XCU Series

Firmware version 2.19

Rugged and reliable IP cameras for challenging environments

User Manual

SIQURA

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

Copyright © 2018 Siqura B.V.

XCU Series 2.19
User Manual v2 (180511-2)
AIT55

Brand names

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

Liability

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

Although considerable care has been taken to ensure a correct and suitably comprehensive description of all relevant product components, this manual may nonetheless contain errors and inaccuracies. We invite you to offer your suggestions and comments by email via t.writing@siqura.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.
Meridiaan 32
2801 DA Gouda
The Netherlands

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

Contents

1 About this manual

What's in this manual

This is version 2 of the user manual for the XCU Series. This document describes:

- How to get access to the unit
- How to communicate with the unit
- How to operate the unit
- How to configure the settings of the unit

Where to find more information

Find product specific datasheets, manuals, EU Declarations of Conformity and firmware updates at http://siqura.com. Make sure that you have the latest version of this manual.

Who this manual is for

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

What you need to know

You will have a better understanding of how this product works if you are familiar with:

- Camera technologies
- CCTV systems and components
- Ethernet network technologies and Internet Protocol (IP)
- Windows environments
- Video, audio, data, and contact closure transmissions
- Video compression methods

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@siqura.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 http://siqura.com, gives a complete overview of open source libraries used by our video encoders and IP cameras.

2 Overview

In This Chapter

2.1 Features

XCU Series

- Single or dual imager
- 4x or 10x zoom full-HD optical camera
- Complete range of uncooled thermal imagers
- Corrosion-free 316L stainless-steel housing
- Compact and robust
- Plug & play
- Nano-coated optical window
- IP66/67
- ONVIF profile S compliant
- Perimeter Intrusion Detection

2.2 Description

The XCU Series is designed to operate in harsh and aggressive environments. Typical applications are found in the heavy industry, in traffic, tunnels, waterways, waste treatment and even in corrosive environments like the marine. The XCU Fusion combines a full-HD ultra-low light imager with an uncooled thermal imager for both day and night vision, while the XCU Compact can be fitted with either the low-light imager or a thermal imager.

3 Get access to the unit

From a standard browser on your PC, you can connect to the web interface of the unit. Use the webpages to view live video over the network and configure the settings of the unit. This chapter explains how to open the web interface in your browser.

In This Chapter

3.1 Get access via web browser

Connect to the unit from your web browser

1 Open your web browser.
2 Type the IP address of the unit in the address bar.
If no DHCP server is found on the network, the unit will revert to its factory-set IP address. This is the same IP address as that found on the sticker on the housing of the camera.
3 Press ENTER.
The Live Stream page is opened.
- or -
If user accounts exist on the unit, you are directed to the *login page* (see "*Log on to the unit*" on page 8).

3.2 Get access via Device Manager

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

Install Device Manager

1 Download the latest version of Device Manager at http://siqura.com.
2 Double-click the setup file.
3 Follow the installation steps to install the software.

Connect to the unit via Device Manager

1 Start Device Manager
The network is scanned.
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 perform a manual search, click the **Rescan** button.

3.3 Get access via UPnP

Universal Plug and Play (UPnP) support is enabled by default on the unit. With the UPnP service enabled in Windows, you can get access to the unit from Windows Explorer.

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 codecs and cameras with UPnP support.
2 Double-click the unit that you want to connect to.
The Live Stream page is opened.
- or -
If user accounts exist on the unit, you are directed to the *login page* (see "*Log on to the unit*" on page 8).

3.4 Log on to the unit

By default, users can freely open the web interface of the camera. They are not required to log on.

User authentication

If user accounts have been created and user authentication is activated, you encounter an authentication box when you connect. You are prompted to supply your user name and password. Only users with a valid account can log on.

Log on to the unit

1 In *User Name*, type your user name.
User name and password are case sensitive.
2 In *Password*, type your password.
3 Click **Log In**.

Use strong passwords

CAUTION: MAKE SURE YOU CREATE AN ADMIN ACCOUNT WHEN YOU OPEN THE WEB INTERFACE FOR THE FIRST TIME. TO KEEP THE ACCOUNT SAFE, SET A STRONG, COMPLEX PASSWORD. THIS HELPS TO PREVENT UNAUTHORISED ACCESS.

Create a strong password

- Use at least eight characters
- Do not include your real name, user name, company name, or other personal information
- Do not use complete words that can be found in a dictionary
- Use a random combination of at least two of the following categories: upper case letters, lower case letters, numbers and special characters

Note: For better protection, especially in high-security systems, we advise you to change the password at regular intervals.

4 Use the web interface

The built-in web interface makes it easy to operate and configure your product over the network. This section describes the layout and main features shared by the webpages.

Embedded Help

Help topics embedded in the webpages provide context-sensitive user assistance. For information about items and settings found on a page, click the question mark (*Show help)* in the Title bar of the page.

Note: The Embedded Help topics offer generic Help information for a range of Siqura products. Whether or not a described feature, mode or setting is available on the unit at hand depends on the model you purchased.

Home page

The Live Stream page is the home page of the unit. It is opened after successfully connecting to the web interface.

Note: Out of the box, the unit is freely accessible. You are not prompted to log on. To prevent unauthorised access, we recommend that you implement user authentication. This is done by creating user accounts and activating user login. For more information, see *User Management*.

Menu

Use the vertical menu on the left to navigate the web interface. Clicking a menu entry opens a page or a submenu.

Nice to know

To find a specific webpage quickly, type its name in the search-as-you-type box above the menu.

Layout

Webpages have a single-page layout or content is organised across a number of tabs. A tab contains related commands and settings. The title of the active tab is highlighted and underlined.

Previews

Pages such as *Live Stream*, *Image Settings*, and *Overlays* include a camera preview. You use it to view live video or determine the effect of your settings when you make changes.

Revert button

A *Revert* button appears when you adjust specific settings. It lets you undo your changes. The button is available until you leave the webpage.

Restore the setting to its original state (at the time of opening the webpage).

5 Live Stream

Functions available on the Live Stream page are model-based.

- View and record live video
- Take snapshots
- Turn on the washer and wiper
- Pan and tilt the camera
- Adjust the zoom, focus and iris

Layout

The Live Stream page is taken up entirely by the preview pane. This is where you can see video from the sensor(s) inside the unit.

Dual preview

On hybrid models, the page is opened in dual-preview mode with video from the optical sensor shown on the left and video from the thermal sensor on the right. Either of the previews can be brought to the foreground by going to single-preview mode. Use the direction buttons which appear when moving your mouse pointer over the preview pane.

	Show previous/next preview
	Show preview associated with selected option button

Toolbar

The buttons in the upper-right corner vary, based on your model.

	Hide PTZ controls		Show PTZ controls
	Wiper on		Wiper off
	Wash		
	Take snapshot		
	Start recording		Stop recording
	Full-screen		Close full-screen

PTZ controls

When viewing video from the optical sensor in single-view mode, PTZ controls can be displayed in the lower-left corner. This is done by clicking **Show PTZ controls** in the toolbar. Note that this button is hidden when PTZ control is disabled. The function can be enabled on the PTZ page.

Important: In the web interface and in this manual, these controls are referred to as "PTZ controls". Note, however, that fixed camera models do not have pan/tilt (PT) functionality. The zoom (Z) function is supported though - that is, if PTZ control is enabled.

Use the wiper

Clicking *Wiper on* activates the wiper function on the unit. The wiper remains active until you click *Wiper off* or until the time-out period (default: 5 s) expires.

Use the washer

Clicking *Wash* starts a washer sequence. The camera temporarily moves to the position required for the washer function and then returns to its previous position.

Take a snapshot

It is possible to take a snapshot of the video in the preview.

- Click **Take snapshot**.
  The picture is saved in JPG format to the designated folder.
  The file name includes the camera name and date/time information.

Record a live stream

A video stream shown in the preview can be recorded and downloaded to your PC.

1 Click **Start recording**.
  The button flashes red to show you started a recording.
2 To stop the recording, click **Stop recording**.
  The recording is saved in AVI format to the designated folder.
  The file name includes date/time information.

Enter full-screen mode

For better observation, you may want to enter full-screen mode.

- Click **Full-screen**.
  The preview fills the entire screen.
  Clicking *Close full-screen* or pressing [Esc] on your keyboard takes you back to standard mode.

Video streaming

Video streaming can be started and paused with the **Play** and **Pause** buttons in the centre of the preview. These buttons are available when the PTZ controls are hidden.

	Play live video stream
	Pause live video stream

Pan/Tilt the camera

A PTZ camera connected to the unit can be controlled from the Live Stream page.

1 Go to the PTZ page to make sure that PTZ control is enabled for the camera.
2 If the PTZ controls are hidden, click **Show PTZ controls**.
3 To pan/tilt the camera, drag your mouse pointer across the preview in the direction you need.
  Clicking in the preview also moves the camera.

Nice to know

In case of a power failure, the unit automatically resumes its prior position when it is powered on again.

Adjust zoom, focus, and iris

To zoom the camera or adjust the focus and iris, use the sliders in the lower-left corner for manual adjustment. Drag the slider to the left or right and watch the preview until you achieve the desired effect. For instant automatic focus adjustment, click the *Focus now* button.

Create a PTZ preset

Camera positions can be stored as PTZ presets.

1 Pan, tilt, zoom and focus the camera as needed.
2 Click **Store current position as preset** (the Star button).
The preset is added to the list with a number to identify it.
3 Type a descriptive name in the Preset text box.
You can also name and rename presets on the PTZ page.

Recall a PTZ preset

Camera positions stored as PTZ preset can be recalled.

- In the **PTZ preset** list, click the required preset.
The camera adopts the recorded position.

Delete a PTZ preset

Camera positions stored as a PTZ preset can be deleted when no longer needed.

1 In the **PTZ preset** list, click the preset you want to delete.
2 Click **Delete preset** (the Recycle button).
Note that a deleted preset is irretrievably lost! You are therefore asked to confirm the deletion.
You can delete multiple presets in one go on the PTZ page.

6 Camera

In This Chapter

6.1 Camera Management

Camera Management is where you can give the camera a name, change the aspect ratio, set the video output mode, and turn on mirrored horizontal view, mirrored vertical view and digital zoom. On hybrid models, there are separate tabs for optical and thermal camera management settings.

Name

Type a unique, descriptive name in the *Name* box for easy identification of the unit on the network. The name can be enabled as an overlay so that it is visible in the web interface previews and in video streams transmitted by the unit.

Aspect ratio

This setting lets you adjust the proportional relationship between the width and the height of the preview images shown in the web interface.

Output mode

Depending on the configuration of your camera, the unit can stream high-definition video (1080p) at 25 or 30 frames per second (fps) or at 7.5 or 8.33 fps. Note that the mode selected here determines the available frame rates on the Streaming Profiles page. For optical sensors, it is recommended to select an output mode with which the frequency of the local power grid is an exact multiple of the frame rate. When used in an area with 50 Hz power, for example, it is recommended to use 25 fps, while 30 fps is best in areas with 60 Hz power.

Mirror horizontal

This function flips the image horizontally to create a mirrored effect.

Nice to know

In a control room, this function can be used to make traffic go in the same direction on all monitors, which is less fatiguing for the operators.

Mirror vertical

This function flips the image vertically to create a mirrored effect.

Digital zoom

Note: Availability of this feature depends on the model at hand.

