Digital Barriers

EDGEVIS SERVER

SETUP GUIDE

VERSION 8.0.3 – JANUARY 23

This document will explain how to install EdgeVis Server, obtain the appropriate licences and then create the encoder and user accounts. This creates the infrastructure a user will need to set up and view the video from an EdgeVis encoder.

EDGEVIS™ Live
Powered by TVI

QUICK START GUIDE 5

INSTALLING EDGEVIS SERVER 6

Before you begin... 6
Cloud/virtual machine users 7
Installing EdgeVis Server on Linux 7
Installing a multi-server installation using MSR 7
Anti-virus exclusions 7
Installing EdgeVis Server on Microsoft Windows 8
Portable Servers 9
Start Menu Shortcuts 10
Logging in to the management portal 10
Browser compatibility for the EdgeVis Server management portal 10
Firewall ports – making the server accessible externally 11
Installing licences on EdgeVis Server 11
Requesting the encoder licence files 12
Installing the licence file onto the server 13
Licences for additional purchases 13

ORGANISATIONAL STRUCTURES WITHIN EDGEVIS SERVER 15

ROLES AND PERMISSIONS 16

Introducing Role-based access control 16
Assigning roles to users and defining the role scope 17
Creating a custom role 18
Assigning a server-wide role to a user 19
Assigning a user role to a specific domain 20
Assigning a user role to a specific group 21
Assigning a user role to a specific encoder 22

DOMAINS 23

Managing domains 23
Export/import of domains 23
Moving encoder and user accounts between domains 24
Promoting a domain user to a Server-wide Administrator 24
Sharing encoders and users across domains 25

SERVER HOMEPAGE 27

Managing server-wide administrators 28
Monitoring active viewers 28
Messaging configuration 28
Automated account creation emails 29
Enabling the e-mail account system 29
Testing the e-mail system 30
Security of links within e-mails 30
Disabling automated e-mail accounts 30
Login and password policies 31
Password settings 31
Viewing client settings 31
Global settings 31
Two factor authentication (2FA) 32

TVI Encryption 34
SSL configuration 35
Sending automated maintenance alerts 36
Editing maintenance alerts *37*
Firmware Management 38
Upgrading an encoder's firmware *38*
Warning: downgrading encoder firmware *39*
Bulk firmware update *39*
Backing up and restoring EdgeVis Server 40

GROUPS 42

Managing groups 42
Group details page 43
Managing users in a group *43*
Managing encoders in a group *43*

USER ACCOUNTS 44

Managing Server-wide Administrators 44
Managing domain users 45
User details page 45
Setting contact preferences *46*
Managing a user's roles and permissions *46*

ENCODER ACCOUNTS/CONFIGURATION 47

Managing encoder accounts 47
New encoder account details page 48
What EdgeVis licence does each product require? *48*
Use the encoder account details to configure the encoder *48*
Online encoder configuration options 49
Section: Device Status *50*
Section: Video *51*
Section: Streaming *53*
Section: Lifecycle management *58*
Section: Advanced settings *59*

USING AN SSL CERTIFICATE WITH THE WEB MANAGEMENT PORTAL 62

Introduction to SSL 62
Setting up EdgeVis Server to use Let's Encrypt 63
Using an Externally Generated Certificate 64
(Optional) Step 1 – Generate request files *64*
Step 2 – Upload the certificate *66*

MESSAGING CONFIGURATION 67

Mobile Push Notifications 67
Server settings for push notifications *67*
Registering users for push notifications 67
SMS Text Message Notifications 68
Server settings for SMS *68*
Important note for US Customers *69*
User settings for SMS *69*
Configuring e-mail for notifications and account e-mails 69

Server settings for E-Mail *69*
Internal SMTP settings *70*
Microsoft Exchange settings *70*
Google Mail settings *71*

Quick Start Guide

This document is a reference guide that outlines the installation and use of EdgeVis Server. While reading the entire document is recommended, the following summary outlines the typical steps required to set up and configure a server for use by encoders and viewers.

Minimum server setup steps:

- Install EdgeVis Server (page 6)
- Open any necessary firewall ports (page 11)
- Install the necessary encoder licences (page 11)
- Create the first domain on the server to hold encoder and user accounts (page 23)

Enable advanced account creation:

- Configure an e-mail server to allow users to receive account creation e-mails (page 28)
- Review two-factor authentication settings (page 32)

Getting an encoder online:

- Take a note of the server's encryption settings (page 32)
- Create the first encoder account, and assign it a licence (page 47)
- Configure the encoder with the necessary login/connection details (see encoder's setup guide)
- Create the first viewer account in the domain, and allow it to access the encoder (page 45)
- Use a viewing client to view the encoder's video stream (see EdgeVis Client Quick Start Guide)
- Customise the encoder's settings using the management portal (page 49)

Customise the server:

- Decide advanced account options and password complexity rules (page 29)
- Obtain an SSL certificate for the management portal (page 35)
- Set up alarm notification messaging - Push notifications, SMS and Email (page 28)
- Provide custom roles and permissions for users (page 18)

Installing EdgeVis Server

EdgeVis Server is a software application that sits on a publicly accessible machine, as a point of contact for EdgeVis encoders and viewers. It is responsible for receiving the video from each encoder and redistributing it to each viewer. This section shows how to install EdgeVis Server within your organisation.

Before you begin…

The following hardware specifications will support up to 500 encoders and 500 video streams simultaneously. Users looking to support more than 500 encoders should consider utilising multiple servers – please refer to the following section **Installing a multi-server installation using MSR**.

- A 64-bit PC running Windows 8 and above or Ubuntu 18.04 LTS/20.04 LTS, Red Hat / Centos 7.6
  Other Linux distros may work, but installation support will be limited on other platforms
- Up to 20 encoders (stand-alone server)
  - Dual-Core 2.0GHz+ processor, Quad-core or Intel i3 or higher recommended
  - 4GB RAM, 8GB recommended
- Up to 200 encoders
  - Intel i5/Xeon Quad-Core 2.5GHz+ processor *(note that many mobile i5/i7 processors are only dual core)*
  - 8GB RAM
- Over 200 encoders
  - Intel i5/Xeon Quad-Core 2.5GHz+ processor *(note that many mobile i5/i7 processors are only dual core)*
  - 16GB RAM
- At least 4GB free disk space
- A static IP address (both on the local network, and externally to the Internet)

All installation types of EdgeVis Server require:

- An internet connection that can support the combined bandwidth needs of the encoders and viewers
- Specific ports opened/forwarded on any intervening Internet firewall/router for video transmission. Not opening individual ports can be used to disable access to those services from the internet:

Encoder	Port 9300 (UDP)
Viewer	Port 9300 (TCP) – Initial connection channel (unencrypted) Port 9301 (TCP) – Initial connection channel (encrypted) Ports 2048 (UDP) – Video / Full-res / Recording Download channel
Server Web Management Interface	Port 9443 (TCP)

- An accurate synchronised system clock (Windows will do this automatically; Linux may require an NTP client)

Running EdgeVis Server in a multiple server configuration requires the following:

- Each of the PCs in the cluster must be accessible to the other PCs *without* using port forwarding. For example, they must all be on the same local network or on networks connected together using a VPN.
- Specifically, these ports must be accessible on each server PC (from every other server PC):
    - Port 1527 (TCP)
    - Ports 47100 & 47500 (TCP)
- The connections between all the server PCs must meet these requirements:
    - Maximum 100ms round trip time
    - Minimum 10mbps bandwidth, 50mbps recommended
      Slower links will result in a longer recovery period after a failure.
- Multiple servers may share one internet connection with port-remapping.

Cloud/virtual machine users

Running in a virtual machine/cloud environment is supported, however be aware that most virtual machines share resources between other users, and performance may suffer in an unpredictable manner.

To counter this it is recommend to over-specify any virtual machine. For example, Amazon users should consider a **m5.xlarge** instance for systems running > 20 encoders.

Installing EdgeVis Server on Linux

Installation on Linux is a more involved process than Windows – with a manual installation and setup process, and as such is outside the scope of this document.

The document **EdgeVis Server v8 – Linux Installation** provides more details on how to install/upgrade servers on the Linux platform.

Installing a multi-server installation using MSR

At its simplest, MSR (Multi-site Resilience) is the ability to have multiple servers work together to provide an automatic fail-over capability so that, should one server fail, the remaining servers take over and all existing encoders/viewing clients continue to operate without user intervention.

MSR is an enterprise level feature that requires careful planning, and as such it is recommended to refer to the **EdgeVis Server v8 - Enabling Multi-site Resilience** document which provides preparation checklists and more details on how to install multiple servers into a server cluster.

Anti-virus exclusions

After installation it is **strongly** recommended that the EdgeVis Server database is excluded from any anti-virus scanning. This is the 'pg_data' directory under the EdgeVis Server application directory (typically C:\Program Files (x86)\EdgeVis Server\ on Windows or /opt/edgevis-server on Linux).

Installing EdgeVis Server on Microsoft Windows

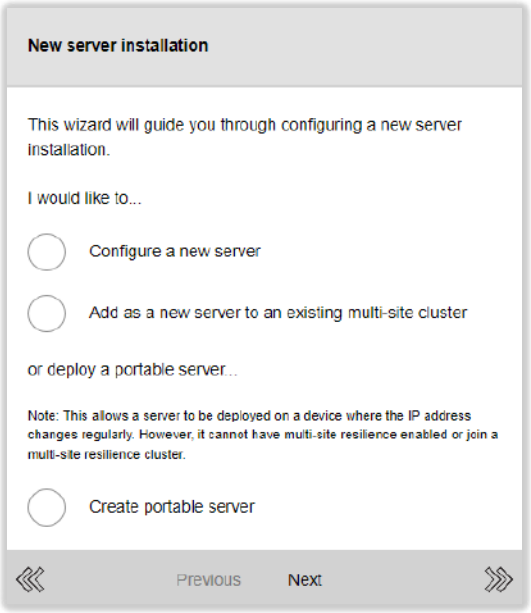
Download the Windows server installer from the Digital Barriers Support Site.

Run this installer (which must be run by a user with administrative privileges) which will install the files and services required for EdgeVis Server. It can also automatically open the required ports on Windows Firewall (please note that any Internet routers or non-Microsoft firewalls will need to be configured separately).

Once the installer has completed copying the files on the PC, the installer will open a web browser at the initial server configuration wizard.

It requires the following pieces of information to be entered:

- **Type of installation** – there are three different options:
  - For the majority of users, the first option is likely the correct option and should be used for a fixed-infrastructure server. This options also allows the user to upgrade the server to multi-server MSR at a later date. **For the purposes of these instructions select this option.**
  - The second option is covered within the MSR documentation, as it is used to create the additional servers required within a multi-server installation.
  - The third option allows the user to create a 'portable server' – this is a server that can be used with internet connections that frequently change (e.g. on a cellular/satellite laptop). Please refer to the following section **Portable Servers** for further details.

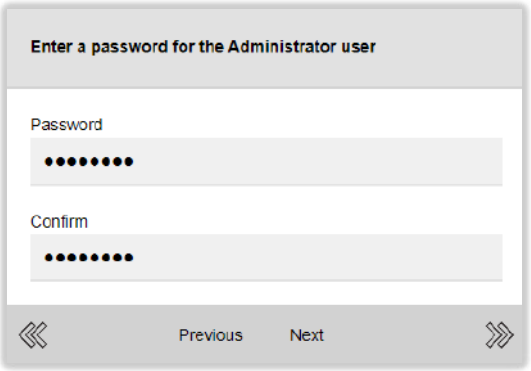


- **Server Name -** the next question is to enter a name for the EdgeVis Server:

  The EdgeVis Server name serves two purposes: a user-friendly display name within EdgeVis Client to distinguish between different EdgeVis Servers; and as part of the encryption process (changes to the name require a new encryption pack to be generated that must be distributed to every TVI encoder – using the USB configuration software or local web configuration interface).

- **Administrator Password** – this allows the user to set the password of the default **Administrator** account.

  This password must be used to log in to the server for the first time.



- **Addresses for this server –** it is required to supply the IP addresses for the server.
  (Not required for portable servers)

  - The external address is the IP address encoders will use to connect to the server from outside the organisation (e.g. from the internet).

    This Google link can help determine the IP address if it is not known.
  - The internal address is the IP address of the server on the local network. *Note: For server redundancy this IP address must be accessible to all PCs that participate in the cluster.*

Once complete the server will take approximately one minute to initialise the databases and services required. Once complete the web browser will load the server management portal.

Portable Servers

During the installation of a standard standalone EdgeVis Server it is necessary to enter the External and Internal IP addresses. This is to allow for a potential Multi-Server MSR installation, where each server has to tell encoders/clients how to connect to this particular server, and to allow MSR servers to connect to each other automatically.

However, in certain circumstances it is not possible to know the internal IP address of the server in advance, or it is an address that may change often (e.g. on a mobile laptop server that uses cellular/satellite communications for internet access).

The EdgeVis Server installer allows the user to skip the requirement to supply internal/external IP addresses during installation, but with the limitation that this server can't be later used to upgrade to an MSR installation automatically.

A portable server does not operationally change how the user/viewers/encoders connects to the server – the only change is that the server does not have the information required to enable MSR.

Start Menu Shortcuts

The installer will also create several shortcuts on the Start menu in a folder called **EdgeVis Server**:

- **EdgeVis Server Login -** opens the web-based configuration for EdgeVis Server in a web browser.
- **Restart Server -** stops and starts the EdgeVis Server.

Logging in to the management portal

Once the installation is complete, the web browser will automatically open the server's web management portal (or, manually by selecting **EdgeVis Server Login** from the **EdgeVis Server** group in the Start Menu). Alternatively open a web browser and, if on the same machine, use the following address:

https://localhost:9443/

If attempting to connect from a different computer, connect as follows:

https://[external ip address]:9443/

If the EdgeVis Server PC or network has a firewall enabled, ensure that port 9443 is opened. The management portal operates over the secure HTTPS protocol and all communication between the web browser and EdgeVis Server is securely encrypted.

A self-signed certificate is created on installation, causing the browser to show a security warning. Accept the security exception to connect. On loading the page, a log-on screen is presented. Enter the default username and password:

- **Username:** Administrator
- **Password:** <as entered during the initial setup>

Browser compatibility for the EdgeVis Server management portal

EdgeVis Server requires an HTML5 browser with JavaScript and local storage enabled. It is tested with: Internet Explorer 10+, and the latest version of Microsoft Edge, Firefox, Chrome, and Safari. Other browsers may work but are unsupported.

Firewall ports – making the server accessible externally

While the installer will automatically open the firewall ports on the installation PC, making EdgeVis Server available to the internet will likely require the same ports opened on any additional firewalls and routers between the server and the internet.

For example, most internet connections have an internet router (or NAT'd firewall) between the internet and the local network. By default, these routers will not allow traffic into the network meaning it is impossible to connect to the EdgeVis Server from outside the local network.

The following ports will need to be opened on any firewall, and port-forwarded to the EdgeVis Server's PC to allow encoders and viewers to connect to the EdgeVis Server:

EdgeVis Encoder and Client Ports

- Port 9300 (UDP) – Encoder connection channel
- Port 9300 + 9301 (TCP) – Viewer control channels (9300 unencrypted, 9301 encrypted)
- Port 2048 (UDP) – Viewer video channel

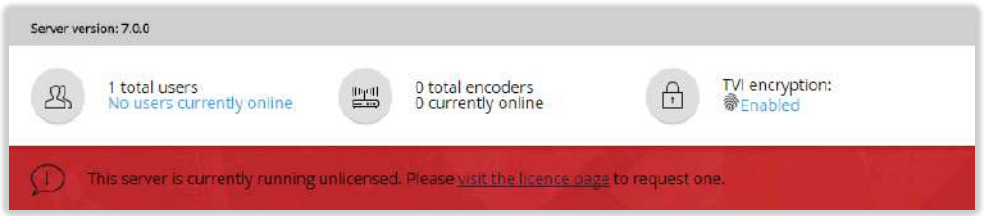
EdgeVis Server Web Management Portal *(optional – if external access is required)*

- Port 9443 (TCP, HTTPS)

Networking security can be a complicated subject - it is recommended that properly trained IT staff should perform this step to ensure the network security of your organisation is maintained.

Installing licences on EdgeVis Server

On logging on to the server for the first time, the server will display a warning on the server homepage that the server does not have any licences installed that would allow encoders to be available on the server.



The different products within EdgeVis require that each be assigned the appropriate types of licence. EdgeVis Server does not come with any pre-installed licences, and so it is necessary to obtain the corresponding licence from Digital Barriers after receiving the encoder. *It is not possible to purchase a hardware encoder without purchasing the equivalent software licences – these licences can be obtained from Digital Barriers during installation.*

Requesting the encoder licence files

From the server homepage click the **visit the licence page** warning message (or use the **Licence Management** option in the **Maintain this server** section on the homepage).

This will display the licence page for the server which will show that there are no available licences:

This should show that the server has no licences available. Select the **Request a new licence** menu option.

This will then prompt for a **Sales reference number**. This can be found on the paperwork received from Digital Barriers with the encoder(s).

