MediaSeal

Encryptor Manual

VERSION 6.0.0

Fortium Technologies Ltd

www.fortiumtech.com

1 CONTENTS

2 MEDIASEAL 9

2.1 MEDIASEAL OVERVIEW 9

3 COMPONENTS 10

3.1 MEDIASEAL ENCRYPTOR CLIENT 10

4 SYSTEM REQUIREMENTS 11

4.1 HARDWARE REQUIREMENTS 11

4.1.1 Minimum Hardware Requirements 11

4.2 SUPPORTED OPERATING SYSTEMS 11

5 REQUIREMENTS 12

5.1 MEDIASEAL ACCOUNT 12

5.2 ILOK ACCOUNT 12

5.3 PERMISSIONS TO INSTALL SOFTWARE 13

5.4 MEDIASEAL ENCRYPTOR CLIENT SOFTWARE 13

5.5 LICENSING 13

5.5.1 Studio License 14

5.5.2 Encryptor Client License 14

6 VERSION COMPATIBILITY 15

6.1 ENCRYPTOR APPLICATION COMPATIBILITY 15

7 INSTALLATION 16

7.1 INSTALLATION ON WINDOWS 16

7.2 INSTALLATION ON MACOS 17

8 ILOK ACTIVATION – REGISTERED MEDIASEAL ACCOUNTS 18

8.1 ACTIVATE ILOK LICENSE 18

8.1.1 Login to your iLok account. 19

8.1.2 Select License to Activate 20

8.1.3 Activation Location *21*
9 STUDIO LICENSE **22**
9.1 INITIAL STUDIO LICENSE 22
10 LOGIN **23**
11 ADDITIONAL STUDIO LICENSES **24**
12 LOGOUT / QUIT **25**
13 MANAGE USER ACCOUNT **26**
14 HOME DASHBOARD **27**
15 SETTINGS **28**
15.1 GLOBAL SETTINGS 29
15.1.1 General *29*
15.1.2 Mail *30*
15.1.3 Security *31*
15.2 LOCAL SETTINGS 32
15.2.1 Zone Connectivity Test *32*
15.2.2 Encryptor Time Zone *33*
15.2.3 Auto Logout Threshold *33*
16 ZONE ENDPOINTS **34**
16.1 ZONE ENDPOINTS OVERVIEW 34
16.2 MANAGING ZONE ENDPOINTS 35
16.2.1 Local Endpoints *35*
16.2.2 Testing Zone Endpoints *36*
16.2.3 Add New Zone Endpoint *37*
16.2.4 Edit Zone Endpoint *38*
16.2.5 Restore Default Zone *38*
16.2.6 Remove Zone *39*
16.3 SETTING PROXY SERVER 40
17 ENCRYPTOR USERS **41**

17.1 MANAGING ENCRYPTOR USERS 41
17.1.1 Create Encryptor User *42*
17.1.2 Edit Encryptor User *43*
17.1.3 Delete Encryptor User *44*
17.1.4 Activate Encryptor User *44*
17.1.5 Deactivate Encryptor User *45*
18 ENCRYPTOR GROUPS 46
18.1 MANAGING ENCRYPTOR GROUPS 46
18.1.1 Create Encryptor Group *47*
18.1.2 Edit Encryptor Group *48*
18.1.3 Delete Encryptor Group *48*
18.1.4 Activate Encryptor Group *49*
18.1.5 Deactivate Encryptor Group *49*
18.1.6 Manage Encryptor Group Memberships *50*
18.2 SET APPLICATION PERMISSIONS 51
18.2.1 Allow Permission: *52*
18.2.2 Deny Permission: *52*
18.2.3 Permission Controls *53*
18.3 SET RECIPIENT PERMISSIONS 55
18.3.1 Add a User / Group / Department: *56*
18.3.2 To Remove a User / Group / Department: *56*
18.3.3 To Remove All Users / Groups / Departments: *56*
19 DECRYPTOR USERS 57
19.1 MANAGE DECRYPTOR USERS 57
19.1.1 To Add a Decryptor User: *58*
19.1.2 To Remove a Decryptor User *58*
19.1.3 Delete a Decryptor User from your Studio *59*
19.1.4 Activate a Decryptor User on your Studio *59*
19.1.5 Deactivate Decryptor Users from your Studio *60*
19.1.6 Clear the search field and retrieve all users *60*
20 DECRYPTOR GROUPS 61

20.1 MANAGE DECRYPTOR GROUPS 61
20.1.1 Create Decryptor Group *61*
20.1.2 Edit Decryptor Group *62*
20.1.3 Manage Members of a Decryptor Group *63*
21 DECRYPTOR DEPARTMENTS 64
21.1 MANAGE DECRYPTOR DEPARTMENTS 64
21.1.1 Create Decryptor Department *64*
21.1.2 Edit Decryptor Department *65*
21.1.3 Manage Members of a Decryptor Department *65*
22 TITLES 66
22.1 MANAGE TITLES 66
22.1.1 Create Title *67*
22.1.2 Edit Title *68*
22.1.3 Delete Title *68*
22.1.4 Activate Title *69*
22.1.5 Deactivate Title *69*
22.1.6 Manage Title Permissions *70*
23 JOBS 72
23.1 JOBS OVERVIEW 72
23.2 SEARCH 72
23.2.1 Search Filters *73*
23.3 CREATE JOB 74
..... 74
23.3.1 To create a new Job: *74*
23.3.2 Source Tab *78*
23.3.3 Destination Tab *81*
23.3.4 Viewers Tab *83*
23.3.5 Viewer Options Tab *84*
23.3.6 Contact Details Tab *85*
23.3.7 Summary Tab *85*
23.4 DUPLICATE JOB 87

23.5 Edit Job 87
23.6 Change Access Permissions 88
23.7 Archive Job 89
23.8 Delete Job 90

24 TEMPLATES 91

24.1 Managing Templates 91
24.1.1 Create Template 91
24.1.2 New Job from Template 92
24.1.3 Export Template 92
24.1.4 Delete a template: 93
24.1.5 Create Shortcut 94

25 FILE VERIFICATION 95

26 UPLOAD AUDIT LOGS 96

27 REPORTING 97

27.1 Viewing Audit Data 98
27.1.2 Audit Types: 99
27.1.3 Filters: 100
27.2 Exporting Audit Data 101

28 COMMAND LINE 102

28.1 Command Line Options 102
28.1.1 Help 103
28.1.2 Local Endpoint 104
28.1.3 Global Endpoint 104
28.1.4 License. 104
28.1.5 Studio Id 104
28.1.6 Job XML File 105
28.1.7 Screen output 105
28.1.8 Auto Quit 105
28.1.9 Multiple Instances 105
28.1.10 Output Status 106

28.1.11 Template ID *106*
28.1.12 Template Job Name *106*
28.1.13 Example Command Line Encryptor (Windows) *107*
28.1.14 Example Command Line Encryptor (MacOS) *108*
28.1.15 Command Line Error Codes *108*
28.2 COMMAND LINE XML FILES 110
28.2.1 Configure the template file: *110*
28.2.2 Using XML File (Windows) *112*
28.2.3 Using XML File (macOS) *112*
28.2.4 User Group Modification *113*
28.2.5 Output Status XML File *115*
28.3 DRAG AND DROP FILE PROTECTION 116
28.3.1 Drag and Drop File Protection (Windows) *116*
28.3.2 Drag and Drop File Protection (MacOS *118*

29 DIAGNOSTIC LOGGING 120

29.1 ENABLE DIAGNOSTIC LOGGING ON WINDOWS 120
29.2 ENABLE DIAGNOSTIC LOGGING ON MACOS 121

30 MEDIASEAL LINUX HEADLESS INSTALLATION 122

30.1 PRE-REQUISITES 122
30.2 INSTALLATION AND CONFIGURATION 123
30.2.1 Installation *123*
30.2.2 Configuration *123*
30.2.3 Building Encryptor.conf *124*
30.3 ENCRYPTOR USAGE 125

31 TROUBLESHOOTING 126

31.1 BASIC TROUBLESHOOTING 126
31.2 MEDIASEAL SUPPORT 127
31.2.1 MediaSeal Support Portal *127*
31.2.2 MediaSeal Email Support *127*

2 MediaSeal

2.1 MediaSeal Overview

MediaSeal

MediaSeal® is a robust, multi-layered content security platform that has been specifically designed for media editing environments.

MediaSeal has been designed to fit smoothly into collaborative workflows with the minimum amount of end user disruption.

Using a combination of sophisticated data encryption techniques and multi-layer access controls, MediaSeal® can protect sensitive content and provide comprehensive security auditing.

3 COMPONENTS

3.1 MEDIASEAL ENCRYPTOR CLIENT

MediaSeal Encryptor is a client application that is used to generate secure content. MediaSeal Encryptor Client can protect content using different factors of authentication, depending on use case and the network environment of the user accessing protected content (who are known as "Decryptor" users).

These authentication methods include password, iLok and Server authentication. Access to protected content can be managed within MediaSeal Encryptor Client when content is protected using Server + Multi Factor (password, iLok and Server) Authentication. The MediaSeal Encryptor Client enables an administrator to dynamically control and monitor access to content.

Different authentication policies can also be used to protect content for use in isolated or restricted environments by using single factor (password-only) or Multi factor (password and iLok) authentication.

MediaSeal Encryptor Client can be used seamlessly in existing workflows by utilising features such as template driven and batch encoding.

4 System Requirements

4.1 Hardware Requirements

4.1.1 Minimum Hardware Requirements

Processor: Dual Core Intel / AMD processor (or Above)

Memory: 4Gb RAM (or Above)

Storage: 1 Gb free space (or Above) + additional space as needed for content Files

4.2 Supported Operating Systems

MediaSeal is supported on a range of operating systems and versions. We regularly update our products to ensure we support the latest operating systems.

For the latest information and list of supported operating systems please visit our support site.

MediaSeal Support Site

---

5 REQUIREMENTS

5.1 MEDIASEAL ACCOUNT

To start using MediaSeal, you must register an account. You will receive an email invitation containing an individual registration link from **noreply@mediaseal.com.**

Click on the link or paste into your browser and then complete the online registration form. If you have not received an invitation to register for a MediaSeal account, please contact the studio owner.

5.2 ILOK ACCOUNT

An iLok account is a 3rd party license management service that is used to manage MediaSeal licenses. As part of the MediaSeal registration process, you will be asked to enter your existing iLok account details or to create a new iLok account.

More information on iLok technologies and where to purchase a physical iLok can be found on the website

https://www.ilok.com

5.3 Permissions to Install Software

You will need administrative permissions on your computer to be able to install the MediaSeal Encryptor Software. If you do not have permissions or are not sure, please contact your System Administrator for further assistance.

5.4 MediaSeal Encryptor Client Software

Links to download MediaSeal Encryptor Client software will be sent to your email address where you can download and install the software for your Operating System (OS).

5.5 Licensing

The MediaSeal Encryptor Client license is managed using iLok PACE technologies. As part of the MediaSeal registration process you will be asked for your iLok account details. You can use either an existing iLok account or create a new iLok account.

5.5.1 Studio License

Each studio has a unique license. To manage that studio and protect content using MediaSeal Encryptor Client, you will need a studio license. A license will be provided by MediaSeal for your own studio, or alternatively, by the owner of the studio.

5.5.2 Encryptor Client License

As part of the MediaSeal registration process, you will be asked to enter your existing iLok account details or create a new iLok account. Once registration is completed, we will deposit a MediaSeal Encryptor license to your iLok account.

You can then activate your license and allocate the license to a physical iLok or to a specific computer (creating a "soft license").

Please see the Activate iLok Section on how to activate your iLok license.

6 VERSION COMPATIBILITY

6.1 ENCRYPTOR APPLICATION COMPATIBILITY

MediaSeal products are regularly updated to include security features and enhancements. On occasion, this requires changes that are incompatible with previous versions.

To ensure compatibility with all MediaSeal components, please ensure you are running the latest version of MediaSeal

7 INSTALLATION

7.1 INSTALLATION ON WINDOWS

To install MediaSeal Encryptor Client for Windows, please ensure that you have closed any open applications and saved your files. MediaSeal Encryptor Client will require you to restart your machine once the installation is completed.

- **Download** the software using the links provided in the email
- **Extract** the contents of the compressed file to locate the installer files inside the compressed folder.
- Launch **setup.exe** and follow the on-screen instructions.

7.2 Installation on MacOS

To install MediaSeal Encryptor Client for macOS, please ensure that you have closed any open applications and saved your files. MediaSeal Encryptor Client will require you to restart your machine once the installation is completed.

- **Download** the software using the links provided in the email
- **Extract** the contents of the compressed file to locate the installer files inside the compressed folder.
- Launch **MediaSealEncryptor.dmg** and follow the on-screen instructions.

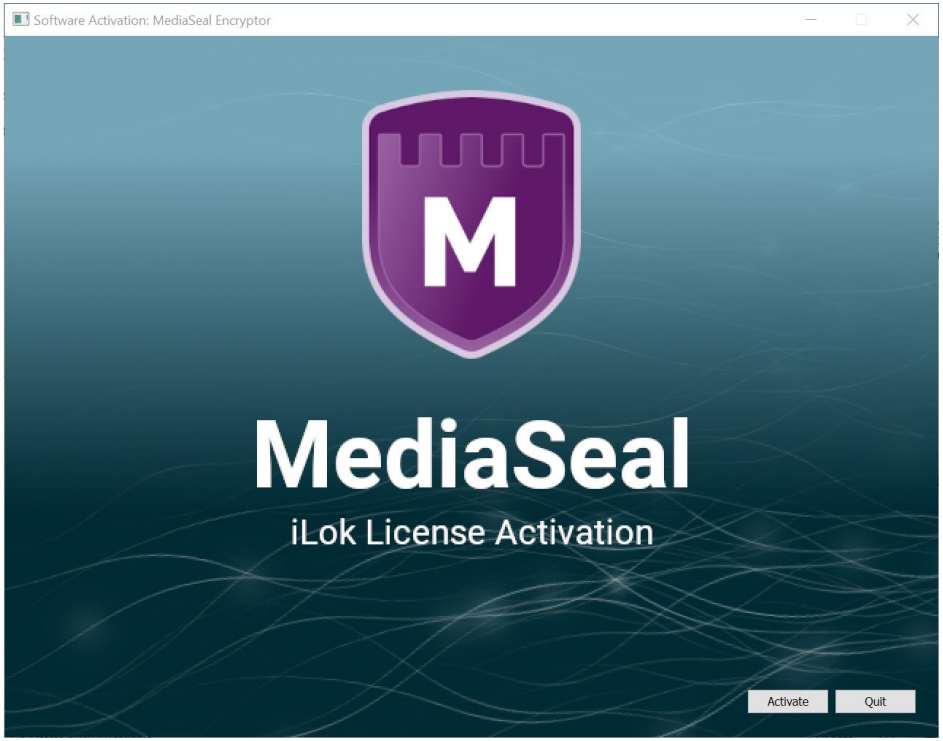
8 iLok Activation – Registered MediaSeal Accounts

8.1 Activate iLok License

On first reboot, MediaSeal Encryptor Client will request you to activate your iLok license.

To activate your iLok License:

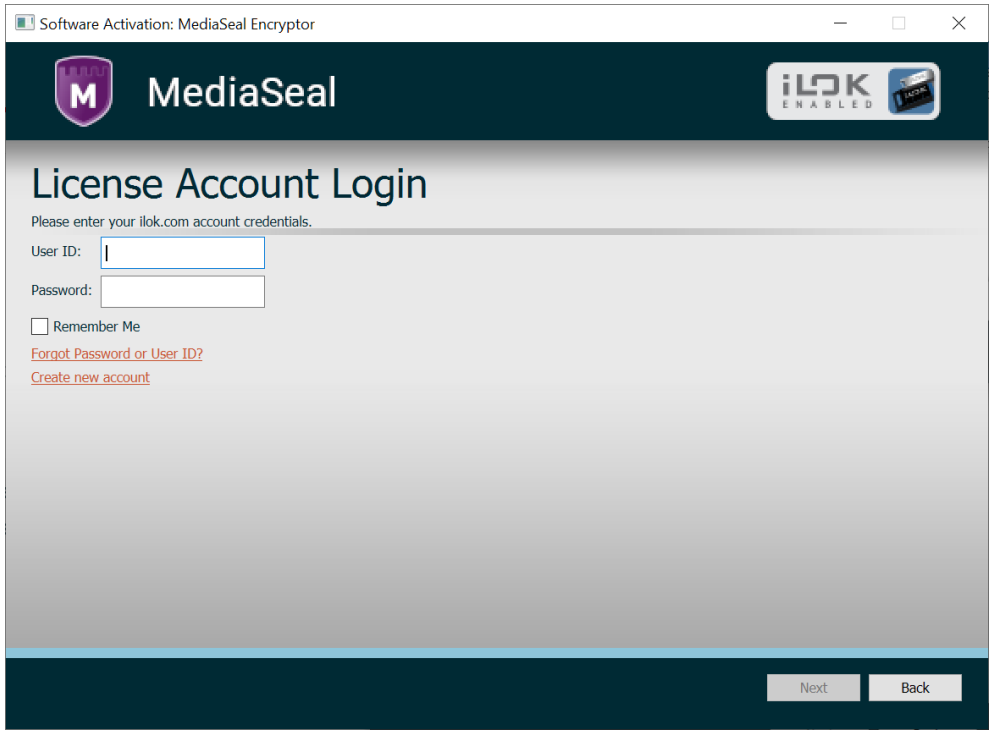
- Launch the **Encryptor Client**
- Click **Activate**



8.1.1 Login to your iLok account.

To activate your Encryptor licence located in your iLok account, please enter your iLok account credentials.

- Enter your **User ID**
- Enter your **Password**
- Click **Next**



*If you have forgotten your iLok account credentials, Click **Forgot Password or User ID?** Or navigate to*

https://www.ilok.com/#!recover

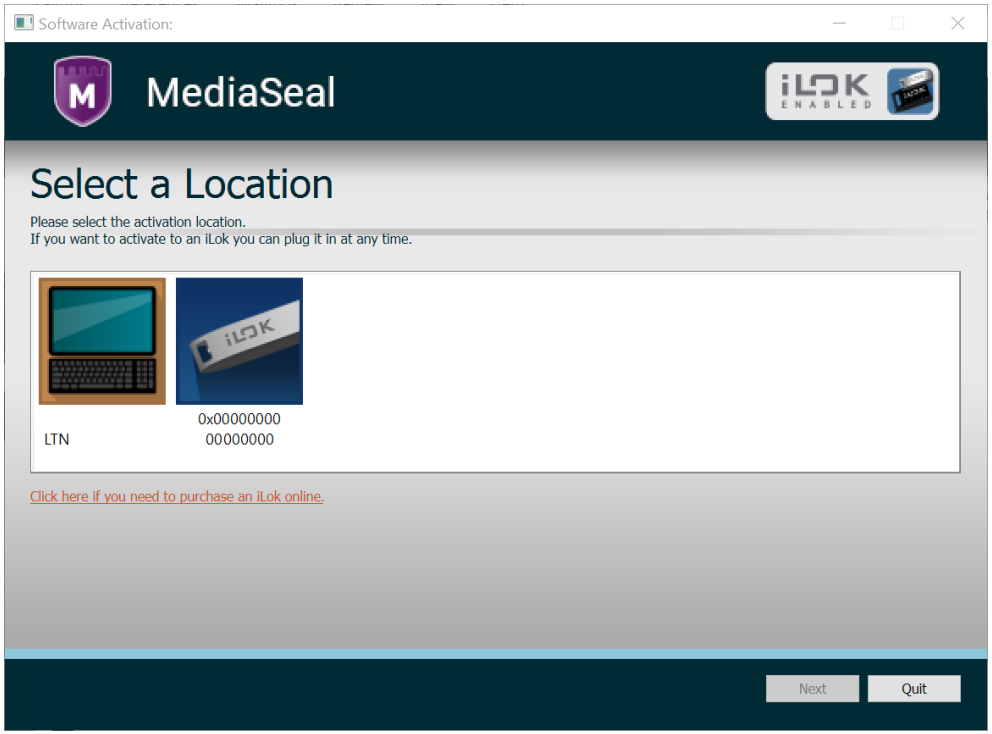
8.1.2 Select License to Activate

Once you have successfully entered your iLok credentials, a screen will display the licenses available to activate.

To select a license to activate:

- Click on **MediaSeal Decryptor License**
- Click **Next**

8.1.3 Activation Location



You can allocate your MediaSeal Encryptor Client license to either a physical iLok or a computer.

- Select Your **Computer** or your **iLok**
- Click **Next**

8.1.3.1 Allocate License to Physical iLok

Allocating the MediaSeal Encryptor Client license to a physical iLok enables you to encrypt sensitive content on multiple computers where MediaSeal Encryptor Client is installed.

8.1.3.2 Allocate License to Computer

Allocating the MediaSeal Encryptor Client license to a specific computer restricts encrypting content to that specific computer. It should only be used if you do not have a physical iLok.

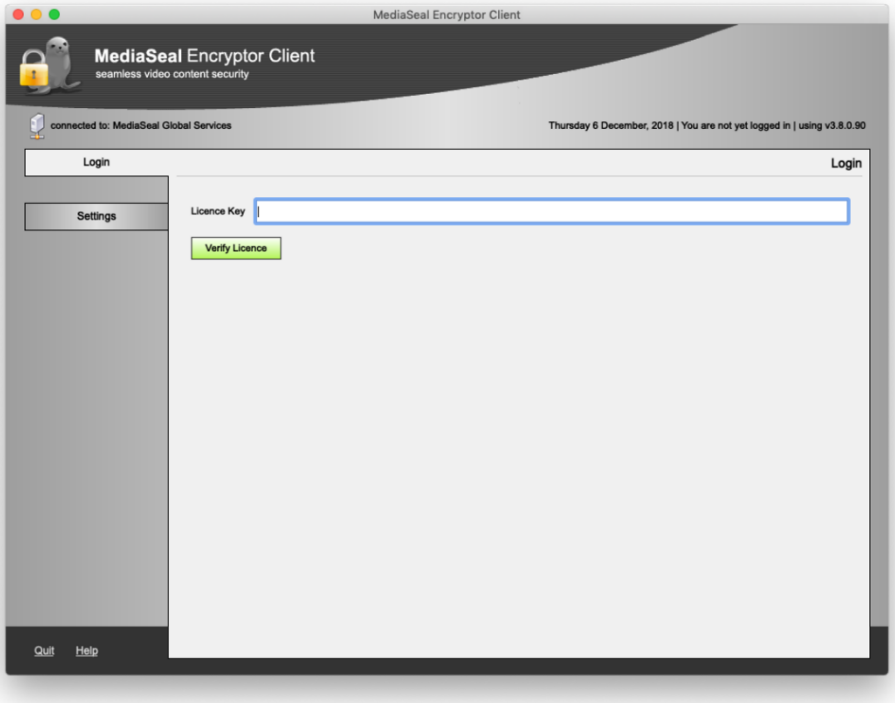
9 Studio License

9.1 Initial Studio License

The first time you launch MediaSeal Encryptor Client, you will be prompted to enter your Studio License Key.