Digital zoom makes it possible to zoom further in digitally on the image when the camera has reached the full optical zoom level. The camera enlarges the area at the centre of the image and trims away the edges. Image quality is reduced when you use digital zoom.

6.2 Image Settings

Layout

The Image Settings page is made up of the preview and a semi-transparent settings pane which partly covers the preview. The settings pane can be lowered to bring the preview to the foreground.

Lower the settings pane

Click the down arrow at the top of the transparent pane to lower it.

Raise the settings pane

Click the horizontal bar under the preview to raise the settings pane.

PTZ controls

The PTZ controls can be overlaid on the preview, as described for the Live Stream page. Use the PTZ button in the upper-right corner to display/hide the controls.

Tabs

The image settings are grouped across multiple tabs on the Settings pane.

Profiles

Above the Image Settings tabs you find the Profiles section. Combinations of settings made on the Image Settings page can be saved here as profiles, to be used for specific applications.

Create a profile

1 In the *Profile* section at the top of the Settings pane, click the leftmost button to open the **Profile** list.
2 Select the profile you want to use as a basis for the new profile.
3 On the Image Settings tabs, configure the settings specific for the new profile.
4 Click **New**.
5 In **Profile name**, type a descriptive name for the profile.
6 Click **Save**.
The profile you started with, plus your changes are saved under the new name.
The new profile is added to the user section of the Profile list.

Apply a profile

1 In the *Profile* section, click to open the **Profile** list.
2 Click the profile you need.
The camera view is updated and adopts the settings of the selected profile.

Delete a profile

Important: Note that a profile that you delete cannot be retrieved!

1 In the *Profile* section, click **Select profile(s) to delete**.
2 In the *user* section of the *Profile* list, select the check box of the profile that you want to delete.
A profile that is currently active does not have a check box.
Unlike profiles created by the user, factory profiles cannot be deleted.
3 Click **Delete profile**.

6.2.1 Exposure

Exposure is the amount of light received by the image sensor and is determined by how wide you open the lens diaphragm (iris adjustment), by how long you keep the sensor exposed (shutter speed), and by other exposure parameters.

Note: Exposure modes and settings on this page vary from model to model.

Exposure mode

Use this list to select the exposure mode.

- *Auto*
  Shutter speed, iris and gain are controlled automatically based on the ambient light level.
- *Shutter priority*
  The shutter speed takes main control of the exposure. Iris and gain are adjusted automatically.
- *Iris priority*
  The size of the iris opening (aperture) takes main control of the exposure. The shutter time and gain are adjusted automatically. The iris can be set manually.
- *Bright*
  The shutter speed keeps its current value. Using the *Bright* slider, you can set a combination of gain and iris. This gives you a single control to adjust the exposure.
- *Manual*
  Shutter speed, iris and gain can be adjusted independently according to the ambient light level.

Actual shutter

Shows the current shutter time with the selected exposure mode.

Minimum shutter time

Use this list to adjust the minimum shutter time. Longer shutter times result in more motion blur, but they admit more light to the sensor.

Maximum shutter time

Use this list to adjust the maximum shutter time. Shorter shutter times reduce motion blur, but they admit less light to the sensor.

Auto slow shutter

Select *Enable* to allow shutter times slower than the frame time. With this function enabled, the camera lowers the frame rate of the camera in low-light conditions. This reduces the noise level, but results in fewer frames per second.

Manual shutter

Use this list to adjust the shutter speed. Decreasing this value causes the camera sensor to pick up less light, but reduces motion blur.

Actual iris

Shows the actual aperture size of the lens (iris) with the selected exposure mode.

Manual iris

Use this slider to adjust the iris. Increasing this value reduces the amount of light reaching the sensor of the camera, but increases the depth of field of the image.

Actual gain

Shows the current amount of gain with the selected exposure mode.

Maximum auto gain

Use this slider to adjust the maximum gain that can be used by the camera. A higher gain level results in more noise in the image.

Manual gain

Use this slider to adjust the gain. Increasing the gain results in a brighter picture but also produces more picture noise.

Manual brightness

Aided by the visual feedback from the camera view, use this slider to adjust the gain and iris values in one go. The *Actual gain* and *Actual iris* values are updated as you move the slider.

EV compensation

Use this function to compensate the exposure value (EV).

- Selecting a positive value produces a brighter picture but it may cause overexposure. You can also consider using the *Highlight correction* function to get more brightness.
- Selecting a selecting a negative value produces a darker picture but it may cause underexposure. You can also consider using the *Wide dynamic range* function to get more darkness.

Wide dynamic range

The wide dynamic range (WDR) function helps the camera provide clear images when there are both very bright and very dark areas simultaneously in the field of view. WDR balances the brightness level of the whole image to provide clear images with details. To prevent the loss of scene details, bright areas are not saturated and dark areas are not too dark.

Wide dynamic range mode

Use this function to select the wide dynamic range mode:

- *Multi exposure*
  The camera makes multiple exposures for the same image. Brighter areas of the image will be captured using shorter exposure times and darker areas of the same image will be captured using longer exposure times. This option will result in an excellent wide dynamic range, but possibly with some 'ghosting' for fast-moving objects.
- *DWDR*
  The camera makes only one exposure for each image and will digitally compensate for brighter and darker areas of the image.

Wide dynamic range level

Use this function to adjust the level of WDR compensation.

Backlight compensation

Backlight compensation (BLC) brings more detail to the dark areas of an object when a strong light source shining on it from behind makes it too dark to be seen clearly. To prevent the object from appearing as a silhouette, the exposure of the entire image is adjusted to achieve a usable light level for the object in the foreground.

Highlight correction

A small but very bright part of the image (for example, headlights of a car or the reflection of the sun in a window) can cause the entire image to become underexposed. Setting the *Highlight correction* function to *Low*, *Mid* or *High* compensates for exposure by strong sources of lights to enhance the overall image quality. This makes it possible to easily read the number of vehicles and number plates in an indoor parking area or outdoors at night.

6.2.2 Zoom/Focus

Note: Availability of this feature depends on the model at hand.

Auto focus mode

The Auto focus (AF) function provides two modes to automatically adjust the focus position.

- *Normal*
  This is the normal mode for AF operations.
- *Interval*
  Use *Auto focus interval* mode to set the interval between AF movements. If there are frequent changes in the camera scene you may want to set a longer interval to prevent frequent AF movements. The time intervals for AF movements and for the timing of the stops can be set in one-second increments using the *Auto focus move time* setting. The default setting for both is set to five seconds.

Auto focus sensitivity

The switching of AF sensitivity can be set.

- *Normal*
  Reaches the highest focus speed quickly. Use this when shooting a subject that moves frequently. Usually, this is the most appropriate mode.
- *Low*
  Improves the stability of the focus. When the lighting level is low, the AF function does not take effect, even though the brightness varies, contributing to a stable image.

Adjust zoom and focus

To zoom the camera or adjust the focus, use the sliders for manual adjustment. Drag the slider to the left or right and watch the preview until you achieve the desired effect. For instant automatic focus adjustment, click the *Focus now* button.

6.2.3 White Balance

Note: Available white balance modes and settings on this page vary from model to model.

A camera needs to measure the quality of a light source and create a reference colour temperature in order to calculate all the other colours. The unit for measuring this ratio is in degree Kelvin (K). Users can select one of the White Balance control modes, according to the operating environment. The table below provides the colour temperatures of some light sources as a general reference.

Light source	Colour temperature in °K
Cloudy sky	6000 to 8000
Noon sun and clear sky	6500
Household lighting	2500 to 3000
75 W Light bulb	2820
Candle flame	1200 to 1500

White balance

A variety of white balance modes is available to correct the colour of different types of light. When you select a mode, the effect of the setting is visible in the preview and the *Actual white balance blue* and *Actual white balance red* values (unavailable in *Manual* mode) are also updated.

- *Auto*
  Using colour information from the entire screen, the camera detects a colour temperature range and calculates an optimal white balance. It corrects the colours using the colour temperature radiating from a black subject based on a range of values from 2500 K to 7500 K.
- *Auto tracing*
  The camera continuously adjusts the colour balance to changes in the colour temperature which may occur. *Auto tracing* is suitable for environments with light sources ranging from 2000 K to 10000 K.
- *Auto outdoor*
  This is an auto white balance mode specifically for outdoor environments. It allows you to capture images with a natural white balance in the morning and evening.
- *Auto sodium lamp*
  The camera automatically compensates for sodium vapour lighting to restore objects to their original colour.
- *Auto outdoor sodium lamp*
  This is an auto white balance mode specifically for outdoor sodium vapour lighting, as used in street lamps, for example.
- *Indoor*
  3200 K Base mode. The camera adjusts the white balance to a colour temperature range suitable for indoor lighting conditions.
- *Outdoor*
  5800 K Base mode. The camera adjusts the white balance to a colour temperature range suitable for outdoor lighting conditions.
- *Sodium lamp*
  This is a fixed white balance mode specifically for sodium vapour lamps.
- *One push*
  Sets the white balance to the optimal white balance currently calculated by the camera.
- *Manual*
  Aided by the visual feedback from the camera view, you can change the white balance value manually by adjusting the *White balance blue* and *White balance red* sliders.

Actual white balance blue

Value showing the current white balance blue level.

Actual white balance red

Value showing the current white balance red level.

White balance blue

Adjusts the white balance blue level.

White balance red

Adjusts the white balance red level.

Adjust white balance

Sets the white balance to the optimal white balance currently calculated by the camera.

6.2.4 Day/Night

Note: Availability of this feature depends on the model at hand.

An infrared (IR) cut-filter can be removed from the image path for increased sensitivity in low-light environments. The filter can automatically engage depending on the ambient light, allowing the camera to be effective in day/night environments.

IR cut filter

The IR cut filter can be set to *Auto*, *On*, and *Off*.

- *Auto*
  Auto mode automatically switches the settings needed for attaching or removing the IR cut filter. With a set level of darkness, the IR cut filter is automatically disabled (Off), and the infrared sensitivity is increased. With a set level of brightness, the IR cut filter is automatically enabled (On).
- *On*
  The IR cut filter is enabled. Use this mode when there is sufficient light (day mode).
- *Off*
  The IR cut filter is disabled. The camera is more sensitive, especially to infrared light. The image becomes black and white.

IR cut filter threshold

In dark conditions (night time, iris extremely closed or extremely short shutter times), the gain of the camera will increase. Use the IR cut filter threshold slider to determine at which gain level the IR cut filter should be removed to allow more light to reach the camera sensor.

High sensitivity

Increases the maximum gain, which makes it possible to produce a brighter output even in a darker environment.

6.2.5 Appearance

Brightness

Use this function to adjust the brightness level of the video images to your viewing conditions.

Contrast

Use this function to adjust the contrast level of the video images to your viewing conditions.

Sharpness

Use this function to adjust image sharpness to your viewing conditions.

Color saturation

Use this function to adjust the intensity (purity) of the colours in the video images.

Hue

Use this function to enhance the colours in the video images if they do not look natural.

6.2.6 Enhancement

Note: Settings on this page vary from model to model.

Stabilizer

The camera system can provide image stabilisation to compensate for small amounts of camera shake. Available options: *Off*, *On*, and *Hold*. Select *Hold* if you want to keep the current image steady.

High resolution

This mode enhances edges and produces images of higher definition.

Noise filter

The NR function can remove noise (both random and non-random) to provide clearer images. You can control the level of noise reduction with the *Noise filter strength* slider.

