# TC620-PID

## Firmware Version 4.22.1

Thermal IP camera with Perimeter Intrusion Detection

# 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.

TC620 v4.22.1
User Manual v6 (151602-6)
AIT55

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.

## 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 About this manual

## What's in this manual

This manual applies to the following TKH Security camera lines:

- TC620-PID
- Explosion-proof (EX) and Safe Area (SA) series cameras with integrated TC620-PID camera.

**Important:** In this manual, "TC620" is the product name used when main features common to all models are described. In descriptions of distinguishing features, the specific model name is used.

This manual explains:

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

## Where to find more information

Find product specific datasheets, manuals, EU Declarations of Conformity and firmware updates at www.tkhsecurity.com/support-files. Make sure that you have the latest version of this manual.

- TC620-PID: For instructions on camera installation and establishing connections, see the separate TC620-PID Installation Manual.
- SA-/EX-BC820v2H3-TC620 D models: For instructions on configuring and operating the BC820v2H3 camera integrated in dual camera units, refer to the User Manual for the BC820v2H3.
- SA/EX models: For instructions on the physical installation of the camera, refer to the Installation Manual for the SA/EX Fixed or SA/EX PTZ Camera Station.

## Who this manual is for

These instructions are for all professionals who will configure and operate this product.

## What you should already know

Adequate knowledge and skills in the following fields are recommended when working with this product:

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

## Before you continue

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

## Why specifications may change

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

## We like to hear from you!

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

## Acknowledgement

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

# 2 Safety and compliance

This chapter gives the TC620 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 TC620 datasheet at www.tkhsecurity.com/support-files.

## Optical safety

*The following optical safety information applies to TC620 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.

Hazard Level 1M

## 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.

## Handle the camera carefully

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

## Do not disassemble the camera

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

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

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

## Never face the camera towards the sun

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

## 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 Protection against overvoltage

The installer is responsible for protection of the camera against overvoltage.

These international standards apply (equivalent standards may also be used):

- IEC 60364-4-44 Electrical installations of buildings - Part 4-443:
  Protection against overvoltages of atmospheric origin or due to switching.
- IEC 60364-5-53 Electrical installations of buildings - Part 5-534:
  Devices for protection against overvoltages
- IEC 62305 Protection against lightning – All parts

The information below can be used to determine the required measures.

### Transient overvoltage immunity test level

The equipment installed in this outdoor enclosure, including camera and power supply, is tested for application in an industrial environment. The transient overvoltage immunity is tested according IEC 61000-6-2 and IEC 61000-4-5 for industrial levels.

- For AC power ports the test level is 2kV Line to Earth and 1kV Line to Line.
- For signal ports the test level is 1kV Line to Earth. (no Line to Line test required)

### Overvoltage Category according IEC 60950-22

Mains-operated outdoor equipment shall be suitable for the highest Overvoltage Category expected in the installation location. The Overvoltage Category for outdoor equipment can be higher than for indoor equipment. This outdoor enclosure and the internal camera equipment is designed for overvoltage category II.

The installer is required to provide additional protection to reduce the overvoltage if the equipment is subject to transient overvoltages exceeding those for Overvoltage Category II.

It is permitted to include protection components within the outdoor equipment. Components used to reduce the Overvoltage Category, Surge Protection Devices (SPD), shall comply with the requirements of IEC 61643-series or equivalent standards.

NOTE: The Overvoltage Category of outdoor equipment is normally considered to be one of the following:

- if powered via the normal building installation wiring, Overvoltage Category II;
- if powered directly from the mains distribution system, Overvoltage Category III;
- if at, or in the proximity of, the origin of the electrical installation, Overvoltage Category IV.

### Protection against lightning strikes (direct and indirect)

Additional protection is also required for protection against direct or indirect lightning strikes according the IEC 62305 series standards, or equivalent standards.

Consideration shall be given to the following:

- The use of properly earthed air-termination rods for pole-mounted or high-mounted cameras
- Avoid wiring loops
- Locate protection devices close to the protected equipment (within 0.5 m)
- Keep wiring to protection devices short.

## 2.3 Compliance

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

# 3 Product overview

This chapter introduces the TC620 and its features.

## In This Chapter

## 3.1 Features

**TC620-PID**

**Outdoor thermal IP camera with Perimeter Intrusion Detection**

- Integrated thermal IP camera
- Built-in Perimeter Intrusion Detection
- Based on analytics certified by i-LIDS® for primary sensor in sterile zone
- ONVIF Profile S conformant
- Video resolution: 336x256
- Robust aluminium housing
- Fully digital

## 3.2 Description

The TC620 is in itself a complete solution for perimeter intrusion detection. It is built around a thermal LWIR sensor and on-board analytics for accurate detection of unwanted intrusions. By using thermal vision, detection is possible in all weather, no-light, and difficult lighting conditions. The TC620 comes as an outdoor camera (IP66).

### Intrusion detection

The embedded ObjectR-Advanced PID analytics is i–LIDS® certified and approved to be used as primary sensor in a sterile zone. Through the web interface, configuration of the ObjectR-Advanced PID analytics is straightforward with either two detection lines or two detection zones. To get the most out of the PID analytics TKH Security offers the VCA Configuration Server. By using a thermal sensor the influence of external factors is limited to a minimum.

### Decision making and situational awareness

Do you often feel that you have lost control? This occurs when – in a mission-critical environment where split-second decision making is crucial – you expect something to happen but it does not. Your expectations are based on all the data that is presented to you and its history. To make the right decision you need to be aware of the environment around you and have access to information relevant only for that specific situation – not the enormous amount of useless data you get when watching 24 CCTV monitors simultaneously, for example. The TC620 extracts useful information from the scene and presents it in the video image itself to a video management system, such as VDG Sense.

## VDG Sense

The TC620 works seamlessly with the VDG Sense video management system. It supports forensic search by storing the PID object data next to the video. The PID events are triggers to the powerful VDG Sense macro engine, which enables you to define how the system should react during certain events. You can set macros to have VDG Sense automatically pop up a camera to inform the operator of an intrusion alert.

## VCA Configuration Server (VCS)

ObjectR-Advanced PID detection analytics physically runs in the TKH Security edge devices. This detection engine, however, is much more powerful when configured by the TKH Security VCA Configuration Server. The configuration server adds more detection templates, such as eight zones or lines. The VCS is capable of storing up to 64 channels of video and object data. Forensic searches are done using the stored object data which speeds up the search up to 10,000 times faster than real-time. This feature is also used to find the best configuration for a camera using the real footage. This configuration is uploaded in the TC620, with the best performance and reliability for the perimeter intrusion detection.

## Thermal imaging

It is possible to use standard CCTV cameras for video analytics but it requires experience and knowledge of the analytics to position them. All sorts of distractions, such as the headlights of a car, can cause false alerts. In certain situations, image clarity is compromised when using visible light cameras, which may result in degraded automatic intruder detection.

*Headlights*

*Sun in lens*

*Streetlights*

Lighting conditions do not pose any problems for the TC620-PID thermal camera. It does not ‘see’ shadows and light beams. It picks up the heat (deep infrared) radiated by the objects themselves.

## Field-hardened

The ruggedised and vandal-resistant die-cast aluminium housing has an IP66 ingress rating to ensure optimal protection in harsh environments.

## Open Streaming Architecture (OSA) and ONVIF

The TC620 is designed with OSA offering standardised streaming video and remote control based on international standards and tested with different vendors. A comprehensive HTTP API gives access to all controls and makes integration easy. The TC620 also fully supports ONVIF and is listed as ONVIF Profile S conformant.

## Web interface

Configuration, management, and live viewing are simplified by the access-controlled web interface. Full in-band control is available through Device Manager and the HTTP API. The TC620 is field-upgradeable.

## FTP push

Upon an event, the TC620 can push a JPG image to one or two FTP servers. The event can be triggered externally by Perimeter Intrusion Detection, VMD, or Tamper Detect. The TC620 can also periodically upload images to the remote server(s).

## SA and EX models

The EX and SA camera lines include fixed and PTZ camera stations with integrated TC620 camera. The camera stations are designed for use in onshore, offshore, marine and heavy industrial environments. EX models are explosion-protected for use in hazardous areas in these environments.

# 4 Interfaces

A variety of methods can be employed to communicate with the TC620. This chapter outlines the interfaces you can use to control the unit and manage the media streams it is handling.

## In This Chapter

## 4.1 ONVIF

The Open Network Video Interface Forum (ONVIF) is an open industry forum for the development of a global standard for the interface of IP-based physical security products. ONVIF is committed to the adoption of IP in the security market. The ONVIF specification ensures interoperability between products regardless of manufacturer. It defines a common protocol for the exchange of information between network video devices including automatic device discovery, video streaming and intelligence metadata. The TC620 fully supports ONVIF. It has been tested to support ONVIF Profile S.

## 4.2 OSA

TKH Security's Open Streaming Architecture (OSA) consists of a standard set of open communication protocols to govern media streaming via RTSP and equipment management via HTTP. OSA enables easy integration of the TC620 with third-party products. The protocol consists mainly of different CGI (Common Gateway Interface) program calls for listing and configuring parameters. A detailed description of the HTTP API is given in the *SPI* specification which can be downloaded at www.tkhsecurity.com/support-files.

## 4.3 Web UI

Using the TC620's web server is the most straightforward way to access the unit. The webpages enable you to configure the settings of the TC620 and view live video images from a standard web browser.

## 4.4 MX/IP

MX/IP is a proprietary TKH Security protocol which gives direct access to the settings of the TC620. Using special MX software, such as *MX Configuration Tool*, TC620 settings can be read from and written to the *Management Information Base* (MIB), a list of variables stored inside the unit. Offering full control of the TC620, the MIB enables you to remotely configure device settings and manage media streams. Additional MX viewing and control software offers real-time monitoring of video streams and playback of recorded images. For more information about MX/IP, the MIB, and the EMX network service, refer to the manuals which document the MX SDK and the MX applications.

**Note:** If you prefer using open standards, you can disable the MX/IP protocol. This is done on the MX tab of the Device Management page. Be aware that doing so prevents you from upgrading the TC620 firmware through *MX Firmware Upgrade Tool*.

## 4.5 SNMP

The Simple Network Management Protocol (SNMP), part of the internet protocol suite, can be used to monitor network devices such as the TC620 for conditions or events that require administrative attention. For more information, refer to appropriate literature on SNMP.

The TC620 supports in-band SNMP. Via SNMP, several status variables can be read and traps can be generated on events. You can configure TC620 SNMP settings on the SNMP tab of the Device Management page.

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

**Note:** The TC620 includes SNMP support for its tamper detect function. A trap is sent when camera tampering is detected.

Required MIB files can be downloaded at www.tkhsecurity.com/support-files.

## 4.6 SAP

The TC620 supports the Session Announcement Protocol (SAP), a protocol used for broadcasting multicast session information. A SAP listening application can listen to the announcements advertised by the TC620 SAP announcer. The application can use this information to receive a video or audio stream that the TC620 is transmitting to the advertised multicast address. For more information, see the description of the Video and Audio pages.

## 4.7 NTCIP

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

The TC620 supports all the mandatory parts and some of the optional parts of the NTCIP CCTV specification as laid down in the NTCIP 1205:2001 v01.08 document. For details about the NTCIP configuration of the TC620, see *Appendix: NTCIP Configuration*.

The TC620 supports the standard NTCIP SNMP MIB. This MIB database is used to store information, which in turn will be used to control cameras and other devices in the transportation management system. An electronic version of the MIB is available from a NEMA FTP site. To get access to the FTP site, send your name, organisation name, and email address to ntcip@nema.org, and request access.

# 5 Stream media via RTSP

The easiest way to extract a video or audio stream from the TC620 is to use the Real-Time Streaming Protocol (RTSP). This chapter explains the role of the TC620 in RTSP media sessions and describes how to open a media stream from the unit in a video player plug-in.

## In This Chapter

## 5.1 RTSP and RTP

The TC620 implements an RTSP server. A hardware or software decoder (the latter within a viewing application, for example) is the RTSP client. Media sessions between client and server are established and controlled with RTSP. Media stream delivery itself is handled by the Real-Time Transport Protocol (RTP). The TC620 supports video and audio streaming via UDP and TCP.

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

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

where:

<**x**> is the number of the Video Input

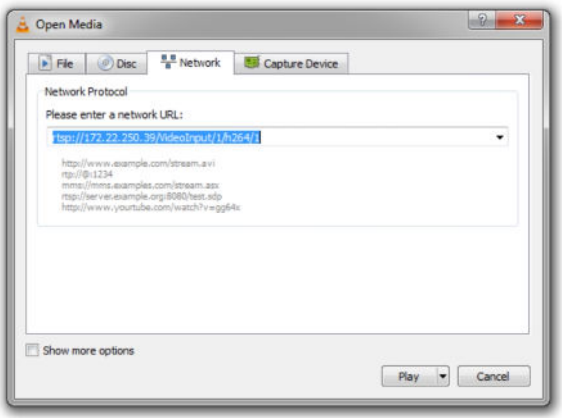
<**y**> is the media type of the required encoder

<**z**> is the encoder number

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

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

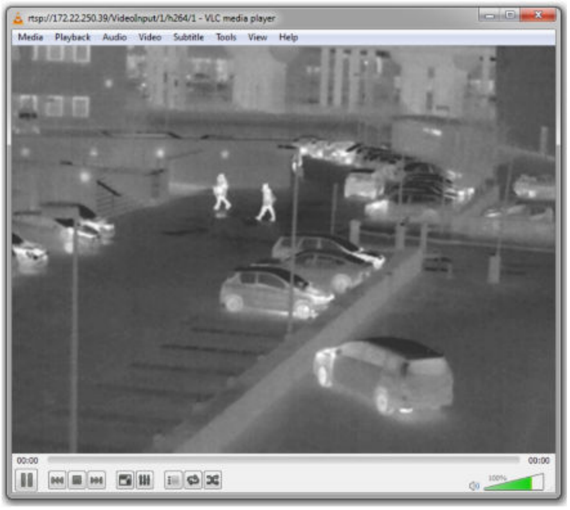
The stream in the following figure will be pulled from the unit with the IP address 172.22.250.39, using Video Input 1 and the first enabled H.264 encoder.



Please enter a network URL: rtsp://172.22.250.39/VideoInput/1/h264/1

Open Media
File
Disc
Network
Capture Device
Network Protocol
http://www.example.com/stream.avi
rtp://@:1234
mms://mms.examples.com/stream.asx
rtsp://server.example.org:8080/test.sdp
http://www.yourtube.com/watch?v=gg64x
Show more options
Play
Cancel

*RTSP URL format*



*A TC620 video stream viewed in VLC*

## 5.2 Transfer via UDP or TCP

The TC620 supports the following types of streaming.

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

The TC620 reports to the client that it supports transfer over UDP and TCP. The choice is made on the client side. In VLC, for example, using a TCP connection can be forced (*Preferences > Inputs and Codecs > Network > RTP over RTSP (TCP)*).

For details on controlling TC620 media streams through HTTP and RTSP, refer to the *SPI* specification. You can download this HTTP API specification at www.tkhsecurity.com/support-files.

# 6 Access the webpages

The webpages of the TC620 offer a user-friendly interface for configuring its settings and viewing live video over the network. This chapter explains how to connect to the web interface of the unit.

## In This Chapter

## 6.1 System requirements

To access the webpages of the TC620 you need the following.

- A PC with a web browser installed.
- An IP connection between the PC and the TC620.

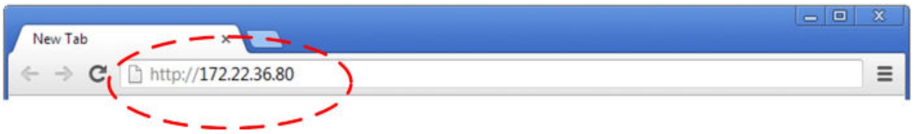
## 6.2 Connect via web browser

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

1. Open your web browser.
2. Type the IP address of the TC620 in the address bar, and then press ENTER.

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

   If the page is not displayed correctly, make sure that JavaScript is enabled in your web browser (see *Appendix: Enable JavaScript*).



*Type the IP address of the TC620 in the address bar of the browser*

# 6.3 Find the unit with Device Manager

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

### ⏩ To install Device Manager

1 Download the latest version of Device Manager at www.tkhsecurity.com/support-files.

2 Double-click the setup file.

3 Follow the installation steps to install the software.

### ⏩ To connect to the unit via Device Manager

1 Start Device Manager

The network is scanned and detected devices appear in the *List View* pane.

2 If multiple network adapters exist, select the appropriate adapter to scan the network that you wish to connect to.

3 To refresh the *List view* pane, click the **Rescan now** button.

4 Use the tabs in the *Tree View* pane to define the scope of your search.

5 Click the column headings in the *List View* pane to sort devices by type, IP address, or name.

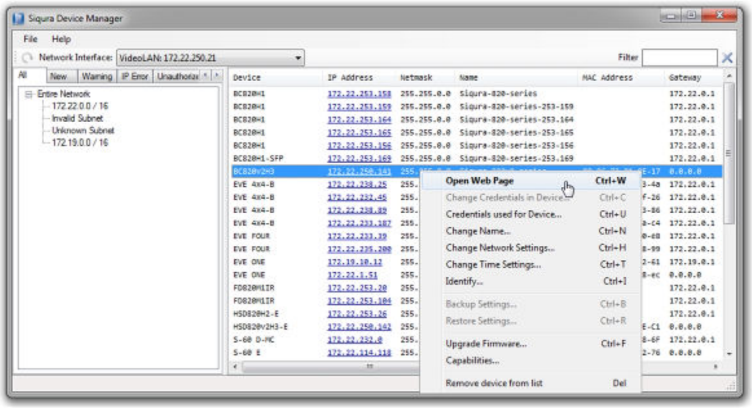
6 Use the *Filter* box, to search for a specific series or model.

7 To connect to the webpages of the TC620, double-click its entry in the device list,

- or -

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

The login page of the TC620 is opened in your web browser.



| Device | IP Address | Netmask | Name | MAC Address | Gateway |
|---|---|---|---|---|---|
| BC820H1 | 172.22.253.158 | 255.255.0.0 | Siqura-820-series | | 172.22.0.1 |
| BC820H1 | 172.22.253.159 | 255.255.0.0 | Siqura-820-series-253-159 | | 172.22.0.1 |
| BC820H1 | 172.22.253.164 | 255.255.0.0 | Siqura-820-series-253.164 | | 172.22.0.1 |
| BC820H1 | 172.22.253.165 | 255.255.0.0 | Siqura-820-series-253-165 | | 172.22.0.1 |
| BC820H1 | 172.22.253.156 | 255.255.0.0 | Siqura-820-series-253-156 | | 172.22.0.1 |
| BC820H1-SFP | 172.22.253.169 | 255.255.0.0 | Siqura-820-series-253.169 | | 172.22.0.1 |
| BC820V2H3 | 172.22.250.141 | 255. | | E-17 | 0.0.0.0 |
| EVE 4X4-B | 172.22.238.25 | 255. | | 3-4a | 172.22.0.1 |
| EVE 4X4-B | 172.22.232.45 | 255. | | f-26 | 172.22.0.1 |
| EVE 4X4-B | 172.22.238.89 | 255. | | 3-86 | 172.22.0.1 |
| EVE 4X4-B | 172.22.233.187 | 255. | | a-c4 | 172.22.0.1 |
| EVE FOUR | 172.22.233.39 | 255. | | 0-e8 | 172.22.0.1 |
| EVE FOUR | 172.22.235.200 | 255. | | 8-99 | 172.22.0.1 |
| EVE ONE | 172.19.10.12 | 255. | | 2-61 | 172.19.0.1 |
| EVE ONE | 172.22.1.51 | 255. | | 8-ec | 0.0.0.0 |
| FD820M1IR | 172.22.253.20 | 255. | | | 172.22.0.1 |
| FD820M1IR | 172.22.253.104 | 255. | | | 172.22.0.1 |
| HSD820H2-E | 172.22.253.26 | 255. | | | 172.22.0.1 |
| HSD820V2H3-E | 172.22.250.142 | 255. | | E-C1 | 0.0.0.0 |
| S-60 D-MC | 172.22.232.0 | 255. | | 8-6F | 172.22.0.1 |
| S-60 E | 172.22.114.118 | 255. | | 2-76 | 0.0.0.0 |

*Connect to a device via Device Manager*

## 6.4 Connect via UPnP

Universal Plug and Play (UPnP) support is enabled by default on the TC620. With the UPnP service enabled in Windows (see *Appendix: Enable UPnP in Windows*), you can access the unit from Windows Explorer.

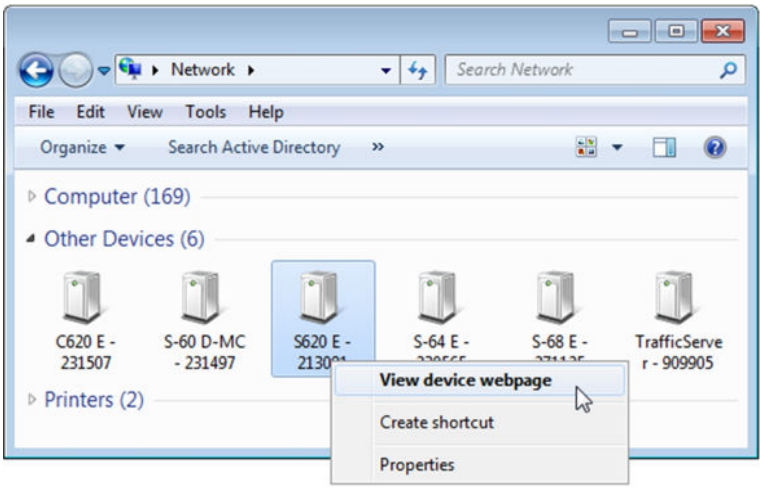
### ⏩ To connect to the unit via UPnP

1 In Windows Explorer, open the **Network** folder.

Detected devices in the same subnet as the computer are displayed, including TKH Security codecs and cameras with UPnP support.

2 Double-click the TC620,
- or -
Right-click the unit, and then click **View device webpage**.

The login page of the TC620 is opened in your web browser.



*Connect to a device via Windows Explorer*

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

## 6.5 Log on to the unit

Users with a valid account for the TC620 can log on to the unit.

### ⏩ To log on to the TC620

1 On the Login page, click **LOGIN**.

2 Log on with the account that was created for you.

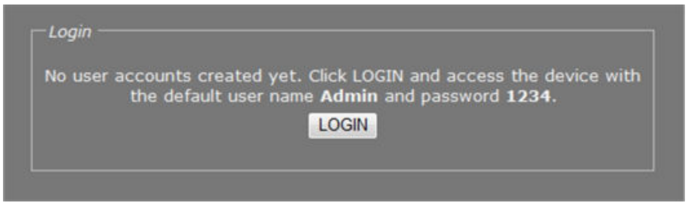
User name and password are case sensitive.

The default user name set at the factory for the TC620 is "Admin" with password "1234".

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

3 Click **OK** or press ENTER.

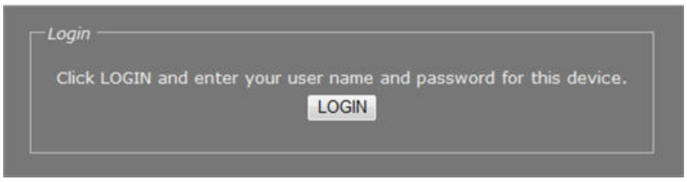
On successful login, the Live Video page appears.



Login

No user accounts created yet. Click LOGIN and access the device with the default user name **Admin** and password **1234**.

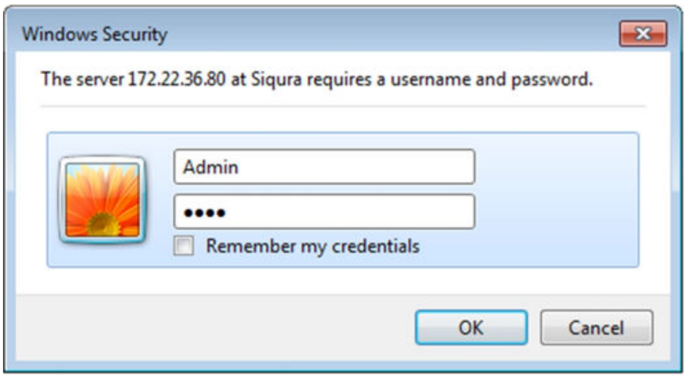
*Access possible with default Admin account only (default Admin password unchanged)*



Login

Click LOGIN and enter your user name and password for this device.

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



Windows Security

The server 172.22.36.80 at Siqura requires a username and password.

Admin

••••

□ Remember my credentials

*Connect dialogue box*

# 7 Navigate the webpages

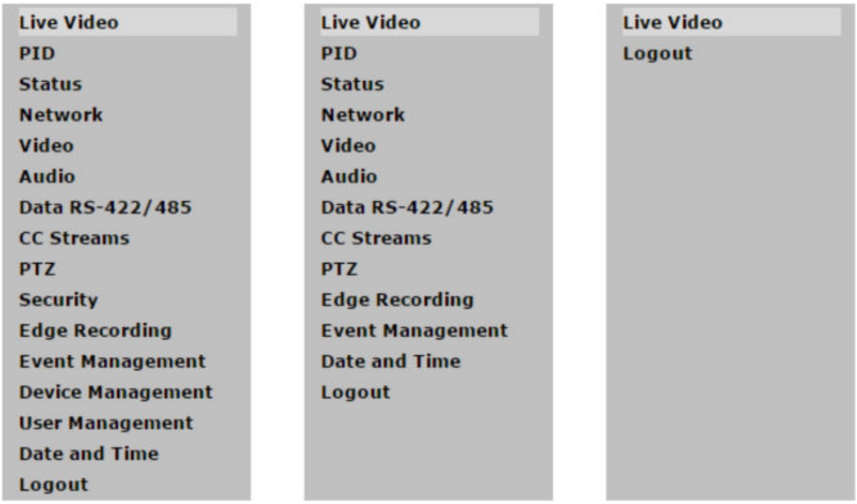
This chapter introduces the webpages and common elements found on them. It also discusses user account types and associated access levels.

## In This Chapter

## 7.1 Menu

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

- Click the option associated with the user or device settings you want to view or configure.
- Click **Live Video** to reopen the home page of the TC620.
- Click **Logout** to log out the current user and display the Login box.



*TC620 menus available to (from left to right) Admin, Operator, and Viewer accounts*

## 7.2 Access control

Whether a specific TC620 webpage is available to you on the navigation menu depends on the user account you logged in with. The unit supports three account types with associated access levels.

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

## 7.3 Webpage elements

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

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

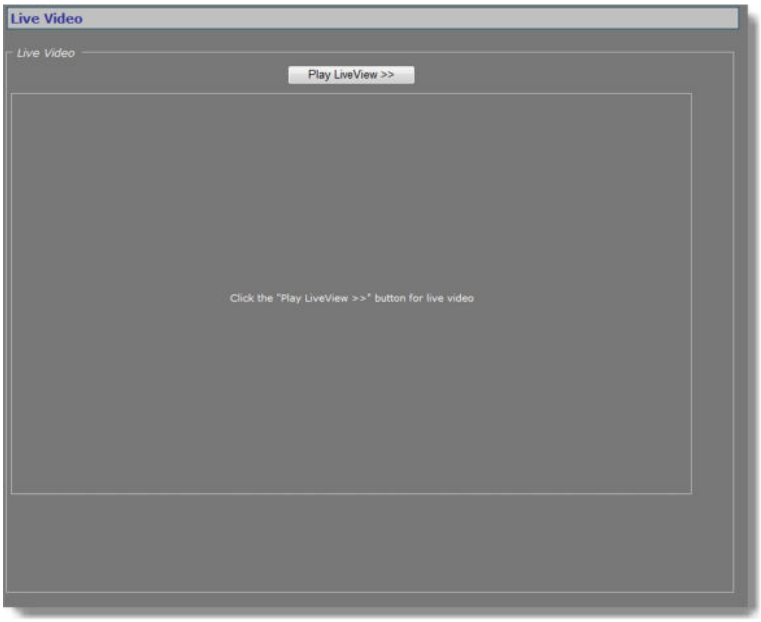
| This Button | Does This | Note |
|---|---|---|
| Save | Writes changes to the unit. | Some sections (for example, those on the VMD tab of the Video page) do not have *Save* and *Cancel* buttons. Changes you make here are immediately written to the device. |
| Cancel | Undoes unsaved changes and shows values as they were before editing. | |
| Advanced >> | Opens the Advanced Settings section with additional settings. | **Important:** Be aware that configuring Advanced Settings requires in-depth understanding of the impact of your changes on the workings of your TC620. If in doubt, do *not* change the default values. |
| << Simplified | Closes the Advanced Settings section. | |

# 8 View live video via browser

On the Live Video page, you can view live video from the TC620 and - if PTZ functionality is implemented - control the camera from your web browser.

## In This Chapter

## 8.1 Activate Live View



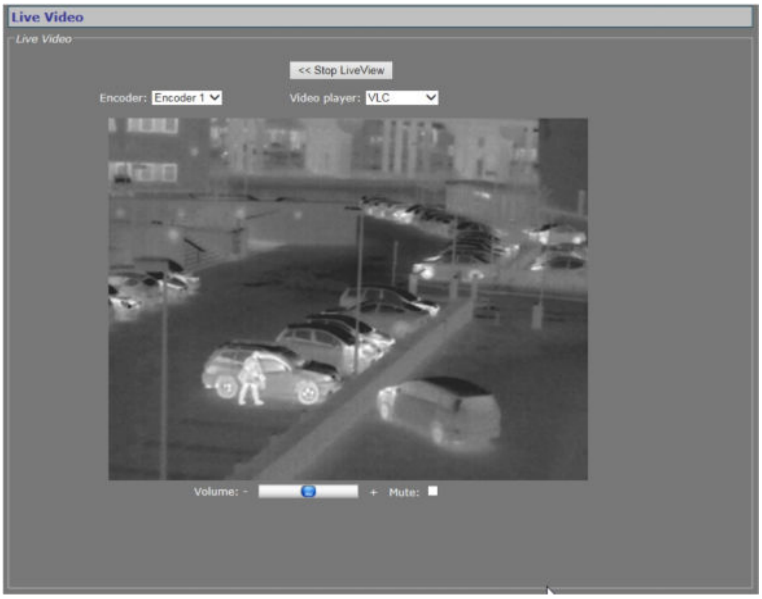
*Live View inactive*

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

### ⏩ To activate Live View

- Click **Play LiveView>>**.

