

S-64 E v2 / EVE

Firmware version 2.1

H.264 Video encoder series

User Manual



T<H
GROUP

**SECURITY
SOLUTIONS**

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

Copyright © 2017 Siqua B.V.

All rights reserved.

S-64 E v2 / EVE 2.1
User Manual v6 (141909-6)
AIT55

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

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

Brand names

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

Liability

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

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

How to contact us

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

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

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

Contents

1	S-64 E v2 / EVE Help	5
2	S-64 E v2 at a glance	6
3	Meet the EVE family	7
4	Get access to the unit	9
4.1	Get access via web browser	9
4.2	Get access via Device Manager	9
4.3	Get access via UPnP	10
4.4	Log on to the unit	10
5	Webpage features	11
6	Live Stream	13
7	Camera	16
7.1	Camera Management	16
7.2	Image Quality	17
7.3	Overlays	18
7.4	Streaming Profiles	21
7.5	PTZ	24
7.6	Privacy Mask (S-64 E v2)	26
8	Event	27
8.1	Management	27
8.2	Connection Monitor	27
8.3	Digital I/O	28
8.4	FTP	29
9	Recording	30
10	Device	32
10.1	Device Management	32
10.2	Network	33
10.3	Date & Time	36
10.4	Security	37
10.5	User Management	39
10.6	SNMP (S-64 E v2)	40
11	Diagnostics	42
11.1	Logging	42
11.2	LED	42
12	Analytics	43
12.1	Motion Detection	43
12.2	Tampering	44
12.3	Quality Monitor	45
13	Advanced	46
13.1	Direct Streaming	46

- 13.2 Data 47
- 13.3 Audio 48

- 14 Troubleshooting 49**
 - 14.1 Date & Time issues 49
 - 14.2 FTP issues 49
 - 14.3 Logon issues 49
 - 14.4 Network issues 50
 - 14.5 PTZ issues 50
 - 14.6 Upgrade issues 51
 - 14.7 Video issues 51
 - 14.8 Webpage issues 52

- Acknowledgements 53**

- Index 54**

1 S-64 E v2 / EVE Help

What's in this manual

This is version 6 of the user assistance for S-64 E v2 and EVE video encoders. It is made up of the Help topics that you can open from the web interface of these units. The topics describe:

- How to operate the unit
- How to adjust device settings
- How to manage user accounts
- How to resolve occurred issues

Note: Functions described in this generic Help information may be supported by all encoders or by specific models only. When describing shared features, this manual uses the generic term "unit" to refer to the S-64 E v2 and EVE encoders. In descriptions of distinguishing features, the individual product name is used.

Where to find more information

You can find the manuals, the datasheet, the EU Declaration of Conformity and firmware updates for your product at www.tkhsecurity.com/support-files. Make sure that you have the latest version of this manual.

Who this manual is for

These instructions are for all professionals who will install, operate or maintain this unit.

What you need to know

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

- CCTV systems and components
- Ethernet network technologies and Internet Protocol (IP)
- Windows environments and web browsers
- 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@tkhsecurity.com. Your feedback helps us to further improve our documentation.

Acknowledgement

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

2 S-64 E v2 at a glance



S-64 E v2

- Four-channel H.264 video encoder
- ONVIF Profile S
- Edge recording
- Picture enhancement
- Image quality monitor
- Advanced tamper detection
- 960H Support
- Duplex serial data
- Open Streaming Architecture (OSA)
- Available with SFP interface

3 Meet the EVE family



EVE ONE

- One-channel H.264 video encoder
- Click & Go – compact DIN rail mounting
- 2x Digital I/O
- Edge storage on μ SDHC card
- Available with Power over Ethernet (PoE)

EVE FOUR

- Four-channel H.264 video encoder
- Click & go: compact DIN rail mounting
- 8x Digital I/O
- 4x Audio in, 1x audio out
- Edge storage on μ SDHC card
- Available with Power over Ethernet (PoE)

EVE 4x4

- Modular 4x four-channel H.264 encoder
- Edge storage on μ SDHC card (4x)
- 4x 4 Audio in; 4x 1 audio out
- 4x 8 Digital I/O

EVE family shared features

- High resolution: 960 H support (960x576 pixels)
- Advanced picture enhancement
- Image quality monitoring
- Tamper detection
- ONVIF Profile S

4 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, remotely operate the PTZ functions, and configure the settings of the unit. This chapter explains how to open the web interface in your browser.

In This Chapter

4.1 Get access via web browser.....	9
4.2 Get access via Device Manager.....	9
4.3 Get access via UPnP.....	10
4.4 Log on to the unit.....	10

4.1 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.
The factory-set IP address of the unit is in the 10.x.x.x range.
- 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 10).