Noise filter strength

Sets the level of noise reduction. The noise reduction effect is applied in levels based on the gain and this setting value determines the limit of the effect. In bright conditions, changing the noise reduction level does not have any effect. This function is available if *Noise filter* is selected.

Defog

Enhances low-contrast images - in foggy weather conditions, for example - to make them stand out more clearly. Available levels: *Off*, *Low*, *Medium*, and *High*.

Highlight mask level

Use this function to mask extremely bright parts of the image with a grey colour.

Picture effect

Includes the following modes.

- *None*
  Does not apply any picture effect.
- *Negative art*
  Reverses negative and positive. Black, white, and colours are reversed.
- *Black and white*
  Produces a black and white (monochrome) image.

6.3 Thermal Settings

Note: Availability of this feature depends on the model at hand.

The Thermal Settings page is where you configure the settings for video from the thermal sensor. Changes you make are immediately applied and shown in the preview.

6.3.1 Color palette

Palette

Use the Palette list to select a colour palette which will map temperatures to colours.

6.3.2 Isotherm

The Isotherm tab is available on models which support hotspot detection and flare stack monitoring.

Temperature ranges

In *Isotherm* mode, the mapping of temperatures to the colour palette is divided into four ranges. The boundaries of these ranges are specified by *Lower threshold*, *Middle threshold*, and *Upper threshold* values.

Clip at

The top of the palette and thus the maximum displayed temperature, is specified by the *Clip at* value. Note that the consecutive values must be incremental.

Isotherm enable

In Isotherm mode, absolute temperatures can be measured - that is, the ones above the Lower threshold. If you select Isotherm enable, all temperatures above the Lower threshold are mapped to colours. Temperature values are shown next to the colour palette. If you clear the Isotherm enable check box, all temperatures are mapped to colours unless you select one of the grayscale palettes (White Hot or Black Hot).

Detection

Automatic hotspot detection and flare monitoring require *Isotherm* mode. Detection is possible using detection zones (see the description in the *Detector* section). Alarm events are generated by any object with a temperature above the configured *Lower threshold* appearing in a zone or a flare entering the "Flare active" or "Flare too large" zone.

6.3.3 Image mode

Range

The camera can visualise temperatures from -40 °C to +160 °C with a Noise Equivalent differential Temperature (NEdT) of 50 mK, or visualise temperatures from -40 °C to +550 °C with an NEdT of 500 mK. In *Auto* mode, the camera itself decides which range to choose based on the scene.

Contrast

Use the Contrast slider to decrease or increase the contrast of the image. When you increase contrast, dark scene content is displayed darker and light scene content with greater brightness.

Sharpness

Use the Sharpness slider to soften or sharpen the image.

Max calibration interval

The sensor inside the unit 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. Use the Max calibration interval slider to control the calibration interval duration to meet the ambient conditions.

Max AGC gain

Use the Max AGC gain slider to optimise the signal level and brighten video images to compensate for low-contrast conditions. Note that a high AGC gain level can introduce noise into the picture.

AGC region

The AGC region defines the part of the scene to be used as a basis for calculating AGC adjustment.

6.3.4 Radiometry

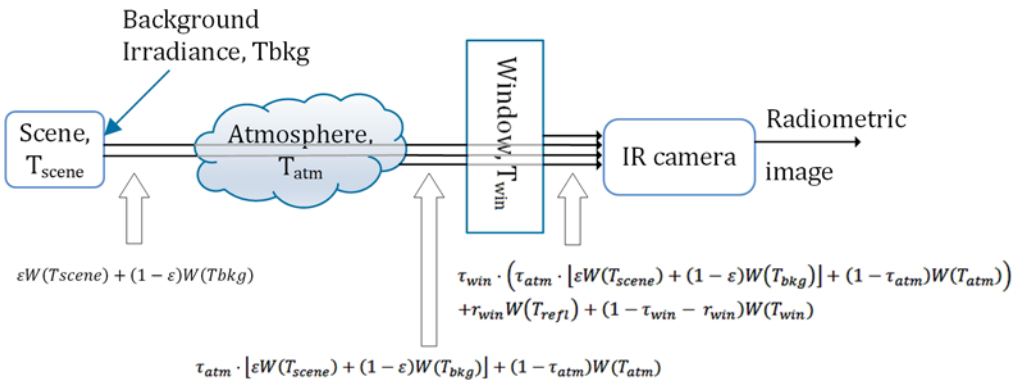
This tab is available on models with radiometric functionality.

Temperature compensation

The camera can compensate the temperature reading for scene emissivity and window transmission and reflection (if applicable).

The correction for emissivity and window factors has been extended to include corrections for atmospheric transmission. The model is based on the fact that the radiation from the scene is attenuated by the absorption along the path and the absorbing elements are emitting radiation related to the temperature of the element.

The following model is used for the temperature compensation:



The incident radiation onto the camera is given by:

$$S = \tau_{win} \cdot \left(\tau_{atm} \cdot \left[\varepsilon W(T_{scene}) + (1-\varepsilon) W(T_{bkg})\right] + (1-\tau_{atm}) W(T_{atm})\right) + r_{win} W(T_{refl}) + (1 - \tau_{win} - r_{win}) W(T_{win})$$

Notation	Description
S	Video input data
ε	Target emissivity (emissivity of the scene)
τ_{win}	Window transmission (transmission coefficient of the window)
T_{win}	Window temperature
r_{win}	Window reflection
T_{refl}	Temperature reflected in the window

Notation	Description
τ_{atm}	Atmospheric transmission (transmission coefficient of the atmosphere between the scene and the camera)
T_{atm}	Atmospheric temperature
T_{bkg}	Background temperature (reflected by the scene)
T_{scene}	Scene temperature
W(T)	Radiated flux (in units of counts) as function of the temperature of the radiating object.

6.4 Overlays

On the Overlays page, text and images can be superimposed on the video streamed by the unit. You can, for example, have the camera name, date and time information, measurements, a custom text or a logo displayed.

Layout

The greater part of the Overlays page is taken up by the preview. To the right of it, you find the functions for overlay creation, overlay alignment, font management and image management.

Section	Functions
Overlay settings	▸ Add/Modify/Delete text overlays ▸ Add/Modify/Delete an image overlay ▸ Set overlay position ▸ Set overlay appearance
Overlay alignment	▸ Move overlay to left/right
Font management	▸ Upload/Delete a font
Image management	▸ Upload/Delete an image

Toolbar

Availability of overlay toolbar buttons varies from model to model.

Button	Name
	Add text overlay
	Add image overlay
	Show/Hide blobs
	Show/Hide configuration
	Show/Hide alarms
	Show/Hide palette

Add a text overlay

You can add up to three text overlays.

1 In the toolbar, click **Add text overlay**.
A shape with a green border is added to the preview.
2 Click the shape to open the shape settings.
3 Type your custom text in the text box located in the *Selected shape* section.
- or -
Click the button to the left of the text box, and then select a predefined entry.
It is possible to reopen the list and click a different entry to append to the selection already in the text box.
4 In the *Render mode* list, select **Outline** or **Border** as needed.
Your adjustment is immediately effective. See the preview for visual feedback.
5 Click **Position**.
6 In the **Position** list, select a preset position.
- or -
Click **Free positioning** and type custom values in the **X position** and **Y position** boxes to freely place the shape over the video image. Using the options in the **Anchor point** list, you can shift the object relative to the anchor point.
You can also position the shape using a drag-and-drop operation.
7 (Optional) Use the **Rotation angle** slider to rotate the text.
8 Click **Colour.**
9 Select a font colour and a border colour.
10 (Optional) Drag the **Transparency** slider to set the transparency level of the text.
11 Click **Font.**
12 Select the font to be used.
Using the Font management section, you can upload your own fonts to the unit.
13 Enter the font size.
As an alternative, you can freely adjust the font size by dragging the resizing handles of the shape.

Add an image overlay

An image that you have uploaded via Image management can be overlaid on the video.

1 In the toolbar, click **Add image overlay**.
An image shape is added to the preview.
2 Click the image to open the shape settings.
3 In the *Image* list, select the image to be used.
4 Click **Position**.
5 In the **Position** list, select one of the preset positions.
- or -
Click **Free positioning** and type custom values in the **X position** and **Y position** boxes to freely place the shape over the video image. Using the **Anchor point** setting, you can shift the shape relative to the anchor point.
You can also position the shape using a drag-and-drop operation.
6 Click **Advanced**.
7 (Optional) Drag the **Transparency** slider to set the transparency level of the image.
8 (Optional) Drag the **X scale** and **Y scale** sliders to adjust the scaling of the image.
As an alternative, you can freely adjust the scaling by dragging the resizing handles of the shape.
9 (Optional) If your overlay is an animated GIF image, define its speed in **Animation speed**.

Delete an overlay

1 Click the overlay shape in the preview.
2 In the *Selected shape* section, click the **Recycle Bin** button.

Show and hide blobs

You can show or hide blobs, i.e. lines, around detected objects.

1 In the toolbar, click **Show blobs**.
Lines will be shown around all objects that exceed the temperature threshold set in the *Thermal settings* page.
2 Click **Hide blobs** to hide the blobs again.

Show and hide configuration

You can show or hide the contours of one or more zone(s) set in the *Detector* page.

1 In the toolbar, click **Show configuration**.
A shape will be shown around each zone set in the *Detector* page.
2 Click **Hide configuration** to hide the shape again.

Show and hide alarms

As soon as a blob enters a zone or if a blob appears inside a zone, an alarm may be shown.

1 In the toolbar, click **Show alarm**.
A red line will be shown around the zone and the detected object(s) as soon as a blob enters a zone or appears inside a zone.
2 Click **Hide alarm** to hide the red line again.

Show and hide palette

You can show or hide the colour palette in the preview.

1 In the toolbar, click **Show palette**.
The colour palette will be shown in the preview. It shows the colours associated with the temperatures set in the *Thermal settings* page.
2 Click **Hide palette** to hide the colour palette again.

Align overlay

In the *Align overlay* section, you can align the shape around a zone in the preview to the left or the right. This may be useful if the shape does not properly cover the object to be detected.

1 Click **Shift left** to move the zone to the left in small (one-arrow button) or bigger (two-arrow button) steps.
2 Click **Shift right** to move the zone to the right in small (one-arrow button) or bigger (two-arrow button) steps.

Upload a font

1 Click the **arrow** which expands *Font Management*.
2 Drag the font file onto the dashed rectangle.
- or -
Use **Click to select file** to locate and select the file.
3 Click **Upload**.

Delete a font

1 Click the **arrow** which expands *Font Management*.
2 Click **Select font to delete**.
3 Click the font you wish to delete.
4 Click **Delete**.

Upload an image

1 Click the **arrow** which expands *Image Management*.
2 Drag the image file onto the dashed rectangle.
- or -

Use **Click to select file** to locate and select the file.
The unit supports .GIF and .JPG files.

3 Click **Upload**.

Delete an image

1 Click the **arrow** which expands *Image Management*.
2 Click **Select image to delete**.
3 Click the image you wish to delete.
4 Click **Delete**.

6.5 Streaming Profiles

Per sensor (optical and/or thermal), the unit has multiple-stream capability for simultaneous streaming of one or more H.264 streams, combined with MJPEG. Two independent H.264/MJPEG encoders can generate full-HD 1080p video streams at full frame rate. Multiple combinations of resolution and frame rate can be configured to satisfy different live viewing and recording scenarios.

