Digital Barriers

EdgeVis Encoder/MiniCam

SETUP GUIDE

VERSION 8.4.0 – NOVEMBER 22

This document follows on from the encoder's Hardware Installation Guide to provide an overview of the steps required to perform the initial configuration of an IP Series, EdgeVis Video Router, EdgeVis MiniCam or 4K-R800 device, including entering the communications settings, connecting to an EdgeVis Server, and configuring any IP cameras as video inputs.

EDGEVIS™ Live
Powered by TVI

Introduction

Thank you for selecting an EdgeVis video recording and transmission device. This document will help set up and configure your device, allowing it to record and be viewable remotely from an EdgeVis Server.

This document outlines the steps involved in setting up an EdgeVis device. It should be read in conjunction with the Hardware Installation Guide that is appropriate to the specific device to be deployed. This Setup Guide explains how the web interface is used in preparing a device for operation.

In common with other devices, many of the key settings (such as picture settings or bandwidths) and functions (such as camera PTZ control or archive playback) can be accessed remotely over-the-air without the need for any local interaction with the device. This makes it extremely simple to use over time.

A note on naming: EdgeVis devices are available in different form factors, from small discrete devices with no built-in storage or modems (the HD-IP250), to all-in-one pole mounted units that integrates the camera and all wireless communications (the EdgeVis MiniCam and HD-Q800). For simplicity's sake this guide refers to the EdgeVis device as an **encoder** – this is how EdgeVis Server refers to all video recording/transmission devices.

Not all functionality is available on each encoder – please refer to **Appendix A** to determine if your product supports a specific feature.

What is covered in this setup guide?

The following aspects are covered in this product documentation:

Section 1	Accessing the local web setup interface *Connecting and logging into the device to manage the initial configuration settings*
Section 2	Overview of the key setup steps *A walk-through of the important settings required to set up the encoder*
Section 3	Additional configuration options *A summary of the remaining settings available on the encoder*
Appendix A	Supported features on each EdgeVis encoder
Appendix B	Supported external communication devices
Appendix C	Frequently asked questions
Appendix D	Troubleshooting camera discovery issues
Next Steps…	Some guidance on what to do after setting up the encoder
Further reading…	Pointers to other relevant documents available on the support site

Section 1 - Accessing the local web setup interface

Connecting to the encoder's local web setup interface

There are two different ways to access the local web interface:

1. Using an automatic Wi-Fi hotspot that is created on new encoders that have no configuration *(useful for setting up and configuring new units quickly)*
2. Connecting a PC directly to one of the encoder's LAN ports *(the normal method for configuring an encoder)*

Option 1: Using a laptop via the on-board Wi-Fi hotspot

Note: HD-IP200 and HD-IP250 require a supported Wi-Fi dongle to be plugged in before powering to use this mode.

A new unit with no configuration (or a factory-reset unit) will create a temporary Wi-Fi Access Point when it is powered up for the first time. The purpose of this Wi-Fi network is to allow Wi-Fi enabled computers to connect to the encoder and configure the device. *(This hotspot will remain active for 30 minutes.)*

1. On a PC, search for a Wi-Fi Access Point Name in the form XXX-YYYYYYYYY *(where X equals the model number, and YYYYYYYYY matches the first part of the encoder's serial number)*
2. Connect to the network, using **password** as the Wi-Fi password
3. Open a web browser on the setup laptop/PC and enter the following URL: **http://192.168.100.1**.

Option 2: Using a laptop via a LAN interface

To access the local web interface, ensure that the setup laptop/PC can connect to the device:

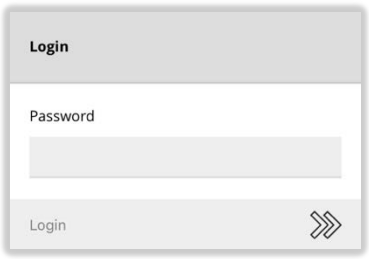
1. Connect your PC to one of the network ports on the encoder (or via a supported USB to Ethernet adapter). From the table below determine the IP Address of the selected port:

• IP200	LAN – 192.168.**10**.1		USB Ethernet – 192.168.**12**.1
• IP250	LAN – 192.168.**10**.1	CAMERA – 192.168.**11**.1	USB Ethernet – 192.168.**12**.1
• IP470	LAN – 192.168.**10**.1	POE1/2 192.168.**11/12**.1	USB Ethernet – 192.168.**20**.1
• EdgeVis MiniCam			USB Ethernet – 192.168.**20**.1
• HD-Q800	LAN (AUX) – 192.168.**10**.1		USB Ethernet – 192.168.**12**.1
• 4K-R800	LAN – 192.168.**10**.1	ECU LAN – 192.168.**11**.1	USB Ethernet – 192.168.**20**.1
• Video Router	LAN1 – 192.168.**10**.1	LAN2 – 192.168.**11**.1	USB Ethernet – 192.168.**20**.1

2. On the PC open the IPv4 network configuration page for the PC's Ethernet port. *(If necessary, refer to these instructions: http://alturl.com/m7zr7)*
3. Select the **Use the following IP address** radio button and enter these settings in the following two fields:
    - IP address: **192.168.X.2** *(where X is taken from the IP Address of the selected port in Step 1)*
    - Subnet mask: **255.255.255.0** and then click **OK** to apply.
4. Open a web browser on the setup laptop/PC and enter the following URL: **http://192.168.X.1** *(where X is the same as the IP Address of the selected port in Step 1 – e.g. 192.168.10.1)*

Logging into the setup web interface

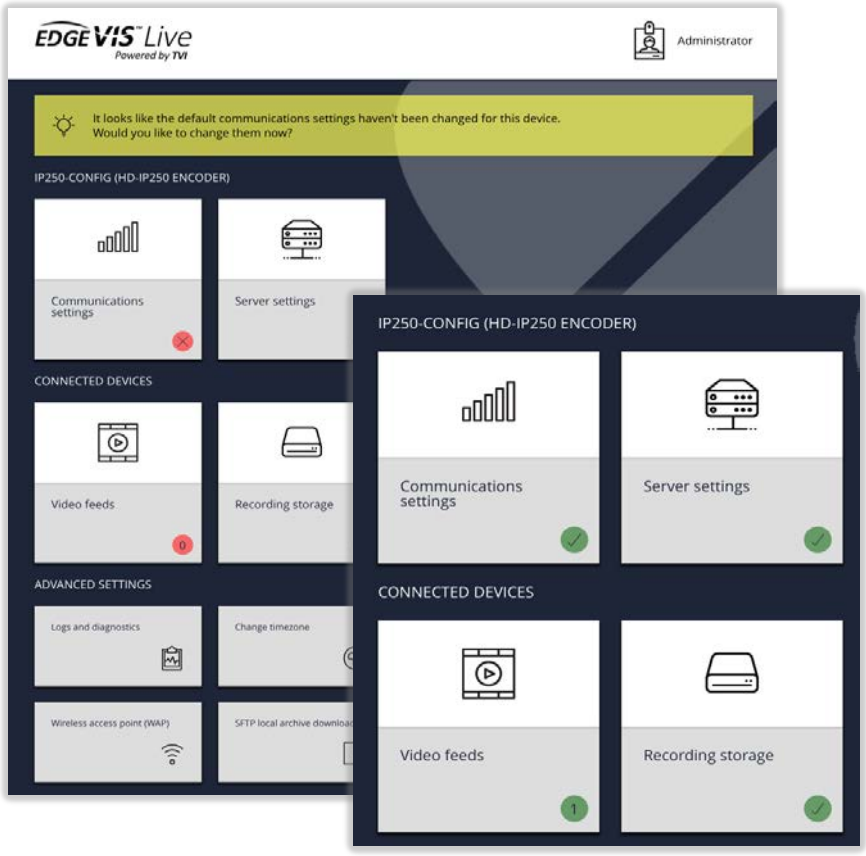
Regardless of the method used, the web browser should now show the login screen for the encoder



The default password is **password**

For security reasons the encoder will now prompt to change the default password to something more secure.

