Siqura A-80

Firmware Version 3.2

8-channel audio and contact closure card

User Manual

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

Copyright © 2013 Siqura B.V.

A-80 v3.2
User Manual v1.1 (102105-1a)
AIT55MW10

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

Brand names

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

Liability

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

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

More information

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

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

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

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

Contents

1 Introduction

Document scope

This manual applies to A-80 v3.2, Siqura's 8-channel audio and contact closure card.
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 A-80.

Assumed skills and know-how

To work with a A-80 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
- Audio and contact closure transmissions

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.

2 Safety Information

This chapter contains the A-80 safety instructions.

In This Chapter

2.1 Safety Information

General

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

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.

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*[*] 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.

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

Optical Safety (A-80 /SFP)

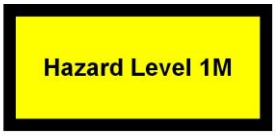
This optical equipment contains Class 1M lasers or LEDs and has been designed and tested to meet **IEC 60825-1:1993+A1+A2** and **IEC 60825-2:2004 safety class 1M** requirements.

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

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

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

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



EMC

The equipment has been tested and found to meet the CE-regulations relating to EMC, and complies with the limits for a Class B device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against interference to radio communications in any installation. The equipment generates, uses, and can radiate radio frequency energy; improper use or special circumstances may cause interference to other equipment or a performance decrease due to interference radiated by other equipment. In such cases, the user will have to take appropriate measures to reduce such interactions between this and other equipment.

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

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

ESD

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

Care and Maintenance

The encoder will normally need no maintenance. In order to keep the module operating reliably, please observe the following.

- Prevent dust from collecting on the module.
- Do not expose the equipment to moisture.
- Keep the module within the appropriate temperature range as described in the Technical Specifications section.

RoHS Statement

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

Product Disposal

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

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

3 Product Description

Siqura A-80 is an eight-channel audio and I/O card for IP applications. This chapter introduces the unit to you by presenting its main features.

In This Chapter

3.1 Product Overview

General

The Siqura® A-80 eight-channel audio and contact closure card offers a compact solution for multiple audio and contact closure channels over IP. The A-80 can be included in almost any existing and new CCTV solution to add audio and contact closures to the system.

Models

The A-80 is to be used in MC 11 or similar Siqura power supply cabinets, but it is also available as a stand-alone module (/SA version). The /SFP version of the A-80 has a pluggable SFP slot for connections via fiber optic cable. A range of multimode or single-mode XSNet™ SFP devices fit the empty SFP slot. Front panel LEDs indicate network status, stream status (sync), and DC power. All models have backup battery power for their clocks.

Audio

The A-80 adds eight separate bidirectional audio channels to the CCTV system. The audio inputs support either line-level or microphone–level with additional biasing to power electret microphones. By using RTP/RTCP in combination with network time synchronization (NTP) the audio streams can be made lip-sync with almost any video stream.

Contact Closures

Eight contact closure inputs can be configured to 'stream' contact closure signals to the Siqura *i*-NVR, for example, or to activate a signal in the API. In addition, the A-80 offers four contact closure outputs to connect with third-party PLCs or other telemetry systems. The CC output can be activated through the API or received CC streams.

Web Interface

Configuration and management are simplified by the access-controlled web interface. Full in-band control is available through Siqura®'s MX™ Configuration Tool Kit or the HTTP API. The Siqura A-80 is field-upgradeable.

Open Streaming Architecture (OSA)

The A-80 is designed to comply with the worldwide adopted standards for streaming audio. OSA offers standardized streaming audio and remote control. All streaming protocols are based on proven standards and tested with different vendors. A comprehensive HTTP API gives access to all controls, which makes integration with third-party equipment easy. The API is available at http://www.siqura.com/. In addition to OSA, the A-80 supports Siqura's unique MX™ protocol.

Compatibility

The A-80 is part of Siqura®, a complete collection of video surveillance equipment and solutions. As such, the A-80 is compatible with Siqura video codecs/servers, IP cameras, video management, network storage, and configuration software. For more information, refer to http://www.siqura.com/.

3.2 Front Panel

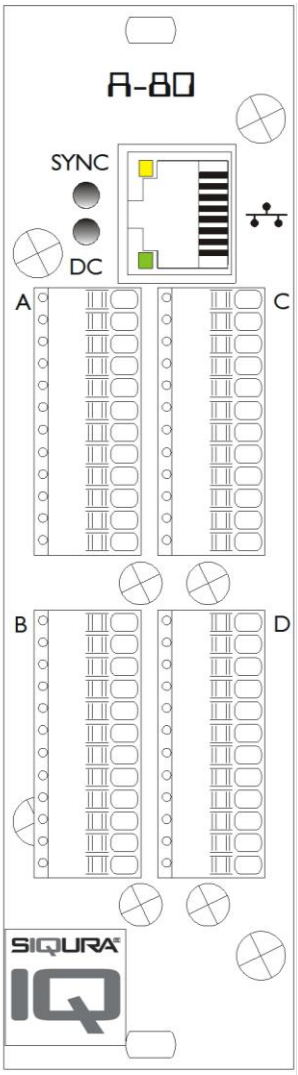
Features and indications

The front panel of the A-80 has the following features.

A-80

🖧	RJ-45 socket or SFP	Ethernet I/O, electrical or fiber
A, B, C, D	12-pole combicon connector	per connector: ▸ 2x audio input/output, ▸ 2x cc input, ▸ 1x cc output
Status indicator LEDs		
***DC**	green	DC power OK; blinks on identification 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
Ethernet socket LEDs	green/yellow	Green on/off: 100/10 Mbit Yellow on/blink: link OK, active Yellow off/flash: link down, TX attempt

A-80 front panel features and indications



Pin assignments are given in section *Connector Pin Assignments* (on page 14).

4 Installation

This chapter describes how to power your A-80 unit and connect network and signal cables.

In This Chapter

4.1 Powering the Unit

To power a rack-mount unit

1. Insert the A-80 into a Siqura 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) A-80 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 A-80 *front panel* (on page 12) to connect network and signal cables.

To connect the A-80 to your 100/10Mbit IP/Ethernet network

- Plug the network cable into the RJ-45 Ethernet socket on the A-80 front panel.

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

To connect audio and/or contact closure sources/destinations

1. Strip off 8 mm (0.44 inch) of insulation from the wire end.

Important: Use wire range 28-20AWG for your audio and contact closure connections.

2. Consult *Connector Pin Assignments* (on page 14), to determine which connector to use for your purpose.
3. Insert the exposed wire end into the spring-cage connector.
4. Pull the wire gently to check that it is properly connected.
   (To disconnect: pull the wire while keeping the orange push-in button pressed).

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.

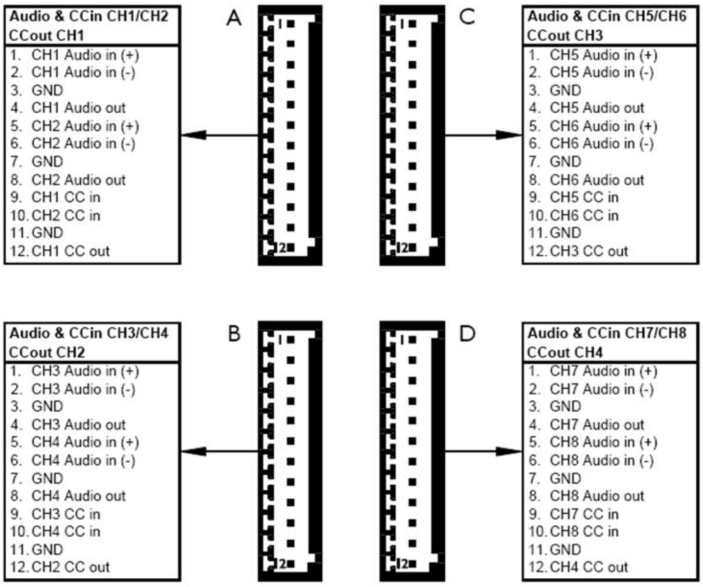
The sync LED displays as described in *Front Panel* (on page 12).

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 17) for details on how this can be done.

4.4 Connector Pin Assignments

Audio and contact closure connectors

The A-80 front panel has four 12-pole combicon connectors. Each connector carries signals for 2 audio inputs/outputs, 2 contact closure inputs, and 1 contact closure output. The figure below shows the connectors and the audio and cc inputs/outputs associated with each one.



Audio & CCin CH1/CH2
CCout CH1
1. CH1 Audio in (+)
2. CH1 Audio in (-)
3. GND
4. CH1 Audio out
5. CH2 Audio in (+)
6. CH2 Audio in (-)
7. GND
8. CH2 Audio out
9. CH1 CC in
10. CH2 CC in
11. GND
12. CH1 CC out

Audio & CCin CH5/CH6
CCout CH3
1. CH5 Audio in (+)
2. CH5 Audio in (-)
3. GND
4. CH5 Audio out
5. CH6 Audio in (+)
6. CH6 Audio in (-)
7. GND
8. CH6 Audio out
9. CH5 CC in
10. CH6 CC in
11. GND
12. CH3 CC out

Audio & CCin CH3/CH4
CCout CH2
1. CH3 Audio in (+)
2. CH3 Audio in (-)
3. GND
4. CH3 Audio out
5. CH4 Audio in (+)
6. CH4 Audio in (-)
7. GND
8. CH4 Audio out
9. CH3 CC in
10. CH4 CC in
11. GND
12. CH2 CC out

Audio & CCin CH7/CH8
CCout CH4
1. CH7 Audio in (+)
2. CH7 Audio in (-)
3. GND
4. CH7 Audio out
5. CH8 Audio in (+)
6. CH8 Audio in (-)
7. GND
8. CH8 Audio out
9. CH7 CC in
10. CH8 CC in
11. GND
12. CH4 CC out

Pin assignments of the four combicon connectors. See also Front Panel *(on page 12).*

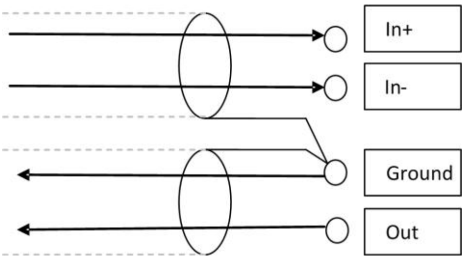
Ethernet connector

No.	Pin
1	TX+
2	TX-
3	RX+
6	RX-

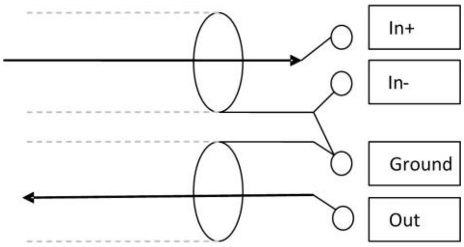
Ethernet connector pin assignment

Balanced and unbalanced audio connections

The A-80 offers balanced audio inputs and unbalanced audio outputs. The following diagrams illustrate how to make balanced and unbalanced connections.