4.2 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 www.tkhsecurity.com/support-files.
Note that Device Manager is 64-bit as of version 1.8.x.
- 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.
- 4 Use the tabs in the *Tree View* pane to define the scope of your search.
- 5 Click the column headings in the *List View* pane to sort devices by type, IP address, or name.
- 6 To connect to the webpages of the unit, double-click its entry in the device list, 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 10).

4.3 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 10).

4.4 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**.

5 Webpage features

The built-in web interface makes it easy to operate and configure the unit over the network.

Access

From a standard web browser on a PC with an IP connection to the unit, you can open the Live Stream page. There you can view live video from one or more connected cameras. Users with appropriate permissions can also open the configuration pages to manage the device and user settings. TKH Security encoders support the latest two versions of Chrome, Internet Explorer, Firefox, and Safari.

Menu

Use the vertical menu on the left to navigate the webpages of the unit. Clicking a menu entry opens a page or a submenu.

	<p>Nice to know</p> <p>To find a specific webpage quickly, type its name in the search-as-you-type box above the menu.</p>
---	---

Layout

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

Preview

Pages such as *Live Stream*, *Overlays*, *Motion Detection*, and *Tampering* include a camera preview. You use it to view live video or determine the effect of your settings when make changes. The *Play/Pause* buttons in the centre of the preview let you control video streaming. To bring up these buttons when hidden, move the mouse pointer over the preview pane.

	Play live video stream
	Pause live video stream

Multichannel

The *Live Stream* page on multichannel units is opened in matrix mode. Video from connected cameras is shown in a two-by-two grid. To bring an individual camera view to the foreground, use the direction buttons that appear when you move the mouse pointer over the previews.

	Show the previous/next camera view.
	Maximise the camera view associated with this option button.

Revert

A *Revert* button appears when you adjust specific settings. You can use it to undo your changes. The button is available until you leave the webpage.



Restore the setting to its original state - that is, at the time of opening the webpage.

6 Live Stream

The Live Stream page is the home page of the unit. This is where you can:

- View and record live video
- Take snapshots
- Control a connected PTZ camera
- Adjust the focus and iris

Layout

The Live Stream page is taken up entirely by the camera preview. This can be a single camera preview (on one-channel units) or a quad camera preview (on multichannel units). In the upper-right corner you see a toolbar which is placed as an overlay on top of the video.

View live video

Video is paused when you open the Live Stream page.

- Click the **Play** button in the centre of the preview.
Streaming video from the connected source(s) is shown.
You can pause the live stream with the *Pause* button.

Maximised mode

On multichannel units, you can enter maximised mode to bring a camera view to the foreground.

- 1 Move your mouse pointer over the preview section.
- 2 Use the Next/Previous buttons (see "Webpage features" on page 11) to go to the camera view you want to maximise.
- or -
Click the relevant camera button at the bottom of the preview section, to go directly to the camera you need.

Overlays

The toolbar and the PTZ controls are shown as overlays on top of the video. The PTZ controls can be hidden (see below). It is possible to create your own overlays. On the Overlays page, you can add up to three text bars and an image, such as a logo.

Toolbar

The toolbar, located in the upper-right corner, may (depending on model and mode) contain the following buttons.

	Hide PTZ controls		Show PTZ controls
	Take snapshot		
	Start recording		Stop recording
	Full-screen		Close full-screen

Full-screen mode

For better observation, you can enter full-screen mode.

- 1 In the upper-right corner of the preview pane, click **Full-screen**.
The preview pane now fills your entire screen.
- 2 To return to the previous mode, click **Close full-screen** or press **Esc** on your keyboard.

Take a snapshot

It is possible to take a snapshot of the camera view(s) on the Live Stream page.

- In the upper-right corner, click **Take snapshot**.
The picture is saved in JPG format to your *Downloads* folder.
The file name includes the camera name and date/time information.

Record a live stream

You can record the video shown in your browser window to your PC. The names of the AVI format files include date and time information to identify the recordings.

- 1 In the upper-right corner, click **Start recording**.
The record button flashes red to show that you started a recording.
- 2 To stop the recording, click **Stop recording**.
Your browser can now download the recording.

Note that the recording function on the Live Stream page records video from your browser to your PC. Event-triggered recording (*Event Management* page) and Continuous recording (*Recording* page) on the other hand record and store the video locally at the S-64 E v2 / EVE. From the microSD card inside the unit, you can download the clips to your PC.

Control a PTZ camera

A PTZ camera connected to the unit can be controlled from your web browser.

Note: First go to the PTZ page (see "PTZ" on page 24) to activate a PTZ driver which is supported by the camera.

With the driver activated, you can operate the camera from the Live Stream page.