Once logged in the encoder's dashboard is loaded:



The dashboard presents the status of the encoder, showing red crosses where an issue requires attention, or a green tick to indicate that section of encoder configuration is operating correctly. The encoder will also display a help tip if any crucial encoder settings are still blank and require configuration.

Section 2 – Overview of the key setup steps

There are four key steps required to configure an encoder:

1. Configure the communications settings for LAN ports, cellular modem, Wi-Fi and USB LAN adapters
2. Provide the details of EdgeVis server and encoder account
3. Add each desired video feed to the encoder
4. Select the desired recording location and encryption settings

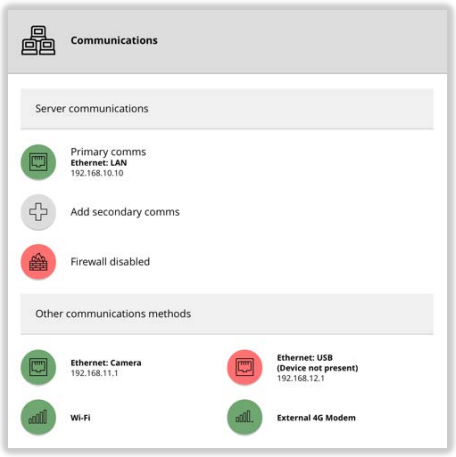
This section describes each of these four key steps, while Section 3 provides an overview of the remaining options.

Step 1 – Configure the communications settings

The encoder can utilise both internal and external communications devices. Please refer to the encoder's hardware installation guide for details of internal options for each specific encoder model, and Appendix B for a list of supported external communication options.

There are four main tasks to perform in this section:

1. Enable and disable communications methods
2. Configure the settings for each communications bearer
3. Select the communications bearers to use to connect to EdgeVis Server (both a primary and secondary)
4. Enable a firewall on the primary/secondary communications bearers



Enable and disable comms methods

For security reasons, it is recommended to disable any comms method that are not required. Click the desired communications method and use the **Enable/Disable this device** menu item.

Configure each comms method's settings

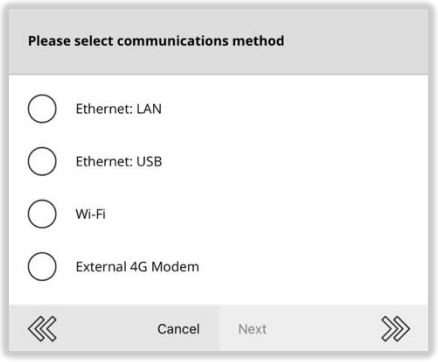
For each comms method that will be used, click on its entry to view its settings, and from there use the **Edit configuration** menu item to enter the settings.

Cellular connection	Cellular connections require an APN, username and password to connect to a mobile data network – either enter these manually or select from the list of common mobile operators. Advanced options include: • Wireless IP address – some private APN networks may require an IP address • Network Technology – force the modem to use 2G, 3G or 4G (or Auto select) Comms Technology – certain modems can work in either GSM or CDMA mode
Wi-Fi connection	It is possible to add the details of multiple Wi-Fi networks to the encoder (in priority order) and the encoder will automatically pick the highest priority network available. Select **Add Wi-Fi configuration** to add a network to the encoder's list. This will display a list of visible Wi-Fi networks, or a manual entry can be added. It is possible to set DHCP/static network setup on a per configuration basis. Once added use the up/down arrows to move entries up and down the priority list.
LAN connection	It is possible, on a per-LAN port basis, to set either DHCP (for connection to a larger network) or a static configuration (usually for direct-connection to a camera).

Select the preferred server comms method

It is necessary to select the primary comms method that the encoder will use to connect to EdgeVis Server and stream content. A secondary method can be also specified for failover for periods when the primary bearer is unavailable.

It is possible to set a primary or secondary method directly from the Communication Settings page, or to use the **Use for primary/secondary communication** menu item on each method's settings page.



Enable the firewall on the primary/secondary comms methods

The only services running on an encoder that are externally accessible are the encoder's web configuration page and, if enabled, the SFTP recordings download service. The default setting is to allow access to these services on any communications method.

For security reasons, it is possible to remove access to these services on communications methods that have been configured as primary/secondary communications methods. Use the **Firewall Settings** menu item to block access to these services.

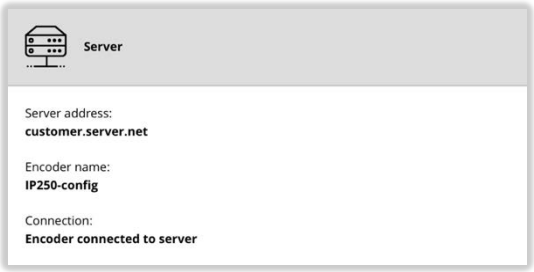
WARNING: You may immediately lose access to the web setup interface if you are currently configuring the unit through the primary/secondary comms method **and** you enable the firewall – this should be the last step you perform!

Step 2 - Enter the encoder's EdgeVis settings

NOTE: Before the encoder can be connected to an EdgeVis Server, it requires an encoder account be created on EdgeVis Server. This step is typically undertaken by an administrator and the details of encoder account management are covered in the **EdgeVis Server Quick Start Guide**.

To proceed a user must have the following details for an encoder:

- The IP Address or Domain Name of the user's EdgeVis Server
- The name and password of the encoder account created on EdgeVis Server
- (Optionally) The encryption fingerprint of the EdgeVis Server



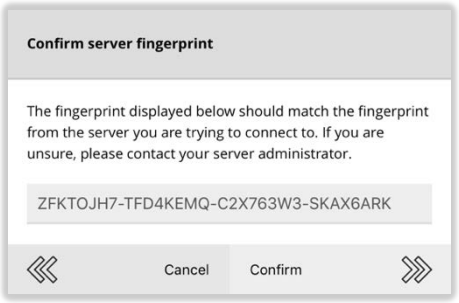
The **Server Settings** page will display the current settings being used to connect to the server, and the status of the connection.

To edit the server connection settings, use the **Change server settings** menu option and enter the details above.

Encryption modes

When connecting to EdgeVis Server it is possible to select one of three encryption modes:

- **Encrypted (online verification)**
  The user will be asked to verify the encryption fingerprint of EdgeVis Server before allowing a connection
- **Unencrypted**
  In some circumstances the EdgeVis Server may not support encryption and so this option should be used
- **Encrypted (offline verification)**
  If connecting to the server is not currently possible to verify the fingerprint this option allows the user to upload the EdgeVis Server's encryption pack (available from EdgeVis Server), which will subsequently be verified when the encoder reconnects to the server



Encoder Licensing

Encoders must also be licensed to connect to an EdgeVis Server. This can be done during the account creation on EdgeVis Server or, if no licence has been assigned, be requested by the encoder during configuration.

If no licence is currently assigned the **Server Settings** page will provide a link where the user can request a licence from the server (if available). The form will also show the features enabled within the selected licence.

NOTE: For IP Series, Video Router, and HD-Q800 request a licence for EACH camera you intend to connect to the encoder. This number is limited to the maximum number of cameras as specified in the encoder's fact sheet.