Balanced system



Unbalanced system

4.5 Updating Device Definitions

If the A-80 is not supported by the Siqura application software on your host PC you can download EMX updates and MX Plug-in updates at www.siqura.com. 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 using the Showroom menu. 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 Siqura MX applications, such as Operator Storage, Operator Office, MX Viewer, MX Configuration Tool, and the MX SDK. An existing installation of the SNM Configuration and Service Tool will also be updated.

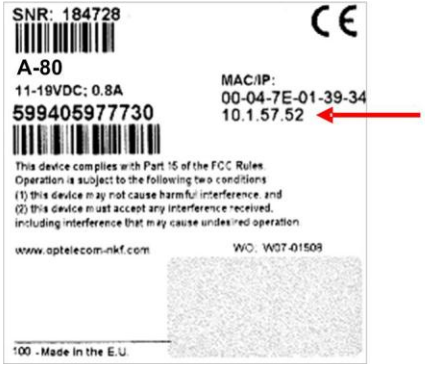
5 Connections

Having installed the A-80, the next step is to establish an IP connection and set up audio and contact closure links. This chapter explains how you can change the factory-set IP address and subnet mask of the A-80 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 A-80 is in the 10.x.x.x range. You will find it printed on a sticker on the unit.



SNR: 184728
A-80
11-19VDC; 0.8A
599405977730
MAC/IP:
00-04-7E-01-39-34
10.1.57.52
CE
This device complies with Part 15 of the FCC Rules.
Operation is subject to the following two conditions
(1) this device may not cause harmful interference, and
(2) this device must accept any interference received,
including interference that may cause undesired operation
www.optelecom-nkf.com
WO. W07-01508
100 - Made in the E.U.

Factory-set IP address

A-80 product sticker

Note: This is the address the unit will revert to if you issue a *Reset to factory settings; incl. network settings* (on page 51) command and reboot the unit.

To open communication with the A-80 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.

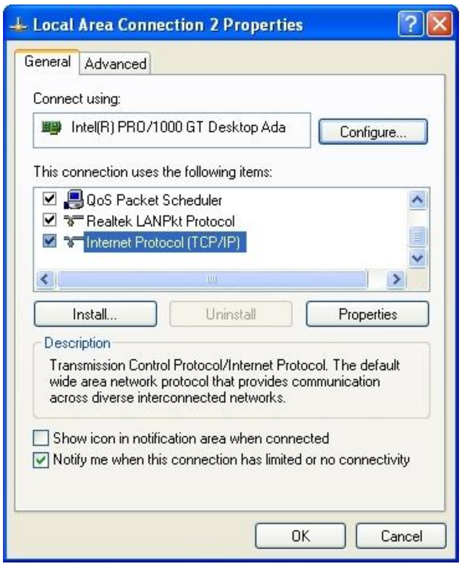
Step 1: Setting the host PC to the factory default subnet of the unit

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**.

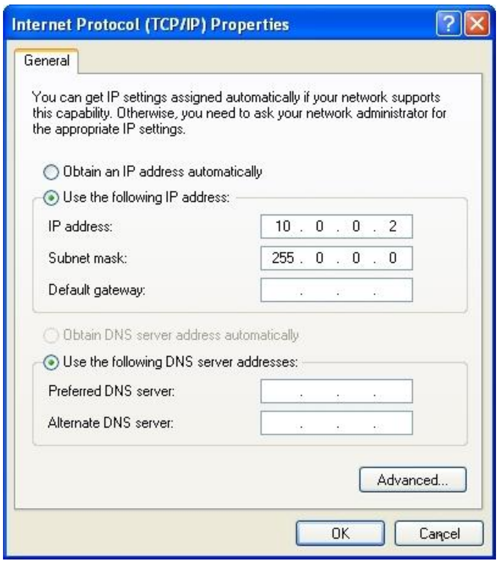

Local Area Connection 2 Properties
General
Advanced
Connect using:
Intel(R) PRO/1000 GT Desktop Ada
Configure...
This connection uses the following items:
Install...
Uninstall
Properties
Description
OK
Cancel

☑ QoS Packet Scheduler
☑ Realtek LANPkt Protocol
☑ Internet Protocol (TCP/IP)

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

Opening IP settings on the host PC



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 10 . 0 . 0 . 2
Subnet mask: 255 . 0 . 0 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

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

At this point, connect your PC to the A-80. 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 A-80'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 Audio and Contact Closure Connections

Connection methods

With the A-80's IP connection established, audio and contact closure connections can be made. The most convenient way to do so is to use the unit's internal web pages. For an elaborate description, see *Working with the Web Pages* (on page 27). A separate application program, such as Siqura's MX Configuration Tool, can be used as well.

Streams and connectors

Each signal stream transmitted and received by the A-80 (see figure below) can be conceived of as using virtual connectors (transmitters and receivers) on the network side. Each of the encoder'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.

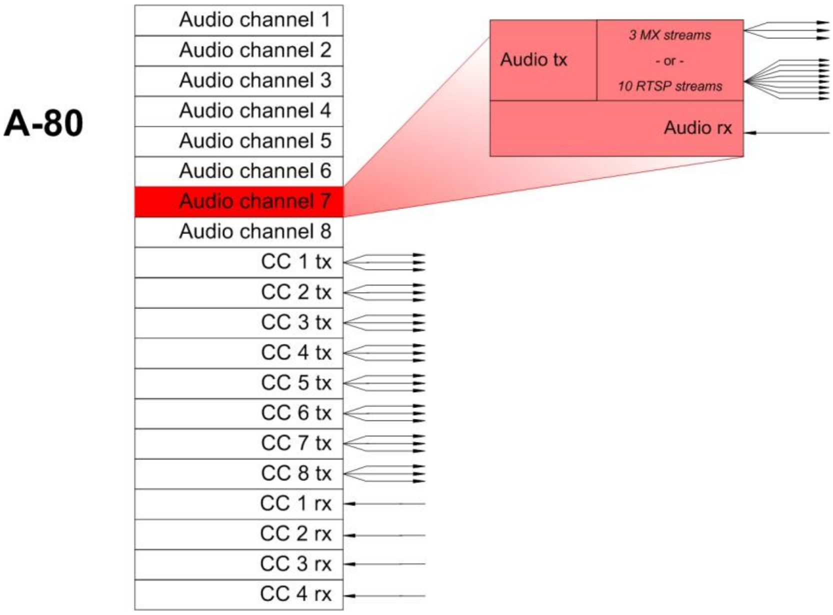
General procedure for making links

In both connection methods mentioned above, making a unicast one-way audio or contact closure link 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 an audio 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 *Appendix: Multicasting, Multi-Unicasting, Port Numbers* (on page 55).



Link facilities of an A-80.
All arrows represent separate and independent connections over Ethernet.
All audio channels have link facilities as depicted here for Audio channel 7.
The acronyms '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

6 Interfaces

A variety of methods can be employed to communicate with the A-80. 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 Web User Interface

Using the A-80's internal web server is the most straightforward way to access an individual unit. The A-80's web pages enable you to configure the unit's settings and monitor the media streams it handles, eliminating the need for a separate application program. For an elaborate description of the web user interface, refer to *Working with the Web Pages* (on page 27).

6.2 MX/IP

MX/IP, a proprietary Siqura 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 A-80 through the MIB, enabling you to remotely configure device settings and manage media streams. Additionally, MX viewing and control software offers real-time monitoring of video streams (Operator Office, MX Viewer Lite) and playback of recorded images (Operator Storage). For more details on the MX/IP protocol, the MIB and Siqura's EMX network service, refer to the manuals documenting the MX Software Development Kit and the above programs.

Note: If you prefer using open standards, you can go to the 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 A-80 firmware through MX Firmware Upgrade Tool.

6.3 SNMP

The Simple Network Management Protocol (SNMP), part of the internet protocol suite, can be used to monitor network devices such as the A-80 for conditions or events that require administrative attention. For more details, refer to appropriate literature on SNMP.

The A-80 supports in-band SNMP. Via SNMP several status variables can be read and traps can be generated on events. A-80 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.siqura.com.

6.4 Open Streaming Architecture (OSA)

Siqura's Open Streaming Architecture (OSA) consists of a standard set of open communication protocols to govern media streaming via RTSP and equipment management via HTTP. The *Siqura Protocol for Codecs & Cameras* enables easy integration of the A-80 with third-party products. The protocol consists mainly of different CGI (Common Gateway Interface) program calls for listing and configuring parameters.

RTSP (Real-Time Streaming Protocol) is used to negotiate media streaming in RTP (Real-Time Transport Protocol). The purpose of RTSP is to establish and control one or more time-synchronized streams of continuous media, such as video and audio. It does not typically deliver the continuous streams itself. RTSP acts as a network "remote control" for the A-80. The A-80 maintains a session labeled by an identifier. RTSP controls a stream which may be sent via a separate protocol, independent of the control channel. For example, RTSP control may occur on a TCP connection while the data flows via UDP.

For more details on controlling A-80 media streams through HTTP and RTSP, refer to Siqura's *PTZ Camera and Codec Programming Interface* specification. You can download this document from the Siqura web site.

6.5 SAP

The A-80 supports the Session Announcement Protocol (SAP). This is a protocol for broadcasting multicast session information. A SAP listening application can listen to the announcements advertised by the A-80 SAP announcer. The application can use this information to receive an audio stream transmitted by the A-80 to the advertised multicast address. For more details, refer to the description of the Audio web page (Advanced Settings).

7 Accessing the Internal Web Server

The web pages of the A-80 offer a user-friendly interface for configuring the unit's settings and monitoring the signal streams it is handling. This chapter explains how to connect to the A-80's built-in web server.