To enter your license key:

- Enter your **License Key**
- Click **Verify License**

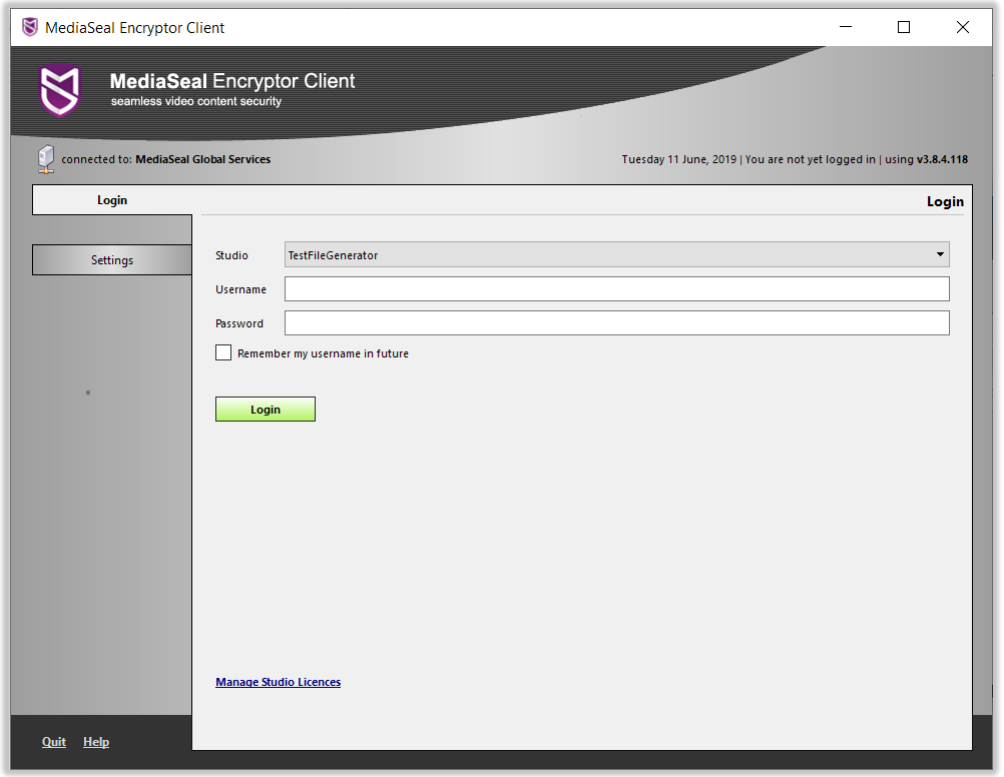


10 LOGIN

To use the MediaSeal Encryptor Client, you first need to select the studio you want to connect to and provide your credentials for that studio.

To select the studio and login:

- Click **Studio** drop down list
- **Select** the correct Studio
- Enter your **Username**
- Enter your **Password**
- Click **Login** button

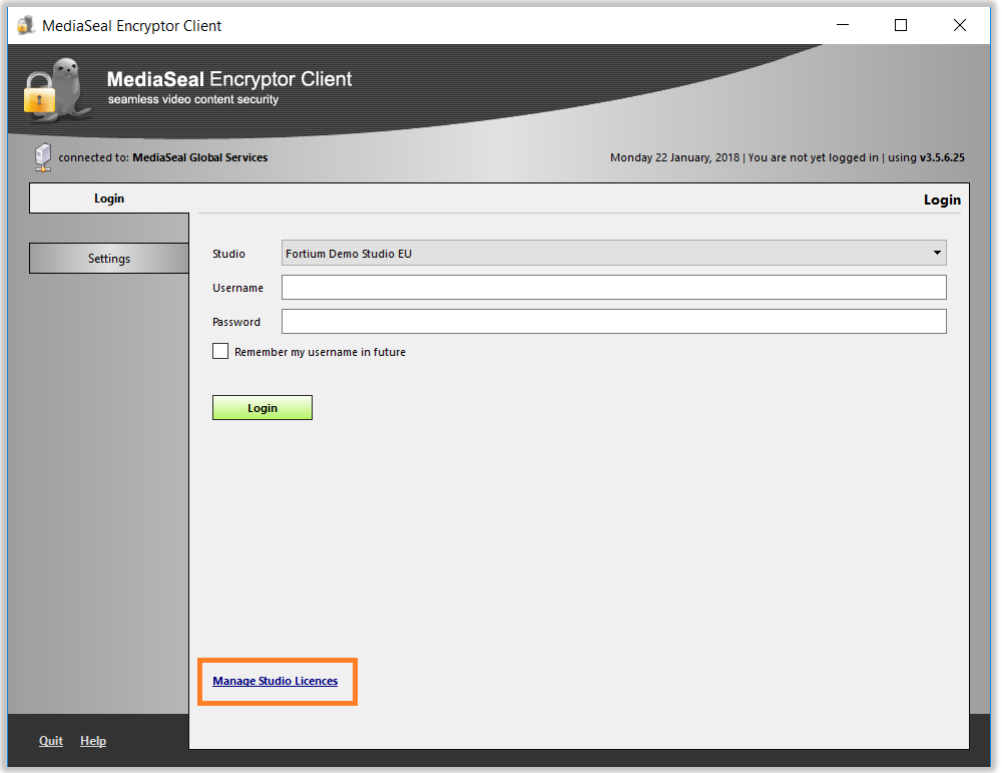


11 ADDITIONAL STUDIO LICENSES

You can add additional studio licenses to the MediaSeal Encryptor Client once an initial license has been configured. This can be achieved from the login screen or the settings screen.

To manage additional studio licenses:

- **Launch** MediaSeal Encryptor Client
- Click on **Manage Studio Licenses**
- Enter **Your Studio License**
- Click **Add Studio License**



12 LOGOUT / QUIT

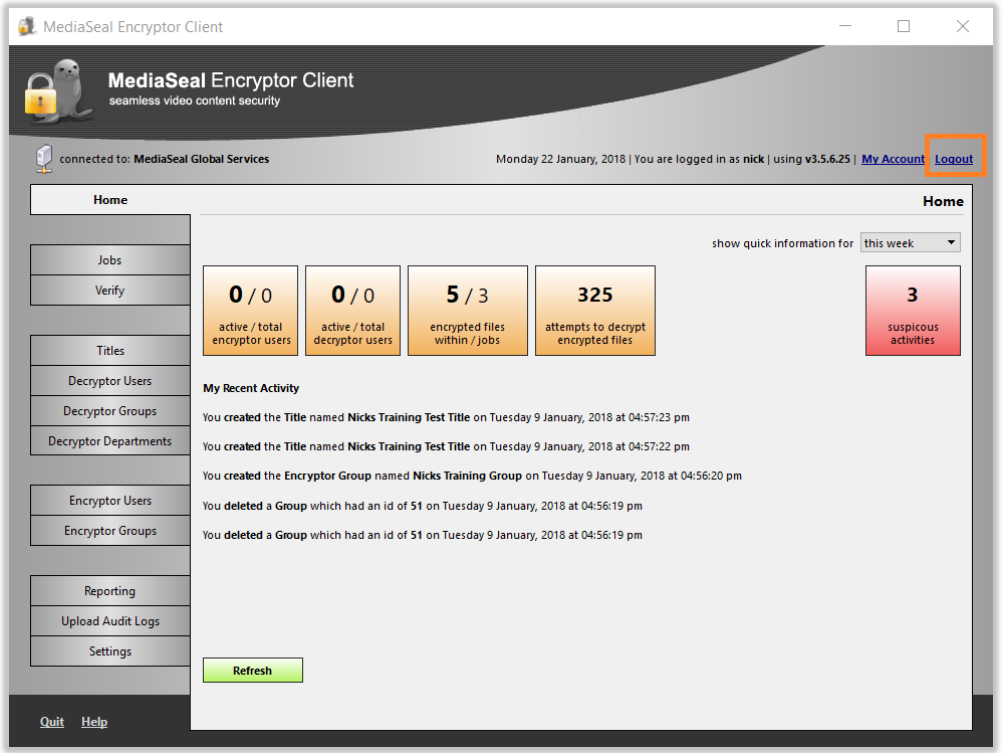
You can either logout of the MediaSeal Encryptor Client, which keeps the application open and enables you to connect to another studio, or you can quit the application completely.

To logout:

- Click the **Logout** link on the top right

To quit:

- Click the **Quit** link on the bottom left.

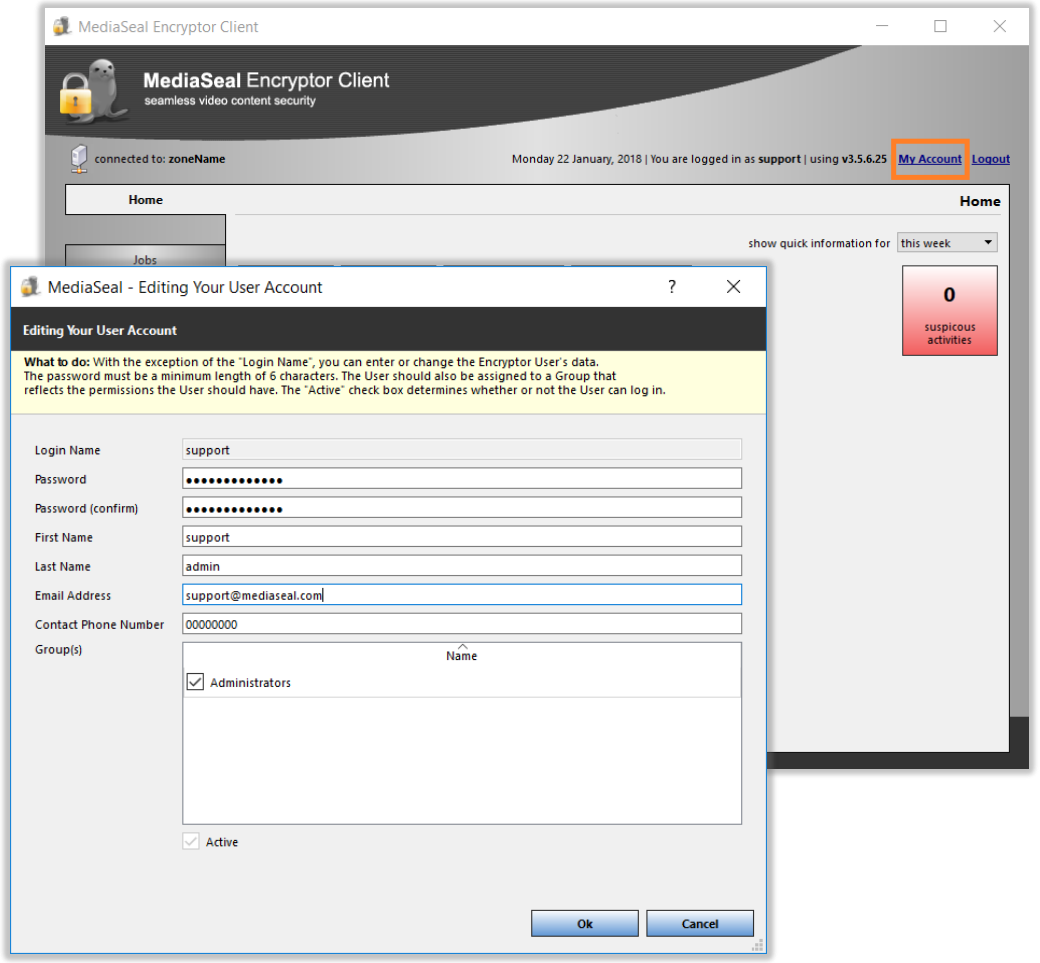


13 MANAGE USER ACCOUNT

You can manage your MediaSeal Encryptor User account at any time by using the My Account link.

To manage your account:

- Click **My Account**
- **Edit** your details as required.
- Click **Ok**



14 HOME DASHBOARD

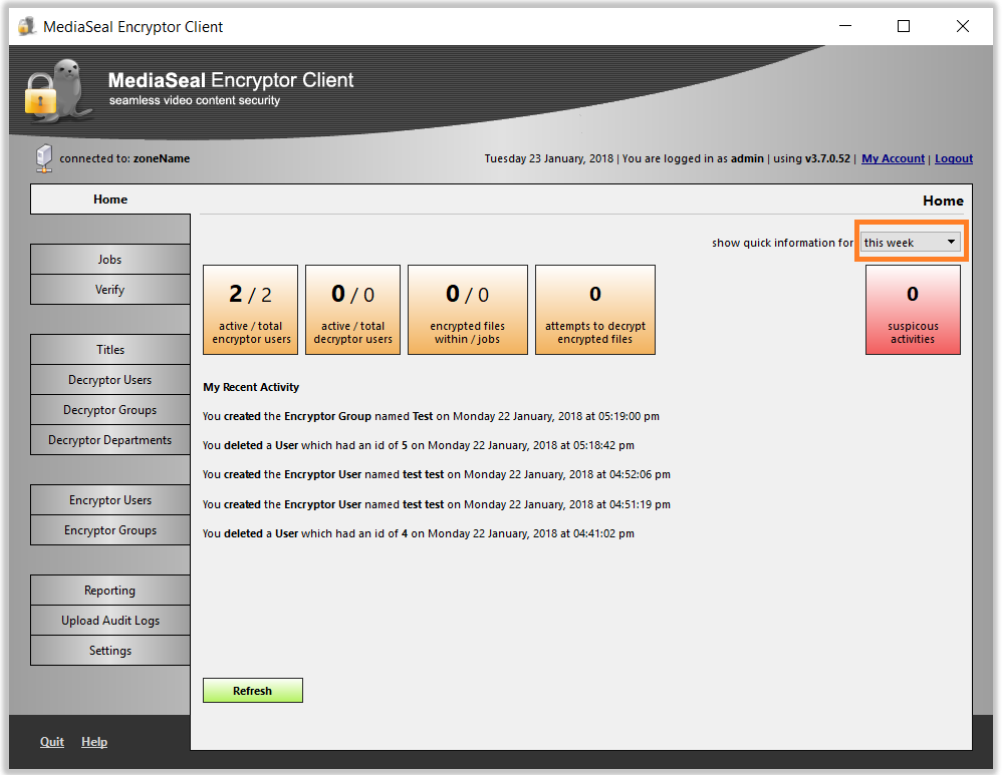
The home dashboard provides a summary of your most recent activity. In addition, it displays the number of Encryptor users, Decryptor users, encrypted files, and the number of attempts to decrypt protected content within your studio server. It also provides a warning indicator of suspicious activity.

By default, the information is displayed for the current week, however you can view additional statistics for **month**, **year,** and **all time**.

To change the view:

- Click on the **drop-down list**
- Select the desired view

You can update the view with the latest information by clicking the Refresh button.

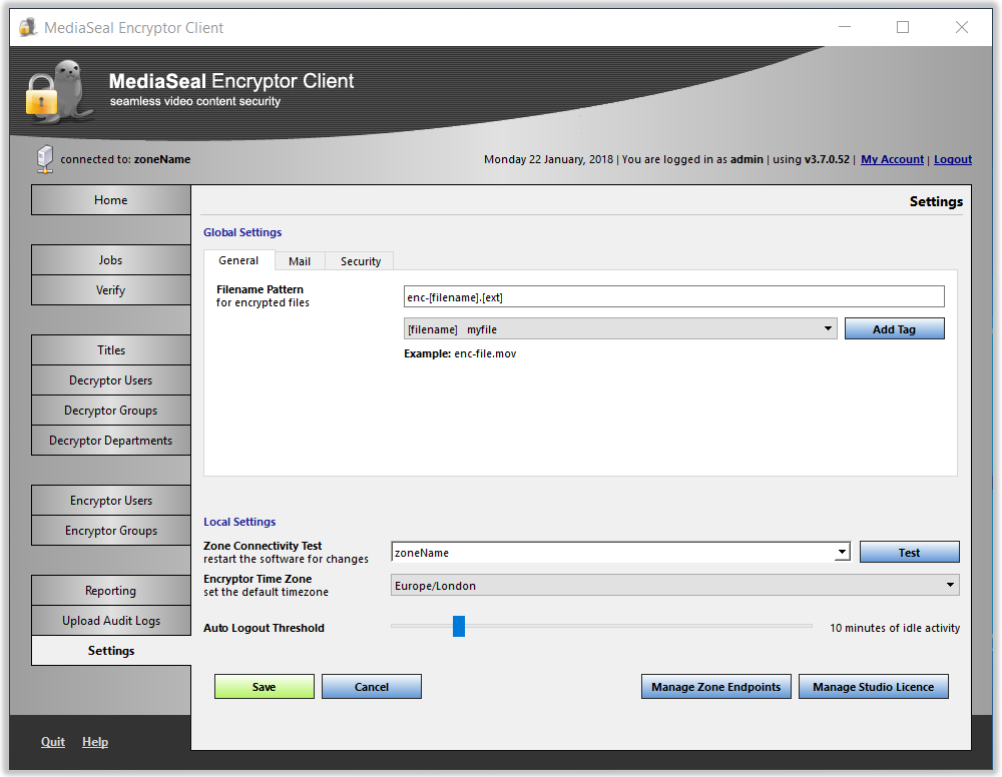


15 SETTINGS

The MediaSeal Encryptor Client settings section enables you to manage your studio licenses, configure your local settings including time zone and Zone Endpoints.

In addition, depending on your permissions, you can also set Global Settings which include filename patterns for new jobs, mail configuration and security settings.

You can view what Zone Endpoint is currently connected above the "Home" button, on the left tool bar. See the **Zone Endpoints** *section for more information.*



15.1 Global Settings

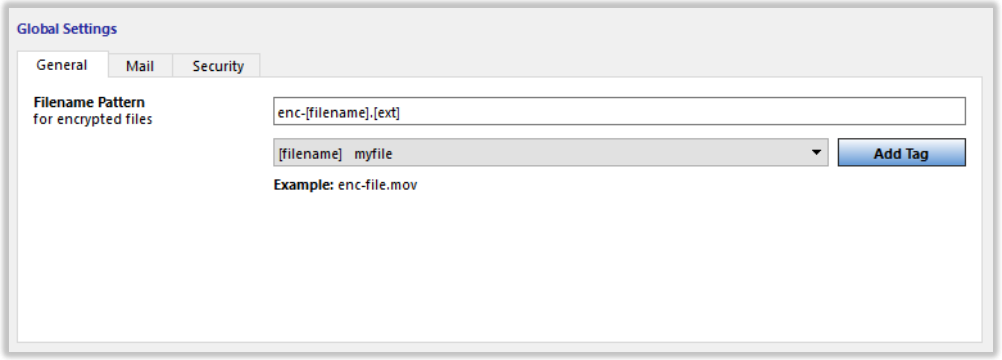
15.1.1 General

You can use the general tab to configure the global filename pattern that will be used as a template when protecting content. The output filename will be based on the template you set. The default setting is **enc-[filename].[ext]**

You can generate a pattern using Tags (variables derived from Jobs) and fixed text. The default setting includes an example of using both types.

To modify the filename pattern:

- Manually type in the Filename pattern any **fixed text** elements.
- Click on the **drop-down list**
- Select the **Tag** you wish to include
- **Position the cursor** in the input field where you wish to insert a Tag
- Click **Add Tag**



15.1.2 Mail

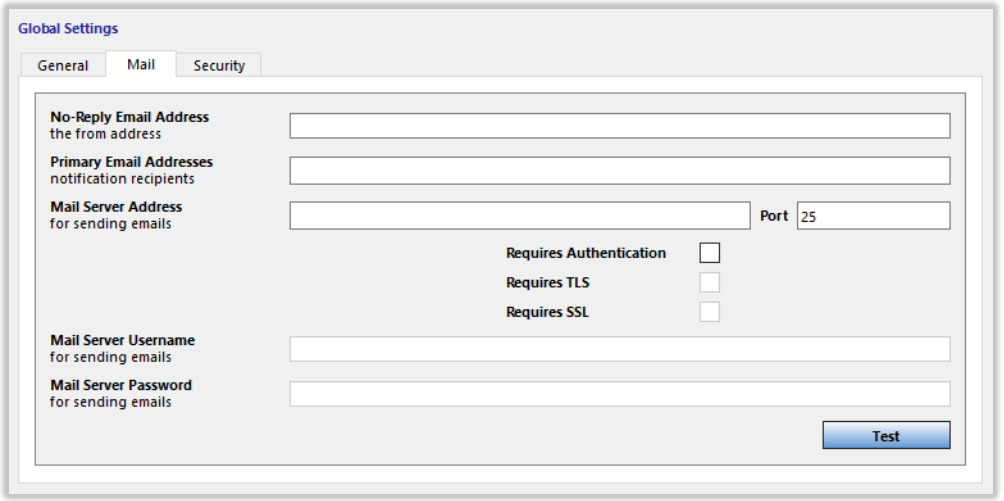
The Mail tab allows you to configure email settings that will be used to send alerts of suspicious activity. It is important that this setting is configured if you wish to be alerted of suspicious activity.

To configure the Mail tab:

- Enter your mail server settings in the respective field.

To test your settings:

- Click the **Test** button



**If you do not know your mail server settings, please contact your System Administrator for assistance.*

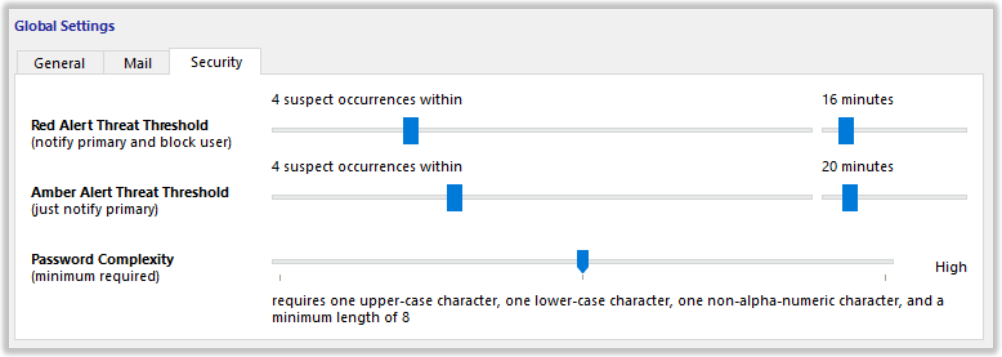
Primary Email Addresses are used to configure which email addresses will receive alerts of suspicious activity.

15.1.3 Security

The security tab allows you to set thresholds for suspicious activities. There are **Red** and **Amber** alert thresholds that can be set to alert a user of any suspect occurrences. It also allows for the setting of required minimum complexity for passwords.

To modify the threat thresholds and/or password complexity:

- Move the **Slider** to the required value



15.1.3.1 Red Alert Threat Threshold

The Red Alert threshold is the number of occurrences that occur within a given time. If the threshold limit is exceeded, then the primary contact (as set in Mail Tab) will be notified and the user will be blocked.

15.1.3.2 Amber Alert Threat Threshold

The Amber Alert threshold is the number of occurrences that occur within a given time. If the threshold limit is exceeded, then the primary contact (as set in Mail Tab) will be notified.

15.1.3.3 Password Complexity

There are 3 different levels of password complexity that can be set, **Medium, High,** and **Strong.** Setting the respective type will display the minimum password complexity requirements in the label.