- 1 On multichannel units, click the **Next/Previous** buttons to select the camera you wish to control.
- 2 In the upper-right corner, click **Show PTZ controls**.
- 3 To pan/tilt the camera, drag your mouse pointer across the preview in the direction you need.
It is also possible to move the camera by clicking in the preview.

Adjust zoom, focus, and iris

To zoom the camera or adjust the focus and iris, use the sliders in the lower-left corner of the preview. Drag the slider to the left or right and watch the preview until you achieve the desired effect.

Create a PTZ preset

Camera positions can be stored as PTZ presets.

- 1 Pan, tilt and zoom the camera as needed.
- 2 Click **Store current position as preset** (the Favourites button next to the PTZ preset list).
The preset is added to the list with a number to identify it.
- 3 Type a descriptive name in the **PTZ preset** box.
You can also (re)name presets on the Camera tab of 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 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 Camera tab of the PTZ page.

7 Camera

Per channel, the unit can take an input signal from an analogue camera and convert it to two digital video streams. On the webpages grouped under *Camera*, you can adjust video streaming, image quality, and camera management settings.

In This Chapter

7.1 Camera Management.....	16
7.2 Image Quality.....	17
7.3 Overlays.....	18
7.4 Streaming Profiles.....	21
7.5 PTZ.....	24
7.6 Privacy Mask (S-64 E v2).....	26

7.1 Camera Management

On the Camera Management page, you can assign a camera name and select the aspect ratio. On S-64 E v2 encoders, you can also enable/disable the video input, set the input impedance, and select a video standard.

Name

In *Name*, type a name for the camera. Use a unique, descriptive name so that you can easily identify it on the network. The camera name can be enabled as an overlay so that it is visible in the web interface previews and in video streams transmitted by the camera.

Input (S-64 E v2)

A video input is enabled by default. You can choose to set this input to *Disabled*. This is typically done when no video signal is connected to an input.

If you disable the input:

- No "Video loss", "Image quality" and "Tamper detect" alarms will be raised.
- The blue screen with "No Video" will not be shown when no input signal is connected.
- A black image with reduced frame rate with only the OSD-texts will be streamed.

Aspect ratio

The aspect ratio determines the proportional relationship between the width and height of the video images. As different cameras may stream differing video standards, you may want to adjust the aspect ratio for optimal image display.

- 1 Click the **Aspect ratio** list.
- 2 Select **4:3** (standard aspect ratio) or **16:9** (wide-screen).

Input impedance (S-64 E v2)

Impedance is the measure of resistance to signal current flow. With one video source on one video input, select *75 Ohm*. With a number of video inputs in parallel using one video source, use *High-Z* on all inputs except the last.

Video standard (S-64 E v2)

This video display standard you select here - *PAL*, *NTSC*, or *Auto* - determines the available frame rates on the Streaming Profiles page - that is 25 fps for PAL and 30 fps for NTSC.

7.2 Image Quality

On the Image Quality page, image quality settings are overlaid over the video shown in the camera preview. Use these settings to enhance the image quality for optimal display in your web browser or in an application you are using to extract the video stream. Any changes you make are immediately effective and visible in the preview.

Note: On multichannel units, use the *Next/Previous* buttons to go to the camera you need, and then make the required changes.

Noise filter

It is possible to (partially) remove noise from the video signal.

- 1 Click the **Noise filter** list.
- 2 Select **Weak**, **Average**, or **Strong** as required.
Selecting *Off* disables the filter.

Auto-enhancement

When set to *On*, this function continuously analyses the images and dynamically adjusts the image quality to compensate for changing conditions.

Manual enhancement

Image quality can be controlled manually.

- 1 Set **Auto-enhancement** to **Off**.
- 2 While observing the changes in the preview, move the **Brightness**, **Contrast**, **Sharpness**, **Colour saturation**, and **Hue** sliders until you achieve optimal viewing quality.

Note: With manual enhancement, the settings are not dynamically adjusted when conditions change.

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.

Colour 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.

7.3 Overlays

It is possible to add independently configurable text lines to the video signal for on-screen display (OSD) purposes. On S-64 E v2 units, you can also add a graphical image.

Note: On multichannel units, use the *Next/Previous* buttons to go to the camera you need, and then make the required changes.

Product	Text lines	Graphic
EVE ONE, EVE FOUR, EVE 4x4	2x	N/A
S-64 E v2	3x	1x

Overview

The Overlays page has these tabs:

- *Overlay management*
Add and delete text lines or a graphic (S-64 E v2).
Position the objects over the video image and determine their appearance.
- *Font management*
Upload and delete fonts.
- *Image management (S-64 E v2)*
Upload and delete graphics.

Overlay management buttons

Overlays are created on the *Overlay management* tab. The **Add text overlay** and **Add image overlay** (S-64 E v2) buttons open a dialogue box with overlay settings.