In This Chapter

7.1 System Requirements

To access the A-80's web pages you need the following:

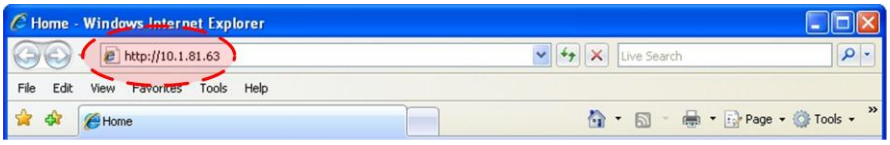
- A PC with a web browser installed.
- An IP connection between the PC and the A-80.
-

7.2 Login Procedure

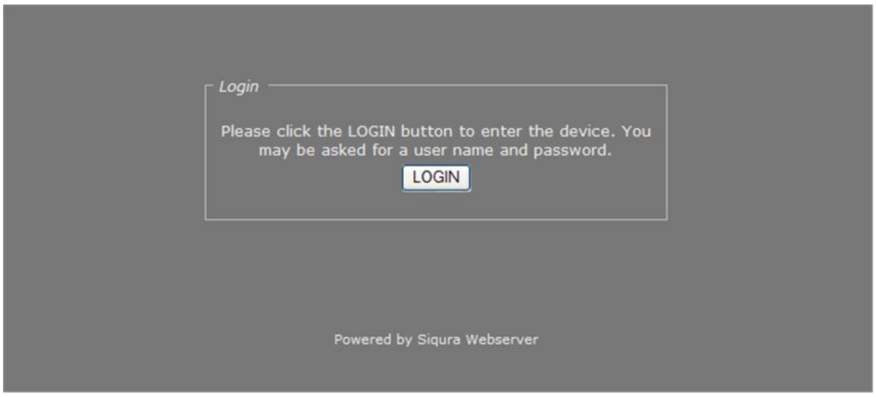
To log on to the unit's internal web server

1. Start your web browser.
2. Enter the A-80 's IP address in the Address Bar of your web browser.
   If your network configuration is correct you are directed to the 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 dialog 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 Overview 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.



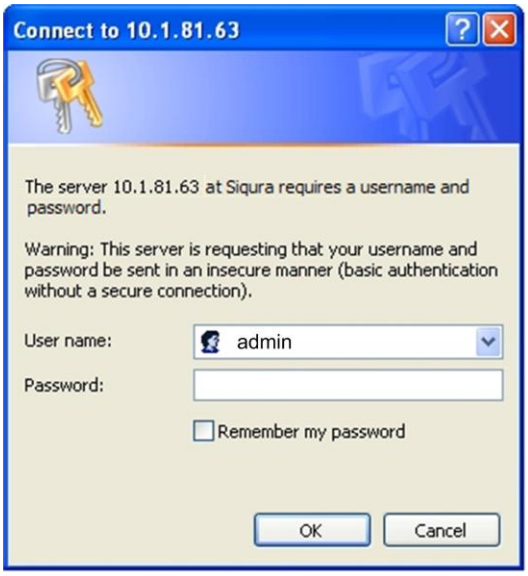
Entering the unit's IP address in the browser's Address Bar



Login

Please click the LOGIN button to enter the device. You may be asked for a user name and password.

A-80 login page



Connect to 10.1.81.63

The server 10.1.81.63 at Siqura requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: admin

Password:

□ Remember my password

Connect dialog box

8 Web Page Features

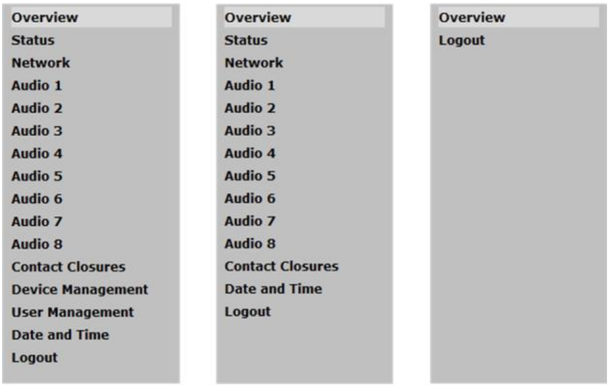
Navigation Menu

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 A-80. 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 A-80 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.



A-80 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 organize page content.
- Check boxes used to select various features.

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

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

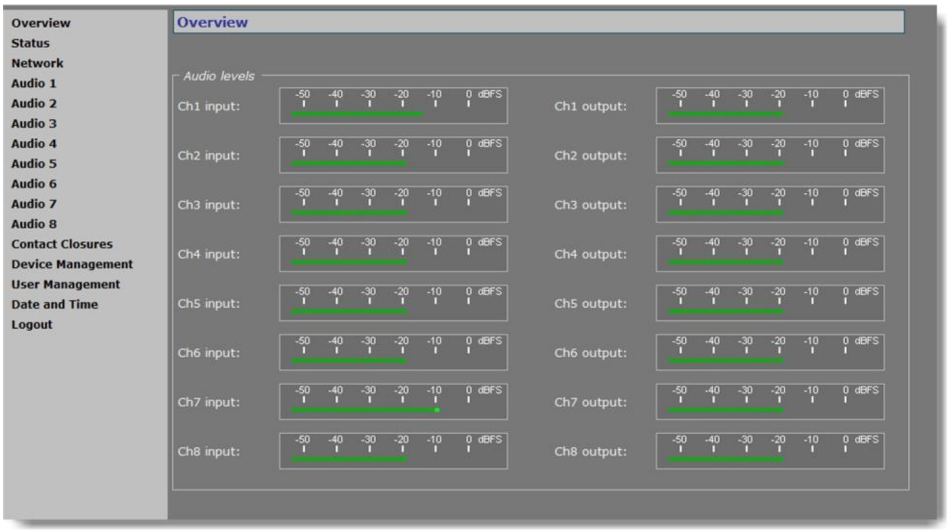
Important: Please be aware that configuring advanced settings requires in-depth understanding of the impact of your changes on the workings of your A-80 unit. If in doubt, do *not* change the default values.

9 Working with the Web Pages

The A-80's web pages enable you to monitor the media streams the unit is handling and to configure its device settings. This chapter discusses the individual pages you can use for this purpose.

In This Chapter

9.1 Overview

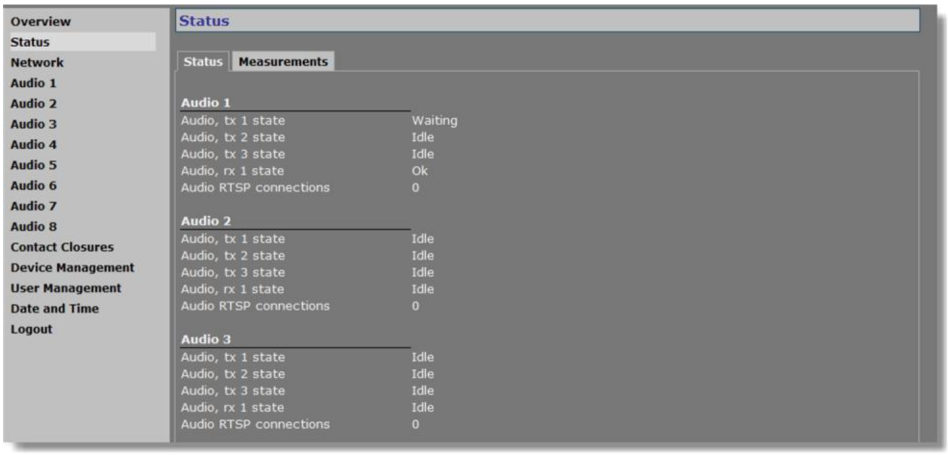


Overview page, the A-80 home page

Audio levels

The Overview page is the home page of your A-80 unit. It has two VU meters for each audio channel to indicate audio input and output levels.

9.2 Status



Audio 1

Audio, tx 1 state	Waiting
Audio, tx 2 state	Idle
Audio, tx 3 state	Idle
Audio, rx 1 state	Ok
Audio RTSP connections	0

Audio 2

Audio, tx 1 state	Idle
Audio, tx 2 state	Idle
Audio, tx 3 state	Idle
Audio, rx 1 state	Idle
Audio RTSP connections	0

Audio 3

Audio, tx 1 state	Idle
Audio, tx 2 state	Idle
Audio, tx 3 state	Idle
Audio, rx 1 state	Idle
Audio RTSP connections	0

Status page: a snapshot with automatic page updating

Tabs

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

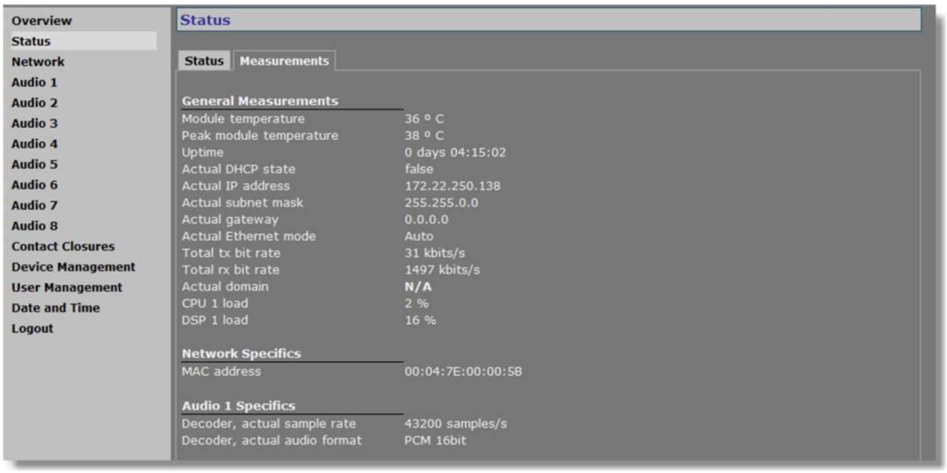
9.2.1 Status

Stream states

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

Stream state	
Ok	There is nothing wrong with the stream.
Idle	The transmitter/receiver is not enabled.
Waiting	The transmitter/receiver has lost its stream connection. Possible causes: ▸ An incorrect port number. ▸ The transmitter/receiver on the other side of the connection is not enabled. ▸ No FloodGuard packets have been received for more than three seconds. For details on the FloodGuard flooding prevention mechanism, see the section on FloodGuard.

9.2.2 Measurements



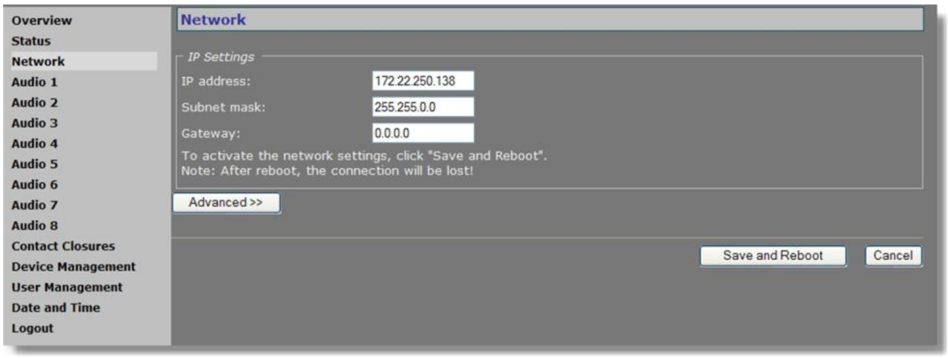
General Measurements	
Module temperature	36 ° C
Peak module temperature	38 ° C
Uptime	0 days 04:15:02
Actual DHCP state	false
Actual IP address	172.22.250.138
Actual subnet mask	255.255.0.0
Actual gateway	0.0.0.0
Actual Ethernet mode	Auto
Total tx bit rate	31 kbits/s
Total rx bit rate	1497 kbits/s
Actual domain	N/A
CPU 1 load	2 %
DSP 1 load	16 %
Network Specifics	
MAC address	00:04:7E:00:00:5B
Audio 1 Specifics	
Decoder, actual sample rate	43200 samples/s
Decoder, actual audio format	PCM 16bit

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.