15.2 LOCAL SETTINGS

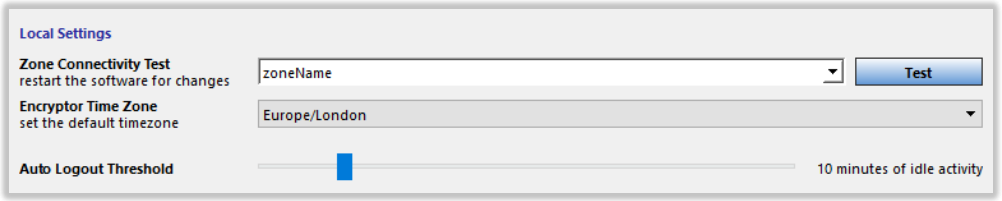
Local settings allow you to set and test your Zone Endpoint, set the time zone and how long before Encryptor will automatically logout.

15.2.1 Zone Connectivity Test

This will allow you to verify connectivity to the Zone Endpoint.

To Test a Zone Endpoint:

- Select the **zone** to check
- Click **Test**



15.2.2 Encryptor Time Zone

This will set the local time zone used by MediaSeal Encryptor Client. This will set the time zone for auditing and reporting, as well as being used as the default time zone when setting start and end dates used to restrict access to content.

To change the time zone:

- Click the **drop-down list**
- Select the desired **time zone**

15.2.3 Auto Logout Threshold

This sets the logout threshold for idle activity within MediaSeal Encryptor Client.

To change the Logout Threshold:

- Move the **slider** left to decrease, or right to increase the Auto Logout Threshold

16 ZONE ENDPOINTS

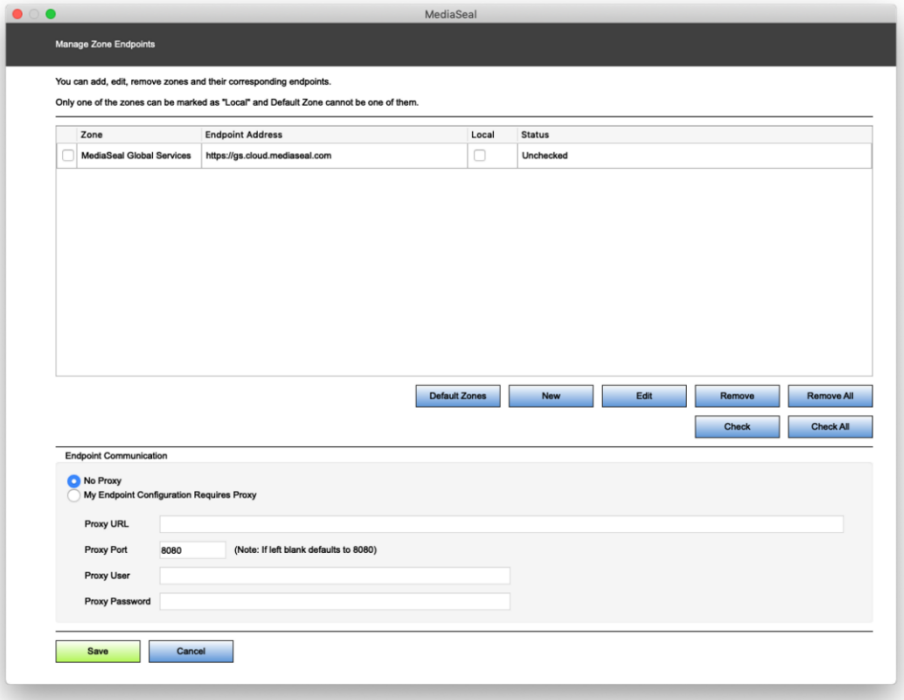
16.1 ZONE ENDPOINTS OVERVIEW

Zone Endpoints are the Studio Servers that the MediaSeal Encryptor Client communicates with.

By default, MediaSeal Encryptor client is set to communicate with the Default Zone "MediaSeal Global Services" (https://gs.cloud.mediaseal.com). This zone acts as a proxy and redirects communication to the correct Studio Server automatically.

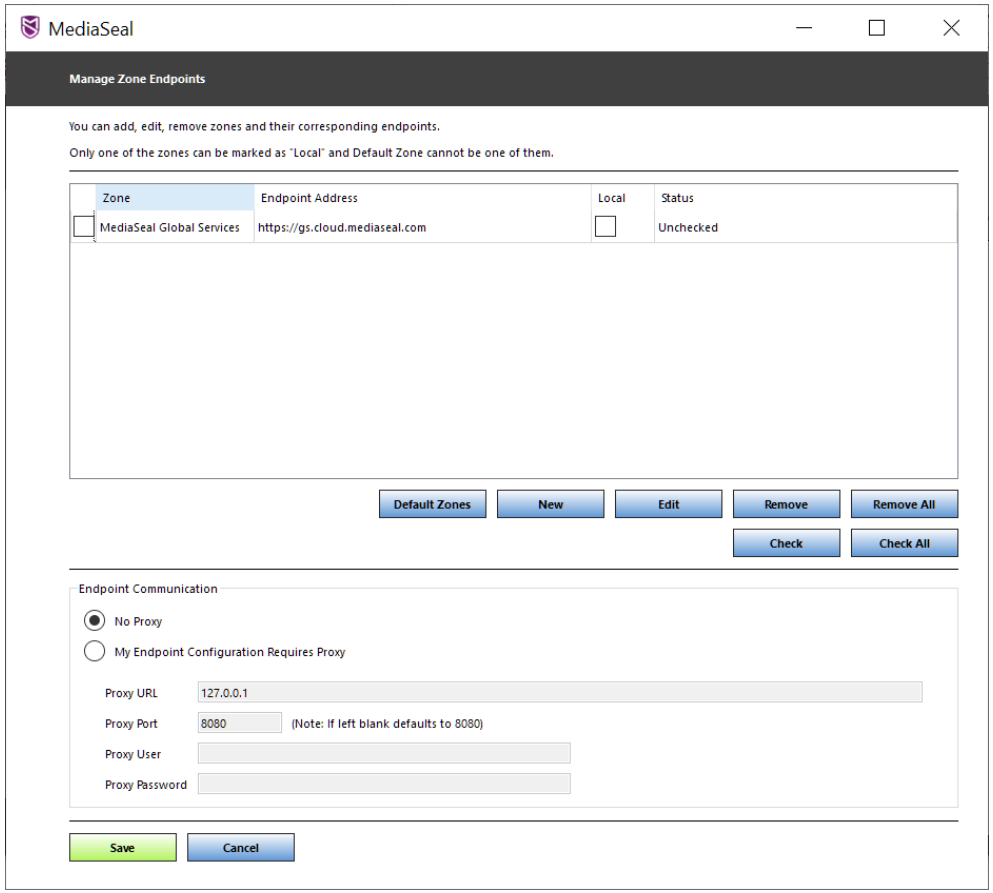
However, you may wish to configure connection directly to a Studio Server, in which case it is necessary to set a Zone Endpoint. You can configure multiple Zone Endpoints if connecting to multiple studios.

Within the Manage Zone Endpoints settings, you can also configure MediaSeal Encryptor Client to use a proxy for communication if required.



16.2 MANAGING ZONE ENDPOINTS

You can manage the Zone Endpoints that the MediaSeal Encryptor Client communicates with.



16.2.1 Local Endpoints

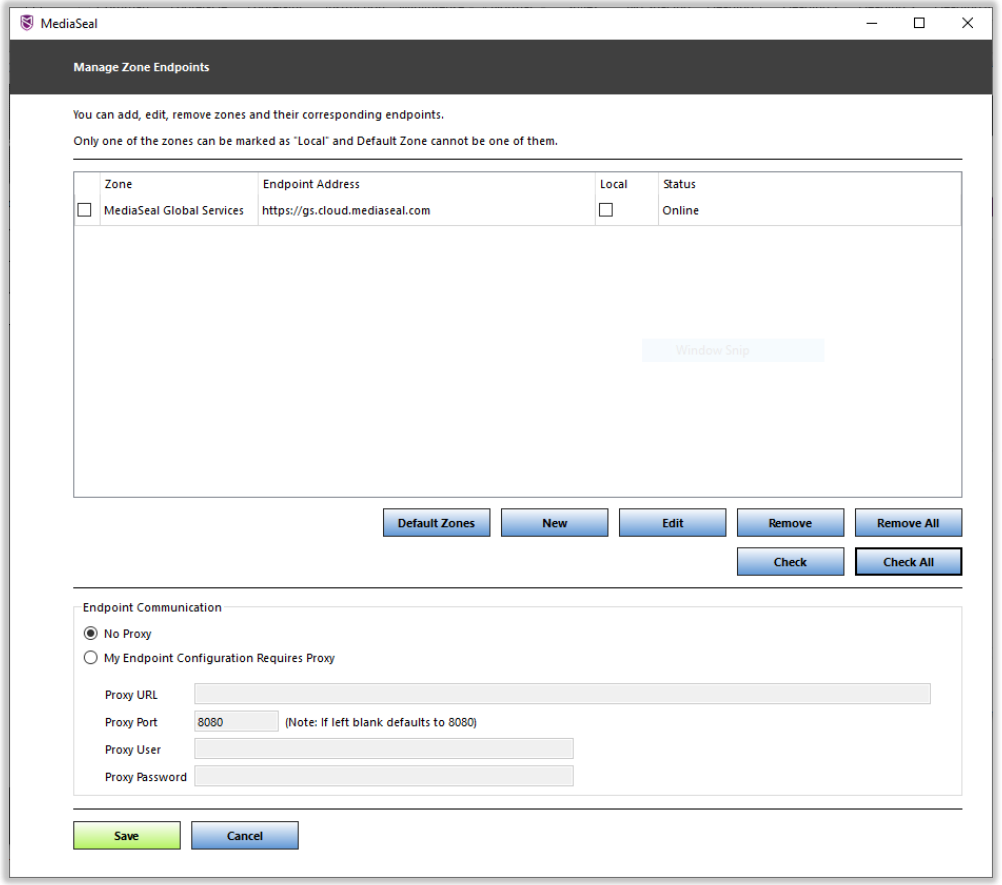
Endpoints can be marked as Local and should only be set when communicating directly with a studio server.

Only one of the zones can be marked local. The Default Zone (MediaSeal Global Services) cannot be marked Local.

16.2.2 Testing Zone Endpoints

You can check a Zone Endpoint status of one, multiple or all endpoints. The Decryptor will check that it can communicate correctly with endpoint.

- **Tick the checkbox** of the Zone you wish to check
- Click **Check**

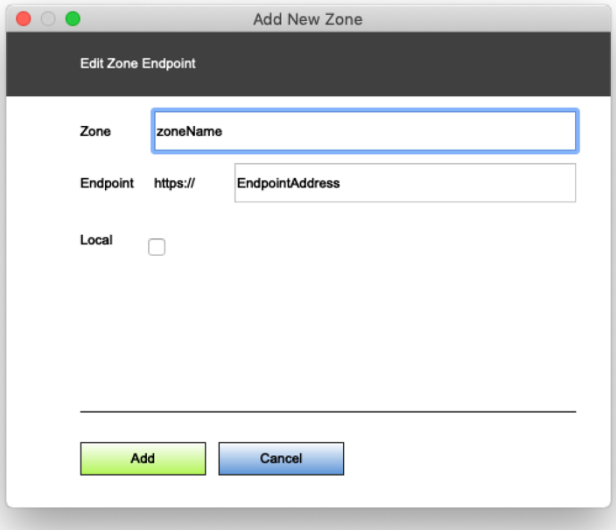


*When connection is successful, the Zone Status will be **Online***

16.2.3 Add New Zone Endpoint

You can add a new zone endpoint by setting a zone name and then the endpoint address by either: specifying a hostname; a fully qualified domain name; or an IP address.

- Click on **Settings** Tab
- Click on **Configuration** Tab
- Click **Manage zone endpoints**
- Click **New**
- Enter **Zone Name** in Zone
- Enter **Endpoint Address**
- Tick **Local** if required
- Click **Add**
- Click **Save**



16.2.4 Edit Zone Endpoint

You can edit any endpoint and modify the zone name, the hostname or fully qualified domain name or IP address as well as checking or unchecking the Local checkbox.

To edit the Zone Endpoint:

- Click on the **Zone** required
- Click **Edit**
- Amend Zone details as required
- Click **Change**

16.2.5 Restore Default Zone

You can quickly reset the zone endpoints back to default. Restoring the default zone endpoint will set the endpoint to MediaSeal Global Services **https://gs.cloud.mediaseal.com.** To set the default zone endpoint:

- Click **Default Zones**

16.2.6 Remove Zone

You can remove zone endpoints. To remove a zone endpoint:

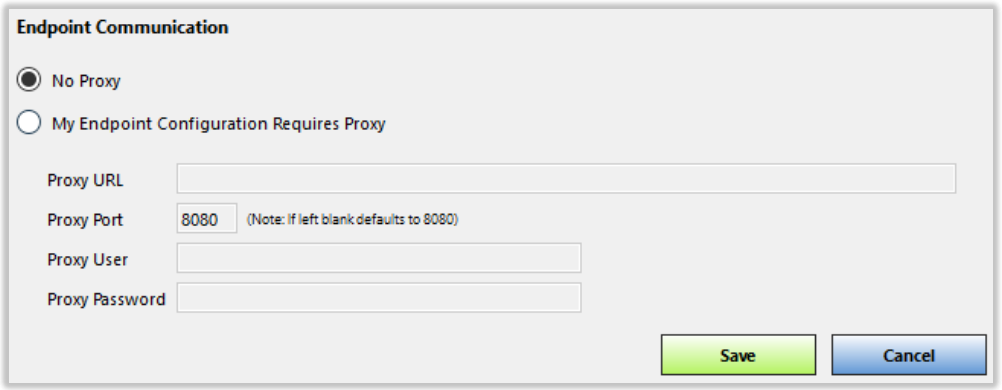
- Tick the **Zone Endpoint** to be removed
- Click **Remove Zone**

16.3 Setting Proxy Server

You can configure MediaSeal Encryptor Client to use a proxy server for communication with MediaSeal Global Services or your custom Zone Endpoint Address.

To configure the MediaSeal Encryptor Client to use a proxy server:

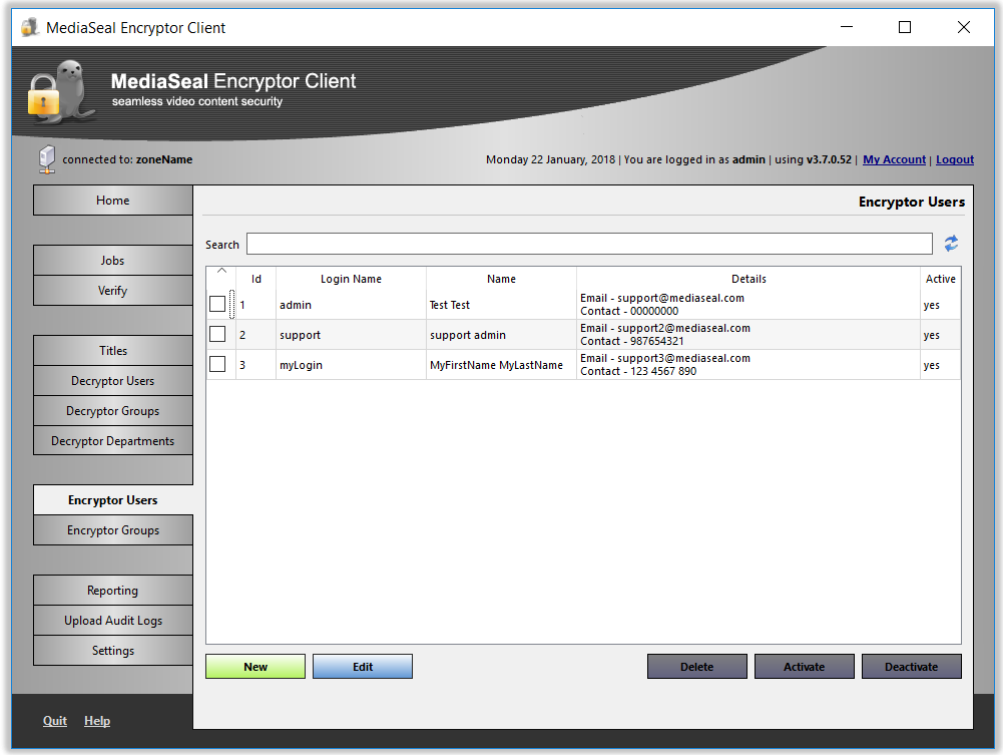
- Click on the **Settings** Tab
- Click **Manage Zone Endpoints**
- Set **Proxy URL**
- Set **Proxy Port** (optional)
- Set **Proxy User** (optional)
- Set **Proxy Password** (optional)
- Click **Save**



17 ENCRYPTOR USERS

17.1 MANAGING ENCRYPTOR USERS

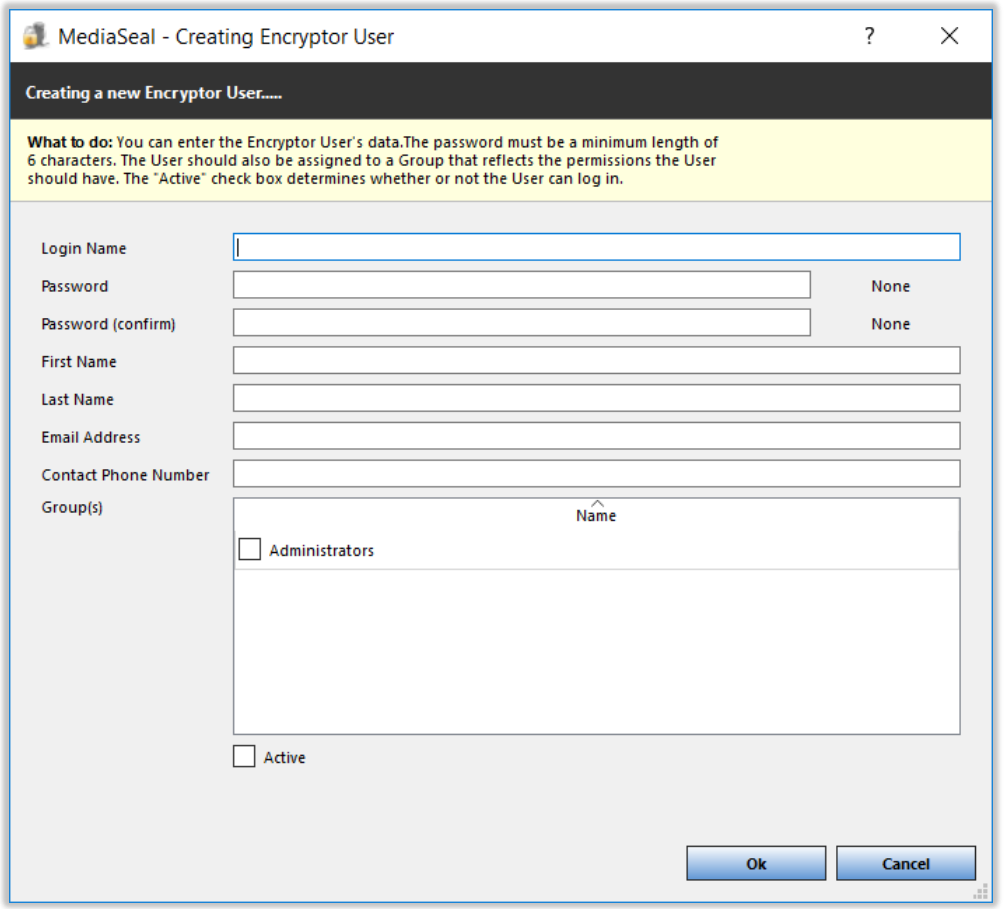
Encryptor Users are users allowed to login to the Studio Server using the MediaSeal Encryptor Client. You can manage these users via the Encryptor Users tab.



17.1.1 Create Encryptor User

To create a new Encryptor User:

- Click on **New**
- Enter the **required details**.
- Select **Groups** this account is a member of
- Tick **Active** to make account active
- Click **Ok**

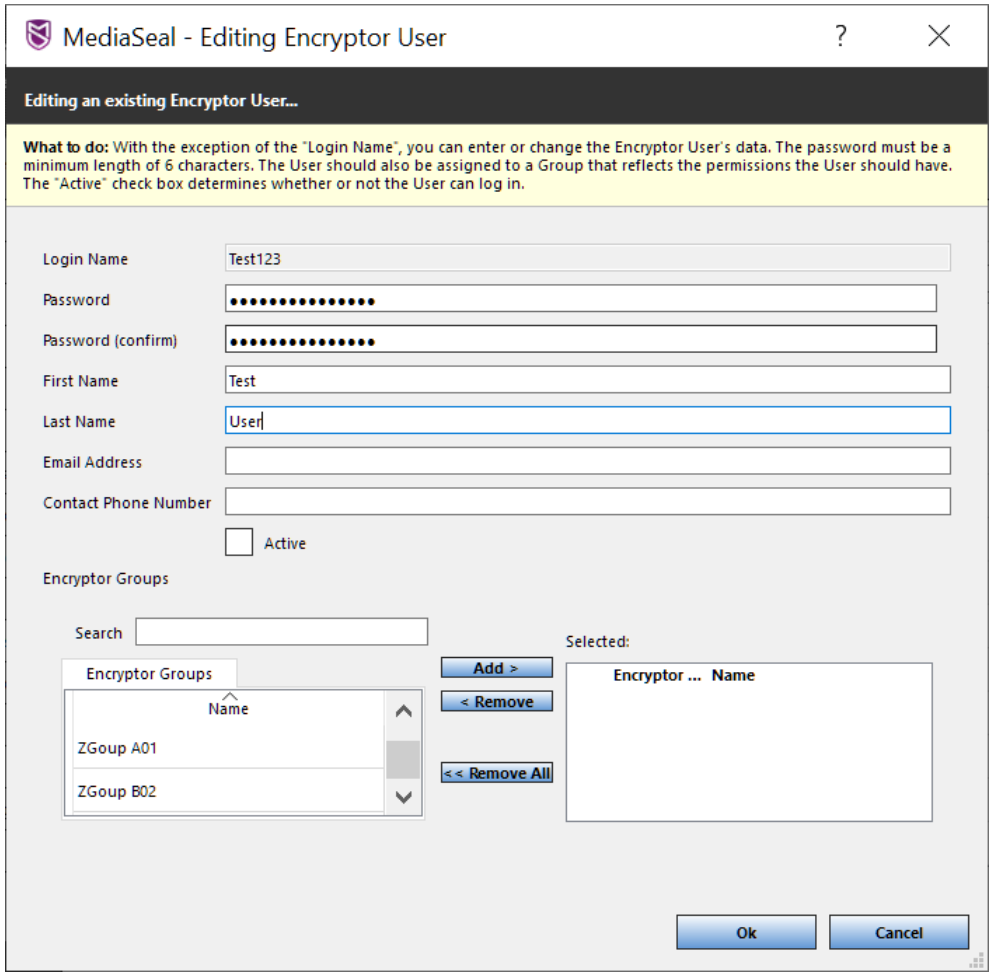


New accounts are not active by default, to make the account active click on the active checkbox.