Max streams

The following streaming limits apply:

- A maximum of 20 streams per encoder
- A maximum of 50 streams in total for the unit
- A maximum of 80 Mbps in total for the unit

Streaming profile types

A straightforward method of configuring the encoding settings for a video stream is to use a *factory-set* streaming profile - that is, a predefined combination of settings for a specific application. The unit offers profiles optimised for video storage, PTZ, or high-quality live viewing, for example. If none of the factory profiles meets your requirements you can create and save *user-defined* streaming profiles.

Use a factory-set profile

A factory-set streaming profile defines the settings that the unit will use for the application indicated by the profile name.

1 At the top of the page, click **Stream 1** or **Stream 2** to select the stream to assign the streaming profile to.
2 In the **Profile** list (below the *Stream* tabs), select the factory profile which is appropriate for (or comes closest to) the intended purpose.
3 Repeat steps 1 and 2 for the other stream, if necessary.

Factory profile settings

When you select a factory profile, the video stream will be encoded with the settings shown below the profile list. For several of these settings, the *actual* value is shown to the right of the defined value.

Create a custom profile

As an alternative to using the factory-set profiles, you can create and use custom streaming profiles.

1 At the top of the page, click **Stream 1** or **Stream 2**, to select the stream to assign the streaming profile to.
2 In the **Profile** list, select the factory profile to be used as a basis for your custom profile.
3 Adjust the profile settings to your requirements.
The custom profile is added to the Profile list (User section) as: `Factory profile-Copy-yymmdd`.

4 To rename the profile, type a descriptive name into the **Name** box.

Delete a custom profile

Custom streaming profiles can be deleted (unlike factory-set profiles).

1 In the **Profile** list, select the profile to be deleted.
2 Click **Delete**.
3 In the information bar, click **Yes, delete** to confirm this action.

Name

Indicates the currently selected streaming profile. You can name and rename custom streaming profiles. The names of the factory-set profiles cannot be changed.

Encoder type

Depending on the application, select the video encoding method that is to be used to compress the video signal.

Frame rate

Here you can set the number of video frames per second for the video transmission. Range: 1-25 fps (PAL); 1-30 fps (NTSC).

GOP size

Determines the distance in frames between two I-frames.

Maximum bit rate

Here you can set the maximum bit rate allowed for the video transmission. You can use this setting to control the network load. The *actual* bit rate is shown to the right of the text box. This value is dynamically updated with the current bit rate to provide feedback on the bit rate that is used on average with the current *Maximum quality* setting.

Maximum quality

Generally speaking: the higher the Maximum 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. When configuring these settings it is good to keep the following in mind.

- If the configured Maximum quality cannot be achieved with the currently set Maximum bit rate, the actual quality will be lower. The actual quality percentage is shown real-time to the right of the configured Maximum quality.
- The actual quality level will never exceed the configured Maximum quality, even if the Maximum bit rate should allow it.

Resolution

Indicates the number of pixels that can be displayed in each dimension (width x height).

Traffic shaping

Traffic shaping sets the maximum network bit rate per encoder. Traffic shaping spreads network traffic bursts which helps the network infrastructure handle the traffic. In its turn, however, traffic shaping increases the latency.

- With traffic shaping set to *Off*, the stream is transmitted with minimum latency but with bursty network traffic.
- With traffic shaping set to *Low*, *Medium* or *High*, the network traffic is more evenly spread out in time, but the latency will increase.

Parameter value combinations

When you create a custom streaming profile, set sensible combinations of *Frame rate*, *GOP size*, *Maximum bit rate*, *Maximum long term bit rate*, *Maximum quality*, and *Resolution*. If in doubt about the effects of specific encoder settings, you are advised to select the factory-set profile offering the closest match to your required application.

Multi image mode

This option enables you to define how video from the optical and thermal sensors is shown in the preview pane.

- With the mode set to *Single*, only one preview is shown.
- With the mode set to *Side by side,* video from the optical sensor is shown side by side with video from the thermal sensor.
- With the mode set to *PIP,* video from the thermal sensor is shown as a picture in a picture (PIP) in one of the four corners of the video from the optical sensor.

Overlay

Use this option to enable or disable display of overlays for the selected stream.

- When *enabled*, any text or image overlays set in the *Overlays* page will be shown for the selected stream.
- When *disabled*, no text or image overlay will be shown for the selected stream.

6.6 PTZ

The PTZ page is where you enable/disable PTZ control and manage the presets you created on the Live Stream page. Presets can be renamed or deleted here. You can also add reserved presets.

Note: On fixed cameras, the term "PTZ" used in the web interface and in this Help topic, applies to the zoom (Z) functionality of the camera. Fixed cameras do not support pan and tilt (PT) operation.

PTZ control

On the Camera-# tab, select/clear the Enable check box to enable/disable PTZ operation from your web browser.

Nice to know

On fixed models, the zoom function is intended for use when the camera is being installed. Generally speaking, it will not be needed at a later stage. Therefore, we strongly advise the installer to disable PTZ control when the installation is complete. This will prevent users with a Viewer account from intentionally or unintentionally changing the zoom position of the camera.

Camera ID

In order to address multiple cameras on the same RS-485 bus, each camera needs to be assigned a unique ID. Make sure to set all connected cameras to a different ID on the camera itself, and then set the camera IDs for all cameras accordingly on this page.

1 Click the **Camera-#** tab.
2 In the **Camera ID** box, type the ID.

Rename a preset

A preset is automatically saved as "PTZ preset #" followed by the preset number. You may want to give it a more descriptive name for easier identification.

1 In the **Preset name** column, click the current name.
2 Type the new name.
The preset can now be found under the new name in the Preset list on the Live Stream page.

Add a reserved preset

Specific functions, such as a wiper/washer system (if supported), can be activated by working with reserved presets.

1 Click **Add Reserved Preset**.
A new row is added to the preset table.
2 Click the appropriate cell under *Preset number.*
3 Type the number that will activate the function.
4 Click the corresponding cell under *Preset name.*
5 Type a descriptive name.
The new preset is added to the preset list on the Live Stream page.

Delete PTZ presets

Note that it is not possible to undo the deletion of a preset!

1 Click to select the check box(es) of the preset(s) you wish to delete.
2 Click **Delete preset**.
You are asked to confirm the deletion.

Upload a PTZ driver

PTZ drivers not included in the factory-default driver list can be uploaded to the unit.

1 On the **Driver management** tab, click **Upload driver**.
2 Drag the driver file (with .js file extension) onto the dashed rectangle.
3 Click **Upload**.
The driver is added to the *User* section of the driver list.

Delete a PTZ driver

Uploaded drivers that you no longer need can be deleted. It is not possible to delete the factory-installed drivers.

1 On the **Driver management** tab, click the list of available drivers.
2 Click the driver you wish to delete.
3 Click **Delete**.

PTZ commands over TCP

The unit supports the streaming of PTZ data over TCP using a client/server connection. The TCP connection is bidirectional.

1 In the **Listening on port** box, specify the port on which the server listens for incoming TCP connections.
Range: [0 ... 65535]. Default: 1024.
2 To activate this function, select **Enable**.

Bit rate

Determines the speed of the digital transmission - that is, the amount of information transferred/processed per unit of time.

Word length

Determines the number of bits that is transferred in a single operation.

Stop bits

Indicates the end of a data character to enable the receiver to resynchronise with the stream.

Parity mode

Enables the sending of an extra bit with each data character for error detection purposes.

Wire mode

The RX-4xx interface type on the data connector is set in software. Select the required type in the *Wire mode* list.

Biasing

If biasing is needed, it should be enabled on at least one module on the bus.

Termination

Normally, the devices at the two extremes of a bus are terminated, while intermediate devices are not. Therefore: RS-422, always enable (being point-to-point); RS-485, enable only for the first and last module connected to the bus configuration.

6.7 Privacy Mask

On the Privacy Mask page, you can mask one or more specific areas of the video streamed by the unit.

Note: Availability of this feature depends on the model at hand.

Add a privacy mask

1 Click **Add privacy mask** in the upper-right corner of the preview.
A dashed shape is added to the preview.
2 Move the shape to the desired location in the preview.
3 (Optional) Drag the resizing handles of the shape to adjust the scaling.
4 (Optional) Change the colour of the shape by selecting a colour from the colour list in the lower-left corner of the preview.

Delete a privacy mask

1 Click the shape in the preview.
2 Click the recycle bin button in the upper-right corner.

7 Event

On the Event pages, you can define how the unit is to handle incoming events.

In This Chapter

7.1 Event Management

On the Event Management page, you can link actions to specific events. Once the event occurs, it triggers the selected action automatically.

Add an event

The Event Management page is blank when you open it for the first time. You can add events by selecting a trigger and linking an action to it.

1 Click **Add event**.
2 In the **Trigger** column, click **Select trigger**.
3 In the **Trigger** list, select the event that will set off the trigger action.
4 In the **Action** column, click the corresponding cell.
5 In the **Action** list, select the action to be taken when the event occurs.
The event is effective as soon as you have defined the trigger and the action.

Note: Make sure that the FTP server settings are configured correctly when you select "FTP image ..." as a trigger action.

Delete an event

1 Select the check box of the event you wish to delete.
2 Click **Delete event**.

7.2 Connection Monitor

The Connection Monitor function can monitor the network connection between the unit and a target host on the network. The unit pings the remote machine - that is, sends data packets to it, at intervals of 15 seconds to determine if the remote machine is accessible and responding.

Edge recording

To prevent loss of video when the connection to a central network video recorder or VMS system is lost, recorded video clips can be stored on the microSD card inside the edge device. From the Edge Recording page, the clips can then be downloaded for further processing.

Steps

Setting up the unit to record video to the SD card when a ping request times out without a response involves the following steps:

- On the *Recording* page, check the SD card status.
- On the *Event Management* page, add a "Connection # lost" trigger and link a "Start recording of Camera #" action.
- On the *Connection Monitor* page, set up and enable the Connection Monitor to monitor the connection to the VMS/NVR.

Note: On models with multiple sensors, a separate connection monitor (tab) is available per sensor.

Set up the connection monitor

1 In **IP address**, type the IP address of the remote machine that is to be pinged.
2 Click **Enable** to activate the monitor.
The connectivity status is given as "Connection present" or "Connection lost".
"Connection present" indicates that the remote machine responds to the ping requests.
"Connection lost" indicates a network failure.

Connection loss

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

- Edge recording starts at the first lost ping.

  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 for devices which have acknowledged their presence on the network at least once by responding to ping messages. This is to prevent unintended recording to the microSD card.

- The connection loss is reported in the *Connection Monitor* page: "Connection lost".
- The associated video clip appears in the *Available clips* section on the *Edge Recording* page with clip status shown as 'Recording'.
- Edge recording continues until the device becomes responsive to ping messages again - that is, on the next received ping.

7.3 Digital I/O

The number of digital I/O channels that is provided depends on your product.

Each of the I/O pins on the unit can function as a digital input or a digital output, but not simultaneously.

Set the pin mode

On the Digital I/O page, you can set the mode for each pin.
1 In the **Mode** column, click the required cell.
2 Select the desired mode.

Mode	Description
Force closed	I/O contact is closed
Input	I/O pin is input pin
Output (inverted)	I/O pin is output pin (output inverted)
Output	I/O pin is output pin

Link an action to a digital I/O event

On the Event Management page, you can add events triggered by "I/O # closed" and define actions to be taken when such events occur.