9.3 Network



IP address: 172.22.250.138

Subnet mask: 255.255.0.0

Gateway: 0.0.0.0

To activate the network settings, click "Save and Reboot".
Note: After reboot, the connection will be lost!

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 A-80, 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 A-80; for details, see Establishing a Network Connection. 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.

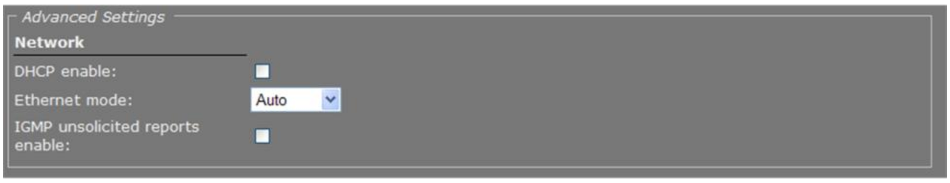
For IP address input to be valid, the unit's IP address:

- 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



Advanced Settings

Network

DHCP enable: □

Ethernet mode: Auto

IGMP unsolicited reports enable: □

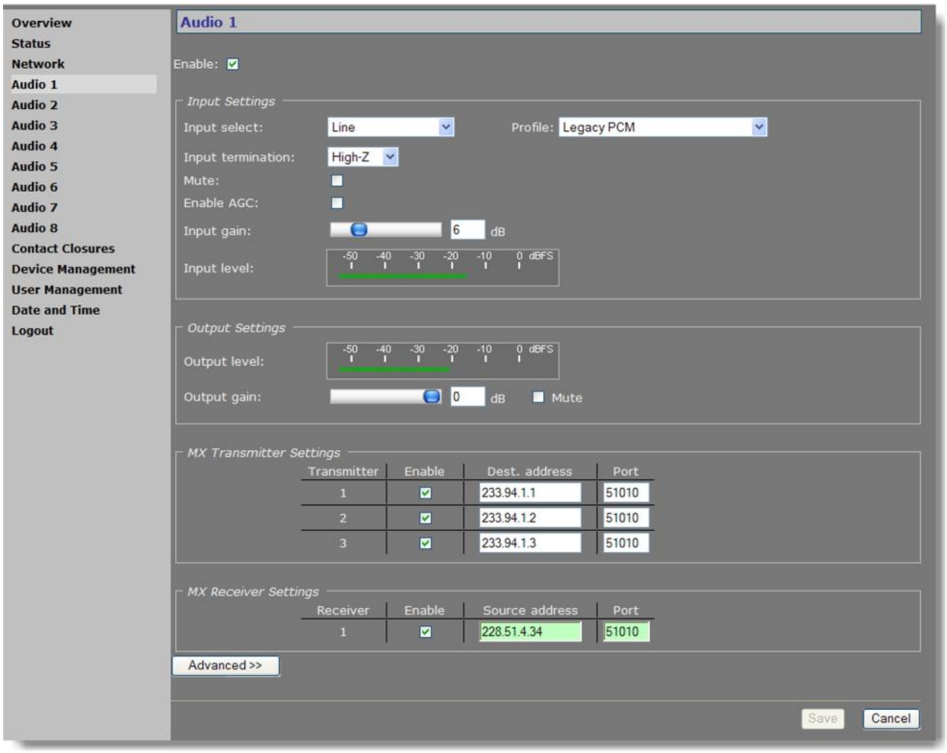
Network page, Advanced Settings

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 Audio



Audio 1

Enable: ☑

Input Settings

Input select: Line
Profile: Legacy PCM
Input termination: High-Z
Mute: □
Enable AGC: □
Input gain: 6 dB
Input level: -50 -40 -30 -20 -10 0 dBFS

Output Settings

Output level: -50 -40 -30 -20 -10 0 dBFS
Output gain: 0 dB □ Mute

MX Transmitter Settings

Transmitter	Enable	Dest. address	Port
1	☑	233.94.1.1	51010
2	☑	233.94.1.2	51010
3	☑	233.94.1.3	51010

MX Receiver Settings

Receiver	Enable	Source address	Port
1	☑	228.51.4.34	51010

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	Select or clear this box to respectively mute or unmute audio.	
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

Input Settings

	G711 µ-law. 1 ch. 8kHz. 64 kbit/s	▸ mainly used in USA ▸ mono, low quality ▸ used for Genetec's Omnicast
	Legacy PCM	▸ 1 channel (mono) ▸ high quality, 15.7 kHz ▸ compatible with all Siqura products (including C-20, C-40, S-40)

Output Settings

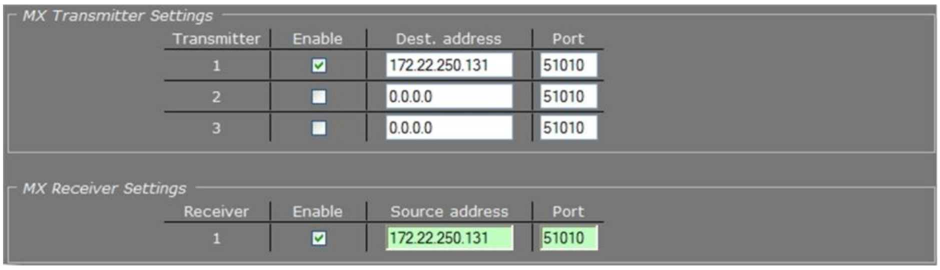
Output level	VU meter to display audio output level.
Output gain	Range: [-80…0] dB.
Mute	Select or clear this box to respectively mute or unmute audio.

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 A-80.



MX Transmitter Settings

Transmitter	Enable	Dest. address	Port
1	☑	172.22.250.131	51010
2	☐	0.0.0.0	51010
3	☐	0.0.0.0	51010

MX Receiver Settings

Receiver	Enable	Source address	Port
1	☑	172.22.250.131	51010

Transmitter and Receiver sections, two-way audio

Audio streams

The A-80 provides 8-channel bidirectional audio. Per channel, the A-80 can send three audio streams to different destinations, multicast or unicast, to any C- or S-series codec with an audio interface. Per channel, it can also receive one (stereo) audio stream from any C-series codec that features audio. A received audio stream is converted to mono.

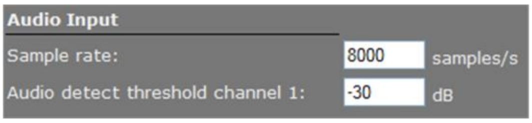
Highlighted fields

The source address and port number fields are highlighted in green (as shown above) when the enabled receiver receives an audio stream from the specified source. The two fields are marked in red when no stream is received with the audio receiver enabled and correctly configured.

Two-way audio

The figure above shows the setup for two-way audio on the side of the A-80. 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 A-80 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.

9.4.1 Advanced Settings



Audio Input

Sample rate: 8000 samples/s

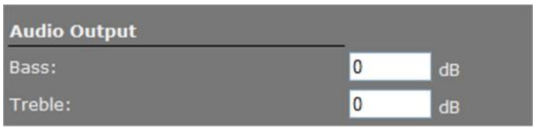
Audio detect threshold channel 1: -30 dB

Advanced Settings, Audio Input

Audio Input

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
Audio 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.

Audio Output



Audio Output

Bass: 0 dB

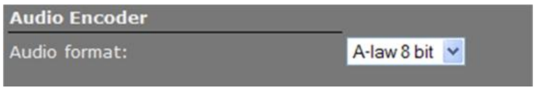
Treble: 0 dB

Advanced Settings, Audio Output

Audio Output

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

Audio Encoder



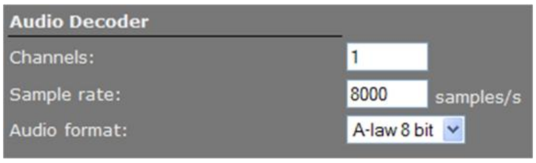
Audio Encoder

Audio format: A-law 8 bit

Advanced Settings, Audio Encoder

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

Audio Decoder



Audio Decoder

Channels: 1

Sample rate: 8000 samples/s

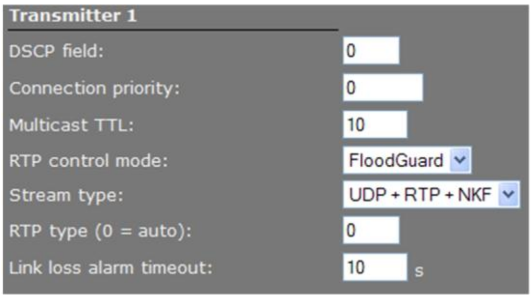
Audio format: A-law 8 bit

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 receiving a stereo audio stream, you can specify a value of 2 here to have the A-80 merge the left and right channel and output the result as one mono signal.
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



Transmitter 1

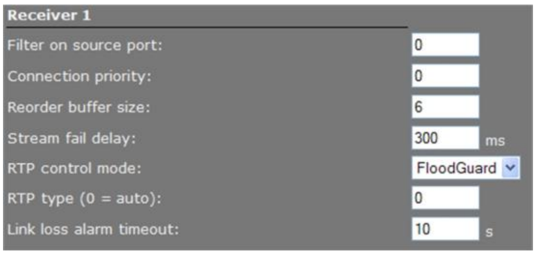
DSCP field:	0
Connection priority:	0
Multicast TTL:	10
RTP control mode:	FloodGuard
Stream type:	UDP + RTP + NKF
RTP type (0 = auto):	0
Link loss alarm timeout:	10 s

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

Receiver 1



Receiver 1

Filter on source port: 0

Connection priority: 0

Reorder buffer size: 6

Stream fail delay: 300 ms

RTP control mode: FloodGuard

RTP type (0 = auto): 0

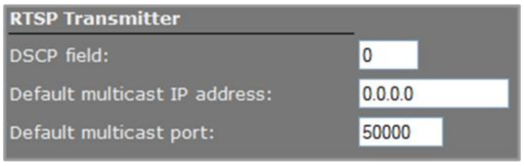
Link loss alarm timeout: 10 s

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 (MX SDK).	
Reorder buffer size	Used to reorder incoming packets.	
Stream fail delay	Range: [0...10000] ms. Default: 300 ms. Timeout in ms before going to NoStream state.	
RTP control mode	Select the transport protocol to control the stream.	
	None	No transport protocol selected.
	FloodGuard	Flooding prevention mechanism. For more information, see the note on FloodGuard later in this chapter.
	RTCP	Real-Time Control Protocol, a network control protocol for use in communications systems to control streaming media servers.
RTP type (0 = auto)	Default value: [0]. This parameter determines the RTP payload format (e.g. H.264, MPEG-2/4, or audio). To avoid an RTP type conflict, the values specified on both sides of the connection must be the same. The default value of "0" automatically sets the appropriate media type. You are advised not to change this setting.	
Link loss alarm timeout	Range: [1...1000] s. Default: 10 s. Time in seconds before alarm sent.	