17.1.2 Edit Encryptor User

To edit an Encryptor User:

- Click the **user account** in the list
- Click **Edit**
- Modify the **required fields**
- Click **Ok**



17.1.3 Delete Encryptor User

To delete an Encryptor User:

- Check the tick box of the **Encryptor User**
- Click **Delete**
- Click **Yes** to confirm deleting the account

17.1.4 Activate Encryptor User

To activate an Encryptor User:

- Check the tick box of the Encryptor User account to activate
- Click **Activate**

17.1.5 Deactivate Encryptor User

To deactivate an Encryptor User:

- Check the tick box of the Encryptor User account to deactivate
- Click **Deactivate**

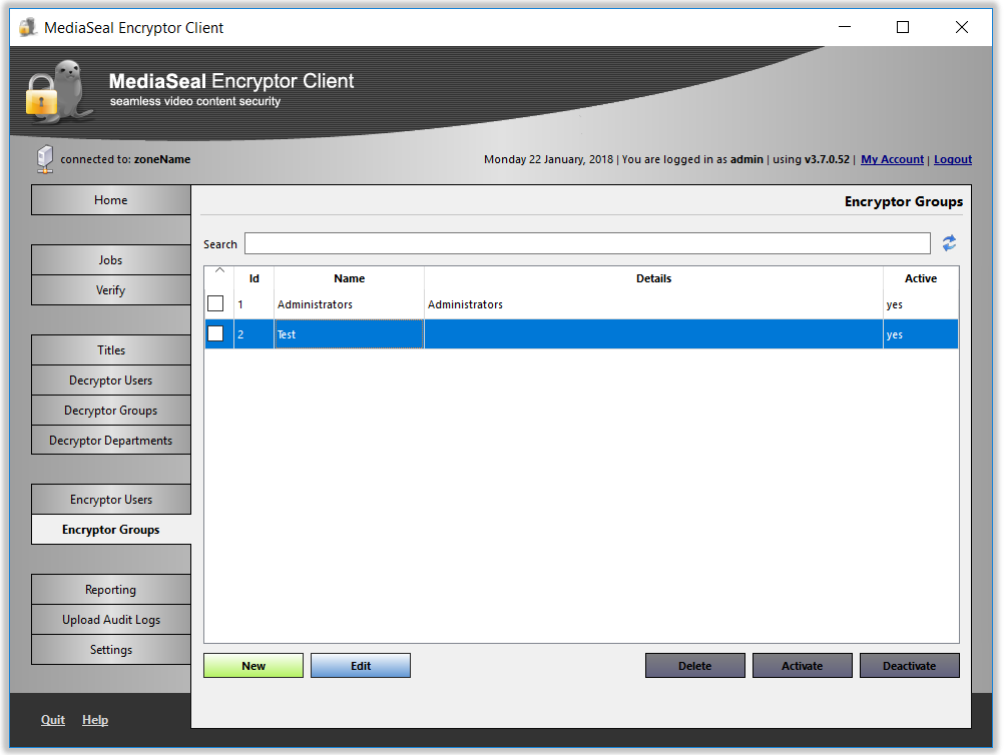
18 Encryptor Groups

18.1 Managing Encryptor Groups

Encryptor groups allow you to group together Encryptor User Accounts.

Within each group you can set application permissions and recipient permissions.

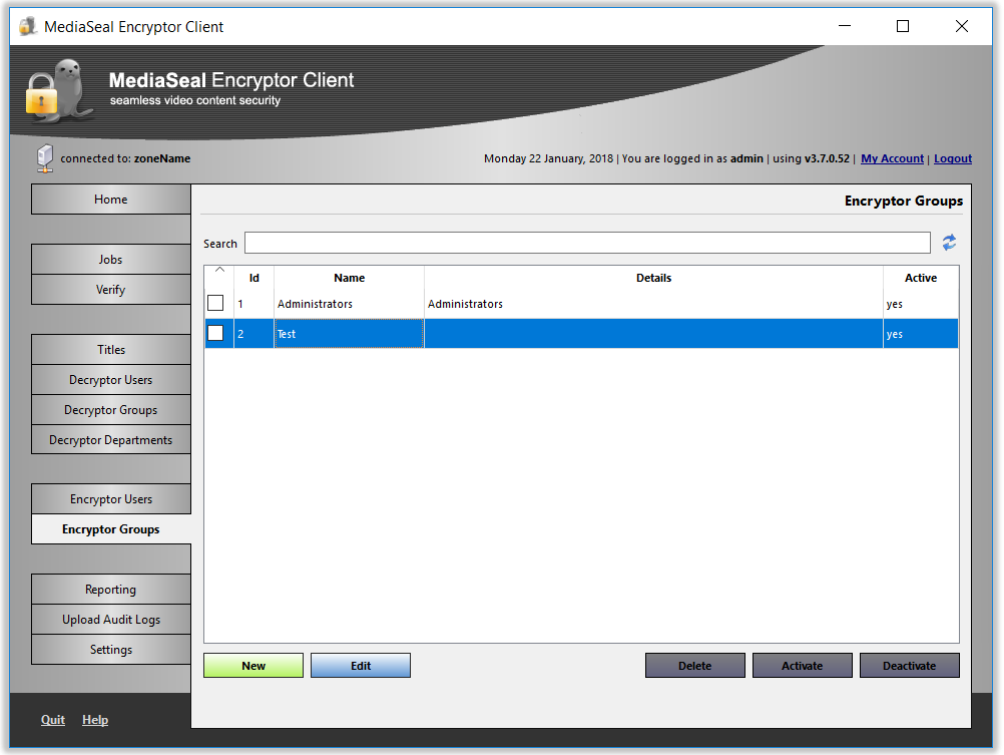
In addition, you can manage group memberships.



18.1.1 Create Encryptor Group

To create an Encryptor Group:

- Click on **New**
- Enter **Name**
- Enter **Description**.
- Tick **Active** to make account active
- Click **Ok**

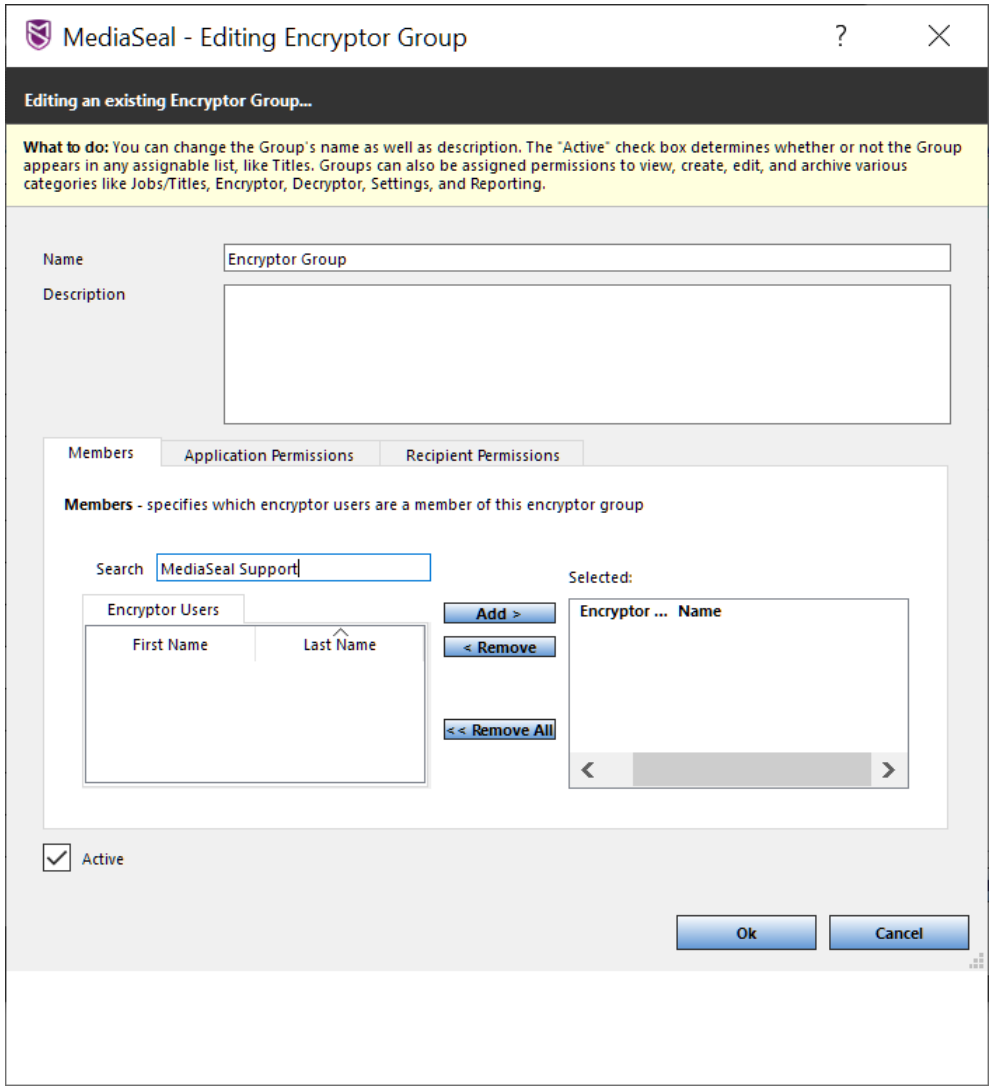


New groups accounts are not active by default, to make the account active click on the active checkbox

18.1.2 Edit Encryptor Group

To edit an Encryptor Group:

- Click the **group** in the list
- Click **Edit**
- Modify the **required fields**.
- Click **Ok**



18.1.3 Delete Encryptor Group

To delete an Encryptor Group:

- Check the tick box of the **Encryptor Group**
- Click **Delete**
- Click **Yes** to confirm deleting the Group

18.1.4 Activate Encryptor Group

To activate an Encryptor Group:

- Check the tick box of the **Encryptor group**
- Click **Activate**

18.1.5 Deactivate Encryptor Group

To deactivate an Encryptor Group:

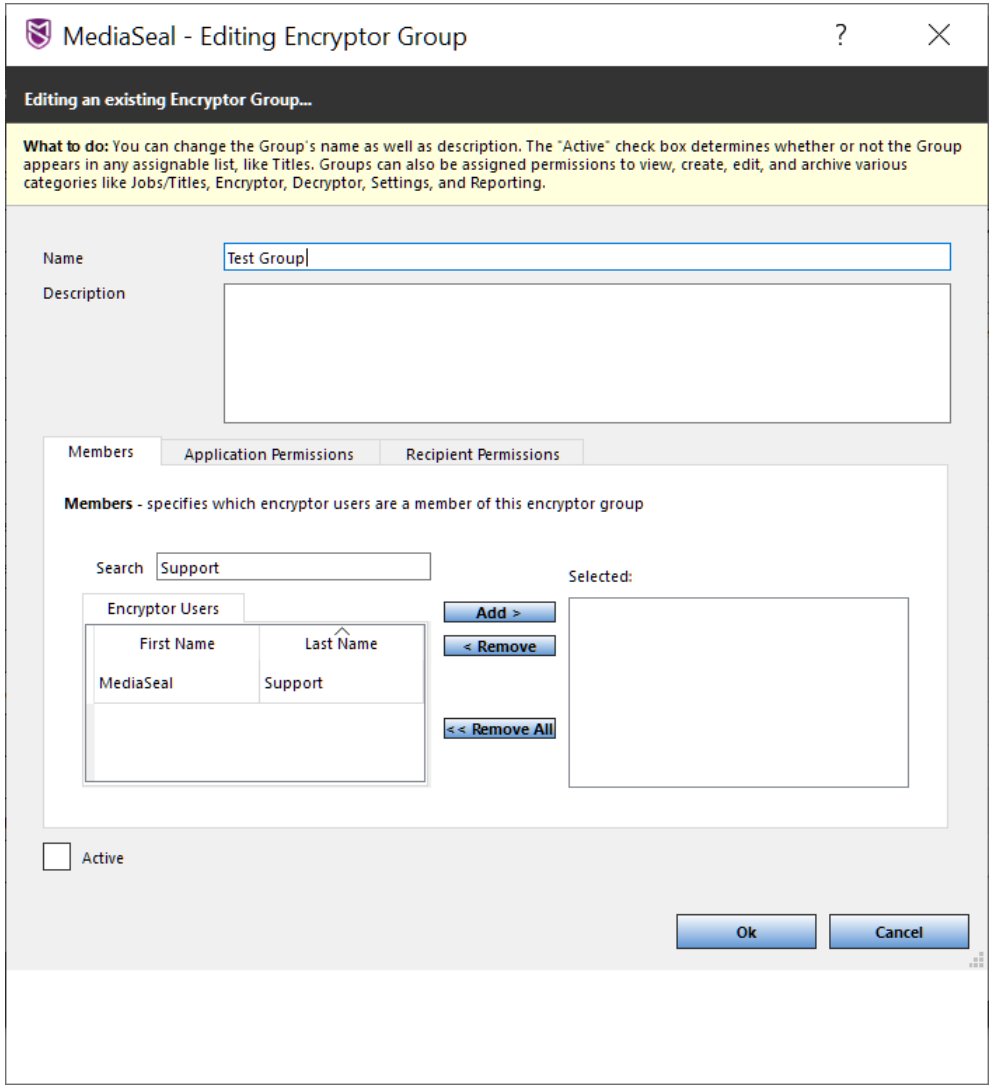
- Check the tick box of the **Encryptor Group**
- Click **Deactivate**

18.1.6 Manage Encryptor Group Memberships

To manage an Encryptor Group:

To edit the Encryptor group:

- Click the **group** in the list
- Click **Edit**
- Click the **Members** Tab
- Tick the Members you wish to **add**
- Untick the Members you wish to **remove**
- Click **Ok**



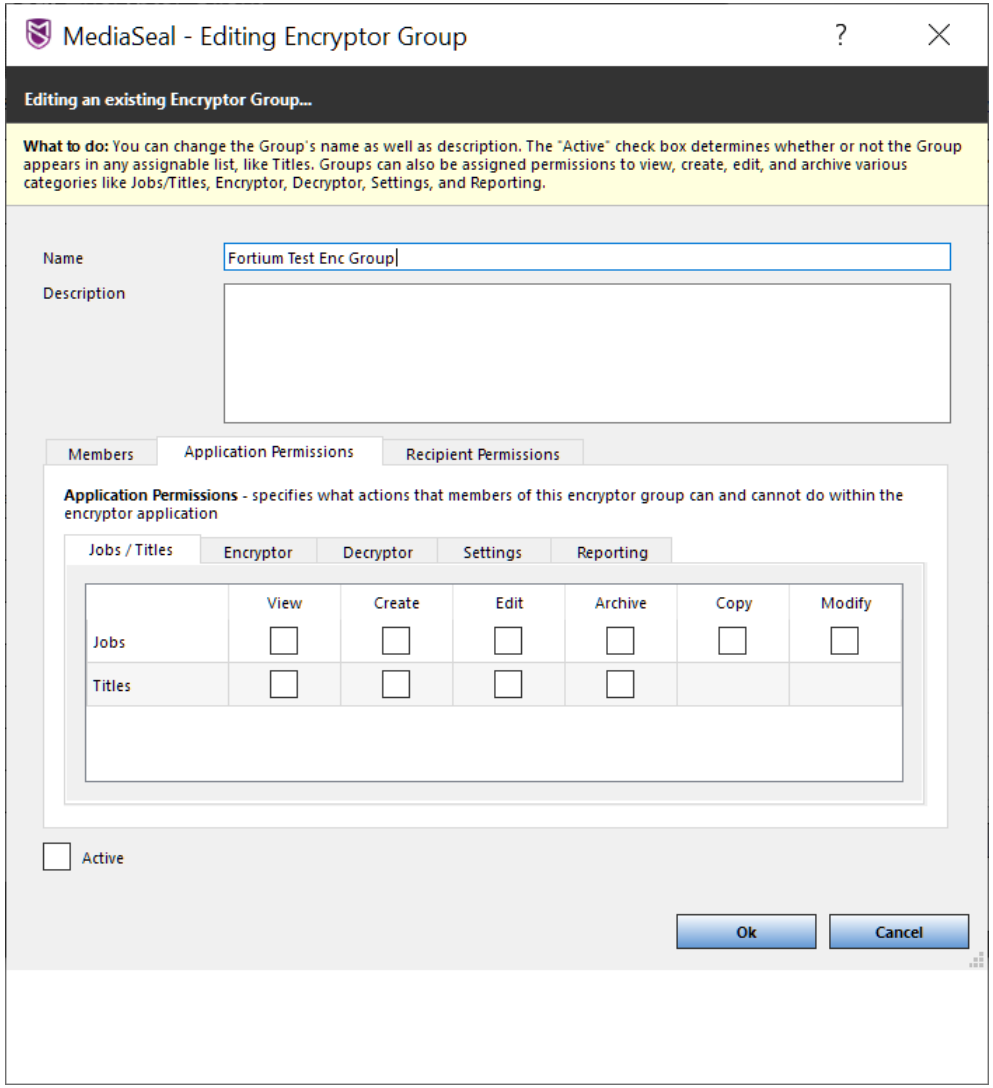
18.2 Set Application Permissions

If you wish to restrict what actions members of the Encryptor Group can and cannot do within the MediaSeal Encryptor Client, you will need to set Application Permissions.

Please see the **Permission Controls** section for a listing of application permission controls.

To set Application Permissions:

- Click the **group** in the list
- Click **Edit**
- Click the **Application Permissions Tab**
- Select the relevant **Tab**



18.2.1 Allow Permission:

To allow the required permission:

- **Tick** the relevant permission

18.2.2 Deny Permission:

To remove / deny the required permission:

- **Untick** the relevant permission

By default, new Encryptor Groups have no permission set. Permission must be explicitly set using Application Permissions.

18.2.3 Permission Controls

Permissions can be set to control access to each of the components.

Jobs / Titles	**Function**	**Permission**	**Description**
	Jobs	View	View Jobs
	Jobs	Create	Create Jobs
	Jobs	Edit	Edit Jobs
	Jobs	Archive	Archive Jobs
	Jobs	Copy	Duplicate Jobs
	Jobs	Modify	Modify Existing Jobs
	Titles	View	View Titles
	Titles	Create	Create Titles
	Titles	Edit	Edit Titles
	Titles	Archive	Archive Titles

Encryptor	**Function**	**Permission**	**Description**
	Encryptor Users	View	View Encryptor Users
	Encryptor Users	Create	Create Encryptor Users
	Encryptor Users	Edit	Edit Encryptor Users
	Encryptor Users	Activate	Activate Encryptor Users
	Encryptor Groups	Create	Create Encryptor Groups
	Encryptor Groups	Modify	Modify Encryptor Groups
	Encryptor Groups	View	View Encryptor Groups
	Encryptor Groups	Activate	Activate Encryptor Groups
Decryptor	Function	Permission	Description
	Decryptor Users	View	View Decryptor Users

	Decryptor Users	Create	Add Decryptor Users
	Decryptor Users	Edit	Edit Decryptor Users
	Decryptor Groups	View	View Decryptor Groups
	Decryptor Groups	Create	Create Decryptor Groups
	Decryptor Groups	Edit	Edit Decryptor Groups
	Decryptor Departments	View	View Decryptor Departments
	Decryptor Departments	Create	Create Decryptor Departments
	Decryptor Departments	Edit	Edit Decryptor Departments

Settings	**Function**	**Permission**	**Description**
	Local Settings	Edit	Edit Local Settings
	Global Settings	Edit	Edit Global Settings
	Personal Details	Edit	Edit Personal Details

Reporting	**Function**	**Permission**	**Description**
	Reporting	View	View Audit Reports
	Reporting	Export	Export Audit Reports

18.3 Set Recipient Permissions

If you wish to restrict which Decryptor Users, Groups or Departments the Encryptor Group can protect content for, you will need to set Recipient Permissions.

To set Recipient Permissions:

- Click the group in the list, so the **group** is highlighted
- Click **Edit**
- Click the **Recipient Permissions Tab**
- Click the Users, Groups or Departments **Tab** for Recipient permission you wish to set

18.3.1 Add a User / Group / Department:

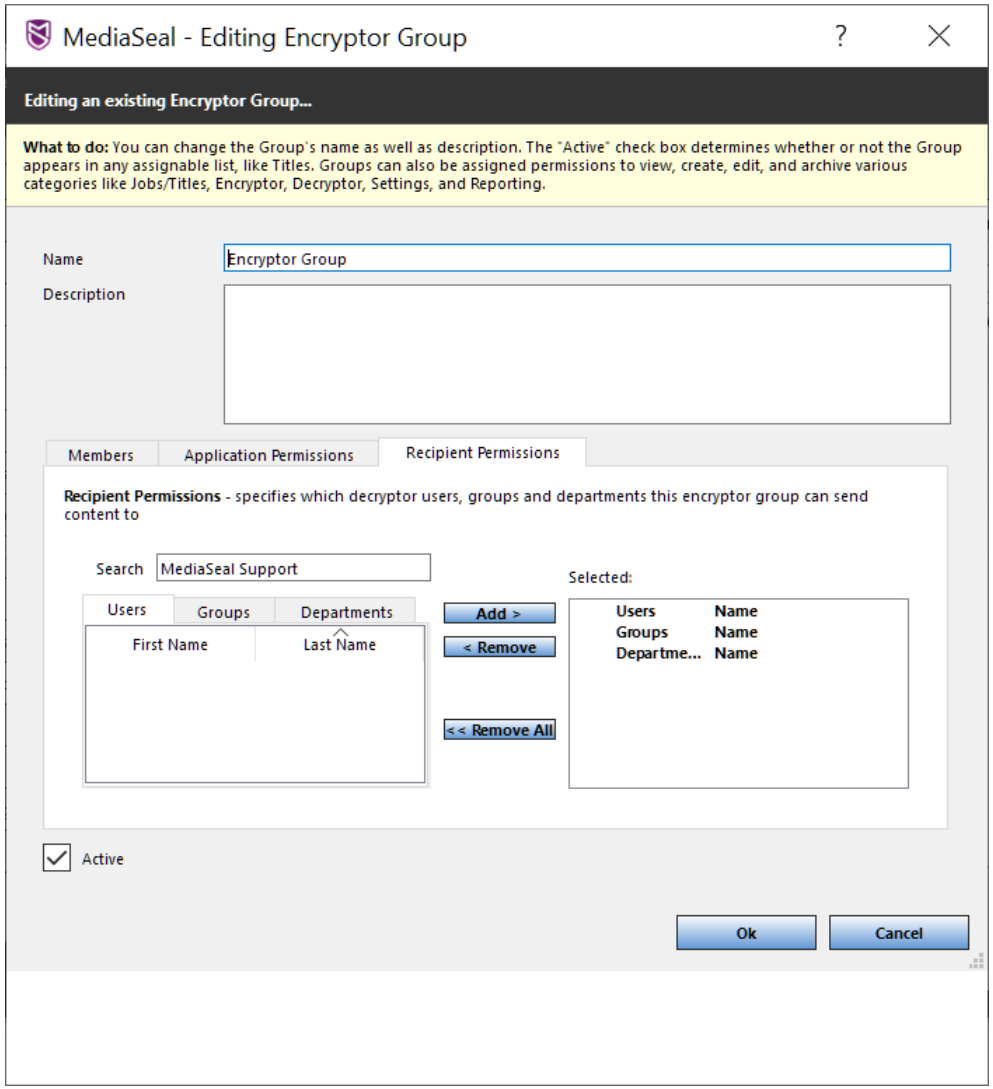
- Click the **Name of the Recipient** you wish to add in the left column
- Click **Add**

18.3.2 To Remove a User / Group / Department:

- Click the **Name of the Recipient** you wish to remove in the right column and
- Click **Remove**

18.3.3 To Remove All Users / Groups / Departments:

- Click **Remove All**
- Click **OK**



19 DECRYPTOR USERS

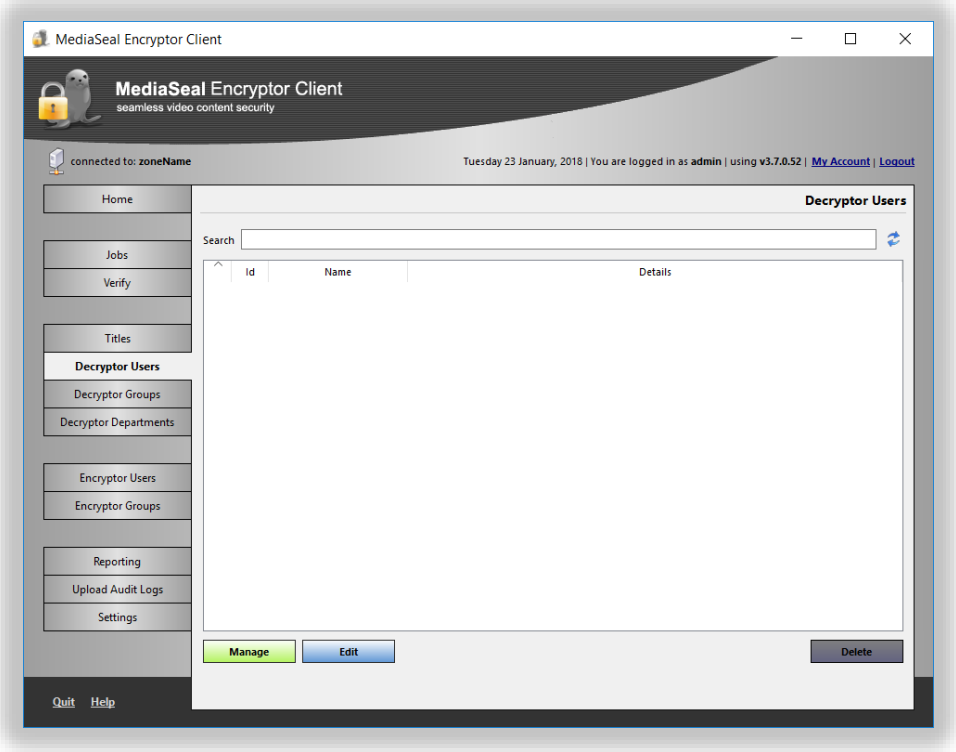
A MediaSeal Account is needed for users that require access to Multi-Factor Authenticated files. In order protect content for a specific user with MFA, it is necessary to import that person into your Studio Server via MediaSeal Encryptor Client.