Button	Name	Button	Available settings
	Add text overlay		Insert text and set the render mode
			Position the text overlay over the video image
			Set font colour, border colour, and transparency
			Select font and set font size
			Delete overlay
	Add image overlay (S-64 E v2)		Select a picture for the overlay
			Position the overlay picture over the video image
			Set transparency, scaling, and animation speed
			Delete overlay

Add a text overlay

Overlays are created independently of each other.

- 1 Click **Add text overlay**.
A dialogue box pops up. It has a toolbar with four buttons.
- 2 In the **Text** box, type your custom text.
- or -
Click the button next to 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.
- 3 In the **Render mode** list, select **Outline** or **Border** as needed.
Your settings are immediately effective. See the preview for visual feedback.
- 4 Click the **Position** button.
- 5 In the **Position** list, select a preset position.
- or -
Click **Free positioning** and use the **X position** and **Y position** sliders or boxes to freely position the object over the video image. Using the **Anchor point** setting, you can shift the object relative to the anchor point.
- 6 (Optional) Use **Rotation angle** to rotate the text.
- 7 Click the **Colour**.
- 8 Select the font colour and border colour.
- 9 Set the transparency of the text overlay.
- 10 Click **Font**.
- 11 Select the font to be used.
- 12 Enter the font size.

Fonts can be uploaded via the *Font management* tab.

Add an image overlay (S-64 E v2)

You can create one image overlay.

- 1 Click **Add image overlay** (upper-right corner).
A dialogue box pops up. It has a toolbar with three buttons.
- 2 Click the **Image** list.
- 3 Select the image for the overlay.
You can add images to the list via *Image management*. The S-64 E v2 / EVE supports .GIF and .JPG images.
- 4 Click **Position**.
- 5 In the **Position** list, select one of the preset positions.
- or -
Click **Free positioning** and use the **X position** and **Y position** sliders or boxes to freely position the object over the video image. Using the **Anchor point** setting, you can shift the object relative to the anchor point.
- 6 Click **Advanced**.
- 7 Set the transparency and scaling with the sliders or text boxes.
- 8 (Optional) If your overlay is an animated GIF graphic, define its speed in the **Animation speed**.

Delete an overlay

- 1 On the **Overlay management** tab, click on the overlay.
- 2 In the editor box, click **Delete overlay** (the Recycle button).

Font management

Fonts for text overlays can be uploaded to the unit. This is done on the *Font management* tab where you can also delete fonts that are no longer needed.

Upload a font

- 1 Click **Upload font**.
- 2 Drag the font file onto the dashed rectangle.
- 3 Click **Upload**.

Delete a font

- 1 Click **Select font to delete**.
- 2 In the **Font** list, select the font to delete.
- 3 Click **Delete**.

Image management (S-64 E v2)

Images that you want to use for graphical overlays can be uploaded to the unit. This is done on the *Image management* tab where you can also delete images which are no longer needed.

Upload an image

- 1 Click **Upload image**.
- 2 Drag the image file onto the dashed rectangle.
The unit supports .GIF and .JPG files.
- 3 Click **Upload**.

Delete an image

- 1 Click **Select image to delete**.

- 2 In the **Image** list, select the image that you want to delete.
- 3 Click **Delete**.

7.4 Streaming Profiles

Dual streaming

The unit can take the analogue video signal from a connected camera and convert it into two independent digital video streams with different video encoding settings.

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 Click the camera name at the top of the webpage.
- 2 Click **Stream 1** or **Stream 2** to select the stream to assign the streaming profile to.
- 3 In the **Profile** list (below the Stream tabs), select the factory profile which is appropriate for (or comes closest to) the intended purpose.
- 4 Repeat steps 1 through 3 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

If the supplied factory-set profiles do not meet your requirements you can create a custom streaming profile.

- 1 Click the camera name at the top of the webpage.
- 2 Click **Stream 1** or **Stream 2**, to select the stream to assign the streaming profile to.
- 3 In the **Profile** list, select the factory profile to be used as a basis for the custom profile.
- 4 Adapt the profile settings to your requirements.
The custom profile is added to the Profile list (User section) as: `Factory profile-Copy-yyymmdd`.
- 5 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.

Maximise long term bit rate

The default setting is not very suited for recording and storage, the total amount of data needed is unpredictable. This mode defines the average bit rate for a period of time. This mode corresponds with a type of Constant Bit Rate.

Select *Enable* to display and activate the *Maximum long term bit rate* parameter. Clear the check box to deactivate and hide that parameter.

Maximum long term bit rate

With this setting, you can optimise the bit rate by specifying an average value allowed for a longer period.

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). See the table below for supported resolutions.