## 8.2 View live video



Encoder: Encoder 1

Video player: VLC

*Live View activated*

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

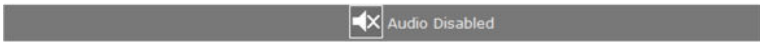
| Item | Description | |
|---|---|---|
| <<Stop Live View | Closes the preview. | |
| Encoder | *Encoder 1* | The video encoder used to encode the images seen in the preview. |
| | *Encoder 2* | |
| | *Live View* | |
| Video player | *QuickTime* | The plug-in used to display the images in the previews on this page and the Video pages. |
| | *VLC* | |
| | *No Player* | Neither QuickTime nor VLC is detected on the host machine. For more information, see *Appendix: Install a video player*. |
| Refresh rate | Available in Live View encoder mode. Indicates the current refresh rate of the webpage. | |
| Preview | Shows live images from the video source as encoded by the selected encoder. H.264 previews are streamed over RTSP. Live View encoder previews are transported to the webpage using the HTTP protocol. | |
| Volume | Available in Encoder 1/2 mode. Drag the sliding button to control audio volume. | |
| Mute | Available in Encoder 1/2 mode. Select or clear this box to mute or unmute audio, respectively. | |

### Enable an encoder

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

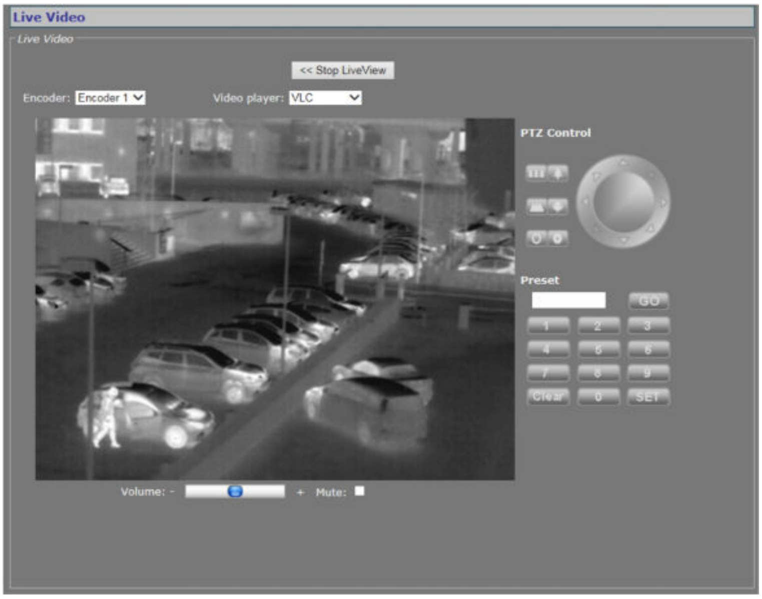
### Enable audio

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



*Audio Disabled warning*

## 8.3 Use your browser for PTZ control



Encoder: Encoder 1

Video player: VLC

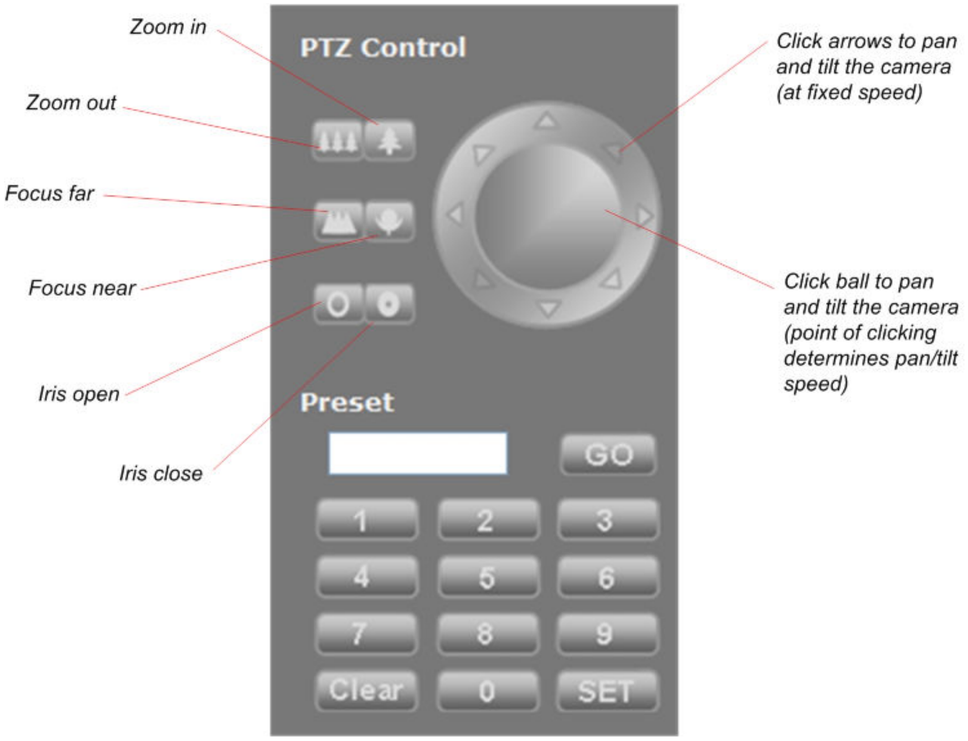
*Live Video page with PTZ Control panel*

### Display the PTZ control panel

Although the TC620 itself does not have PTZ functionality, it can be mounted on a PTZ mounting bracket which can then be controlled from the TC620's serial data port (RS-4xx). With a PTZ driver selected on the PTZ webpage, the PTZ control panel is available on the Live Video page. If the TC620 supports the PTZ driver, you can use the panel to control the camera and manage the presets via the mounting bracket. PTZ drivers not included in the driver list on the PTZ page can be uploaded to the TC620 via PTZ Driver Management on the same page.

### PTZ control

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


Zoom in
Zoom out
Focus far
Focus near
Iris open
Iris close
PTZ Control
Preset
GO
1
2
3
4
5
6
7
8
9
Clear
0
SET
Click arrows to pan and tilt the camera (at fixed speed)
Click ball to pan and tilt the camera (point of clicking determines pan/tilt speed)

*PTZ Control panel*

## Preset

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

### ⏩ To enter and save a preset camera position

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

2 Adjust the position of the camera for the desired view.

3 When satisfied with the position, click **SET**.

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

### ⏩ To recall a preset camera position

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

2 Click **GO**.

### ⏩ To erase a preset camera position

1 Call the preset.

2 Press **Clear**.

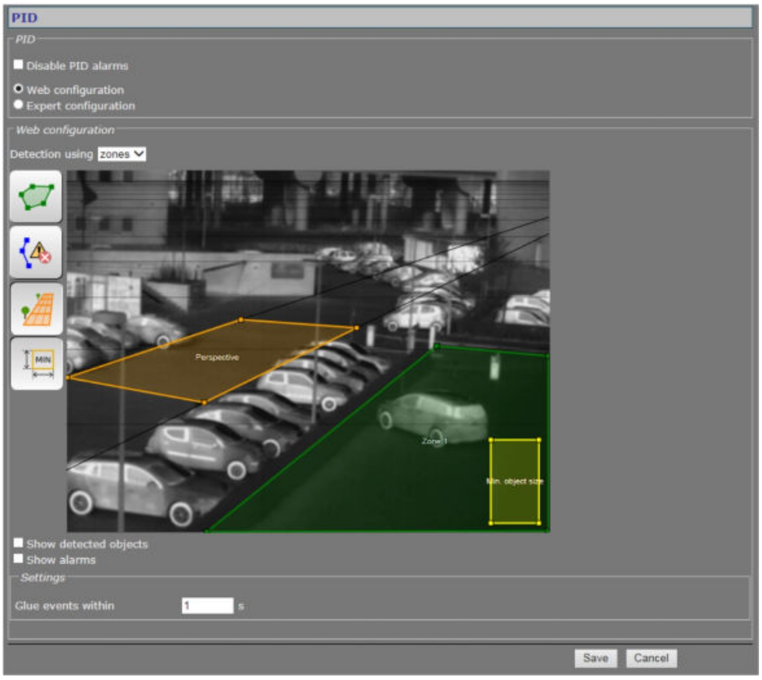
3 If desired, override the preset with a new preset position.

# 9 PID

The TC620 is a complete solution for perimeter intrusion detection. This chapter explains how to use the web interface to configure the on-board analytics for accurate detection of unwanted intrusions.

## In This Chapter

## 9.1 PID



PID

*PID*

□ Disable PID alarms

● Web configuration
○ Expert configuration

*Web configuration*

Detection using zones

□ Show detected objects
□ Show alarms

*Settings*

Glue events within 1 s

*PID*

Perimeter Intrusion Detection (PID) is an early warning application which triggers an alert when a predefined perimeter within the area monitored by the TC620 is violated. The PID video analytics uses configurable detection zones, detection lines, and object size with perspective correction to identify and track an object through the camera scene. The video content analysis algorithms continuously monitor the video images and decide when to issue an alert.

Through the Event Management webpage, PID events can be associated with a CC Output, a CC Stream, or an FTP Push event to notify an operator in a control room of security issues. Once alerted, it is up to the operator to assess the specific event and undertake appropriate action.

## 9.1.1 Camera installation

The following sections describe how to use the PID page to set up the PID functionality. However, before you are ready to embark on this task, it is imperative to make sure that the camera is properly installed for PID application.

Installing cameras and lighting for surveillance purposes requires specific professional skills. The requirements for camera images processed with automatic PID functionality differ significantly from the requirements for images monitored by human observers.

For example, in conventional surveillance camera setups, the camera is often aligned such that it provides a clear overview of the entire site, including a natural horizon showing some of the sky. For PID purposes, however, the only relevant part of that image is the detection zone. All other parts of the image are irrelevant and can decrease PID sensitivity, because they leave fewer pixels for the objects within the detection zone, thus potentially leading to degraded detection performance.

Also, for example, sky in the image causes the Automatic Gain Control (AGC) of the camera to adjust, possibly degrading the image in which objects are to be detected.

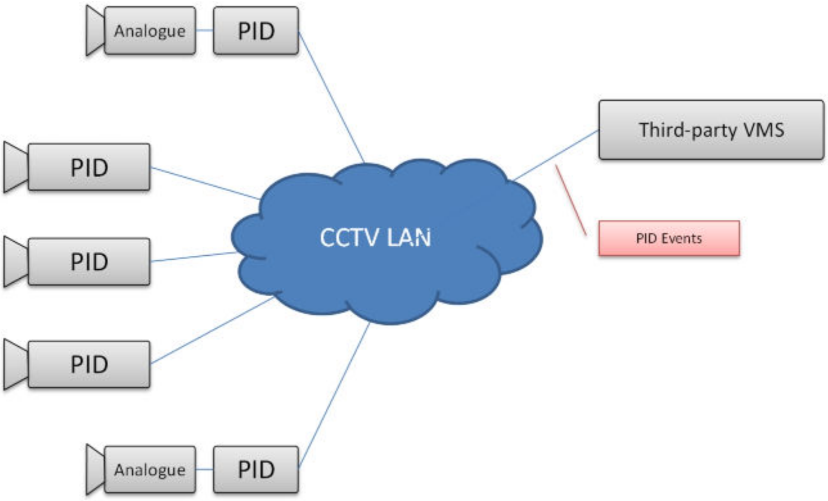
## 9.1.2 PID solutions

PID detection can be active in an edge device, such as the TC620, or in a remote server. The detector analyses the images and separates the moving objects from the background. These objects are called ‘blobs’. By adding detection lines or detection zones, specific rule sets are applied on the blobs triggering events, which can be read by VDG Sense or other video management systems.

TKH Security offers a variety of intrusion detection solutions:

- Stand-alone TKH Security PID device
- TKH Security PID device(s) and VDG Sense VMS
- TKH Security PID device(s) and VCA Configuration Server (VCS)

### 9.1.2.1 Stand-alone solution

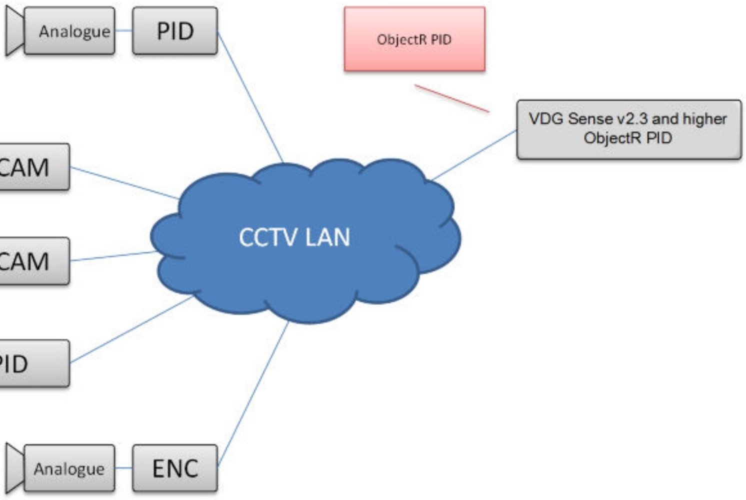


*Stand-alone PID devices (3x camera with PID, 1x video encoder with PID)*

The TC620 can run stand-alone. The device offers an intuitive web interface to draw the multipoint detection lines or zones in the image as described later in this chapter.

The detection is limited to either two direction-sensitive multipoint detection lines or two multipoint detection zones.

### 9.1.2.2 TC620/VDG Sense solution



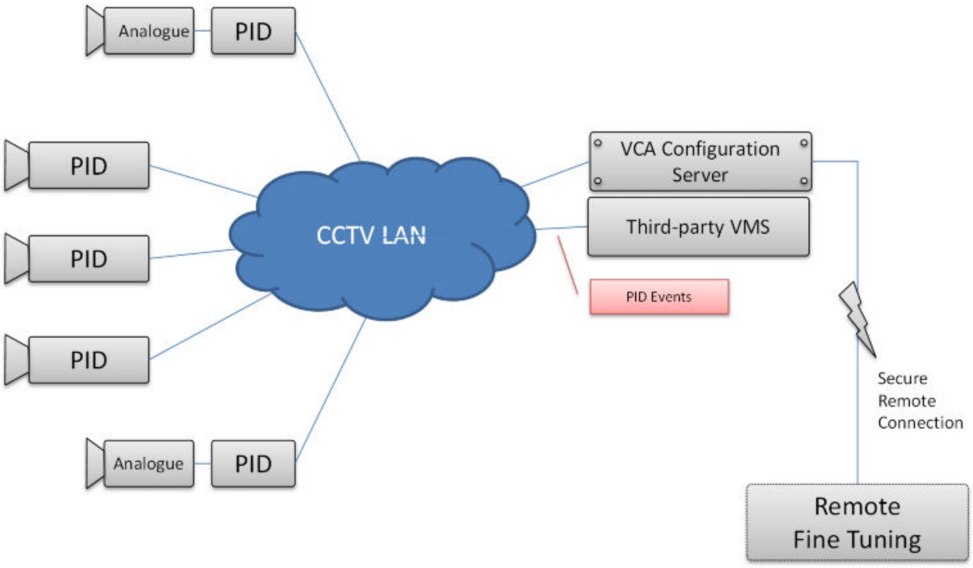
*TC620/VDG Sense solution*

In the TC620/VDG Sense solution, detection is done either in the TC620 or in VDG Sense if other (non-PID) IP cameras are connected. In both cases VDG Sense can be used for configuration and recording of the blob stream.

The VCA features available together with VDG Sense are:

- Super fast forensic search on the recorded images
- 8x Multipoint detection zones
- 4x Multipoint detection lines, direction sensitive
- Perspective, minimum and maximum object size
- Object life time and displacement
- Counting

### 9.1.2.3 TC620/VCS solution



*TC620/VCS solution*

In case of an installation without VDG Sense, the TKH Security VCA Configuration Server (TKH Security VCS) can be used to extend the number of VCA features.

The VCA features available together with the TKH Security VCS are:

- Super fast forensic search on the recorded images
- 8x Multipoint detection zones
- 4x Multipoint detection lines, direction sensitive
- Perspective, minimum and maximum object size
- Object life time and displacement
- Counting
- (Remote) PID Fine tuning

## 9.1.3 Configuration methods

The PID functionality on the TC620 can be set up from the PID page in the following ways.

- Use **Web configuration** to configure settings on the fly.
- Use **Expert configuration** to upload an external configuration file containing predefined settings to the unit.

## 9.1.4 Web configuration

Configuring PID from the webpage involves the following steps.

1 Enable web configuration
2 Select a detection type
3 Set up the detection layout
4 Configure zone and line properties
5 Configure event settings

**Note:** After you have gone through the steps above it may take a few minutes before PID performance is optimal. The TC620 uses this time to process the scene, the detection layout, and the event settings.

## 9.1.4.1 Enable web configuration

### ⏩ To enable Web configuration

- In the *PID* section, (if necessary) click **Web configuration**.

  The preview and various buttons, options, and parameters are now available for configuration.

## 9.1.4.2 Set the detection type

Perimeter intrusion can be detected using zones or lines. It is not possible to use the two types simultaneously.

### ⏩ To select a detection type

1 In *Web configuration*, click to open the **Detection using** list

2 Select either **zones** or **lines**.

The associated shape button is displayed to the left of the preview.

## 9.1.4.3 Shapes

To establish the exact dimensions and position of the area(s) to be monitored for events, you overlay shapes over the preview.

Shapes come in three categories.

- trigger shape
- ignore shape
- helper shape

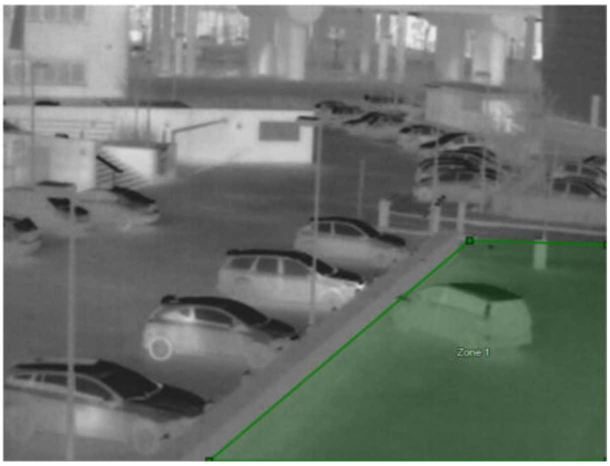
Trigger shapes are used to define the area where objects can trigger an event. Ignore shapes do the opposite. They suppress the triggering of events. Helper shapes are used to provide a visual (graphical) input for object size.

The following overlays are available.

- Detection zone (trigger)
- Detection line (trigger
- Ignore line (ignore)
- Perspective (helper)
- Minimum object size filter (helper)

### Detection zone

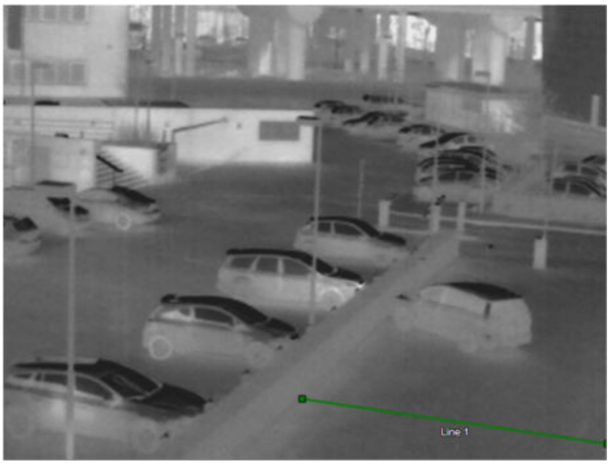
A detection zone shape is initially drawn as a box, but nodes can be added to allow for more complex shapes. Trigger conditions can be set through the context menu of the zone.



*Detection zone shape*

### Detection line

A detection line is a single line between two points which triggers when an object crosses it. Extra nodes can be added to provide a more flexible line. Trigger conditions can be set through the context menu of the line.



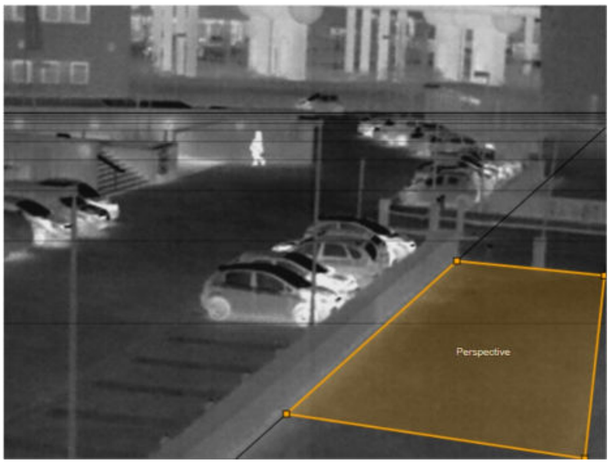
*Detection line shape*

### Ignore line

The ignore line is a single line between two points which can be placed to suppress the triggering of an event for a limited amount of time. An ignore line suppresses *all* triggers from *all* objects. Trigger conditions can be set through the context menu of the line.

### Perspective

The perspective shape is used to establish the perspective of the scene. To make calculations of the perspective correction as accurate as possible it is best to draw it in a part of the scene that shows the perspective, the bottom line and the top line of the shape must run parallel.



*Correct placement of perspective shape*

### Minimum object size filter

The Minimum object size shape describes the size of the required objects. If used in combination with the Perspective shape the Minimum object size shape will be perspective corrected.

## 9.1.4.4 Edit the preview

The Web configuration section has the following shape buttons.

| This button | | Does this |
|---|---|---|
| | **Add detection zone** | Overlays a detection zone shape over the preview<br>• Mode: detection using zones<br>• Maximum: 2 detection zones |
| | **Add detection line** | Overlays a detection line shape over the preview<br>• Mode: detection using lines<br>• Maximum: 2 detection lines |
| | **Add ignore line** | Overlays an ignore line shape over the preview<br>• Maximum: 1 ignore line |
| | **Perspective** | Overlays a perspective shape over the preview |
| MIN | **Minimum object size filter** | Overlays a minimum object size filter shape over the preview |

### ⏩ To add a shape

- Click the respective button.

### ⏩ To position a shape

- Drag the shape to where you want it.

### To resize a shape

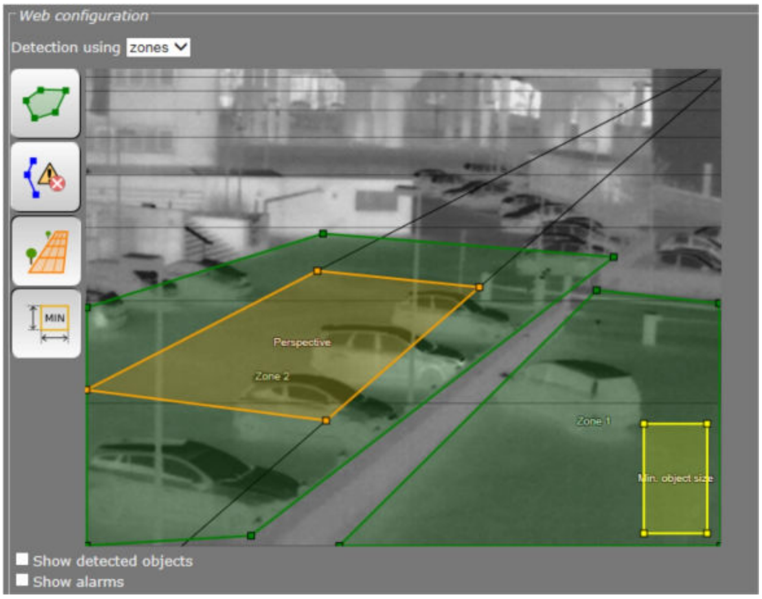
- Drag the the sizing handle(s) of the shape in the desired direction.

### To add a node to a detection zone or detection line

- Right-click the shape, and then click **Add node** on the context menu.

### To remove a shape

- Right-click the shape, and then click **Remove ...** on the context menu.
  - or -
  Click the button once again (Perspective or Minimum object size filter shape only).



Web configuration

Detection using zones

□ Show detected objects
□ Show alarms

*Detection layout example with two Detection zones, a Perspective box, and a Minimum object size box. Zone 2 has an extra node to enable resizing the shape to the desired detection area. Black horizontal lines (appearing on insertion of a Perspective box) give you a good perspective and depth perception, and can be used as guide lines when drawing detection zones or lines.*

## 9.1.4.5 Configure shape settings

The trigger conditions of a detection zone, detection line, and ignore line can be defined through their respective context menus. You can use these settings as a filter to determine when an object triggers an event. Right-click a shape to open its context menu.

### Detection zone

| Item | Description | |
|---|---|---|
| Detect delay | The time to elapse after the events described below, before a trigger is generated. | |
| Trigger mode | *Touch*<br>*Inside*<br>*Enter*<br>*Exit* | Determines whether an object needs to touch, be inside, enter, or exit the zone to generate a trigger. |
| Trigger point | *Center of gravity* | The zone is triggered when the center of gravity of an object enters or exits the zone. |
| | *Bottom center* | The zone is triggered when the bottom center of an object enters or exits the zone. |
| | **Note:** *Center of gravity* and *Bottom center* do not apply to trigger modes *Touch* and *Inside* (they are ignored in these modes). | |

### Detection line

| Item | Description | |
|---|---|---|
| Trigger Mode | *Touch*<br>*Pass CW*<br>*Pass CCW*<br>*Pass either* | Determines whether an object needs to touch the detection line or pass it clockwise, counterclockwise, or either of these two, to generate a trigger. |
| Trigger Point | *Center of gravity* | The line is triggered when the center of gravity of an object passes it CW, CCW, or either of these. |
| | *Bottom center* | The line is triggered when the bottom center of an object passes it CW, CCW, or either of these. |
| | **Note:** *Center of gravity* and *Bottom center* do not apply to trigger mode *Touch* (they are ignored in this mode). | |

### Ignore line

| Item | Description | |
|---|---|---|
| Ignore time | After the ignore line is touched or completely covered (see below), the event is suppressed for the number of seconds set here. | |
| Type | Touch | Ignore time countdown starts when an object touches the ignore line. |
| | Completely cover | Ignore time countdown starts when an object completely covers the ignore line. |

## 9.1.4.6 Show detected objects and alarms

### ⏩ To display detected objects and/or alarms in the preview

- In *Web configuration*, select the respective option(s).

Detected objects are shown in blue. Alarms are highlighted in red boxes.

## 9.1.4.7 Glue events

If consecutive events occur with short intervals it may be more efficient to "glue" them together. This means that one longer event is generated.

### ⏩ To set the glue events time

- In the *Settings* section, specify the Glue events time in the *Glue events within box*.

  The effect of the glue time is that for a given event the start time remains the same, but the peak time and end time are pushed forward in time for every glued event. When the event is retrieved, the peak time will be that of the last glued event.

## 9.1.5 Expert configuration

As an alternative to configuring PID settings on the fly through Web configuration, you can use Expert configuration to upload a configuration file to the TC620.

> **Note:** Creating a configuration file for optimal PID performance is a complex task which requires a high level of PID expertise. The technical specialists of TKH Security can assist you with this and with a variety of other tasks.

### ⏩ To upload a PID configuration file

1. In the *PID* section, select **Expert configuration**.
2. In the *Upload* section, click **Choose file** (or **Browse**).
3. Browse and select the file, and then click **Open**.
4. Click **Add**.

   The file can now be selected on the configuration file list.

### ⏩ To remove a PID configuration file

1. In the *Upload* section, (under *Filename*) select the file that you wish to remove.
2. Click **Del**.
3. Click **Save**.

### ⏩ To download the active PID configuration to your PC

- In *Expect configuration*, click **Export**.

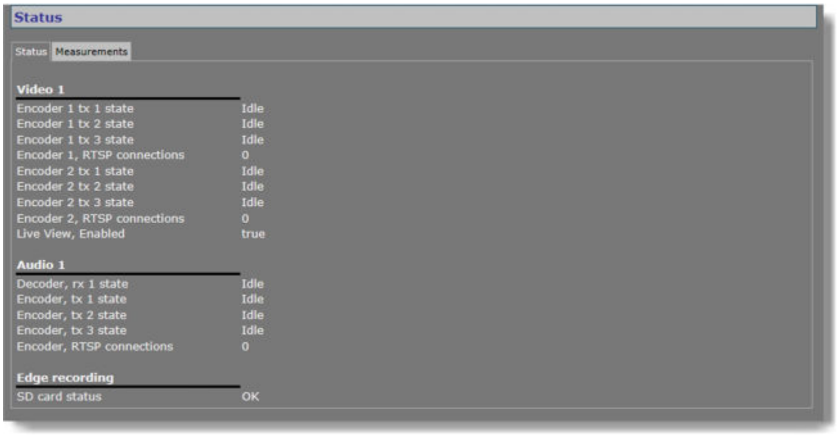
  The file is exported to your download folder.