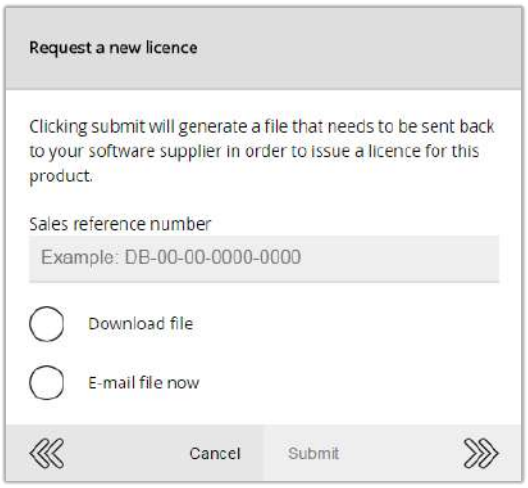
This number takes a standard form:

DB-XX-XX-XXXX-XXXX (where X is numeric)

This will generate a licence request that must be sent to Digital Barriers. It is possible to either download the request, or embed it directly into an e-mail. Whatever mechanism is selected this information should be e-mailed to:

licences@digitalbarriers.com

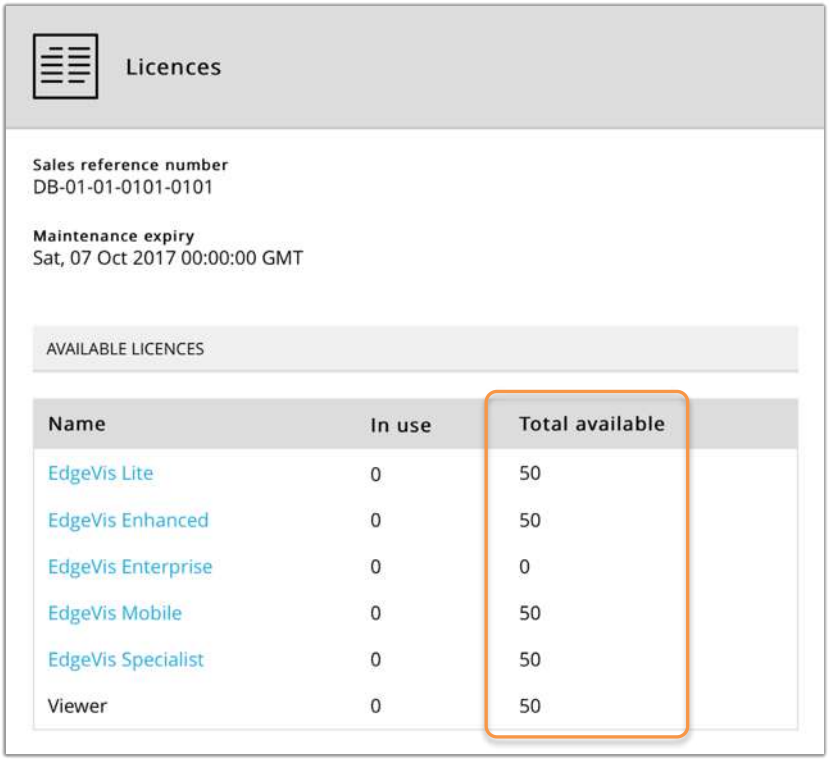
Digital Barriers will create the appropriate licence file that will be returned to the e-mail sender, allowing the licences to be installed onto the server.



Installing the licence file onto the server

Once the licence file has been received from Digital Barriers the next step is to upload the file to EdgeVis Server. Return to the **Licence Management** page and use the **Upload a new licence** menu option. This allows the received licence file to be uploaded to the server.

The new licence file contents should now be reflected on the **Licence management** page:



With the licences installed it is now possible to create the accounts necessary to attach an encoder to the server.

Licences for additional purchases

To purchase additional encoders to use on the server the above steps must be carried out again, to install the additional licences for the new encoders. The process is almost identical, with one simplification. During the purchase of the new encoders the original **Sales Reference Number** of the EdgeVis Server must be supplied to Digital Barriers – this is presented within the **Licence management** page.

When requesting a new licence file EdgeVis Server will remember the original **Sales Reference Number** entered during the initial setup and will not request a new Sales Reference Number. Send the request as described above, which must include the original Sales Reference Number.

SERVER ORGANISATION CONCEPTS AND CONTROLS

This section of the manual explains the organisational structures used within EdgeVis Server, the roles and permissions system, and the organisation of encoders and users into self-contained domains.

Organisational structures within EdgeVis Server

EdgeVis Server offers a number of organisational structures to allow administrators to segment their servers into logical groupings and manage different operational needs.

Encoders

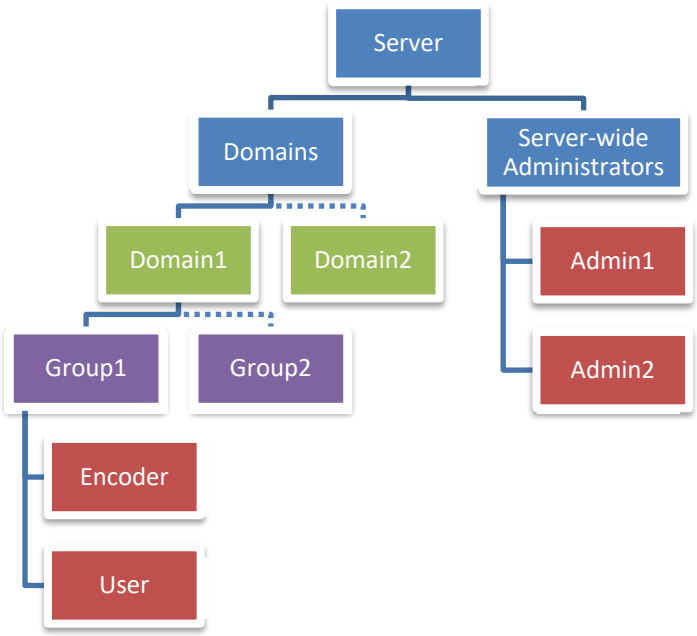
An encoder is an entity (that can be a hardware device or a software package) that can publish services within EdgeVis, including live TVI video streams, edge video recording, alarm triggers, location data.

Users

A user is an entity (including viewing clients or third-party integration tools) that accesses EdgeVis in order to consume a service from an encoder.

Server-wide administrators

A special type of user who has access to every domain, encoder and user within the system and, if granted the appropriate permissions, has the right to configure and manage the server.



Domains

All encoders and users must exist within a domain. A domain is a segmented area within EdgeVis Server where all encoders and users are only visible to other users within the domain. This allows server administrators to keep different customers/user communities separate (and hidden) from each other - a user within the domain can't see a server-wide administrator or a user in another domain. It is possible to create multiple domains on the server.

When creating alarm rules, users can send notifications to any other user within the domain.

Groups

A group is a mechanism used to simplify role and permission management. For example, if there is a building with five encoders (providing video surveillance) and a number of security guards who must be provided access to those encoders there are two ways to provide the security guards access:

Without groups, it is necessary to assign each security guard the appropriate viewing permissions to each encoder individually. When a new guard is hired, they too must be given five permissions (one to each encoder), and if a new encoder is added to the building it is necessary to find each security guard's account and individually grant them permission to view the new encoder.

With groups, it becomes considerably simpler to manage, as a group is created to hold all the encoders **and** all the security guards. When adding a new security guard to the group they are granted one viewing permission, *to the group*, meaning they have access to all encoders within the group. When a new encoder is added to the group, all security guards are immediately granted with the same level of access.

An encoder and user can be added to multiple groups – in the example above a security guard may have permission to access encoders across multiple buildings by being a member of multiple groups.

Roles and permissions

Introducing Role-based access control

EdgeVis Server uses Role-based Access Control (RBAC) to regulate users' access to the server, groups and encoders. Rather than assign individual permissions to a user on a case-by-case basis, it is first necessary to create a **Role** that contains all the desired permissions for a user and assign *that* role to a user.

The permissions within EdgeVis Server fall into three different categories:

- Server permissions
  The ability to manage the server, including managing domains, server settings, backup/restore and role editing
- Account management
  The ability to create/edit/delete groups, encoders and users
- Encoder usage
  The ability to control how encoders are configured and used within viewing clients

Each category has several sub-categories, each of which contain many granular permissions for each sub-category. The following table outlines the different categories, sub-categories, and number of available permissions within each.

Role *contains one or more permissions from the following…*		
Server permissions *(Server-wide administrators only)*	**Account management**	**Encoder usage**
Domain management User role management Server configuration Backup/restore database Encoder firmware	Manage group accounts Manage encoder accounts Manage user accounts	Viewing client permissions Accessing edge recordings Configure streaming parameters Encoder configuration Encoder maintenance

There are four built-in roles (that can't be modified or deleted):

- **Server Administrator** – all permissions available within the system
- **Domain Administrator** – all permissions related to managing all actions within domains
- **Encoder Administrator** – all permissions within the **Encoder usage** section
- **Viewer** – all operator-level permissions within **Encoder usage**

It is also possible to create roles that contain any combination of permissions to match operational requirements.

Assigning roles to users and defining the role scope

Once a role has been created/selected for a user, the second decision an administrator must make is to decide the **scope** the user has access to. There are four possible scopes:

- **Server-wide** – the top level of the server, above all domains. A user granted a role at the server level will have those permissions on any encoder/user/group in any domain in the system.
- **A specific domain** – assigning a user a domain-wide role will grant them the appropriate permissions on any encoder/user/group in the specified domain.
- **A specific group of encoders** – to limit a user to only using/administering a group of specific encoders
- **A specific encoder** – to limit a user to only using/administering one specific encoder

For example, the following table describes the effects of assigning a user one of the built-in roles (Server Administrator, Domain Administrator, Encoder Administrator or Viewer) to each of the different scopes (Server-wide, a specific domain, and a specific group/encoder):

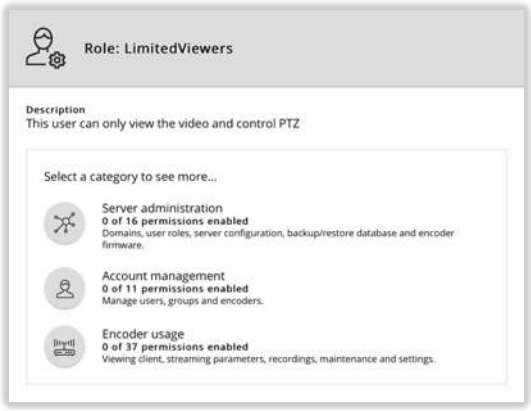
	Role Scope Examples *the user is given the following permissions based on the following scopes…*		
Role	**Server-wide**	**A specific domain**	**A specific group or encoder**
Server Administrator	All permissions available on the server, on any domain and on any group/encoder (i.e. full access)	All permissions in the **Account Management** and **Encoder usage** section on… any encoder/user in the domain	All permissions in the **Account Management** and **Encoder usage** section on… the specified group/encoder
Domain Administrator	All permissions in the **Account Management** and **Encoder usage** section on… any encoder/user on the server	All permissions in the **Account Management** and **Encoder usage** section on… any encoder/user in the domain	All permissions in the **Account Management** and **Encoder usage** section on… the specified group/encoder
Encoder Administrator	Can perform any **Encoder usage** permission on… any encoder on the server	Can perform any **Encoder usage** permission on… any encoder in the domain	All **Encoder usage** permissions on… the specified group/encoder
Viewer	Can perform any viewer permission on… any encoder on the server	Can perform any viewer permission on… any encoder in the domain	Can perform any viewer permission on… the specified group/encoder

Creating a custom role

From the **User roles** page use the **Create role** menu option to create a new custom role. After entering a name and description the role details page is listed.

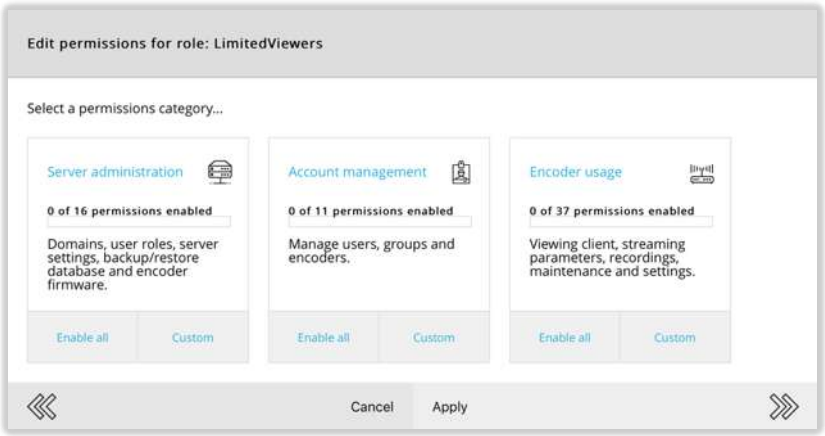
This page lists a summary of the permissions granted to the role – by default any new role has no permissions assigned.

To assign permissions to a role (or to change an existing role's permissions) use the **Edit permissions** menu option.



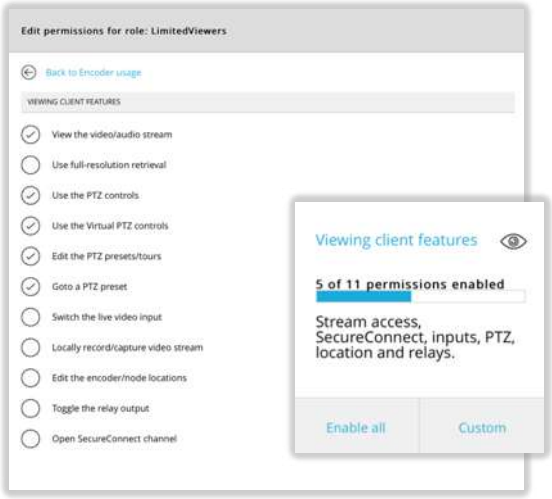
Tip: it is recommended to enter a meaningful description that describes the purpose of the role, to help administrators who assign roles to users – this avoids having to drill down into the role to determine the permissions assigned to a role.

There are over sixty individual permissions within EdgeVis Server – to help make permissions more manageable they are categorised into three areas (Server administration, Account management, Encoder usage), each of which contains a number of sub-categories.



Each category (and sub-category) has a master **Enable/disable all** to quickly toggle all permissions on or off, or use the **Custom** button to drill down into the permissions contained within the category.

At the lowest level, it is possible to enable individual permissions within each category. There are no restrictions on the combinations allowed - except for the **Account management** category, where the interface will force certain permissions to avoid creating invalid roles (e.g. to create a user account, it is required to have the edit user account permission).

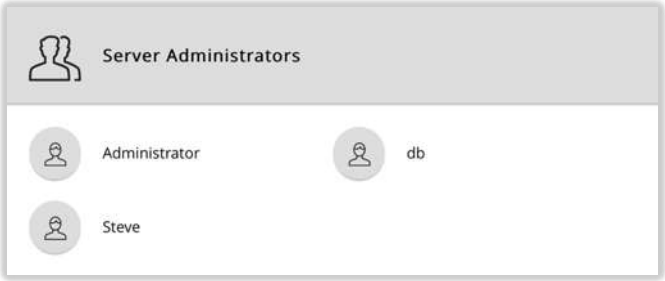


Assigning a server-wide role to a user

When to use: There is a requirement to either provide a user the ability to configure/monitor the server or provide the user with a level of access to **all** domains, and groups/encoders/users within each domain.

Users with a server-wide role do not exist within any domain and can be viewed by selecting the **Server Administrators** button on the server home page.

This will display a list of Server Administrators, including the default **Administrator** account. To view an existing user's details, including their assigned role, click on their name. To create a new user with a server-wide role use the **Create user** menu option and enter a name and password – this will then display the new user's details.



The user's detail page will display their communication preferences and the role(s) they have been assigned.

To add or change the roles, click the roles icon in the **Server Wide Access** section (which may indicate that no roles are currently applied).

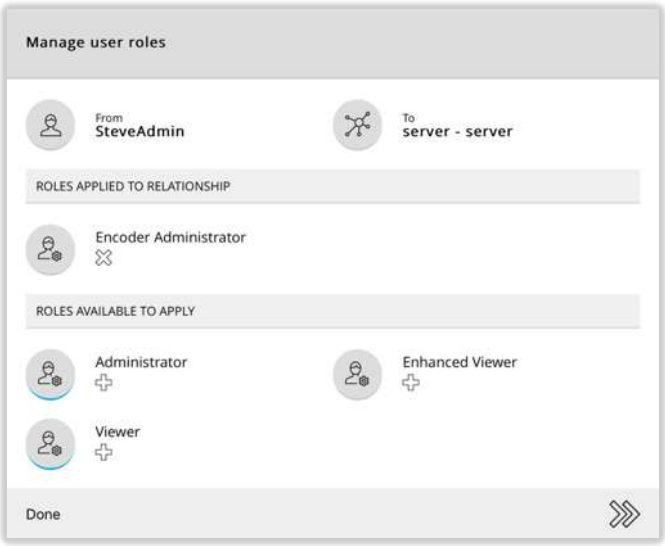
This will open the **Manage user roles** page which will display the user's existing roles.

The bottom section of the page lists all the roles available on the system, which can be assigned to the user by using the plus icon.

The middle section of the page lists the roles assigned to the user. To remove a role, use the delete icon.

To view the permissions a role will grant, click on the role's icon. This will display a summary of the role, where it is possible to drill down into each role's categories and the individual permissions within.

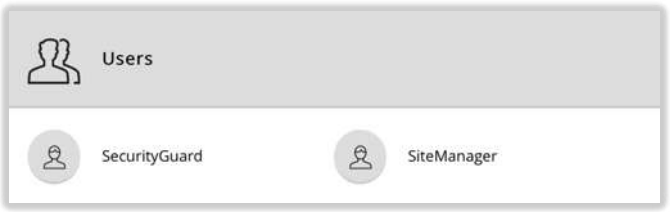
It is possible to assign multiple roles to a user, which creates an additive effect granting the user all the permissions contained within each role.



Assigning a user role to a specific domain

When to use: There is a requirement to provide a user, within a **specific** domain, a level of access (for example account management) to **all** groups/encoders/users within that domain.

From the domain's homepage select the **Users** icon to display a list of users within the domain. To view an existing user's details, including their assigned role(s), click on their name. To create a new user, use the **Create user** menu option and enter a name and password – this will then display the new user's details.



The user's detail page will display their communication preferences and the role(s) they have been assigned.

To add or change any domain-wide role, click the roles icon in the **Domain Wide Access** section (which may indicate that no roles are currently applied).