	PAL	NTSC
960H	960x576	960x480
D1	720x576	720x480
2/3 D1	480x576	480x480
1/2 D1	352x576	352x480
4CIF	704x576	704x480
2CIF	720x288	720x240
CIF	352x288	352x240
QCIF	176x144	176x120
VGA	640x480	640x480
QVGA	320x240	320x240

Traffic shaping (S-64 E v2)

Traffic shaping sets the maximum network bit rate per encoder. Traffic shaping will spread network traffic bursts which helps the network infrastructure handle the traffic. In its turn, however, traffic shaping will increase 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 *High*, the network traffic is 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.

Use Quad view (S-64 E v2)

To see live video from the S-64 E v2, you can use a web browser or video viewing software. In a browser, the Live Stream page presents the four camera views arranged in quad layout. For closer viewing, you can select an individual camera. Likewise, if you use viewing software to extract video, you can request a quad view RTSP stream or open a separate RTSP stream per channel. Note that the unit's Quad view function is disabled by default.

- 1 On the *Quad view* tab, click **Enable**.
- 2 Configure the encoding settings as needed.
- 3 In your viewing application, specify the URL containing the IP address of the S-64 E v2.
- 4 Add `/quad` after the IP address.

For example: `rtsp://10.50.3.72/quad`

On successful connection, the S-64 E v2 quad view is streamed to your application.

Tip: Depending on the chosen settings, the overall performance will be reduced when the quad view stream is enabled. To prevent reduced frame rate or increased latency, it is recommended to set any unused streams to low resolution and low frame rate.

7.5 PTZ

Overview

The PTZ page has the following tabs:

- *Camera-#*
Use this tab to enable PTZ camera control from your browser, assign an ID to the camera and manage the PTZ presets you have created on the Live Stream page.
- *Driver management*
Use this tab to activate PTZ control, upload and delete PTZ drivers, and configure data settings.

PTZ control

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

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

Presets are automatically saved as "PTZ preset #" followed by the preset number. On the Camera # tab, you can rename a preset to give it a more descriptive name.

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

Add a reserved preset

Certain functions of a connected camera (such as a wiper/washer system, for example) can be activated by working with reserved presets, if the camera supports these.

- 1 Click **Add Reserved Preset**.
A new row is added to the preset table.
- 2 Click the appropriate cell under *Preset number* and type the number that will activate the camera function.
- 3 Click the corresponding cell under *Preset name* and type a descriptive name.
The 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.

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 (S-64 E v2)

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

Biasing (S-64 E v2)

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

Termination (S-64 E v2)

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.

7.6 Privacy Mask (S-64 E v2)

To avoid intrusive monitoring, privacy masks can be used to conceal sensitive areas within the field of view of a camera.

Add a privacy mask

You can create up to ten privacy masks.

- 1 In the upper-right corner, click **Add privacy mask**.
The mask appears as an overlay.
- 2 Drag the mask to the area that you want to conceal.
- 3 Drag the sides of the mask to resize it.
It is recommended to set the mask to twice the size of the sensitive area.
- 4 In the **Colour** list (lower-left corner), select a colour for the mask.

Delete a privacy mask

- 1 Click on the mask to select it.
- 2 In the upper-right corner, **Delete privacy mask**.

8 Event

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

In This Chapter

8.1 Management.....	27
8.2 Connection Monitor.....	27
8.3 Digital I/O.....	28
8.4 FTP.....	29

8.1 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**.

8.2 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.

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.

8.3 Digital I/O

The number of digital I/O channels that is provided depends on the model of your encoder (see the table below). Each of the I/O pins can function as a digital input or a digital output (but not simultaneously).

Product	Digital I/O channels
EVE ONE	2
EVE FOUR	8
EVE 4x4	4x8
S-64 E v2	8

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.
- 3 (Optional) Go to the Event Management (see "Event" on page 27) page and add an event with I/O closed as an event trigger.

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

8.4 FTP

On the Event Management page (see "Event" on page 27), 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.

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.

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-1. This can be used if the client is not allowed to access the server root folder.

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**.

9 Recording

The S-64 E v2 / EVE, provides edge recording. This function makes it possible to record and store video locally - that is, at the S-64 E v2 / EVE itself. Recorded video clips are stored on the microSD card inside the unit. From the Edge Recording page, the clips can be downloaded for further processing.

Record

Use the stream list at the top of the page to select Stream 1 or Stream 2 for recording.

Recording types

Two types of edge recording are available:

- Continuous recording
- Event-triggered recording

Continuous recording

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

Important: Be aware that frequent recording in continuous mode for extended periods of time will wear out the flash memory of your microSD card prematurely.

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
- motion detection
- image quality issues
- signal loss
- audio level rising above a threshold

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

Persistent recording

Recording to the microSD card is persistent. This means that rebooting the unit 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 Download 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**.

microSD card

The unit supports μ SDHC 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.
The unit reboots.