# 10 Status

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

## In This Chapter

## 10.1 View status information



**Video 1**

| | |
|---|---|
| Encoder 1 tx 1 state | Idle |
| Encoder 1 tx 2 state | Idle |
| Encoder 1 tx 3 state | Idle |
| Encoder 1, RTSP connections | 0 |
| Encoder 2 tx 1 state | Idle |
| Encoder 2 tx 2 state | Idle |
| Encoder 2 tx 3 state | Idle |
| Encoder 2, RTSP connections | 0 |
| Live View, Enabled | true |

**Audio 1**

| | |
|---|---|
| Decoder, rx 1 state | Idle |
| Encoder, tx 1 state | Idle |
| Encoder, tx 2 state | Idle |
| Encoder, tx 3 state | Idle |
| Encoder, RTSP connections | 0 |

**Edge recording**

| | |
|---|---|
| SD card status | OK |

*Status page: a snapshot with automatic page updating*

### 10.1.1 Stream states

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

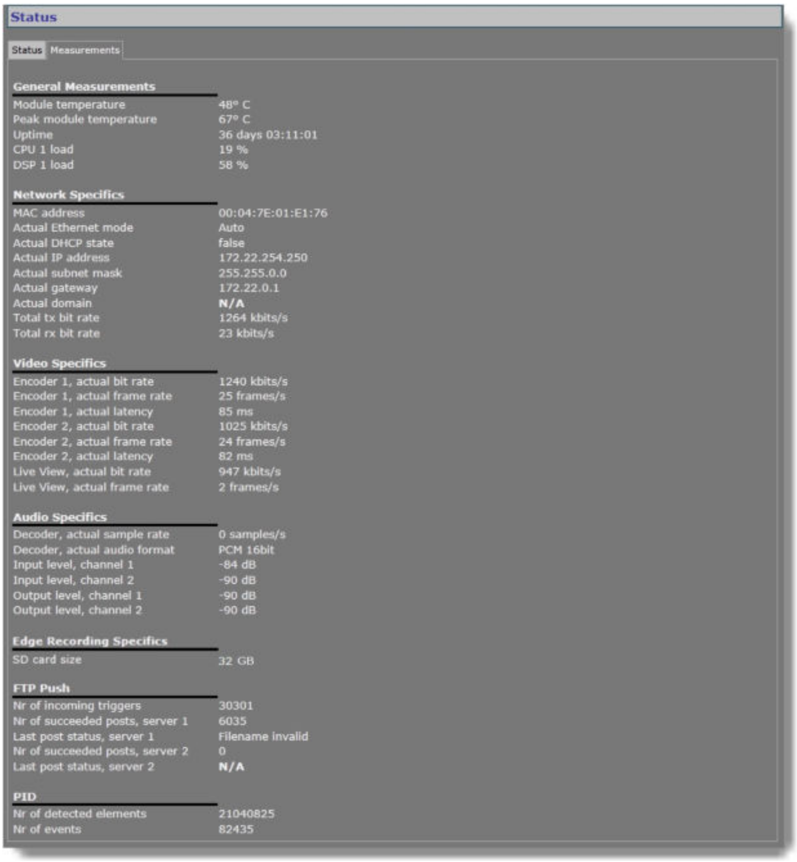
| Stream state | Description |
|---|---|
| OK | There is nothing wrong with the stream. Note that if the video signal is removed from the video input on the encoder side, the Decoder rx state is still reported as *OK*, since the video transmitter is sending a stream - that is, a *No Video* image - to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

### 10.1.2 Edge recording

The Edge recording section shows whether an SD card is present and if it can be accessed.

| Item | Description | |
|---|---|---|
| SD card status | *OK* | SD card present and functioning. |
| | *Error* | Unable to access SD card. Possible damage to card, connectors, or slot. |
| | *Not present* | No SD card detected. |

## 10.2 View measurements data



Status

**General Measurements**

| | |
|---|---|
| Module temperature | 48° C |
| Peak module temperature | 67° C |
| Uptime | 36 days 03:11:01 |
| CPU 1 load | 19 % |
| DSP 1 load | 58 % |

**Network Specifics**

| | |
|---|---|
| MAC address | 00:04:7E:01:E1:76 |
| Actual Ethernet mode | Auto |
| Actual DHCP state | false |
| Actual IP address | 172.22.254.250 |
| Actual subnet mask | 255.255.0.0 |
| Actual gateway | 172.22.0.1 |
| Actual domain | **N/A** |
| Total tx bit rate | 1264 kbits/s |
| Total rx bit rate | 23 kbits/s |

**Video Specifics**

| | |
|---|---|
| Encoder 1, actual bit rate | 1240 kbits/s |
| Encoder 1, actual frame rate | 25 frames/s |
| Encoder 1, actual latency | 85 ms |
| Encoder 2, actual bit rate | 1025 kbits/s |
| Encoder 2, actual frame rate | 24 frames/s |
| Encoder 2, actual latency | 82 ms |
| Live View, actual bit rate | 947 kbits/s |
| Live View, actual frame rate | 2 frames/s |

**Audio Specifics**

| | |
|---|---|
| Decoder, actual sample rate | 0 samples/s |
| Decoder, actual audio format | PCM 16bit |
| Input level, channel 1 | -84 dB |
| Input level, channel 2 | -90 dB |
| Output level, channel 1 | -90 dB |
| Output level, channel 2 | -90 dB |

**Edge Recording Specifics**

| | |
|---|---|
| SD card size | 32 GB |

**FTP Push**

| | |
|---|---|
| Nr of incoming triggers | 30301 |
| Nr of succeeded posts, server 1 | 6035 |
| Last post status, server 1 | Filename invalid |
| Nr of succeeded posts, server 2 | 0 |
| Last post status, server 2 | **N/A** |

**PID**

| | |
|---|---|
| Nr of detected elements | 21040825 |
| Nr of events | 82435 |

*Status page: a snapshot with automatic page updating*

### 10.2.1 General, network, and stream measurements

The Measurements tab shows general measurements, such as the module temperatures (current and peak) and the module uptime.

You also find network specifics here, such as the MAC address, the actual IP address, the network load from this module, the load information per processor, and signal stream-specific details.

### 10.2.2 SD card size

Note that the storage capacity available for edge recording is limited to 75% of the actual SD card size given under Edge Recording Specifics - that is, for example, 24 GB of a 32 GB SD card. This limit is to prevent slow read/write speeds.

### 10.2.3 FTP Push

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

### 10.2.4 PID

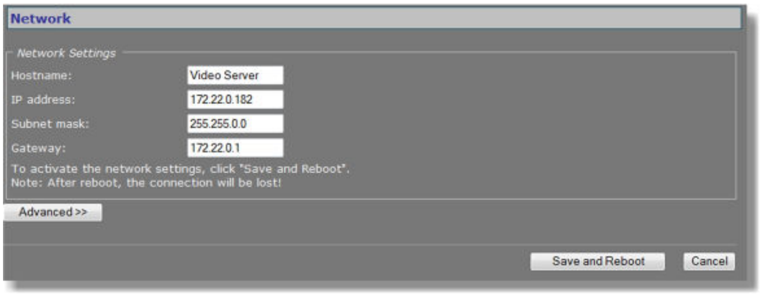
The PID section shows counts of PID events and detected elements.

# 11 Network

On the Network page, you can change the network settings of the TC620. In this chapter, you learn how to set a valid, fixed IP address and, alternatively, how to have an IP address automatically assigned by a DHCP server.

### In This Chapter

## 11.1 Network settings



Network

*Network Settings*

Hostname: Video Server

IP address: 172.22.0.182

Subnet mask: 255.255.0.0

Gateway: 172.22.0.1

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

*Network page*

On the Network page, you can set the name of the unit, the IP address, the subnet mask, and the gateway IP address. For correct functioning of the TC620, 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 TC620. Once you have made the webpages accessible in this way, you can use the Network page to change the default network settings to the desired settings.

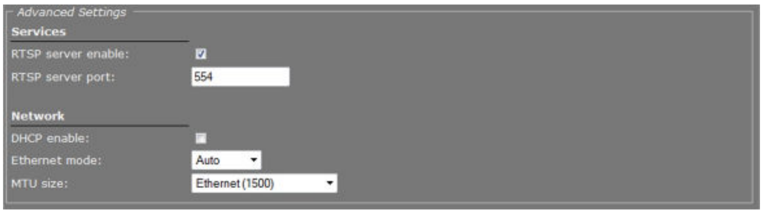
For IP address input to be valid, the unit's IP address:

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

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

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

# 11.2 Advanced



Advanced Settings

**Services**

RTSP server enable: ☑

RTSP server port: 554

**Network**

DHCP enable: □

Ethernet mode: Auto

MTU size: Ethernet (1500)

*Network > Advanced*

## 11.2.1 Services

| Item | Description |
|---|---|
| RTSP server enable | Select this check box to enable the TC620 to act as a server in RTSP media sessions. |
| RTSP server port | This is the port number used to contact the RTSP server. The default transport layer port number for the RTSP protocol is 554 for both UDP and TCP transports. |

## 11.2.2 Network

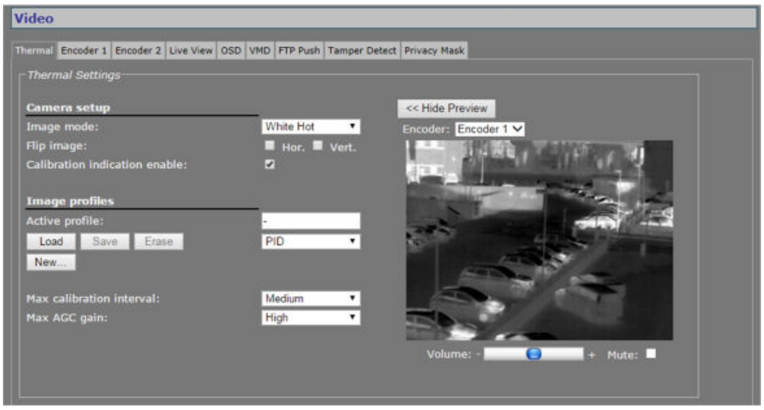
| Item | Description | |
|---|---|---|
| DHCP enable | Allows assigning of the IP address by a DHCP server instead of using static IP addressing. | |
| Ethernet mode | Transmission mode and speed. | |
| | *Auto* | Autonegotiation (default). |
| | *10 HDX* | Half duplex, 10 Mbit. |
| | *10 FDX* | Full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

# 12 Video

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

## In This Chapter

## 12.1 Thermal



Camera setup

Image mode: White Hot

Flip image: □ Hor. □ Vert.

Calibration indication enable: ☑

Image profiles

Active profile: -

PID

Max calibration interval: Medium

Max AGC gain: High

Encoder: Encoder 1

Mute: □

*Video > Thermal*

On the Thermal tab, you can configure the thermal settings of the TC620. Any changes you make are immediately applied. Click **Show Preview>>** to open the camera preview and see the effect of your changes.

## 12.1.1 Camera setup

| Item | Description | |
|---|---|---|
| Image mode | Thermal images can be viewed as white hot or black hot. Select the mode that gives the best viewing results, depending on the time of day, weather conditions, and ambient temperature. | |
| | *White Hot* | Warmer objects are displayed in white or light shades. Black or dark shades indicate colder objects. |
| | *Black Hot* | Warmer objects are displayed in black or dark shades. White or light shades indicate colder objects. |
| Flip image | *Hor.* | Rotates the image around a vertical axis through the centre of the image (left becomes right, and vice versa). See pictures below. |
| | *Vert.* | Rotates the image around a horizontal axis through the centre of the image (top becomes bottom, and vice versa). See pictures below. |
| Calibration indication enable | When the sensor inside the TC620 is being calibrated, an indication can be shown as an overlay on top of the video. Select/clear this textbox to have the indication displayed/hidden, respectively. | |

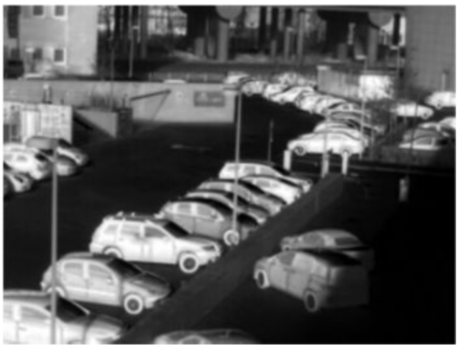


*Image mode: White Hot*

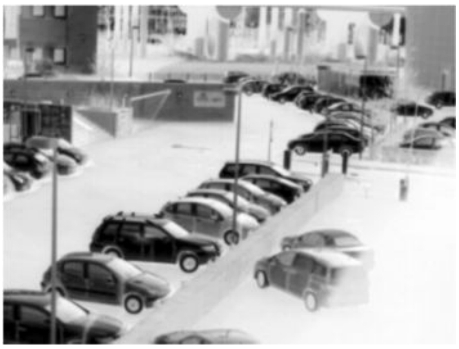
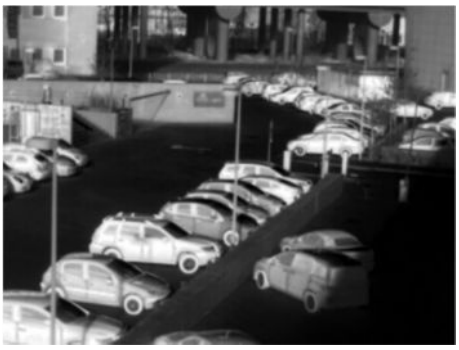


*Image mode: Black Hot*



*No image rotation*

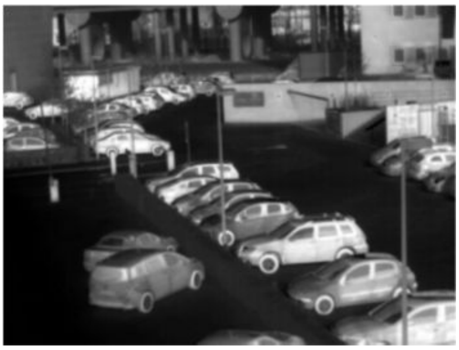


*Image rotation: Flip horizontal*

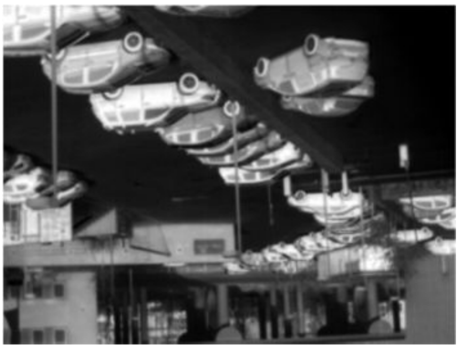


*Image rotation: Flip vertical*

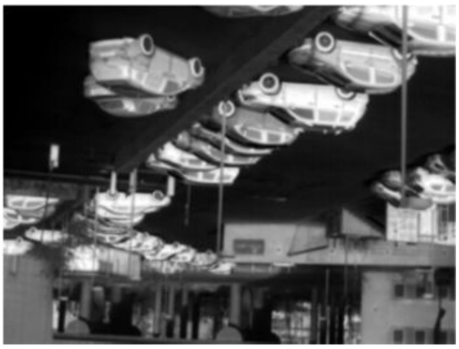


*Image rotation: Flip horizontal and vertical*

## 12.1.2 Image settings

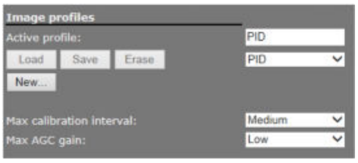


Image profiles

Active profile: PID

PID

Max calibration interval: Medium

Max AGC gain: Low

*Video > Thermal > Image profiles*

### Calibration

The sensor inside the TC620 detects differences in temperature. To compensate for temperature drift and to maintain reliable detection, it must be calibrated at regular intervals. The image freezes for a second during calibration. Using the options in the *Max calibration interval* list, you can control the calibration interval duration to meet the ambient conditions.

### Max AGC gain

The presets in the *Max AGC gain* list can be used to optimise the signal level and brighten video images to compensate for low-contrast conditions. Note, however, that setting the level to *High* can introduce noise into the picture.

## Image profiles

Combinations of image settings can be created and saved as Image profiles, for later use. By default, the TC620 is supplied with the PID image profile. In this profile, *Max calibration interval* is set to *Medium*, and *Max AGC gain* is set to *Low*. When a profile has been selected, changing one of its defined parameters sets the Profile box to "-".

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

### ⏩ To create a custom image profile

1 On the **Video** page, click the **Thermal** tab.

When creating a custom profile, it is possible to use an existing profile as a basis.

2 In the *Image profiles* section, click to open the profile list.

3 Select the profile that comes closest to the profile that you want to create.

4 Click **New**.

5 Enter a name for the new profile, and then click **OK**.

6 Select the required levels in the *Max calibration interval* and *Max AGC gain* lists.

7 Click **Save**.

### ⏩ To load an image profile

1 On the **Video** page, click the **Thermal** tab.

2 In the *Image profiles* section, click to open the profile list.

3 Select the profile, and then click **Load**.

The profile displays in the Active profile box and the camera adopts the new settings.

### ⏩ To erase an image profile

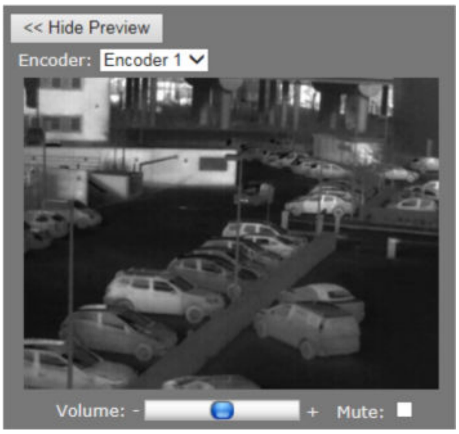
1 On the **Video** page, click the **Thermal** tab.

2 In the *Image profiles* section, click to open the profile list.

3 Select the profile, and then click **Erase**.

The profile is removed from the profile list.

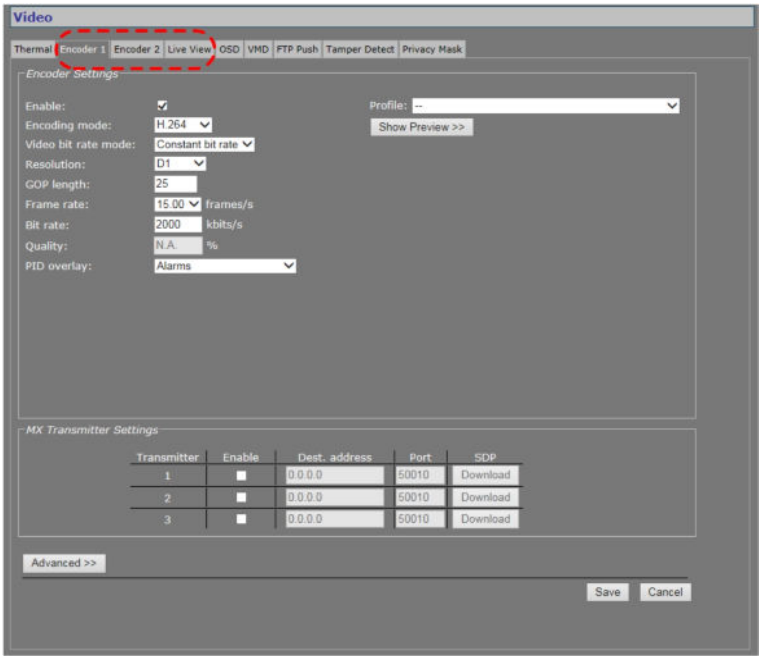
## 12.1.3 Preview



*Video > Thermal > Preview*

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

# 12.2 Video encoding overview



*Encoder Settings*

| | |
|---|---|
| Enable: | ☑ |
| Encoding mode: | H.264 |
| Video bit rate mode: | Constant bit rate |
| Resolution: | D1 |
| GOP length: | 25 |
| Frame rate: | 15.00 frames/s |
| Bit rate: | 2000 kbits/s |
| Quality: | N.A. % |
| PID overlay: | Alarms |
| Profile: | -- |

*MX Transmitter Settings*

| Transmitter | Enable | Dest. address | Port | SDP |
|---|---|---|---|---|
| 1 | □ | 0.0.0.0 | 50010 | Download |
| 2 | □ | 0.0.0.0 | 50010 | Download |
| 3 | □ | 0.0.0.0 | 50010 | Download |

*Encoder tabs on Video page*

### Video encoding

The TC620 features a built-in video server. Two video encoders can simultaneously generate independent digital video streams with different resolutions and frame rates. Encoders 1 and 2 can each convert the video signal into H.264 or MJPEG format.

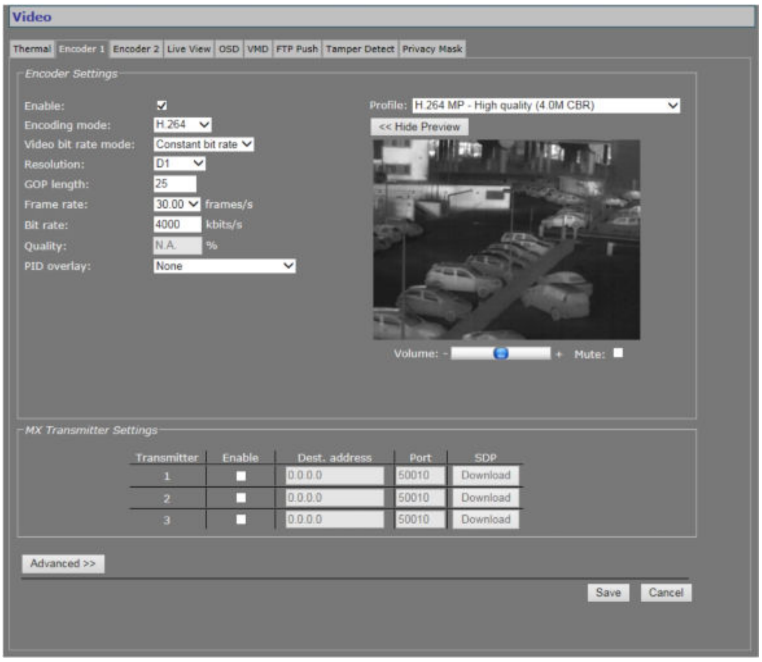
### Multistreaming

Up to twenty streams can be retrieved using RTSP. A total of six copies – three per independent encoder – can be transmitted to different unicast and/or multicast destinations using TKH Security's proprietary MX protocol. The TC620 supports source-specific multicast (SSM). H.264 and audio streams can also be transmitted to multicast destinations using the Session Announcement Protocol (SAP).

### Live View encoder

The Live View encoder can convert the analogue video input signal to (M)JPEG format for streaming to web applications or remote devices using the HTTP protocol. Via FTP Push, JPEG images can also be posted on an FTP server.

## 12.3 Encoder 1



*Encoder Settings*

Enable: ☑
Encoding mode: H.264
Video bit rate mode: Constant bit rate
Resolution: D1
GOP length: 25
Frame rate: 30.00 frames/s
Bit rate: 4000 kbits/s
Quality: N.A. %
PID overlay: None
Profile: H.264 MP - High quality (4.0M CBR)
Mute: □

*MX Transmitter Settings*

| Transmitter | Enable | Dest. address | Port | SDP |
|---|---|---|---|---|
| 1 | □ | 0.0.0.0 | 50010 | Download |
| 2 | □ | 0.0.0.0 | 50010 | Download |
| 3 | □ | 0.0.0.0 | 50010 | Download |

*Video > Encoder 1*

## 12.3.1 Encoder Settings

| Item | Description | |
|---|---|---|
| Enable | All encoders are enabled by default. Use this check box to disable/re-enable this specific encoder. | |
| Encoding mode | *H.264 or MJPEG* | The method used to compress the video signal. |
| | TC620 can stream (M)JPEG over UDP and HTTP.<br>● To enable and configure **UDP**/MJPEG streaming, select MJPEG from the Encoding mode list and configure settings.<br>● To transport JPEG over **HTTP** and/or use the Live View previews in the web pages, go to the Live View tab, enable the Live View encoder, and configure its settings. | |
| Video bit rate mode | Controls variations in bit rates. | |
| | *Constant quality* | Keeps the image quality constant, with varying network load. See *Constant Quality Mode (CQM) configuration* (below) for TKH Security's recommended strategy for controlling image quality. |
| | *Constant bit rate* | Keeps network load constant at the cost of varying image quality. Frames may be skipped. |

**Note:** The TC620 will simultaneously handle dual H.264/MJPEG encoding at full frame rate, and Live View encoding at 5 frames per second. The total output bandwidth, including streams controlled by RTSP, and those enabled through SAP, should not exceed 25 Mb/s.

| Item | Description | |
|---|---|---|
| GOP length | Distance in frames between two I-frames. | |
| Frame rate | Range depends on selected front end: 1-7.5 fps (-S models) or 1-30 fps (-F models). | |
| Bit rate | Constant bit rate mode only | The speed of the digital transmission - that is, the amount of information transferred/processed per unit of time. |
| Actual bit rate | Constant quality mode only | This field is dynamically updated with the current bit rate to provide feedback on the bit rate that is used on average with the current *Quality* setting. |
| Quality | Constant quality mode only | Reflects the amount of compression. Generally speaking: the higher the quality setting, the lower the compression ratio and the more bits are consumed. This means a trade-off has to be found between the desired quality level and available bandwidth. |
| PID Overlay | PID alarms and PID configuration can be shown as overlays over the camera image in the preview. | |
| Profile | Preset combinations of settings for specific purposes. When a profile has been selected, changing one of its defined parameters sets the Profile box to '--', to indicate that a custom profile has been configured. When a freely chosen parameter value combination matches a preset profile, the name of the profile shows in the Profile box. | |
| Show Preview>> | Click to view live images and see the effect of the current settings. | |
| <<Hide Preview | Closes the preview. This may improve webpage responsiveness. | |

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

## 12.3.2 Parameter value combinations

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

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

## 12.3.3 Constant Quality Mode configuration

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

### ⏩ To configure CQM settings

1. In *Encoder Settings*, open the **Video bit rate mode** list, and then select **Constant quality**.
2. With the video source connected and the encoder enabled, go to the *Quality* field and set the desired quality (range: [0 ... 100%]), aided by the visual feedback in the Preview.
3. Press **Save** to store your settings.

   The Actual bit rate field is dynamically updated with the current bit rate.
4. Determine if the average bit rate used with the current *Quality* setting is acceptable. If not, modify the *Quality* setting.
5. To set the upper limit for the bit rate, open the **Advanced Settings** section and use the *CQM max bit rate* field to specify the maximum bit rate.

   Generally, it is not necessary to change the default setting of 6000 kbit/s, unless there are physical limitations on the network.
6. Press **Save** to store your settings.

## 12.3.4 Make a video connection

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

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

### ⏩ To configure the encoder settings

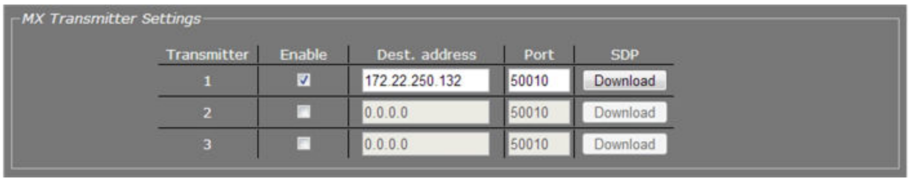
1. Open the webpages of the encoder, go to the Video page, and then open the appropriate Encoder tab.
2. In the MX Transmitter Settings section, specify the destination IP address.

This is the address of the video decoder which will receive the video stream.

3 Enter the port number of the decoder.

For more information about port numbers, see the *Port Numbers* section.

4 Select **Enable**, and then click **Save**.



MX Transmitter Settings

| Transmitter | Enable | Dest. address | Port | SDP |
|---|---|---|---|---|
| 1 | ☑ | 172.22.250.132 | 50010 | Download |
| 2 | □ | 0.0.0.0 | 50010 | Download |
| 3 | □ | 0.0.0.0 | 50010 | Download |

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

### ⏩ To configure the decoder settings

1 Open the webpages of the decoder, go to the Video page, and select the Decoder tab.

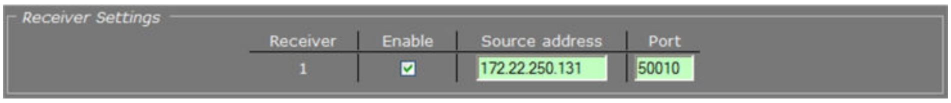
2 In the MX Receiver Settings section, specify the source IP address.

This is the address of the video encoder which will transmit the video stream.

3 Enter the port number of the decoder.

For more information on port numbers, see the *Port Numbers* section.

4 Select **Enable**, and then click **Save**.



Receiver Settings

| Receiver | Enable | Source address | Port |
|---|---|---|---|
| 1 | ☑ | 172.22.250.131 | 50010 |

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

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

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

## Highlighted fields

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

## SDP download

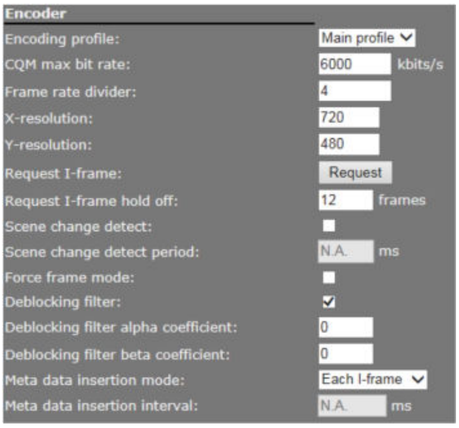
Use the SDP Download button to download a Session Description Protocol (SDP) file from the encoder. SDP files contain streaming media initialisation parameters and properties. An SDP file does not deliver media itself but through file association the media stream can be opened in media players such as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

## 12.3.5 Advanced

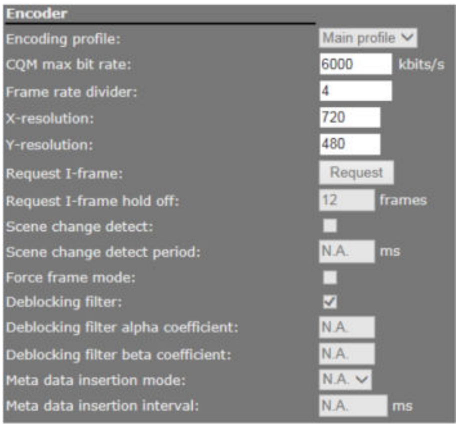
**Important:** If in doubt about these settings, do *not* change the default values.