RTSP Transmitter



RTSP Transmitter

DSCP field: 0

Default multicast IP address: 0.0.0.0

Default multicast port: 50000

Advanced Settings: RTSP Transmitter

RTSP Transmitter

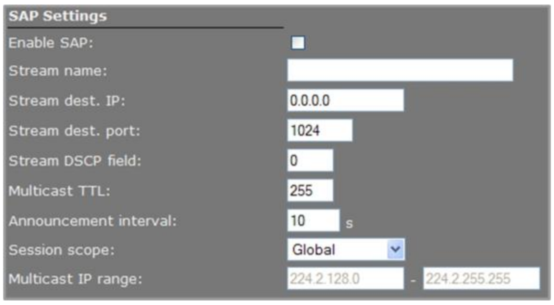
DSCP field	Range: [0...63]. DSCP (Differentiated Services Code Point) uses the first 6 bits of the ToS (Type of Service) field in the header of IP packets for packet classification purposes. The bit pattern in the field indicates the type of service and forwarding behavior at the next node. With 26 bits,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

Note on Differentiated Services: Differentiated Services (DiffServ, or DS) is a method for adding QoS (Quality of Service) to IP networks. In routed networks, critical network traffic such as video and audio streams, which require a relatively uninterrupted flow of data, can get blocked due to other traffic. DiffServ can be used to classify network traffic and give precedence - i.e. low-latency, guaranteed service - to high-priority traffic, while offering best-effort service to non-critical traffic such as file transfers or web traffic.
Each stream has a DSCP (Differentiated Services Code Point) field in the IP header. Routers will identify the network service type in the DSCP field and provide the appropriate level of service. Low-latency service can be realized, for example, through priority queuing, bandwidth allocation, or by assigning dedicated routes.

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

SAP Settings

The A-80 includes a SAP announcer. The Session Announcement Protocol is used to advertise that a media stream generated by the A-80 is available at a specific multicast address and port. For more information about SAP, see the note below.



SAP Settings

Enable SAP: □

Stream name:

Stream dest. IP: 0.0.0.0

Stream dest. port: 1024

Stream DSCP field: 0

Multicast TTL: 255

Announcement interval: 10 s

Session scope: Global

Multicast IP range: 224.2.128.0 - 224.2.255.255

Advanced section: SAP Settings

SAP Settings

Enable SAP	When selected, session announcements are sent at the frequency determined by the Announcement interval parameter and the media stream is transmitted to the multicast IP address specified in the Stream dest. IP address box.
Stream name	Enter a descriptive name to identify the media stream.
Stream dest. IP	Enter the multicast IP address the media stream is to be sent to. The address must be within the range defined by the Multicast IP range parameter.
Stream dest. port	The destination port number. Default: 1024.
Stream DSCP field	Range: [0…63]. See the note on DSCP.
Multicast TTL	Range: [0...255]. Range: [0...127]. Specify the number of routers (hops) that multicast traffic is permitted to pass through before expiring on the network.
Announcement interval	Determines the frequency of announcements.
Session scope	*Global*, the default session scope, sets the *Multicast IP range* parameter to 224.2.128.0 - 224.2.255.255 (IPv4 global scope sessions). A SAP listening application will recognize the global scope and automatically listen for SAP announcements at the 224.2.127.254 multicast IP address. The *Administrative* session scope allows you to enter a custom IP range within the 239.0.0.0 - 239.255.255.255 (IPv4 administrative scope sessions) range. For an Administrative session scope, the multicast address for SAP announcements will be set to the highest address in the relevant administrative scope. For example, for a scope range of 239.16.32.0 - 239.16.33.255, the IP address 239.16.33.255 is used for SAP announcements.
Multicast IP range	See Session scope.

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

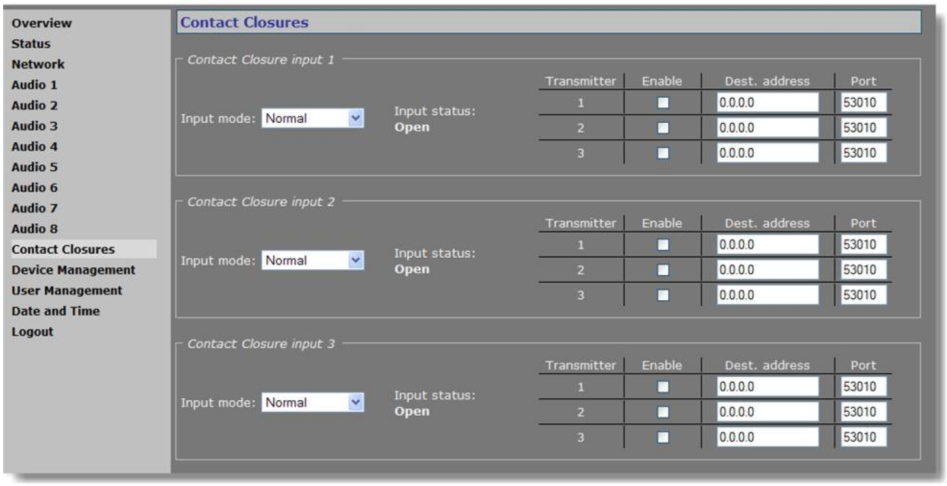
9.4.2 FloodGuard

Note on FloodGuard: FloodGuard is a stream control mechanism that can be enabled/disabled independently for each audio 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.

9.5 Contact Closures



Contact Closures

Contact Closure input 1

Input mode: Normal

Input status: **Open**

Transmitter	Enable	Dest. address	Port
1	□	0.0.0.0	53010
2	□	0.0.0.0	53010
3	□	0.0.0.0	53010

Contact Closure input 2

Input mode: Normal

Input status: **Open**

Transmitter	Enable	Dest. address	Port
1	□	0.0.0.0	53010
2	□	0.0.0.0	53010
3	□	0.0.0.0	53010

Contact Closure input 3

Input mode: Normal

Input status: **Open**

Transmitter	Enable	Dest. address	Port
1	□	0.0.0.0	53010
2	□	0.0.0.0	53010
3	□	0.0.0.0	53010

Contact Closures page: CC # input settings

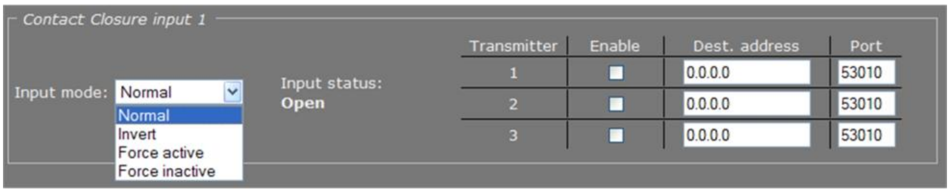
CC inputs and outputs

The A-80 offers eight contact closure (CC) inputs, each of them capable of transmitting three copies per signal. The inputs can be configured to stream CC signals to an i-NVR or to activate a signal in the API, for example. The A-80 also has four contact closure outputs to connect with PLCs or other telemetry systems. The CC output can be activated through the API or received CC streams.

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.

Contact Closure Input



Contact Closure input 1

Input mode: Normal

Input status: **Open**

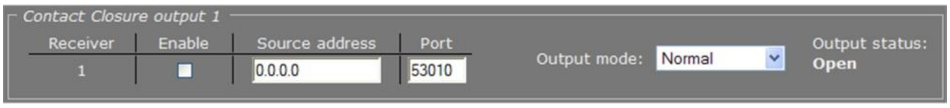
Transmitter	Enable	Dest. address	Port
1	□	0.0.0.0	53010
2	□	0.0.0.0	53010
3	□	0.0.0.0	53010

CC Input 1 settings

Contact Closure Input

Input mode	*Normal*	Direction.
	Invert	
	Force active	Always on (e.g. for testing purposes).
	Force inactive	Always off.
Input status	*Open*	The receiver relays are normally open.
	Closed	
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.	

Contact Closure Output



Contact Closure output 1

Receiver	Enable	Source address	Port
1	□	0.0.0.0	53010

Output mode: Normal

Output status: **Open**

CC output # settings

Contact Closure Output

Output mode	*Normal*	Direction.
	Invert	
	Force active	Always on (e.g. for testing purposes).
	Force inactive	Always off.
Output status	*Open*	Normally open.
	Closed	
Enable	Select/Clear to enable/disable the stream reception, respectively.	
Dest. address	IP address of the codec that will transmit the stream.	
Port	The local port number of the A-80.	

9.5.1 Making Contact Closure Connections

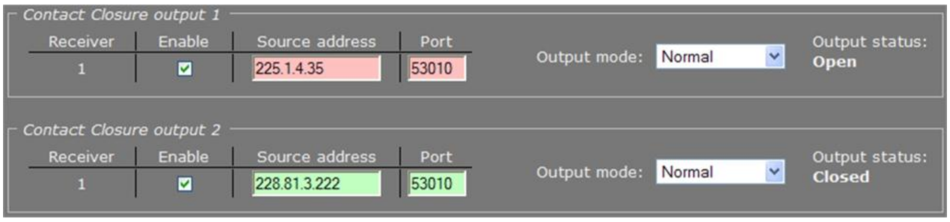
To make a contact closure connection

- 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.



Contact Closure output 1

Receiver	Enable	Source address	Port
1	☑	225.1.4.35	53010

Output mode: Normal

Output status: **Open**

Contact Closure output 2

Receiver	Enable	Source address	Port
1	☑	228.81.3.222	53010

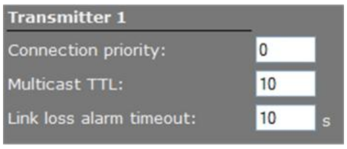
Output mode: Normal

Output status: **Closed**

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

9.5.2 Advanced Settings

CC Input # Settings, Transmitter



Transmitter 1

Connection priority: 0

Multicast TTL: 10

Link loss alarm timeout: 10 s

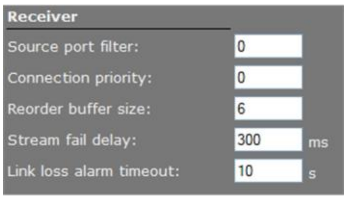
Advanced Settings, CC Input #,

Transmitter #

Transmitter

Connection priority	Parameter intended for use with MX Software Development Kit (MX SDK).
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.
Link loss alarm timeout	Range: [1...1000] s. Default: 10 s. Time in seconds before alarm sent.