We advise to use high-grade, highly-durable microSD cards. Note that microSD cards are limited to the number of write cycles ranging from 1000 (off-the-shelf high-grade card MLC or TLC NAND) to 100.000 (4 GB 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.

10 Device

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

In This Chapter

10.1 Device Management.....	32
10.2 Network.....	33
10.3 Date & Time.....	36
10.4 Security.....	37
10.5 User Management.....	39
10.6 SNMP (S-64 E v2).....	40

10.1 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.

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 Click **Click to select file**.
- 3 Browse to the folder which holds the upgrade file.
- 4 Select the upgrade file (`.sqrfw` extension), and then drag it onto the dashed rectangle.
- 5 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 default* 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 *Download* folder on your PC.
File name convention: `yymdd-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 Click **Restore previously created backup**.
- 2 Select **Keep network settings** if you want to preserve the current network settings.
- 3 Select **Keep SSL certificates** if you want to preserve the currently installed SSL certificates.
- 4 Drag the backup file (with `.tar` extension) onto the dashed rectangle.
- 5 Click **Restore**.
The unit becomes unresponsive for some 30 seconds while the backup is restored.

10.2 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.

Important: On the S-64 E v2, DHCP is disabled by default. The unit is initially accessible through the factory-set IP address which can be found on a sticker on the unit. This is also the IP address to which the unit reverts when you reset it to the factory-defaults discarding the network settings. On EVE encoders, DHCP is enabled by default.

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.

Host name

Identifies the unit on the network. You can set the host name on the Device Management page (see "Device Management" on page 32).

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

With DHCP enabled, the unit 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 www.tkhsecurity.com/support-files. 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. 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 (S-64 E v2)

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.

Use a static IP address

Instead of using an IP address assigned by DHCP you can set a static IP address.

- 1 Clear the **DHCP** check box.
- 2 Type the new network settings in the appropriate boxes.

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.

Services (S-64 E v2)

On the Services tab of the Network page, you can enable or disable the unit's RTSP, ONVIF, MX, and UPnP services as needed. For more information, see the service descriptions below.

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 TKH Security 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.

10.3 Date & Time

The date and time on S-64 E v2 units can be set manually or you can use a time server. The S-64 E v2 has a battery-supported real-time clock. When you reboot this unit, the correct date and time information is retained. EVE encoders do not include a battery. They need to be connected to a time server.

Manual date and time setting (S-64 E v2)

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

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> or similar websites for current information.

	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
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 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 (see "Network" on page 33).

Note: Since DHCP is disabled by default on the S-64 E v2, the *Obtain time server from DHCP* function is also disabled by default.

Time server address

Here you can set the address of a time server.

- 1 To activate this function, clear the **Obtain time server from DHCP** check box.
- 2 In the **Time server address** box, 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 (see "Network" on page 33).

10.4 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.

10.5 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 only	View live video, PTZ control
Operator	All pages except User Management	Configure, manage and operate the unit. User management not allowed.
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.

» To 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**.

10.6 SNMP (S-64 E v2)

The Simple Network Management Protocol (SNMP) can be used to monitor the S-64 E v2 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 S-64 E v2 includes SNMP support for its image quality monitor and tamper detect functions. A trap is sent when bad image quality or camera tampering is detected and another one when the situation returns to normal.

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

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 S-64 E v2 alarm status change generates a trap which can be caught by any SNMP manager. The S-64 E v2 can, for example, send traps on the occurrence of Image Quality and Camera Tampering events. Variables, which can be read from the S-64 E v2 's MIB through an SNMP manager, indicate why the alarm occurred. The OPTC-VCA-MIB required for this can be downloaded, together with the other S-64 E v2 MIBs, at www.tkhsecurity.com/support-files.

- 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 **Alternative IP Address** box, if desired, type an alternative destination IP address.
- 5 In the **Alternative 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 S-64 E v2 has an SNMP agent running which listens for information requests from the SNMP manager on port 161 by default.

11 Diagnostics

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

In This Chapter

11.1 Logging.....	42
11.2 LED.....	42

11.1 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**.

11.2 LED

To identify the unit you can make the status LED blink for a selectable time span.

Start blinking

- 1 Click to open the **Start blinking LED** list.
- 2 Click a time span.

Stop blinking

- 1 Click to open the **Start blinking LED** list.
- 2 Click **Stop blinking LED**.

12 Analytics

TKH Security video encoders include video analytics which can monitor the video images and raise an alert when the following events occur:

- The image quality becomes too poor.
- The camera's position or field of view has changed.
- Movement is detected in a predefined area of the image.

In This Chapter

12.1 Motion Detection.....	43
12.2 Tampering.....	44
12.3 Quality Monitor.....	45

12.1 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.