Step 3 - Adding video feeds to the encoder

There are two main ways to add an IP camera:

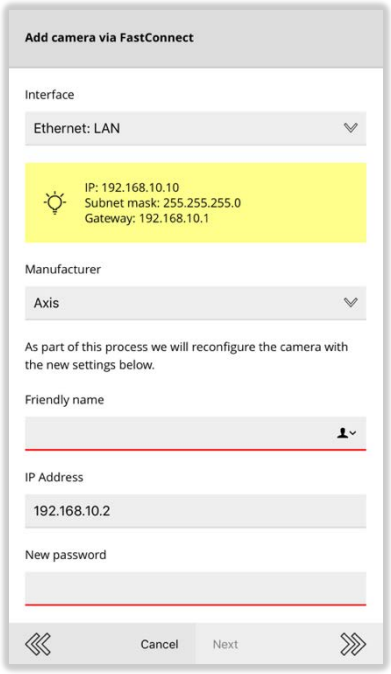
- **FastConnect** – designed to make it simple to add new cameras 'out-of-the-box' directly to an encoder, without the need for the user to know the camera IP Address or configure the camera in advance of connection.
- **Auto-Discover** – designed for discovering cameras, either directly connected to the encoder or through a LAN connection that has already been configured with the correct network settings.

Consider the following questions when deciding which method to use:

	FastConnect	**Auto-Discover**
Who is it for?	Users with **new** Axis, Bosch or Canon cameras who are **directly connecting** the camera to the encoder	Users of a compatible camera who have configured the camera to be on the same network subnet as their encoder
Suitable for one-to-one connections between camera and encoder?	YES	YES
Suitable for finding cameras on a LAN network?	NO	YES
Supports adding more than one camera per port?	NO	YES
Compatibility	Axis, Bosch and Canon cameras on the compatibility list	Any named camera on the camera compatibility list
Prerequisites	- Camera must have default IP Address and default admin password set. - Camera must be connected directly to the device. - The LAN port configured for use on the IP Series device must be set for Static IP.	- Encoder LAN port in use can either be set to static IP for direct connection or configured to connect to a LAN network. - Camera must be pre-configured with an IP Address that can be accessed by the encoder (usually on the same sub-net)

The first entry on the video feeds page displays the maximum number of cameras that can be added to the encoder. This is determined by the hardware limitations of the encoder **and** the number of EdgeVis licences assigned to the encoder's account on EdgeVis Server.

Adding an IP camera using FastConnect



From the **Camera Settings** page click the Add button to start the Add Camera wizard.

- Select the **Add a camera via FastConnect** menu option.
- Select the network interface the camera is **directly** attached to.
- Select the brand of camera you are adding to the encoder.
- Enter a friendly name that EdgeVis should use to refer to this camera
- Enter a new administrator password for the IP camera

Please take note of both the new IP Address and password, as these may be required later if configuring the camera through its web configuration pages.

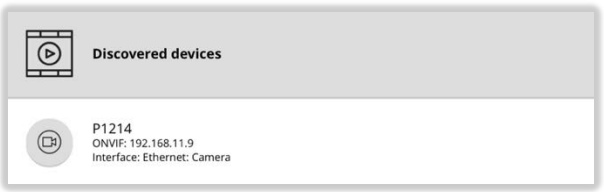
The next stage is for the encoder to then attempt to find the camera attached to the device, and if found, will reconfigure the camera and add it to the list of cameras connected to the encoder.

NOTE: This will only succeed if the camera has factory default settings, including all network settings.

Auto discover a connected IP Camera

For cameras that are not configured using FastConnect, it is recommended to search for the camera using the **Search local network for cameras** menu option.

NOTE: The IP camera and the port (on the encoder) it is connected to must have compatible IP Address settings. Usually this means that the IP Address of the camera, and address of the encoder port must both be 192.168.X.Y, where X is the same, but Y is unique on the network.



The encoder will search all enabled network interfaces for IP cameras and display a list of all cameras available.

To select a camera, click on its entry in the list.

This will then prompt for:

- A friendly name that EdgeVis should use to refer to this camera
- The login details of the camera (required for most cameras)
- Whether to allow EdgeVis Client to access the camera's web interface via SecureConnect
- Whether to automatically configure the camera to 'safe' quality settings – see **Supported Camera Settings** section for further details

Once entered the camera should now be added to the encoder's list of video feeds.

If the desired camera is not listed in the discovered cameras, it may still be possible to add the camera, either by reconfiguring the camera/encoder's network settings to match or by adding the camera manually. Appendix D offers some advice and trouble-shooting tips if required.

Adding a camera manually

There are two reasons why it may be necessary to add a camera using the **add manually** option:

- The camera was not discovered using ONVIF discovery
- The camera does not support ONVIF, but you do have the RTSP address of the camera feed.

To add an ONVIF camera… you must know these details in advance:

- The camara's IP address
- The port number (this is usually 80, but some cameras allow this to be changed)
- A username / password that has permission to view the stream

To add an RTSP camera… you must know these details in advance:

- The camera's IP address
- The port number (this is usually 554, but some cameras allow this to be changed)
- A username / password that has permission to view the stream (some cameras allow unauthenticated access)
- The URL path to the appropriate camera feed

You may be supplied the IP camera's RTSP address as a full URL. For example:

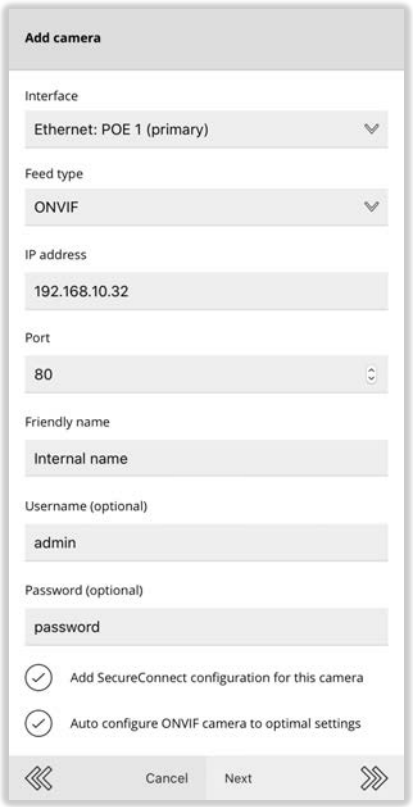
```
rtsp://admin:password@192.168.10.1:554/playstream.sdp?channel=1&subtype=0
```

This can usually be broken down to obtain the information using this format (although many fields are optional and may not be present)

```
rtsp://<user name>:<password>@<ip address>:<port>/<url path>
```

To add a camera:

- Select the encoder interface the camera is connected to
- Select the feed type (either ONVIF / RTSP)
- Enter the IP address and port of the camera (the port number will automatically be set to the appropriate default port number)
- (RTSP Only) Enter the URL Path
- Enter a friendly name for the camera – this will be displayed to the user in EdgeVis Server and EdgeVis Client
- Most cameras will also require a username and password to access the camera feed



The last two options allow you to decide:

- Whether to allow EdgeVis Client to access the camera's web interface via SecureConnect
- Whether to automatically configure the camera to 'safe' quality settings – see **Supported Camera Settings** section for further details

Supported Camera Settings

IP Cameras must supply a feed that complies with the following characteristics:

- Incoming video format must be H.264, audio format (if present) must be G711
- Video resolution must be 1080p, 720p, 576p or 480p – higher/non-standard resolutions are not supported
- Frame rate must not be greater than 30fps
- It is not recommended to use bitrates higher than 10 Mbps. IP cameras bitrates can often spike over configured settings with high motion scenes. This can negatively affect encoder performance and recording duration

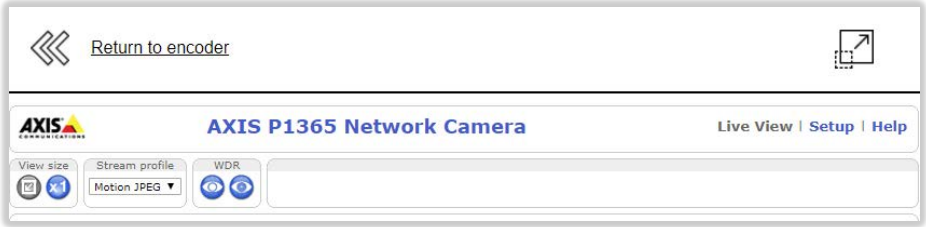
When adding an ONVIF camera, by default, the encoder will automatically configure the camera to 1080p, 25/30fps @ 10 Mbps. This ensures that the quality is the highest possible, while keeping the camera bitrate to recommended levels.