19.1 MANAGE DECRYPTOR USERS

You can manage which Decryptor Users you would like to be imported to your Studio Server by using the Manage button.

To manage users:

- Click on the **Decryptor Users** Section
- Click **Manage**
- In the Search box, type the **first or last name** of the Decryptor User you would like to manage



19.1.1 To Add a Decryptor User:

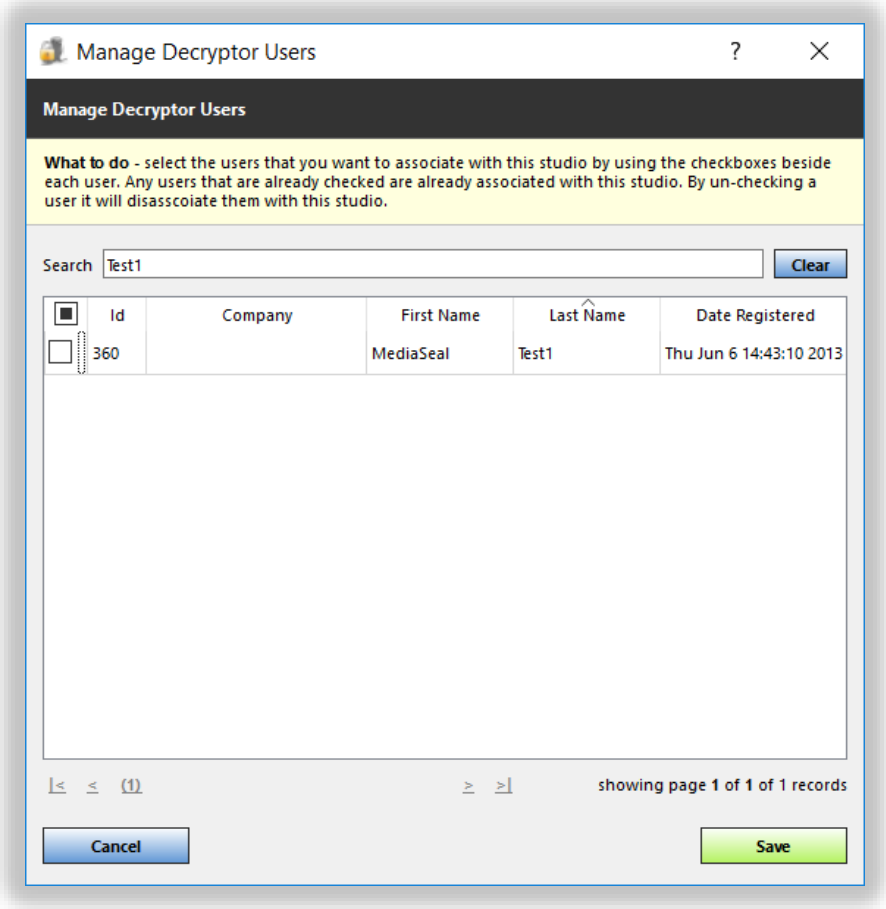
To add a Decryptor user:

- Tick the **Decryptor User**
- Click **Save**

19.1.2 To Remove a Decryptor User

To remove a Decryptor user:

- Untick the **Decryptor User**
- Click **Save**



19.1.3 Delete a Decryptor User from your Studio

To delete a Decryptor user:

- Click on the **Decryptor Users** Section
- Select the **Decryptor User** to remove
- Click **Delete** button

19.1.4 Activate a Decryptor User on your Studio

To activate a Decryptor user:

- Click on the **Decryptor** Users Section
- Click the **Decryptor User**
- Click **Edit** button
- Tick the **Active checkbox**

19.1.5 Deactivate Decryptor Users from your Studio

To deactivate a Decryptor user:

- Click on the **Decryptor Users** Section
- Click the **Decryptor User**
- Click **Edit** button
- Untick the **Active** checkbox

19.1.6 Clear the search field and retrieve all users

To clear the search field:

- Click the **Clear** button

20 DECRYPTOR GROUPS

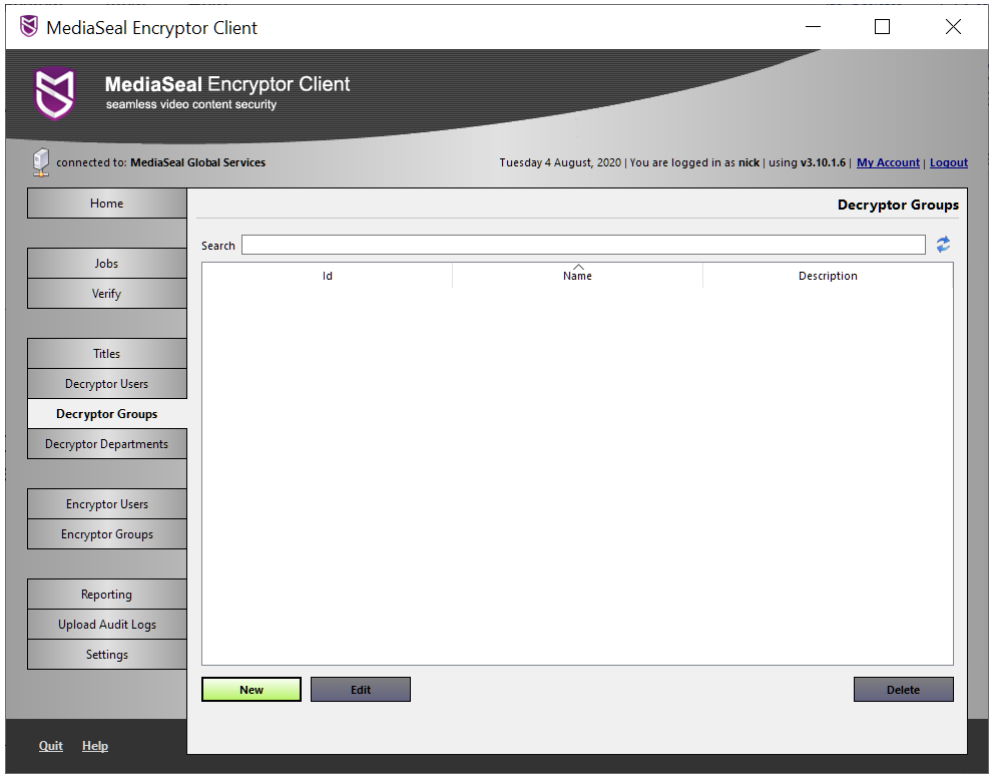
20.1 MANAGE DECRYPTOR GROUPS

You can group Decryptor users into a Decryptor Group. This allows you to protect content using a group rather than managing content on a per user basis. It also enables for easier management, like granting file access or revoking permissions when using Server authentication.

20.1.1 Create Decryptor Group

To create a new Decryptor Group:

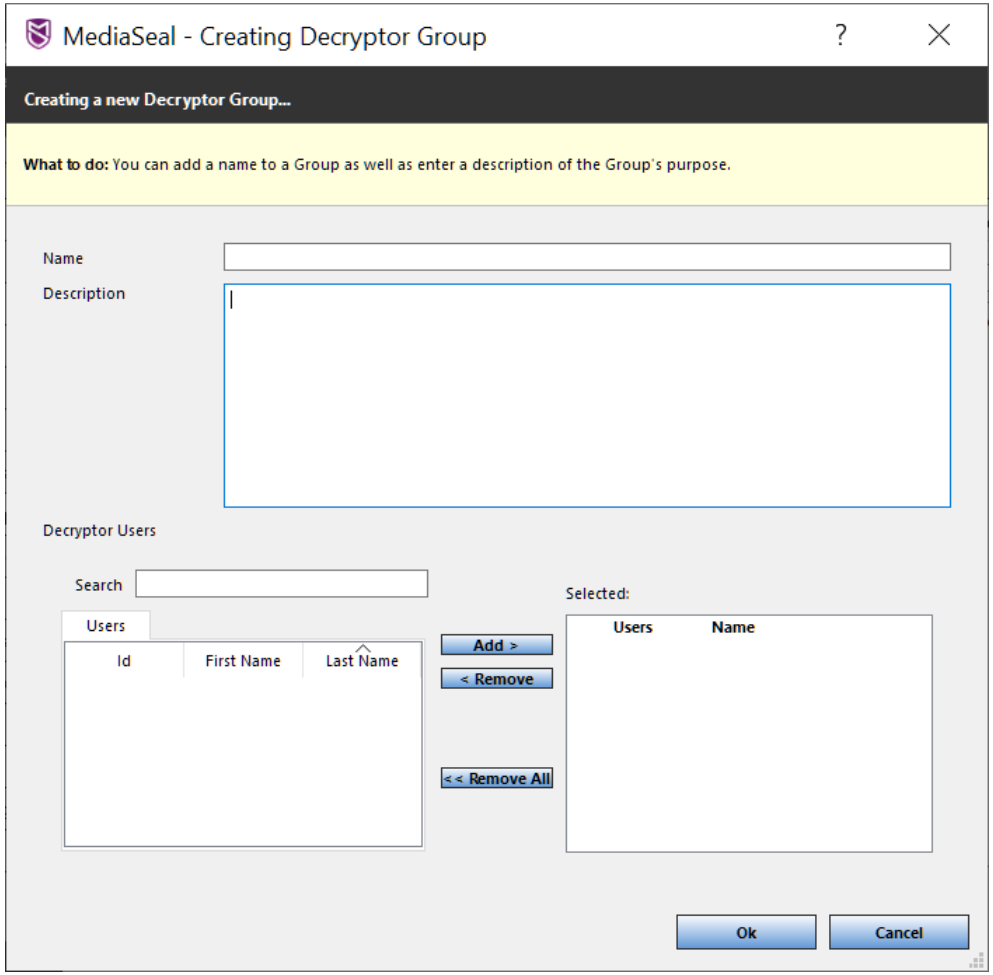
- Click on the **Decryptor Groups** section
- Click **New**
- Enter a **Name** and **Description**
- Click **OK**



20.1.2 Edit Decryptor Group

To edit a Decryptor Group:

- Click the **group** in the list, so the group is highlighted
- Click **Edit**
- Modify the **required fields**
- Click **Ok**



20.1.3 Manage Members of a Decryptor Group

To add members to a Decryptor Group:

- Click the **group** in the list, so the group is highlighted.
- Click **Edit**
- Tick the **Decryptor Users** you wish to Add
- Untick the **Decryptor Users** you wish to Remove
- Click **Ok**

21 DECRYPTOR DEPARTMENTS

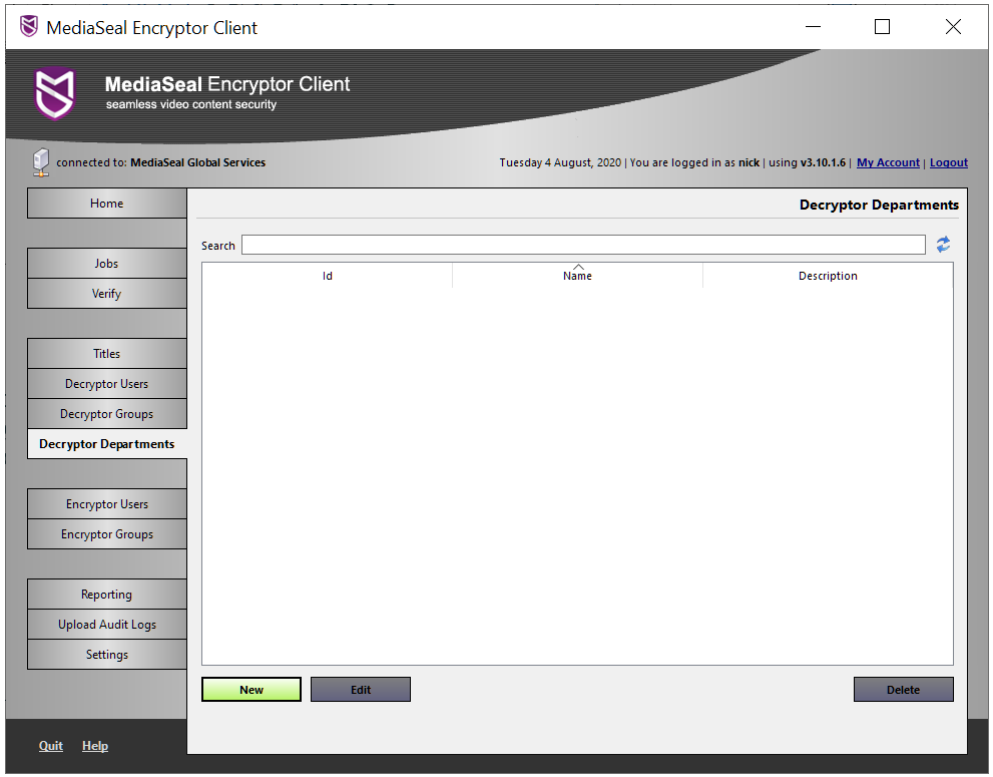
21.1 MANAGE DECRYPTOR DEPARTMENTS

You can group Decryptor users in a Decryptor Department. This allows you to protect content using a department rather than managing content on a per user or per group basis. It also enables for easier management, like granting file access or revoking permissions when using Server authentication.

21.1.1 Create Decryptor Department

To create a new Decryptor Department:

- Click on the **Decryptor Departments** section
- Click **New**
- Enter a **Name** and **Description**
- Click **Ok**



21.1.2 Edit Decryptor Department

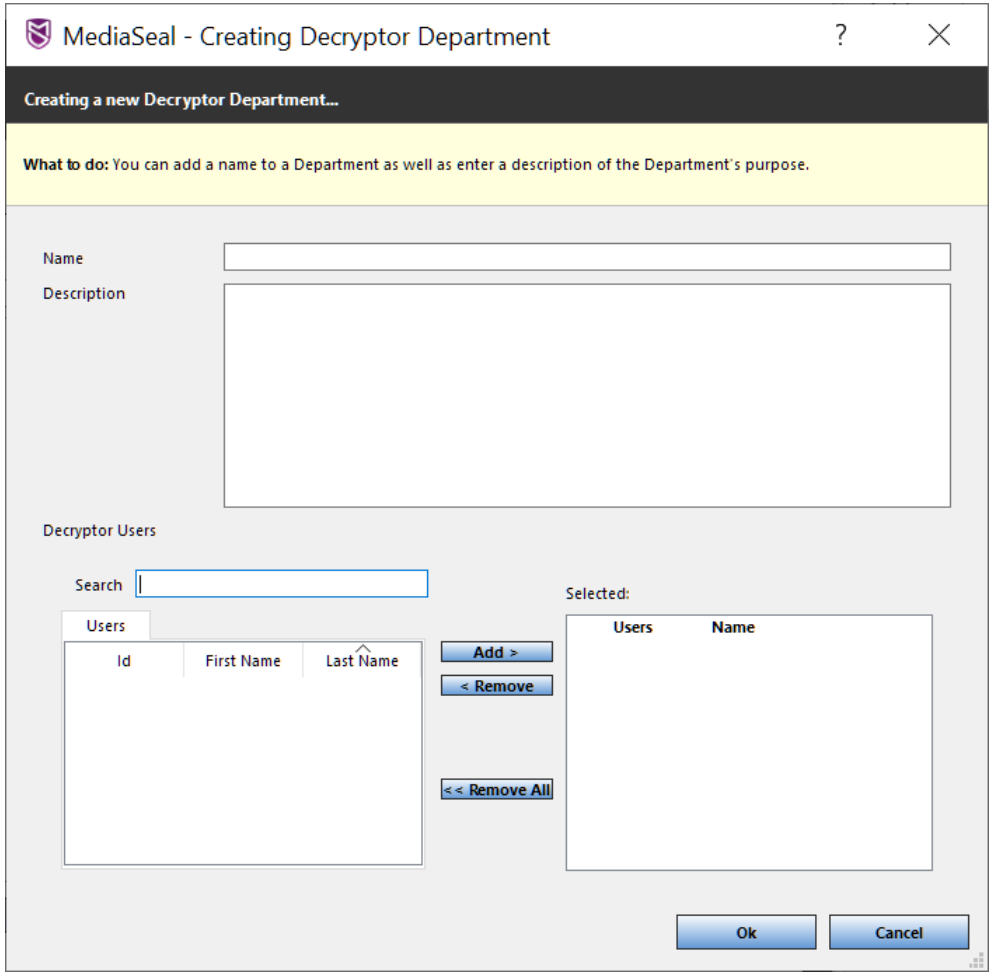
To edit a Decryptor Department:

- Click the **Department** in the list
- Click **Edit**
- Modify the **required fields**
- Click **Ok**

21.1.3 Manage Members of a Decryptor Department

To add members to a Decryptor Department:

- Click the **Department** in the list, Click **Edit**
- Select the **Decryptor Users** you wish to Add
- Untick the **Decryptor Users** you wish to Remove
- Click **Ok**



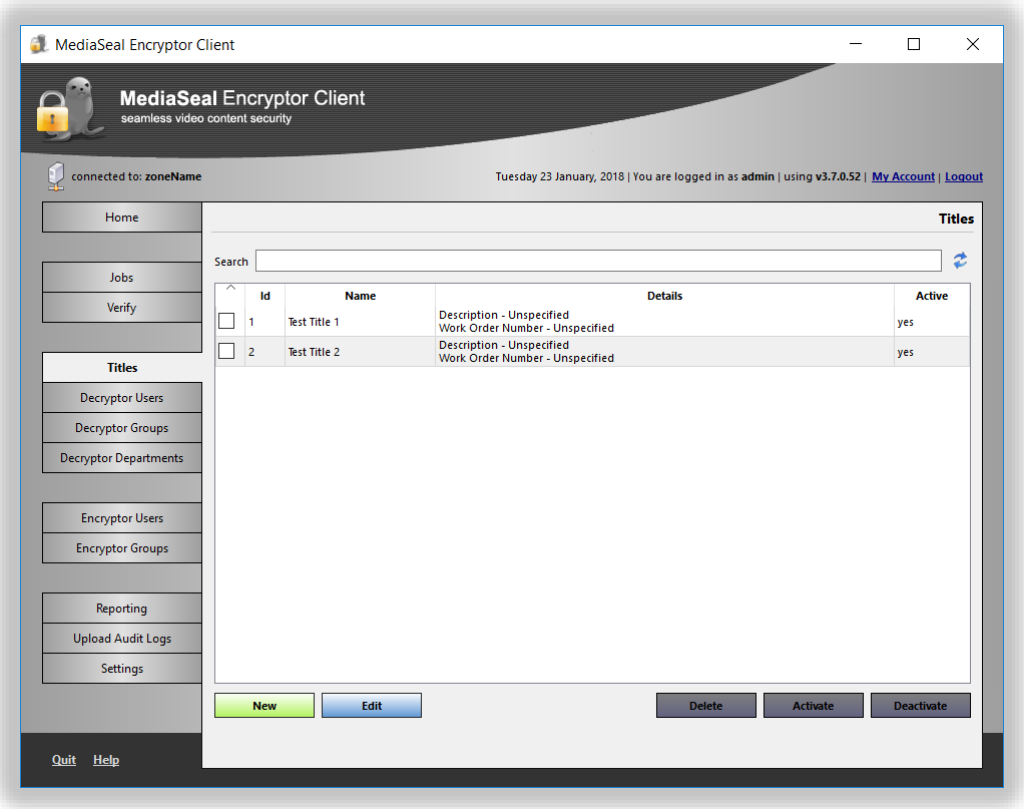
22 TITLES

22.1 MANAGE TITLES

Titles is a mechanism to allow you to group a collection of jobs, e.g. a new project or title.

It requires setting permissions for Encryptor Users and/or Encryptor Groups.