CC Output # Settings, Receiver



Receiver

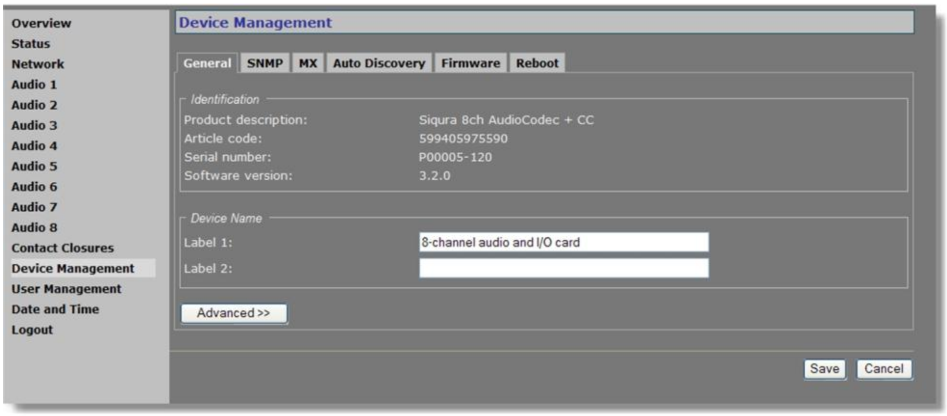
Source port filter:	0	
Connection priority:	0	
Reorder buffer size:	6	
Stream fail delay:	300	ms
Link loss alarm timeout:	10	s

Advanced Settings, CC Output #, Receiver

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 (MX SDK).
Reorder buffer size	Used to reorder incoming packets.
Stream fail delay	Range: [0...10000] ms. Default: 300 ms. Timeout in ms before going to NoStream state.
Link loss alarm timeout	Range: [1...1000] s. Default: 10 s. Time in seconds before alarm sent.

9.6 Device Management



Identification

Product description: Siqura 8ch AudioCodec + CC
Article code: 599405975590
Serial number: P00005-120
Software version: 3.2.0

Device Name

Label 1: 8-channel audio and I/O card
Label 2:

Device Management page, General tab

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

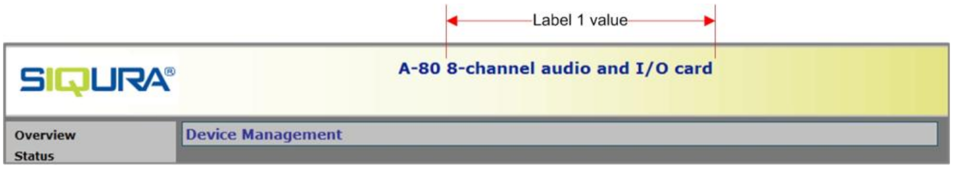
9.6.1 General

Identification

This section offers administrative module information.

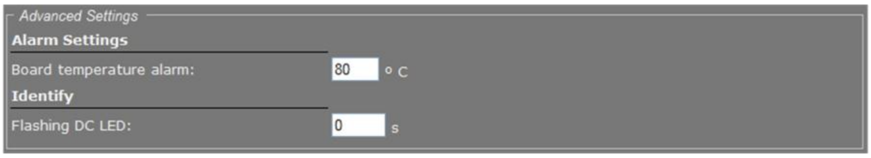
Device name

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



Label 1 value in Title pane

9.6.1.1 Advanced Settings



Advanced Settings

Alarm Settings

Board temperature alarm: 80 °C

Identify

Flashing DC LED: 0 s

Device Management: Advanced Settings

Alarm Settings

Board temperature alarm

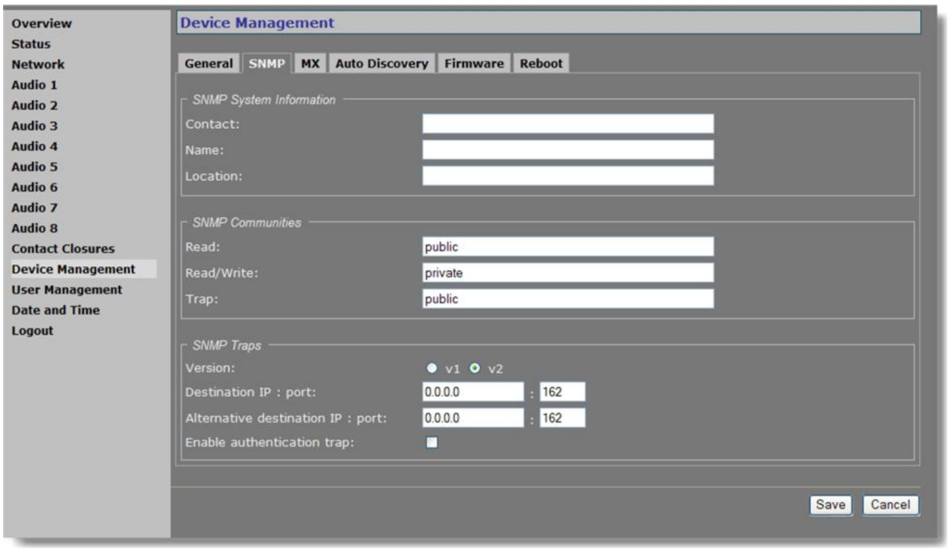
A notification is issued on the network when the temperature value set here is exceeded. Module alarms can be read and processed using additional Siqura software (which will also enable you to configure alarm levels and destinations).

Identify

Flashing DC LED

Range: [0 …1000]. To identify a A-80, 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.

9.6.2 SNMP



SNMP System Information

Contact:

Name:

Location:

SNMP Communities

Read: public

Read/Write: private

Trap: public

SNMP Traps

Version: ○ v1 ● v2

Destination IP : port: 0.0.0.0 : 162

Alternative destination IP : port: 0.0.0.0 : 162

Enable authentication trap: □

Device Management page, SNMP tab

SNMP MIB

To prepare a A-80 for SNMP management, the database documenting the A-80 variables that can be read or modified must be registered with the program; such SNMP MIB documents (indicated OPTC) are available from Siqura or from its web site.

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 A-80 alarm status change will generate a trap which can be caught by any SNMP manager. *Version* and *Destination IP : port* are required fields.

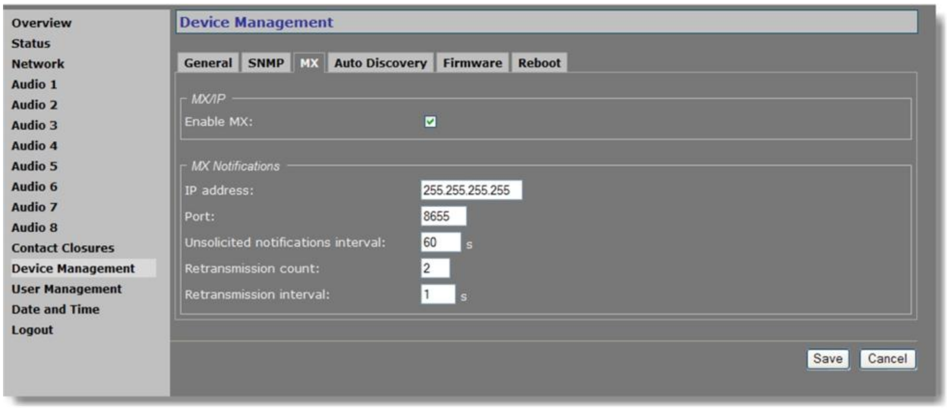
SNMP Traps

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

9.6.3 MX



Enable MX: ☑

IP address: 255.255.255.255

Port: 8655

Unsolicited notifications interval: 60 s

Retransmission count: 2

Retransmission interval: 1 s

Device Management: MX

MX/IP

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

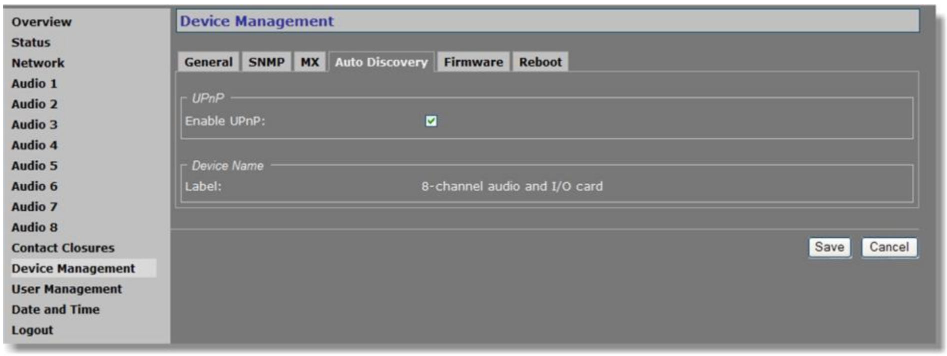
MX/IP

Enable MX	In addition to the proprietary MX/IP protocol, a A-80 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 A-80 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.

9.6.4 Auto Discovery



Enable UPnP: ☑

Label: 8-channel audio and I/O card

Device Management: Auto Discovery

Advertising the A-80 on the network

On the Auto Discovery tab you can enable UPnP (Universal Plug and Play). If enabled, UPnP will allow the A-80 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.

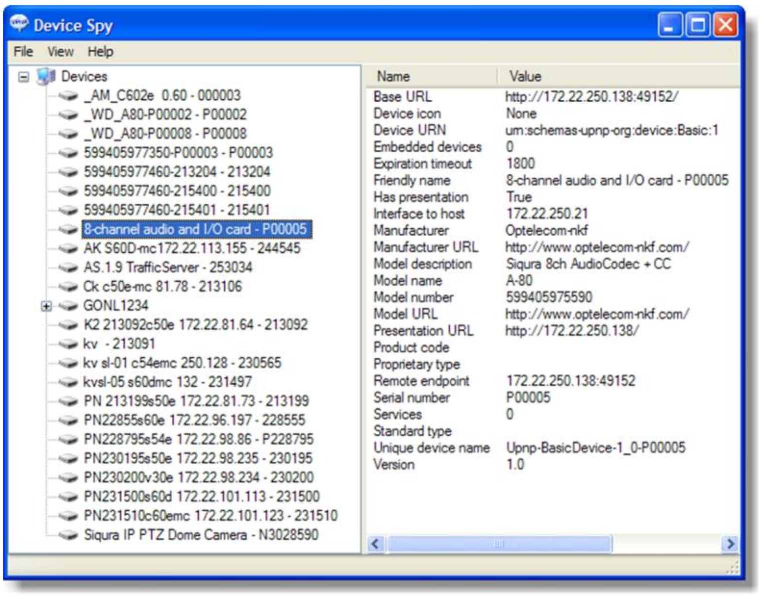
The A-80 supports the following Universal Plug and Play (UpnP) functionality: Discovery, Description (partly supported), and Presentation.