### 12.3.5.1 Encoder

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



| Encoder | | |
|---|---|---|
| Encoding profile: | Main profile | |
| CQM max bit rate: | 6000 | kbits/s |
| Frame rate divider: | 4 | |
| X-resolution: | 720 | |
| Y-resolution: | 480 | |
| Request I-frame: | Request | |
| Request I-frame hold off: | 12 | frames |
| Scene change detect: | ☐ | |
| Scene change detect period: | N.A. | ms |
| Force frame mode: | ☐ | |
| Deblocking filter: | ☑ | |
| Deblocking filter alpha coefficient: | 0 | |
| Deblocking filter beta coefficient: | 0 | |
| Meta data insertion mode: | Each I-frame | |
| Meta data insertion interval: | N.A. | ms |



| Encoder | | |
|---|---|---|
| Encoding profile: | Main profile | |
| CQM max bit rate: | 6000 | kbits/s |
| Frame rate divider: | 4 | |
| X-resolution: | 720 | |
| Y-resolution: | 480 | |
| Request I-frame: | Request | |
| Request I-frame hold off: | 12 | frames |
| Scene change detect: | ☐ | |
| Scene change detect period: | N.A. | ms |
| Force frame mode: | ☐ | |
| Deblocking filter: | ☑ | |
| Deblocking filter alpha coefficient: | N.A. | |
| Deblocking filter beta coefficient: | N.A. | |
| Meta data insertion mode: | N.A. | |
| Meta data insertion interval: | N.A. | ms |

*H.264 encoding, Constant Quality Mode*

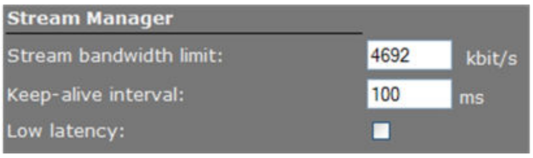
*MJPEG encoding, Constant Quality Mode*

*Video > Encoder 1/2 > Advanced Settings > Encoder*

| Item | Description | |
|---|---|---|
| Encoding profile | *Main profile* | Compatibility mode for decoders which do not support High profile. |
| | *High profile* | Improved encoding quality (as compared to Main profile). |
| CQM max bit rate | Available in *Constant quality* mode (CQM). Use this setting to set the maximum bit rate for a given picture quality configured in the Encoder Settings section. | |
| Frame rate divider | Relates to the frame rate configured in the Encoder Settings section. Recommended setting: 1 (-F models) or 4 (-S models). | |
| X-resolution | Variables that enable you to freely set picture resolution instead of using the resolution presets in the Encoder Settings section. | |
| Y-resolution | | |
| Request I-frame | When joining a multicast stream in the middle of a long GOP, requesting an I-frame will speed up response time, i.e. image display will start sooner. | |
| Request I-frame hold off | Range: [0…255] frames. Requesting (too) many I-frames may add to latency. To prevent this, you can specify the distance in frames, starting after the previous I-frame, before another I-frame is sent upon request. | |
| Scene change detect | Enables the scene detection algorithm. If enabled, the encoder can fully restart a new GOP with an I-slice and an instantaneous decoding refresh (IDR) picture, depending on image content. | |
| Scene change detect period | Sets the minimum time between scene changes in milliseconds. This is a hold-off mechanism that prevents a scene change for the specified time, starting from the previous scene change. | |
| Force frame mode | If Force frame mode is enabled on <ManufacturerNames> video encoders, the H.264 video stream is compressed and sent using entire frames (Frame mode). If disabled, the stream is compressed and sent using entire frames or the separate fields (Field mode). Note, however, that the TC620 operates with frame mode only. There is no need to select or clear this check box, therefore. | |
| Deblocking filter | Enables the in-loop deblocking filter in the AVC encoder. H.264 encoding can handle portions of the video image in blocks of varying sizes which can be processed independently. The deblocking filter enhances image quality by smoothing block edges and reducing blocking distortion. Be aware, however, that applying the filter requires substantial processing power. | |
| Deblocking filter alpha coefficient | Set the alpha/beta coefficients of the deblocking filter. Entering experimental values for these coefficients may help you in achieving optimal image quality. | |
| Deblocking filter beta coefficient | | |
| Meta data insertion mode | Determines the method used to add meta data to the stream. For details, see the section on Meta Data Insertion. | |
| | *Disabled* | No meta data added to the stream. |
| | *Fixed interval* | Activates *Meta data insertion interval* parameter. |
| | *Each I-frame* | Data block is added after each I-frame. The interval is determined by the GOP length, therefore. |

| Item | Description |
|---|---|
| Meta data insertion interval | Range: [100-10000] ms. Sets the (fixed) interval at which meta data is added to the stream. Activate this parameter by setting *Meta data insertion mode* (see above) to *Fixed interval*. |

## 12.3.5.2 Stream Manager



Stream Manager

Stream bandwidth limit: 4692 kbit/s

Keep-alive interval: 100 ms

Low latency: □

*Video > Encoder # > Advanced > Stream Manager*

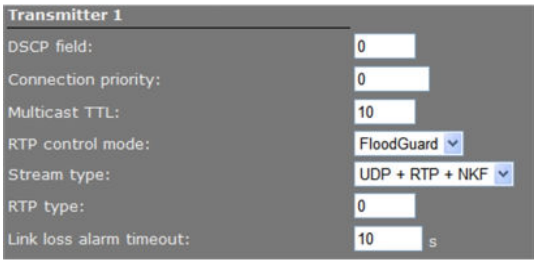
### Balancing network load

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

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

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

## 12.3.5.3 Transmitter #



Transmitter 1

DSCP field: 0

Connection priority: 0

Multicast TTL: 10

RTP control mode: FloodGuard

Stream type: UDP + RTP + NKF

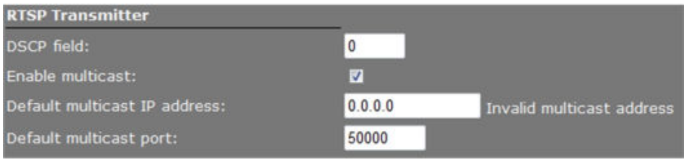
RTP type: 0

Link loss alarm timeout: 10 s

*Video > Encoder # > Advanced > Transmitter 1*

| Item | Description | |
|---|---|---|
| DSCP field | Range: [0...63]. DSCP (Differentiated Services Code Point) uses the first 6 bits of the ToS (Type of Service) field in the header of IP packets for packet classification purposes. The bit pattern in the field indicates the type of service and forwarding behavior at the next node. With 26 bits, up to 64 network service types can be defined. RFC 2724 (see - http://www.ietf.org/rfc/rfc2474.txt) describes the Differentiated Services (DS) field and the DiffServ Code Point. See also the note on Differentiated Services later in this chapter. | |
| Connection priority | Parameter intended for use with MX Software Development Kit. | |
| Multicast TTL | Range: [0...127]. Specify the number of routers (hops) that multicast traffic is permitted to pass through before expiring on the network. | |
| RTP control mode | Select the transport protocol to control the stream. | |
| | *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 | Default value: [0]. This parameter determines the RTP payload format (e.g. H.264, MPEG-2/4, or audio). To avoid an RTP type conflict, the values specified on both sides of the connection must be the same. The default value of "0" automatically sets the appropriate media type. You are advised not to change this setting. | |
| Link loss alarm timeout | Range: [1...1000] s. Default: 10 s. Time in seconds before alarm sent. | |

## 12.3.5.4 RTSP Transmitter



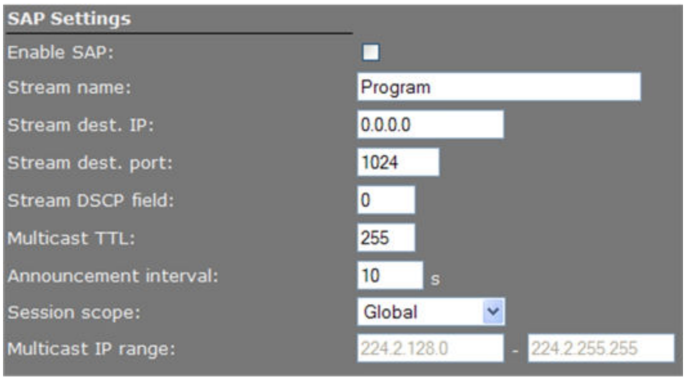
RTSP Transmitter

| | |
|---|---|
| DSCP field: | 0 |
| Enable multicast: | ☑ |
| Default multicast IP address: | 0.0.0.0 Invalid multicast address |
| Default multicast port: | 50000 |

*Video > Encoder # > Advanced > RTSP Transmitter*

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

## 12.3.5.5 SAP Settings



SAP Settings

| | |
|---|---|
| Enable SAP: | □ |
| Stream name: | Program |
| 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 |

*Video > Encoder # > Advanced > SAP Settings*

### SAP announcer

The TC620 includes a SAP announcer. The Session Announcement Protocol is used to advertise that a media stream generated by the TC620 is available at a specific multicast address and port.

The TC620 can send SAP multicast streams generated by its H.264 and audio encoders. The video streams will include audio if audio is enabled on the Audio web page and if the multicast IP range is the same as for video. Note that audio in itself can also be received as a separate stream. For more information about SAP, see the note later in this chapter.

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

### ⏩ To configure SAP settings, do the following

1 In the SAP settings section, select **Enable SAP**.

2 Enter a stream name.

3 In the Session scope list, select **Global** or **Administrative**.

4 If you selected *Administrative* in the previous step, specify the Multicast IP range.

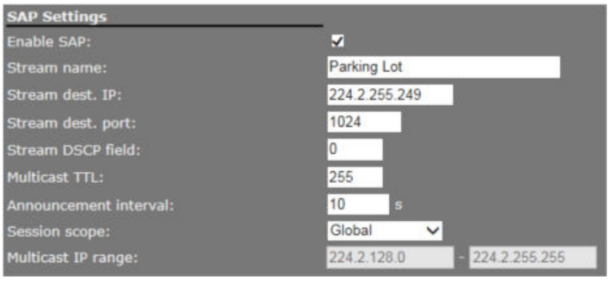
5 Enter the Stream Destination IP address and the port number.

The IP address must be within the scope range displayed for the Multicast IP range parameter.

6 Enter/modify the values for Stream DSCP field, Multicast TTL, and Announcement Interval, if desired.

7 Click **Save**.

The video stream can now be viewed in a media player, such as QuickTime or VLC.



SAP Settings

Enable SAP: ☑

Stream name: Parking Lot

Stream dest. IP: 224.2.255.249

Stream dest. port: 1024

Stream DSCP field: 0

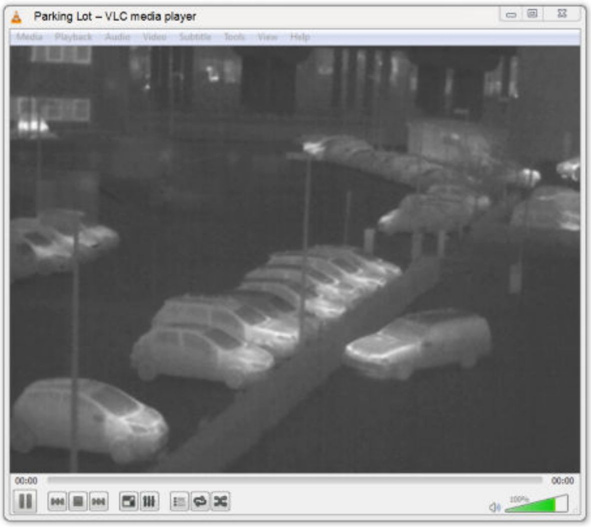
Multicast TTL: 255

Announcement interval: 10 s

Session scope: Global

Multicast IP range: 224.2.128.0 - 224.2.255.255

*SAP example settings*



*TC620 SAP network stream opened via VLC Playlist*

## 12.3.6 Meta data insertion

### Enabling

All TC620 encoders can be configured to include meta data in the video streams they generate. The insertion of meta data is enabled by setting an interval via the Advanced Settings of the encoder. A meta data message is added to the stream as a block of data with a fixed format (see examples below). The messages can contain user data, product info, and status info.

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

### User data message

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

| | | | | |
|---|---|---|---|---|
| 0x00 | 0x00 | 0x01 | 0xB2 | User data message |

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

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

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

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

### Product info message

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

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

### Status info message

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

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 'O' | 'P' | 'T' | 'C' | 0x01 | Status1 | Status2 | Status3 | Status4 |

(future expansion possible)

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

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

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

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

### User defined text message

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

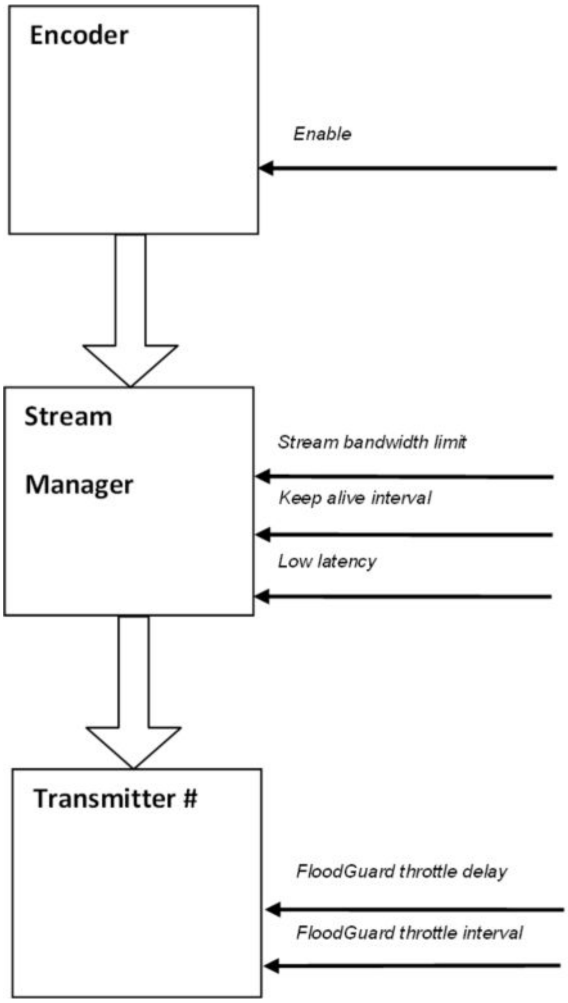
## 12.3.7 Notes

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

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

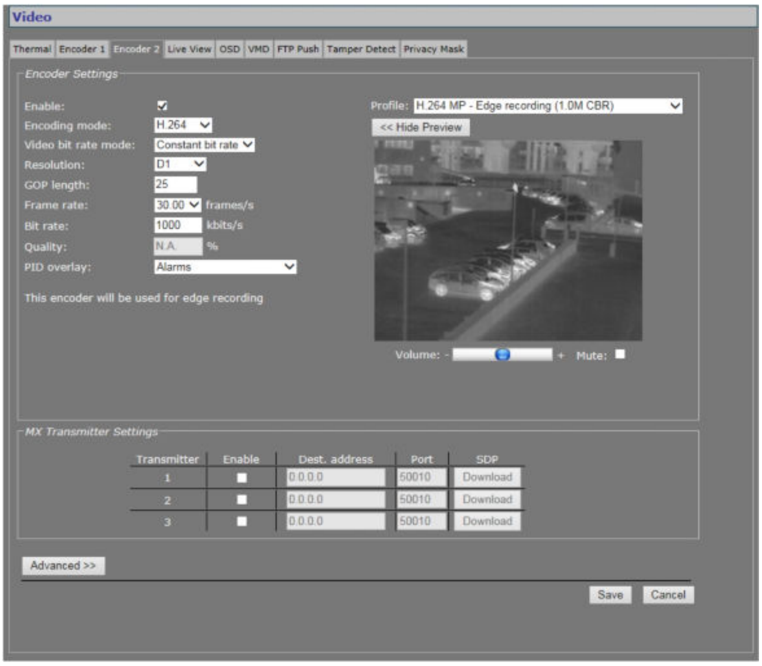
**Note on the Session Announcement Protocol (SAP):** SAP, defined in RFC 2974 (see RFC 2974 - http://www.ietf.org/rfc/rfc2974.txt), is a protocol for advertising multicast session information. A SAP announcer periodically broadcasts announcement packets which include the session description information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

**Note on FloodGuard:** FloodGuard is a TKH Security proprietary stream control mechanism that can be enabled/disabled independently for each video and sampled data transmitter. FloodGuard throttles the transmitter when it no longer receives control messages from the receiver, thereby preventing the transmitter from flooding the network.
*FloodGuard only works when enabled on both the transmitter and the receiver, and when the transmitter sends to a unicast address.*
When a transmitter is enabled, it opens a control receive port with the port number equal to its source port number + 1. This port listens for control packets from the destination receiver. When no FloodGuard packets come in during the time set for the *FloodGuard throttle delay*, the receiver is expected to have disappeared (powered off, receiver disabled, network problem, etc.) and the stream is 'throttled'. In throttled mode the transmitter - in order to contact the intended receiver (again) - sends empty packets into the network at an interval determined by the *FloodGuard throttle interval* parameter. After reception of a valid FloodGuard packet the transmitter immediately resumes streaming.



*Stream Manager and FloodGuard*

# 12.4 Encoder 2



Encoder Settings

Enable: ☑

Encoding mode: H.264

Video bit rate mode: Constant bit rate

Resolution: D1

GOP length: 25

Frame rate: 30.00 frames/s

Bit rate: 1000 kbits/s

Quality: N.A. %

PID overlay: Alarms

This encoder will be used for edge recording

Profile: H.264 MP - Edge recording (1.0M CBR)

Mute: □

MX Transmitter Settings

| Transmitter | Enable | Dest. address | Port | SDP |
|---|---|---|---|---|
| 1 | □ | 0.0.0.0 | 50010 | Download |
| 2 | □ | 0.0.0.0 | 50010 | Download |
| 3 | □ | 0.0.0.0 | 50010 | Download |

*Video > Encoder 2*

## 12.4.1 Edge recording

Configuring Encoder 2 settings is done in the same way as for Encoder 1. It is important to bear in mind, however, that edge recording uses video generated by Encoder 2 and that this requires specific *Video bit rate*, *GOP length*, and *Bit rate* settings.

**Important:** If you change these settings, edge recording may become impossible.

⚠ Current settings prevent edge recording. To fix this, enable the encoder and select the edge recording profile.

*Warning: Incorrect encoder settings for edge recording*

### ⏩ To configure settings for edge recording

1 Select **Enable** to enable the encoder.

2 On the **Profile** list, select **H.264 - Edge recording**.

3 Click **Save**.

This creates the following settings.

- Video bit rate mode: Constant bit rate
- GOP length: 25
- Bit rate: 1000 kbit/s

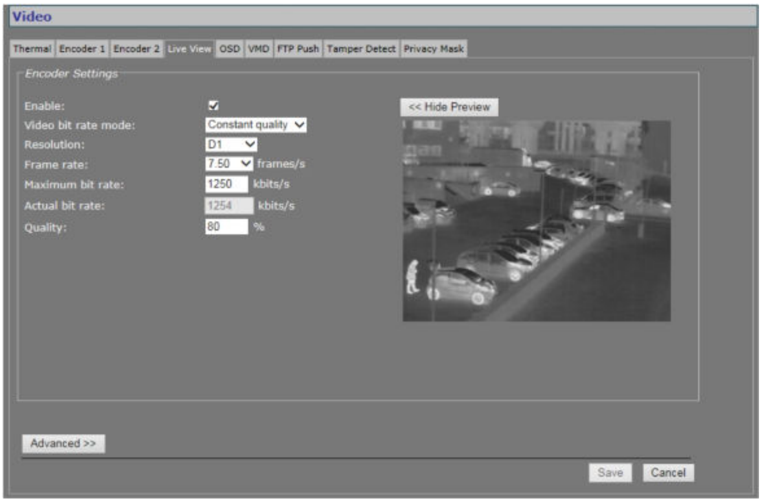
These settings are also the out of the box factory-default settings for Encoder 2. If they are no longer correct just select the *H.264 - Edge recording* profile to restore the proper settings.

### Custom settings

If you need to apply custom settings, you can do so with the following restrictions.

- Video bit rate mode: always set to *Constant bit rate*.
- GOP length: ≥ 25
- Bit rate: ≤ 1000 kbit/s
- Resolution: CIF (recommended)

## 12.5 Live View



Encoder Settings

Enable: ☑

Video bit rate mode: Constant quality

Resolution: D1

Frame rate: 7.50 frames/s

Maximum bit rate: 1250 kbits/s

Actual bit rate: 1254 kbits/s

Quality: 80 %

*Video > Live View*

### 12.5.1 (M)JPEG output

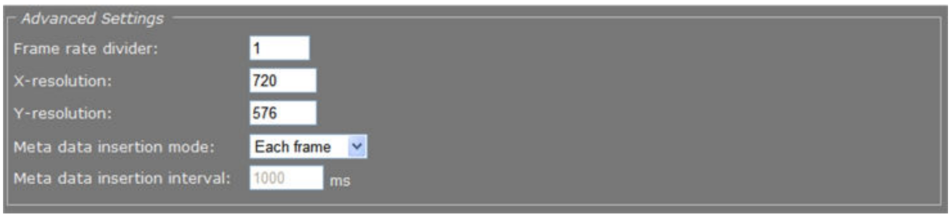
The TC620 provides multiple (M)JPEG output methods.

- To transport JPEG over **HTTP** and/or to use the Live View previews in the webpages, enable the Live View encoder and configure its settings.
- To enable and configure **UDP**/MJPEG streaming, go to the Encoder 1/2 tab, select MJPEG encoding mode and configure settings.
- To activate the uploading of JPEG images to an FTP server, configure the required settings on the FTP Push tab and the Event Management page.

## 12.5.2 Encoder Settings

| Item | Description | |
|---|---|---|
| Enable | All encoders are enabled by default. Use this check box to disable/re-enable this specific encoder. | |
| Video bit rate mode | Controls variations in bit rates. | |
| | *Constant quality* | Keeps the image quality constant, with varying network load. The quality is determined by the value set for the *Quality* parameter (see below). |
| | *Constant bit rate* | Keeps network load constant at the cost of varying image quality. Frames may be skipped. |
| Resolution | Set sensible combinations of mode, resolution, frame rate and (maximum) bit rate. | |
| Frame rate | | |
| (Maximum) bit rate | | |
| Actual bit rate | Constant Quality Mode (CQM) only | This field is dynamically updated with the current bit rate to provide feedback on the bit rate that is used on average with the current *Quality* setting. |
| Quality | Constant Quality Mode (CQM) only | Reflects the amount of compression. Generally speaking: the higher the quality setting, the lower the compression ratio and the more bits are consumed. This means a trade-off has to be found between the desired quality level and available bandwidth. |
| Show Preview>> | Click to view live images and see the effect of the current settings. | |
| <<Hide Preview | Closes the preview. This may improve webpage responsiveness. | |

## 12.5.3 Advanced



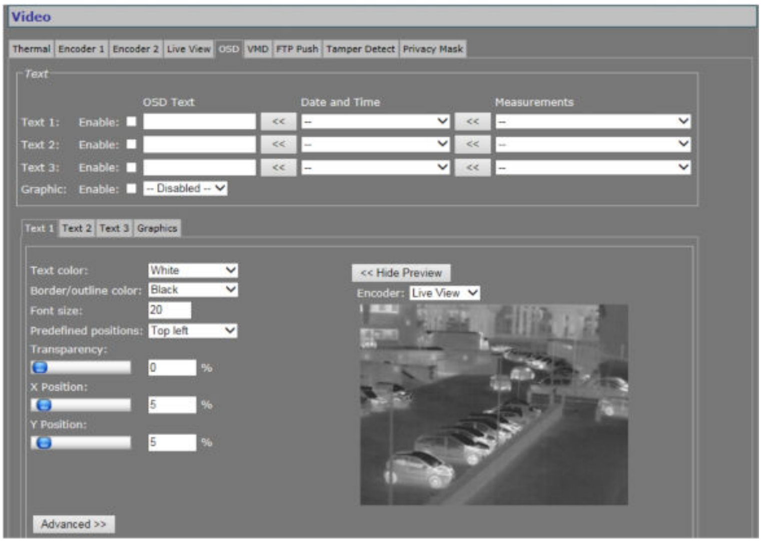
*Advanced Settings*

| | |
|---|---|
| Frame rate divider: | 1 |
| X-resolution: | 720 |
| Y-resolution: | 576 |
| Meta data insertion mode: | Each frame |
| Meta data insertion interval: | 1000 ms |

*Video > Live View > Advanced*

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

# 12.6 OSD



| | | OSD Text | Date and Time | Measurements |
|---|---|---|---|---|
| Text 1: | Enable: □ | | -- | -- |
| Text 2: | Enable: □ | | -- | -- |
| Text 3: | Enable: □ | | -- | -- |
| Graphic: | Enable: □ | -- Disabled -- | | |

Text color: White
Border/outline color: Black
Font size: 20
Predefined positions: Top left
Transparency: 0 %
X Position: 5 %
Y Position: 5 %
Encoder: Live View

*Video > OSD*

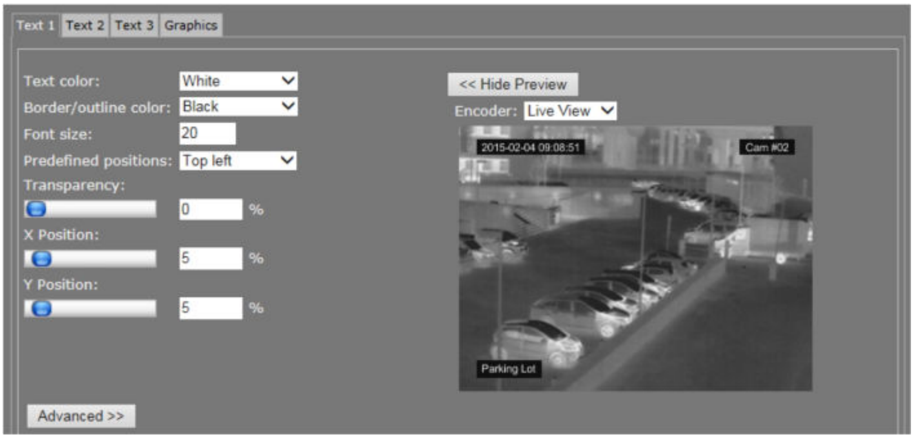
## 12.6.1 OSD facilities

The TC620 features programmable on-screen display (OSD) facilities. One graphic and up to three OSD text bars can be displayed, each of which can be independently configured. Visual feedback is provided in the preview.

## 12.6.2 Text Settings

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

## 12.6.3 Text #

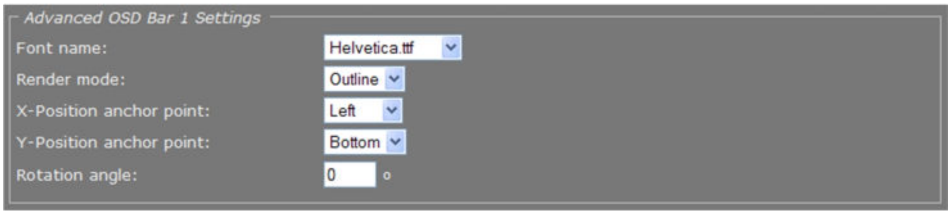


Text color: White
Border/outline color: Black
Font size: 20
Predefined positions: Top left
Transparency: 0 %
X Position: 5 %
Y Position: 5 %
Encoder: Live View

*Video > OSD > Text 1, with three OSD bars in the preview (render modes: Border)*

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

## 12.6.3.1 Advanced

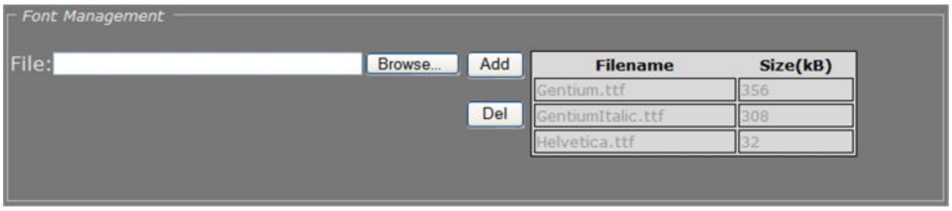


Advanced OSD Bar 1 Settings

| | |
|---|---|
| Font name: | Helvetica.ttf |
| Render mode: | Outline |
| X-Position anchor point: | Left |
| Y-Position anchor point: | Bottom |
| Rotation angle: | 0 ° |

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

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



Font Management

File: Browse... Add

Del

| Filename | Size(kB) |
|---|---|
| Gentium.ttf | 356 |
| GentiumItalic.ttf | 308 |
| Helvetica.ttf | 32 |

*Video > OSD > Text 1 > Advanced > Font Management*

### ⏩ To upload a font

1 In the Font management section, click **Browse**.

The Open dialog box displays.

2 Browse to the folder containing the font to be uploaded.

3 Select the correct file (.ttf extension), and then click **Open**.

The file appears in the File text box on the web page.