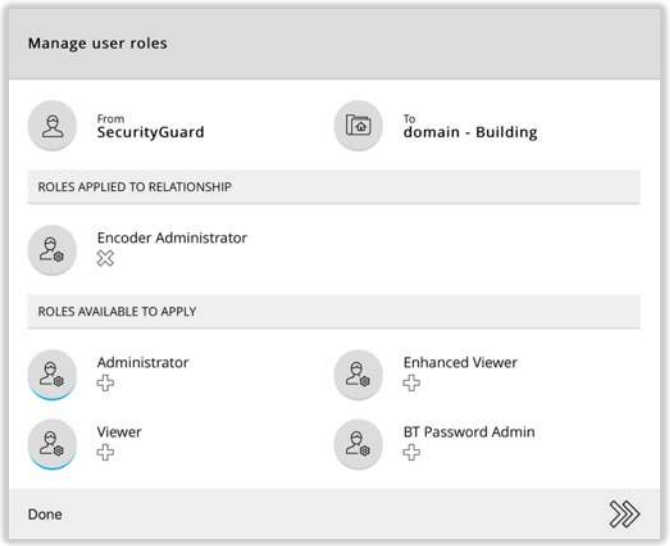
This will open the **Manage user roles** page which will display the user's existing roles.

The bottom section of the page lists all the roles available on the system, which can be assigned to the user by using the plus icon.

The middle section of the page lists the roles assigned to the user. To remove a role, use the delete icon.

To view the permissions a role will grant, click on the role's icon. This will display a summary of the role, where it is possible to drill down into each role's categories and the individual permissions within.

It is possible to assign multiple roles to a user, which creates an additive effect granting the user all the permissions contained within each role.



Assigning a user role to a specific group

When to use: There is a requirement to provide a user a level of encoder access to a specific group of encoders within a specific domain.

This is the preferred method of assigning roles and permissions for users who predominately configure or view video from encoders, as it limits access to only the encoders contained within the group.

Step 1 - If necessary, create the user and encoder accounts for the encoders/users.

Step 2 - From the domain's homepage select the **Groups** icon to display a list of groups within the domain. Either select an existing group, or use the **Create group** menu option and enter a name and description – this will then display the new group's details.

The group's detail page will display any existing encoders and users in the group.

*Use the **In this group** list box to toggle between showing encoders and users in the group.*

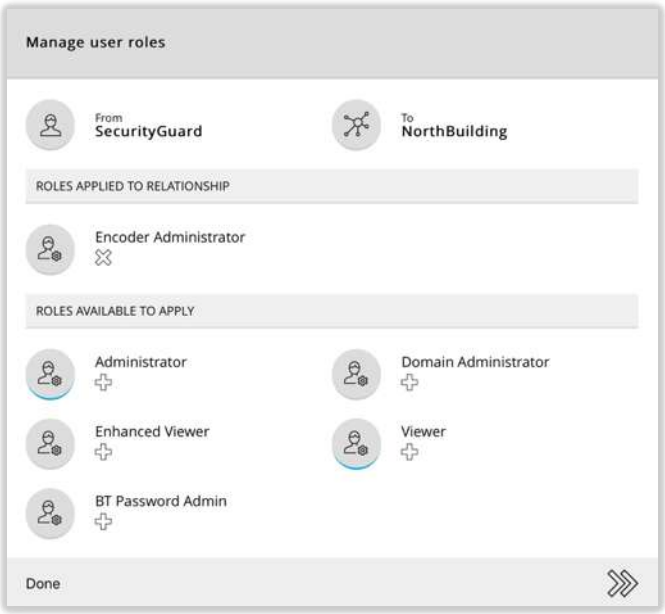
Step 3 – Use the **Add encoder to group** menu option to select the desired encoder accounts to add to the group.

Step 4 – Use the **Add user to group** menu option and select the first user.

This will then display the **Manage user roles** page which allows for the selection of the user's role. *To view the permissions a role will grant, click on the role's icon.*

The bottom section of the page lists all the roles available on the system, which can be assigned to the user by using the plus icon.

The middle section of the page lists the roles assigned to the user (this should be empty to start with). To remove a role, use the delete icon.



Note: Only permissions applicable to **Encoder usage** will be granted to the user, as the scope has been limited to a group. For example, granting the user the **Administrator** role will allow the user to administer the encoders within the group, but will not allow the user to administer the user accounts in the domain or provide any server-wide permissions.

It is possible to assign multiple roles to a user, which creates an additive effect granting the user all the permissions (applicable to encoders) contained within each role.

Repeat Step 4 to add each user to the group. The role granted will be applied to every encoder in the group.

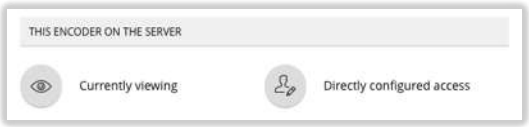
Assigning a user role to a specific encoder

When to use: There is a requirement to provide a user a level of encoder access to an individual encoder within a specific domain.

While it is possible to provide access to individual encoders it is the least flexible method of managing roles. Using groups to manage roles allows for easier ongoing management of users and encoders.

Step 1 - From the domain's homepage select the **Encoders** icon to display a list of encoders within the domain. Either select an existing encoder, or use the **Create encoder** menu option and enter a name and password – this will then display the new encoder's details.

The encoder's detail page will display a number of configuration icons within the **Encoder configuration** section, varying on encoder model and online/offline status.

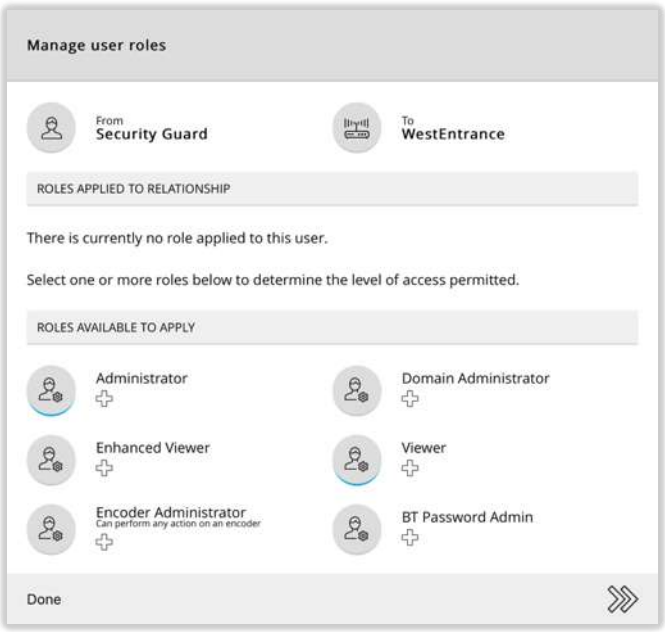


Step 2 – Use the **Directly configured access** icon to display the list of groups and users who have access to the encoder.

Step 3 – Use the **Add user to encoder** menu option to select the existing user to grant access.

The user must already exist – if not return to the domain home page and create a new user first.

Step 4 – Selecting a user will then display the **Manage user roles** page which allows for the selection of the user's role. *To view the permissions a role will grant, click on the role's icon.*



The bottom section of the page lists all the roles available on the system, which can be assigned to the user by using the plus icon.

The middle section of the page lists the roles assigned to the user (this should be empty to start with). To remove a role, use the delete icon.

Note: *Only permissions applicable to* ***Encoder usage*** *will be granted to the user, as the scope has been limited to an encoder. For example, granting the user the* ***Administrator*** *role will allow the user to administer the encoder, but will not allow the user to administer the user accounts in the domain or provide any server-wide permissions.*

It is possible to assign multiple roles to a user, which creates an additive effect granting the user all the permissions (applicable to encoders) contained within each role.

Domains

All encoders and users must exist within a domain. A domain is a segmented area within EdgeVis Server where all encoders and users are only visible to other users within the domain. This allows Server Administrators to keep different customers/user communities separate (and hidden) from each other - a user within the domain can't see a Server Administrator or a user in another domain. It is possible to create multiple domains on the server.

There are some rules around domains and users:

- A user with a Server-wide role will be able to see all domains (and encoders and users within). On logging in they will be taken to the server's home page, which lists all domains on the server. Selecting a domain will take the user to the domain homepage where they can view the groups, users and encoders within.
- A user who has a role within a domain will only be able to see the encoders and users within the domain. On logging in they will be taken directly to the domain's home page.

If segregation of users is not required it is possible to create only one domain, in which to keep all encoders and users.

Managing domains

A Server Administrator (with the appropriate permission) can create domains, edit the domain's description or delete an existing domain.

- **To create a domain**
  From the server home page click the **Domains** icon, then use the **Create domain** icon to create the domain. It is recommended to enter a meaningful description, as this will be displayed throughout the portal to help users disambiguate different domains.
- **To edit the domain's description**
  From the server home page click the **Domains** icon, then select the desired domain. This will display the domain's homepage. Click the **Edit domain** option to enter a new description for the domain.
- **To delete a domain**
  From the server home page click the **Domains** icon, then select the desired domain. This will display the domain's homepage. Click the **Delete domain** option to delete the domain.
  This will also delete all groups, encoder and user accounts contained within.

Export/import of domains

A Server Administrator (with the appropriate permission) can create a backup of the groups, encoders and users within a domain. This backup can either be re-imported to the same server, or imported onto a different server.

To export, on the domain's homepage click the **Export domain** icon. This will create a backup (stored locally on the server) that can be restored at a later date (or manually moved to another server and imported there). Backups are stored in the EdgeVis Server installation folder in the 'bin\backup' folder.

Note: *For security reasons a domain export only saves the encoder, group and user accounts and* ***not*** *the roles and permissions used within the domain. Only performing a full server backup will save all roles and permissions.*

To import a previously saved domain, enter the **Domains** page from the server home page and then select the **Import domain** icon. This will list all previously exported domains on the server.

Note: It is only possible to import a domain if there are no items on the server with the same name.

Moving encoder and user accounts between domains

Any encoder or user account (within a domain) can be moved to a different domain by a Server Administrator with the appropriate role (e.g. Administrator).

From within the existing domain open the details page for the desired encoder or user account. Select the **Move domain** menu option on the right. This will display a list of domains that the account can be moved to.

Moving an account will delete all existing group memberships, alarm rules, and assigned roles/user access.

Promoting a domain user to a Server-wide Administrator

It is possible to promote an existing domain-level user to a server-wide administrator using the **Move Domain** feature described above. When selecting **Move Domain** the list of available domains includes an **Administrators** item – select this option to move the selected user from the current domain to the **Server-wide Administrators**.

Sharing encoders and users across domains

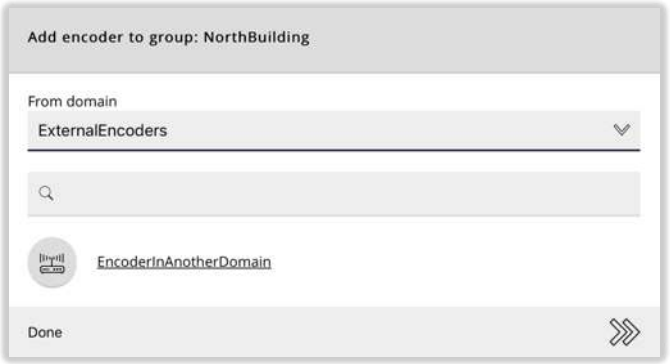
While an encoder or user can only be a member of one domain it is possible to allow users in other domains to share access to selected encoders within a different domain, or allow users from another domain to access encoders. A user with server-wide access and full user-account permissions (create, edit and delete) is required to perform this action.

To grant access to an encoder from another domain:

Step 1 – Sharing an encoder requires a group to be created in the target domain. Either create a new group or select an existing group as the destination of the encoder(s).

Step 2 – Use the **Add encoder to group** menu option. This will display all encoders within the target domain.

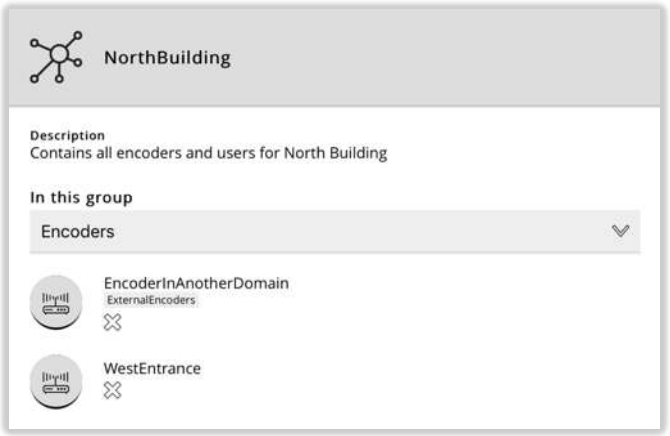
Step 3 – Use the **From domain** list box to select the domain containing the desired encoder. The page will now list the encoders available in the target domain.



Step 4 – Select the desired encoder. This will then be added to the group and should be listed in the encoder list.

To signify that the encoder is from another domain the encoder will show a sub-heading with the name of the original domain.

Note: *Users in the group will be granted the same level of access to the imported encoder that they have to non-imported encoders. This may expose other information about the encoder or the name of other users in the original domain (e.g. users who are assigned to receive notifications for an alarm rule).*



To grant access to a user from another domain:

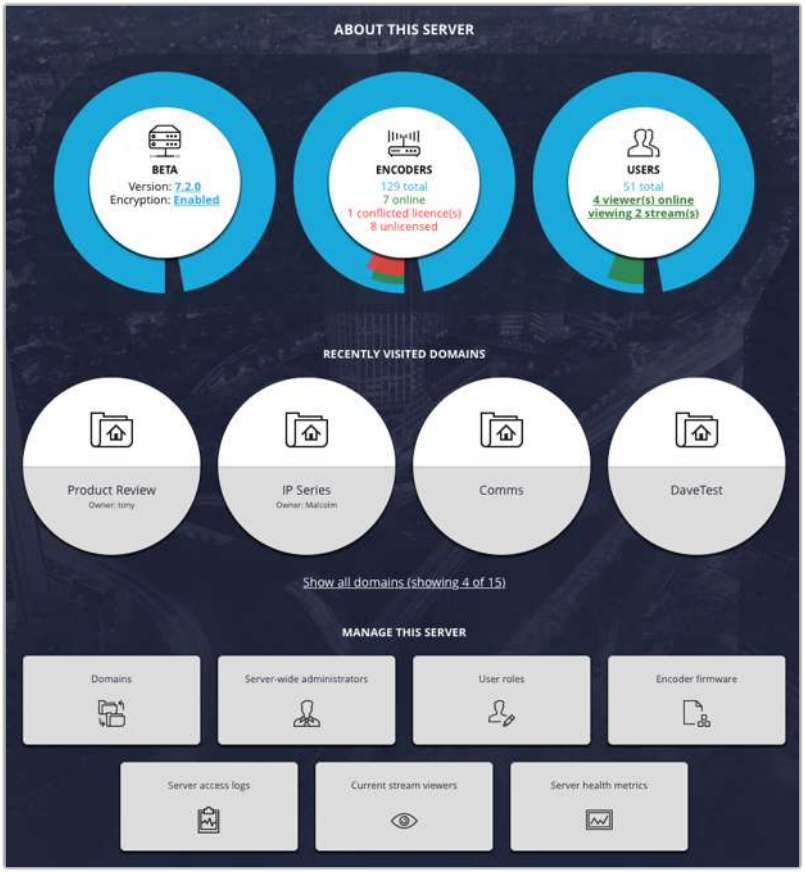
Repeat the above steps, but using the **Add user to group** menu option in Step 2.

SERVER-WIDE ADMINISTRATORS

This section of the manual explains the setup and configuration functions that can be performed by an administrator who has server-wide access.

Server Homepage

The default **Administrator** account is provided with full Server Administrator permissions. Users who have Server-wide access will be taken to the server homepage when they first log in.



The homepage is split into three sections:

- **Summary information –** including the server version number, total number of accounts created (and in use) and a link to the TVI encryption details
- **Domains in this server –** either use the domain search function to find a domain, quick access to the first four domains, or use the **Show all domains** function to list all domains on the server
- **Manage this server –** manage the domains, server-wide users, user roles and firmware uploaded to the server, as well as performing system management functions including licence management, and server settings

Managing server-wide administrators

Select the **Server-wide administrators** icon on the server homepage to display a list of all users who have system-wide access.

Users within this section can have different levels of permission, which will depend on the role they have been assigned. The role they have been given will provide server-wide access to potentially all domains, encoders, and users on the server – care should be taken to only create users in this section who require access to the entire sever.

Users within this section can be recipients of alarm notifications. However, domain users are unable to view them as normal domain users do not have visibility of system-wide users.

For more information on creating a server-wide user or changing an existing user's role refer to **Assigning a server-wide role to a user** (page 19).

Monitoring active viewers

The summary bar on the server homepage displays the number of users viewing video streams, and the number of streams they are viewing. Click on the link to open the **Viewers** page which lists every viewer on the system - displaying the encoder being viewed, how long they have been viewing, and signifying if they are using any services (including PTZ and full-resolution retrieval).

If a user has accidentally left a video stream open in a viewing client it is possible to kick the user's stream by clicking on their user name and using the **Kick selected viewer** menu option.

Additionally, many services (e.g. PTZ) can only be used by one user. If a viewer has any of these services in use then additional menus options will be presented to allow those services to be freed.

Messaging configuration

EdgeVis Server can communicate with users using various mechanisms:

- iOS and Android push notifications (for users of EdgeVis Client) - for alarm notifications
- SMS - for alarm notifications
- Email - for alarm notifications and account management e-mails

Each of these services rely on third-party software/services and must be enabled with the appropriate settings.

*For further details on enabling each service refer to the later chapter **Messaging Configuration**.*

Automated account creation emails

EdgeVis Server supports two different modes of account creation:

E-mail new user(s) their account automatically

- Administrator enters each user's account name, e-mail address, and role
- EdgeVis Server sends an e-mail to each user automatically
- User receives a link that allows them to create their own password

Offline

- Admins create a user's account and password, and then manually distributes the login details

In most circumstances it is more convenient to have users receive their login details via e-mail and improve security by ensuring passwords are only known by their respective users. Additionally, users can reset their own passwords using an automated e-mail system directly from the server login page. E-mails sent can be customised using individual templates.