Testing the A-80'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 A-80 correctly advertizes its presence and device description on the network.

⏩ To view the A-80 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 A-80 in the left-hand-panel.
   The device description is shown in the right-hand panel.



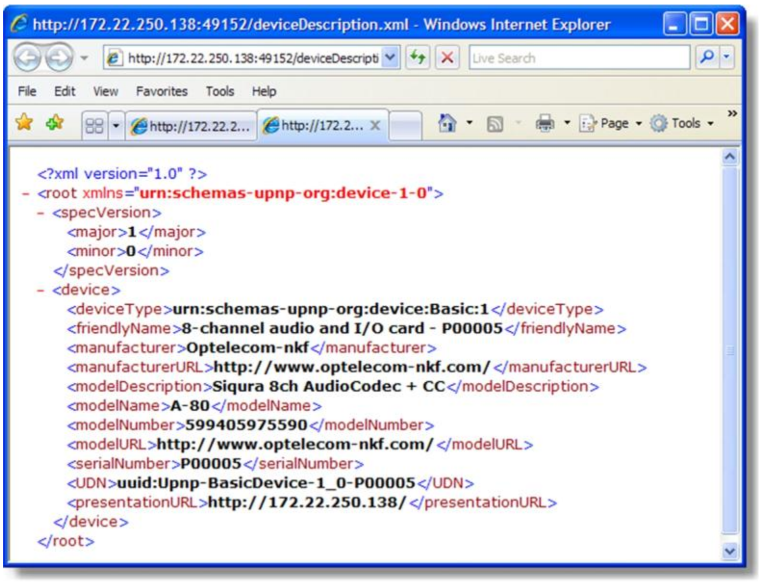
Devices
- _AM_C602e 0.60 - 000003
- _WD_A80-P00002 - P00002
- _WD_A80-P00008 - P00008
- 599405977350-P00003 - P00003
- 599405977460-213204 - 213204
- 599405977460-215400 - 215400
- 599405977460-215401 - 215401
- 8-channel audio and I/O card - P00005
- AK S60D-mc172.22.113.155 - 244545
- AS.1.9 TrafficServer - 253034
- Ck c50e-mc 81.78 - 213106
- GONL1234
- K2 213092c50e 172.22.81.64 - 213092
- kv - 213091
- kv sl-01 c54emc 250.128 - 230565
- kvsl-05 s60dmc 132 - 231497
- PN 213199s50e 172.22.81.73 - 213199
- PN22855s60e 172.22.96.197 - 228555
- PN228795s54e 172.22.98.86 - P228795
- PN230195s50e 172.22.98.235 - 230195
- PN230200v30e 172.22.98.234 - 230200
- PN231500s60d 172.22.101.113 - 231500
- PN231510c60emc 172.22.101.123 - 231510
- Siqura IP PTZ Dome Camera - N3028590

Name	Value
Base URL	http://172.22.250.138:49152/
Device icon	None
Device URN	urn:schemas-upnp-org:device:Basic:1
Embedded devices	0
Expiration timeout	1800
Friendly name	8-channel audio and I/O card - P00005
Has presentation	True
Interface to host	172.22.250.21
Manufacturer	Optelecom-nkf
Manufacturer URL	http://www.optelecom-nkf.com/
Model description	Siqura 8ch AudioCodec + CC
Model name	A-80
Model number	599405975590
Model URL	http://www.optelecom-nkf.com/
Presentation URL	http://172.22.250.138/
Product code	
Proprietary type	
Remote endpoint	172.22.250.138:49152
Serial number	P00005
Services	0
Standard type	
Unique device name	Upnp-BasicDevice-1_0-P00005
Version	1.0

A-80 device description in Device Spy

⏩ To view the A-80 device description in XML (using Device Spy)

1. Start Device Spy.
2. In the left-hand panel, right-click the A-80 entry.
3. Select **Get Device XML**.
   The XML device description opens in your web browser.


http://172.22.250.138:49152/deviceDescription.xml - Windows Internet Explorer
http://172.22.250.138:49152/deviceDescripti
Live Search
File Edit View Favorites Tools Help
http://172.22.2...
http://172.2...
Page
Tools

```
  <?xml version="1.0" ?>
- <root xmlns="urn:schemas-upnp-org:device-1-0">
  - <specVersion>
      <major>1</major>
      <minor>0</minor>
    </specVersion>
  - <device>
      <deviceType>urn:schemas-upnp-org:device:Basic:1</deviceType>
      <friendlyName>8-channel audio and I/O card - P00005</friendlyName>
      <manufacturer>Optelecom-nkf</manufacturer>
      <manufacturerURL>http://www.optelecom-nkf.com/</manufacturerURL>
      <modelDescription>Siqura 8ch AudioCodec + CC</modelDescription>
      <modelName>A-80</modelName>
      <modelNumber>599405975590</modelNumber>
      <modelURL>http://www.optelecom-nkf.com/</modelURL>
      <serialNumber>P00005</serialNumber>
      <UDN>uuid:Upnp-BasicDevice-1_0-P00005</UDN>
      <presentationURL>http://172.22.250.138/</presentationURL>
    </device>
  </root>
```

A-80 XML device description

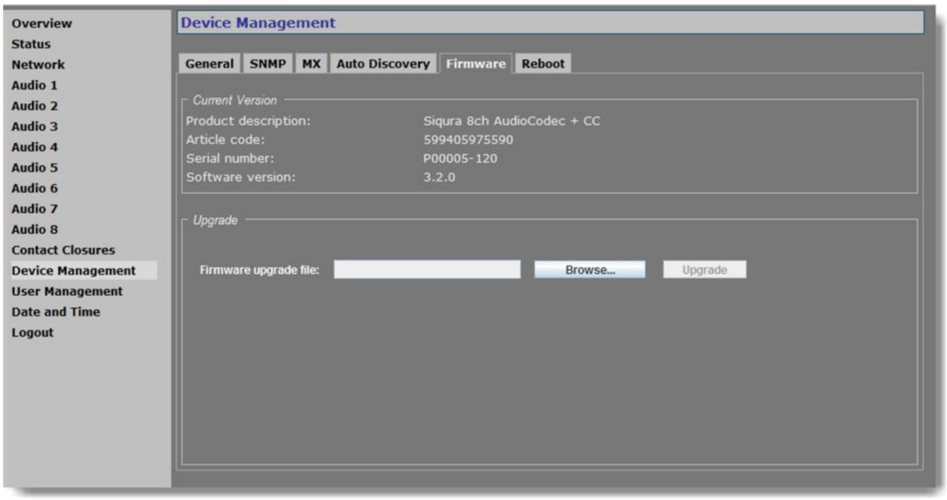
To access the A-80's web pages via Device Spy

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 A-80 entry, and then select **Display Presentation Page**.

The login page of the A-80 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.

9.6.5 Firmware



Product description: Sigura 8ch AudioCodec + CC
Article code: 599405975590
Serial number: P00005-120
Software version: 3.2.0

Firmware upgrade file:

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 A-80 firmware upgrade feature requires Java Runtime Environment 1.6 or higher. The Siqura application does not give rise to any security risks. You can run it safely.

Firmware images

The A-80 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 A-80 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 A-80.

Important: If an error should occur during the upgrade procedure, the A-80 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.

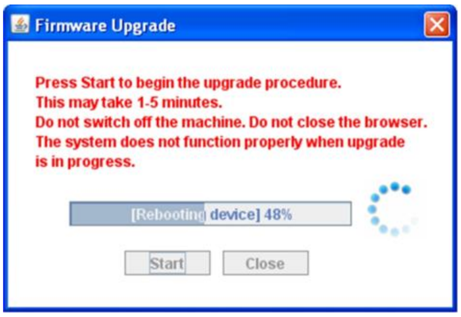
To upgrade the A-80 firmware

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**.



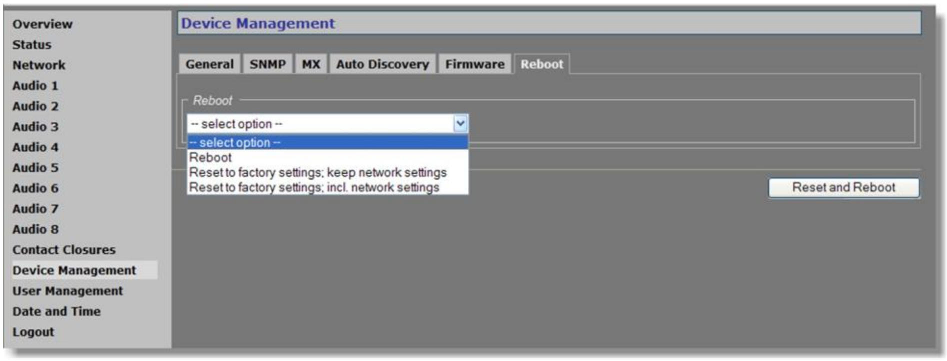
Firmware Upgrade

Press Start to begin the upgrade procedure.
This may take 1-5 minutes.
Do not switch off the machine. Do not close the browser.
The system does not function properly when upgrade
is in progress.

[Rebooting device] 48%

Firmware upgrade progress

9.6.6 Reboot

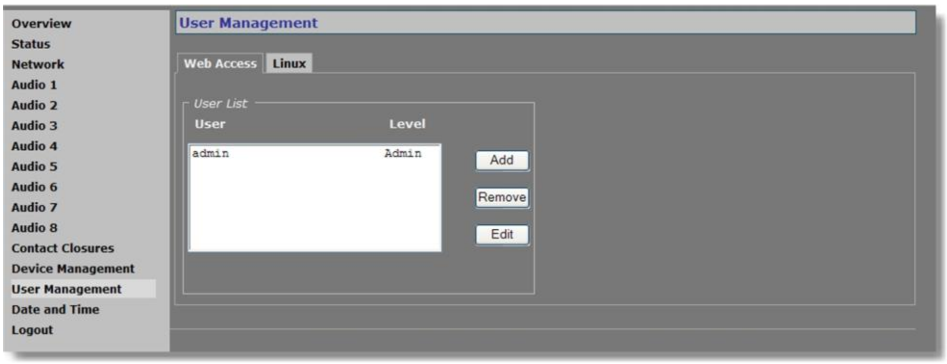


Device Management: Reboot options

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 A-80.