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

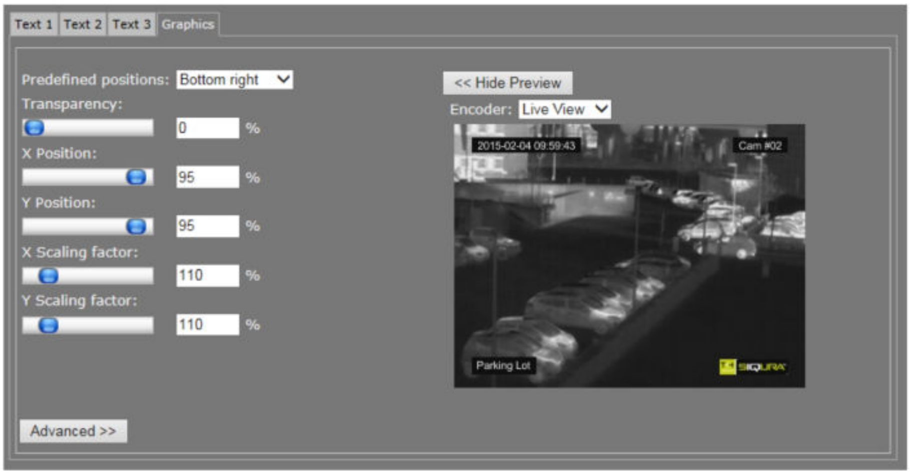
The new font is added to the Font list and to the Font name list in the Advanced OSD Bar # Settings section.

### ⏩ To remove a font

1 In the Font management section, select the font.

2 Click the **Del** button.

## 12.6.4 Graphics



Predefined positions: Bottom right

Transparency: 0 %

X Position: 95 %

Y Position: 95 %

X Scaling factor: 110 %

Y Scaling factor: 110 %

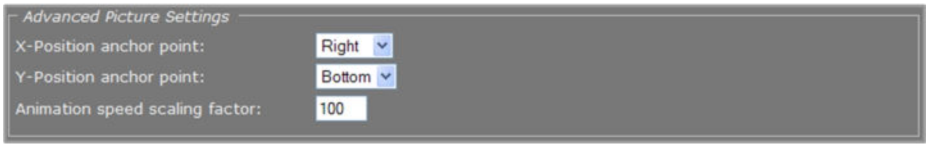
Encoder: Live View

*Video > OSD > Graphics, with three OSD bars and one graphic (bottom right) in the preview*

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

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

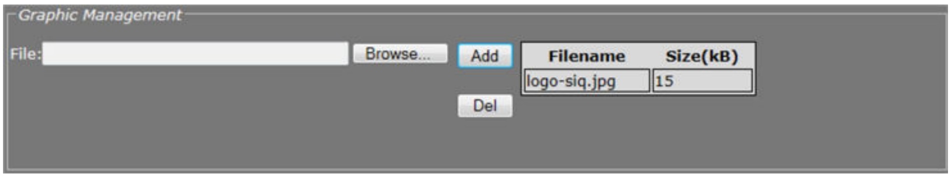
### 12.6.4.1 Advanced



X-Position anchor point: Right
Y-Position anchor point: Bottom
Animation speed scaling factor: 100

*Video > OSD > Graphics > Advanced > Advanced Picture Settings*

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



| Filename | Size(kB) |
|---|---|
| logo-siq.jpg | 15 |

*Video > OSD > Graphics > Advanced > Graphic Management*

You can upload your own graphics with a maximum file size of 100 kB to the TC620. If necessary, use a picture resize tool to reduce the file size.

#### ⏩ To upload a graphic

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

2 Browse to the folder containing the graphic to be uploaded.

3 Select a file with the correct file extension (.bmp, .gif, .jpg, jpeg), and then click **Open**.

The file appears in the *File* textbox.

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

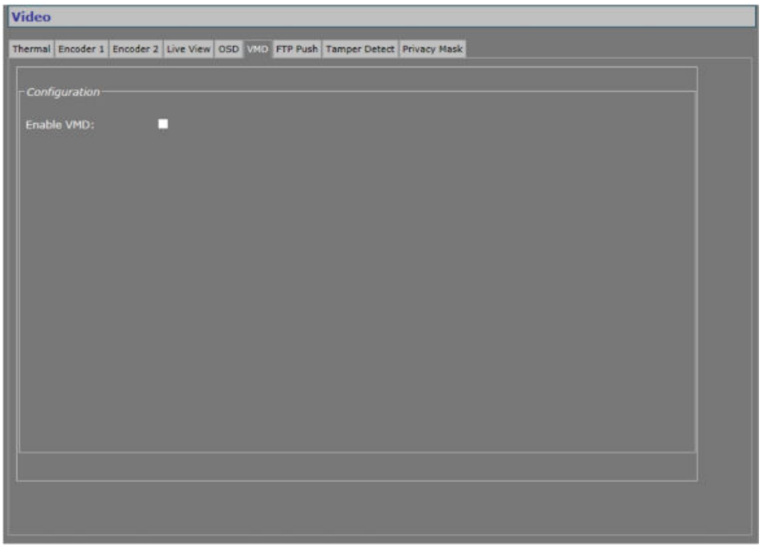
The graphic is added to the graphics list and to the *Graphic* drop-down list in the *Text* section.

### ⏩ To remove a graphic

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

2 Click **Del**.

## 12.7 VMD



Configuration

Enable VMD: □

*Video > VMD*

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

### 12.7.1 VMD startup

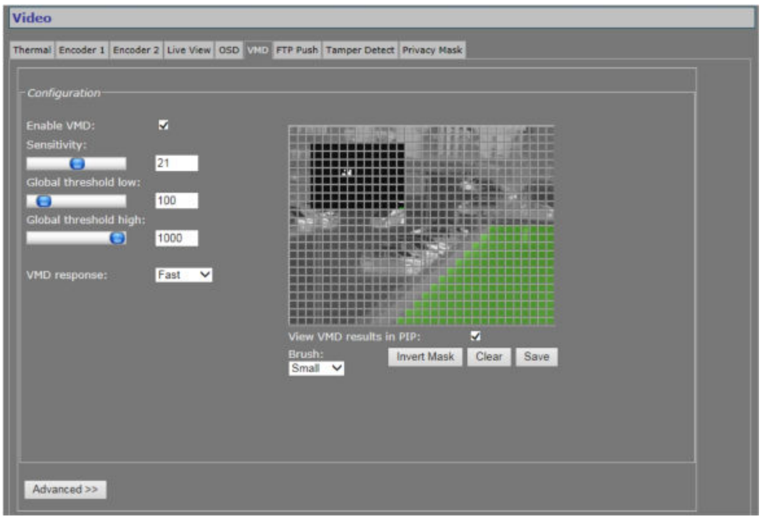
### ⏩ To start Video Motion Detection

1 On the Video page, click the **VMD** tab.

2 Select **Enable VMD** to activate the detection process.

Depending on the current VMD settings, a VMD alarm will be generated on changes in the picture.

## 12.7.2 Configure detection parameters



Enable VMD: ☑
Sensitivity: 21
Global threshold low: 100
Global threshold high: 1000
VMD response: Fast
View VMD results in PIP: ☑
Brush: Small

*Video > VMD > Configuration*

*VMD enabled: Configuration section with controls, video picture, and motion detection inset, the latter with mask applied. The mask permits motion detection in the left and upper areas of the picture.*

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

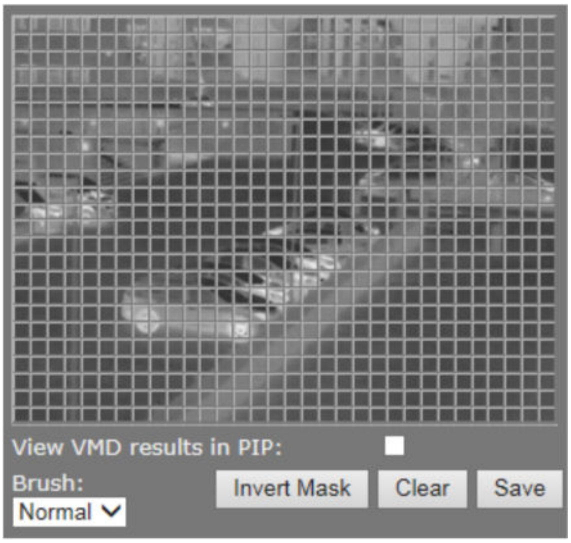
## 12.7.3 Set the mask

### ⏩ To set a mask

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

### ⏩ To delete a mask

- Press the **Clear** button.



View VMD results in PIP: □

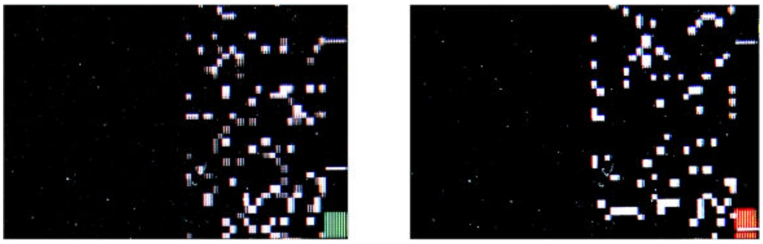
Brush: Normal

*Masking grid*

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

## 12.7.4 VMD detection window

The VMD detection window shows up as a small picture within the larger picture. Depending on the thresholds set, the motion detection bar on the right side of the picture shows up green or red (see figures below), the latter indicating a VMD alarm will be generated. In the pictures, the upper and lower thresholds are shown as two white markers. If the bar runs over the highest marker, it will turn green again and there will be no alarm condition.

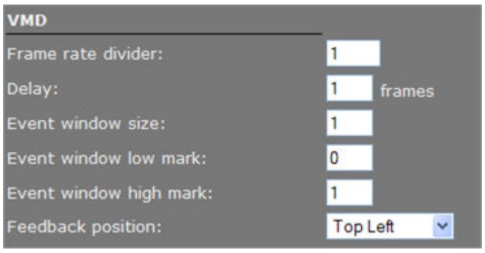


*VMD detection windows, with mask applied to the left half of the window. The small white blocks indicate grid elements where change occurred above the sensitivity level. The summed change is reflected in the bars on the right, the green one (left) not reaching the lower threshold. The red one (right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

## 12.7.5 VMD alarm

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

## 12.7.6 Advanced



**VMD**

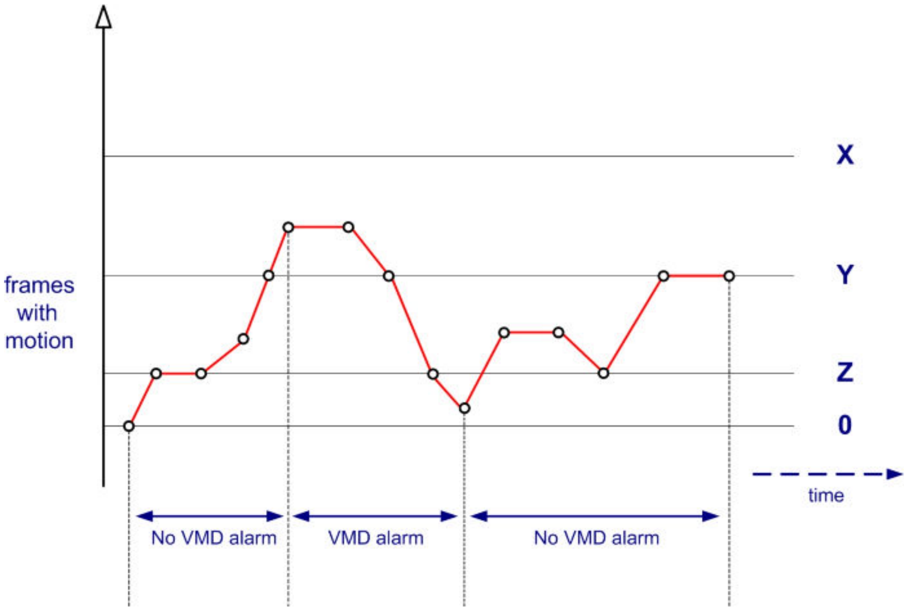
| | |
|---|---|
| Frame rate divider: | 1 |
| Delay: | 1 frames |
| Event window size: | 1 |
| Event window low mark: | 0 |
| Event window high mark: | 1 |
| Feedback position: | Top Left |

*Video > VMD > Advanced > VMD*

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

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

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

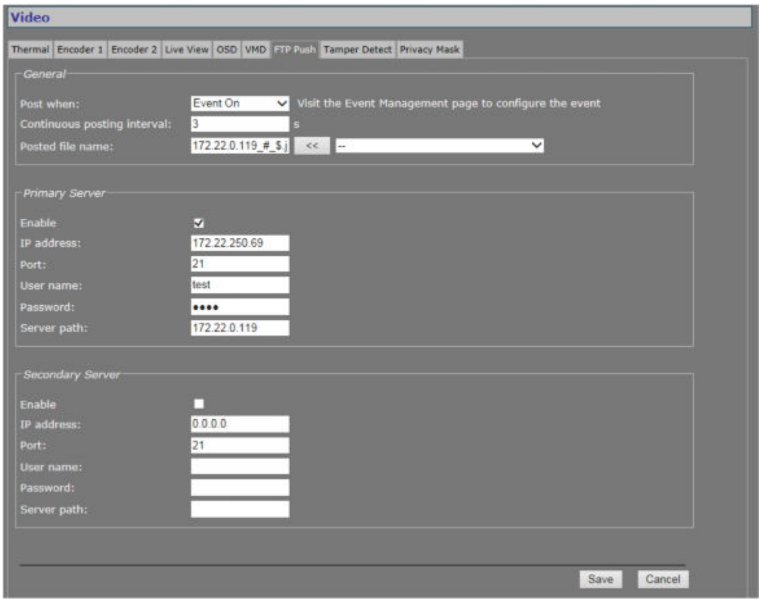


*VMD Alarm: Event window high/low mark*

X = Event window size
Y = Event window high mark
Z = Event window low mark

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

## 12.8 FTP Push



*General*

Post when: Event On — Visit the Event Management page to configure the event
Continuous posting interval: 3 s
Posted file name: 172.22.0.119_#_$.j << --

*Primary Server*

Enable ☑
IP address: 172.22.250.69
Port: 21
User name: test
Password: ••••
Server path: 172.22.0.119

*Secondary Server*

Enable □
IP address: 0.0.0.0
Port: 21
User name:
Password:
Server path:

*Video > FTP Push*

## 12.8.1 Post JPEG images

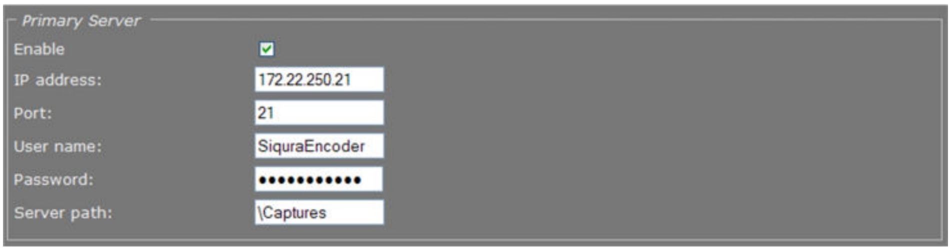
The TC620 can be configured to upload images, generated by its Live View encoder, to an FTP server. Posting the files in JPEG format can be set to be continuous or event-triggered. On the Event Management page, one or more events can be associated with FTP Push.

## 12.8.2 General

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

## 12.8.3 FTP server

A target FTP server must hold a user account associated with the TC620. You can assign a primary server and a secondary server. Images are posted simultaneously to both the primary server and secondary server.



Primary Server

Enable ☑

IP address: 172.22.250.21

Port: 21

User name: SiquraEncoder

Password: ●●●●●●●●●●●

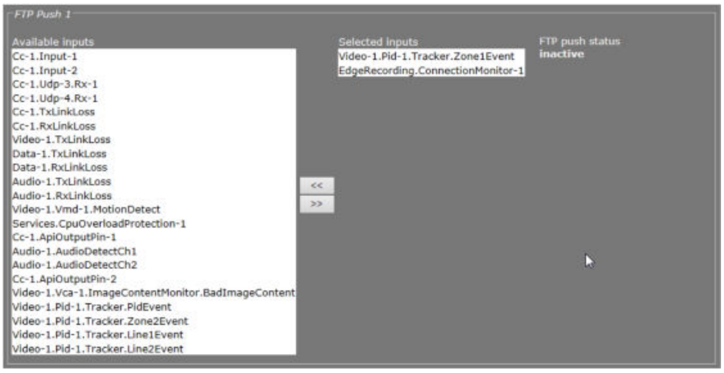
Server path: \Captures

*Video > FTP Push > Primary Server, example settings*

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

## 12.8.4 Event management

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



FTP Push 1

Available inputs

Cc-1.Input-1
Cc-1.Input-2
Cc-1.Udp-3.Rx-1
Cc-1.Udp-4.Rx-1
Cc-1.TxLinkLoss
Cc-1.RxLinkLoss
Video-1.TxLinkLoss
Data-1.TxLinkLoss
Data-1.RxLinkLoss
Audio-1.TxLinkLoss
Audio-1.RxLinkLoss
Video-1.Vmd-1.MotionDetect
Services.CpuOverloadProtection-1
Cc-1.ApiOutputPin-1
Audio-1.AudioDetectCh1
Audio-1.AudioDetectCh2
Cc-1.ApiOutputPin-2
Video-1.Vca-1.ImageContentMonitor.BadImageContent
Video-1.Pid-1.Tracker.PidEvent
Video-1.Pid-1.Tracker.Zone2Event
Video-1.Pid-1.Tracker.Line1Event
Video-1.Pid-1.Tracker.Line2Event

Selected inputs

Video-1.Pid-1.Tracker.Zone1Event
EdgeRecording.ConnectionMonitor-1

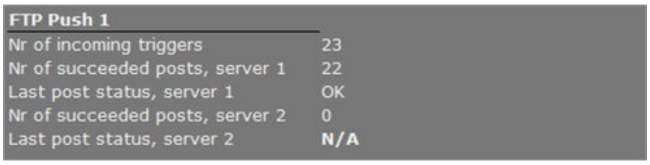
FTP push status

inactive

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

## 12.8.5 Monitor and troubleshoot FTP Push

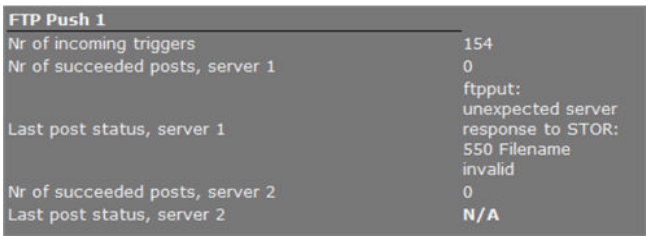
You can monitor FTP push on the Measurements tab of the Status page. Measurements on this tab are continuously updated. In the FTP Push section, you can compare the number of incoming triggers with the number of succeeded posts.



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

*Status > Measurements > FTP Push 1*

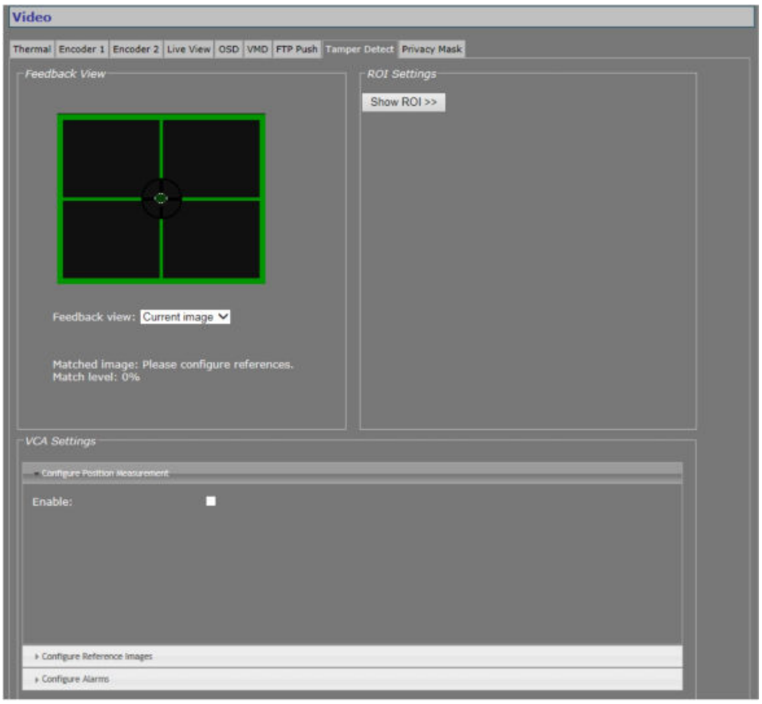
If you need to troubleshoot the file upload process, the messages reporting the last post status will in most cases point you to possible causes of problems.



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

*Last post status: example of error message*

# 12.9 Tamper Detect



Feedback view: Current image

Matched image: Please configure references.
Match level: 0%

Enable: □

*Video > Tamper Detect*

## 12.9.1 Camera movement and scene changes

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

## 12.9.2 Enable Tamper Detect

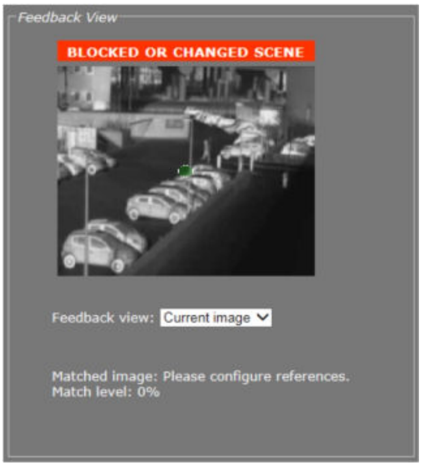
Tamper Detect is disabled by default.

### ⏩ To enable Tamper Detect

- In the *VCA Settings* section, select **Enable**.

  The Position Measurement settings are opened.

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



Feedback view: Current image

Matched image: Please configure references.
Match level: 0%

*Tamper Detect enabled: No reference images found*

## 12.9.3 Reference images

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

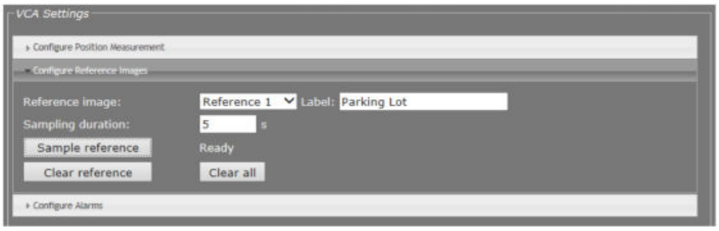
## 12.9.4 Create a reference image

### ⏩ To create a reference image

1. In the *VCA Settings* section, click **Configure Reference Images**.
2. Open the **Reference image** list, and then select the image you want to create.
3. Enter a descriptive name in the *Label* box.
4. Enter a value (in seconds) for the *Sampling duratio*n.

   This parameter enables you to capture the background of a scene only and have specific elements such as moving objects filtered out of the image. With a longer time span for the sampling duration, persons passing in front of the camera, for example, or cars driving on a highway can be smoothed out to prevent them from triggering a changed scene alarm.
5. Click the **Sample reference** button.

   The current image is sampled.

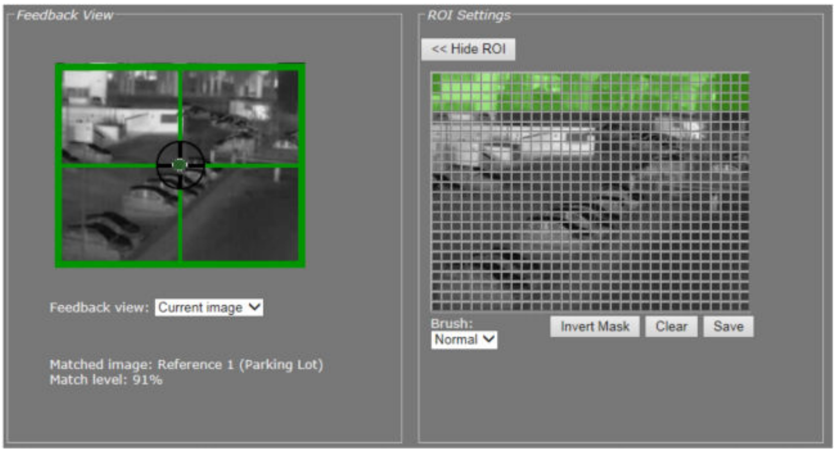


Reference image: Reference 1 Label: Parking Lot
Sampling duration: 5 s
Ready

*Reference image 1 created*

## 12.9.5 Region of Interest (ROI)

You can use the ROI settings section to exclude portions of the image from monitoring.



Feedback view: Current image

Matched image: Reference 1 (Parking Lot)
Match level: 91%

Brush: Normal

*Video > Tamper Detect > ROI Settings. Region of less interest (upper part of image) masked.*

### ROI preview

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

### ⏩ To set a mask

- To edit the mask, click on the grid that is put over the image.

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

### ⏩ To delete a mask

- Press the **Clear** button.

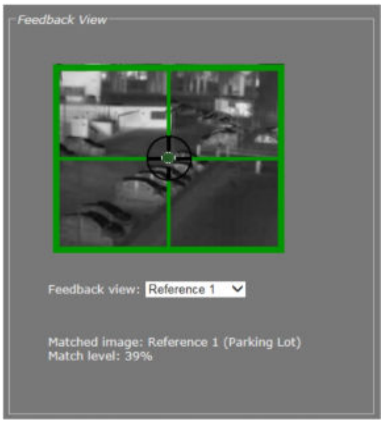
| Item | Description | |
|---|---|---|
| Brush | *Normal* | Allows grid elements to be accessed in 4-element groups. |
| | *Large* | Allows grid elements to be accessed in 16-element groups. |
| | *Small* | Allows grid elements to be accessed one at a time. |
| Invert Mask | Enables you, for example,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

## 12.9.6 Compare images

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

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

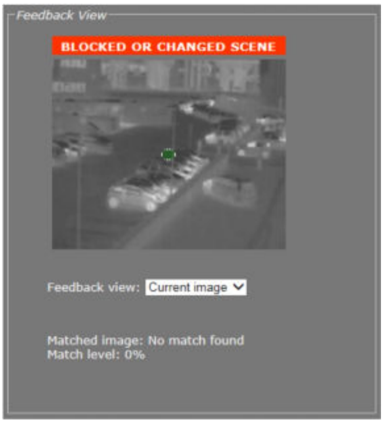
If no match is found a BLOCKED OR CHANGED SCENE alarm is raised.



Feedback view: Reference 1

Matched image: Reference 1 (Parking Lot)
Match level: 39%

*Current image matches Reference 1*

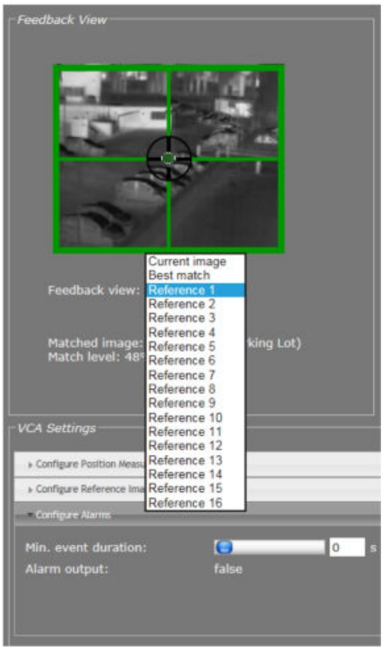


Feedback view: Current image

Matched image: No match found
Match level: 0%

*Reference image(s) available. No match found with current image, though.*

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



Feedback view: Reference 1

Matched image: king Lot)
Match level: 48

Min. event duration: 0 s
Alarm output: false

*Feedback view list*

## 12.9.7 Delete a reference image

### ⏩ To delete a reference image

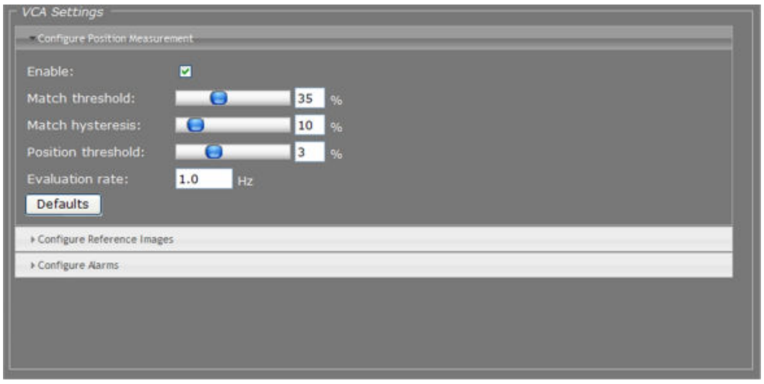
1 In the *VCA Settings* section, open the **Reference image** list.

2 Select the image you wish to delete.

3 Press **Clear reference**.

Note that the *Clear all* button deletes *all* available references.