However, it is recognised that not all installations have access to an e-mail server and so it is possible to create accounts in an offline manner. This is the default mode and requires no further configuration.

Enabling the e-mail account system

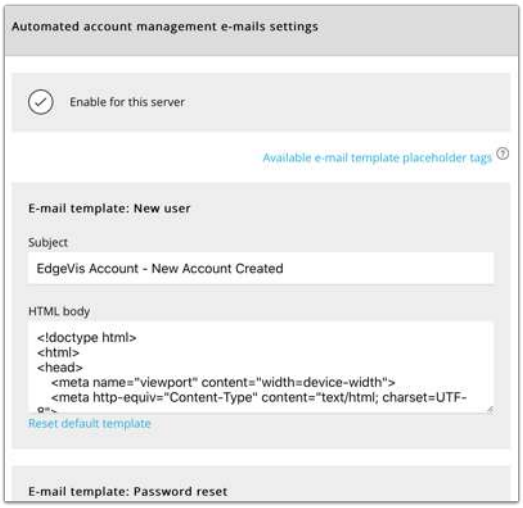
A pre-requisite is to ensure that e-mail is configured and working on your EdgeVis Server. The chapter **Messaging Configuration** outlines the how to enable e-mail and provides examples for various common e-mail systems.

To enable e-mail accounts, go to the server's **User Settings** page (under Server home page -> **Advanced settings**). From the available options select **Automated account management e-mails**. This will display the current setting.

To enable e-mail accounts use the **Edit settings** menu button on the right.

After ticking the enable button, it is also possible to customise the e-mails sent by EdgeVis. There are three e-mails the server can send:

- **New user** – sent when a new account is created
- **Password reset** – sent when the user asks to reset their password
- **E-mail changed** – sent to the old e-mail address when the user changes their e-mail address.



EdgeVis does not include an HTML editor and it is recommended to copy and paste the current template into your HTML editor of choice for editing, before pasting back into the server.

There are a number of live substitutions that the server can make when sending the e-mail – click the **Available e-mail template placeholder tags** help link that outlines the tags that can be used in each type of e-mail.

Testing the e-mail system

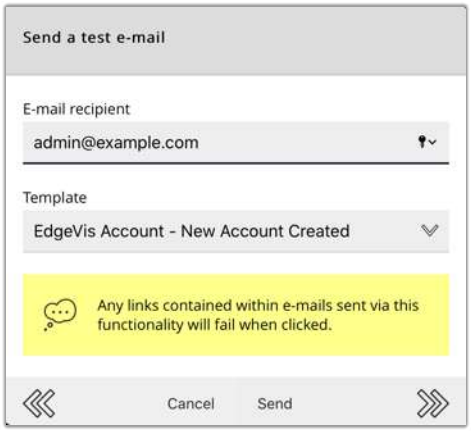
Once enabled, and you have modified the templates as necessary, a new option appears on the **Available e-mail template placeholder tags** page to help test the system without sending out real e-mails to users.

Select the **Send test e-mail** menu button to send test e-mails to a specific e-mail address.

After entering the e-mail address select the desired template to send.

If you have edited the built-in templates it is highly recommended to send test e-mails to various e-mail systems (e.g. Gmail, Outlook, iOS Mail) as:

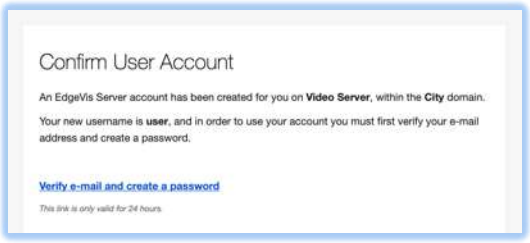
- HTML rendering of e-mail is not as consistent as Web browsers
- EdgeVis Server will auto-create a plain-text version of the HTML template for users who are using older templates or have disabled HTML rendering for security/privacy reasons.



Security of links within e-mails

New user and *Change password* e-mails contain links that allow the user to set new passwords on the server. In order to better protect user accounts there are a number of protections the server employs with these e-mail links:

- Each link can only be used once
- The link is only valid for 24 hours for a new user, or 3 hours for a password reset



Should a user try to use the link a second time they will be directed to complete a password reset request. This would ensure only the original recipient received subsequent links. For expired links the system will automatically send the user another e-mail with a fresh link.

Disabling automated e-mail accounts

It is possible to disable the e-mail account feature at any point – however it is not recommended to subsequently toggle this setting on a production server as all existing automated e-mails will cease to work when the e-mail accounts are disabled.

Login and password policies

It is possible to configure encoder and user accounts to follow organisational policies regarding account usage and password rules and complexity. These settings can be set at both server and domain level. By default, the server settings:

- Propagate down to all domains
- Can be locked so that no domain administrator can change them
- If not locked, can be overridden by a domain administrator

Password settings

By default, EdgeVis Server will allow any password to be set that is 5 characters or more and will not expire it or prevent its reuse. It is possible to set stricter rules to enforce a stronger password policy.

These settings can be configured independently for users and encoders and are available from the **Password settings** section of **User settings** and **Encoder settings** respectively. Options include:

- **Reuse period –** stop users from reusing previously used passwords
- **Expiry period for domain users –** force password changes on domain-level users after a defined number of days. *System-wide user account passwords never expire*
- **Minimum length** – force users to set longer passwords.
- **Check for common words** – ensure users don't use dictionary words (or variations such as 'P@sswOrd')

It is also possible to force users to use numbers, uppercase characters and symbols.

Note: Any new settings will only take effect on subsequent password changes. Existing passwords will remain unchanged.

Viewing client settings

It is possible to set additional options that control the client's behaviour:

- **Viewer timeout –** viewing clients can auto-disconnect from a video stream after the specified period
- **Account lock out –** auto-lock user accounts if too many failed login attempts are made
- **Enable single sign-on mode –** by default a username can be used by multiple viewing clients simultaneously. Enable this option to only allow each username to be used by one viewing client (who may view multiple streams).
- **Allow users to save password within client –** this will determine whether the viewing client will allow the user to save their login credentials.

Global settings

There are a number of settings that are applied globally on the server within the **User settings** section that can't be set on a per-domain basis. These are contained within the **Account Settings** section:

- **Account inactivity limit –** expire old accounts after a period of inactivity
- **Minimum length of names –** by default any username must be a minimum of 2 characters long

Two factor authentication (2FA)

EdgeVis can protect user accounts using two factor authentication (2FA). This uses the industry standard 6-digit code scheme used by many other systems, and is recommended for maximum security. 2FA is not applicable to encoder accounts.

Recommended 2FA Apps

As part of enrolling for 2FA, users will need to scan a QR code into a suitable 2FA app that can then generate the 6-digit login tokens.

There is no EdgeVis 2FA app supplied by Digital Barriers, and it is recommended to use one of the many third-party 2FA apps available. Two common free applications are Google Authenticator and Authy – both can be found on iOS and Android app stores.

Note: Google Chrome has an Authenticator extension in its app store. This app is not a Google app and is not connected to Google Authenticator, and does not synchronise its registered 2FA services with Google Authenticator.

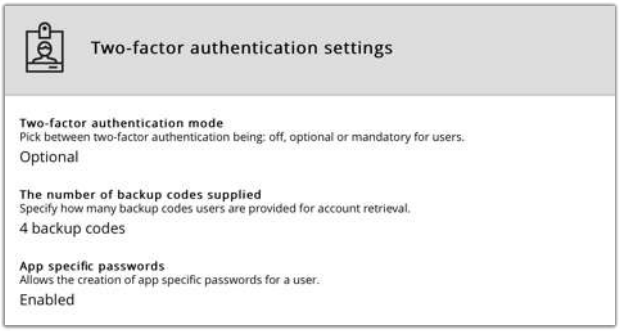
Enabling 2FA for users

The following settings are available from the **Two-factor authentication settings** section of **User settings** at both server and domain level.

The first setting (**Two factor authentication mode)** has three options:

- Off
- Optional **(default)**
- Mandatory

By default, EdgeVis allows users to enrol in 2FA if they desire. However, many corporate policies mandate the compulsory use of 2FA – set the 2FA mode to **mandatory** to force all users to enrol.



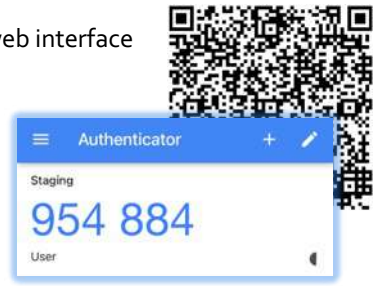
The second setting allows admins to decide how many 2FA backup codes the user is presented with during the enrolment process (or even disable them all together). These codes are one-time emergency codes the user can use should they lose their 2FA device/app.

Finally, admins can decide whether to allow users to create app-specific passwords. These can be used with third party applications (e.g. Milestone VMS) that support EdgeVis, but do not support 2FA.

User enrolment in 2FA

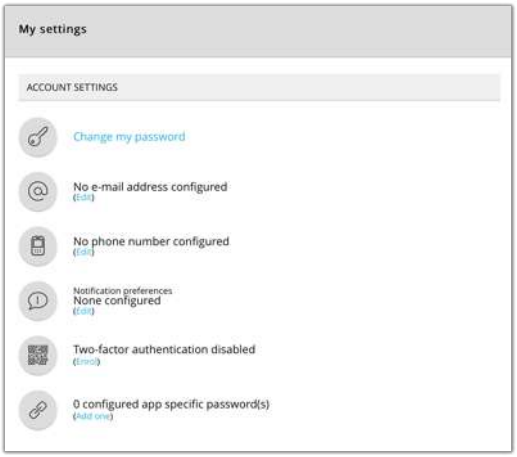
When 2FA mode is set to mandatory:

- EdgeVis Client users will be automatically directed to the EdgeVis Server web interface where enrolment must be completed.
- EdgeVis Server users will be prompted to complete enrolment after entering their username and password.
- The user is presented with a QR code – they scan this into their Authenticator app.
- The app then presents a 6-digit code – this must be entered below the QR code in EdgeVis Server to complete setup.



When 2FA is optional:

- A user must log into EdgeVis Server to enable 2FA
- After logging in users can enrol in 2FA from the **My Settings** page.
- The **Enrol** button will present the user with a QR code – they scan this into their Authenticator app.
- The app then presents a 6-digit code – this must be entered below the QR code in EdgeVis Server to complete setup.



Once enabled the user will be requested to enter a 2FA code every time they log in to EdgeVis Server. EdgeVis Client users will see one of two behaviours:

- If the user is allowed to save their password (and chooses to do so), EdgeVis Client will only request the 2FA code when adding the server to their list of available servers.
- If the user is not allowed to save their password, or chooses not to, then they must enter their password and 2FA code every time they attempt to connect to the server.

Resetting a user's 2FA registered app/device

There are occasions when a user may no longer have access to the app or device that generates the 6-digit codes. In this circumstance it is advisable to reset a user's 2FA registered device, so that they can re-enrol.

If the user has access to a backup code (that they recorded/downloaded during the original enrolment) then they can log into EdgeVis Server and reset their 2FA settings themselves. The **My Settings** page will have a **Reset** option in the Two-factor authentication section.

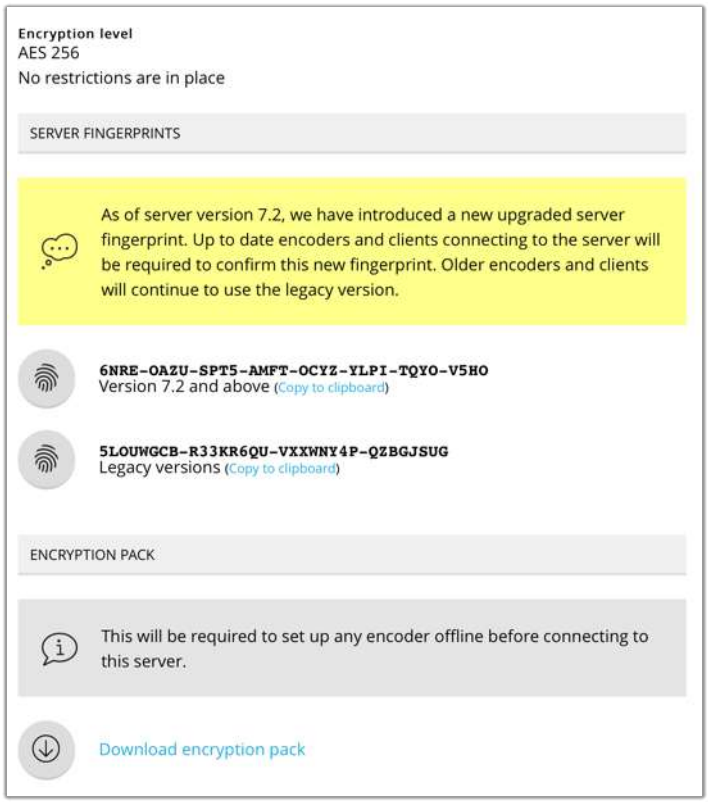
If the user does not have any backup codes available then they must contact an administrator who has the necessary permissions to edit their account. Again, the Administrator should use the **Reset** option in the Two-factor authentication section.

TVI Encryption

EdgeVis Server can employ AES-256 encryption to the TVI links between the server and all encoders/viewers, securing all transmissions from interception. Encryption keys are generated on the fly and are regularly rotated for maximum security.

The first detail on the **TVI Encryption** page will display the encryption strength (if enabled).

To ensure encoders/viewers are connecting to the intended server (and not a hostile man-in-the-middle) the server, during installation, creates a unique public/private key pair to verify the identity of the server. The private key is stored on the server and never distributed to users.



The public key can be distributed to users as:

- a **server fingerprint** that contains a shorter (40 character) human readable version of the public key. Users setting up an encoder using the web setup interface, or connecting to a sever using a viewing client will be asked to visually confirm the fingerprint of the server during the initial connection to the server.
  *Use the **Copy to clipboard** function to copy the server's fingerprint to the clipboard for distribution to users.*
- an **encryption pack**, which is a file that contains the server's public key. Older encoders (without interactive web configuration interfaces) must use the encryption pack during USB configuration.
  *Use the **Download encryption pack** menu option to download the encryption pack.*

Note: It is safe to distribute this information to users as it is not used during the encryption process – it is only used to verify the identity of the server. If this information is lost/stolen, there is no security risk or requirement to reset the server's encryption fingerprint/pack.

SSL configuration

The EdgeVis Server web management portal uses a self-signed SSL certificate by default. This allows the server to encrypt the web traffic but will fail browser security checks which require web sites to have a publicly verifiable SSL certificate installed on the server.

While this does not prevent the web portal's traffic being encrypted, it can be disconcerting to end-users and can open the server to man-in-the-middle attacks.

EdgeVis Server supports:

- Manual creation and upload of a valid SSL certificate (verified by a third-party certificate authority)
- Auto-generation of an SSL certificate using the free Let's Encrypt service

Using either of these schemes will remove the security warning and provide users with the standard 'green padlock' they expect to see on a secure website.

For further details on using a custom SSL certificate refer to the later chapter ***Using an SSL certificate with the web management portal****.*

Sending automated maintenance alerts

It is possible to configure EdgeVis Server to send alerts when a server or encoder detects an unusual event (e.g. an encoder's camera has gone offline). These alerts can be sent using the same mechanisms as the alarm management system:

- As an e-mail to an external e-mail address
- As an SMS message to a phone number
- To an EdgeVis user (and respecting their message settings - push notification/e-mail/SMS)

There are two classes of maintenance alerts:

- **Server alerts**
  Multi-server health monitoring
  Database backup progress
  Firmware uploads
  Licensing issues
- **Encoder alerts**
  Encoder disconnects
  Recording disk issues
  Environmental issues (temperature/voltage)

It is possible to create a rule to send alerts at both the server level and the domain level (if the user has the appropriate permission).

Maintenance alarm rules		
Level	**Rules location**	**Alerts Available**
Server level	Server home page -> Advanced server settings -> Maintenance alerts configurations	• Server alerts • Encoder alerts for all encoders on server
Domain level	Domain home page -> Maintenance alerts configurations	• Encoder alerts for all encoders within that domain

Editing maintenance alerts

At the server level, and individual domain level there is a list of current active rules for sending alerts *(at the locations specified in the previous table)*.

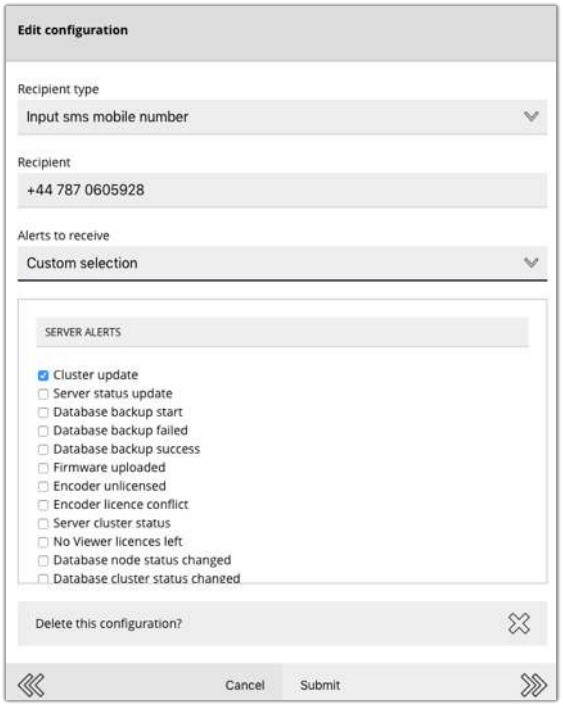
The icon for each rule will signify if it's an e-mail, SMS, or EdgeVis recipient. To edit an existing rule, select it from the list. Select the **Add new maintenance alert rule** menu item to create a new rule.