It is possible to stop this default behaviour by unticking the **Auto configure ONVIF camera to optimal settings** while adding the camera. It is then the user's responsibility to check the camera meets the above requirements. After adding the camera, the Stream Information section will display the live characteristics of the received stream:

Connecting directly to attached IP cameras

The camera details page allows the user to connect directly to the web interface of any IP camera by proxying the data via the configuration web page. This functionality can be accessed by selecting the **Connect directly to this camera** menu option. This feature allows for easier configuration of any camera specific settings that require the camera's web interface.

The **Return to encoder** button can be used to navigate back to the encoder configuration pages. The button in the top right of the page will open the camera's web interface in a new browser window, which may be required if the camera web interface fails to load.



Special instructions for Axis camera users

ONVIF access is enabled by default on any new ONVIF-capable Axis devices, and it should be possible to add a new camera without issue. However, if the user uses the camera independently of the encoder (and sets a new root password on the camera using the web interface) ONVIF access is automatically **disabled**.

To re-enable ONVIF access:

1. Use the **Connect Directly** feature described above or from a PC, access the camera's interface using a web browser (http://<camera IP address>/)
2. Click **Setup** from the main page
3. Navigate to **System Options** -> **Security** -> **ONVIF**
4. Click **Add** to create a new user in the Users List
5. Enter a username and password, and ensure the **User Group** is set to **Administrator**
   *This user is **only** for ONVIF access, and is separate from users created in System Options -> Security -> Users*

Some Axis camera also require Relay Attack Protection to be disabled before an encoder can use the camera – the following steps can be performed if the above steps are not enough to successfully add/use the camera with your encoder.

6. Navigate to **System Options** > **Advanced** > **Plain Config**
7. From the dropdown menu **Select a group of parameters to modify** and click **WebService**
8. Click **Select Group**
9. Un-check **Enable relay attack protection**
10. Click **Save**

It should now be possible to add the Axis camera to the encoder.

Wired HDMI/3G-SDI/Composite cameras (4K-R800 only)

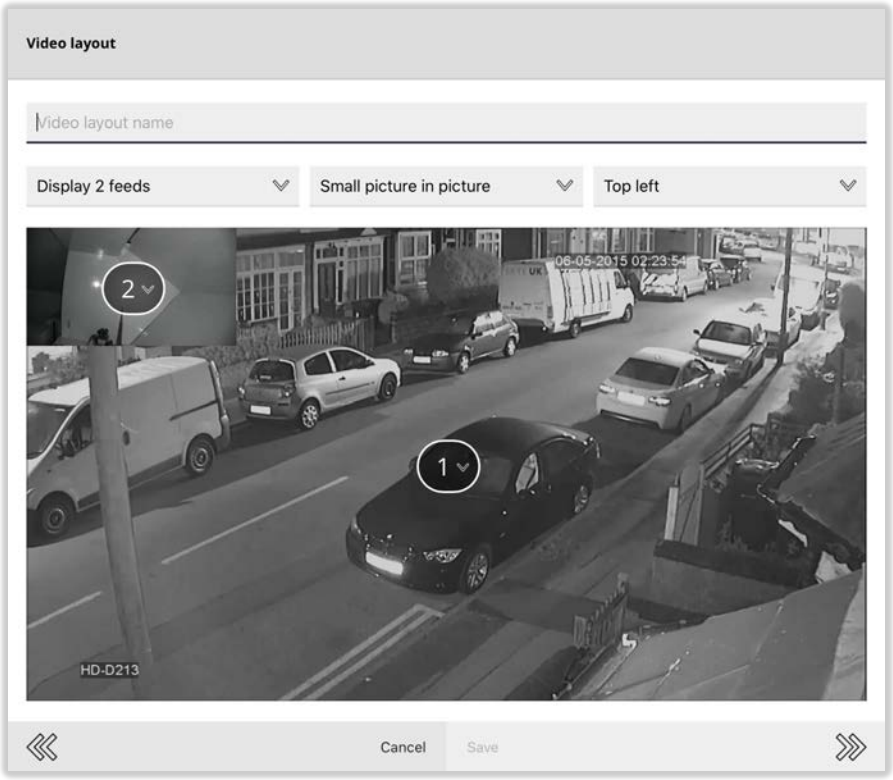
There is no special configuration required to enable wired cameras – simply plug the camera into the encoder.

Add a Picture-in-Picture or Quad View layout

For an encoder with more than one camera it is possible to create virtual video feeds which can either contain:

- a 4-way quad view, where each camera fills one quarter of the image
- a Picture-in-Picture view where one camera fills the whole image, and a second camera is superimposed in a smaller window on top of the image in one of the corners (selectable)

To create a new layout, use the **Add video layout** menu option and select the desired layout format.



Step 4 – Setting recording settings

An encoder can save recordings to a number of locations:

- The internal recording disk (not available on all encoders)
- Onto an SD Card inserted into the encoder (only available on 4K-R800)
- An external USB Disk (Fat32 formatted, at least 20GByte, USB 3.0 preferred)
- An external NAS Disk (using Windows File Share/SMB)

Note: The maximum supported capacity on an internal or external hard drive is 2TB. It is possible to use larger drives, but they must be formatted by the encoder and the recording space will be reduced to 2TB.

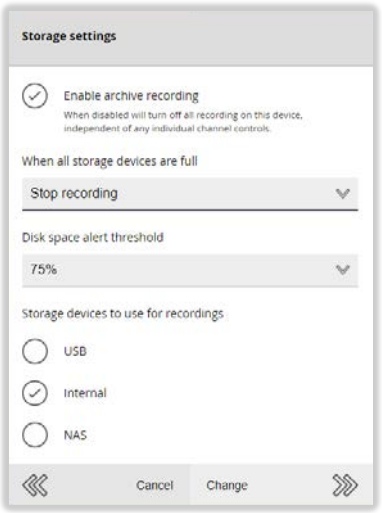
The **Recording Storage** page will list all available recording locations. If multiple locations are available, the encoder will pool the locations to increase the available storage duration.

The **Storage Settings** menu option can be used to configure various aspects of the recording. For security reasons, it is possible to enable/disable individual types of recording devices (or to turn off recording entirely).

When all storage devices become full it is possible to either:

- Overwrite oldest recordings (default)
- Stop recording

When **stop recording** is selected the encoder will start to send out notifications when each disk starts to become full (the threshold is configurable). The Rule Builder functionality in EdgeVis Server Web Management Interface can be used to turn these notifications into email, SMS or push notification alerts to specific users.