7.4 FTP Push

On the Event Management page, events can be set to trigger an FTP push. When such an event occurs, the unit posts a camera image on one or two FTP servers. A target server must hold a user account associated with the unit. If you assign two servers, images are posted simultaneously to FTP server 1 and FTP server 2.

7.4.1 Servers

Set up the FTP server connection

1 Select the **Enable** check box of **Send to this server**.
2 In **IP address**, type the IP address of the FTP server you want to use.
3 In **Port**, type the port number to be used.
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.
4 In **Name**, type the user name that is needed for authentication before you can access the server.
5 In **Password**, type the password that is needed for authentication before you can access the server.
6 (Optional) Repeat steps 1-5 for the second FTP server.

7.4.2 Camera-#

On the Camera-# tab, you can set the path to an FTP server and configure settings for continuous posting.

Server path

In the Server path box, type the name of the folder on the FTP server which is assigned to the FTP client. Example: `\Captures\Cam-` This can be used if the client is not allowed to access the server root folder.

Click **Test FTP settings** to make sure that the server path has been set correctly. A message in the top of the screen will indicate if the camera has been able to make a connection with the FTP server or not.

Continuous posting

Image upload to an FTP server can be event-triggered but you can also set it to be continuous.
1 In **Interval**, type a value to determine the interval between two image posts.
2 In **File name**, type a descriptive name or accept the default name.
With the append button you can add extra information to the file name.
3 To activate continuous posting, select **Enable**

8 Recording

The unit provides edge recording and NAS recording. The edge recording function makes it possible to record and store video locally - that is, on the microSD card inside the unit -, or on an external NAS server. From the Edge Recording page, the clips can be downloaded for further processing.

In This Chapter

8.1 Camera-#

Recording types

Two types of edge recording are available:

- Continuous recording
- Event-triggered recording

Recording source

Each camera input has multiple streams. In the **Recording source** list, select the stream to be recorded.

Recording destination

Recordings can be stored either on an SD card or a configured NAS server. In the **Recording destination** list, select the desired storage medium.

Continuous recording

Selecting *Enable* activates continuous recording of the chosen video stream to the microSD card. Recording continues until you clear the check box to disable the function.

Important: Recording in continuous mode for extended periods of time requires a microSD card with extended capacity.

Event-triggered recording

Unlike 24-hour recording by an NVR or VMS, event-triggered recordings are typically short recordings. Start and stop times for the recordings are triggered by specific external events. On the Event Management page, you can link a "Start recording" action to triggers such as:

- A lost connection to an NVR or VMS
- Camera tampering
- A closed I/O contact
- Image quality issues

Note: If you set connection loss as a trigger you need to set up the Connection Monitor to monitor the connection.

Persistent recording

Recording to the microSD card is persistent. This means that powering the unit off and on does not erase the existing recordings on the microSD card. Be aware, though, that the oldest recordings will be overwritten by new recordings when the card is 90% full.

Available 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.

Download a clip

1 In the *Available clips* section, click the clip's **Ready** or **Recording** status indication.
The file is saved to the designated folder on your PC.
2 In the information bar, click **Open** or **Show in folder**.
Clip names are created automatically using UTC date/time information.

Note: Downloading a clip to your PC does not remove the clip from the microSD card. You can delete clips manually on the Edge Recording page (see below).

Delete a clip

1 In the *Available clips* section, select the clip by clicking the check box.
2 Click **Delete selected clip**.

8.2 SD Card

microSD card

The unit supports µSDHC and XC cards with a maximum capacity of 32 GB. You can check the card storage capacity and available space through the *SD card* tab on the Edge Recording page. When the SD card is 90% full, new recordings will overwrite the oldest recordings.

Format the SD card

1 Click **Format SD card**.
2 To confirm, click **Yes, format**.
The existing data on the SD card is erased.

Maximum retention period

Indicates how long recordings will be stored on the SD card. If you set the maximum retention period to, for instance, 1 week, all recordings older than 1 week will automatically be deleted.

SD card usage

We advise to use high-grade, highly-durable microSD cards. Note that microSD cards are limited to the number of write cycles ranging from 200 (off-the-shelf TLC NAND) to 100.000 (industrial SLC NAND). Intensive usage will eventually wear out the card.

The number of write cycles times the capacity of the microSD card gives you the total amount of data that can be written to the card in its life time. A 32 GB microSDHC with 2000 write cycles, for example, can write 64 TB before it should be replaced.

Card status

Indicates the status of the SD card. Possible statuses are:

- *Not present*
  No SD card is found.
- *Not recognized*
  The SD card found is not recognized by the camera.
- *OK*
  The SD card is present and recognized.
- *Error*
  There is an unknown error with the SD card.
- *Formatting*
  The SD card is currently being formatted.
- Retrieving
  The SD card is currently being retrieved.

Card size

Indicates the total storage capacity of the SD card. The diagram indicates how much of the storage capacity is currently in use.

8.3 NAS recording

The unit supports NAS (Network Attached Storage) using the SMB/CIFS or NFS protocol.

Use NAS client

To activate the NAS client, select **Enable**.

8.3.1 Server settings

Type

In the **Type** list, select the protocol to be used for NAS storage: either SMB/CIFS (also known as SAMBA or Windows file sharing) or NFS.

Address

In the **Address** box, type the host name or the API address of the NAS server. Examples:

- 1.2.3.4
- storage-1.example.net

Path

In the **Path** box, type the name of the folder where the unit should store its recording data. For SMB/CIFS, the path always starts with the share name, followed by the directory in the share. Example: camera/camera0016.

User name

In the **User name** box, type the user name to be used to connect to the NAS server (only applicable for SMB/CIFS).

Password

In the **Password** box, type the password to be used to connect to the NAS server (only applicable for SMB/CIFS).

Bit rate limiting

If the unit is connected to a network with limited bandwidth, it is recommended to limit the bandwidth for communication to and from the NAS. This is to make sure that enough bandwidth remains available for other data, for example video streams.

Select the Enable check box to limit the bandwidth.

Bit rate limit

In the **Bit rate limit** box, type the number of kilobits per second to which you wish to limit the bandwidth for communication to and from the NAS.

Apply server settings

Click **Apply server settings** to apply all server settings at once.

Status

Indicates the status of the connection to the NAS server.

Storage size

Indicates the total storage capacity of the NAS server. The diagram indicates how much of the storage capacity is currently in use.

Maximum retention period

Indicates how long recordings will be stored. If you set the maximum retention period to, for instance, 1 week, all recordings older than 1 week will automatically be deleted.

9 Device

Users with an Administrator or Operator account have access to the Device pages. They can configure the device, network, date and time, security, and SNMP settings. Administrators can also manage user accounts.

In This Chapter

9.1 Device Management

On the Device Management page, you can restart the unit, reset it to the factory-default settings, create and restore backup files, and upgrade the firmware.

Name

Type a descriptive name in the *Name* box. This makes identification of the unit easier when you scan the network in Device Manager. The unit must be restarted for the change to take effect.

Description

Defines the device type.

Article code

Administrative information for article identification.

Serial number

Uniquely identifies the unit. You may be asked to provide this number when you contact our technical support.

Firmware version

Indicates the currently active firmware version.

Power mode

Indicates how power is supplied to the camera.

- *External/PoE+*
  Power is supplied via an external power supply or via PoE+.
- *PoE*
  Power is supplied via an ethernet cable (Power over Ethernet).

Sensor information items

The sensor information identifies the optical and/or thermal sensor(s) integrated in the unit. You may be asked to provide this information when you contact Siqura technical support.

Uptime

The time elapsed since the camera system became operational.

Firmware upgrade

The unit 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.

Using the Firmware upgrade section you can write a new firmware version to the upgrade image area. An upgrade image can replace an existing upgrade image written to the unit at an earlier upgrade.

Important: It is essential that the upgrade image is compatible with the unit.

1 To open the upgrade section, click **Firmware upgrade**.
2 Drag the firmware file (`sqrfw` extension) onto the dashed rectangle.
- or -
Use click **Click to select file** to locate and select the file**.**
3 Click **Upgrade**.
The firmware is upgraded. The unit is unresponsive for 30 seconds.

Restart the unit

The *Restart* button restarts the unit without resetting variables. During the restart the unit is unresponsive for 30 seconds.

Reset to factory defaults

With the options accessed via the *Reset to factory defaults* button, you can reset all variables that can be set by the user. After clicking either of the options the unit restarts and is unresponsive for 30 seconds.

- If you need to keep the current network configuration, click **Keep network settings**.
- If you want a complete reset which restores all device settings, including the IP address and subnet mask, to their original, default values, click **Discard network settings**.

Warning: "Discard network settings" restores the unit to the factory-set IP address. This could make the unit unreachable for in-band communications. In that case the webpages are accessible only by moving a PC to the same subnet as the unit.

Create a backup file

It is possible to back up the settings of the unit, so that you can restore them if a problem should occur.

1 Click **Create backup file**.
The backup file is saved to the designated folder on your PC.
File name convention: `yymmdd-backup.tar`
2 Store the file in a safe location (designated for backups, for example).

Restore a backup

You can restore a backed-up configuration.

1 To open the upgrade screen, click **Restore previously created backup**.
2 Click **Do not restore network settings from backup** if you want to preserve the current network settings.

3 Drag the backup file (with `.tar` extension) onto the dashed rectangle.
4 Click **Restore**.
The unit becomes unresponsive for some 30 seconds while the backup is restored.

9.2 Network

For correct functioning of the unit, its network settings must be compatible with the network to which it is added. On the Network page, you can set a static IP address or enable DHCP to have an IP address assigned dynamically.

After you make changes on this page, the unit must be restarted for the changes to take effect. While restarting, the unit is unresponsive for 30 seconds.

Layout

The Network page has two tabs:

- *Network*
  Set a static IP address or enable DHCP
  Configure HTTP, HTTPS and MTU settings
- *Services*
  Enable/Disable RTSP, ONVIF, MX and UPnP

9.2.1 Network

Host name

Identifies the unit on the network. You can set the host name on the Device Management page.

HTTP port

The port used for connections over HTTP. Default: port 80.

HTTPS port

The port used for secure communication over the network. Default: port 443.

Use DHCP

By default, DHCP is enabled. With DHCP enabled, the unit dynamically requests an IP address and other networking parameters from a DHCP server on the network. There are two possible outcomes.

- A DHCP server is found and an IP address is assigned from its pool of addresses.
  The unit can then be found with Device Manager - a software tool available for download at http://siqura.com. You can use this tool to connect to the web interface of the unit.
- No DHCP server is found.
  The unit then reverts to its factory-set IP address. This is the same IP address as that found on the sticker on the housing of the camera. To get access to the web interface, take the following steps:
  1. Set the network adapter of a browsing PC to the factory-default subnet of the unit.
  2. Connect the unit to the PC.
  3. From a browser on the PC, open the web interface of the unit and go to the *Network* page.
  4. Configure the network settings as needed.

It is also possible to request a time server address via DHCP. You can activate this function on the Date & Time page.

MTU size

This value is set to *1500 (Ethernet)* 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. You can use the (default) values on the list or type a custom value. An MTU size that you specify here must be supported on the other side of the link.

IP address

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

For IP address input to be valid, the IP address of the unit:

- must be within the 10.0.0.1 ~ 223.255.255.254 range.
- cannot start with 127 (reserved for loopback on local host).