- Select the desired recipient type – either e-mail, SMS or EdgeVis user.
- Selecting an EdgeVis user will allow selection from any user within the server-wide administrators group (and domain-users if creating the rule in a domain).
- EdgeVis users will be sent alerts based on their notification preferences (e-mail, SMS or push notification) and control the delivery mechanism themselves.

There are a number of choices for the types of alerts to send:

- All maintenance alerts (both server and encoder)
- Custom selection
- All server alerts
- All encoder alerts

Selecting **Custom selection** allows the user to see a list of all notifications available, in both the Server and Encoder groupings.

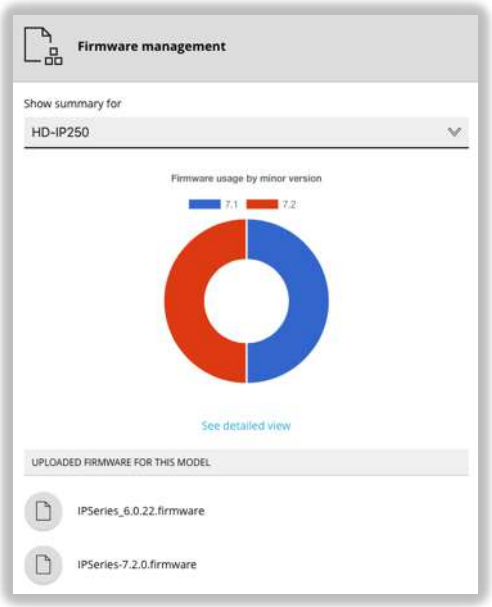


Once a server grows beyond a small number of encoders/users it is not recommended to utilise the **All XXX alerts** options as this can generate a **significant** number of alerts.

Note: If using a third-party SMS/e-mail provider please monitor alert generation to ensure that the costs of using this service are understood. On a larger server it is possible for hundreds of alerts to be generated per day.

Firmware Management

EdgeVis Server allows the firmware on encoders to be remotely upgraded. It is possible for server-wide administrators to upload encoder firmware to EdgeVis Server, where users with the appropriate permissions may then select from any of the uploaded firmware to upgrade (or downgrade) their encoder to a newer (or older) version.



From the server home page select the **Encoder firmware** button – this will then list all firmware that have been uploaded to the server, along with a breakdown of the firmware version of encoders on the server (both online and offline).

As an EdgeVis deployment could consist of different encoder families (each with their own dedicated firmware) it is possible to narrow down the list of firmware to a particular product. Select the desired product from the **Show summary for** list box to narrow down the list of firmware, and installation statistics, to a particular model.

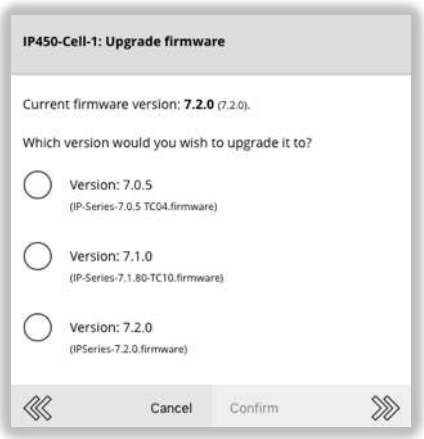
Note that a firmware may be listed under multiple products, e.g. the same firmware can be used to upgrade an HD-IP150 and an HD-IP250. Click on a firmware to list the products a firmware may be used with.

- To add a new firmware to the list, select the **Upload firmware** menu option on the right, and select a firmware on the local PC to upload to the server.
- To delete an existing firmware, click on the firmware from the list and select the **Delete firmware** menu option.

Upgrading an encoder's firmware

Any user whose role includes the '**Upload a firmware to the encoder'** permission has the ability to upgrade (or downgrade) an encoder's firmware. To view an encoder's current firmware, and/or upgrade the firmware:

- Select the encoder by clicking the encoder's account icon within the appropriate domain.
- The **Status and diagnostics** section will list the encoder's current firmware – select this item to view further information.
- Use the **Upgrade firmware** menu item on the right to view available firmware – selecting one will begin the transfer of the firmware to the encoder.
- The firmware is sent to the encoder using the same secure channel as the video and is trickle-fed to ensure that the video stream continues uninterrupted during the transfer.
- Once the transfer is complete the encoder will reboot and apply the new firmware – this should only take around 1-2 minutes.



Warning: downgrading encoder firmware

EdgeVis generally has no restrictions on downgrading an encoder's firmware. However, downgrading is generally not recommended for deployed encoders as there may be unintended consequences - feature changes in later firmware may temporarily break (or remove) certain encoder functionality if downgraded.

Examples include newer changes in recording formats that earlier firmware do not understand or upgraded transmission encryptions that are required to connect to a server.

Should issues be encountered after a downgrade it is possible to reset the encoder to a 'factory fresh' condition by:

- Factory-resetting the encoder
- Reformatting the encoder's recording disk (if appropriate)

This should wipe any incompatible settings/recordings, allowing the encoder to operate correctly again.

Digital Barriers does not test encoder firmware downgrading and accepts no responsibility should the user encounter any issues or require the encoder to be returned for repair.

Note: It is **never** recommended to downgrade a firmware below the version supplied with the encoder – modem drivers may be required that are not present on earlier firmware.

Bulk firmware update

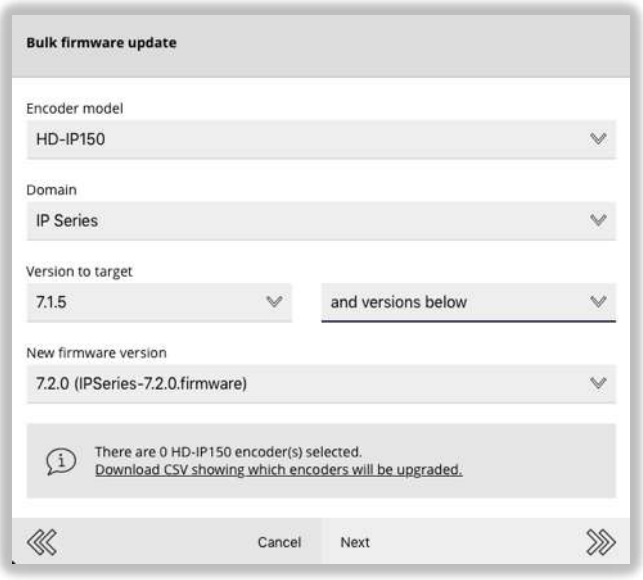
For users with many encoders to upgrade it is possible to batch upgrade encoders with older firmware. From the **Firmware management** page select the **Bulk update encoders** menu option. This will present a selection tool that allows the user to:

- Select which encoder model to upgrade.
- Either select all encoders or to narrow down the list to a specific domain.
- Select encoders with either a specific firmware, or firmware older/newer than a specific version.

The info message at the bottom of the page will show how many encoders meet these criteria (the next page allows a fine-grained choice of including/excluding an encoder.

- Finally select which firmware to upgrade all selected encoders with.

Once the user has confirmed which encoders to upgrade, EdgeVis Server will begin firmware upgrades on each encoder. This uses the same process as manually upgrading the encoder described above.



Backing up and restoring EdgeVis Server

It is possible to save the EdgeVis Server databases (which include all domains/roles/accounts/alarm rules) to a single file on the server PC. This can be used to keep a backup copy of the server or to easily transfer the EdgeVis Server to a different server machine.

To start the process, select the **Server backup/restore** icon on the server homepage, and then use the **Create database backup** menu option. A prompt dialog will request a file name to be entered. The database will now be backed up and stored in a folder called 'backup' in the EdgeVis Server application directory (typically c:\Program Files (x86)\EdgeVis Server\). This file can be stored securely or copied to the same folder on the new EdgeVis Server machine.

To restore a database, select the **Server backup/restore** icon on the server homepage – this will list all backups stored on the server. Select the desired backup and use the **Restore database backup** menu option to begin the restore. Once the restore has begun, the interface will log the user out. There is no indication when the restore is complete – please allow approximately 60 seconds before attempting to log back in.

Note: Restoring the database will delete all existing domains/roles/accounts/alarm rules, before restoring from the backup. This may also delete the account being used by the person restoring the database.

It is recommended to perform a database backup before performing a restore.

DOMAIN-WIDE USERS

This section of the manual explains how to make the best use of domains, including encoder and user accounts and the use of groups to manage granting of permissions between them.

Groups

EdgeVis Server can utilise **groups** for improved and simplified roles and permissions management. A group can hold any number of encoders and users, where adding a user allows them to be assigned a role within the group which grants them that level of access to all encoders within the group.

For example, if there is a building with five encoders (providing video surveillance) and a number of security guards who must be provided access to those encoders there are two ways to provide the security guards access:

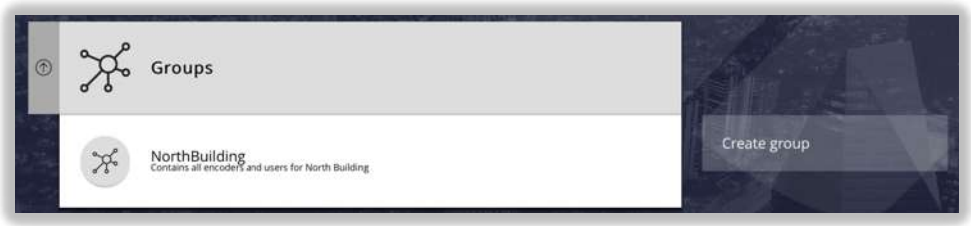
Without groups, it is necessary to assign each security guard the appropriate viewing permissions to each encoder individually. When a new guard is hired, they too must be given five permissions (one to each encoder), and if a new encoder is added to the building it is necessary to find each security guard's account and individually grant them permission to view the new encoder.

With groups, it becomes considerably simpler to manage, as a group is created to hold all the encoders **and** all the security guards. When adding a new security guard to the group they are granted one viewing permission, *to the group*, meaning they have access to all encoders within the group. When a new encoder is added to the group, all security guards are immediately granted the same level of access.

An encoder and user can be added to multiple groups – in the example above a security guard may have permission to access encoders across multiple buildings by being a member of multiple groups.

Managing groups

From the domain homepage click the **Groups** icon to open the groups page, which lists all groups in the domain and provides the ability to create a new group using the **Create group** menu option. When creating a group, it is possible to enter a description which will be displayed as a subheading underneath the group's name. To open the details page for the desired group, select the appropriate item from the list.

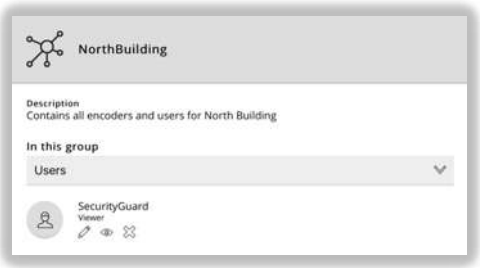


It is also possible to search for the group from the domain homepage, by entering part of the group's name within the search box. The page will then find all assets (groups, encoders and users) within the domain that match the search string. Select the desired group from the search results to go directly to the detail page for the group.

Group details page

The group details page displays the group description (if set) and the list of all users that have been added to the group.

To view the encoders added to the group use the **In this group** list box to switch between displaying the encoders and users in the group.



Managing users in a group

- **To add a user to the group:**
  Use the **Add user to group** menu option to select the user to add to the group. After selecting the user, the second step is to assign a role to the user to grant the appropriate permissions to the encoders in the group. This process is described in more detail in 'Assigning a user role to a specific group' (see page 21 for further details).
- **To view a user's role(s) and permissions:**
  The user's role(s) is displayed below the username. To view the flattened permissions this grants within the group click the eye icon. This will show a permissions browser which outlines the permissions within the role.
- **To change a user's role(s):**
  Use the pencil icon to modify the user's role(s).

Tip: Removing all roles from the user will allow the user to remain in the group, but will not provide the user any access to the encoders in the group. This can be useful to create a notification-only group, where membership of the group is only used to determine who receives alarm notifications from the alarm management system.

- **To delete a user from the group:**
  Use the cross icon to delete the user from the group.

Managing encoders in a group

- **To add an encoder to the group:**
  Use the **Add encoder to group** menu option to select the encoder to add to the group. Adding an encoder to the group will immediately grant all users access to the encoder with the same permissions their roles provide (to all other encoders within the group).
- **To delete an encoder from the group:**
  Use the cross icon to delete the encoder from the group.

User Accounts

EdgeVis Server employs strict security rules, ensuring that before any user can connect to the server they have the appropriate login credentials to the server - there is no concept of guest or anonymous usage within EdgeVis. Once created a user account can then be granted a level of access (e.g. a specific domain) and permissions to access resources within that level (e.g. Encoder Administrator).

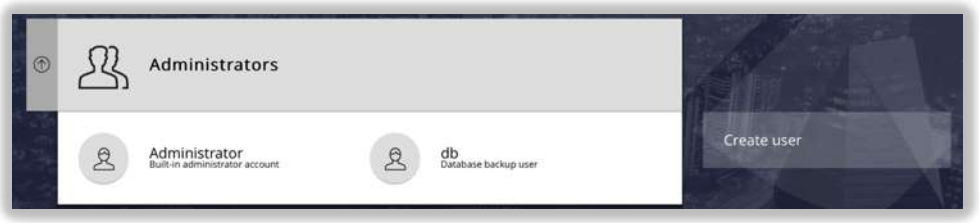
There are two kinds of users:

- **Server-wide Administrators**
  These users have server-wide access, and if given the appropriate role, can perform:
  - Server administration and configuration
  - Domain management
  - Group, Encoder and User Account Management
  - Encoder configuration
- **Domain Users**
  These users have specific access within a domain, and if given the appropriate role, can perform:
  - Group, Encoder and User Account Management
  - Encoder configuration

Given the server-wide access granted, in normal operation it would be expected to create a limited number of Server Administrators. Normal users should be created within a domain, and only granted access to the required encoders or account management permissions.

Managing Server-wide Administrators

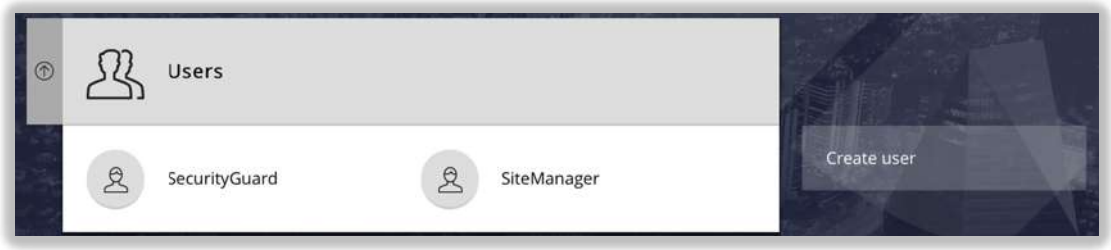
From the server homepage click the **Server-wide Administrators** icon to open the users page, which lists users with server-wide access and provides the ability to create new Server Administrators using the **Create single user** menu option. When creating a user, it is possible to enter a description which will be displayed as a subheading underneath the user's name. To open the details page for the desired user, select the appropriate item from the list.



Tip: Version 7.2 introduces the ability to quickly create multiple user accounts using the **Create multiple users** function. It is possible to either specify a single password to use with all supplied usernames, or to individually specify a unique password for every user. Each user can also be created with a chosen role – if selected each user is assigned the same role on a server/domain-wide basis.

Managing domain users

From the domain homepage click the **Users** icon to open the users page, which lists all users in the domain and provides the ability to create a new user using the **Create user** menu option. When creating a user account, it is possible to enter a description which will be displayed as a subheading underneath the user's name. To open the details page for the desired user, select the appropriate item from the list.

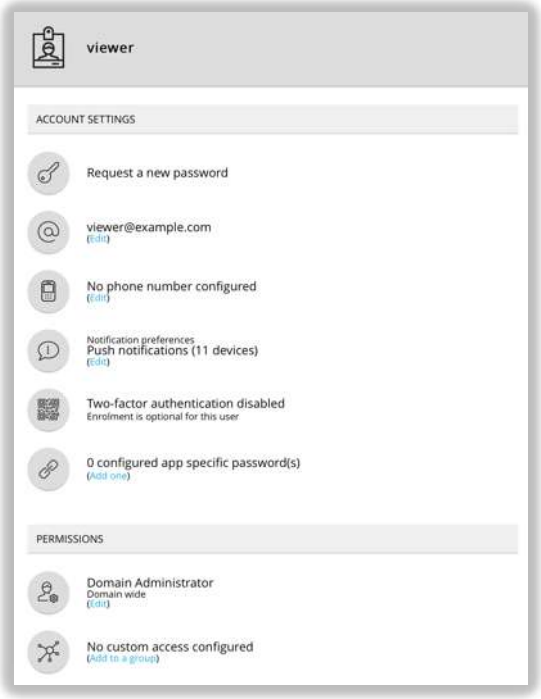


It is also possible to search for a user from the domain homepage, by entering part of the user's name within the search box. The page will then find all assets (groups, encoders and users) within the domain that match the search string. Select the desired user from the search results to go directly to the detail page for the user.

User details page

The user details page displays the user's description (if set), and then the user's account settings

- password options (including set a password, reset password, resend welcome e-mail)
- the contact details for the user (e-mails and phone number)
- push notification settings (send via email/sms and/or push notification)
- two-factor authentication (enrol or reset depending on server options)
- app specific password (for creating special passwords to use on third-party systems that don't support 2FA)



For Server Administrators the **Permissions** section displays a list of roles granted to the user on a server-wide basis, while for a domain user it displays:

- a list of roles granted to the user on specific groups
- a list of roles granted on a domain-wide basis

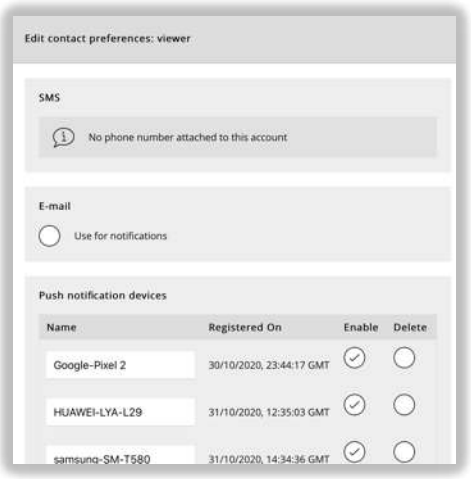
The **Edit account** menu option should be used to change the user's password and description, while the **Edit options** menu option allows editing of an account's login options – these can include:

- disabling the account
- forcing the user to change password on next login

A **Move Domain** option is present that allows a user with the appropriate permission (requires server-wide access) to move the user into another domain. Be aware that moving a user will remove their existing roles and permissions.