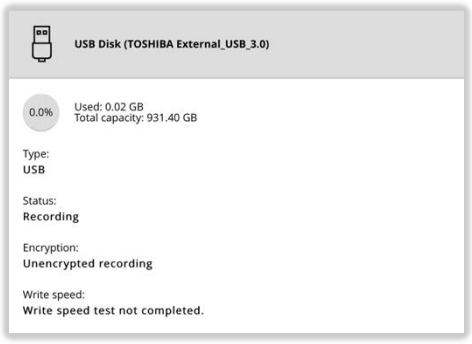
To view the settings and status of a recording location select it from the list.

As well as showing the status of the device (including how full it is) it also allows the user to format the drive, or safely eject the drive from the encoder.

Users wishing to use a NAS drive will require the Windows file share information:

- The IP Address of the NAS (e.g. 192.168.10.12)
- The name of the share (e.g. share)
- The username/password to connect to the NAS

Recording drives can also be speed tested to determine if the storage device is fast enough for recording purposes.



Setting the recording encryption settings

By default, the encoder will not encrypt, or password protect the recordings. This allows the recordings to be played on any PC by anyone who has the appropriate playback software.

Using the **Recording Encryption Settings** menu option, it is possible to encrypt the recordings so that only those with the encryption key can review the recordings on the disk.

Changing the recording key will stop recording until all attached recording disks are reformatted.

Section 3 - Additional configuration options

There are several additional configuration options available on the encoder's home page:

Power Settings *(HD-IP250 Only)*

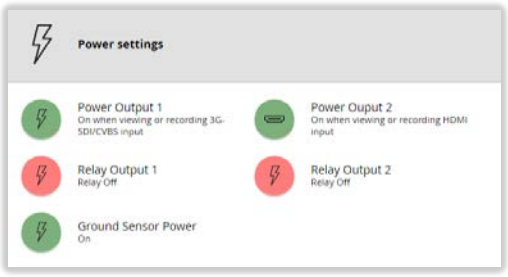
It is possible to adjust two power options on the HD-IP250

- **PoE Power** – disable PoE power output on the camera port
- **Fan Power** – to reduce the noise made by the encoder it is possible to disable the fan. This will reduce the maximum supported temperature of the HD-IP250 by 10°C (18°F)

Power Settings *(4K-R800 Only)*

The 4K-R800 is able is able to provide power to a number of external devices:

- Wired cameras (both 3G-SDI and HDMI ports) – this interface provides the ability to always power the camera, or to only power it when required (i.e. during recording or viewing).
- Relay outputs – the encoder has a number of relay outputs that can be opened/closed that will allow the incoming power (up to 2 amps) to pass through.
- Ground sensor – if the appropriate cable is available the encoder can provide power for the ground sensor serial port.



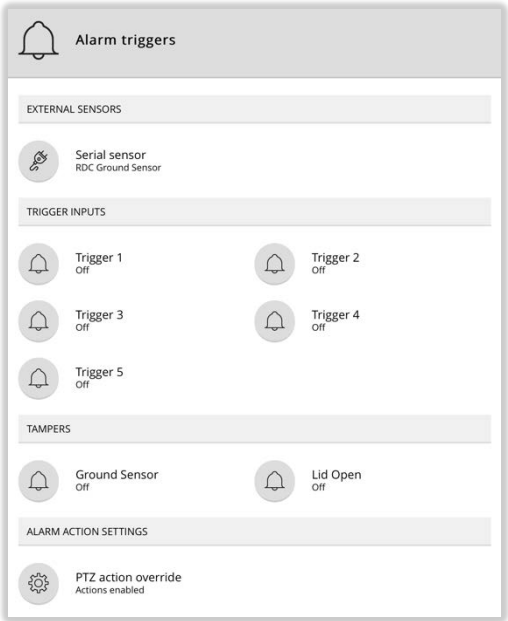
Alarm triggers (4K-R800 Only)

The triggers page on a 4K-R800 allows for the configuration of the alarm capabilities including:

- Selecting the desired ground sensor system
- Enabling up to 5 close contact triggers (configurable low-to-high, high-to-low, or any transition)
- Enabling the lid open or ground sensor tamper (if wired)

Additionally, it is possible to customise the behaviour of certain alarm actions:

- PTZ behaviour during alarm activation (should alarm triggers overrule manual PTZ control?)
- FTP Push settings (required if the user wishes to send recordings to an FTP server as part of alarm rule action



Change time zone

The time used by the encoder (for both live video and recordings) is automatically set by synchronising with EdgeVis Server. The encoder saves all recordings in UTC (GMT), and during display of both live video and recordings the viewing client will offset the time displayed by the time-zone configured in this setting.

NTP Service

Many IP cameras can display the current date/time overlayed on the video. To print the correct time, IP cameras need an accurate time source – to help provide this the encoder can run an NTP (Network Time Protocol) server to ensure that the encoder and all IP cameras use the same date and time.

The option to enable/disable NTP is available from the **Time and date settings** page. Once enabled it is necessary to log in to each IP camera and configure it to use NTP as a time source. The address for the NTP server should be the IP Address of the encoder's LAN port (that it is connected to).

SecureConnect

SecureConnect is a feature that allows IP cameras, video analytics and other edge devices to be remotely configured and controlled using the secure EdgeVis architecture. This allows a remote user to operate IP devices using EdgeVis Client.

The most common use case is to access the configuration web pages of attached IP cameras – and the encoder can automatically add a SecureConnect channel for each camera when adding the camera to the encoder.

The SecureConnect page displays all configured SecureConnect channels on the encoder, allowing the user to add/edit/delete entries. Additionally, the user can decide how much of the configured streaming bandwidth can be used by all SecureConnect users combined – the higher the bandwidth ratio, the lower the amount of remaining bandwidth for video transmission.

For more information on SecureConnect please refer to the Knowledge Base Article: **Using SecureConnect to access remote devices**.

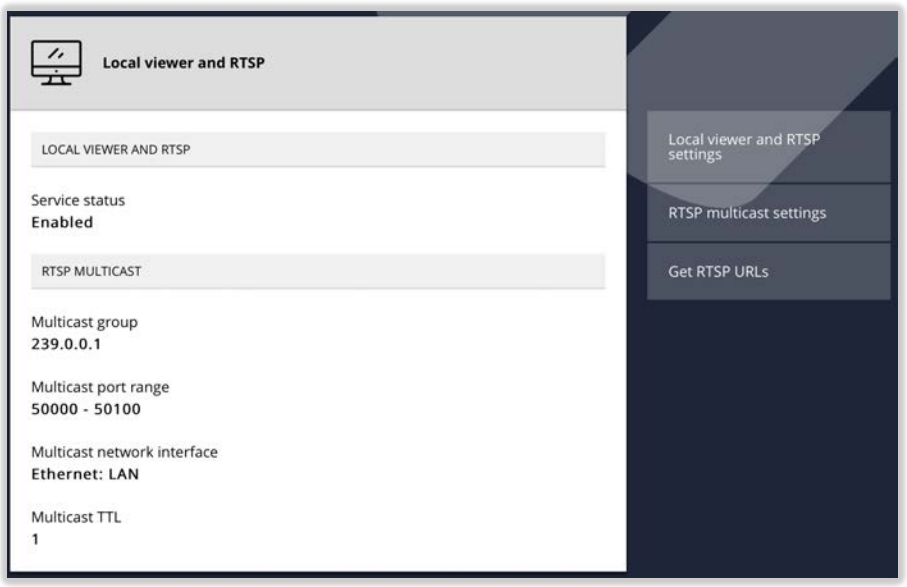
Local viewer and RTSP

Local viewer is an application (available in the EdgeVis Client Suite installer) that allows you to connect to the encoder if you are on the same physical network and:

- View any of the original high-quality video stream from any camera attached to the encoder – the encoder will reflect the original RTSP feed for IP camera or generate an RTSP stream for physically connected cameras.
- PTZ control
- Review and download recordings
- Monitor when on-board alarm triggers

Please review the local viewer documentation for full details of the capabilities available.