## 12.9.8 Position measurement



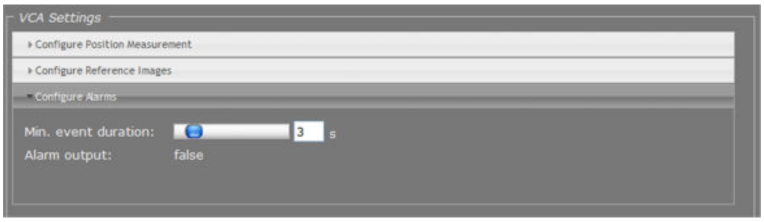
Enable: ☑
Match threshold: 35 %
Match hysteresis: 10 %
Position threshold: 3 %
Evaluation rate: 1.0 Hz

*Video > Tamper Detect > Position Measurement*

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

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

## 12.9.9 Alarms



Min. event duration: 3 s

Alarm output: false

*Video > Tamper Detect > Configure Alarms*

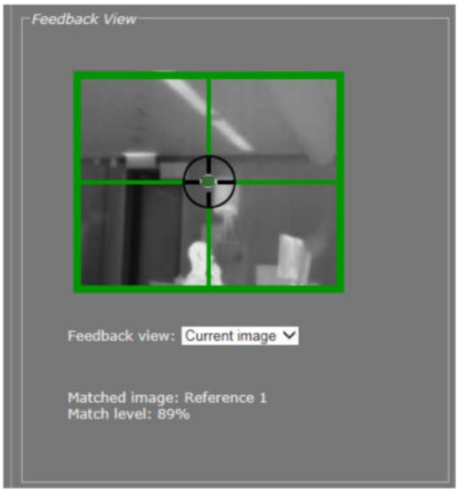
The Configure Alarms section enables you to view the current status of the alarm output and to set a delay for the activation/deactivation of alarm outputs.

**Note:** In addition to the status indication in this section, alarms can also be read from the TC620 's internal Management Information Base (MIB) using appropriate software, or through TKH Security's Open Streaming Architecture (OSA) - that is, the "SPI API". The TC620 includes SNMP support for its image monitor and tamper detect functions. A trap is sent when bad image quality or camera tampering has been detected and another one when the situation returns to normal. This support requires a new SNMP MIB, the OPTC-VCA-MIB, which can be downloaded at www.tkhsecurity.com/support-files.

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

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

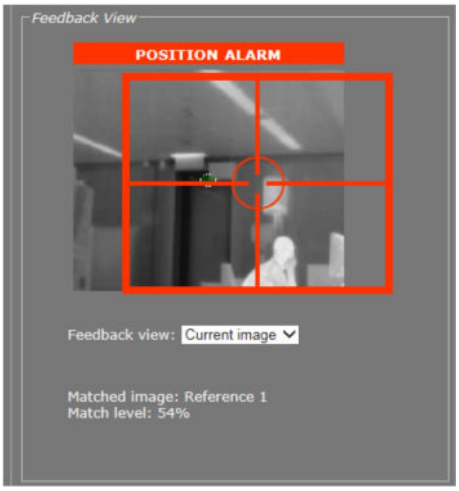
## 12.9.9.1 Alarm examples



Feedback view: Current image

Matched image: Reference 1
Match level: 89%

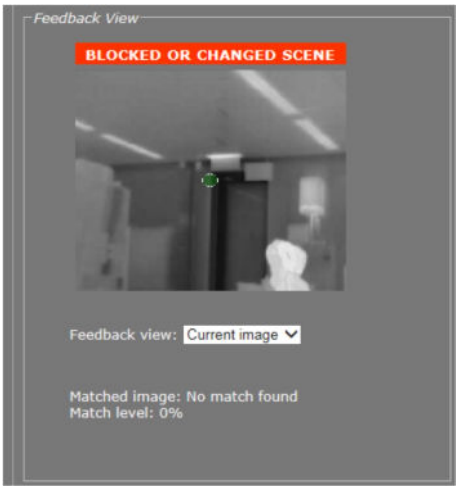
*Original camera position*



Feedback view: Current image

Matched image: Reference 1
Match level: 54%

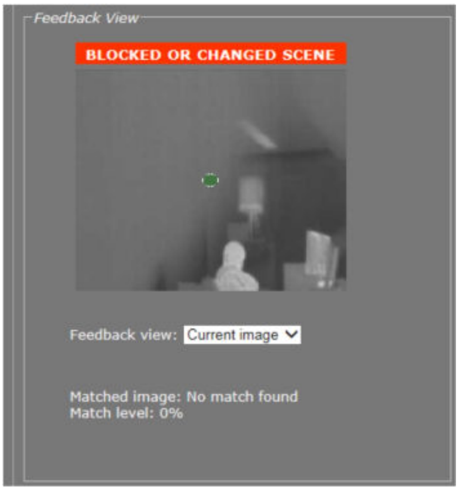
*Camera has moved to the left. Although the current image still matches Reference 1, the changed camera position results in a position alarm.*



Feedback view: Current image

Matched image: No match found
Match level: 0%

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

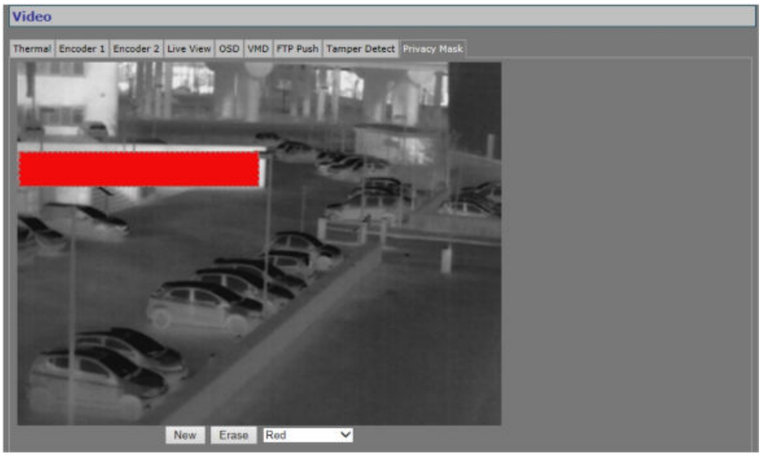


Feedback view: Current image

Matched image: No match found
Match level: 0%

*Camera lens is being spray-painted, resulting in a blocked scene alarm.*

# 12.10 Privacy Mask



*Video > Privacy Mask*

The privacy mask function aims to avoid intrusive monitoring. The TC620 supports up to 10 masks.

### ⏩ To create a privacy mask

1 On the *Video* page, click the **Privacy Mask** tab.

2 Under the preview, click **New**.

A square mask appears as an overlay in the centre of the preview.

3 Use the pointer to position and size the mask.

If desired, click to select the mask, and then select a mask colour from the list under the preview.

### ⏩ To delete a mask

1 On the *Video* page, click the **Privacy Mask** tab.

2 Using the pointer, select the mask in the preview.

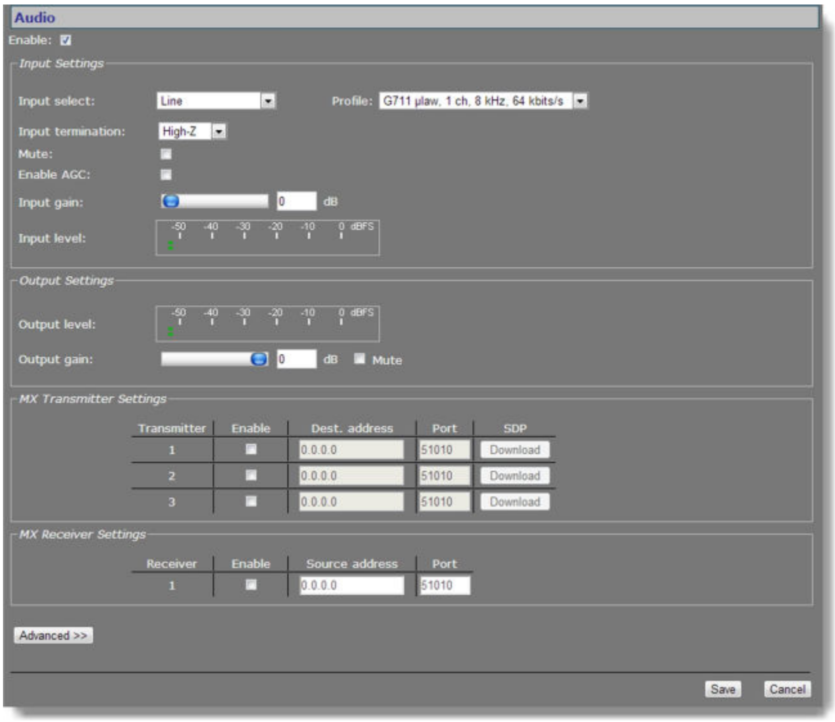
3 Click **Erase**.

# 13 Audio

This chapter describes the functionality and settings found on the Audio page of the TC620.

## In This Chapter

## 13.1 Enable audio



**Audio**

Enable: ☑

*Input Settings*

Input select: Line ▾ Profile: G711 µlaw, 1 ch, 8 kHz, 64 kbits/s ▾

Input termination: High-Z ▾

Mute: □

Enable AGC: □

Input gain: 0 dB

Input level:

*Output Settings*

Output level:

Output gain: 0 dB □ Mute

*MX Transmitter Settings*

| Transmitter | Enable | Dest. address | Port | SDP |
|---|---|---|---|---|
| 1 | □ | 0.0.0.0 | 51010 | Download |
| 2 | □ | 0.0.0.0 | 51010 | Download |
| 3 | □ | 0.0.0.0 | 51010 | Download |

*MX Receiver Settings*

| Receiver | Enable | Source address | Port |
|---|---|---|---|
| 1 | □ | 0.0.0.0 | 51010 |

*Audio page*

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

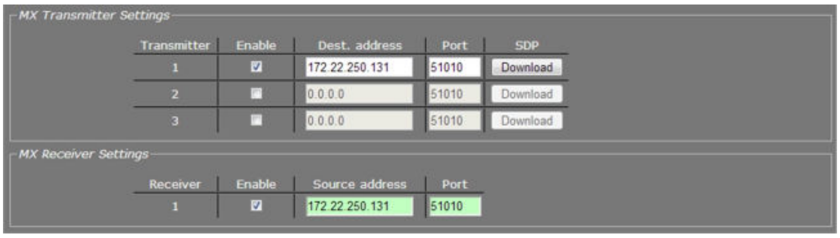
### 13.1.1 Input Settings

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

### 13.1.2 Output Settings

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

# 13.2 Make audio connections



MX Transmitter Settings

| Transmitter | Enable | Dest. address | Port | SDP |
|---|---|---|---|---|
| 1 | ☑ | 172.22.250.131 | 51010 | Download |
| 2 | □ | 0.0.0.0 | 51010 | Download |
| 3 | □ | 0.0.0.0 | 51010 | Download |

MX Receiver Settings

| Receiver | Enable | Source address | Port |
|---|---|---|---|
| 1 | ☑ | 172.22.250.131 | 51010 |

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

### Audio streams

The TC620 provides bidirectional audio. The TC620 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 TC620. 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 TC620 as the destination and source. Transmitters and receivers must be enabled in order for streaming to start. Remember to *Save* a configuration to make it effective.

### SDP download

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

## 13.2.1 MX Transmitter Settings

| Item | Description |
|---|---|
| Enable | Select/Clear to enable/disable the stream transmission, respectively. |
| Dest. address | IP address of the codec that will receive the stream. |
| Port | The local port number of the codec that will receive the stream. |
| SDP | To download a Session Description Protocol (SDP) file from the encoder, click the Download button. |

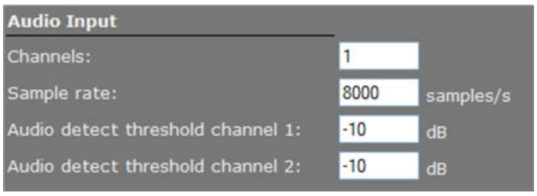
### 13.2.2 MX Receiver Settings

| Item | Description |
|---|---|
| Enable | Select/Clear to enable/disable the stream reception, respectively. |
| Source address | IP address of the codec that will transmit the stream. |
| Port | The local port number of the TC620. |

## 13.3 Advanced

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

### 13.3.1 Audio Input



**Audio Input**

Channels: 1

Sample rate: 8000 samples/s

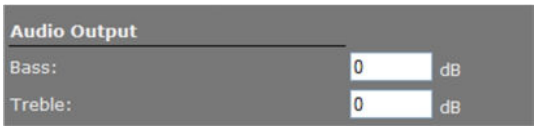
Audio detect threshold channel 1: -10 dB

Audio detect threshold channel 2: -10 dB

*Audio > Advanced > Audio Input*

| Item | Description |
|---|---|
| Channels | Range: [1…2]. When selecting 1 channel, only the signal on the 'A1' input is used (either line or microphone). |
| Sample rate | Range: [7850…48000]. Allows you to enter custom settings (other than those included in the Profile list in the Input Settings section), e.g., for communication with a C-20 codec.<br>Examples:<br>• 7850 Hz A-law<br>• 15710 Hz A-law<br>• 15710 Hz PCM<br>• 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 | |

## 13.3.2 Audio Output



Audio Output

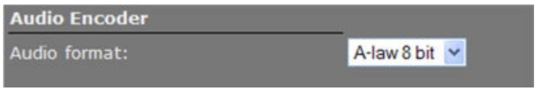
Bass: 0 dB

Treble: 0 dB

*Audio > Advanced > Audio Output*

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

## 13.3.3 Audio Encoder



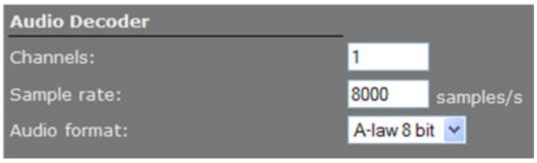
Audio Encoder

Audio format: A-law 8 bit

*Audio > Advanced > Audio Encoder*

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

## 13.3.4 Audio Decoder



Audio Decoder

Channels: 1

Sample rate: 8000 samples/s

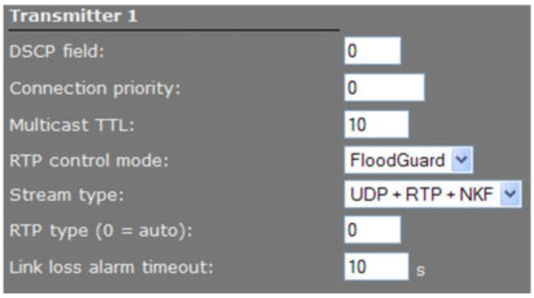
Audio format: A-law 8 bit

*Audio > Advanced > Audio Decoder*

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

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

## 13.3.5 Transmitter #



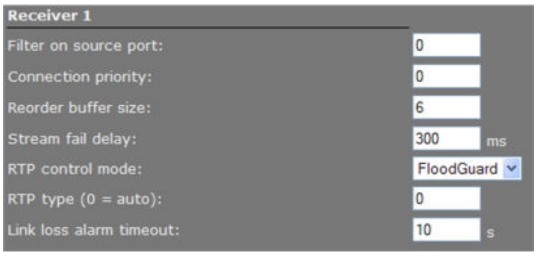
Transmitter 1

| | |
|---|---|
| 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 |

*Audio > Advanced > Transmitter #*

| Item | Description | |
|---|---|---|
| DSCP field | Range: [0...63]. DSCP (Differentiated Services Code Point) uses the first 6 bits of the ToS (Type of Service) field in the header of IP packets for packet classification purposes. The bit pattern in the field indicates the type of service and forwarding behavior at the next node. With 26 bits, up to 64 network service types can be defined. RFC 2724 (see - http://www.ietf.org/rfc/rfc2474.txt) describes the Differentiated Services (DS) field and the DiffServ Code Point. See also the note on Differentiated Services later in this chapter. | |
| Connection priority | Parameter intended for use with MX Software Development Kit. | |
| Multicast TTL | Range: [0...127]. Specify the number of routers (hops) that multicast traffic is permitted to pass through before expiring on the network. | |
| RTP control mode | Select the transport protocol to control the stream. | |
| | *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. | |

## 13.3.6 Receiver 1



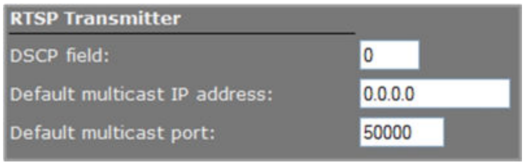
Receiver 1

| | | |
|---|---|---|
| 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 |

*Audio > Advanced > Receiver 1*

| Item | Description | |
|---|---|---|
| Filter on source port | Can be used to filter incoming signals. With multiple signals sent to the same IP address and destination port number, *Filter on source port* can be used to filter the input, i.e. to accept only signals from the transmitting port specified here. The filter will not be active if set to 0 (the default and recommended setting). | |
| Connection priority | Parameter intended for use with MX Software Development Kit. | |
| 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. | |

## 13.3.7 RTSP Transmitter



RTSP Transmitter

DSCP field: 0

Default multicast IP address: 0.0.0.0

Default multicast port: 50000

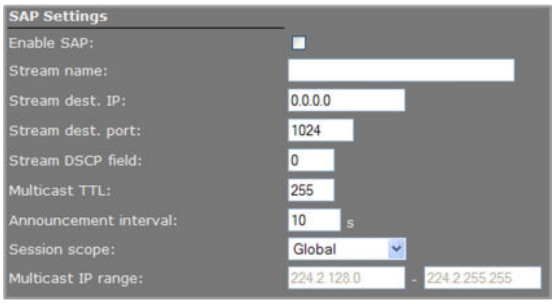
*Audio > Advanced > RTSP Transmitter*

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

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

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

## 13.3.8 SAP Settings



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 |

*Audio > Advanced > SAP Settings*

The TC620 includes a SAP announcer. The Session Announcement Protocol is used to advertise that a media stream generated by the TC620 is available at a specific multicast address and port. For more information about SAP, see the note below.

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

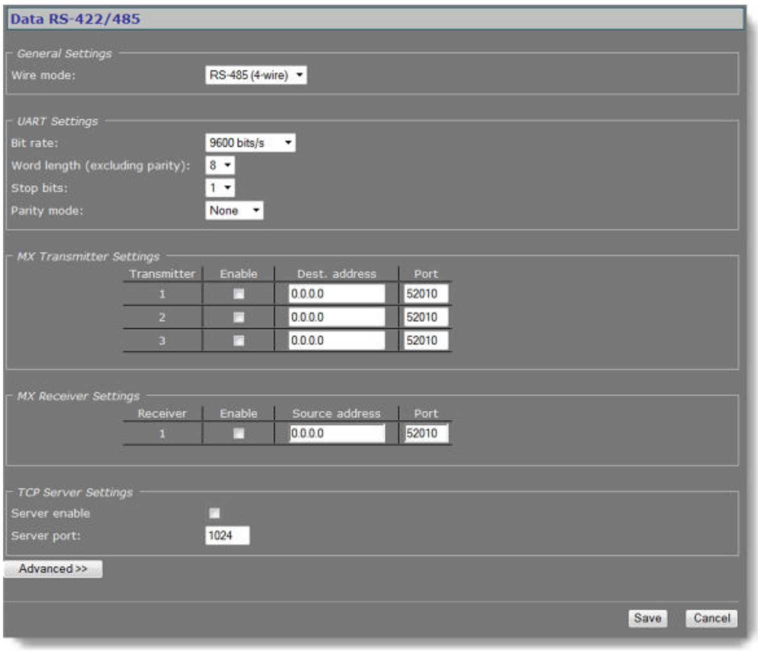
**Note on the Session Announcement Protocol (SAP):** SAP, defined in RFC 2974 (see RFC 2974 - http://www.ietf.org/rfc/rfc2974.txt), is a protocol for advertising multicast session information. A SAP announcer periodically broadcasts announcement packets which include the session description information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

# 14 Data RS-422/485

This chapter describes the Data RS-422/485 page of the TC620.

## In This Chapter

## 14.1 General Settings



**Data RS-422/485**

*General Settings*

Wire mode: RS-485 (4-wire)

*UART Settings*

Bit rate: 9600 bits/s

Word length (excluding parity): 8

Stop bits: 1

Parity mode: None

*MX Transmitter Settings*

| Transmitter | Enable | Dest. address | Port |
|---|---|---|---|
| 1 | □ | 0.0.0.0 | 52010 |
| 2 | □ | 0.0.0.0 | 52010 |
| 3 | □ | 0.0.0.0 | 52010 |

*MX Receiver Settings*

| Receiver | Enable | Source address | Port |
|---|---|---|---|
| 1 | □ | 0.0.0.0 | 52010 |

*TCP Server Settings*

Server enable □

Server port: 1024

*Data RS-422/485 page*

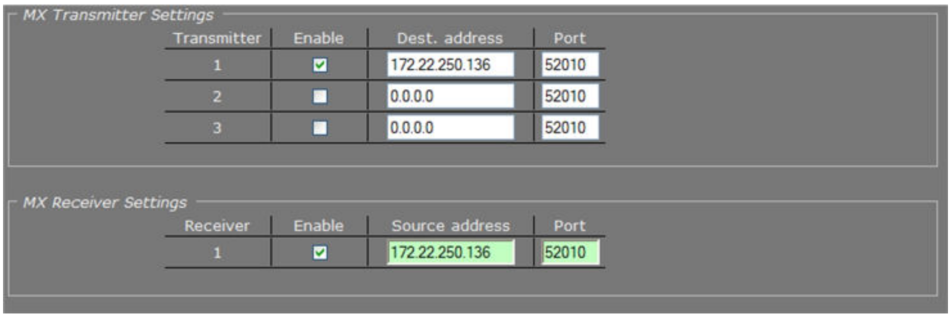
| Item | Description | |
|---|---|---|
| Wire mode | *RS-422*<br>*RS-485 (2-wire)*<br>*RS-485 (4-wire)* | The RX-4xx interface type is set in software. Select the appropriate type from this list. |

## 14.2 UART Settings

The TC620 uses a Universal Asynchronous Transmitter/Receiver (UART) for data transmission. The UART recognises and reproduces the words in the data stream. This is only possible if the UART is programmed to understand the serial data format.

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

## 14.3 Make data connections



MX Transmitter Settings

| Transmitter | Enable | Dest. address | Port |
|---|---|---|---|
| 1 | ☑ | 172.22.250.136 | 52010 |
| 2 | □ | 0.0.0.0 | 52010 |
| 3 | □ | 0.0.0.0 | 52010 |

MX Receiver Settings

| Receiver | Enable | Source address | Port |
|---|---|---|---|
| 1 | ☑ | 172.22.250.136 | 52010 |

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

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

### ⏩ To configure a data link

1 In the *Transmitter Settings* section, set at least one destination IP address.

2 Set a port number or leave it at the default.

3 Enable the stream.

4 Click **SAVE** to write the new configuration to the device.

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

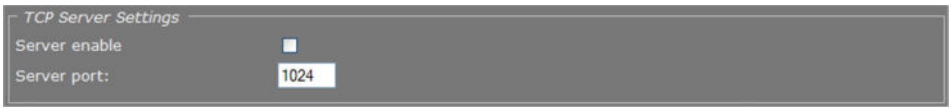
Do not forget to enable both the transmitter and the receiver, and to configure the UART correctly (see Advanced Settings).

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

### Highlighted fields

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

## 14.4 TCP Server Settings



TCP Server Settings

Server enable □

Server port: 1024

*Data RS-422/485 > TCP Server Settings*

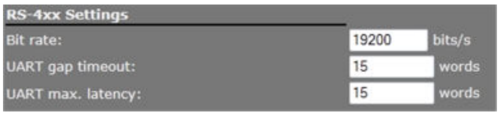
TCP connections are always bidirectional, so no separate transmitter and receiver settings are needed.

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

## 14.5 Advanced

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

### 14.5.1 RS-4xx Settings



RS-4xx Settings

Bit rate: 19200 bits/s

UART gap timeout: 15 words

UART max. latency: 15 words

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

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

| Item | Description |
|---|---|
| Bit rate | Range: [300...115200]. The speed of the digital transmission, that is - the amount of information transferred/processed per unit of time. Enables you to set a bit rate other than the presets in the UART settings section. |
| UART gap timeout | Range: [0...255] data words. Will have the next packet sent when the line has remained idle for longer than the timeout. |
| UART max. latency | Range: [0...255] data words. The maximum latency of the data channel is controlled by forcing a packet to be sent when the first data word of the packet was received longer ago than the number of word times set here. |

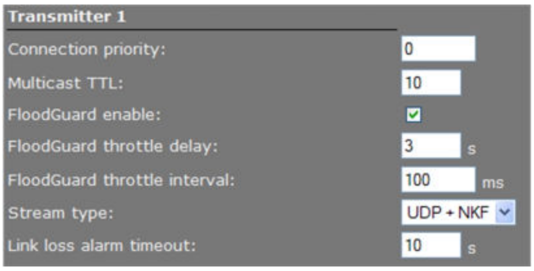
**Note on Data Transfer Optimisation:** A 'word time' is the transmit time for one data word. The amount of time one data word takes to travel on the line is determined by bit rate and word length. Using the *UART gap timeou*t and *UART max. latency* variables you can tailor the data channel for your 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.

## 14.5.2 Transmitter #



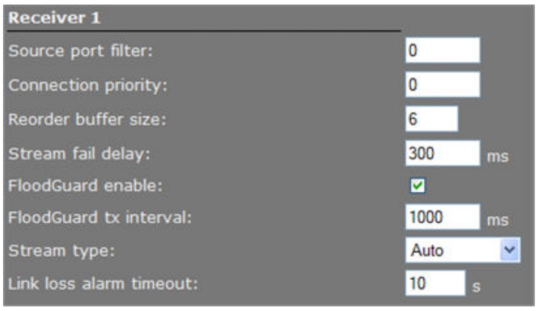
Transmitter 1

| | |
|---|---|
| Connection priority: | 0 |
| Multicast TTL: | 10 |
| FloodGuard enable: | ☑ |
| FloodGuard throttle delay: | 3 s |
| FloodGuard throttle interval: | 100 ms |
| Stream type: | UDP + NKF |
| Link loss alarm timeout: | 10 s |

*Data RS-422/485 > Advanced > Transmitter 1*

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

## 14.5.3 Receiver 1



Receiver 1

| | | |
|---|---|---|
| Source port filter: | 0 | |
| Connection priority: | 0 | |
| Reorder buffer size: | 6 | |
| Stream fail delay: | 300 | ms |
| FloodGuard enable: | ☑ | |
| FloodGuard tx interval: | 1000 | ms |
| Stream type: | Auto | |
| Link loss alarm timeout: | 10 | s |

*Data RS-422/485 > Advanced > Receiver 1*

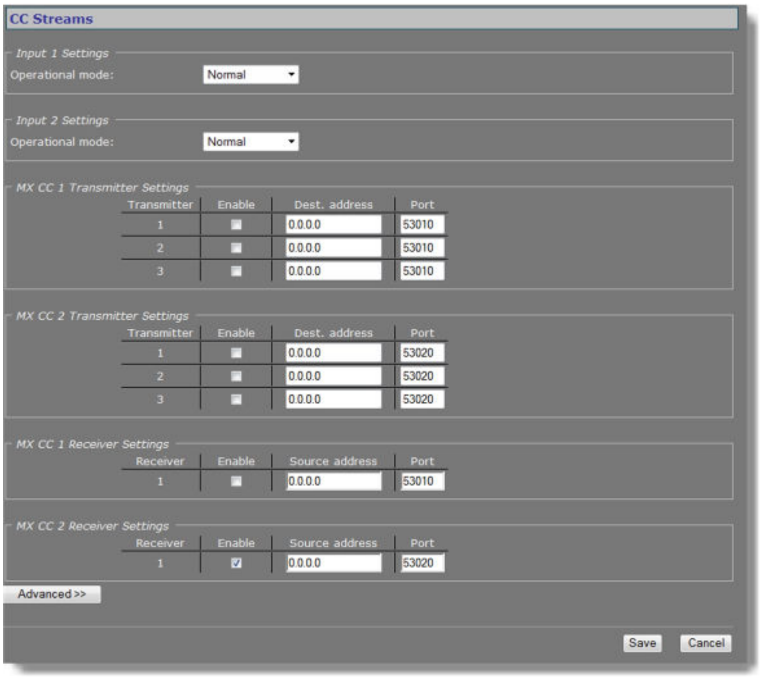
| Item | Description |
|---|---|
| Source port filter | Can be used to filter incoming data traffic. With multiple signals sent to the same IP address and destination port number, Source port filter can be used to filter the input, that is - to accept only data from the transmitting port specified here.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

# 15 CC Streams

This chapter provides information about the TC620's contact closure (CC) channels, CC status, and alarms.

## In This Chapter

## 15.1 CC channels, CC status, and alarms



CC Streams

Input 1 Settings

Operational mode: Normal

Input 2 Settings

Operational mode: Normal

MX CC 1 Transmitter Settings

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

MX CC 2 Transmitter Settings

| Transmitter | Enable | Dest. address | Port |
|---|---|---|---|
| 1 | □ | 0.0.0.0 | 53020 |
| 2 | □ | 0.0.0.0 | 53020 |
| 3 | □ | 0.0.0.0 | 53020 |

MX CC 1 Receiver Settings

| Receiver | Enable | Source address | Port |
|---|---|---|---|
| 1 | □ | 0.0.0.0 | 53010 |

MX CC 2 Receiver Settings

| Receiver | Enable | Source address | Port |
|---|---|---|---|
| 1 | ☑ | 0.0.0.0 | 53020 |

CC Streams page

### CC channels

The contact closure channels of the TC620, 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

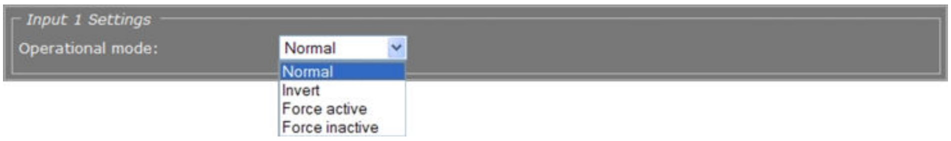
The receiver relays are normally open (fail-safe). Each CC input is sampled 100 times per second. Changes are transmitted directly, so overall latency of the contact closure signals is <20 ms. To confirm, the actual contact closure status is transmitted every 100 ms; there is no further forward error 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 TC620, 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 TC620 and check for the module alarm. Stream alarms (link alarms in the modules, at both link ends) become active if the link fails.