Setting contact preferences

The contact preferences are used by the server when the user is the recipient of a notification from the alarm management system. The server will send a notification to **each** enabled contact method:



- **SMS**
  For users who enter a phone number in their account, they can enable SMS notifications to that number.
- **Email**
  For users who have added an e-mail address to their account, they can enable e-amil notifications to that address.
- **Push notifications**
  A user with an iOS or Android device who connects to the server using EdgeVis Client will automatically be registered for push notifications on that device. This page will list all devices that have previously been registered to receive notifications for that user – the device will continue to receive notifications for as long as the app is installed.
  This page allows you to either disable or delete devices – this will immediately stop those devices from receiving notifications via push.

Managing a user's roles and permissions

The bottom section of the user details page lists:

Server-wide Administrator accounts only

The **Server Wide Access** section displays the roles the user has been granted on a server-wide basis.

- See 'Assigning a server-wide role to a user' (page 19) for details on how to assign/change the user's role.

Domain users accounts only

The **Group and Encoder Access** section displays the roles granted on a group basis (signified by the group icon), and on an individual encoder basis (signified by the encoder icon).

- See 'Assigning a user role to a specific group' (page 21) for details on how to assign/change group roles.
- See 'Assigning a user role to a specific encoder' (page 22) for details on how to provide access to encoders.

It is also possible to add a user directly to a group from the user detail page using the **Add to group** menu option.

The **Domain Wide Access** section lists the roles the user has been granted on a domain-wide basis

- See 'Assigning a user role to a specific domain' (page 20) for details on how to assign/change the user's role.

It is security best-practice to only provide the minimum level of access required to any user. It is recommended to only provide domain wide access to users who are required to manage the accounts within a domain, and to use groups to provide access to users who use and manage encoders.

Encoder Accounts/Configuration

EdgeVis Server employs strict security rules, ensuring that before encoders can connect to the server it has appropriate login credentials to the server.

All encoder accounts must exist within a domain – an encoder account can not be created at the server level.

Managing encoder accounts

From the domain homepage click the **Encoders** icon to open the encoders page, which lists all encoders in the domain and provides the ability to create a new encoder account using the **Create one encoder** menu option. When creating an encoder account, it is possible to enter a description which will be displayed as a subheading underneath the encoder's name.

The encoder list uses colour and a status string to indicate the encoder's live status:

- The encoder is online, licensed and ready to use
- The encoder is sleeping – click icon to view the wake-up time or to cancel sleep
- The encoder requires attention before it will be ready for use, e.g. assigned the wrong licence type
- The encoder is offline, and the account may require attention, e.g. assigning a licence
- The encoder is offline, but has a valid licence

To open the details page for the desired group, select the appropriate item from the list.

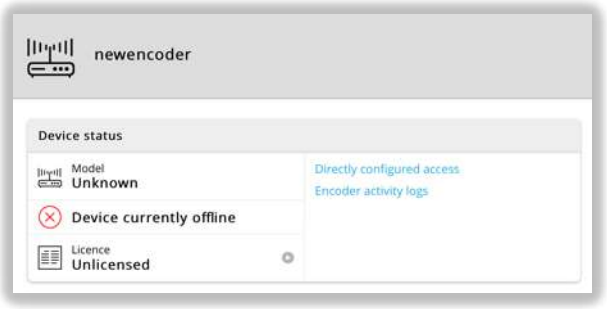
It is also possible to search for an encoder from the domain homepage, by entering part of the encoder's name within the search box. The page will then find all assets (groups, encoders and users) within the domain that match the search string. Select the desired encoder from the search results to go directly to the detail page for the encoder.

Tip: It is possible to quickly create multiple encoder accounts using the **Create multiple encoders** function. Either specify a single password to use with all supplied encoder names, or individually specify a unique password for every account.

New encoder account details page

Once created, the encoder's detail page will show that the encoder is offline and is unlicensed.

In addition to requiring an account to connect to the server, an encoder also requires a licence be installed on the server.



While some encoders can automatically obtain a licence from the server on first connection, certain licence types must be manually assigned (either using this page, or from the encoder's web configuration). This is because they are licensed per-camera input, and several licence levels are available (offering different levels of functionality).

Click on the **Licence** icon to open the encoder's licensing page and use the **Edit Licence** menu option to select the appropriate licence (and if appropriate, the number of camera channels to enable on the device.

If a licence is set using this web page, then the encoder's web configuration interface can not override the licence choice.

What EdgeVis licence does each product require?

- **EdgeVis Specialist Licence (one per encoder)**
  Existing TVI Products C200, C300, C310, U310, S400, I200, I300, R300, M350, R400
  S Series HD-S600
  R Series SD-R500 (formerly Tri-Star), HD-R700, 4K-R800
- **EdgeVis Mobile Licence (one per encoder)**
  Mobile Encoder for iOS and Android
- **EdgeVis Lite, Enhanced or Enterprise Licence (one per camera channel)**
  IP Series IP100, IP150, HD-IP200, HD-IP250, HD-IP350, HD-IP450, HD-IP470
  Q Series SD-Q600 (formerly MiniCam), HD-Q800
  Video Router Video Router 1, Video Router 4

Use the encoder account details to configure the encoder

Once the encoder account has been created and, if necessary, a licence assigned the encoder should be configured using the details of the server. Refer to the encoder's hardware installation guide for details on how to configure the encoder, however you should have the following information to proceed:

- The server's external IP address
- The server's encryption fingerprint (available from the server homepage) for web-based configuration
- The server's encryption pack (available from the server homepage) for USB-based configuration
- The encoder name
- The encoder password

Once configured the encoder should attempt to connect to the server, logging in using the account details provided. If successful, the encoder will appear with a green status icon in the encoder list.

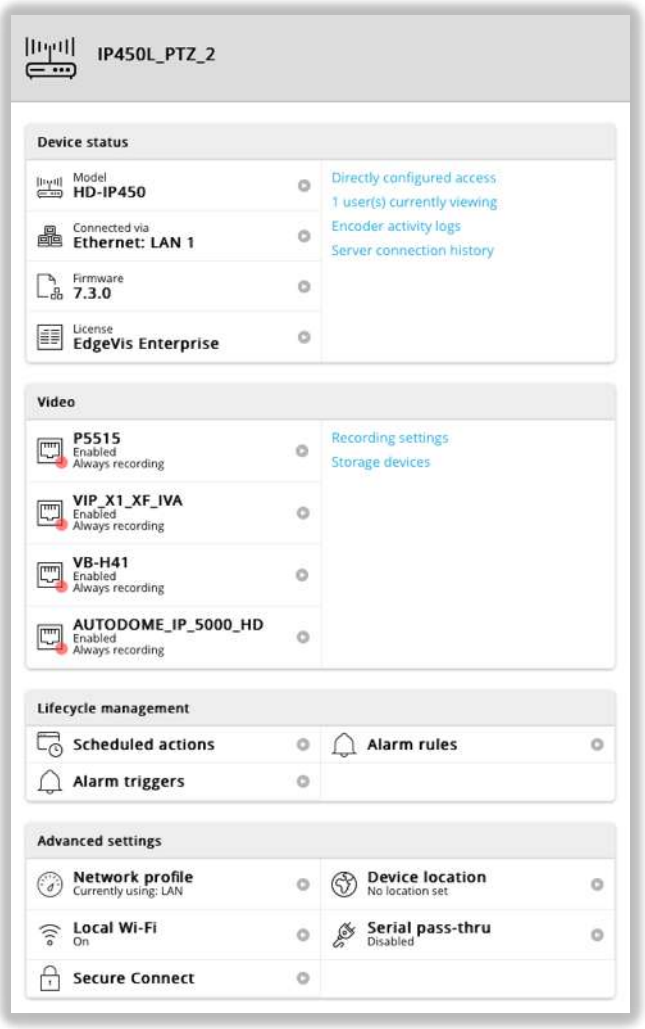
Online encoder configuration options

When an encoder is online the encoder details page will contain a number of new icons, each signifying the status and settings for an area of functionality on the encoder.

Each encoder model supports different levels of functionality and features - the options available on this page will change depending on the model of encoder and the firmware that is installed on this encoder.

Additionally, the user performing configuration of the encoder must have been granted the appropriate permissions within each section.

The following sections provide an overview of each configuration section and how to use it. The pages shown should only be treated as examples, given the difference between encoder products - refer to the encoder's manuals for more complete information on how to configure and get the best out of a specific encoder.



Section: Device Status

The first section provides a high-level overview of the encoder, with a summary view of:

- **Encoder model name** – click to view the status and diagnostics pages *(see next section)*
- **Communications bearer** – click to view the history of the encoder's communications bearers and their connection to the server.
- **Firmware version** – click to view the encoder's current firmware version, and to upgrade the encoder to a newer firmware
- **EdgeVis licence** – click to view the encoder's assigned EdgeVis licence and any licence extensions (e.g. Safezone-2D licence extensions)

Additionally, the right hand options offer the ability to review which users have been granted direct access to the encoder, a list of who is currently viewing the encoder, and access to the encoder's event log.

Status and diagnostics page

The encoder's **Status** page displays useful information about the current status of the encoder, including:

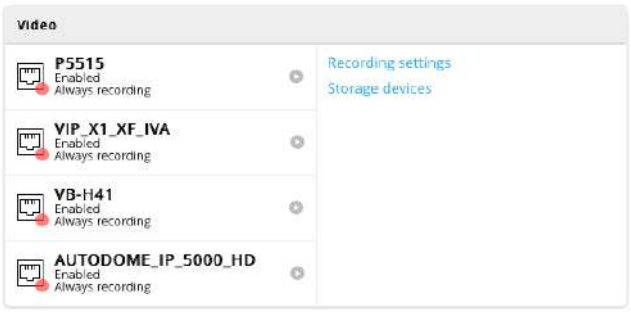
- **Encoder firmware version**
  Use the **Upgrade firmware** menu option to select from the compatible firmware on the server (firmware can be uploaded to the server by server-wide administrators).
- **Encoder model and serial number**
- **Input Voltage**
- **Internal CPU temperature**

Connection details:

- The communications bearer currently being used to connect to the server
- The primary and secondary communications bearers
- Secondary information on the communications bearers (e.g. the LAN MAC address)

Section: Video

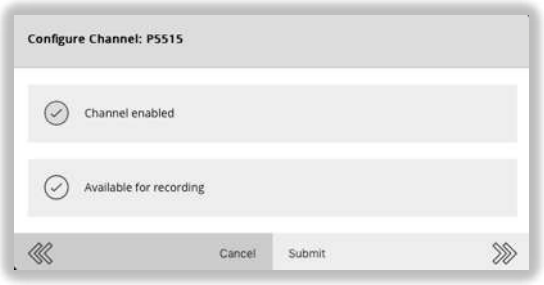
The **Video Inputs** section lists all of the cameras/video inputs that are available on the encoder. This can include:



- Physical camera inputs
  (e.g. PAL/NTSC composite input or HD-SDI)
- Built-in cameras
  (e.g. mobile phone cameras, Q800 dome)
- IP Cameras
  (added during initial configuration)
- Video layouts
  (e.g. Picture-in-picture or Quad-view)

The right section offers additional settings (which may only appear on certain encoder models) for configuring the recording, audio and PTZ settings – these are described in the following sections.

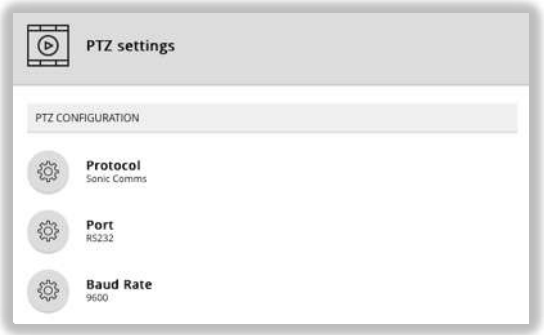
If a user selects one of the listed video inputs they may be offered several options:



- **Enable/Disable the channel**
  This determines if the video input should be listed as an available channel within viewing clients
- Make the input **Available for recording**
  Should this video input be recorded when the encoder is instructed to record (either through 24/7 recording or recording on alarm).
  For non-IP video inputs it is possible to set various recording parameters (e.g. frame-size, recording quality)
- **Audio source**
  On encoders with physical audio inputs it is possible to associate audio inputs with a corresponding video input – this affects both live and recorded video stream.

PTZ settings

The encoder's **PTZ settings** page allows the user to configure the PTZ settings (for non-IP cameras).

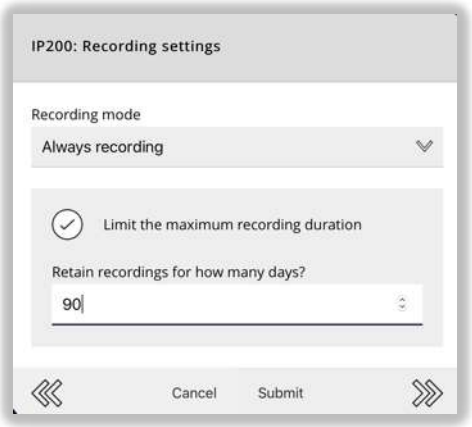


For encoders that support composite or HD-SDI cameras the user must manually configure the PTZ protocol and port using the **Configure PTZ** menu option. Refer to the camera manufacturer's documentation to determine the appropriate settings.

For encoders that support IP cameras, PTZ is set up automatically when adding the camera using the encoder's local web interface (and, as a consequence, this menu option is not available).

Recording settings

The first setting controls how the encoder should behave - encoders can operate in one of two **Recording modes**:



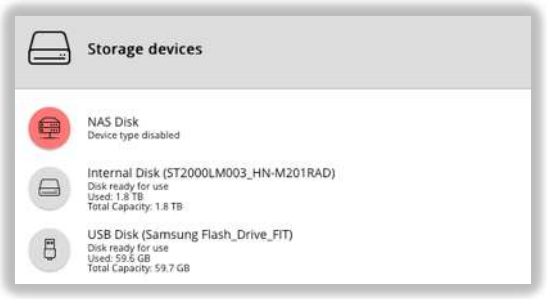
- **Always recording**
  Recordings should be made 24/7, regardless of any alarm rules
- **Record on alarm action**
  By default the encoder should not record, and the user must create alarm rules to initiate recording (usually for a fixed duration).

Additionally, several other options can be present including:

- **Limit the maximum recording duration**
  For legal reasons it is often desired/required to limit the number of days the encoder should retain recordings for. This setting does not guarantee that the encoder will be able to record for this many days (as this is dependent on the size of the disk), only that it will automatically delete recordings once they are over the duration specified.

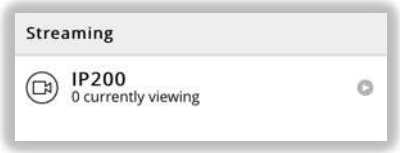
Storage devices

Within the **Storage devices** page the available recording devices are listed, along with their recording status. Click on a device to display further information and options including the disk space available, the option to enable/disable recording to the device, and the ability to remotely erase all recordings on the device.



Section: Streaming

List of output streams (V8.0+ encoder firmware only)



This section contains a list of output video streams on the left-hand side. For every encoder this will only contain one entry, except the 4K-R800 and Video Router 4 that will contain up to two (for 4K-R800) or four (for Video Router 4). Each entry lists two items:

- The name of the output stream
- The number of viewers currently watching this video stream

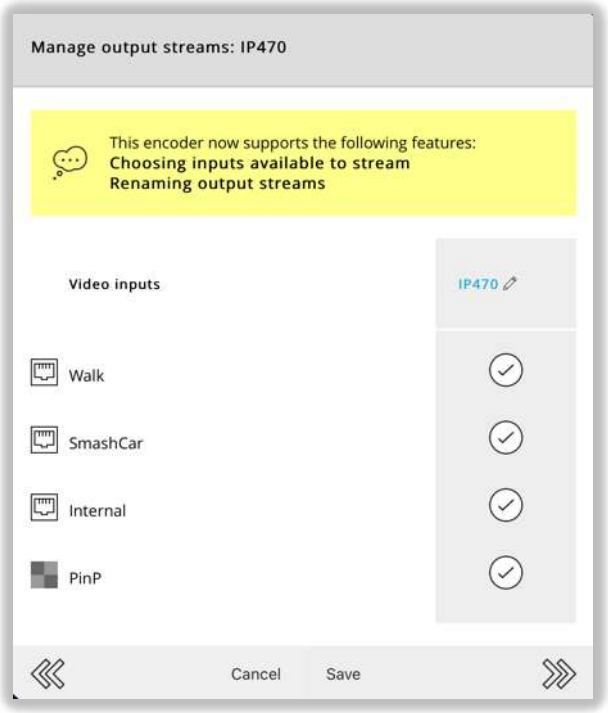
Encoders have both:

- **An encoder name (this is fixed)**
  This is the name of the encoder's account that is programmed into the encoder. This is displayed within EdgeVis server when listing and configuring encoders – and at the top of the encoder's configuration page.
- **A stream name (this can be changed)**
  This is the name displayed within viewing clients – this is what is listed in this section.

Clicking on an item will allow you to configure the output parameters for this stream:

To rename the output video stream:
Click the name of the stream. This will allow you to select a new name that is shown to all viewing clients.