Subnet mask

Used to subdivide the IP network for security or performance purposes.

Default gateway

The IP address of the network node (router) which serves as the entry point and exit point to the network.

Preferred DNS

The IP address of the DNS server that will be used first for DNS name resolution.

Alternate DNS

The IP address of the server which will be used as the secondary DNS server.

9.2.2 Services

RTSP

The unit 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). Select the RTSP check box to enable RTSP streaming.

RTSP port

The port number used for RTSP media sessions. Default port: 554.

ONVIF

Enables the ONVIF service on the unit. 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 and video streaming. The unit fully supports the ONVIF standard. It has been tested to support ONVIF Profile S.

ONVIF Discovery

Makes the unit discoverable for ONVIF clients. Clear this check box if you prefer to disable discovery. In that case, the unit can still be controlled from ONVIF clients that "know" of its existence.

MX

Select this check box if you need to establish MX connections. MX/IP is a proprietary UDP protocol used to communicate with Siqura equipment over a network connection.

UPnP

If enabled, UPnP (Universal Plug and Play) allows the unit 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, you can connect to the unit from Windows Explorer.

9.3 Date and Time

The date and time on the unit can be set manually or you can use a time server.

Set the date and time manually

1 Clear the **Use time server** check box.
2 Click the **Date & Time** button.
3 Make your adjustments in the *Date* and *Time* boxes.

Nice to know

Depending on the model purchased, it may lose its time settings if kept in storage for a longer period. In that case, the unit will be equipped with a supercapacitor which can deliver charge for up to 10 days and will take 20 hours to recharge. Therefore, in case of a power outage, the unit retains the correct date and time information for a maximum of 10 days.

Format

The date and time are displayed in fixed format in the web interface - that is, `yyyy-mm-dd` and `hh:mm:ss`. On the *Overlays* page, you can select an alternative format for text overlays.

Time zone

Set the local zone depending on the physical location of the unit.

Adjust automatically for DST

The unit can adjust the time automatically for daylight saving time (DST).
1 Select **Adjust automatically for DST**.
2 Use **To daylight saving time** and **To standard time** to set the appropriate start and end details.
The unit will automatically adjust at the given dates and times.
The table below gives DST change information. Note that these dates and times are subject to change. Refer to *http://www.timeanddate.com/time/dst* *http://www.timeanddate.com/time/dst* or similar websites for current information.

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

Country	DST begins	DST ends
USA	2:00 AM local time, second Sunday in March	2:00 AM local time, first Sunday in November

Use a time server

We strongly recommend that you use a time server. Without a time server, the real-time clock will deviate from the actual time after a few days. There are two options for specifying which time server is to be used.

- The time server IP address can be obtained via DHCP.
- The time server IP address can be set manually. This can be the address of an NTP server or that of a Video Management System (VMS) with time server functionality, such as VDG Sense

Obtain time server address from DHCP

It is possible to have the IP address of a time server included in the settings received through DHCP. Using this function requires that DHCP is enabled on the Network page.

- Click to enable **Obtain time server from DHCP**.

Set the time server address

1. Clear the **Obtain time server from DHCP** check box.
2. In **Time server address**, type the IP address or the name of the time server.
   Identifying the time server through its name requires the presence of a DNS server to translate the name into an IP address. The DNS server IP address can be included in the DHCP settings or you can set it on the Network page.

Time service query interval

Indicates the time interval, in minutes, used by the camera to retrieve the current time from the time server.

9.4 Security

Via the Security page, Administrators can install security certificates to enable secure connections between the unit and web browsers. It is also possible to activate authentication for users who want to start an RTSP video stream or extract JPEG snapshot images.

Authentication for camera viewing

This function is disabled by default. Users can freely connect to the unit over RTSP and extract a video stream that it is generating. This may be undesirable from a security perspective. Therefore, it is possible to restrict access to the unit to users with a valid account. Administrators can create and delete user accounts via User Management.

- Select **Enable**.
  On attempting to open an RTSP connection, users are now asked to provide a user name and password.

Secure connections

With HTTPS implemented and activated, a safe exchange of data between the unit and a web browser is ensured. Information transported over the network - for example, device settings and user credentials - is encrypted to protect it against intrusions and infections that can compromise the security and privacy of the information.

Certificates

To implement HTTPS on the unit, 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.

Certificate information

The following information must be provided to create a certificate.

Item	Description
Country	The country where the certificate is to be used
Country code	Two-letter country code
Days until expiration	The valid period (in days) of the certificate. Default: 365
State/Province	The administrative region in which the organisation is located
Common name	The name of the entity to be certified by the certificate
City	City where the organisation is based
Email	The contact email address
Organisation	The name of the organisation which owns the entity specified in the "Common name" box
Organisation unit	The name of the organisational unit which owns the entity specified in the "Common name" box

Important: Make sure that the *Common name* that you specify matches the URL that is used to access the webpages of the unit. Generally, this is its IP address.

Install a self-signed certificate

1 Enter the required information as described above.
2 Click **Create self-signed certificate**.
The certificate is created and installed.

Install a CA-issued certificate

1 Enter the required information as described above.
2 Click **CA created certificate**.
3 Click **Create and download certificate request**.
4 Go to your download folder, copy the `certificate_request.csr` file, and then send it to a CA.
Once you have received the signed certificate from the CA:
5 Click **CA created certificate**.
6 Click **Upload certificate**.
7 Drag the certificate file onto the dashed rectangle.
8 Click **Upload**.

Open a secure connection

With a security certificate installed, you can establish a secure connection.
1 Click **Self-signed certificate** or **CA created certificate** (depending on the type you want to use).

2 At the top of the page, activate HTTPS by selecting **Certificate required**.
3 Refresh the page.
4 Log on to the unit.
Your browser is now using a secure connection to communicate with the unit.

9.5 User Management

Initial setup

Out of the box, the unit is freely accessible - that is, when you connect to the web server you are not prompted to log on. To prevent unauthorised access, we recommend that you implement user authentication. This is done by creating user accounts and activating user login. The number of user accounts you can create is virtually unlimited.

Roles

The unit supports three account types with associated access levels.

Account	Page access	Permissions
Viewer	Live Stream	View live video, PTZ control (if enabled)
Operator	All pages except User Management	Configure, manage and operate the unit.
Admin	Full access	Full control

Use strong passwords

CAUTION: MAKE SURE YOU CREATE AN ADMIN ACCOUNT WHEN YOU OPEN THE WEB INTERFACE FOR THE FIRST TIME. TO KEEP THE ACCOUNT SAFE, SET A STRONG, COMPLEX PASSWORD. THIS HELPS TO PREVENT UNAUTHORISED ACCESS.

Create a strong password

- Use at least eight characters
- Do not include your real name, user name, company name, or other personal information
- Do not use complete words that can be found in a dictionary
- Use a random combination of at least two of the following categories: upper case letters, lower case letters, numbers and special characters

Note: For better protection, especially in high-security systems, we advise you to change the password at regular intervals.

Add a user

Before you can add users and activate user login you must create an Admin account.
1 Click **Add user**.
2 Click **Enter user name**.
3 Type the user name.
User names and passwords are case sensitive.
4 Click **Enter password**.
5 Type the password.
6 Repeat steps 1-5 as needed and select the role which is applicable.
7 (Optional) Refresh the page to sort the user list by name.

Activate user authentication

Once you have an Admin account, you can activate user authentication for the unit.

- On the **User Management** page, click **Activate user login**.
  Users will now be prompted to supply their user name and password when they connect to the unit.

Edit a user

Admins can change user passwords and assign new roles.

1 Click the **Password** box.
2 Type a new password.
3 Click the **Role** box.
4 Select a new role.
The user name cannot be modified.

Delete a user

Admins can delete user accounts.

1 Click the check box of the user you wish to delete.
2 Click **Delete user**.
3 In the information bar, click **Yes, delete**.

9.6 SNMP

The Simple Network Management Protocol (SNMP) can be used to monitor the unit for conditions or events which require administrative attention. Via SNMP, several status variables can be read and traps can be generated on events.

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

Note: The unit includes SNMP support for its Image Quality monitor and Tamper Detect functions. A trap is sent when bad image quality or camera tampering is detected and another one when the situation returns to normal.

Required MIB files can be downloaded at http://siqura.com.

System information

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

1 In the **Contact** box, type the name of the service manager.
2 In the **Node name** box, type the host name of the unit.
3 In the **Location** box, type the name of the physical location of the unit.

Communities

The community strings (names which can be regarded as passwords) in the 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.

Traps

An alarm status change in the unit generates a trap which can be caught by any SNMP manager. The unit can, for example, send traps on the occurrence of Image Quality and Camera Tampering events. Variables, which can be read from the unit'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 MIBs for the unit, at http://siqura.com.

1 In the **Version** list, click the SNMP version used.
2 In the **IP Address** box, type the IP address associated with the manager program.
3 In the **Port** box, type the destination port number.
Default: 162.

Note: *Version*, *IP Address*, and *Port* are required fields.

4 In the **Alternate IP Address** box, if desired, type an alternative destination IP address.

5 In the **Alternate Port** box, if desired, type an alternative destination port number.

6 If desired, select **Enable** to activate **Authentication trap**.
This adds an authentication trap to catch attempts at access using the wrong community string.

Agent

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

9.7 Heater

The heater prevents condensation of the camera window.

Mode

You can set the heater *on*, *off* or to *automatic* mode. By default, the heater is set to *automatic* mode.

Temperature threshold

Drag the *Temperature threshold* slider to set the temperature threshold. By default, the threshold is set to 10^0C. If the temperature drops below this threshold, the camera heater will switch on.

Heater state

Indicates whether the heater is on or off. If the heater state indicates a power error, it means that the device is not properly powered. See also *Troubleshooting* (on page 61).

10 Diagnostics

The *Logging* page can assist you when you need to troubleshoot encountered issues.

In This Chapter

10.1 Logging

The unit includes logging functionality which can be used for diagnostic purposes.

Download a log file

To view the logfile of the unit, you need to download it to your computer.

1 Click **Download log file**.

2 In your download folder, click `system.log`.

The file is opened in Notepad.

Use a syslog server

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

1 In the **Syslog server IP address** box, type the IP address of the syslog server you will be using.

2 To activate **Send log to syslog server**, select **Enable**.

11 Analytics

Video analytics can monitor the video images and - depending on the model purchased - raise alerts triggered by tampering, motion detection, image quality issues, hotspot detection or flare stack monitoring.

In This Chapter

11.1 Tampering

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

Set up tamper detection

The Tampering function enables the unit to trigger an alarm when camera position changes or scene changes are detected in a specified area of the field of view - that is, the Region of Interest ROI). Tampering detection needs a reference image for comparison with the current image.

1 In the centre of the camera view, click **Play**.
Video streaming is started.
2 In the lower-left corner, click **Select** to open the PTZ preset list.
3 Click the PTZ preset for which you want to create a reference image.
4 Click **Activate Tamper Detection**.
The button turns green and additional buttons appear.
5 (Optional) Click **Draw ROI**.
If you do not need a ROI, you can skip steps 5 and 6. In that case, the entire field of view becomes the ROI.
6 (Optional) Drag the mouse pointer across the preview to draw the Region of Interest (ROI).
This defines the area which will be monitored for changes.
7 Click **Add reference image**.
The reference image is created. Progress is indicated by a progress bar.
Once created, the reference image appears as a monochrome overlay with a green border.
8 Click **Show reference images**.
9 Click the new reference image.
10 Type a name in the **Name** box.
11 Close the dialogue box.
Detection starts immediately.
When the camera scene or position is changed, a warning is displayed: "`Camera has been tampered with!!!`" and the reference image border goes from green to red.
12 To create more reference images, repeat steps 2-11 as needed.