9.7 User Management



User	Level
admin	Admin

User Management: Web Access

Tabs

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

9.7.1 Web Access

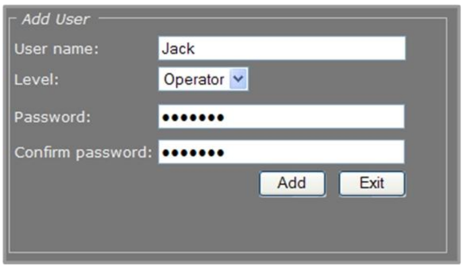
Three-level access control

The A-80 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 A-80 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.



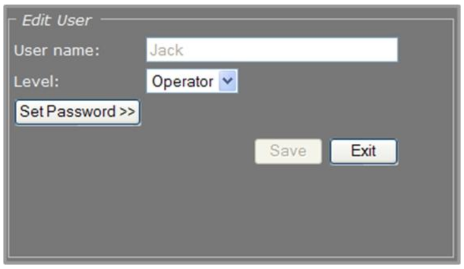
User name: Jack
Level: Operator
Password: •••••••
Confirm password: •••••••

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**.



Edit User

User name: Jack

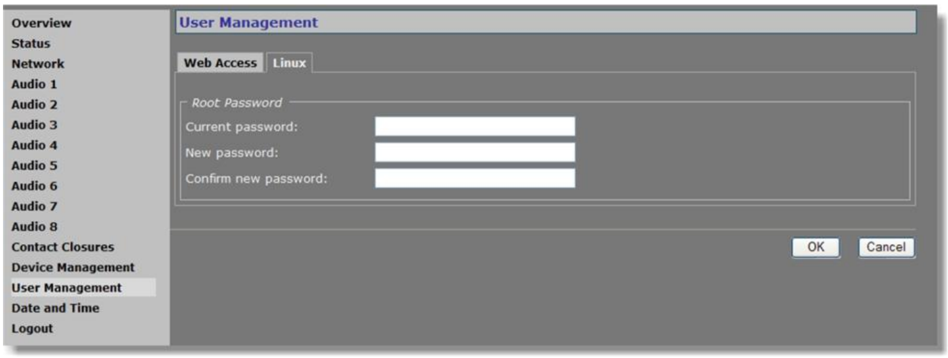
Level: Operator

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**.

9.7.2 Linux



User Management

Root Password

Current password:

New password:

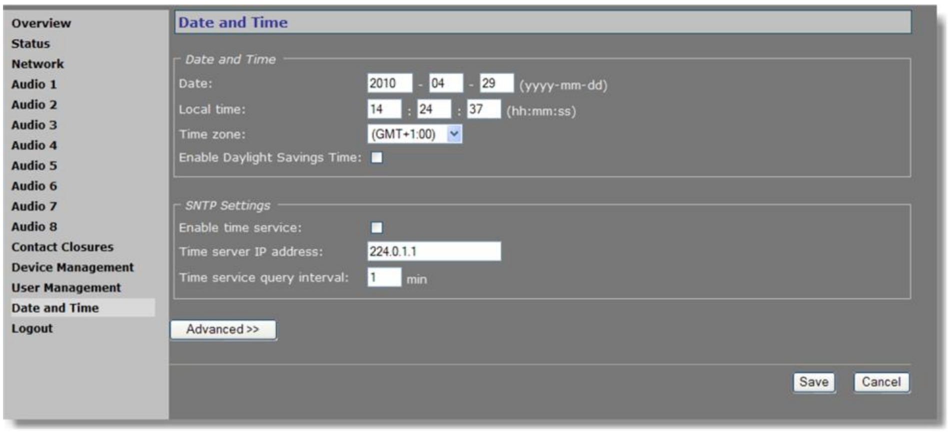
Confirm new password:

User Management: 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.

9.8 Date and Time



Date and Time

Date and Time

Date: 2010 - 04 - 29 (yyyy-mm-dd)

Local time: 14 : 24 : 37 (hh:mm:ss)

Time zone: (GMT+1:00)

Enable Daylight Savings Time: □

SNTP Settings

Enable time service: □

Time server IP address: 224.0.1.1

Time service query interval: 1 min

Date and Time settings

Date and Time

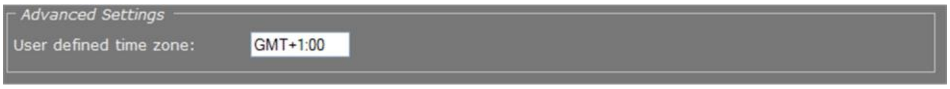
The A-80 has a battery-supported real-time clock that can be adjusted either manually (as shown above), or automatically with the aid of an SNTP (Simple Network Time Protocol) server. After entering changes, press **Save** to make them permanent.

Date and time displayed can be adjusted as indicated in the above figure. Do not forget to set the correct time zone first. On enabling daylight savings time, the time displayed is also adjusted.

SNTP Settings

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

9.8.1 Advanced Settings (Date and Time)



Advanced Settings

User defined time zone: GMT+1:00

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 Appendix: Multicasting, Multi-Unicasting, Port Numbers

Multicasting

The A-80 can be used in a multicasting setting. *The network switches and other devices used must be carefully configured for, and capable of, handling multicasting and its associated protocols (most notably IGMP v2).* 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 A-80 itself, although it is compounded by the density of the UDP streams used.

To define a multicast group, a source unit should be assigned a valid multicasting ('destination') TX stream address and the destination units should get this same address as source. 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.

Multi-unicasting

Alternatively, the A-80 features 'multi-unicasting', i.e. sending out up to max. 10 RTSP or 3 MX audio streams per input, and 3 contact closure streams per input. If the bit rates selected are moderate, it may be more convenient to use this mechanism instead of multicasting, even though the network gets more signal to carry from the encoder.

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

Port numbers

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

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

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

Default port numbers

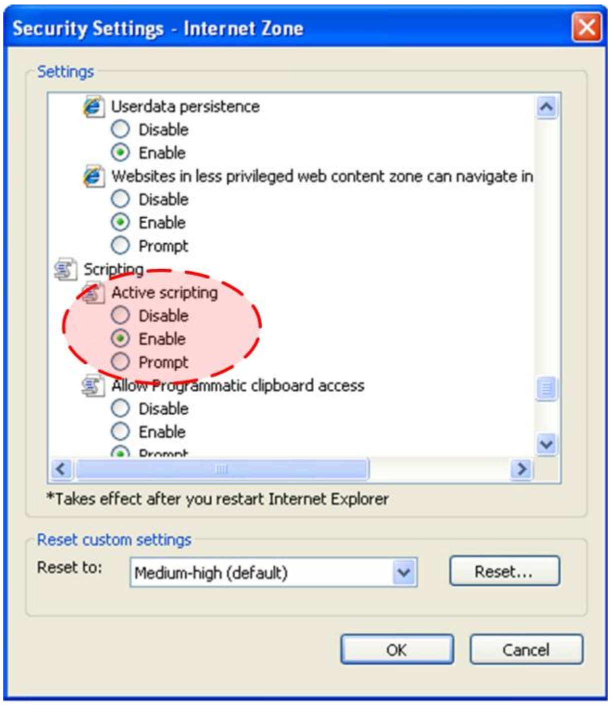
Siqura MX applications using automatic port number allocation may use 55000 and up.

11 Appendix: Enabling JavaScript

In order for the A-80 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.



Security Settings - Internet Zone

Settings

Userdata persistence
○ Disable
● Enable

Websites in less privileged web content zone can navigate in
○ Disable
● Enable
○ Prompt

Scripting

Active scripting
○ Disable
● Enable
○ Prompt

Allow Programmatic clipboard access
○ Disable
○ Enable
● Prompt

*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium-high (default)

Active scripting enabled

12 Appendix: Technical Specifications

Siqura A-80	8-channel audio and contact closure card
AUDIO	
Number of channels	8 (mono, full-duplex)
Number of streams	Max. 10 RTSP or 3 MX streams per input (multi- and/or unicast)
Maximum bandwidth	20 Hz to 8 kHz
Compression	G.711 (A- or µ-law)
Input level	Adjustable, mic or line (phantom powered)
Output level	Adjustable, 3 Vrms max.
Input impedance	600Ω or 20 kΩ balanced
Output impedance	100Ω unbalanced
Connector type	push-in spring-cage connector
CONTACT CLOSURE	
Number of channels	8x in, 4x out
Number of streams	3 MX streams per input (multi- and/or unicast)
Output	Fail-safe, open collector
Connector type	push-in spring-cage connector
TRANSMISSION INTERFACE	
Number of interfaces	1
Interface	10/100Base-TX Fast-Ethernet, Auto-Negotiation, half-duplex/full-duplex, 10/100 Mb
SFP option	Empty SFP slot for 100 Mbps SFP device
Protocols	RTP, RTCP, RTSP, TCP, UDP, IP, DHCP, IGMPv2, (S)NTP, MX/IP, HTTP, SNMP v2, FTP, TelNet, DiffServ, SAP, UPnP
Connector type	RJ-45
MANAGEMENT	
LED status indicators ▸ DC ▸ SYNC	 Power-on indicator (green) All links are operational (green); failure in RX stream(s) (yellow); failure in TX stream(s) (red)
Ethernet port	Green LED: on=100 Mb, off=10 Mb; Amber LED: on=link okay, flashes with activity
Network management & Control	SNMP v2, MX™, HTTP API, HTML (password protected)
POWERING	
Power consumption	<6W
Rack-mount units	MC10 and MC11 power supply cabinets

Siqura A-80	8-channel audio and contact closure card
Stand-alone units (/SA)	11 to 19 VDC (PSA-12 DC/25 or PSR-12 DC)
ENVIRONMENTAL	
Operating temperature	-10°C to +60°C (+14°F to +140°F)
Relative humidity	<95% as long as there is no condensation.
MTBF	>200,000 hours
Safety & EMC	IEC/EN 60950-1, IEC/EN 60825, IEC/EN 61000, EN 50130-4, EN 50081-1, EN 55022, FCC part 15
MECHANICAL	
Dimensions (h x w x d)	128 x 34 x 190 mm (5.04 x 1.34 x 7.5 in.)
Weight (approx.)	450g (15.80 oz.)
Housing	Rack-mount or stand-alone (/SA)

TKH Security Sales Offices

China

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

Czech Republic

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

Denmark

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

France

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

Germany

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

Italy

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

The Netherlands

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

Poland

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

Singapore

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

Spain

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

Sweden

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

United Arab Emirates

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

United Kingdom

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

USA

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