12.2 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 (EVE encoders)

Tamper detection needs a reference image for comparison with the current image.

- 1 Click **Activate Tamper Detection**.
The button turns green and reference image learning starts. Progress is indicated by a progress bar.
Once created, the reference image is displayed as an overlay over the current image. Detection starts immediately.
When the camera scene or position is changed, a warning is displayed: "Camera has been tampered with!!!".
- 2 If required, go to the Events Management page (see "Event" on page 27), add an event with a "Camera # tampering detected" trigger, and then define the subsequent action.
- 3 To delete the current reference image, click **Deactivate Tamper Detection**.
Clicking **Activate Tamper Detection** once more will create a new reference image.

Set up tamper detection (S-64 E v2)

The Tamper Detection 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). Tamper detection needs a reference image for comparison with the current image.

- 1 Click **Activate Tamper Detection**.
The button turns green and additional buttons appear.
- 2 If the selected camera is a PTZ camera, click **Select** to open the PTZ preset list in the lower-left corner, and then click the PTZ preset for which you want to create a reference image.
Drawing a ROI is optional. If you do not need a ROI, proceed to step 5. In that case, the entire field of view becomes the ROI.
- 3 Click **Draw ROI**.
- 4 Drag the mouse pointer across the preview to draw the Region of Interest (ROI).
This defines the area which will be monitored for changes.
- 5 Click **Add reference image**.
The reference image is created. Progress is indicated by a progress bar.
Once created, the reference image appears as an overlay with a green border.
- 6 Click **Show reference images**.
- 7 Click the new reference image, type a name in the **Name** box, and then close the dialogue box.
- 8 To create more reference images, repeat steps 2-7 as needed.
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.
- 9 If required, go to the Events Management page (see "Event" on page 27), add an event with a "Camera # tampering detected" trigger, and then define the subsequent action.
- 10 To delete a reference image, click **Show reference images**, point to the image to be deleted, and then click the **Recycle** button.

12.3 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 four measurements are enabled by default. 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

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.

13 Advanced

The Advanced menu gives access to the Direct Streaming, Data, and Audio (if supported) pages.

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

13.1 Direct Streaming.....	46
13.2 Data.....	47
13.3 Audio.....	48

13.1 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.

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

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**.

Audio and data streaming

Per camera, you can set up direct streaming of audio and data (if supported by the unit). Specify the appropriate destination/source IP addresses and port numbers, and then select **Enable** to activate Direct Streaming.

Quad view (S-64 E v2)

On the Quad view tab, you can configure settings for Quad view streaming using RTSP Multicast or Direct Streaming. Note that Audio, Data, and SAP settings are not available. For more information about Quad view streaming, see also Camera > Streaming Profiles > Quad view.

13.2 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 (S-64 E v2)

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

Biasing (S-64 E v2)

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

Termination (S-64 E v2)

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.

13.3 Audio

The following audio channels are provided by the S-64 E v2, EVE FOUR, and EVE 4x4 (per blade) encoders:

- Audio in: 4 channels (line level), or two channels line level and two channels mic level (with bias).
- Audio out: 1 channel (line level)

Input select

Settings: *Line, Microphone, Microphone Bias*

Profile

Preset combinations of settings.

- 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).

14 Troubleshooting

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

In This Chapter

14.1 Date & Time issues.....	49
14.2 FTP issues.....	49
14.3 Logon issues.....	49
14.4 Network issues.....	50
14.5 PTZ issues.....	50
14.6 Upgrade issues.....	51
14.7 Video issues.....	51
14.8 Webpage issues.....	52

14.1 Date & 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.

14.2 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.

14.3 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.

Use the reset button

If you have forgotten your Admin password or are otherwise locked out of your video encoder you can regain access by using the reset button on the front panel of the unit.

- 1 Insert a straightened paper clip into the reset button hole which is located:
 - to the left of the VIDEO IN BNC connector (EVE ONE).
 - below the Digital I/O connector (EVE FOUR).
 - to the right of the Digital I/O connector (EVE 4x4).
 - to the left of the Digital I/O connector (S-64 E v2).
- 2 Keep the reset button depressed for at least three seconds.

This erases the upgrade firmware (if present) in the upgrade image area.
The unit will revert to its factory-set network settings.
- 3 Use the IP address found on the sticker on the unit to access the webpages.

14.4 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. EVE encoders request an IP address via DHCP by default. If no server is found, the unit reverts to its factory-set IP address in the 10.x.x.x range. On S-64 E v2 units, DHCP is disabled by default.

Solution: Install Device Manager (available for download at www.tkhsecurity.com/support-files) 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.

14.5 PTZ issues

No PTZ control from Live Stream page

Cause: The connected camera has no PTZ functionality.