Link an action to a tampering event

On the Event Management page, you can link actions to tampering events.

Delete a reference image

1 In the upper-right corner, click **Show reference images**.
2 Point to the image to be deleted.
3 Click the **Recycle** button.

Disable tampering detection

- In the upper-right corner of the Tampering page, click **Deactivate Tamper Detection**.
  The button goes from green to red.
  Reference images - if any - will be preserved and can be reused when tamper detection is reactivated.

11.2 Motion Detection

Motion detection enables the user to define a portion of the screen and to detect picture changes there. These changes could be caused by motion or varying lighting, for example.

Set up motion detection

The Motion Detection function enables the unit to trigger an alarm when motion in a specified area of the field of view - that is, the Region of Interest (ROI), reaches or exceeds a configured sensitivity threshold value.

1 In the upper-right corner, click **Activate Motion Detection**.
  The button turns green and the *Draw ROI* button appears.
  Drawing a ROI is optional. If you do not need a ROI, proceed to step 4. In that case, the entire field of view becomes the ROI.
2 Click **Draw ROI**.
3 Drag the mouse pointer across the preview to draw the Region of Interest (ROI).
  If the ROI is not the correct size or in the wrong place you can repeat steps 2 and 3.
4 Drag the **Alarm level** slider to set the sensitivity of the detection.
  Local change is only detected if its level exceeds the defined value (indicated by the red horizontal line). The *Alarm level* setting can be used to eliminate unwanted ('false') triggering (for example, caused by background noise or constant local movement). You may need to try out several alarm levels to achieve the best detection.
5 If required, go to the Event Management page and add an event with motion detection as an event trigger.

Deactivate motion detection

You can (temporarily) deactivate motion detection.

- Click **Deactivate Motion Detection**.
  The Motion Detection button turns red and the ROI is hidden. Clicking the button once again reactivates motion detection using the same ROI.

11.3 Quality Monitor

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

Examples of detectable occurrences

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

Measurements

The Quality Monitor can measure the contrast level, exposure, SNR (Signal-to-Noise Ratio) and picture detail. The camera health is being measured continuously.

State	Description
	Error state
	Hysteresis: the area where the alarm output is either "true" or "false" depending on the preceding alarm state
	Correct performance

Link an action to a Quality Monitor alarm

On the Event Management page, you can add events triggered by various image quality states, such as "... image too bright", "... contrast too low", or "... detail too low", and then define actions to be taken when a specific state occurs.

11.4 Detector

The Detector page is where you set the detection mode and configure the detection settings for units which support zone, line and hot spot detection and flare stack monitoring.

11.4.1 Zone and line detection

Detection zone and detection line shapes are used to define the area where objects can trigger an event.

- A detection zone shape is initially drawn as a box, but nodes can be added to allow for more complex shapes.
- 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.

Ignore lines do the opposite of what detection shapes do. An 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.

Toolbar

Using the toolbar in the Settings section, you can add detection zones or (ignore) lines to the preview.

Button		Function
		Add a new zone

Button		Function
		Add new tripwire
		Remove the selected zone
		Add new ignore line
		Add/Remove perspective
		Add/Remove minimum object size
		Edit zone nodes

Add a zone

Use this button to overlay a detection zone shape over the preview. Up to two zones can be added.

1 On the **Detector** page, select the **Zones** detection mode.
2 In the toolbar, click **Add new zone**.
The zone appears as an overlay over the video. You can position and resize it.
3 Position your mouse pointer on the zone.
4 Click and drag the zone to the desired position.
5 (Optional) Using the **Edit zone nodes** button, add or delete nodes as needed.
6 With the zone selected, use the nodes to resize and reshape the zone.
7 (Optional) With the zone selected, set the **Detect delay** time.
This is the time to elapse from the moment when an object is detected, before a trigger is generated.
8 (Optional) Add an ignore line (see below).
9 (Optional) Add a perspective shape (see below).
10 (Optional) Add a minimum object size shape (see below).
11 (Optional) In the *Settings* section, set the glue events within time (see below).

Add a line

Use this button to overlay a detection line shape over the preview. Up to two lines can be added.

1 On the **Detector** page, select the **Lines** detection mode.
2 In the toolbar, click **Add new tripwire**.
The line appears as an overlay over the video. You can position and resize it.
3 Position your mouse pointer on the line.
4 Click and drag the line to the desired position.
5 (Optional) Using the **Edit zone nodes** button, add or delete nodes as needed.
6 With the line selected, use the nodes to resize and reshape the line.
7 (Optional) With the line selected, set the **Trigger mode**.
The trigger mode determines whether an object needs to touch the detection line or pass it clockwise, counter-clockwise, or either of these two, to generate a trigger.
8 (Optional) With the line selected, set the **Trigger point**.
- If you select **Center of gravity**, the line is triggered when the center of gravity of an object passes it clockwise, counter-clockwise, or either of these.
- If you select **Bottom center**, the line is triggered when the bottom center of an object passes it clockwise, counter-clockwise, or either of these.

Note that Center of gravity and Bottom center do **not** apply to trigger mode Touch (they are ignored in this mode).
9 (Optional) Add an ignore line (see below).

10 (Optional) Add a perspective shape (see below).
11 (Optional) Add a minimum object size shape (see below).
12 (Optional) In the *Settings* section, set the glue events within time (see below).

Add an ignore line

Use this button to overlay an ignore line shape over the preview. Up to one line can be added.

1 In the toolbar, click **Add new ignore line**.
The ignore line appears as an overlay over the video. You can position and resize it.
2 Position your mouse pointer on the ignore line.
3 Click and drag the ignore line to the desired position.
4 (Optional) Using the **Edit zone nodes** button, add or delete nodes as needed.
5 With the ignore line selected, use the nodes to resize and reshape the ignore line.
6 (Optional) With the ignore line selected, set the **Detect delay** time.
This is the time to elapse from the moment when an object is detected, before the event is suppressed.
7 (Optional) With the line selected, set the **Type**.
The type determines whether the object needs to touch the ignore line or completely cover it, to suppress the event.

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.

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.

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. 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.

Activate alarms

With the detection areas properly configured, you can activate hot spot detection alarms.

- In the *Settings* section, click to select the **Enable** check box of *Alarms*.

11.4.2 Hot spot detection

Automatic hotspot detection is available in Isotherm mode (see *Camera* > *Thermal* Settings). Any object with a temperature above the configured Lower threshold appearing in a detection zone generates an alarm event.

Set up hospot detection

Setting up hotspot detection involves three steps.

1 On the **Detector** page, select the **Hotspot** detection mode, configure the detection settings (see below), and then enable the alarms.
2 On the **Event Management** page, add a zone event output trigger for Camera 2, and then link an action to the trigger.
3 On the **Recording** page or the **FTP Configuration** page (depending on the linked action), configure the settings required for successful action execution.

Add a zone

Using the toolbar in the Settings section, you can add Hotspot detection zones to the preview. Up to two zones can be added.

1 In the toolbar, click **Add new zone**.
The zone appears as an overlay over the video. You can position and resize it.
2 Position your mouse pointer on the zone.
3 Click and drag the zone to the desired position.
4 (Optional) Using the **Edit zone nodes** button, add or delete nodes as needed.
5 With the zone selected, use the nodes to resize and reshape the zone.
6 (Optional) With the zone selected, set the **Detect delay** time.
This is the time to elapse from the moment when a hotspot is detected, before a trigger is generated.
7 (Optional) Add a perspective shape (see above).
8 (Optional) Add a minimum object size shape (see above).
9 (Optional) In the *Settings* section, set the glue events time (see above).

11.4.3 Flare stack monitoring

Set up flare stack monitoring

Setting up flare stack monitoring involves the following steps:

1 On the **Detector** page, select **FlareMonitor** mode, configure the detection settings (for details, see below), and then enable the alarms.
2 On the **Event Management** page, add a Camera 2 "flare active" and/or "flare too large" event output trigger, and then link an action to the trigger.
3 On the **Recording** page or the **FTP Configuration** page (depending on the linked action), configure the settings required for successful action (step 2) execution.

Detection areas

In *FlareMonitor* mode, the preview shows three areas:

- a red arc labelled "Flare too large"
- a green arc labelled "Flare active"
- the centre area (grey half circle)

Centre area

As long as flames emerging from the stack do not exceed the grey half circle in the centre, no alert is raised.

Flare active

The detection level becomes "Flare active" when flames enter the green area but do not exceed it. This level triggers a *Flare active* event if *Alarms* (in the *Settings* section) is enabled and an event of this type has been added on the Event Management page.

Flare too large

The detection level becomes "Flare too large" when flames enter the red area, possibly exceeding it. This level triggers a *Flare too large* event if *Alarms* (in the *Settings* section) is enabled and an event of this type has been added on the Event Management page.

Position the areas

The detection areas can be positioned to match the flare position.

1 Position your mouse pointer on one of the arcs.
2 Click and drag the arcs (in one go) to the desired position.

Resize an area

The three areas can be resized to adjust the alarm levels.

1 Click the area that you want to resize.
A dashed outline with a single (white) resizing handle appears.

2 To adjust the size, drag the resizing handle up/down.
The adjacent area will adapt accordingly, if necessary.

Zone activation time

With the green area (flare active zone) or the red area (flare too large zone) selected, set the zone activation time. This is the time to elapse from the moment flames enter the green or red area, before an event is triggered.

Activate alarms

With the detection areas properly configured, you can activate flare event alarms.

- In the *Settings* section, click to select the **Enable** check box of *Alarms*.

11.5 License Plate Recognition

The License Plate Recognition page is where you can view the read license plates and configure the settings for license plate recognition.

11.5.1 Reads

The Reads tab lists the license plates read (i.e. recognized) by the camera. The most recently read license plate is added at the top of the list.

Use the single-arrow buttons at the bottom of the list to scroll one page forward or backward through the pages. The double-arrow buttons allow you to scroll fast forward or backward (i.e. in steps of ten pages) through the pages.

Of each license plate, the tab gives the following information:

- The **Time** column indicates the time (yyyy-mm-dd hh-mm-ss-ms) when the license plate was read.
- The **Type** column indicates the type of recognition. LPR stands for License Plate Recognition.
- The **Plate** column indicates the license plate number.
- The **Country** column indicates the country code on the license plate. WORLD means that no specific country codes are recognized by the camera.
- The **Confidence** column indicates the level of accuracy (in percentages) of the read license plate.

11.5.2 Camera

The License Plate Recognition function enables the unit to read a license plate when a license plate is detected in a specified area of the field of view - that is, the Region of Interest ROI.

The Camera # tab allows you to draw the Region of Interest and to configure the settings for license plate recognition.

Draw a Region of Interest

Using the toolbar in the Settings section, you can draw the region of interest.

Function	
	Add region of interest
	Remove region of interest
	Edit ROI nodes

If you do not need a region of interest, you can skip the following steps. In that case, the entire field of view becomes the region of interest.