## 15.2 Input # Settings



Input 1 Settings

Operational mode: Normal

*CC Streams > Input 1 Settings*

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

## 15.3 Make contact closure connections

Making CC links is similar to making video/data/audio links, but without additional interface configuration.

### ⏩ To make a contact closure connection

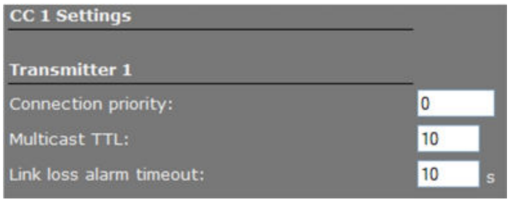
- On the Transmitter side, fill in a destination IP address and port number for each codec you want a CC stream to go to, and then enable the stream.
- On the other side of the link (i.e. the codec you want to receive the CC stream), fill in the source IP address, the local port number (the same as specified for the transmitter), and then enable the receiver.

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

# 15.4 Advanced

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

## 15.4.1 Transmitter #



CC 1 Settings

Transmitter 1

Connection priority: 0

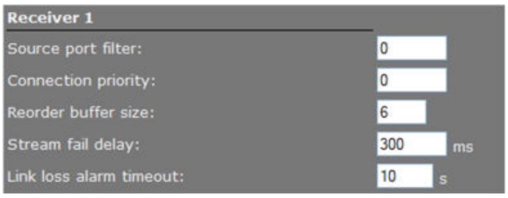
Multicast TTL: 10

Link loss alarm timeout: 10 s

*CC Streams > Advanced > Transmitter 1*

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

## 15.4.2 Receiver 1



Receiver 1

Source port filter: 0

Connection priority: 0

Reorder buffer size: 6

Stream fail delay: 300 ms

Link loss alarm timeout: 10 s

*CC Streams > Advanced > Receiver 1*

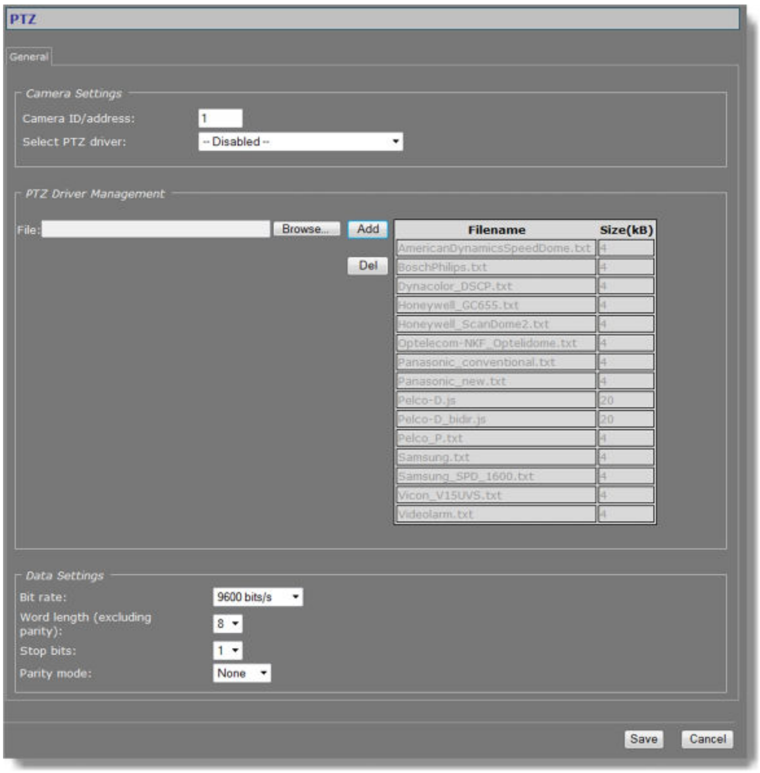
| Item | Description |
|---|---|
| Source port filter | Can be used to filter incoming data traffic. With multiple signals sent to the same IP address and destination port number, Source port filter can be used to filter the input, that is - to accept only data from the transmitting port specified here.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

# 16 PTZ

The TC620 itself does not have PTZ functionality, but it can be mounted on a PTZ mounting bracket which can then be controlled from the TC620's serial data port (RS-4xx). With a PTZ driver selected on the PTZ web page, the PTZ control panel is available on the Live Video page. This chapter explains how to enable PTZ control, upload and remove PTZ drivers, and configure data settings.

## In This Chapter

## 16.1 Enable PTZ control



*Camera Settings*

Camera ID/address: 1

Select PTZ driver: -- Disabled --

*PTZ Driver Management*

File:

| Filename | Size(kB) |
|---|---|
| AmericanDynamicsSpeedDome.txt | 4 |
| BoschPhilips.txt | 4 |
| Dynacolor_DSCP.txt | 4 |
| Honeywell_GC655.txt | 4 |
| Honeywell_ScanDome2.txt | 4 |
| Optelecom-NKF_Optelidome.txt | 4 |
| Panasonic_conventional.txt | 4 |
| Panasonic_new.txt | 4 |
| Pelco-D.js | 20 |
| Pelco-D_bidir.js | 20 |
| Pelco_P.txt | 4 |
| Samsung.txt | 4 |
| Samsung_SPD_1600.txt | 4 |
| Vicon_V15UVS.txt | 4 |
| Videolarm.txt | 4 |

*Data Settings*

Bit rate: 9600 bits/s

Word length (excluding parity): 8

Stop bits: 1

Parity mode: None

*PTZ page*

PTZ camera control is enabled by selecting a driver that is supported by the camera. If the required driver is not included in the PTZ driver list, you can upload it to the TC620.

### ⏩ To enable PTZ control

1 In the *Camera Settings* section, specify the Camera ID/address.

2 From the *PTZ driver* list, select the protocol supported by the PTZ device you wish to control.

3 Click **Save**.

You can now control the camera with the control panel on the Live Video page.

## 16.2 Upload/Remove PTZ drivers

### ⏩ To upload a PTZ driver

1 In the *PTZ Driver Management* section, click **Browse**.

2 In the *File to Upload* dialog box, browse to the folder containing the driver.

3 Select the appropriate file (`.txt` or `.js` extension), and then click **Open**.

The driver displays in the *File* text box.

4 Click the **Add** button.

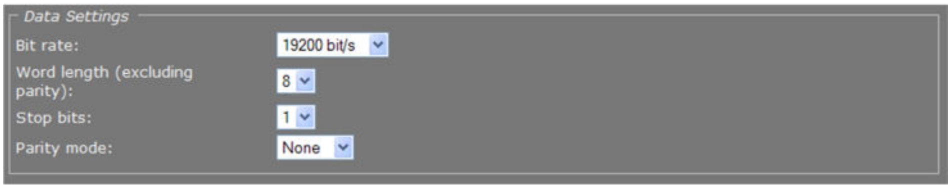
The driver is added to the list of available drivers in the *PTZ Driver Management* and *Camera Settings* sections.

### ⏩ To remove a PTZ driver

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

2 Click the **Del** button.

## 16.3 Data Settings



Data Settings

Bit rate: 19200 bit/s

Word length (excluding parity): 8

Stop bits: 1

Parity mode: None

*PTZ > Data Settings*

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

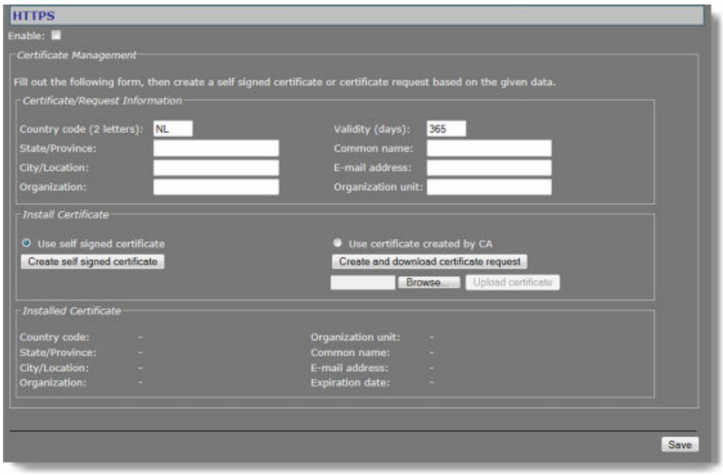
**Note:** Changes you make in the Data Settings section are copied to the RS-422/485 page.

# 17 Security

From the Security page, Administrators can install security certificates to enable secure connections between the TC620 and web browsers. Certificates can be self-signed or obtained from a Certificate Authority.

## In This Chapter

## 17.1 HTTPS



HTTPS

Enable: □

*Certificate Management*

Fill out the following form, then create a self signed certificate or certificate request based on the given data.

*Certificate/Request Information*

| | | | |
|---|---|---|---|
| Country code (2 letters): | NL | Validity (days): | 365 |
| State/Province: | | Common name: | |
| City/Location: | | E-mail address: | |
| Organization: | | Organization unit: | |

*Install Certificate*

● Use self signed certificate ○ Use certificate created by CA

Create self signed certificate
Create and download certificate request
Browse...
Upload certificate

*Installed Certificate*

| | | | |
|---|---|---|---|
| Country code: | - | Organization unit: | - |
| State/Province: | - | Common name: | - |
| City/Location: | - | E-mail address: | - |
| Organization: | - | Expiration date: | - |

*Security page*

### Secure connections

An HTTPS connection is a standard HTTP connection on top of an SSL/TLS connection, adding the security capabilities of SSL/TLS to standard HTTP communication. With HTTPS implemented and used on the TC620, a safe exchange of data between the unit and a web browser is ensured. Information transported over the network, such as device settings and credentials, is encrypted to protect it against eavesdropping.

### Certificates

To implement HTTPS on the TC620, you need to install an HTTPS certificate. You can use a self-signed certificate or one created by a Certificate Authority (CA). CA-issued certificates provide a higher level of security and inspire more trust than self-signed certificates. Self-signed certificates are often installed for test purposes or as a temporary solution until a CA-issued certificate has been obtained.

## 17.2 Certificate/Request information

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

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

**Important:** Make sure that the *Common name* you specify when you generate a security certificate matches the URL that is used to access the webpages of the TC620. Generally, this is the IP address of the unit, followed by "/frame.html". For example: 10.50.3.72/frame.html

## 17.3 CA-Issued certificate

Steps towards implementing a certificate created by a CA

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

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

### ⏩ To generate a certificate request

1. In the *Certificate/Request Information* section, enter the required information as described above.
2. Click **Create and download certificate request**.

   A pop-up displays.
3. In the pop-up, click **Save**.

   You can copy the request from your download folder now and then send it to a CA.

### ⏩ To install a signed certificate from a CA

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

A warning displays.

4 Click **Yes** to continue.

## 17.4 Self-signed certificate

### ⏩ To create a self-signed certificate

1 In the *Certificate/Request Information* section, enter the required information as described above.

2 Click **Create self-signed certificate**.

## 17.5 Open a secure connection

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

### ⏩ To enable HTTPS and open a secure connection

1 On the *Security* page, select **Use self-signed certificate** or **Use certificate created by CA** (depending on the type of certificate you want to use).

2 At the top of the page, select **Enable**.

3 Click **Save**.

4 Refresh the page.

5 Log on to the TC620 again.

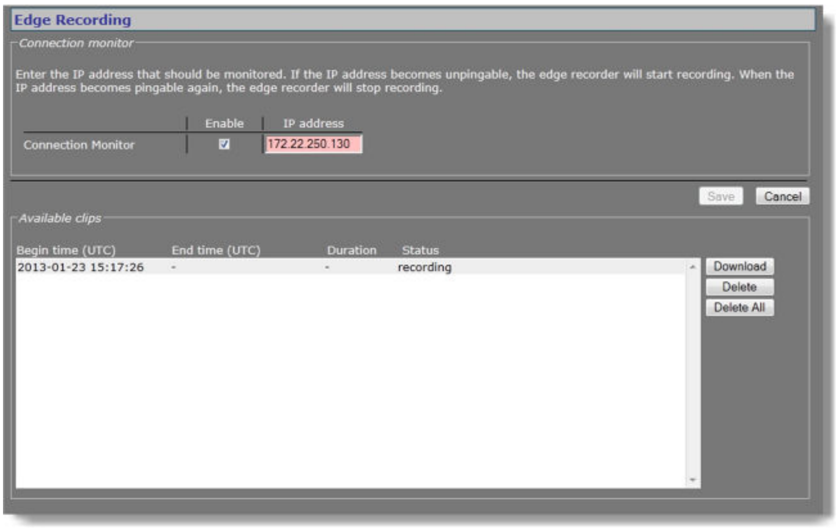
Your browser is now using a secure connection to communicate with the unit.

# 18 Edge recording

This chapter describes how you can use edge recording to record video from the TC620 to the embedded SD card.

## In This Chapter

## 18.1 Edge recording basics



**Edge Recording**

*Connection monitor*

Enter the IP address that should be monitored. If the IP address becomes unpingable, the edge recorder will start recording. When the IP address becomes pingable again, the edge recorder will stop recording.

| | Enable | IP address |
|---|---|---|
| Connection Monitor | ☑ | 172.22.250.130 |

*Available clips*

| Begin time (UTC) | End time (UTC) | Duration | Status |
|---|---|---|---|
| 2013-01-23 15:17:26 | - | - | recording |

*Connection monitor enabled. Edge recorder is recording video (the specified IP address is unpingable).*

Edge recording makes it possible to record and store video locally - that is, at the TC620. To prevent loss of video when the connection to a central network video recorder or VMS sytem is lost, recorded video clips can be stored on the SD card inside the TC620. From the Edge recording page, the clips can then be downloaded for further processing.

> **Note:** By default, on the Event Management page, the Edge Recording connection monitor is selected as a trigger for edge recording. Note that you can also assign other alarm sources as a trigger on that page.

## 18.2 Monitoring

Unlike 24-hour recording by an NVR, edge recordings are typically short recordings. Start and stop times for the recordings are triggered by external events, such as a lost or restored connection to an NVR or VMS, for example. To detect these events, the TC620 monitors the network connection to the device specified by its IP address. This is done by pinging it at regular intervals to test its reachability over the network.

### ⏩ To monitor a connection

1. In the *Connector monitor* section, specify the IP address to be monitored.
2. Select **Enable**.
3. Click **Save**.

   The device is now pinged every 15 seconds.

   If the device is reachable, IP address highlighting goes from pink to green.

## 18.3 Recording

Detecting a loss of connection to the device at the monitored IP address triggers the following:

- Edge recording starts.
- The IP address of the device is highlighted in pink to indicate the connection loss.
- The video clip appears in the *Available clips* section with clip status shown as 'recording'.

  A recording status reported as 'pending' is an indication that the encoder used for edge recording is either not enabled or not correctly configured for edge recording.
- Edge recording continues until the device becomes responsive to ping messages again.

**Important:** Recording does not start if the device at the specified IP address has not been detected previously. In other words, recording is only possible if the device has acknowledged its presence on the network at least once by responding to ping messages. This is to prevent unintended recording to the SD card.

## 18.4 Clips

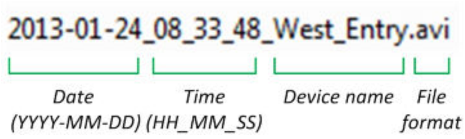
Details about clips can be found in the *Available clips* section.

- Clips with recording status 'recording' or 'ready' are available for download in .avi format.
- Clips include 30 seconds of prerecorded video and five seconds of postrecorded video. The prerecording mechanism is active at all times.
- Clip file size will not exceed 500 MB. If a recording requires more storage capacity, multiple clips are created.
- Clips can be deleted one at a time (select the clip, and then click *Delete*), or all in one go (click *Delete all*).

### ⏩ To download a clip

1. In the *Available clips* section, select the clip.
2. Click **Download**.
3. Specify if you want to open, save, or cancel the download.

Clip file names are created automatically using UTC date/time information and the device name.



## 18.5 SD card

You can check the SD card storage capacity through the Status page (see the Measurements tab).

**Important:** Note that the storage capacity available for edge recording is limited to 75% of the actual SD card size - that is, for example, 24 GB of a 32 GB SD card. This limit is to prevent slow read/write speeds.>

When the SD card is full, recording stops and a message is sent to the syslog (for a description of the syslog function, see *Device Management*).

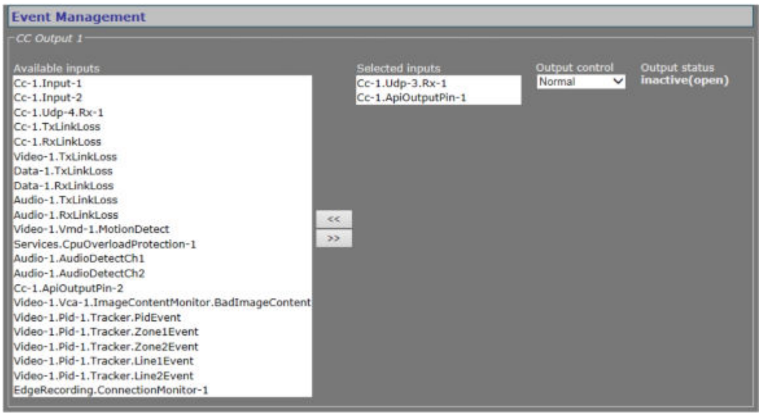
⚠ **Warning:** Powering down or rebooting the TC620, or insertion into an operational unit erases all content on the SD card! Clips will be irretrievably lost.

# 19 Event Management

This chapter describes the Event Management page.

## In This Chapter

## 19.1 Associate events with output facilities



Event Management

CC Output 1

Available inputs

- Cc-1.Input-1
- Cc-1.Input-2
- Cc-1.Udp-4.Rx-1
- Cc-1.TxLinkLoss
- Cc-1.RxLinkLoss
- Video-1.TxLinkLoss
- Data-1.TxLinkLoss
- Data-1.RxLinkLoss
- Audio-1.TxLinkLoss
- Audio-1.RxLinkLoss
- Video-1.Vmd-1.MotionDetect
- Services.CpuOverloadProtection-1
- Audio-1.AudioDetectCh1
- Audio-1.AudioDetectCh2
- Cc-1.ApiOutputPin-2
- Video-1.Vca-1.ImageContentMonitor.BadImageContent
- Video-1.Pid-1.Tracker.PidEvent
- Video-1.Pid-1.Tracker.Zone1Event
- Video-1.Pid-1.Tracker.Zone2Event
- Video-1.Pid-1.Tracker.Line1Event
- Video-1.Pid-1.Tracker.Line2Event
- EdgeRecording.ConnectionMonitor-1

Selected inputs

- Cc-1.Udp-3.Rx-1
- Cc-1.ApiOutputPin-1

Output control: Normal

Output status: inactive(open)

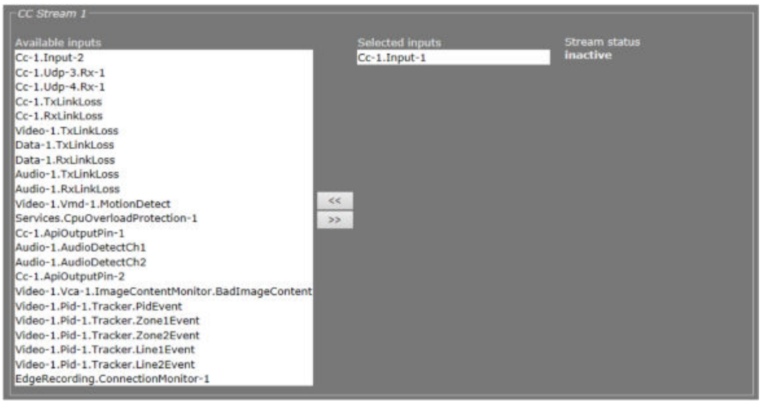
*Event Management*

On the Event Management page, you can configure how the TC620 is to handle incoming events/alarms. The event sources listed under Available inputs can be routed to a CC output, CC stream, FTP push, and an edge recording.

## 19.2 CC Output #

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

## 19.3 CC Stream #



Available inputs
Cc-1.Input-2
Cc-1.Udp-3.Rx-1
Cc-1.Udp-4.Rx-1
Cc-1.TxLinkLoss
Cc-1.RxLinkLoss
Video-1.TxLinkLoss
Data-1.TxLinkLoss
Data-1.RxLinkLoss
Audio-1.TxLinkLoss
Audio-1.RxLinkLoss
Video-1.Vmd-1.MotionDetect
Services.CpuOverloadProtection-1
Cc-1.ApiOutputPin-1
Audio-1.AudioDetectCh1
Audio-1.AudioDetectCh2
Cc-1.ApiOutputPin-2
Video-1.Vca-1.ImageContentMonitor.BadImageContent
Video-1.Pid-1.Tracker.PidEvent
Video-1.Pid-1.Tracker.Zone1Event
Video-1.Pid-1.Tracker.Zone2Event
Video-1.Pid-1.Tracker.Line1Event
Video-1.Pid-1.Tracker.Line2Event
EdgeRecording.ConnectionMonitor-1

Selected inputs
Cc-1.Input-1

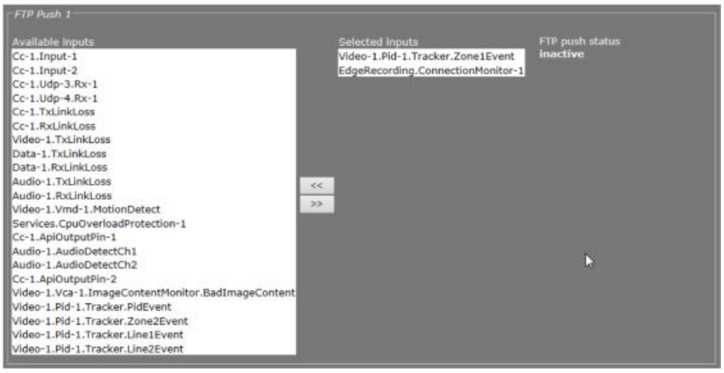
Stream status
inactive

*Event Management > CC Stream 1*

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

## 19.4 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).



Available inputs
Cc-1.Input-1
Cc-1.Input-2
Cc-1.Udp-3.Rx-1
Cc-1.Udp-4.Rx-1
Cc-1.TxLinkLoss
Cc-1.RxLinkLoss
Video-1.TxLinkLoss
Data-1.TxLinkLoss
Data-1.RxLinkLoss
Audio-1.TxLinkLoss
Audio-1.RxLinkLoss
Video-1.Vmd-1.MotionDetect
Services.CpuOverloadProtection-1
Cc-1.ApiOutputPin-1
Audio-1.AudioDetectCh1
Audio-1.AudioDetectCh2
Cc-1.ApiOutputPin-2
Video-1.Vca-1.ImageContentMonitor.BadImageContent
Video-1.Pid-1.Tracker.PidEvent
Video-1.Pid-1.Tracker.Zone2Event
Video-1.Pid-1.Tracker.Line1Event
Video-1.Pid-1.Tracker.Line2Event

Selected inputs
Video-1.Pid-1.Tracker.Zone1Event
EdgeRecording.ConnectionMonitor-1

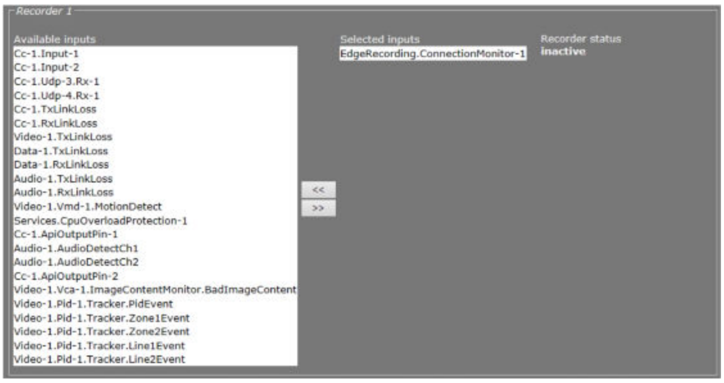
FTP push status
inactive

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

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

## 19.5 Recorder

It is possible to use an incoming alarm from an event source to trigger the recording of live video to the built-in SD card. The trigger selected by default is the Edge Recording connection monitor. Other sources can be selected from the *Available inputs* list as well.



Available inputs
Cc-1.Input-1
Cc-1.Input-2
Cc-1.Udp-3.Rx-1
Cc-1.Udp-4.Rx-1
Cc-1.TxLinkLoss
Cc-1.RxLinkLoss
Video-1.TxLinkLoss
Data-1.TxLinkLoss
Data-1.RxLinkLoss
Audio-1.TxLinkLoss
Audio-1.RxLinkLoss
Video-1.Vmd-1.MotionDetect
Services.CpuOverloadProtection-1
Cc-1.ApiOutputPin-1
Audio-1.AudioDetectCh1
Audio-1.AudioDetectCh2
Cc-1.ApiOutputPin-2
Video-1.Vca-1.ImageContentMonitor.BadImageContent
Video-1.Pid-1.Tracker.PidEvent
Video-1.Pid-1.Tracker.Zone1Event
Video-1.Pid-1.Tracker.Zone2Event
Video-1.Pid-1.Tracker.Line1Event
Video-1.Pid-1.Tracker.Line2Event

Selected inputs
EdgeRecording.ConnectionMonitor-1

Recorder status
inactive

*Event Management > Recorder*

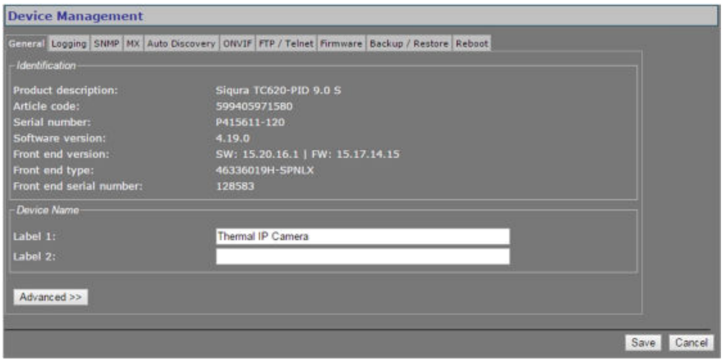
| Item | Description |
|---|---|
| Available inputs | List of sources that can be selected as triggers for edge recording. |
| Selected inputs | On selection of multiple inputs, the inputs are connected with a logical OR. Any one will trigger edge recording. |
| Recorder status | *Inactive* or *active.* Active: one or more of the selected inputs is true. Inactive: none of the selected inputs is true. |

# 20 Device Management

On the Device Management page, you can view identification information and assign device labels. In addition, you can configure logging settings, prepare the TC620 for SNMP management, and enable support for TKH Security's MX protocol, Auto Discovery, and ONVIF. You can also upgrade/downgrade the embedded firmware, back up and restore a configuration, and reboot the TC620 from this page.

### In This Chapter

## 20.1 General



Product description: Siqura TC620-PID 9.0 S
Article code: 599405971580
Serial number: P415611-120
Software version: 4.19.0
Front end version: SW: 15.20.16.1 | FW: 15.17.14.15
Front end type: 46336019H-SPNLX
Front end serial number: 128583

Label 1: Thermal IP Camera
Label 2:

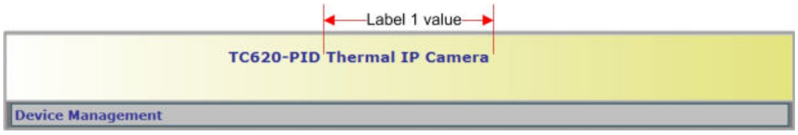
*Device Management > General*

### 20.1.1 Identification

This section offers administrative module information.

### 20.1.2 Device Name

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

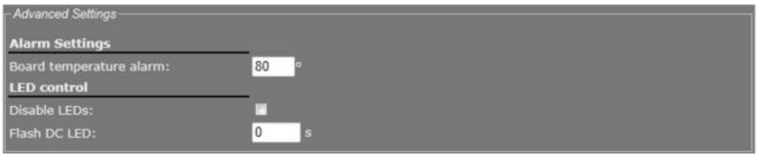


TC620-PID Thermal IP Camera

Device Management

*Title pane with Label 1 value*

### 20.1.3 Advanced


Advanced Settings

Alarm Settings

Board temperature alarm: 80 °

LED control

Disable LEDs: □

Flash DC LED: 0 s

*Device Management > General > Advanced*

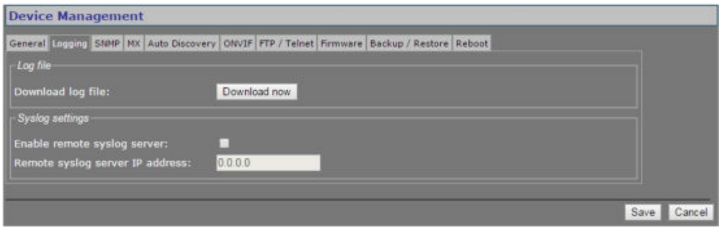
#### 20.1.3.1 Alarm Settings

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

#### 20.1.3.2 LED control

| Item | Description |
|---|---|
| Disable LEDs | For security reasons or energy efficiency you can deactivate all LEDs on the unit here. |
| Flash DC LED | Range: [0 …1000]. To identify a TC620 among other units, enter a value and click **Save**. The power LED on this particular unit will blink for the number of seconds you set. |

# 20.2 Logging



Device Management

*Log file*

Download log file:

*Syslog settings*

Enable remote syslog server: □

Remote syslog server IP address: 0.0.0.0

*Device Management > Logging*

## 20.2.1 Log file

Press the *Download now* button to download a log file from the TC620 to your computer. The 'system.log' file which opens in Notepad may prove useful when you are troubleshooting issues.