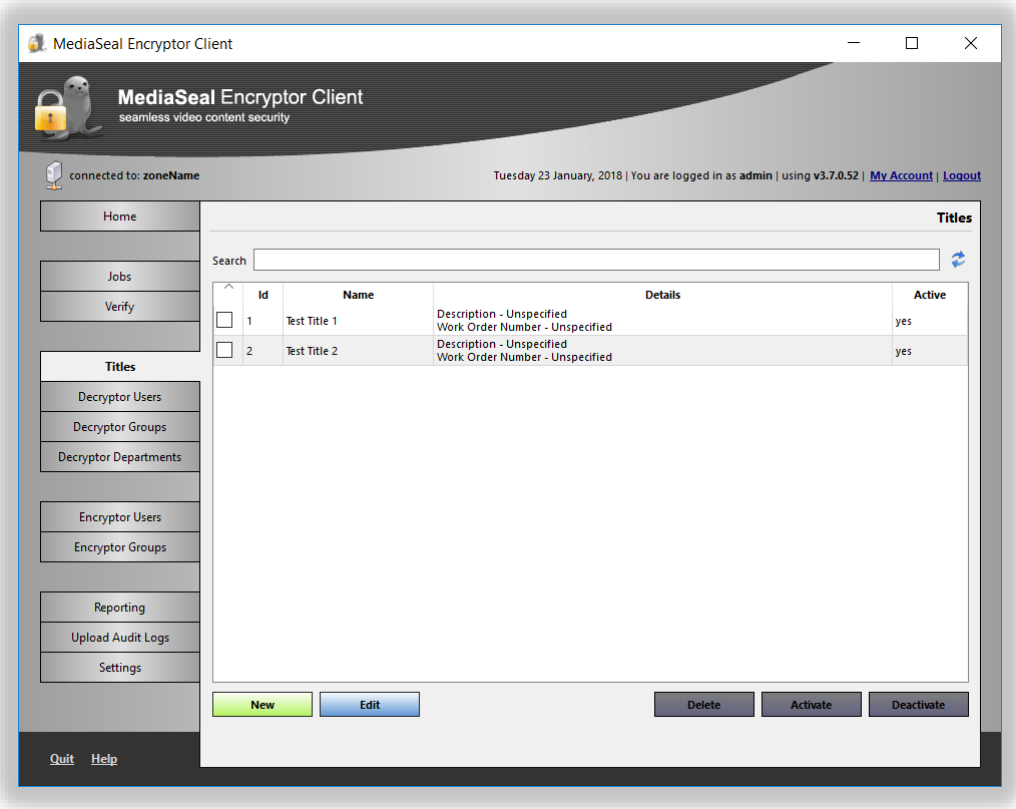
This restricts which Encryptor Users or Encryptor Groups can use Jobs associated with a title.



22.1.1 Create Title

To create a Title:

- Click on the **Titles** Section
- Click on **New**
- Enter **Name and Description**
- Click **Ok**

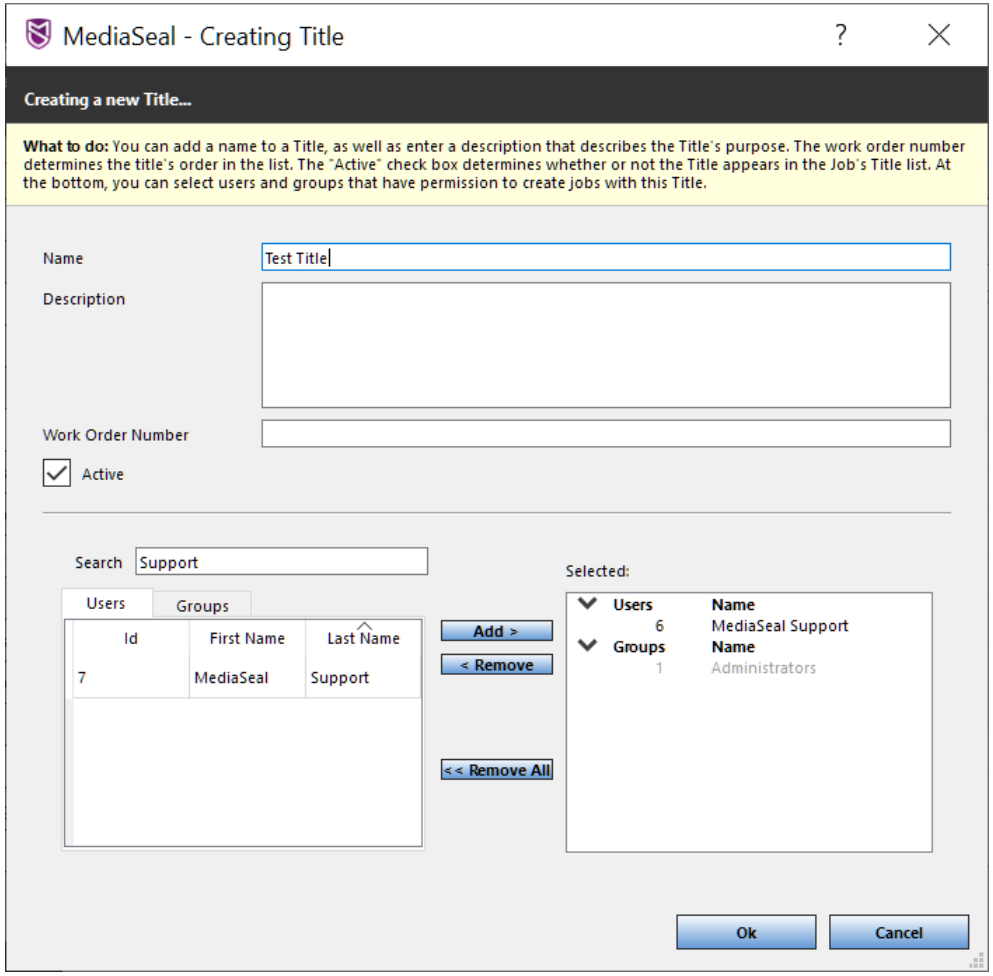


*By default, new titles are Active. You can deactivate the new title by unticking the active checkbox. Alternatively see the **Deactivate Title** section*

22.1.2 Edit Title

To edit a Title:

- Click the **Title** in the list
- Click **Edit**
- Modify the **required fields**
- Click **Ok**



22.1.3 Delete Title

To delete a Title:

- Check the tick box of the **Title** to delete
- Click **Delete**
- Click **Yes** to confirm deleting the Group

22.1.4 Activate Title

To activate a Title:

- Check the checkbox of the **Title** to Activate
- Click **Activate**
- Click **Yes** to confirm activating the Title

22.1.5 Deactivate Title

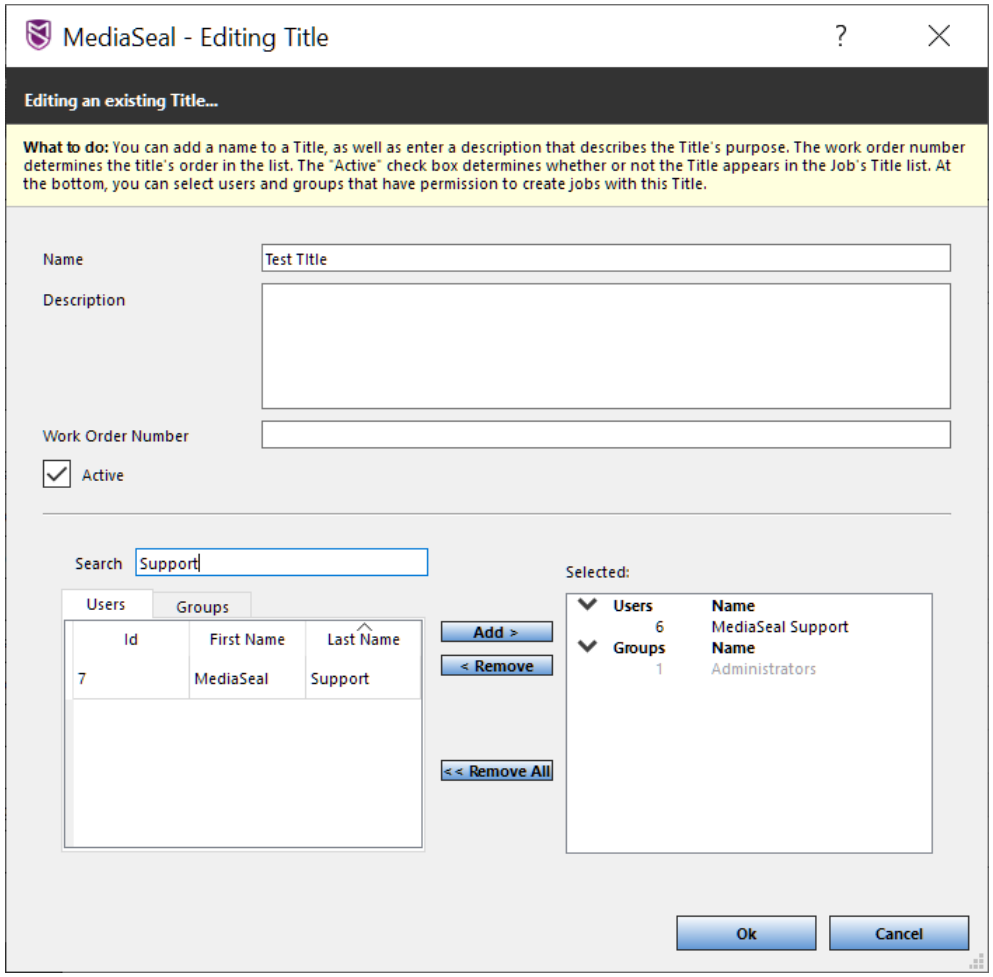
To deactivate a Title:

- Check the checkbox of the **Title** to deactivate
- Click **Deactivate**
- Click **Yes** to confirm deactivating the Title

22.1.6 Manage Title Permissions

To set Encryptor Users or Groups with permission to use jobs for the title:

- Click the **Title** in the list
- Click **Edit**



22.1.6.1 Add User or Group

To add a user or group:

- Select the **Users** or **Groups** Tab
- Click on the **Name** of the User or **Group** in the left column
- Click **Add**

22.1.6.2 To Remove User or Group

To remove a user or group:

- Select the **Users** or **Groups** Tab
- Click on the **Name** of the User or **Group** in the right column
- Click **Remove**
- Click **OK**

22.1.6.3 Remove All Users

To remove all users:

- Click **Remove All**
- Click **OK**

23 JOBS

23.1 JOBS OVERVIEW

The Jobs section contains 3 tabs: Jobs, Templates and Archived Jobs. Jobs is where the activity of protecting content is undertaken. Templates is where templates can be managed. Jobs can be created from any template that you create. Archive Jobs is where you store jobs that are no longer needed.

23.2 SEARCH

You can search for specific jobs, templates, or archived jobs in the relevant tab by using the search facility.

To search:

- Type the **search term** in the search box

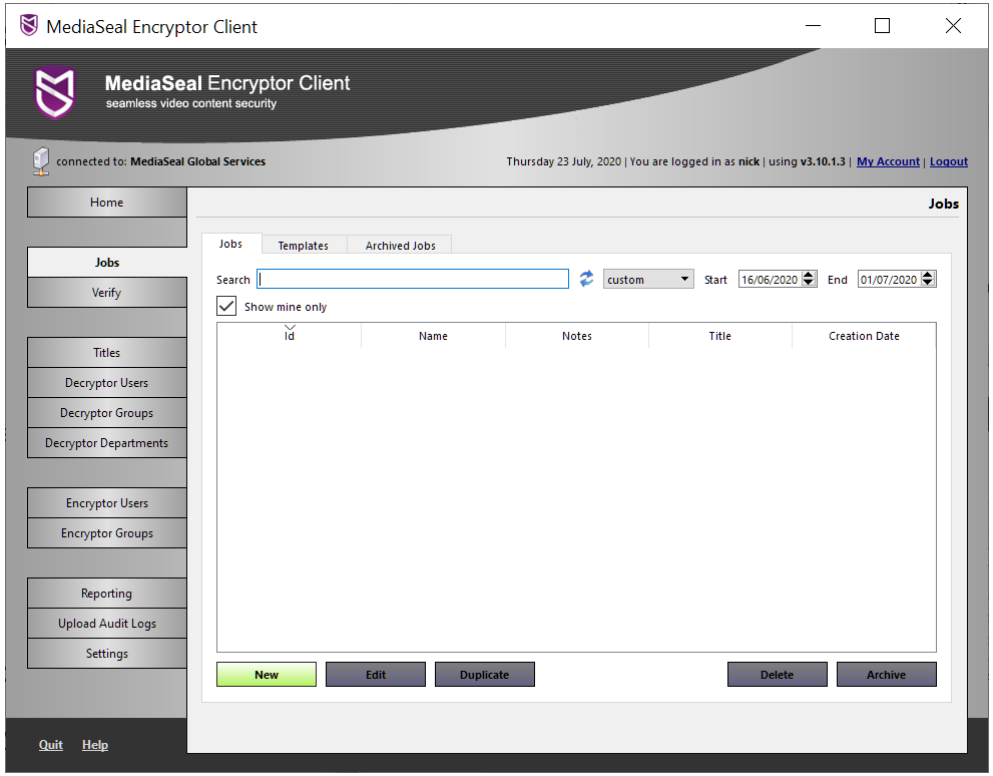
23.2.1 Search Filters

You can filter searches for Jobs, Templates and Archive Jobs by date and owner by using filters. You can use the drop-down list to select a date range of **week**, **month**, **year**, **all time** or **custom**.

When using **custom,** you can manually set the start and end dates as required.

You can also limit the views to only Jobs, Templates or Archive Jobs that have been created by you.

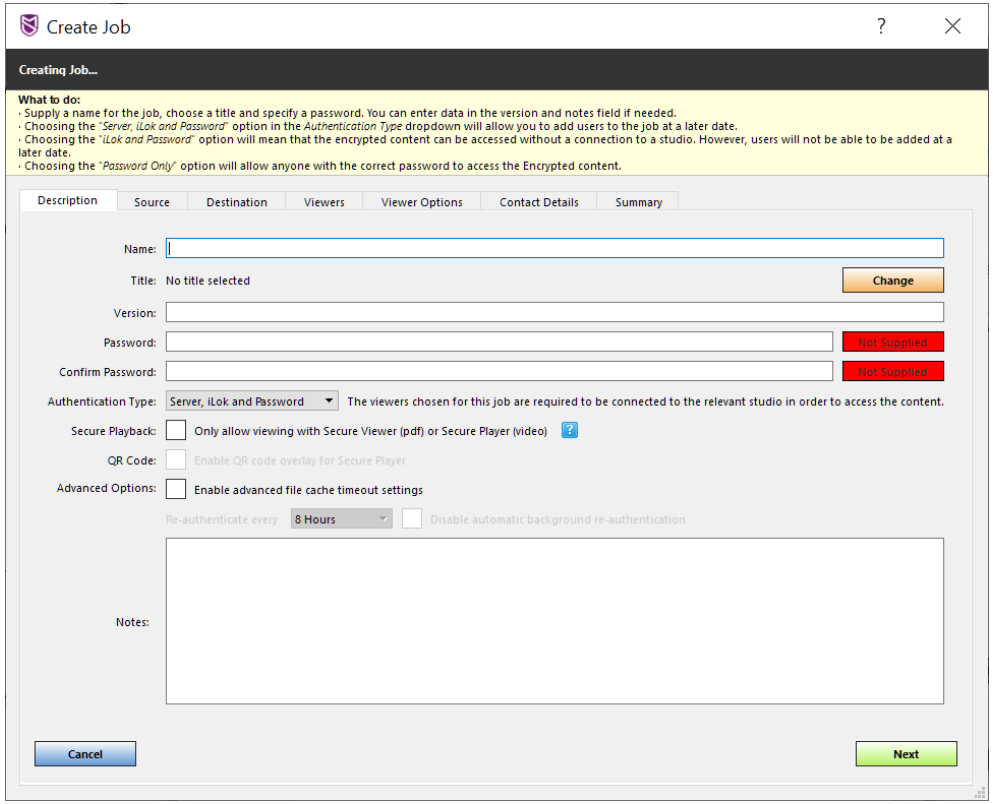
To do this, use the **Show My Jobs Only, Show My Templates Only** or **Show My Archive Jobs** checkboxes, respectively.



23.3 Create Job

23.3.1 To create a new Job:

- Click the **Jobs** section
- Click **New**
- In the Description Tab enter the **required details**
- Click **Next**



Description	**Field**	**Description**
	Name:	Name of the Job
	Title	The Title this job belongs to
	Version	The version of the Job
	Password	The default password used to open the content
	Verify Password	Verification of the default password used to open the content
	Authentication Type	The content authentication type to be used
	Secure Playback	Restrict Access to MediaSeal Secure Player (Video) or Secure Viewer (PDF) Application
	QR Code	Enable QR code overlay for Secure Player
	Advanced Options	Enable Advanced file cache timeout
		• Re-Authenticate every [x] hours
		• Disable automatic background authentication
	Notes	Any notes for this job

The passwords you set must match and meet the password complexity as defined in the Security Setting section.

23.3.1.1 Authentication Types

The content can be protected using different authentication levels. These levels define the requirements that must be met by the MediaSeal Decryptor Client user to authenticate and access the protected content.

Authentication Type	**Factor Level**	**MediaSeal Authentication**	**Requirements**
	1 Factor Authentication	Password Only	MediaSeal Decryptor Client
	Multi Factor Authentication	Password and iLok	MediaSeal Decryptor Client MediaSeal Portal Account iLok Account / License
	Server + Multi Factor Authentication	Password, iLok and Server	MediaSeal Decryptor Client MediaSeal Portal Account iLok Account / License Connection to Zone Endpoint

23.3.1.2 Secure Playback

Content can be protected so that it may only be accessed using MediaSeal Secure Player or MediaSeal Secure Viewer. This option provides additional security by restricting playback to MediaSeal Secure Player or MediaSeal Secure Viewer which is bundled as part of MediaSeal Decryptor Client software.

MediaSeal Secure Player and MediaSeal Secure Viewer are compatible with Microsoft Windows and Mac OSX 10.10 and above.

23.3.1.3 QR Code

Content that is restricted to Secure Playback via MediaSeal Secure Player can have a QR code overlay containing information about the authorised viewer during content playback.

23.3.1.4 Advanced Options

23.3.1.4.1 Re-Authenticate Every [x] Hours

This allows the asset owner to enforce re-authentication every x number of hours. After the timeout is reached, access to the content will be re-authenticated.

Re-authentication triggers creation of an audit record, thus decreasing the time between re-authentication requests will increase the number of audit records for file access.

23.3.1.4.2 Disable Automatic Background Authentication

This disables automatic background authentication and will require the end user to re-input the content password after the file cache timeout setting has been reached.

By default, once a file is successfully authenticated, seamless automatic background reauthentication occurs if the file is still in use for longer than 8 hours and every subsequent 8 hours. This does not require user interaction.

23.3.2 Source Tab

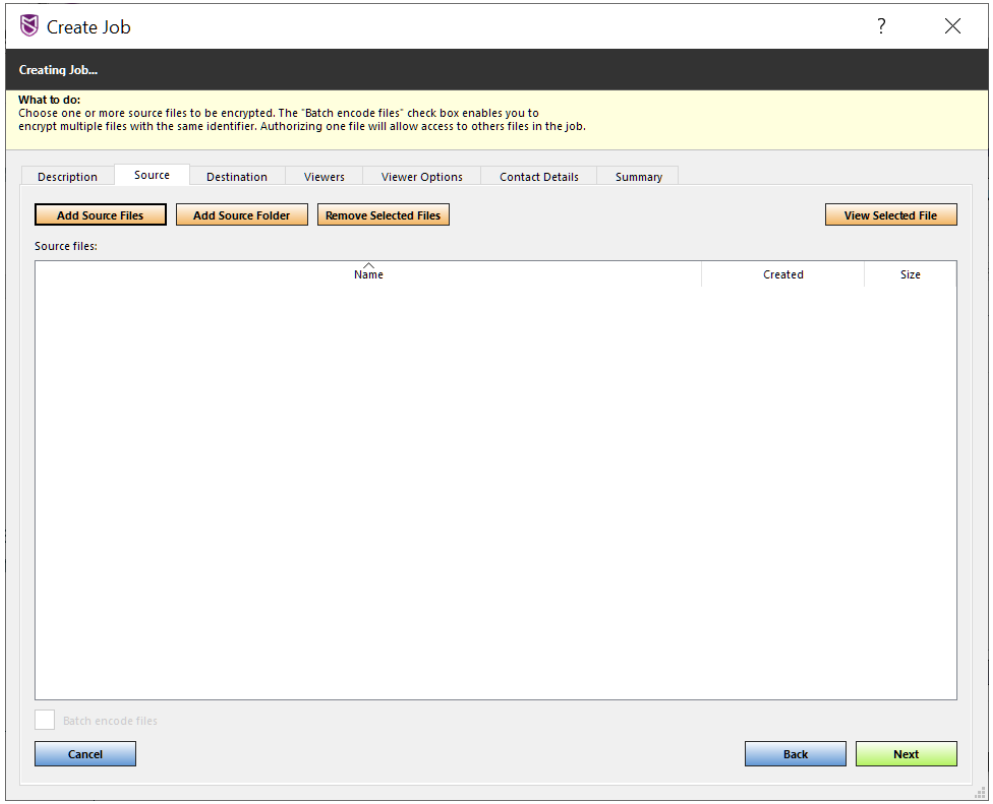
The source tab is used to specify the content you wish to protect. You can add individual files or folders.

23.3.2.1 To add source files:

- Click **Add Source Files**
- Select the **Source Files**

23.3.2.2 To add source folders:

- Click **Add Source Folders**
- Select the **Source Folders**



23.3.2.3 Batch Encoding

Batch encoding provides the ability to set authenticate all files within a batch after the first file in the batch is successfully authenticated. If you do not set batch encoding, then each file will require independent authentication.

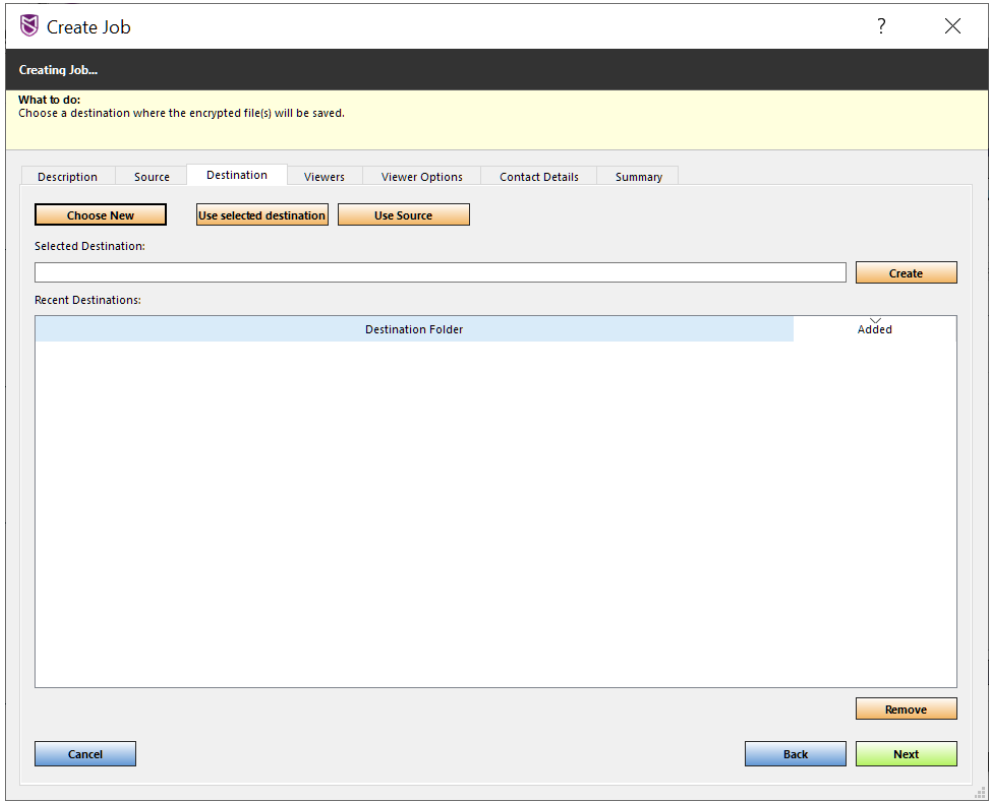
23.3.2.3.1 To encode files in a batch

- Tick **Batch encode files** checkbox.