For security reasons this feature is **disabled** by default. To enable the local viewer service, use the **Local viewer and RTSP setting** menu button. As part of enabling the service you must enter a password – this is used to protect access to the encoder and must be entered when connecting to the encoder with Local Viewer.



The encoder can also provide the same RTSP feed of any connected camera for users who have their own local software – this feature is available when the local viewer service is enabled but does not require Local Viewer to function.

To access the RTSP stream use the **Get RTSP URLs** menu button and select:

- Which camera you wish to view
- Whether to use unicast or multicast (unicast is recommended for most customers, as multicast delivers the video stream to every device on the network).

This will then present the RTSP URL you can use in the third-party application. Note that the username for the RTSP stream is always **user** but the password will be the same password you set when enabling the service.

For advanced users, it is possible to configure the networking settings (including the encoder network connection to transmit the multicast stream on) – use the **RTSP multicast settings** menu button to access these settings.

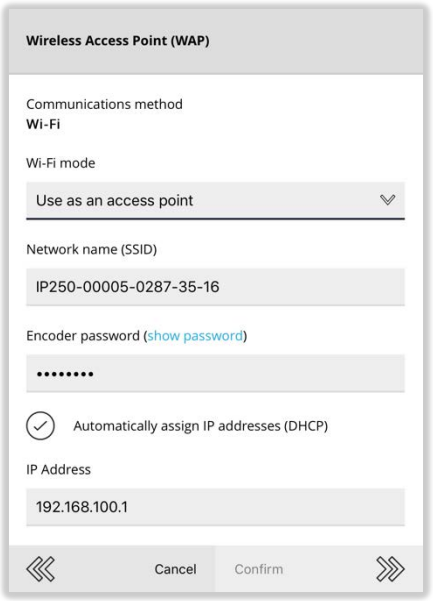
Import/Export Settings

It is possible to configure an encoder, and then selectively export categories of settings to a downloadable file. This file can then be imported into other encoders to decrease setup time.

NOTE: Exporting the encoder's settings will save the various passwords used by the encoder, some of which are viewable in plain text – use care when utilising this feature.

Wireless Access Point

If supported by the encoder (or when used in combination with a supported USB Wi-Fi adapter) it is possible for the encoder to create its own Wi-Fi hotspot, which allows the user to directly connect to the encoder remote configuration over Wi-Fi, remotely download video recordings over SFTP, or allow Wi-Fi cameras to connect directly to the encoder.



The encoder has three modes of operation:

- **Use for communications** – the Wi-Fi will only connect **to** other Wi-Fi routers (as configured in the communications settings page).
- **Use as an access point** – the Wi-Fi will broadcast a Wi-Fi access point. This will ignore any Wi-Fi configuration settings in the communications settings page, and Wi-Fi can't be used to connect to EdgeVis Server.
- **Switched** – the ability to switch between the first two options remotely (using EdgeVis Client or EdgeVis Server). This is useful when normally the encoder should transmit to EdgeVis Server using Wi-Fi but switch to access point mode during 'drive-by' collection of recordings using SFTP.

When configured to allow a Wi-Fi hotspot there are several options available:

- **Network name** – the name of the Wi-Fi network that will be visible to other Wi-Fi users.
- **Wi-Fi password** – the password required to connect to the Wireless Access Point
- **Auto assign IP Addresses (DHCP)** – normally left on, this provides an IP Address to any user who connects
- **Encoder IP Address** – this is the IP address to use when accessing the encoder when connected via the wireless access point
- **Inactivity timeout** – (switched mode only) when switched by the user into access point mode the encoder will automatically revert to communication mode after the encoder has sent/received no network traffic on the access point for the supplied number of minutes.

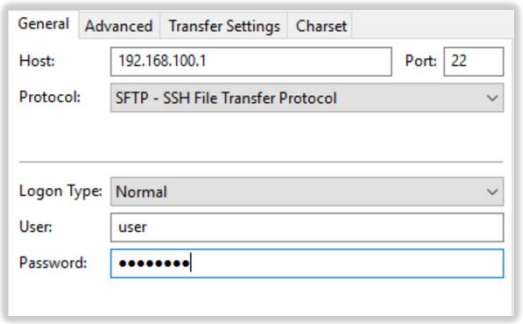
SFTP recordings download

The encoder supports the ability to download recordings using an industry standard SFTP (Secure FTP) download client, without the need to eject the disk. Once enabled there is only one setting required – a password that is used to protect access to the SFTP service.

If enabled an SFTP service will be available on every active communications method on the encoder *(if the firewall is enabled SFTP will not be available on the communications methods used to connect to EdgeVis Server)*.

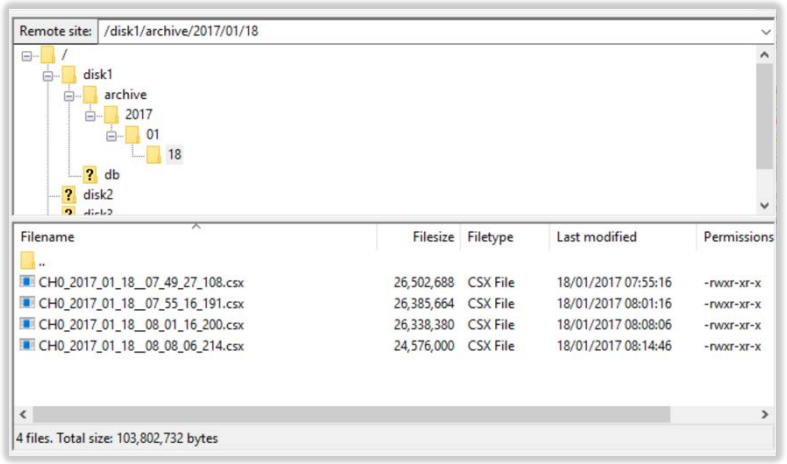
TIP: SFTP can be combined with the Wireless Access Point feature to provide a 'drive-by' recording download facility. The Wireless Access Point can be enabled/disabled easily from within EdgeVis Server and EdgeVis Client – once enabled a user can connect their laptop to the encoder using the Wi-Fi hotspot created by the encoder and then connect to the SFTP service to download the desired recordings. The Wi-Fi hotspot will then automatically disable itself 30 minutes after the final download is completed.

To connect to the SFTP service download and install an SFTP client (there are many free and open source SFTP clients available including WinSCP and Filezilla) and enter the following details:



- **Host / IP Address** – the IP Address of the encoder, on the communications method used to connect to the encoder (e.g. if connecting to the encoder via the Wireless Access Point the default is 192.168.100.1)
- **Protocol –** SFTP
- **Port –** Must be set to 22
- **Username –** user
- **Password –** as configured in the SFTP options

Once connected there will be four folders displayed (**disk1, disk2, disk3, disk4**) – an encoder may have multiple recording locations available. If only one recording location is in use all recordings will be in **disk1**.



The recordings will be organised within the following folder structure **archive / [Year] / [Month] / [Day]**, with each folder containing the recordings for that day. The filename is composed of the recording channel, followed by the date and time the recording was started at.

Once the desired folder/files have been identified use the download function to start the transfer of the files to the PC.

When the transfer is complete use the Media Manager application to review the encoder recordings.

NOTE: All recording timestamps are in UTC (GMT +0). For users in other time zones, it is necessary to manually perform the time zone adjustment when downloading specific files. For example, users in EST (-5hrs) should add 5 hours to the desired time to convert from EST to UTC.