1 In the toolbar, click **Add region of interest**.
2 Drag the mouse pointer across the preview to draw the region of interest.
This defines the area which will be monitored.
3 (Optional) Using the **Edit ROI nodes** button, add or delete nodes as needed.
4 With the region of interest selected, use the nodes to resize and reshape the region of interest.
5 (Optional) Using the **Remove region of interest**, you can remove the selected region of interest.

In the General tab you can configure the general license place recognition settings.

Fine rotation

Indicates the rotation angle (in degrees) under which vehicles may appear to the camera. Enter a positive value for a clockwise rotation relative to the X-axis. Enter a negative value for a counter-clockwise rotation relative to the X-axis.

Value: between -20 and +20.

Min. letter height

Indicates the minimum letter height for the camera to read a license plate. For instance, a minimum letter height of 0.03 means that the camera will only read license plates of which the letters measure at least 3% of the image height.

Value: between 0 and 1.

Max. letter height

Indicates the maximum letter height for the camera to read a license plate. For instance, a maximum letter height of 0.6 means that the camera will only read license plates of which the letters measure less than 60% of the image height.

Value: between 0 and 1.

Min. characters

Indicates the minimum number of characters (letters and digits only) on the license plate for the camera to read the license plate. A dash sign on a license plate is not considered a character.

Value: between 1 and 20.

Max. characters

Indicates the maximum number of characters (letters and digits only) on the license plate for the camera to read the license plate. A dash sign on a license plate is not considered a character.

Value: between 1 and 20.

Max. plate angle

If vehicles can appear under a certain angle to the camera, the unit may be instructed to search for plates in a wider angle relative to the X-axis. The parameter indicates the maximum rotation of the license plate (in degrees), clockwise or counter-clockwise, for the camera to read the license plate.

Value: between 0 and 90.

Min. contrast

Indicates the minimum contrast level of the license plate image for the camera to read the license plate.

Value: between 0 and 100.

Min. detections

Indicates the minimum number of identical detections of a license plate for the camera to read the license plate.

Value: between 0 and 100.

Min. plate confidence

Indicates the minimum level of accuracy (in percentages) for the camera to read the license plate.

Value: between 0 and 100.

Storage destination

Reads can be stored to internal memory, on an SD card or a NAS server. In the **Storage destination** list, select the desired storage medium.

Apart from storing reads on a storage medium, you can also send them to a server. Configure the server settings in the Event tab.

HTTP Events

Select the **Enable** check box to activate sending reads to an HTTP server.

Host

IP address of the server.

Port

Port number used to connect to the server.

Path

URL used to access the server.

Embed JPEG

Select the **Enable** check box if you also want to include sending images to the server.

12 Advanced

Under the Advanced menu, you find the Direct Streaming page.

Important: We recommend that you have in-depth understanding of the Advanced settings and their values before you make any changes. If in doubt, do *not* change the default values.

In This Chapter

12.1 Direct Streaming

On the Direct Streaming page you can enter IP settings for direct streaming to a unicast or multicast IP address.

Multicast

The unit 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 media streams from an IP camera or a video encoder 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).

SAP

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

1 In **IP address**, type the multicast destination IP address for the announcements and media streams.
Range: 224.2.128.0 ~ 224.2.255.255.

2 In **Port**, type the destination port number.
Default: 1024. Use even numbers only.

3 Select **Enable**.
Session announcements and media streams will now be sent to the given IP address.
The media stream can be identified through the *Program name* which is made up of the camera name and stream number.

Direct Streaming

The unit supports direct media streaming to a multicast or unicast IP address (a decoder or viewing application, for example).

1 In **IP address**, type the destination IP address.

2 In **Port**, type the destination port number.
Default: 50010. Use even numbers only.
3 Select **Enable**.

Download SDP

Use the Download SDP button to download a Session Description Protocol (SDP) file from the unit. 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 URL in your web browser.

12.2 Data

PTZ commands over TCP

The unit supports the streaming of PTZ data over TCP using a client/server connection. The TCP connection is bidirectional.

1 In the **Listening on port** box, specify the port on which the server listens for incoming TCP connections.
Range: [0 ... 65535]. Default: 1024.
2 To activate this function, select **Enable**.

Bit rate

Determines the speed of the digital transmission - that is, the amount of information transferred/processed per unit of time.

TX/RX

The TX and RX indicators next to the Bit rate setting are highlighted in green when data is transmitted (TX) or received (RX) via the serial port.

Word length

Determines the number of bits that is transferred in a single operation.

Stop bits

Indicates the end of a data character to enable the receiver to resynchronise with the stream.

Parity mode

Enables the sending of an extra bit with each data character for error detection purposes.

Wire mode

The RX-4xx interface type on the data connector is set in software. Select the required type in the *Wire mode* list.

Biasing

If biasing is needed, it should be enabled on at least one module on the bus.

Termination

Normally, the devices at the two extremes of a bus are terminated, while intermediate devices are not. Therefore: RS-422, always enable (being point-to-point); RS-485, enable only for the first and last module connected to the bus configuration.

12.3 Audio

Input select

Settings: *Line*, *Microphone*

Profile

Preset combinations of settings.

- PCM 16bit: uncompressed 16-bit audio, sample rate 48 kHz
- PCM 24bit: uncompressed 24-bit audio, sample rate 48 kHz
- G.711 A-law: mainly used in Europe and Australia
- G.711 µ-law: mainly used in USA and Japan

Input gain

Drag the slider to adjust the input gain. Range: 0 ~ 30 dB.

Input level

Graphic bar to indicate the audio input level in dBFS (decibels below full scale).

Output gain

Drag the slider to adjust the output gain. Range: -80 ~ 0 dB.

Output level

Graphic bar to indicate the audio output level in dBFS (decibels below full scale).

12.4 RTSP

RTSP Multicast

The unit supports multicast media streaming via the Real-Time Streaming Protocol (RTSP). The RTSP transmitter does not require enabling.

1 In **Multicast address**, type the destination multicast IP address.

2 In the **Port** box, type the destination port number.
Default: 50000. Use even numbers only.

13 Troubleshooting

If you experience problems with your unit the following sections may help you to identify and resolve underlying causes.

In This Chapter

13.1 Date and time issues

No time server active!

Cause: Obtain Time server from DHCP is enabled, but on the Network page **DHCP** is disabled.

Solution: Open the Network page and enable **DHCP** or set the **Time server address** manually on the Date & Time page.

Cause: The Time server address is set manually but the address cannot be reached.

Solution: Verify the **Time server address**. If the address is specified as a name, a DNS server must be available. Open the Network page and check the **Preferred DNS** and **Alternate DNS** addresses.

13.2 FTP issues

Unable to upload to FTP server

Cause: The FTP server does not hold a user account associated with your encoder.

Solution: Request a user account from the FTP server.

13.3 Logon issues

Unable to log on

Cause: Incorrect user name or password. User name and password are case sensitive.

Solution: Supply correct user name and password.

Cause: Unknown user.

Solution: Request Administrator to create a user account.

13.4 Network issues

No network connection between the unit and the browsing PC

Cause: Physical network issue(s).

Solution: Verify that all network devices are properly connected and powered up. Follow the cables, make sure they are plugged into the correct connectors, and check every connector thoroughly.

Cause: Network configuration issue(s). To establish an IP connection, the unit and the browsing PC must be on the same subnet. DHCP is disabled by default on the unit. It has a factory-set IP address in the 10.x.x.x range.

Solution: Install Device Manager, a software tool available for download at http://siqura.com, on the browsing PC. Scan the network with Device Manager. If the unit is not detected, set the network adapter of the PC to the factory-set subnet of the unit. The IP address is printed on a sticker on the unit. Use Device Manager or a browser to access the unit from the PC, and then modify its network configuration as needed.

Cause: Security issue(s). The connection is blocked by a firewall.

Solution: Check if there is a firewall on the PC or on the network which is blocking the connection. Contact your system or network administrator for assistance, if necessary.

13.5 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

Cause: 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.

Solution: Issue one upgrade request at a time and wait for the unit to respond.

Invalid firmware file

Cause: 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 `.sqrfw` extension, it displays this error message.

Solution: Use a firmware file with `.sqrfw` extension.

Device hardware is incompatible

Cause: 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.

Solution: Use a firmware file which is compatible with the unit.

Firmware file is corrupt

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

Solution: Download and install usable firmware.

Rule validation failed

Cause: The firmware file is not suitable for this particular device.

Solution: Upgrade with firmware intended for this unit.

Failed to write firmware to flash

Cause: 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**.

Solution: Prevent a loss of connection or a reboot during the upgrade procedure. Do not leave the Device Management page or close your browser.

13.6 Video issues

Corrupted video stream, visible smears or stuttering video

Cause: Not all data is received by the receiver due to network congestion.

Solution: Make sure there is enough bandwidth available in the network for the stream to be transported from the camera or encoder to the receiver. You can also reduce any overload caused by peak traffic from the encoder. To do this, set the Traffic Shaping to a higher value. See Camera > Streaming Profiles > Stream > Traffic shaping.

13.7 Heater issues

The heater does not switch on and the heater state shows a power error.

Cause: The device is powered by PoE, in which case the heater cannot be activated.

Solution: Make sure that the device is connected to a network switch that provides PoE+.

13.8 Webpage issues

The built-in webpages are displayed incorrectly in your web browser

Cause: The unit supports only recent web browser versions.

Solution: Only use the latest two versions of Chrome, Firefox, Internet Explorer or Safari.

Cause: JavaScript is not enabled in your web browser.

Solution: Open the Privacy (or Security settings) of your web browser and enable JavaScript (Active scripting).

Acknowledgements

Our units use the following Open Source Components / Libraries:

Component/Library	URL
Linux Kernel 2.6 - licensed under the GNU General Public License (GPL), version 2	*https://www.kernel.org/*
alsa-lib - licensed under the GNU Lesser Public License (LGPL), version 2.1	*https://www.kernel.org/*
alsa-utils – licensed under the GNU General Public License (GPL), version 2	*http://alsa-project.org/*
boost - Boost Software License, Version 1.0	*http://boost.org/ http://boost.org/*
BusyBox - licensed under the GNU General Public License (GPL), version 2	*http://busybox.net/ http://busybox.net/*
ethtool – licensed under the GNU General Public License (GPL), version 2	*https://www.kernel.org/pub/software/network/ethtool/*
freetype - Copyright 1996-2002, 2006 David Turner, Robert Wilhelm, and Werner Lemberg	*http://www.freetype.org/*
ftpd – (c) Copyright 1995-2000 Trolltech AS. Copyright 2001 Arnt Gulbrandsen	
iproute - licensed under the GNU General Public License (GPL), version 2	*http://www.linuxfoundation.org/collaborate/workgroups/networking/iproute2*
libupnp - Copyright (c) 2000-2003 Intel Corporation, Copyright (c) 2005-2006 Rémi Turboult, Copyright (c) 2006 Michel Pfeiffer and others	*http://pupnp.sourceforge.net/*
logrotate - licensed under the GNU General Public License (GPL), version 2	*https://fedorahosted.org/logrotate/*
msntp - (c) Copyright, N.M. Maclaren, (c) Copyright, University of Cambridge	*http://www.hpcf.cam.ac.uk/export/*
newlib - Copyright (c) 1994-2009 Red Hat	*https://sourceware.org/newlib/*
openssl - Copyright (C) 1995-1998 Eric Young, Copyright (c) 1998-2011 The OpenSSL Project	*https://www.openssl.org/*

Note: The URLs given above are subject to change and can become outdated.