- New stream names must be unique on the server (and this is checked against all existing stream and encoder names).
- Version 8.0 clients will pick up any stream change automatically within the **Home** page, while older clients will need to log out/in.
- Clients viewing a stream that is renamed will find that their video stream playback will stop. To continue they should close any tabs related to this encoder and reopen them using the new name.



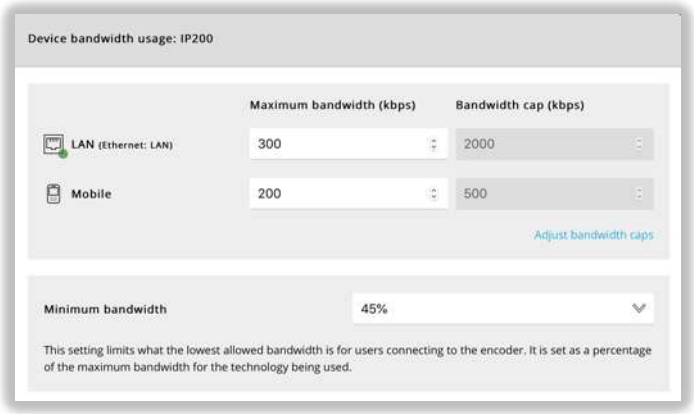
To change the list of video inputs that are listed within the clients:
Tick/untick each desired camera or video layout to show/hide it within clients. This only affects the live transmission capability and will not change any recording or alarming capability.

Device bandwidth usage

This page lists the bandwidth settings for the enabled communications methods on an encoder.

For each entry there are two settings:

- **Bandwidth cap**
  This is an admin setting that can be used to control the maximum bandwidth a user may set for live streaming. It is only configurable on EdgeVis Server, and by default is set to the highest supported bandwidth for that type of connection.
- **Maximum bandwidth**
  This is the live setting a user will use operationally when setting streaming bandwidths – users may set this within EdgeVis Server or EdgeVis Client up to the **Bandwidth cap** limit set.



Both of these settings are protected by different permissions. This allows an admin to manage costs by limiting the user's ability to set higher rates, while still providing the end users the permission to set their desired bandwidth up to the desired bandwidth cap limit.

Minimum bandwidth

Users viewing an EdgeVis stream all receive the same stream from an encoder. The stream is transmitted once from the encoder to EdgeVis Server, and the server distributes that stream to all clients.

As part of the continual quality-of-service monitoring of each link, an individual client can detect it does not have enough available bandwidth to view the encoder's stream at the current bitrate. It can request that the encoder temporarily lower the bandwidth so that it may continue to view the stream (based on what the client believes it can achieve).

As the same stream is received by all clients if one client requests to reduce the video bitrate, then all clients will receive the same lower quality stream. In order to stop one rogue viewer from dropping the video bitrate significantly for all users it is possible to set a **minimum bandwidth** level (as a percentage of the maximum bandwidth).

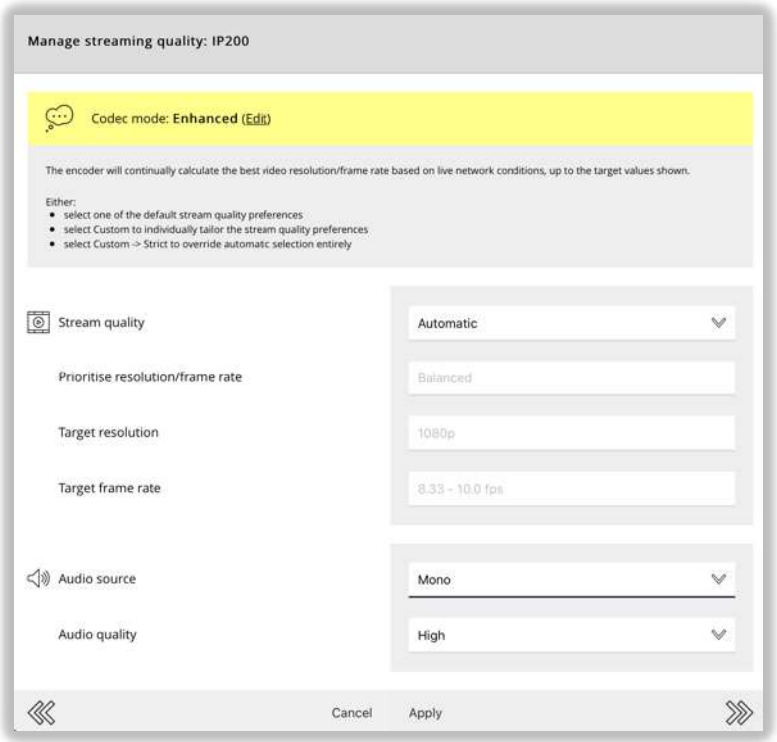
Should a viewer's available bitrate fall below that level, then they will not be able to lower the bitrate any further and they will soon be unable to view the stream without interruption.

Manage streaming quality

This page allows the user to control the video resolution and frame rate of the live video stream. Version 8.0 encoders support two modes of operation:

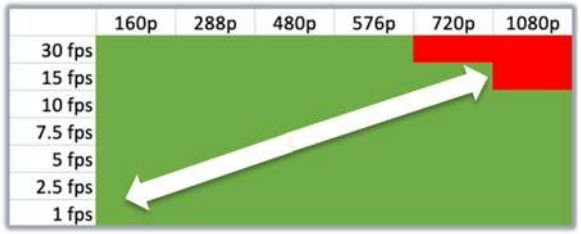
- **Compatible (default for new and upgraded encoders)**
  For users who have legacy version 7 clients (or third-party applications that the v7 Decoder SDK, e.g. Milestone VMS [as of November 2020]). The automatic selection of video resolution and frame-rate is only performed:
  - When the first viewer starts streaming
  - When the user selects any new quality/ bandwidth setting
  - When the encoder switches between communications methods
- **Enhanced (recommended)**
  For users who have no legacy viewers it is recommended to use the **Enhanced** video codec mode. This will allow the encoder to dynamically and continually alter the video resolution and frame rate based on live bandwidth conditions observed by the encoder. This powerful capability allows the encoder to maintain a consistent quality level during periods of difficult or ever-changing bandwidth conditions.
  However older v7 clients will be unable to view the video stream produced in Enhanced mode.

To switch between codec modes use the **Edit** button.



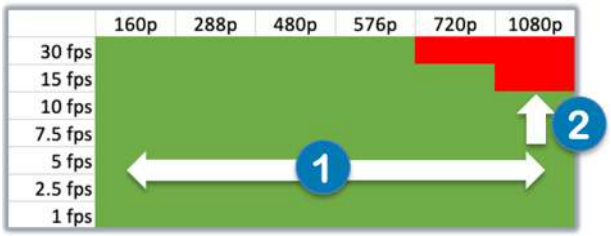
Stream quality settings

This section provides controls for tailoring the video quality settings. The highest-level configuration option contains four different preferences - designed so that most customers will be best served with a fully **automatic** setting, with some alternative presets to satisfy more specific deployment scenarios.



Automatic: Balance changes in resolution and frame rate to maintain a constant quality level

Best frame rate: Attempt to increase frame rate to maximum first and then, if possible, increase resolution



Best resolution: Attempt to increase resolution to maximum and then, if possible, increase the frame rate

Economy: Limit frame rate and resolution to 160p, up to 3.5fps to minimize bandwidth usage

While the four main preset options should satisfy most customers, you can also tailor the encoder's behaviour further. Select **Custom** from the **Stream quality** menu to customise the encoder's streaming settings:

You can choose between four schemes in **Prioritise resolution / framerate:**

- **Balanced (Enhanced mode only)**
  Similar to Automatic, but the encoder won't select a value above the selected target resolution or frame rate.
- **Prioritise frame rate (Enhanced mode only)**
  Similar to Best frame rate, the encoder will increase the frame rate until it hits the target frame rate, and then it will increase the resolution up to the target resolution.
- **Prioritise resolution (Enhanced mode only)**
  Similar to Best resolution, the encoder will increase the resolution until it hits the target resolution, and then it will increase the frame rate up to the target frame rate.
- **Strict**
  The encoder will disable all automatic adjustment and will use target resolution and frame rate.

Notes:

The target frame rate and resolution options will filter out unavailable combinations. For example if you select 1080p then the target frame rates will be limited to 10fps, in line with the encoders' capabilities.

These options do not reflect the incoming RTSP video stream for IP cameras. Should the camera present a lower resolution/frame rate the encoder will automatically reduce to match.

Audio Settings

There are two audio settings available to encoders who have a video stream that contains an audio source.

- **Audio source**
  Select whether the incoming audio stream should be transmitted as **Mono** or **Stereo**, or whether it should be disabled entirely. Be aware that stereo audio transmission will use twice as much bandwidth as mono.
- **Audio quality**
  The encoder can adjust the audio quality dynamically, should the overall live bandwidth drop to a point where the audio bitrates would negatively affect the video stream. This setting can be configured to one of three quality levels: Low / Medium / High. This dictates the minimum proportion of bandwidth the encoder should allocate to the audio from the chosen maximum bandwidth. Higher settings ensure, should the available live bandwidth drop, that more bandwidth is reserved for the audio.

Section: Lifecycle management

The pages within this section predominately deal with three interrelated sections of functionality

- Physical alarm configuration
- Alarm rules and scheduled actions
- Encoder sleep modes

These are advanced capabilities and beyond the scope of this document. Further information on how to best utilise alarms and sleep modes can be obtained from the **EdgeVis Alarm and Sleep Management Guide**.

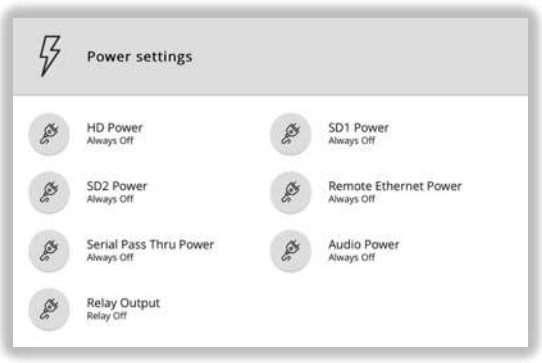
Additionally, some encoders can also provide power to external devices – the next section describes this configuration.

Power settings

Some encoders can provide power to external devices (e.g. to supply power to attached cameras). It is normally possible to enable/disable the power supply to these devices remotely.

Click on the desired power option to change the configuration. Some encoders only allow the power to be manually enabled/disabled, while others have additional options where the power can be intelligently enabled (e.g. when a viewer starts viewing the video stream).

This section also allows the user to toggle any relay output on/off.



Section: Advanced settings

Local Wi-Fi

If supported, the encoder may support the creation of a local Wi-Fi hotspot. This is primarily used to access the local web interface, or to perform 'drive-by' download of recordings.

Local Wi-Fi can operate in one of two modes:

- Always on
- Switched – where Wi-Fi is normally used to connect to a wireless router to provide a connection to the server, but can be switched to hotspot mode remotely, to allow local access

The **Local Wi-Fi** page allows the user to configure the settings of the wireless access point created, as well as switching in/out of Local Wi-Fi mode when in Switched mode.

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.

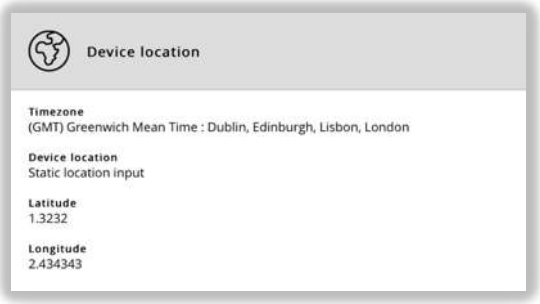
The **SecureConnect** page lists the channels configured on the encoder, allowing the user to edit the channel, remove the channel, or add a new one using the **Add channel** menu option.

Using a SecureConnect channel (through EdgeVis Client) will use some of the same bandwidth that is normally allocated to the live video stream (lowering the video quality). Use the **Edit bandwidth** menu option to change the maximum percentage of bandwidth all SecureConnect users will share.

Further details on SecureConnect can be found in the KB Article IP Series - Using SecureConnect to access remote devices.

Location Settings

The encoder's **Device Location** page can be used to configure the time zone that should be used when reporting time from the encoder, and the settings used to transmit the encoder's location to viewing clients. There are three options available (depending on the encoder model):



- Internal GPS module
- External USB/Serial GPS module (e.g. the USB GlobalSat BU353 and Serial BU355 dongles – other NMEA 0183 devices may be compatible)
- Static location (manually enter GPS longitude/latitude co-ordinates)

Most external GPS devices that require a baud-rate operate at 4800 baud.

Serial Pass–Thru

Serial Pass-Thru is a feature that allows remote serial devices, attached to the encoder, to be controlled remotely through the secure EdgeVis infrastructure. It is an advanced feature, and it is recommended to contact Digital Barriers support for further information on its use.

The **Serial Pass-Thru** page displays the current settings and allows the user to select which serial port and baud-rate to use.

The **Send out-bound serial data to all viewers** option allows the user to broadcast all serial data (received on the encoder's serial port) to all viewing clients, as opposed to the user who has the Serial Pass-Thru channel open.

ADVANCED SERVER CONFIGURATION

This section of the manual explains how to perform advanced configuration of the server (including the use of SSL and alarm management messaging).

Using an SSL certificate with the web management portal

Introduction to SSL

SSL is a protocol that secures the link between a web browser and the server where a web page resides. It has two functions:

- Encrypt the traffic between the browser and the server so that no one can eavesdrop on it.
- Verify the identity of the server communicating with the browser. This ensures that no one can pretend to be the server and intercept communications meant for it.

The protocol uses digital certificates to perform these functions. These both communicate the encryption keys required to encrypt the traffic and a signature of those keys that verifies the server's identity. Certificates also have a limited lifetime, after which they will expire and will need to be renewed.

EdgeVis Server only allows access to the web interface using SSL. By default, a certificate is generated during installation. This certificate, referred to as a 'self-signed' certificate, can provide the required keys and enable encryption of the link. However, the signature is not from a trusted source and the web browser will report it as insecure.

There are two options for supplying a trusted SSL certificate for EdgeVis Server:

1. Automatically using the **Let's Encrypt** service. This is a free, third-party service that automatically generates valid certificates for web servers that are accessible over the public internet. EdgeVis Server can use this service to automatically create and renew certificates.

Note: Be aware that *Let's Encrypt* is a third-party service. Digital Barriers cannot guarantee the security or availability of this service.

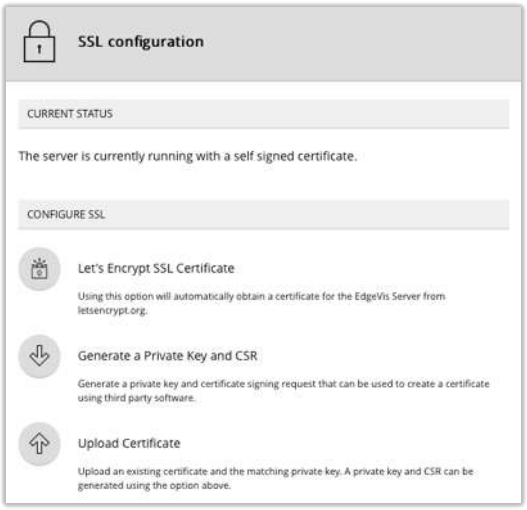
2. Manually using a third-party or internal **Certification Authority (CA)**. It is possible to upload a certificate that has been generated using an internal or third-party CA to EdgeVis Server. This allows using certificates from Microsoft Active Directory or an external service like DigiCert or Verisign.

Setting up EdgeVis Server to use Let's Encrypt

To be able to use a Let's Encrypt certificate, the EdgeVis Server deployment must meet these requirements:

- The server must be **accessible** via the **public internet**. The server must be directly connected to the internet or behind a firewall that is configured to allow the server to connect to the Let's Encrypt service over port **443**.
- Let's Encrypt must be able to access port **80** on the EdgeVis Server. This port is used by Let's Encrypt to verify that the server is available on the **DNS name** it is claiming the certificate for. **Note: EdgeVis Server will only open this port while doing the initial certificate request and when renewing the certificate (once every 2 months).**
    - If EdgeVis Server is behind a **firewall** port **80** must be allowed through that firewall and forwarded to EdgeVis Server.
    - Port **80** must not be used by any other software running on the same machine as EdgeVis Server.
    - If EdgeVis Server is installed on **Linux**, the user that it is running as must be **allowed to use port 80**. Normally this is restricted to **root**. However, some Linux installations allow configuration for other users to use this port.
- The server must have a **public DNS name** assigned to it. For example, it will be accessible using a DNS address, e.g. 'https://server.company.com:9443/, and not a raw IP address, e.g. 'https://192.168.0.1:9443/'. This must be set up using a third-party service, e.g. GoDaddy or Netnames.
- *Let's Encrypt* requires a valid E-Mail address to be supplied along with certification requests. This address will be stored by *Let's Encrypt* and associated with the requests made by EdgeVis Server.

1. Collect the required information:
    a. The (already registered) DNS name to be used by EdgeVis Server
    *(e.g. **server.company.com**)*
    b. An E-Mail address to be sent to *Let's Encrypt* with certificate requests
2. From the Server Home Page go to **Advanced Settings -> SSL configuration**
3. Select **Let's Encrypt SSL Certificate**



4. Enter the information from **Step 1** into the form and submit the form to begin the process.
5. The server will attempt to obtain the certificate
6. If successful, refresh the web browser and it should report the connection as secure (clicking on the padlock in the address bar should show the certificate's information and show that it was created by Let's Encrypt).