Connecting an RDC Master Node *(HD-IP450/HD-IP470 only)*

It is possible to connect an RDC ground sensor system (from Digital Barriers) to the HD-IP450. This allows the encoder to perform local actions (e.g. send SMS, begin recording) and to send alert notifications to end-users upon detection.

Requires (either):

- RDC Master Node USB Serial Converter Cable (Part Number 1660-0090-0002)
- RDC Master Node to IP450 Cable (Part Number 1660-0317-0001)

Once the RDC master node is connected to the HD-IP450 it is necessary to enable RDC support by editing the encoder's settings page on EdgeVis Server. There are two ways to open the settings page:

1. Logging into the EdgeVis Server management interface
2. Use the search function to find the encoder, or manually enter the appropriate domain and select the encoder from the **Encoders** section

Or

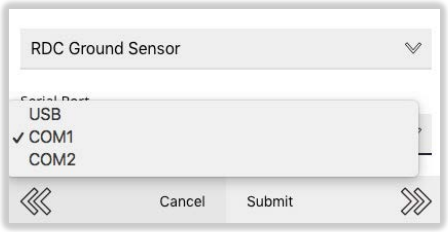
1. Open the video stream in EdgeVis Client v7.1+
2. Select **Configure Encoder** from the **Settings** menu

From the resultant settings page, the following options must be enabled:

Alarm triggers

From the **Alarm triggers** section:

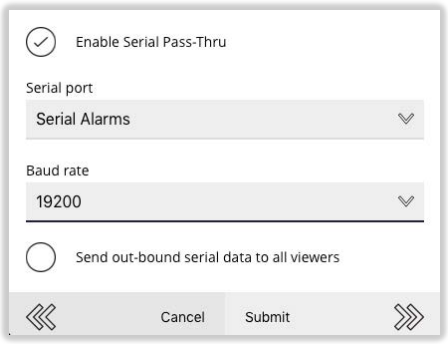
- Click the **Serial Sensor** item
- Select **RDC Ground Sensor** from the list
- Select the appropriate **Serial Port**, depending on the cable used to connect the RDC master node and the port it is connected to on the IP450.



Serial Pass-Thru

From the **Serial Pass-Thru** section:

- Tick **Enable Serial Pass-Thru**
- For **Serial Port** select **Serial Alarms**
- For **Baud Rate** select **19200**
- Ensure **Send out-bound serial data to all viewers** is not ticked



Once these settings have been configured, the IP450 will now be able to communicate with the RDC master node. Please refer to RDC documentation for further instructions on how to set up and configure RDC.

Persistent Logging

By default, an encoder maintains a developer-level debug log in its volatile memory to help with support issues. This can often be requested by Digital Barriers to diagnose customer issues. However, as the log is stored in memory, it is lost if the unit reboots or is powered down, making diagnosis difficult for some scenarios (e.g. vehicle deployments, or a comms issue that causes the encoder to reboot).

To help with difficult debug scenarios, it is possible to store the encoder's log files on the recording disk by logging into the local web configuration interface, and from the **Logs and Diagnostics** menu, select **Log Settings** and enable **Persist Log Files**.

This ensures that logs will persist after a reboot.

Note: Debug logs do not disclose encoder/user passwords, but will show messaging between the encoder and server, potentially disclosing information about encoder usage and server location.

As this is a potential security issue (storing debug logs on a removable disk) this feature is **DISABLED** by default. Please consider the deployment scenario carefully to ensure security.

Appendix A – Supported features on each EdgeVis encoder

As this manual covers multiple products, the following table should show if your product supports a specific feature:

	EdgeVis Video Router 4	HD-IP200	HD-IP250	HD-IP470	HD-Q800	EdgeVis MiniCam	4K-R800
Cellular	Built-in	Built-in	USB (Optional)	Built-in	Built-in	Built-in	Built-in
Wi-Fi	Built-in	USB	USB (Optional)	Built-in	Built-in	Built-in	Built-in
LAN/POE	2 x LAN	1 x LAN	2 x LAN (1 POE)	2 x LAN (2 POE)	1 x LAN (1 POE)		1 x LAN (1 x LAN via ECU port)
Wired Cameras					1 Built-in	1 Built-in	1 HDMI, 1 3G-SDI/ Composite
Maximum IP Cameras*	16	1	1	8	1 (external IP)	0	1
Picture in Picture	Y	N	N	Y	Y	N	Y
Quad View	Y	N	N	Y	N	N	Y
Recording disk	1 x Internal, USB, NAS	USB, NAS	USB, NAS	1 x Internal, USB, NAS	1 x Internal	1 x Internal	1 x SD Card, USB, NAS
RDC Support	N	N	N	Y	N	N	Y
SFTP	Y	Y	Y	Y	Y	Y	Y
SecureConnect	Y	Y	Y	Y	Y	Y	Y

* Assumes appropriate EdgeVis licence is available

Appendix B – Supported external communication devices

The encoder can support external USB communication devices to expand the available communication methods.

NOTE: Manufacturers can, and will, change chipsets used within their products, often without changing the product name/code. It is recommended to carefully check the chipset used within any desired adapter before committing to any large purchases. Devices with different chipsets will **not** work with the encoder.

To use an adapter

- plug the device into the encoder
- enable the communications device

Only one adapter of each type may be used in an encoder at once – use of multiple devices is not supported.

USB LAN Adapters

Using the latest firmware, the encoder includes a driver for the following USB LAN chipsets:

- Asix AX88772 chipset
- Asix AX88179 chipset (requires firmware V8.1 or greater)

Any USB LAN Adapter that uses any of these chipsets should be compatible with the encoder.

Devices known to contain the Asix AX88772 include:

- Edimax EU-4208 USB 2.0 Fast Ethernet Adapter
- UtechSmart USB 2.0 to 10/100 Fast Ethernet LAN Wired Network Adapter

Devices known to contain the Asix AX88179 include:

- Anker AK-A7610011
- Trendnet TU3-ETG
- Trendnet TU3-ETG

On EdgeVis MiniCam and Q800 it is recommended to only use a USB LAN Adapter for configuration, to avoid compromising the IP rating of the encoder. If required for comms, the Q800 provides an AUX LAN port which should be used.

USB Wi-Fi Adapters (IP Series only)

The encoder includes a driver for the following USB Wi-Fi chipsets:

- Realtek RTL8188CUS chipset (requires firmware V8.3 or greater)
- Realtek RTL8192CU chipset
- Realtek RTL8188EU chipset (requires firmware V8.1 or greater)

Any USB Wi-Fi Adapter that uses any of these chipsets should be compatible with the encoder.

Devices known to contain the Realtek RTL8188CUS include:

- Edimax N150 EW-7811Un V2

Devices known to contain the Realtek RTL8192CU include:

- Belkin N300 Micro Wireless USB Adapter (F7D2102)
- Edimax EW-7811UN V1

Devices known to contain the Realtek RTL8188EU include:

- StarTech USB150WN1X1
- TP-Link TL-WN725N Ver 3.0
- D-Link DWA-121

USB Cellular Modems (IP Series only)

The following cellular modems are supported. Please ensure the modem code **exactly** matches the listed modem as others are unlikely to work.

- **Skyus DS Europe** (Modem: MC7304)
- **Skyus DS** (Modem: MC7354)
- **Skyus 4G** (Modem: MC7354)
- **Skyus DS2** (Modem: MC7455)

It is also possible to add cellular support to an encoder using a LAN-based 4G modem. There are many different types available – including Teltonika LTE 4G and PocketPort 2 routers.