Solution: Connect a PTZ camera.

Cause: The active PTZ driver is not compatible with the connected camera.

Solution: On the PTZ page, select a driver which is supported by the camera. Required drivers can be uploaded to your video encoder if necessary.

14.6 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.

14.7 Video issues

Frames are being dropped

Cause: On multichannel units, the four encoders can simultaneously handle video encoding at full frame rate at 960H resolution. It is not recommended, however, to generate eight video streams at 960H. This may overtax the hardware and lead to frames being dropped.

Solution: Set a lower resolution for one or more video streams and disable the quad view stream if not needed.

Frame rate drops

Cause: On multichannel units, the four encoders can simultaneously handle video encoding at full frame rate at 960H resolution. It is not recommended, however, to generate eight video streams at 960H. This may overtax the hardware and lead to drops in frame rate (see the actual frame rate measurement).

Solution: Set a lower resolution for one or more video streams and disable the quad view stream if not needed.

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.

14.8 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
<ul style="list-style-type: none"> Linux Kernel 2.6 - licensed under the GNU General Public License (GPL), version 2 	https://www.kernel.org/
<ul style="list-style-type: none"> alsa-lib - licensed under the GNU Lesser Public License (LGPL), version 2.1 	https://www.kernel.org/
<ul style="list-style-type: none"> alsa-utils - licensed under the GNU General Public License (GPL), version 2 	http://alsa-project.org/
<ul style="list-style-type: none"> boost - Boost Software License, Version 1.0 	http://boost.org/
<ul style="list-style-type: none"> BusyBox - licensed under the GNU General Public License (GPL), version 2 	http://busybox.net/
<ul style="list-style-type: none"> ethtool - licensed under the GNU General Public License (GPL), version 2 	https://www.kernel.org/pub/software/network/ethtool/
<ul style="list-style-type: none"> freetype - Copyright 1996-2002, 2006 David Turner, Robert Wilhelm, and Werner Lemberg 	http://www.freetype.org/
<ul style="list-style-type: none"> ftpd - (c) Copyright 1995-2000 Trolltech AS. Copyright 2001 Arnt Gulbrandsen 	
<ul style="list-style-type: none"> iproute - licensed under the GNU General Public License (GPL), version 2 	http://www.linuxfoundation.org/collaborate/workgroups/networking/iproute2
<ul style="list-style-type: none"> libupnp - Copyright (c) 2000-2003 Intel Corporation, Copyright (c) 2005-2006 Rémi Turbault, Copyright (c) 2006 Michel Pfeiffer and others 	http://pupnp.sourceforge.net/
<ul style="list-style-type: none"> logrotate - licensed under the GNU General Public License (GPL), version 2 	https://fedorahosted.org/logrotate/
<ul style="list-style-type: none"> msntp - (c) Copyright, N.M. Maclaren, (c) Copyright, University of Cambridge 	http://www.hpcf.cam.ac.uk/export/
<ul style="list-style-type: none"> newlib - Copyright (c) 1994-2009 Red Hat 	https://sourceware.org/newlib/
<ul style="list-style-type: none"> 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.

Index

A		
Acknowledgements.....	53	
Advanced.....	46	
Analytics.....	43	
Audio.....	48	
C		
Camera.....	16	
Camera Management.....	16	
Connection Monitor.....	27	
D		
Data.....	47	
Date & Time.....	36	
Date & Time issues.....	49	
Device.....	32	
Device Management.....	32	
Diagnostics.....	42	
Digital I/O.....	28	
Direct Streaming.....	46	
E		
Event.....	27	
F		
FTP.....	29	
FTP issues.....	49	
G		
Get access to the unit.....	9	
Get access via Device Manager.....	9	
Get access via UPnP.....	10	
Get access via web browser.....	9	
I		
Image Quality.....	17	
L		
LED.....	42	
Live Stream.....	13	
Log on to the unit.....	10	
Logging.....	42	
Logon issues.....	49	
M		
Management.....	27	
Meet the EVE family.....	7	
		Motion Detection..... 43
N		
Network.....	33	
Network issues.....	50	
O		
Overlays.....	18	
P		
Privacy Mask (S-64 E v2).....	26	
PTZ.....	24	
PTZ issues.....	50	
Q		
Quality Monitor.....	45	
R		
Recording.....	30	
S		
S-64 E v2 / EVE Help.....	5	
S-64 E v2 at a glance.....	6	
Security.....	37	
SNMP (S-64 E v2).....	40	
Streaming Profiles.....	21	
T		
Tampering.....	44	
Troubleshooting.....	49	
U		
Upgrade issues.....	51	
User Management.....	39	
V		
Video issues.....	51	
W		
Webpage features.....	11	
Webpage issues.....	52	