If you batch encode files, the Audit information will only report that the job was accessed. It will not report which specific file was accessed.

23.3.3 Destination Tab

The destination is the output directory the protected content will be output to after being protected.



23.3.3.1 To select a new destination:

- Click **Choose New**
- Select an **output folder**

23.3.3.2 To select the most recent output destination:

- Select a **Folder** in the list, highlighting the destination folder
- Click **Use Select Recent**

23.3.3.3 To use source directory:

- Click **Use Source**

23.3.3.4 To remove recent output destinations:

- Select a **folder** in the list, highlighting the destination folder
- Click **Remove**

23.3.3.5 To manually create a folder:

- Type the **path** in the Selected Destination input field
- Click **Create**

23.3.4 Viewers Tab

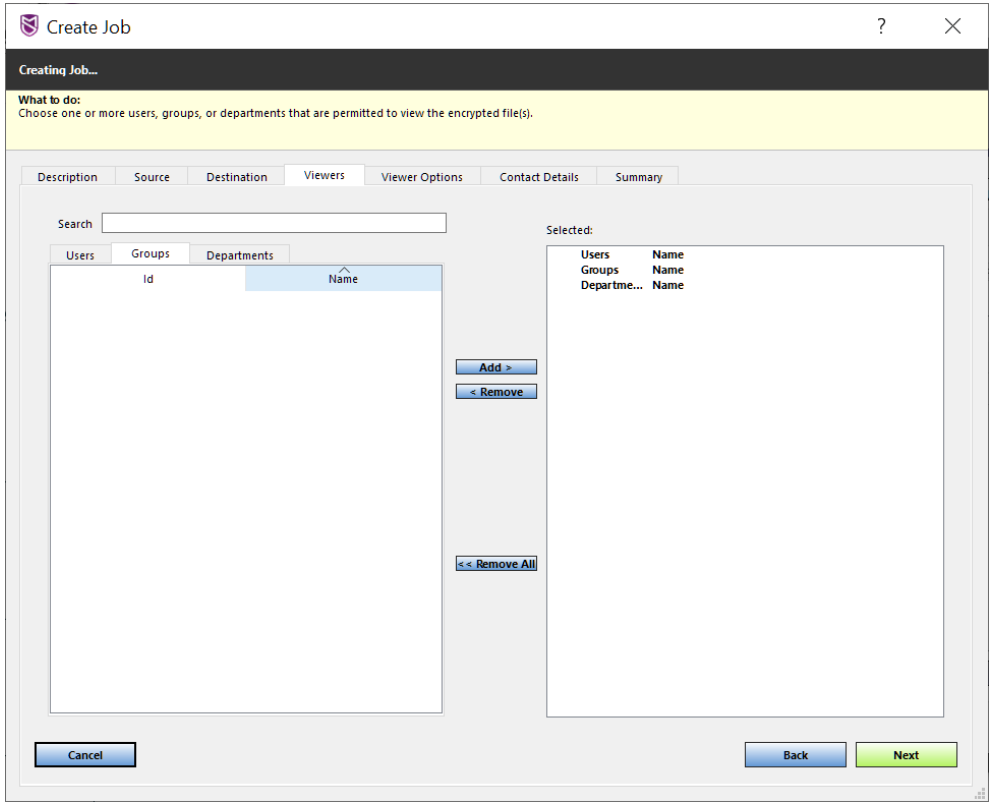
The viewers tab is used to select the MediaSeal Decryptor Users, Groups or Departments the content is to be protected for.

23.3.4.1 To add the User, Group or Department

- Click on the **Name** in the left column
- Click **Add**

23.3.4.2 To remove the User, Group or Department

- Click on the **Name** in the right column
- Click **Remove**

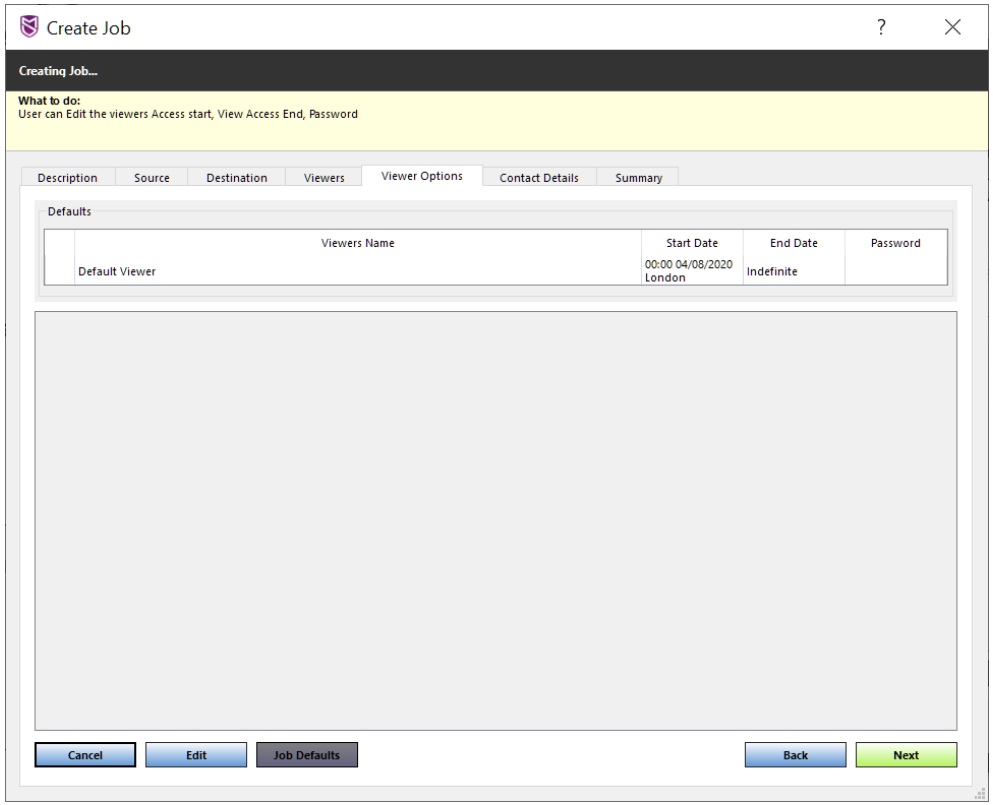


23.3.4.3 To Remove all Users, Groups and Departments

- Click **Remove All**

23.3.5 Viewer Options Tab

The viewer options tab allows the modification of the default content controls including start date, end date, time zone and password. The viewer options tab also allows more granular controls. Content controls can be set on per user, per group and per department.



23.3.5.1 To edit content controls:

- Tick the default, **user, group, or department** to modify
- Click **Edit**
- Modify **fields as required**.

23.3.6 Contact Details Tab

The contact details are the details displayed to the MediaSeal Decryptor Client when accessing content. This allows the MediaSeal Decryptor Client to identify the asset owner of the file.

23.3.6.1 To set the contact details:

- Complete **Contact Name** and **Contact Number**

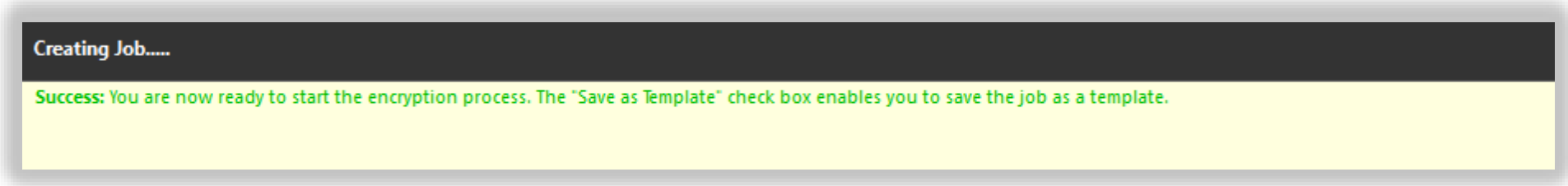
23.3.7 Summary Tab

The summary page provides a summary of the job prior to executing. An information message at the top of the screen provides a message indicating any configuration errors. You can also save the job as a template; this will enable you to create another job based on the same configuration settings later.

23.3.7.1 To save as a template:

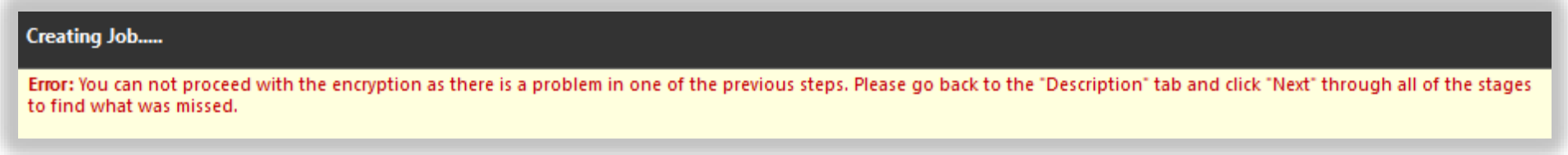
- Tick **Save as Template** checkbox

If the following message is displayed:



- You can click **Start Job**

If not, and the following message is displayed:



- Please **check each of the tabs** for any missing elements.

23.4 Duplicate Job

Instead of using templates to create a job with the same configuration settings, you can also duplicate an existing job.

To duplicate a job:

- Click the **Job** in the list
- Click **Duplicate**
- Set **Source** and **Destination**
- Amend **details as Required**
- Click **Start Job**

23.5 Edit Job

You can edit an existing job, this allows you to make selective changes to the job including changing passwords or assigning or revoking permissions when using server authentication and modify content controls.

23.5.1.1 To edit a job:

- Click the **Job** in the list
- Click **Edit**
- Amend **details as Required**
- Click **Update Job** from the Summary Tab

23.6 Change Access Permissions

You can dynamically change access permissions when using Server + Multi Factor Authentication (Password, iLok and Server). This is particularly useful to add or revoke access to MediaSeal protected content

23.6.1.1 To change access permissions:

- Click the **Job** in the list
- Click **Edit,** click **Viewers** Tab
- **Add** or **remove users** as required
- Click **Update Job** from the Summary Tab

23.7 Archive Job

Jobs that cannot be deleted, or jobs that are no longer relevant can be archived. The job will be moved and accessible in the Archived Jobs Tab

23.7.1.1 To archive a job:

- Tick the checkbox of the **Job** you wish to delete
- Click **Archive**

23.7.1.2 To un-archive a job:

- Tick the checkbox of the **Job** you wish to delete
- Click **Unarchive**

23.8 Delete Job

Jobs can be deleted if they have been created in error or are not required. The job will be permanently removed and cannot be restored.

Jobs can only be deleted if MediaSeal protected files are not associated with that job.

23.8.1.1 To delete a job:

- Tick the checkbox of the **Job** you wish to delete
- Click **Delete**

24 TEMPLATES

24.1 MANAGING TEMPLATES

Templates provide a mechanism to store configuration settings which can be applied to multiple jobs. They also provide a mechanism to run jobs from the command line.

The templates are in the Jobs section in a separate tab.

24.1.1 Create Template

Create template does not allow setting source content or output destination locations. All other fields can be created the same as creating a job. See the **Create Job** section for more information.

24.1.1.1 To create a template:

- Click the **Jobs** Section
- Click **Templates** Tab
- Click **New Template**
- Enter the **required configuration**
- Click **Save**

24.1.2 New Job from Template

You can create a job using an existing template. This allows the configuration settings from the template to be pre-set in the new job. Creating a job using a template is the same as creating a job. See the **Create Job** section for more information.

24.1.2.1 To create a job using a template:

- Click the **template** in the list, highlighting the template
- Click ***New Job from Template***
- Add **Source files** and **destination** location
- Amend **details as Required**
- Click **Start Job**

24.1.3 Export Template

The export template is primarily used for used for generating a Job XML File <JobXMLFILE> that can be used on the command line.

This feature allows for easy generation of the Job XML File for command line use.

24.1.3.1 To export a template:

- Click the **template** in the list
- Click **Export Template**
- Save to **required destination**.

For information on using the Job XML Template, please see the Command Line section

24.1.4 Delete a template:

Templates that are no longer required can be deleted

24.1.4.1 To delete a template

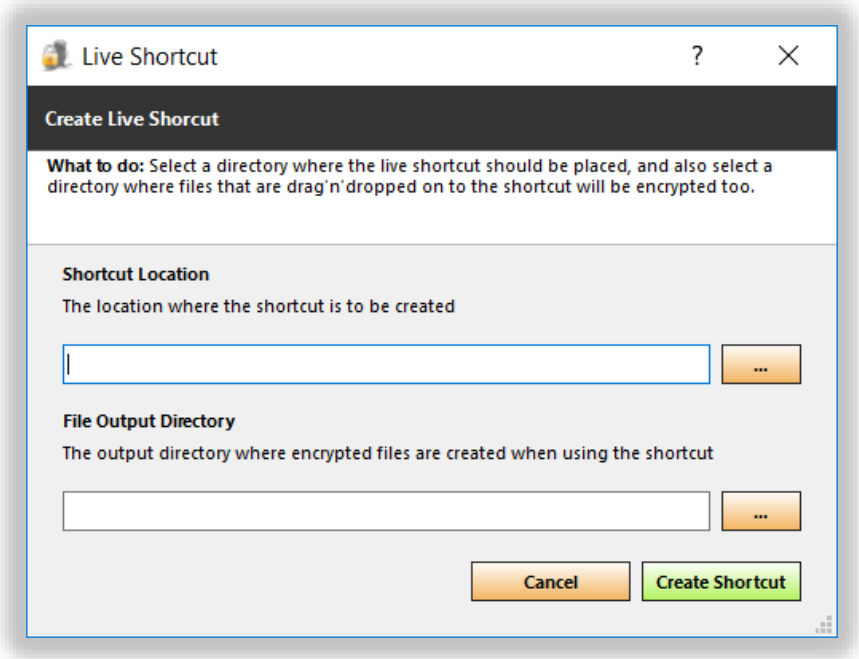
- Click the **Job** in the list
- Click **Delete**

24.1.5 Create Shortcut

Create shortcut allows for implementing drag and drop file protection. This process can be done manually or via the MediaSeal Encryptor Client. To generate a drag and drop shortcut manually, please see the **Drag and Drop File Protection** section.

24.1.5.1 To create a shortcut:

- Click the **template** in the list
- Click **Create Shortcut**
- Set the **Shortcut Location**
- Set the **File Output Directory**
- Click **Create Shortcut**



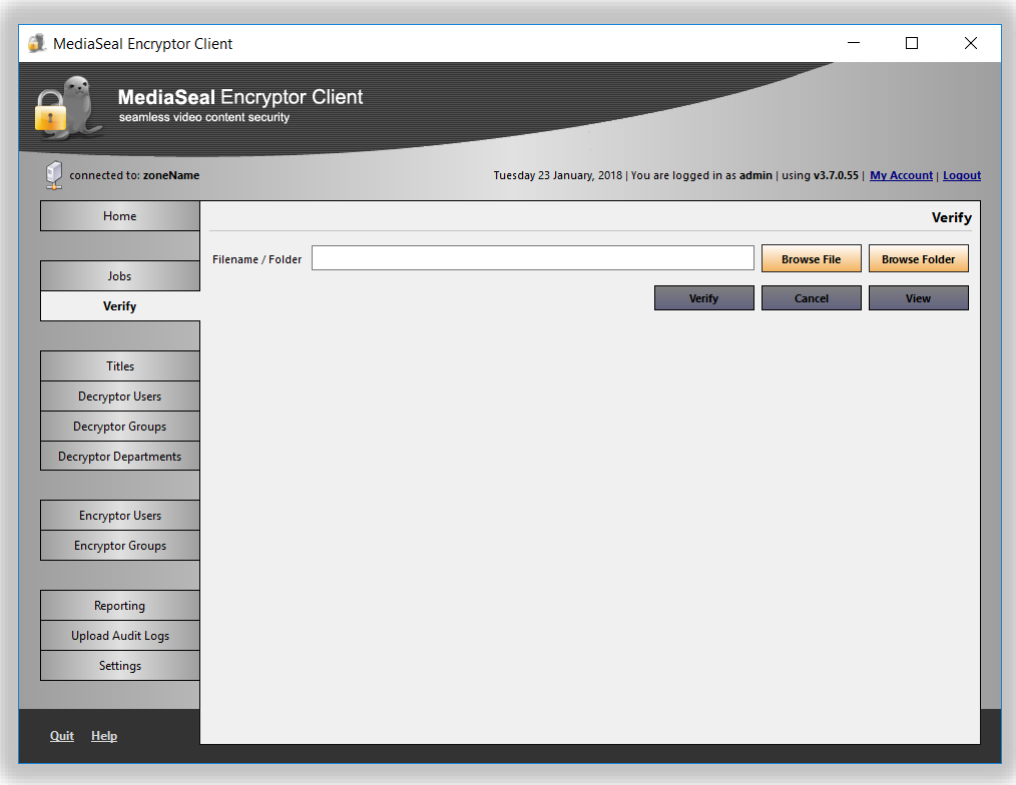
If you drag and drop files onto this shortcut, it will run a job to protect the files.

25 File Verification

Verify is a means to verify that a file is a valid MediaSeal protected file. This is a useful tool for validating files after a job has completed to verify that the file is valid. You can check a single file or multiple files within a folder.

25.1.1.1 To verify a file or files:

- Click **Browse File** or **Browse Folder**
- **Select** the file or folder you wish to verify
- Click **Verify**



The results will be displayed in the window. If you wish to cancel the operation:

- click the **Cancel** button

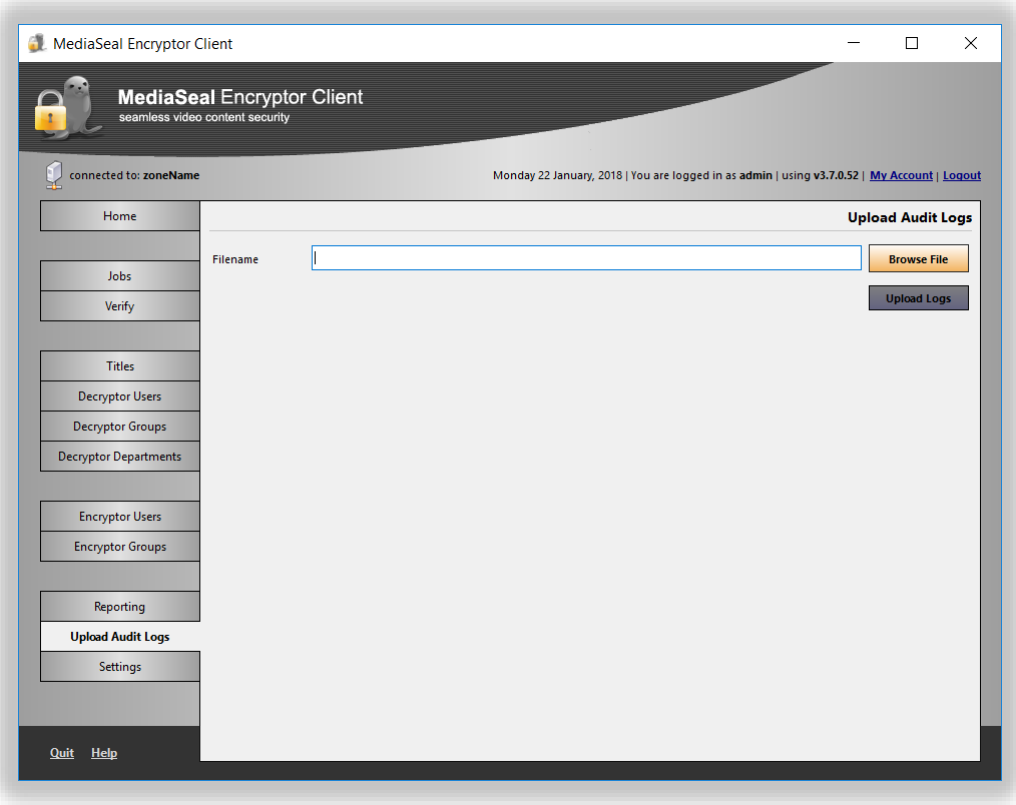
When selecting an individual file, you can open the file using your default application by clicking the View button

26 UPLOAD AUDIT LOGS

Upload Audit Logs section enables you to upload audit logs generated by MediaSeal Decryptor Clients that do not have a connection to your studio server. Once uploaded, the audit data is integrated into the studio server enabling you to utilise the integrated reporting features of MediaSeal Encryptor Client.

You will need to request the MediaSeal Decryptor Client user to export their Audit Logs.

(Please see the MediaSeal Decryptor Client Manual for more information on exporting user audits)



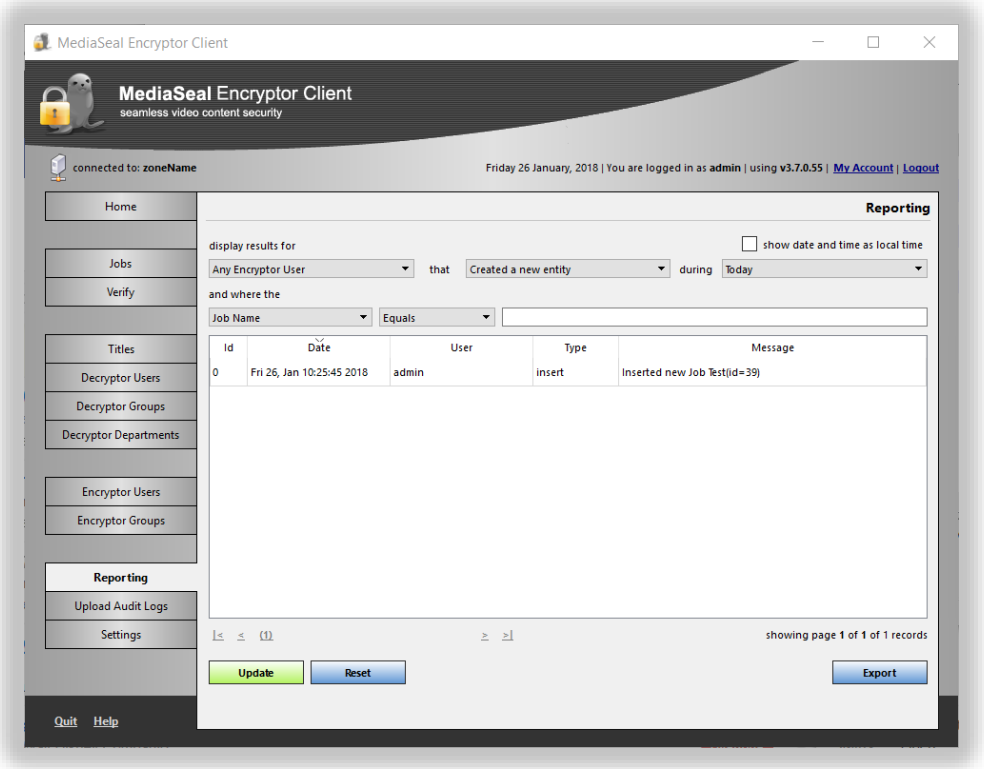
26.1.1.1 To upload audit logs:

- Click on **Upload Audit Logs** Tab
- Click on **Browse File**
- Select the **File**
- Click **Open**
- Click **Upload Logs**

27 REPORTING

The reporting feature allows you view and export Encryptor and Decryptor audit data.