It should be noted that when using a LAN-based modem the encoder cannot detect when the modem switches from one technology (e.g. 4G) to another (e.g. 2G). The encoder will still auto-adapt the video bandwidth to ensure a consistent video stream, however it will not adjust the framerate/dimensions automatically based on the network technology's profile. This is more of an issue with mobile encoders where the technology would be expected to change continually, as opposed to a static encoder where it would be expected that the network technology should be fairly consistent.

Appendix C – Frequently asked questions

What web browser can I use for the setup?

A web browser with JavaScript enabled and HTML5 compatible is required. The encoder's web interface should work with Internet Explorer 10+ and the latest versions of Microsoft Edge, Firefox, Chrome and Safari.

How is firmware upgraded on an encoder?

Once notified of a new software release by Digital Barriers, updates are available for download from the EdgeVis support site for installation onto the device.

There are three ways to update the firmware – locally using a USB Pen, or remotely using EdgeVis Server, or using the encoder's local web interface.

- To update remotely, a System Administrator must upload the new firmware to the Firmware section within EdgeVis Server web interface and then, from within the Encoder page (under the Firmware section) select Upgrade Firmware.
- Copy the firmware file onto a USB flash drive and insert into a USB port on the front of the unit. For devices with multiple three-colour LEDs they will all turn solid green upon completion. For those devices that do not have LEDs it is recommended to use a timer to measure 20-30 seconds before unplugging the USB. Then, if successful the encoder will reboot.
- Log into the local web interface and select the **Upgrade firmware** menu option from the **Advanced Settings** section at the bottom of the main page.

What if I do not know the login password?
What if I need to restore the encoder to default factory settings?

It is possible to factory reset an encoder. Create an empty file called **FACTORY_RESET** on a blank USB Flash Drive and insert it into a powered encoder. After approximately 30 seconds the encoder should be reset to factory defaults.

What if the encoder can't connect to my EdgeVis Server?

An encoder will only connect to the EdgeVis Server once all stages of the setup process have been completed.

If all the stages have been completed the home page should show green ticks for communication and server settings to signify the encoder is now connected to the server and is available for viewing. The following checklist should provide some guidance if the encoder does not connect to the server:

- Confirm the encoder account created in EdgeVis Server matches the account on the encoder, and that the appropriate licence has been allocated to the encoder account
- Ensure the IP address for the EdgeVis Server is correct and that the server is accessible from the internet
- Try disabling server encryption (if it is enabled) to ensure that it is not an encryption pack issue
- Cellular users should ensure that the right SIM slot has been used and that the configured APN settings are correct. Test the SIM card with a smart phone to check the SIM settings and confirm there is a mobile signal
- LAN/Wi-Fi users should ensure the network that the encoder is configured to use is connected to the Internet

If this list does not help, try some alternative settings to try and narrow down the issue. For example, using a different encoder account, EdgeVis Server or communications bearer to eliminate server/comms/account issues.

Appendix D - Troubleshooting camera discovery issues

What makes and models of IP camera does the encoder support?

EdgeVis encoders only have two camera drivers; ONVIF or RTSP, and only H.264 is supported.

The ONVIF driver has been tested with a wide range of cameras (including those from Axis, Bosch, Canon and Panasonic). For the latest list of tested cameras, refer to the appropriate Knowledge Base article on the Digital Barriers support site: http://tvi-support.digitalbarriers.com/.

What if I cannot see my camera listed when I search for cameras?

Unfortunately, auto-discovery can sometimes fail to find a camera. This can be for a number of reasons:

- The IP camera and the encoder do not have compatible IP addresses
  Check that they are on the same subnet, but do not have the same IP address
- IP cameras are also mini-computers that can take time to boot up (often several minutes)
  Allow the camera time to boot up before the auto-discovery process – or reboot if it has crashed
- The IP camera may not be a supported device
  Review the camera model against the IP Series Camera Compatibility List
- The firmware on the IP camera may be out of date and causing an issue
  Check the version of firmware that is installed on your IP camera and update if required

If the encoder is still unable to find the IP camera automatically, try adding the camera manually. Use the **Add camera manually** menu option and enter its IP address/login details manually.

What if I cannot successfully add the IP camera?

If the camera will not add (and provide a 'green tick'), or is not available to preview, the following check list provides some guidance on how to fix this issue:

- If the camera uses PoE for power, check that the camera is receiving power from the encoder. If possible, try to power the camera independently during testing to eliminate PoE issues. On the IP250, ensure that POE is also enabled on the encoder
- Ensure the camera is booted up and available by allowing at least 30-120 seconds for it to 'warm up'
- Try restarting the camera in case it has crashed
- Delete and add the camera again, confirming the username and password is correct
- If multiple services are offered while adding the camera try selecting an alternative video service
- Plug the camera into a different network and log into it directly to confirm it is operating correctly and can be connected on the IP Address. *ONVIF Device Manager is a free open source tool that can be used to view the video feed from the camera*

What if I don't know the IP address (or login details) of my IP camera?

The simplest way to overcome the loss of any details for an IP camera is to download the manual for the camera, which should provide instructions on resetting the IP camera to its factory settings and obtaining the factory configured IP address, username and password. With the default camera details in hand, it should then be possible to connect the camera to the encoder and enter the correct details.

Setting the IP address on a camera to function with an encoder

To modify the IP settings on a camera, refer to the instructions from the camera manufacturer. These will outline how to log into the camera (using a PC/laptop), which will require the username and password for the camera. If unavailable, refer to instructions for performing a factory reset (note that it may be necessary to download a setup application from the manufacturer). It is important to note that any Power-over-Ethernet (PoE) cameras must be connected to a laptop/PC via a PoE switch to both connect to, and power the camera.

After logging into the IP camera, it will be possible to set the IP address within the ranges compatible with the encoder. Note that each camera connected to an encoder **must** have a different IP address to avoid conflicts.

Setting the IP address of a port to function with an existing camera

To connect a camera to an encoder device without modifying the camera's settings, the IP address of the corresponding port will need modified to be on the same subnet as the camera. For example, if the IP address of the camera is **192.168.54.11**, the IP address of the port would be entered as **192.168.54.X**, where **X** is any number in the range between 2 and 254. The subnet mask for the port should be entered as **255.255.255.0**.

What if my IP camera supports multiple video streams?

If the IP camera can supply multiple video feeds (e.g. the Axis F44 supports four independent camera sensors) the encoder will detect this and present a list of available ONVIF 'sources' that the camera offers. The names listed are supplied by the camera - it may not be immediately obvious which service relates to each camera.

If it is not possible to determine the camera from the name listed, it is recommended to add each service in turn and use the **Preview video feed** menu option (within the camera settings page) to determine which service provides each video feed.

Next steps…

After completing the steps contained within the previous sections you should have an encoder connected to an EdgeVis Server. This section outlines the steps you should take next.

Installing a viewing client

Once the encoder is configured and connected to EdgeVis Server the next step is to install EdgeVis Client to allow remote access to the video from the encoder. EdgeVis Client is available on Windows, iOS or Android, and can be downloaded directly from the Digital Barriers Support Site, along with the **EdgeVis Client Quick Start Guide**.

Configuring the streaming parameters

Once the encoder is configured and connected to EdgeVis Server, it is possible to perform a more in-depth configuration of the unit using EdgeVis Server's web configuration interface. Refer to the **EdgeVis Server Setup Guide** for further details.

Creating alarm rules and utilising low power modes

It is possible to customise the behaviour of an encoder by utilising alarm triggers to perform actions such on-demand recording, camera positions, relay triggering, and user notification. Long-term battery deployments (on specialist encoders) are also made possible using a combination of alarm rules and low-power sleep modes. For further information please refer to the **EdgeVis Alarm and Sleep Management Guide**.