## 20.2.2 Syslog settings

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

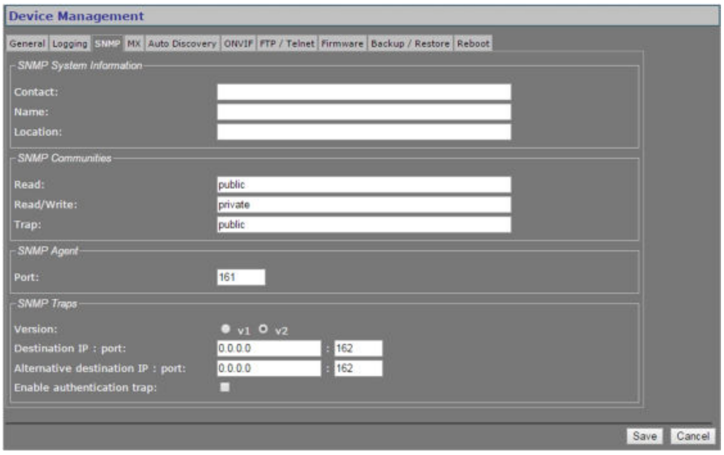
### ⏩ To enable a remote syslog server

1 In *Syslog settings*, select **Enable remote syslog server**.

2 Specify the IP address of the remote syslog server.

3 Click **Save**.

# 20.3 SNMP



Device Management

*SNMP System Information*

Contact:

Name:

Location:

*SNMP Communities*

Read: public

Read/Write: private

Trap: public

*SNMP Agent*

Port: 161

*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 > SNMP*

### 20.3.1 SNMP System Information

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

### 20.3.2 SNMP Communities

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

### 20.3.3 SNMP Agent

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

### 20.3.4 SNMP Traps

A TC620 alarm status change generates a trap which can be caught by any SNMP manager. The TC620 can, for example, send traps on the occurrence of Image Quality and Camera Tampering events. Variables, which can be read from the TC620's MIB through an SNMP manager, indicate why the alarm occurred. The OPTC-VCA-MIB required for this can be downloaded, together with the other TC620 MIBs, at www.tkhsecurity.com/support-files.

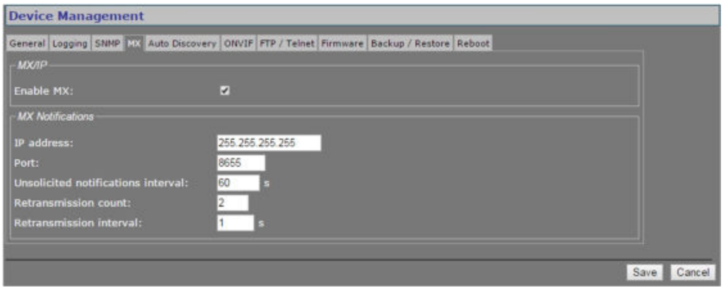
Note that *Version* and *Destination IP : port* are required fields.

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

### 20.3.5 Polling

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

# 20.4 MX



MX/IP

Enable MX: ☑

MX Notifications

IP address: 255.255.255.255

Port: 8655

Unsolicited notifications interval: 60 s

Retransmission count: 2

Retransmission interval: 1 s

*Device Management > MX*

## 20.4.1 MX/IP

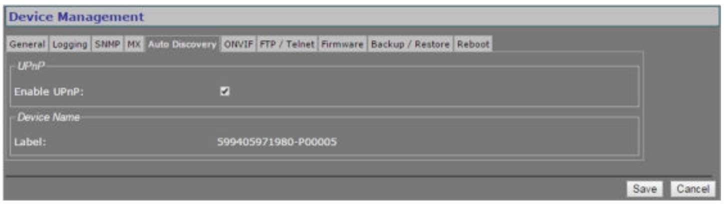
MX/IP is a UDP protocol used to communicate with TKH Security equipment over a network connection. TKH Security applications use the MX/IP protocol to access, configure, and control TKH Security network devices.

| Item | Description |
|---|---|
| Enable MX | In addition to the proprietary MX/IP protocol, a TC620 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 TC620 firmware through the MX Firmware Upgrade Tool application. |

## 20.4.2 MX Notifications

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

# 20.5 Auto Discovery



*UPnP*

Enable UPnP: ☑

*Device Name*

Label: 599405971980-P00005

*Device Management > Auto Discovery*

## 20.5.1 Advertise the TC620

On the Auto Discovery tab, you can enable UPnP (Universal Plug and Play). If enabled, UPnP allows the TC620 to advertise its presence and services to control points on the network. A control point can be a network device with embedded UPnP, a VMS application or a spy software tool, such as Device Spy. With the UPnP service enabled in Windows (see *Appendix: Enable UPnP in Windows 7*), you can connect to the TC620 from Windows Explorer.

### 20.5.1.1 Note

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

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

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

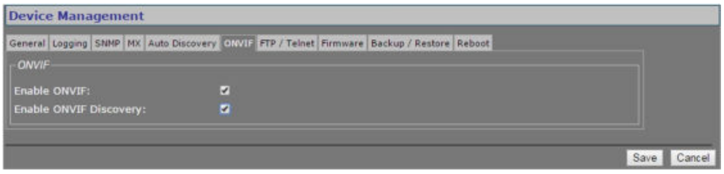
**Step 3:** *Control*. The control point can send actions to a device's service.

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

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

The TC620 supports the following Universal Plug and Play (UPnP) functionality: *Discovery*, *Description* (partly supported), and *Presentation*.

# 20.6 ONVIF



Enable ONVIF: ☑
Enable ONVIF Discovery: ☑

*Device Management > ONVIF*

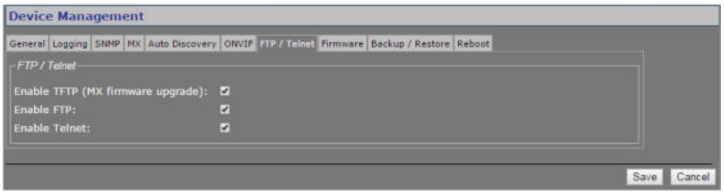
The TC620 supports the ONVIF standard. On the ONVIF tab, you can enable ONVIF compatibility and ONVIF discovery.

| Item | Description |
|---|---|
| Enable ONVIF | Enables the ONVIF interface on the TC620. |
| Enable ONVIF Discovery | Makes the TC620 discoverable for ONVIF clients. Clear this check box if you prefer to disable discovery. In that case, the TC620 can still be controlled from ONVIF clients that "know" of its existence. |

## 20.6.1 Note

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

# 20.7 FTP/Telnet



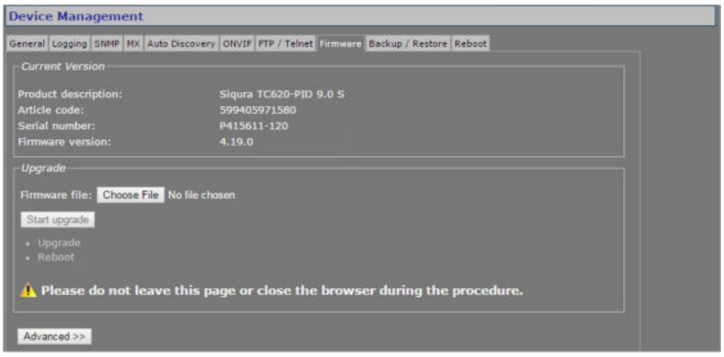
Enable TFTP (MX firmware upgrade): ☑
Enable FTP: ☑
Enable Telnet: ☑

*Device Management > FTP/Telnet*

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

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

# 20.8 Firmware



Product description: Siqura TC620-PID 9.0 S
Article code: 599405971580
Serial number: P415611-120
Firmware version: 4.19.0

Firmware file: No file chosen

- Upgrade
- Reboot

⚠ Please do not leave this page or close the browser during the procedure.

*Device Management > Firmware*

## 20.8.1 Firmware images

The TC620 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 TC620 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 TC620.

## 20.8.2 Current Version

This section offers information on the currently active firmware version.

## 20.8.3 Upgrade

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

**Important:** On upgrading a TC620 to firmware version 4.0 and higher, all existing users are deleted. After a successful upgrade, you can access the webpages with the default Admin account (user name = Admin; password = 1234).

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

### ⏩ To upgrade the TC620 firmware

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

   **Note:** Files with an `.nkffw` extension cannot be used to upgrade the TC620 via the webpage. You can use them to upgrade the unit through MX Firmware Upgrade Wizard. This software is embedded in MX Configuration Tool and is also available as a stand-alone tool.

5. Click **Start upgrade**.

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

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

   A "Successfully upgraded to version ..." message indicates a successful upgrade.

6. Click **refresh now** to refresh the web page immediately, or wait for it to refresh automatically after 30 seconds.

   The new software version displays in the Current Version section of the Firmware tab.

## 20.8.4 Troubleshoot upgrade issues

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

- *Upgrade procedure already in progress*

  The unit received multiple upgrade requests at approximately the same time. However, only one request can be handled at a time. The later request receives this error message.

- *Invalid firmware file*

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

- *Device hardware is incompatible*

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

- *Firmware file is corrupt*

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

- *Rule validation failed*

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

- *Failed to write firmware to flash*

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

- *Failed to revert back to the factory firmware.*

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

## 20.8.5 Advanced

For various reasons you may want to downgrade the TC620 firmware to the original factory-installed image kept in the fixed image area. This can be done in the Advanced Settings section of the Firmware tab.

### ⏩ To revert to the TC620's fixed image

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

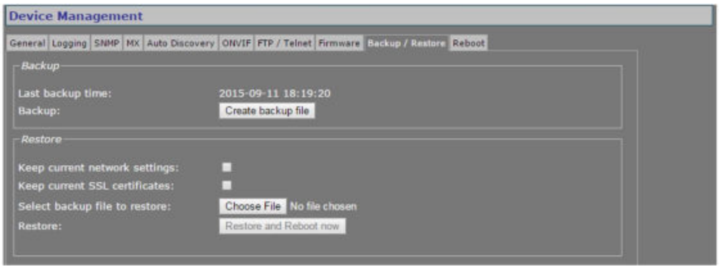
   Progress of the downgrade process is shown under the *Revert to factory version* button.

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

   A "Successfully reverted to version ..." message indicates a successful downgrade.
5. Click **refresh now** to refresh the web page immediately, or wait for it to refresh automatically after 30 seconds.
6. Log on to the unit again.

   On reopening the Firmware tab, the Current Version section has the version number of the factory-installed image.

# 20.9 Backup/Restore



Backup

Last backup time: 2015-09-11 18:19:20

Backup:

Restore

Keep current network settings: □

Keep current SSL certificates: □

Select backup file to restore: No file chosen

Restore:

*Device Management > Backup/Restore*

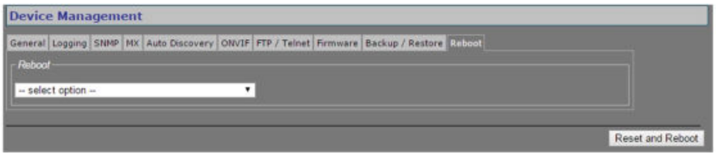
## 20.9.1 Backup

| Item | Description |
|---|---|
| Last backup time | Date and time of the most recent backup. |
| Backup | Saves the current configuration of the TC620 to the designated download folder. |

## 20.9.2 Restore

| Item | Description |
|---|---|
| Keep current network settings | Select to preserve the current network settings when you restore a backed-up TC620 configuration. |
| Keep current SSL certificates | Select to preserve currently installed SSL certificates, if any, when you restore a backed-up TC620 configuration. |
| Select backup file to restore | Browse for and select the backed-up TC620 configuration you wish to restore. |
| Restore | Starts the restore process using the selected backup file. |

# 20.10 Reboot



*Device Management > Reboot*

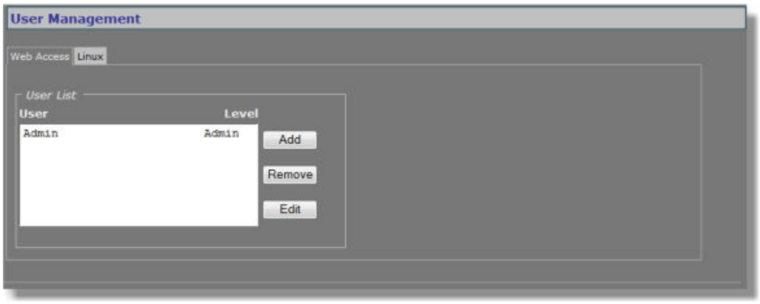
| Item | Description |
|---|---|
| Reboot | Reboots the unit without resetting variables. |
| Reset to factory settings: keep network settings | Reset option for all variables that can be set by the user, with the exception of the network settings. |
| Reset to factory settings; incl. network settings | A complete reset which will restore the unit's settings, including the IP address/subnet mask, to their original, default values. This could make the unit unreachable for in-band communications, in which case the internal web pages are accessible only by (temporarily) moving a PC to the same subnet as the TC620. |

# 21 User Management

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

## In This Chapter

## 21.1 Web Access



*User Management > Web Access*

### 21.1.1 Access control

The TC620 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 TC620 supports up to 20 users at a time.

**Important:** On upgrading a TC620 to firmware version 4.0 and higher, all existing users are deleted. After a successful upgrade, you can access the webpages with the default Admin account (user name = Admin; password = 1234).

### 21.1.2 Manage user accounts

#### ⏩ To add a user

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

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

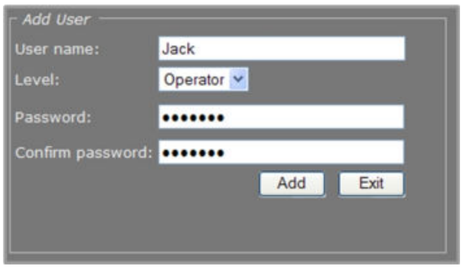
The Add User section displays.

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

4 Select the appropriate access level.

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

The user is added to the User List.



Add User

User name: Jack

Level: Operator

Password: •••••••

Confirm password: •••••••

*Adding a user*

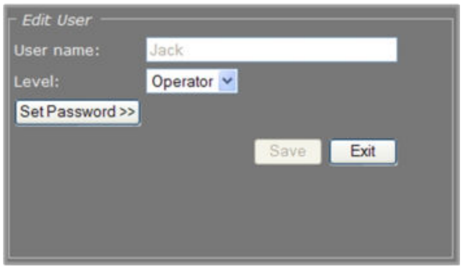
1 On the *User Management* page, open the **Web Access** tab.

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

The Edit User section displays.

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

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



Edit User

User name: Jack

Level: Operator

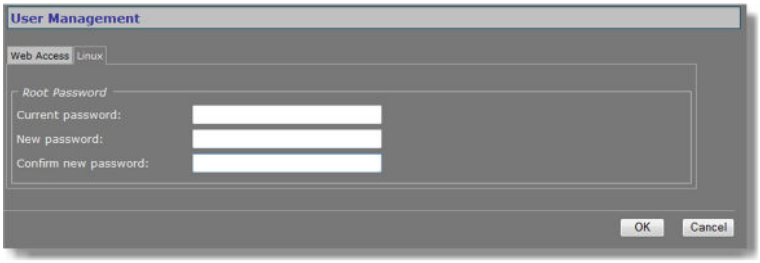
*Editing a user*

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

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

3 To confirm the deletion, press **OK**.

## 21.2 Linux



User Management

Root Password

Current password:

New password:

Confirm new password:

*User Management > Linux*

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

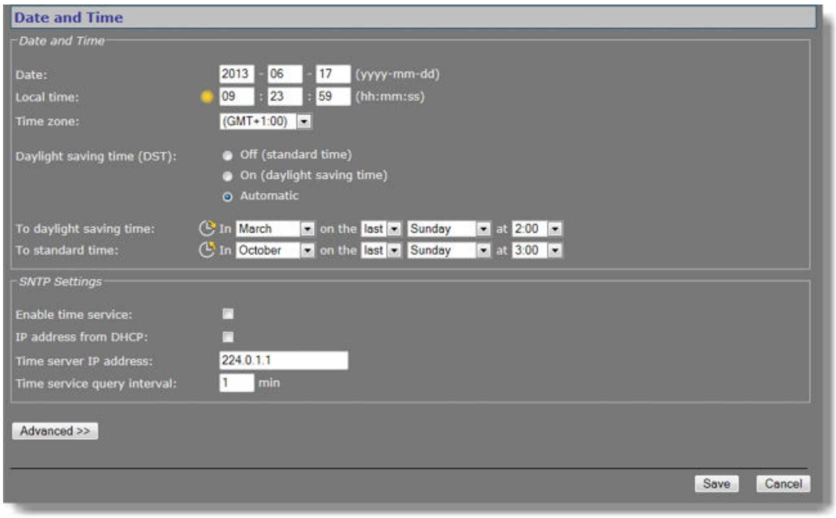
**Note:** Root account access requires that the Telnet service is enabled on the unit. For more information, see *Device Management > FTP/Telnet*.

# 22 Date and Time

The TC620 has a battery-supported real-time clock. This chapter explains how to adjust the date and time.

## In This Chapter

## 22.1 Date and time



Date and Time

*Date and Time*

Date: 2013 - 06 - 17 (yyyy-mm-dd)

Local time: 09 : 23 : 59 (hh:mm:ss)

Time zone: (GMT+1:00)

Daylight saving time (DST):
○ Off (standard time)
○ On (daylight saving time)
● Automatic

To daylight saving time: In March on the last Sunday at 2:00

To standard time: In October on the last Sunday at 3:00

*SNTP Settings*

Enable time service: □

IP address from DHCP: □

Time server IP address: 224.0.1.1

Time service query interval: 1 min

*Date and Time*

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

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

### ⏩ To set the date and time manually

1 In the SNTP Settings section, clear **Enable time service**.
This activates the Date and Local time text boxes.

2 Set the date and local time.

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

### ⏩ To disable Daylight saving time

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

### ⏩ To activate Daylight saving time manually

- Select **On (daylight saving time)**.

  This adds one hour to the currently configured local time. The unit will not automatically switch between summer and winter time.

### ⏩ To activate automatic Daylight saving time switchover

1. Select **Automatic**.
2. Use the *To daylight saving time* and *To standard time* lists to enter the appropriate start and end details.

   The unit will automatically adjust at the given dates and times.

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

## 22.2 SNTP Settings

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

### ⏩ To set up the TC620 for use with an SNTP server

1. In *SNTP Settings*, clear **Enable time service**, and then click **Save**.
2. In *Date and Time*, open the **Time zone** list, and then select your local zone.
3. Select the *Daylight saving time (DST)* option to be applied.
4. Click **Save**, and then wait for 2 seconds.
5. Set the **Date** and **Local time** values.

   A maximum error of 5 minutes is allowed for these settings.
6. Click **Save**.
7. In *SNTP Settings*, select **Enable time service**.
8. Select **IP address from DHCP** or specify the IP address of the time server.

   Assigning the IP address via DHCP requires that DHCP is enabled in section Advanced of the Network page.
9. Adjust the **Time service query interval** (if necessary), and then click **Save**.

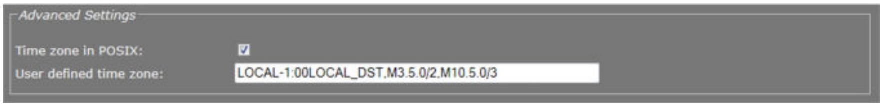
   The unit will now synchronise (within the interval set in the SNTP Settings section) to the time server and remain synchronised, also after reboots.

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

### Notes for advanced users

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

## 22.3 Advanced



Advanced Settings

Time zone in POSIX: ☑

User defined time zone: LOCAL-1:00LOCAL_DST,M3.5.0/2,M10.5.0/3

*Date and Time > Advanced*

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

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

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

### ⏩ To adjust the time zone and DST through POSIX

1 Select **Time zone in POSIX**.

2 In the *User defined time zone* text box, enter a valid POSIX time zone string.

If the string is recognised, the Date and Local time values in the Date and Time section are adjusted accordingly.

# 23 Multicast, multi-unicast, and port numbers

The TC620 can be used in a multicast setting. This chapter outlines IP multicast and one of its methods in particular: source-specific multicast. It then describes the concept of multi-unicast. You also learn about assigning valid port numbers.

## In This Chapter

## 23.1 Multicast

### IP multicast

The TC620 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 TC620 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 TC620 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 TC620, and the receivers to send and receive multicast messages. To define a multicast group, the source unit should be assigned a valid multicasting ('destination') TX stream address and the destination units should get this same address as source. IPv4 uses the address range 224.0.0.0 through 239.255.255.255 for multicast applications. The source unit has no knowledge of how many receivers there are. The group vanishes when the source is disabled, but the source will *not* automatically be disabled when the last remaining destination is cancelled and will keep transmitting at least towards the nearest switch. Additionally, it is possible to have the multicast group units send unsolicited membership reports, keeping it alive even if only one - any - unit of the group is still active.

### Source-specific multicast

The TC620 also supports source-specific multicast (SSM). This technique allows a receiver to specify a specific source sending to the multicast group and receive traffic originating from that source only. Singling out the source in this way can considerably reduce the network load. Note that SSM must be supported by the last-hop router and the receiver's operating system, and that the receiver requires IGMPv3 to be able to specify the specific source.

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

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

rfc4607
rfc4570
rfc3569
rfc5760

## 23.2 Multi-unicasting

As an alternative to multicasting, the TC620 features 'multi-unicasting', that is - sending out up to 2x3 independent copies of video, and 3 of audio, data and contact closure streams. If the bit rates selected are moderate, it may be more convenient to use this mechanism instead of multicasting, even though the network gets more signal to carry from the encoder.

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

## 23.3 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.

# Appendix: Enable Javascript

To have the TC620 webpages displayed correctly, JavaScript must be enabled in your web browser.

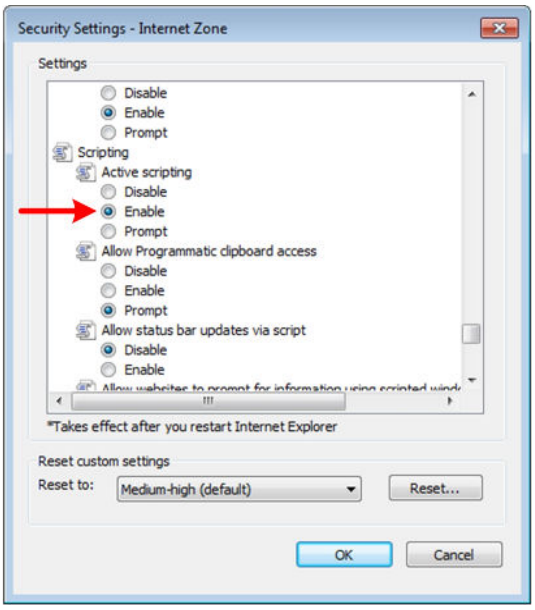
## ⏩ To enable JavaScript in Internet Explorer

1 On the *Tools* menu, click **Internet Options**.

2 On the *Security* tab, click the Internet globe icon, and then click **Custom level**.

3 On the *Settings* list, search for *Active scripting*, and then click **Enable**.

4 Click **OK**, and then close *Internet Options*.



Security Settings - Internet Zone

Settings

○ Disable
● Enable
○ Prompt
Scripting
Active scripting
○ Disable
● Enable
○ Prompt
Allow Programmatic clipboard access
○ Disable
○ Enable
● Prompt
Allow status bar updates via script
● Disable
○ Enable
Allow websites to prompt for information using scripted windo

*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium-high (default)

*Active scripting enabled*

# Appendix: Enable UPnP in Windows

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

## ⏩ To enable UPnP

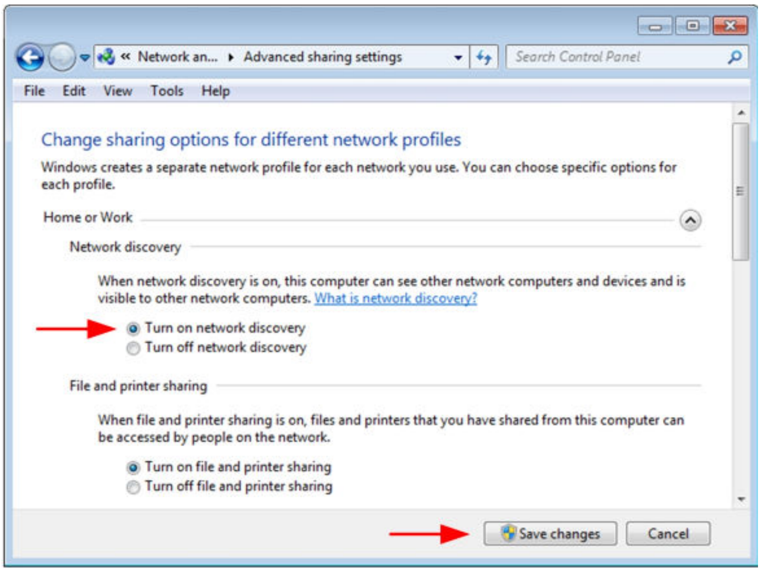
1 In *Control Panel*, click **Network and Sharing Center**.

2 In the left pane, click **Change advanced sharing settings**.

3 Under the relevant network profile, click **Turn on network discovery**.

4 Click **Save changes**

UPnP will automatically start when you turn on your computer.



Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Home or Work

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?

● Turn on network discovery
○ Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

● Turn on file and printer sharing
○ Turn off file and printer sharing

*Enable network discovery*

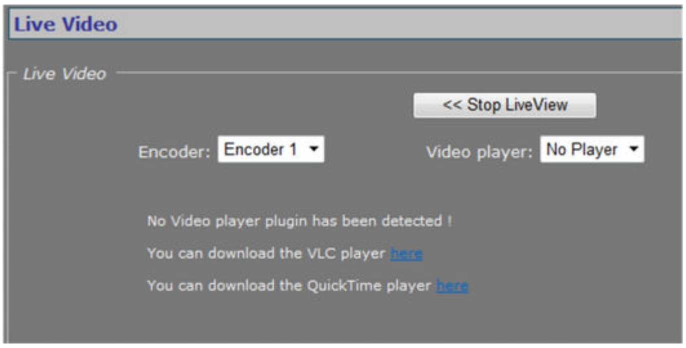
# Appendix: Install a video player

Viewing video streams on the webpages of the TC620 requires a video player installation on the machine running the web browser. This appendix provides instructions for installing QuickTime and VLC, the video plug-ins supported by the TC620.

### In This Chapter

## Download video player software

The TC620 supports QuickTime and VLC. If neither is detected when you attempt to open a video stream in the webpages, the Video player list indicates "No Player". You can use the hyperlinks on the webpage (see below) to download the required software.



Encoder: Encoder 1

Video player: No Player

No Video player plugin has been detected !

You can download the VLC player here

You can download the QuickTime player here

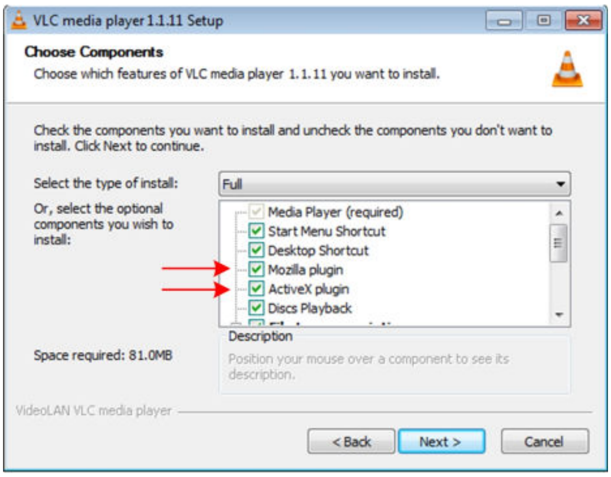
*Live Video page with video player download links*

## Install QuickTime

QuickTime installation is straightforward and self-explanatory.

## Install VLC

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



VLC media player 1.1.11 Setup

**Choose Components**

Choose which features of VLC media player 1.1.11 you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Full

Or, select the optional components you wish to install:

- ☑ Media Player (required)
- ☑ Start Menu Shortcut
- ☑ Desktop Shortcut
- ☑ Mozilla plugin
- ☑ ActiveX plugin
- ☑ Discs Playback

Space required: 81.0MB

Description

Position your mouse over a component to see its description.

VideoLAN VLC media player

*Required components: Mozilla and ActiveX plug-ins*

**Note:** The support of VLC, an open source community, may differ between releases. The TC620 has been successfully tested with VLC v2.1.0.

## VLC and Windows 7

### ⏩ To configure VLC media player settings when running this plug-in on a Windows 7 PC.

1 Open the VLC media player.

2 On the *Tools* menu, click **Preferences**.

3 In the *Show settings* section (lower left corner), click **All**.

4 Expand the **Video** list, and then click **Output Modules**.

5 In the *Video output module* list, click either DirectX video output, OpenGL video output, or Windows GDI video output.

6 Expand **Output Modules**, and then click **DirectX**.

7 Clear the **Use hardware YUV > RGB conversions** check box.

8 Click **Save**.

# Appendix: NTCIP configuration

The National Transportation Communications for ITS Protocol (NTCIP) provides a communications standard that ensures the interoperability and interchangeability of traffic control and Intelligent Transportation Systems (ITS) devices. This appendix provides information about the conformance groups which are supported by the TC620.

## In This Chapter

## Supported conformance groups

The TC620 firmware supports all the mandatory parts and some of the optional parts (see table below) of the NTCIP CCTV specification as laid down in the NTCIP 1205:2001 v01.08 document. This means that - in terms of section 4 of this document - the following conformance groups are supported.

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

*Conformance statement table*

### Configuration

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

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

## CCTV configuration

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

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

## Motion control

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

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

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

## SNMP MIB

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