Please note, there may be a delay in downloading and accessing audit data from MediaSeal Decryptor clients who are using the MediaSeal Global Services Zone Endpoint.



Complete Decryptor User Audit Data is dependent on either Server + Multi Factor Authentication (Password, iLok and Server), and uploading MediaSeal Decryptor Client User Audit Data.

27.1 VIEWING AUDIT DATA

You can view audit data for both Encryptor and Decryptor users.

27.1.1.1 To view audit data:

- Click the drop-down list **display results for** the required User/s
- Change the **filters as required**

27.1.2 Audit Types:

Decryptor User Audit Types	**Audit Type:**	**Description:**
	Attempted to access a file	An attempt was made to access a file
	Was denied access to a file	Access to a file was denied
	Was granted access to a file	Access to a file was granted
	Save file having open assets	A file was saved whilst protected content was open

Encryptor User Audit Types	**Audit Type:**	**Description:**
	Attempted to login	An attempt was made to login
	Was denied a login	Login attempt was denied
	Was granted a login	Login attempt was successful
	Created a new entry	A new entity was created
	Updated an existing entity	An entity was updated
	Deleted an existing entity	An entity was deleted

27.1.3 Filters:

You can filter the results by date of the audit types. The options available are **Any time**, **Today**, **Yesterday**, **This Week**, **This Month** and **This Year**. You can also show the date and time as local time.

27.1.3.1 To change the date selection:

- Click on the drop down **during**
- Select the **required date range**
- Tick **checkbox show date and time as local time** if required

For MediaSeal Decryptor Client user audit data it is also possible to filter by additional parameters.

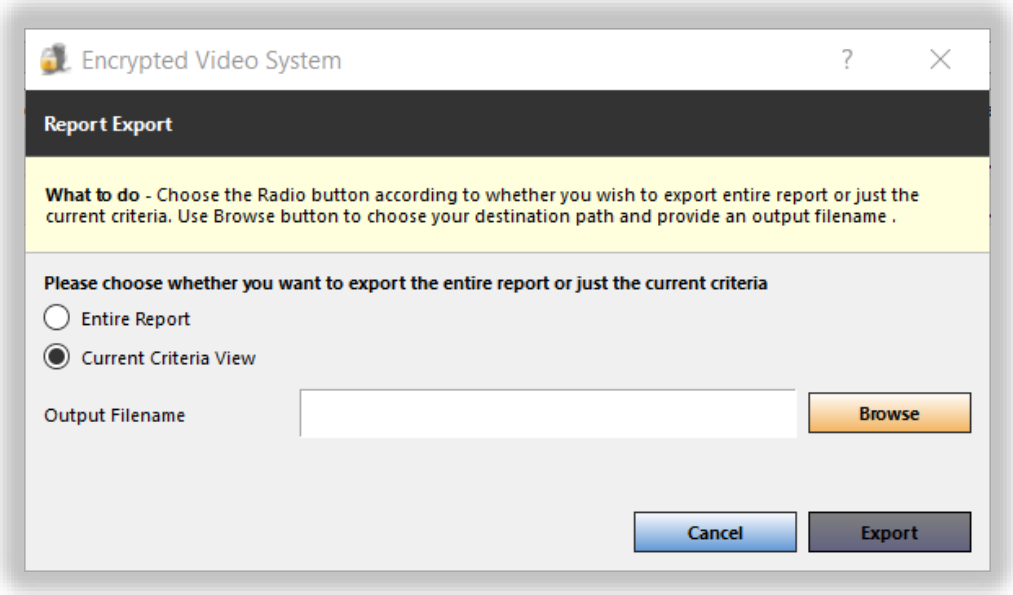
Decryptor User Filters	**Filter Type:**	**Description:**
	Filename	The name of the file
	File Id	The File Id of the file
	Machine Name	The hostname of the machine
	IP Address	The IP address of the machine
	MAC Address	The network MAC Address of the machine
	Host User Name	The username used on the machine

27.2 Exporting Audit Data

You can specify to export the entire report, alternatively you can export only the current view.

To export audit data:

- Click **Export**
- Select **Entire Report** or **Current Criteria View**
- Specify an **Output Filename**
- Click **Export**



The file will be exported in Comma Separated Values (CSV) format.

28 COMMAND LINE

28.1 COMMAND LINE OPTIONS

The MediaSeal Encryptor Client can be executed from the command line or from a script that enable MediaSeal protection to be implemented easily into existing workflows.

Options:	Function	Description:
-?, -h, --help	Help	Displays this help.
-c, --commandline <jobXmlFile>	Job XML File	Job Template XML File
-e, --localendpoint <localendpoint>	Local Endpoint	Local endpoint override
-g –globalendpoint	Global Endpoint	Global endpoint override
--license <license>	Licence	License key to use with the global endpoint override
--studioid <studioid>	Studio Id	Studio id that corresponds to the license key.
-l, --list	List Users & Groups	Get a list of groups and studio users for the job template file.
-u, --username <username>	Username	Username
-p, --password <password>	Password	Password
-o, --output <OutputStatusFile>	File Output	Operation status file output
-s, --screenoutput	Screen Output	Display output on Screen Dialog
--id, --templateid <templateid>	Template Id	Command line run template id
-n, --templatejobname <templatejobname>	Template Job Name	Command line run job name
--opath, --outputpath <outpath>	Output Path	Command line run output path
-q, --autoquit	Auto Quit	Command line to automatically quit on complete
-m, --allow-multiple-instances	Multiple Instances	Allow multiple instances of the Encryptor

You will need administrative permissions to run Encryptor from the Command Line

28.1.1 Help

Displays the help text for the Encryptor. On macOS or Linux you can display the help menu by passing the command line switch --help or -h to the Decryptor Client.

- Open **Terminal**
- Type **Encryptor --help**
- Press **Enter**

**The help menu does not show for the Windows platform; however, all command line functions can be performed as indicated.*

28.1.2 Local Endpoint

Overrides the current Encryptor endpoint settings. This is used when connecting directly to a local endpoint KeyServer.

28.1.3 Global Endpoint

Overrides the current Encryptor endpoint settings. This is used when connecting to a Global Services endpoint.

*Requires License and Studio Id settings

28.1.4 License.

The MediaSeal studio License required to connect to the server. *This is required when specifying the Global Endpoint setting.

28.1.5 Studio Id

The MediaSeal studio Identification to connect to the server. *This is required when specifying the Global Endpoint setting.

28.1.6 Job XML File

You can use the Job XML file as a configuration file to be used for executing a command line job. Please see the **Export Template** section for more details on creating a Job XML File.

28.1.7 Screen output

When screen output is enabled, the username and password can be optionally provided on the command line. If a username is present and there is no password provided or an incorrect password is entered, a login window will appear.

Please note that both --screenoutput and --output cannot be used at the same time.

28.1.8 Auto Quit

If auto quit is set using the command line, the Encryptor will exit at the end of the encryption. Once authentication is processed, a window with progress and logs will appear.

28.1.9 Multiple Instances

The multiple instances argument allows multiple instances of MediaSeal Encryptor Client to run simultaneously

28.1.10 Output Status

The -o, –output option creates an XML status file containing a summary of the protection process. If the status file does not exist, it will create a new file. If the status file already exists, it will be overwritten with new entries.

A lock mechanism is used to synchronise reading and writing to the file. The lock file is named the same as the status file with '.lock' appended to the end of the file.

If no --output(-o) option was specified, the result will be directed to stdout. The output directed to stdout will be XML format with whitespace removed. Each update to the status will appear as a new line on stdout.

Please note that both --screenoutput and --output cannot be used at the same time.

28.1.11 Template ID

This option allows you to reference the template created in the MediaSeal Encryptor Client to be used on the command line by referencing the template identification number.

28.1.12 Template Job Name

This is the name of the job that will be created in MediaSeal Encryptor Client when MediaSeal Encryptor from the command line.

28.1.13 Example Command Line Encryptor (Windows)

An example of running MediaSeal Encryptor Client command line:

```
"C:\Program Files (x86)\MediaSeal\Encryptor\Encryptor.exe" --screenoutput --autoquit --templateid 1226 --templatejobname test --outputpath c:\some\output\folder\ -u myusername -p mypassword c:\some\file\to\encrypt.mp4 c:\some\folder\to\encrypt
```

28.1.14 Example Command Line Encryptor (MacOS)

An example of running MediaSeal Encryptor Client command line:

```
/Application/MediaSeal/Encryptor.app/Contents/MacOS/Encryptor --screenoutput --autoquit --templateid
1226 --templatejobname test --outputpath /some/output/folder/ -u myusername -p mypassword
/some/file/to/encrypt.mp4 c:/some/folder/to/encrypt
```

28.1.15 Command Line Error Codes

After MediaSeal Encryptor Client command line process has completed, a numerical status or exit code will be generated by the process that indicates the result of the operation.

Return Codes:	**Result Code:**	**Description**
	0	Success
	1	Command line parameter error
	2	Connection error
	3	Login error
	4	Error opening or reading task file
	5	Error opening or updating status file
	6	Error during encryption process

Any process errors will be written to the MediaSeal Encryptor Client log file.

If you specified an output status file, errors will be written to the status file. If you do not specify an output status file you can type still examine the exit or status code by using the in-built operating system functionality.

If the MediaSeal Encryptor process is spawned by another process, please review the calling framework for determining error codes.

28.1.15.1 Windows

To determine the exit code on Microsoft Windows operating systems, you need to check the %errorlevel% environment variable.

- Type **echo %errorlevel%** and hit **Enter**

28.1.15.2 MacOS

To determine the exit status on Apple macOS operating systems, you need to expand to the exit status of the most recently executed foreground pipeline by using the shell's special parameters.

- Type **echo $?** and hit **Enter**

28.2 Command Line XML Files

XML configuration files are a convenient method of passing template information to the Encryptor command line. To export a template to an xml file, please see the Export Template section.

28.2.1 Configure the template file:

To configure the template:

```
<?xml version="1.0" encoding="UTF-8"?>
<EncryptionJob>
   <JobName></JobName>
   <OutputDirectoryPath></OutputDirectoryPath>
   <SourceFilePathList/>
   <TemplateId>1</TemplateId>
</EncryptionJob>
```

- Enter a job name **<JobName>my test job</JobName>**
- Enter an output directory **<OutputDirectoryPath>C:\Users\user1\output</OutputDirectoryPath>**

28.2.1.1 Encrypt a single file:

To encrypt a single file:

- Add the full path of the file **<SourceFilePathList>C:\Users\user1\test1.mov</SourceFilePathList>**

```
<?xml version="1.0" encoding="UTF-8"?>
<EncryptionJob>
   <CreateJobData>
      <JobName>my test job</JobName>
      <OutputDirectoryPath>C:\Users\user1\output</OutputDirectoryPath>
      <SourceFilePathList>
          <listitem>C:\Users\user1\test1.mov
          </listitem>
          <listitem>C:\Users\user1\test2.mov
          </listitem>
      </SourceFilePathList>
      <TemplateId>1</TemplateId>
   </CreateJobData>
</EncryptionJob>
```

28.2.1.2 Encrypt multiple files:

To encrypt multiple files:

- To encrypt multiple files, add each file as a list item **<SourceFilePathList><listitem>C:\Users\user1\test1.mov</listitem><listitem>C:\Users\user1\test2.mov</listitem></SourceFilePathList>**

28.2.2 Using XML File (Windows)

An example of running the command line on Windows (assuming MediaSeal Encryptor is installed in c:\Program Files (x86)):

```
"C:\Program Files (x86)\MediaSeal\Encryptor\Encryptor.exe" -c C:/Users/testuser/testinput.xml -u user1 -p password -o C:/Users/testuser/testStatus.xml
```

28.2.3 Using XML File (macOS)

An example of running the command on macOS from terminal, assuming the application bundle is in /Applications/MediaSeal, you can use the following syntax

```
/Application/MediaSeal/Encryptor.app/Contents/MacOS/Encryptor -c /Users/testuser/testinput.xml -u user1
-p password -o /Users/testuser/testStatus.xml
```

28.2.4 User Group Modification

To modify users associated with a group from the command line, you can generate an xml file as per below and then use the -c command line parameter and xml file to import back the changes.

To generate the xml file:

```
Encryptor.exe -c changeusers.xml -u user1 -p password
```

- Using the template that is exported, modify the **GroupId, UserId and OperationType** as required.

```
<?xml version="1.0" encoding="UTF-8"?>
<ModifyGroup>
   <ModifyGroupUsersData>
      <OperationList>
         <listitem>
            <GroupModificationOperation>
               <GroupId>34</GroupId>
               <UserId>1</UserId>
               <OperationType>REMOVE</OperationType>
            </GroupModificationOperation>
         </listitem>
         <listitem>
            <GroupModificationOperation>
               <GroupId>34</GroupId>
               <UserId>2</UserId>
               <OperationType>ADD</OperationType>
            </GroupModificationOperation>
         </listitem>
      </OperationList>
   </ModifyGroupUsersData>
</ModifyGroup>
```

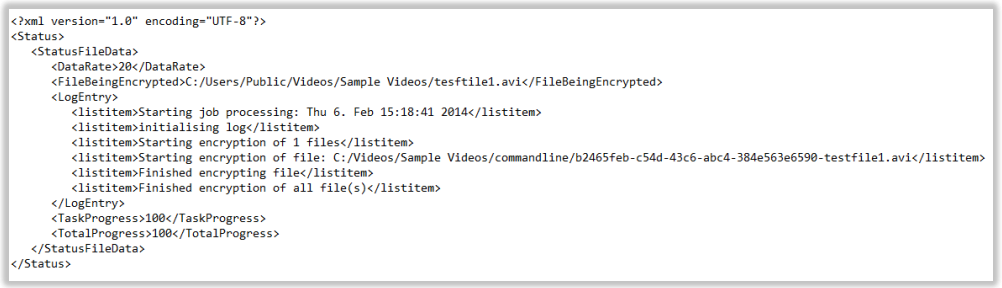
Supported Operation Types: **[ADD] [REMOVE]**

28.2.5 Output Status XML File

A status file can be created indicating the status levels of a job during the encryption processing instead of outputting status directly to stdout.

28.2.5.1 To create the status output file

Use the –**output** (-o) command line option along with the file path of the output file



A status file will be created if one does not already exist. If it exists, it will be overwritten with new entries during the encryption processing.

A lock file is created, named the same as the status file with '.lock' appended to the end of the file path, this is used to synchronise file reads and writes. It is safe to read the status file if you can obtain a read lock on the lock file. The lock must be released immediately after a read, so the process can get a write lock to update it.

If the --output(-o) command line option is not specified, the output is sent to stdout as per the above xml format but with whitespace removed. Each update to the status appears as a new line on stdout.

28.3 Drag and Drop File Protection

You can use the command line feature of MediaSeal Encryptor Client to automate the protection of files. MediaSeal Encryptor Client User Interface is used to create templates that can then be used in the command line. A shortcut or an Automator task can also be created manually or by using the MediaSeal Encryptor Client to enable drag and drop protection of files and folders. To create a shortcut using the MediaSeal Encryptor Client, please see the Create Shortcut section

28.3.1 Drag and Drop File Protection (Windows)

- On the Desktop right click and Select **New Shortcut**
- Click **Browse** and select **Encryptor.exe** from the MediaSeal Encryptor Client installation directory
- Append any **required commands.**
- Click **Next**, type a **Name** for the shortcut, then click **Finish**

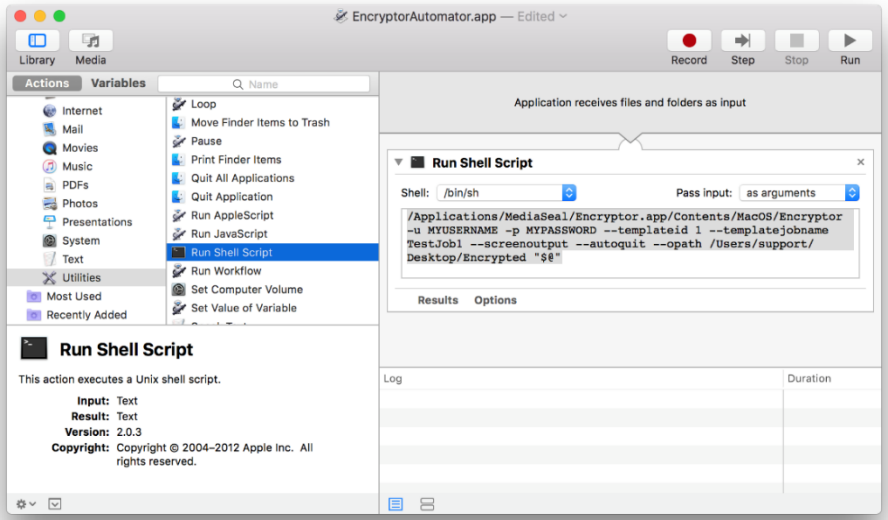
28.3.1.1 Windows Example shortcut with appended commands:

If you drag and drop files onto this shortcut, it will run a job to protect the files.

```
"C:\Program Files (x86)\MediaSeal\Encryptor\Encryptor.exe" -u myusername -p mypassword -screenoutput -autoquit -templateid 34 -templatejobname Test1 -output c:\Users\User1\
```

28.3.2 Drag and Drop File Protection (MacOS

Drag and drop file protection can be configured on macOS by creating an Automator Task.



28.3.2.1 To create an Automator script:

- Launch **Automator.**
- Select **Application** as the type of document and click **Choose**
- From actions list select **Utilities**, and then double click **Run Shell Script**

- In the “Run Shell Script” change the Pass input to **as arguments** and change shell to **/bin/sh**

- Enter the **required commands**
- Select **File**, **Save**

28.3.2.2 macOS Example shortcut with appended commands:

If you drag and drop files onto this shortcut, it will run a job to protect the files.

```
/Applications/MediaSeal/Encryptor.app/Contents/MacOS/Encryptor -u MYUSERNAME -p MYPASSWORD --templateid
1 --templatejobname TestJob1 --screenoutput --autoquit --opath /Users/support/Desktop/Encrypted "$@"
```

If you drag and drop files onto this Automator, it will run a job to protect the files.

29 DIAGNOSTIC LOGGING

By default, only basic logging is enabled, and diagnostic logging is turned off. However, to assist the MediaSeal Support Team diagnose issues you can enable diagnostic logging. Firstly, enable diagnostic logging, then try to replicate the issue and finally, send the diagnostic log to the MediaSeal Support Team.

29.1 ENABLE DIAGNOSTIC LOGGING ON WINDOWS

The default diagnostic log file location on Microsoft Windows is **%Appdata%\MediaSeal\Storage\Encryptor.log**

To start Encryptor in diagnostic mode:

- **Quit** the Encryptor
- Open **command prompt**
- Type **C:\Program Files (x86)\MediaSeal\Encryptor\Enryptor.exe --level trace**
- Press **Enter**

29.2 Enable Diagnostic Logging on macOS

The default locations for Decryptor.log file on macOS and Linux is **~/.config/MediaSeal/Storage/Encryptor.log**

To start the Decryptor in diagnostic mode:

- **Quit** the Encryptor
- Open **Terminal**
- Type **/Applications/MediaSeal/Encryptor.app/Contents/MacOS/Encryptor --level trace**
- Press **Enter**

30 MediaSeal Linux Headless Installation

30.1 Pre-Requisites

The following dependencies are required to be installed (libharfbuzz0b libgl1-mesa-glx libfontconfig1 libsm6 xvfb). These packages may be missing in a headless environment.

To install dependencies:

- **sudo apt update**
- **sudo apt install libharfbuzz0b libgl1-mesa-glx libfontconfig1 libsm6 xvfb**

30.2 Installation and Configuration

30.2.1 Installation

Unzip MediaSeal_[version]-[platform].zip to required install directory (e.g /opt/mediaseal/)

30.2.2 Configuration

Navigate to the installation directory

Ensure the following file is made executable:

Encryptor-x86_64.AppImage

- **chmod +x Encryptor-x86_64.AppImage**

30.2.3 Building Encryptor.conf

Before using MediaSeal Encryptor you will be required to build an initial configuration file named Encryptor.conf

This file should be created at ~/.config/MediaSeal/Encryptor.conf

An example Encryptor.conf layout

```
[General]
defaultTimeZone=Europe/London
loginName=user1
masterZone0IsLocal=false
masterZoneCount=1
masterZoneEndpoint0=https://gs.cloud.mediaseal.com
masterZoneName0=MediaSeal Global Services
studioCount=1
studioId=100
studioLicenceKey0=9hAq123qwerty==Waz
studioName0=MediaSeal
```

30.3 ENCRYPTOR USAGE

To encrypt, run the command with specified options

- **xvfb-run -a /opt/mediaseal/Encryptor-x86_64.AppImage [options]**

A list of options can be seen by specifying

- **xvfb-run /opt/mediaseal/bin/Encryptor-x86_64.AppImage -h**

Example:

```
xvfb-run -a /opt/mediaseal/Encryptor-x86_64.AppImage -u admin -p password --id 3 -n TestJob --opath
/home/admin/encrypt/ TestFile.mkv
```

31 TROUBLESHOOTING

31.1 BASIC TROUBLESHOOTING

Before checking for alternative solutions. Please perform these basic checks:

Activate iLok License

Make sure you have activated your MediaSeal Encryptor Client License after installation.

Make sure you have plugged in the correct iLok if using a physical iLok

MediaSeal Encryptor Zone Endpoints

Make sure you have configured the correct Zone Endpoint and that you are connected.

Make sure you are using the correct password.

31.2 MEDIASEAL SUPPORT

For MediaSeal support, the latest information, tutorials, and solutions, please visit the MediaSeal Support Portal. If you still require further information or assistance, please email the MediaSeal Support Team.

31.2.1 MediaSeal Support Portal

MediaSeal Support Portal

https://mediaseal.fortiumtech.com

31.2.2 MediaSeal Email Support

MediaSeal Support Email

support@mediaseal.com