Using an Externally Generated Certificate

To use an externally generated certificate with EdgeVis Server the certificate must meet the following requirements:

- The certificate must be valid for the address used to access EdgeVis Server. For example, **server.company.com** in **https://server.company.com:9443/**.
- It must be an x***509*** certificate in ***base64*** format. These are text files that begin with this line:

  -----BEGIN CERTIFICATE-----

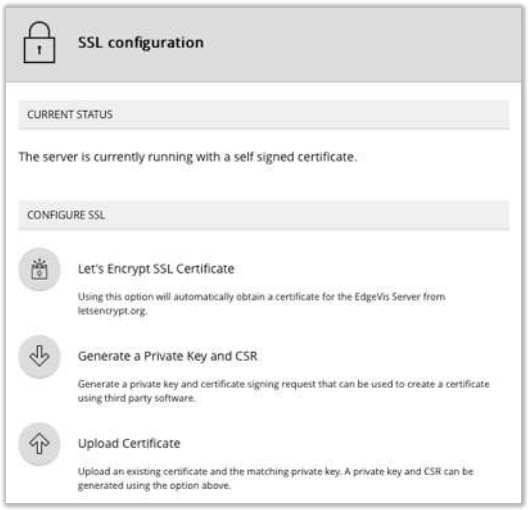
- A **Private Key** that goes with the certificate. It must be an ***RSA PKCS8*** key in ***base64*** format and should be a minimum of **2048 bits** in length. These are text files that begin with this line:

  -----BEGIN RSA PRIVATE KEY-----

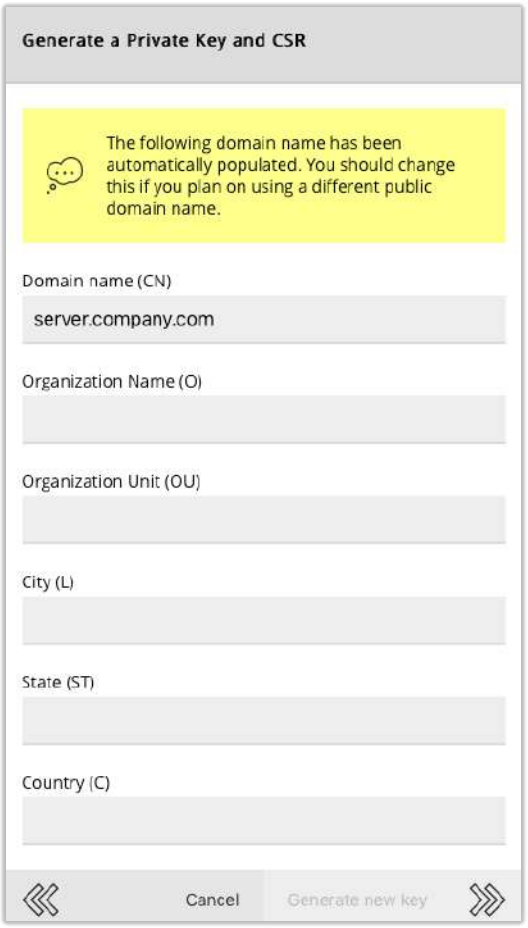
(Optional) Step 1 – Generate request files

EdgeVis Server can generate a private key and a **Certificate Signing Request**. The key generated is **4096 bits** in length and the certificate request will create a certificate, which is valid for **two years**. This step is not required, but can make it easier to generate a valid certificate:

1. Collect the required information:
   a. **Address assigned to EdgeVis Server in the certificate**
   *(For example **server.company.com**)*
   b. **Subject information for the certificate.** The need for each of the following fields and what should go in them is dependent on the service generating the certificate. The available fields are:
      - **Organisation** – the company or organisation legal name.
      - **Unit** – the department or divisional name.
      - **Locality** – the city where the department is based.
      - **State** – the state or county that the city is in.
      - **Country** – the two-letter code for the country that the city resides in.
2. From the Server Home Page go to **Advanced Settings -> SSL configuration**.
3. Select **Generate a Private Key and CSR**.



4. Fill in the required information from **step 1** into the form and select **Generate new key**
5. The server will then generate the following two files, that will be downloaded by the web browser.
    c. **EdgeVis-Server-SSL-Certificate-Request.txt** – this contains the **Certificate Signing Request** to be given to the service that will generate the certificate.
    d. **EdgeVis-Server-SSL-Private-Key.txt** – this contains the private key that goes with the certificate.
6. Send the **Certificate Signing Request** to the service or person responsible for generating the certificate.
7. Receive the signed certificate back.



Note: The private key *must* be backed-up and kept secure. If the private key is lost, then the certificate cannot be used to rebuild the server in the event of failure. The private key can be used by an attacker to eavesdrop on connections secured with the certificate if it is stolen. This key is *not* to be sent to the service generating the certificate.

Step 2 – Upload the certificate

Uploading a **Certificate** and **Private Key** to EdgeVis Server:

1. Collect the required information:
    a. **Address assigned to EdgeVis Server in the certificate**
    (For example **server.company.com**)
    b. The **Certificate** and **Private Key** files in the correct format.
    If the certificate was generated using a request and key generated by EdgeVis Server, the two files required are the certificate that came back after submitting the request and the **EdgeVis-Server-SSL-Private-Key.txt** file downloaded when generating the request.
2. From the Server Home Page go to **Advanced Settings -> SSL configuration**.
3. Select **Set up SSL** from the **Advanced Server Actions** menu available at the top right of the **Server Status**
4. Select **Upload Certificate**.
5. Ensure that the **Domain** field has the address from **Step 1.a** in it.
6. Browse to the **Private Key** and **Certificate** files in the other two fields in the dialog.
7. Select **Upload**
8. Reload the web browser, which should now report the connection as secure.

Note: All certificates have a limited lifetime. Check how to get a renewed certificate from the generating service or person. Once renewed, the new certificate must be uploaded using the same procedure.

Messaging Configuration

EdgeVis Server supports sending notifications on alarm events via Mobile Push, SMS and E-Mail. This allows users of the system to receive alarm notifications - even when they are not using EdgeVis Client.

This section provides guidance on how to set up and configure each of these methods of communication.

Note: Be aware that each of these services will send alarm notifications through third-party services. Digital Barriers can not guarantee the security or speed of delivery of any notifications sent through these mechanisms.

Mobile Push Notifications

Using Mobile Push Notifications, EdgeVis Server is able to send notifications to a user's smart phone. This is a free service offered by Digital Barriers and provided using Amazon Web Services. It is disabled by default and requires a server administrator to enable it. Once enabled it applies to all domains.

Server settings for push notifications

The push notification service uses Amazon Web Services, which requires that the EdgeVis Server meets the following requirements:

- It must be able to reach Amazon's servers at **sns.eu-west-1.amazonaws.com** using **HTTPS** on port **443**.
- Any filtering/proxy of web traffic from the server mustn't alter/delay the requests going to Amazon's servers.

To enable/disable push notifications:

1. From the Server Home Page go to **Advanced Settings -> Messaging configuration**
2. Select Mobile push notifications
3. Check the **Enable Mobile Push Notifications** check box to enable the service.

Registering users for push notifications

When the user logs in to the server using EdgeVis Client for iOS or Android, the device is automatically registered and assigned to the user. Once registered the device will receive notifications under the following conditions:

- Any alarm rule notifications assigned to this user are sent to all their device(s).
- If the user logs in using multiple devices, then all of those devices will receive push notifications.
- If the device is used to log in to another server then notifications will be received from both servers.
- If another user logs in using the same device, they take ownership of the device and only their notifications from that server will be received.
- Uninstalling EdgeVis Client will stop notifications on the device. The device will need to log in and register again to start receiving notifications after the client is re-installed.
- If the notifications setting is disabled for EdgeVis Client on the device, no notifications will be received until they are re-enabled. (See device manufacturer's documentation for details)
- The device's behaviour on receiving a notification will be dependent on how it has been configured. For example, no ring tone will play if the device is set to silent.

To view the devices registered to a user, go to the user's page within EdgeVis Server, then click the **Push notifications** button. The user themselves can see their list from the **Settings** menu within EdgeVis Client.

SMS Text Message Notifications

Using SMS, EdgeVis Server can send notifications to any phone number capable of receiving SMS text messages.

Note: In EdgeVis Server 7.2 and below, this service was implemented using the Cardboardfish messaging platform. The Cardboardfish platform has been acquired by Sinch and is no longer allowing new users to use the Cardboardfish interface. The settings for Cardboardfish will be preserved for existing users, however, we **strongly recommend** migrating to a provider that allows access via SMPP.

Server settings for SMS

This feature requires access to an SMS provider that supports sending messages using the SMPP protocol. There are a number of commercial providers who offer this service, usually charging by the message.

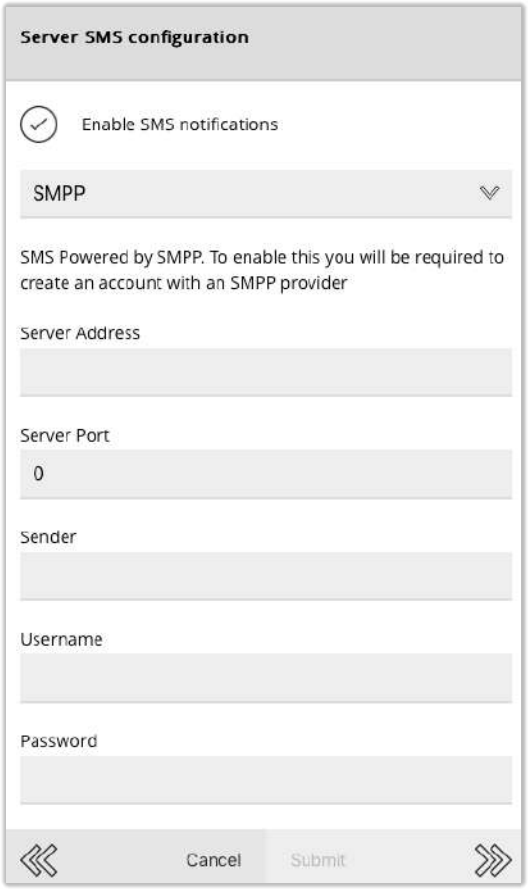
Requirements for service provider:

- Must support an alphanumeric sender (e.g. "EdgeVis Server" or "12345") -
  *This is what the '**from**' of the SMS will be set to*
- Must support sending to E.164 phone numbers (e.g. "441234567")
- EdgeVis Server must be able to reach the **address** and **port** supplied by the SMPP provider

To enable SMS on the server:

1. From the Server Home Page go to **Advanced Settings -> Messaging configuration**
2. Select **SMS**
3. Check the **Enable SMS Notifications** check box and select **SMPP** from the drop down.
4. Enter the server address/port and login details from the SMS Provider.
5. The **Sender** field should be set to reflect what the '**from**' part of the SMS should be. This can be a short phrase or phone number. Check with the SMS Provider what they allow for exact limits.

   Users within the United States should be aware of additional restrictions around the use of SMS – please refer to the next section for further detail.



Important note for US Customers

US law has strict rules regarding SMS and its use in commercial situations.

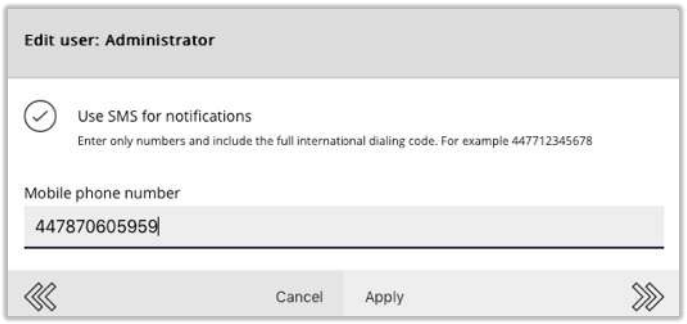
Users within the US must contact their provider to obtain a **Toll Free Number** (a small monthly charges will apply). As a commercial user of SMS, all SMS must be sent from a Toll Free Number to allow commercial SMS to be identified as such.

Note: Users who fail to obtain a Toll Free Number may find the SMS service will silently fail when the recipient is within the US – the SMS will send, but never be received.

User settings for SMS

For each user who desires to receive notification by SMS, they must first

1. Open the user's page within EdgeVis Server
2. Click **SMS**
3. On the SMS setting page, tick **Use SMS for notifications**, then enter the user's phone number. This should be in full international phone number format (omitting any preceding zeros or plus signs)



Configuring e-mail for notifications and account e-mails

EdgeVis Server supports sending e-mail notifications and user account e-mails using **SMTP** and **SMTPS** protocols. This allows administrators to use most internal and third-party e-mail services.

Note: SMTP does not encrypt any data sent allowing anyone who can intercept it to read it. If the mail system you are connecting to is not on a secure network with EdgeVis Server, it is **strongly** recommended that EdgeVis Server is configured to use the encrypted **SMTPS** protocol instead.

Server settings for E-Mail

The requirements for EdgeVis Server to send e-mail are as follows:

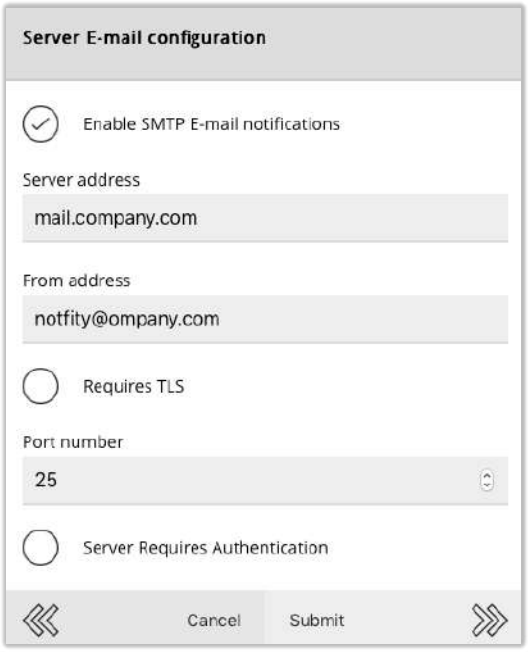
- An internal mail server **or** valid account on a third-party e-mail service.
- EdgeVis Server must be able to contact the e-mail server using **SMTP** or **SMTPS**.
- For **SMTPS**, the SSL certificate for the e-mail server must be trusted by the machine running EdgeVis Server.

The following sections describe how to enable e-mail notifications with an internal SMTP server, a Microsoft Exchange Server, and Google Mail's SMTP service.

Internal SMTP settings

Connecting to an internal **SMTP** server with no authentication:

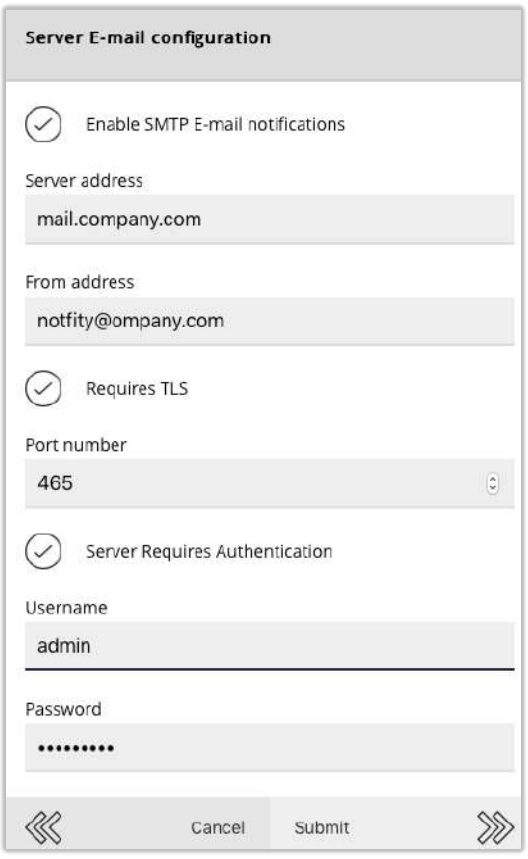
1. Collect the following information from your Email administrator:
    a. **Email server address**
    for example: mail.company.com
    b. **SMTP port number**
    *The default is **25***
    c. **The Email address notifications will come from**
    for example: notifications@company.com
2. From the Server Home Page go to **Advanced Settings -> Messaging configuration**
3. Select **Email**
4. Check the **Enable SMTP Email Notifications** check box and enter the information from step 1 into the fields on the dialog box. Make sure **Requires TLS** and **Server Requires Authentication** are left un-checked.



Microsoft Exchange settings

Connecting to a Microsoft Exchange server:

1. Collect the following information from your Email administrator:
    a. **Exchange server address**
    for example: mail.company.com
    b. **Exchange secure SMTP port number**
    *The default is **465***
    c. **The Email address notifications will come from**
    for example: notifications@company.com
    d. **User that corresponds to the above address**
    for example: notifications
    e. **Password for the above user**
2. From the Server Home Page go to **Advanced Settings -> Messaging configuration**
3. Select **Email**
4. Check the **Enable SMTP Email Notifications** check box and enter the information from step 1 into the fields on the dialog box. Check **Requires TLS** and **Server Requires Authentication** as well.



Google Mail settings

Connecting to Google Mail service:

1. Collect the following information from your Email administrator:
    a. **The Google Mail address notifications will come from**
    for example: notifications@gmail.com
    b. **Password for the above address**
2. Several Google settings must be configured to allow access
    a. Log in to Google Mail and follow **Step 1** in the **Set up Gmail with Outlook, Apple Mail, or other mail clients** instructions available here: https://support.google.com/mail/troubleshooter/1668960?hl=en
    b. Users who employ Google's two-factor authentication are required to create an app-specific password to use with EdgeVis Server. Follow this link to create such a password (for Step 12): https://security.google.com/settings/security/apppasswords?pli=1
    c. If not using two-factor authentication Google Mail needs to be configured to allow plain password authentication. To do this follow the instructions here: https://support.google.com/accounts/answer/6010255?hl=en
3. From the Server Home Page go to **Advanced Settings -> Messaging configuration**
4. Select **Email**
5. Check the **Enable SMTP Email Notifications** check box
6. Enter **smtp.gmail.com** as the **Server Address**
7. Enter the Google Mail address from step 1 as the **From Address**
8. Check the **Requires TLS** check box
9. Enter **587** as the **Port Number**
10. Check the **Requires Authentication** check box
11. Enter the Google Mail address from step 1 as the **Username**
12. Enter the password from step 1 as the **Password** (or Step 2b. for two-factor authentication users).