: Enabling JavaScript

In order for the S-60 D-MC web pages to display correctly, JavaScript must be enabled in your web browser.

To enable JavaScript in Internet Explorer

1 From Internet Explorer's Tools menu, select **Internet Options**.
2 On the Security tab, click the **Internet globe** icon, and then click **Custom level**.
3 In the settings list, search for Active scripting and select **Enable**.
4 Click **OK**, and then close the Internet Options dialog box.



Active scripting enabled