# Table of Contents

## 2 MediaSeal – Encryption While You Work

- 2.1 MediaSeal Overview ................................................................. 8

## 3 MediaSeal Encryptor Client

- 3.1 Encryptor Client Overview .......................................................... 9
- 3.2 Licensing ................................................................................. 9
- 3.3 Encryptor Client Support ............................................................... 10
  - 3.3.1 MediaSeal Support Portal ......................................................... 10
  - 3.3.2 MediaSeal Email Support ......................................................... 11

## 4 Version Compatibility ..................................................................... 12

## 5 System Requirements .................................................................... 13

- 5.1 Hardware Requirements .............................................................. 13
- 5.2 Supported Operating Systems ..................................................... 13

## 6 Additional Requirements ............................................................... 14

- 6.1 MediaSeal Account .............................................................. 14
- 6.2 MediaSeal Encryptor Client Software ......................................... 14
- 6.3 Permissions to Install Software .................................................. 14

## 7 Installation .................................................................................. 15

- 7.1 Installation on Windows ............................................................... 15
- 7.2 Installation on MacOS ................................................................. 16

## 8 Encryptor License Activation ......................................................... 17

- 8.1 Activate iLok License ................................................................. 17
- 8.2 Activation Location .................................................................. 20
  - 8.2.1 Allocate License to Physical iLok ......................................... 20
  - 8.2.2 Allocate License to Computer ............................................. 20

FOR SUPPORT VISIT: mediasel.fortiumtech.com

MediaSeal Encryptor Client Manual 3.9.2

02 October 2019
17.2 Edit Decryptor Group.................................................................................................................. 41
17.3 Delete Decryptor Group.................................................................................................................. 42
17.4 Activate Decryptor Group............................................................................................................... 42
17.5 Deactivate Decryptor Group.......................................................................................................... 42
17.6 Manage Decryptor Group Memberships....................................................................................... 43
17.7 Set Application Permissions......................................................................................................... 44
17.7.1 Permission Controls.................................................................................................................... 45
17.8 Set Recipient Permissions........................................................................................................... 47

18 Decryptor Users.................................................................................................................................. 48
18.1 Manage Decryptor Users.............................................................................................................. 48
18.2 Delete Decryptor Users.................................................................................................................. 49
18.3 Activate Decryptor User................................................................................................................. 50
18.4 Deactivate Decryptor User............................................................................................................ 50

19 Decryptor Groups.................................................................................................................................. 51
19.1 Create Decryptor Group.................................................................................................................. 51
19.2 Edit Decryptor Group...................................................................................................................... 52
19.3 Manage Members of an Decryptor Group....................................................................................... 52

20 Decryptor Departments...................................................................................................................... 53
20.1 Create Decryptor Department....................................................................................................... 53
20.2 Edit Decryptor Department............................................................................................................ 53
20.3 Manage Members of a Decryptor Department............................................................................... 54

21 Titles.................................................................................................................................................... 55
21.1 Create Title....................................................................................................................................... 55
21.2 Edit Title......................................................................................................................................... 56
21.3 Delete Title..................................................................................................................................... 56
21.4 Activate Title.................................................................................................................................... 56
21.5 Deactivate Title............................................................................................................................... 57
21.6 Manage Title Permissions................................................................................................................ 58

22 Jobs..................................................................................................................................................... 60

MediaSeal Decryptor Client Manual 3.9.2
02 October 2019
FOR SUPPORT VISIT: mediaseal.fortiumtech.com

27.1.3 Auto Quit ................................................................. 85
27.1.4 Multiple Instances .................................................... 85
27.1.5 Output Status ............................................................ 85
27.1.6 Template ID .............................................................. 86
27.1.7 Template Job Name .................................................... 86
27.1.8 Command Line Encryptor (Windows) .......................... 86
27.1.9 Command Line Encryptor (MacOS) ............................. 86
27.1.10 Command Line Error Codes ...................................... 87

27.2 Command Line XML Files ............................................. 88
27.2.1 Create Job Using XML Template File .......................... 88
27.2.2 Output Status XML File ............................................. 90
27.2.3 User Group Modification ........................................... 92

27.3 Drag and Drop File Protection ......................................... 93
27.3.1 Drag and Drop File Protection (Windows) .................... 93
27.3.2 Drag and Drop File Protection (MacOS) ....................... 94

28 Troubleshooting .................................................................. 96
28.1 Basic Troubleshooting ...................................................... 96
28.2 Advanced Troubleshooting .............................................. 96
2 MEDIASEAL – ENCRYPTION WHILE YOU WORK

2.1 MEDIASEAL OVERVIEW

MediaSeal® is an advanced security solution that has been specifically designed to protect sensitive information. Using a combination of sophisticated data encryption techniques and multi-layer access controls, MediaSeal® can protect sensitive content and provide comprehensive security auditing.

MediaSeal® keeps sensitive files encrypted whilst they are being used. It has been designed to fit smoothly into collaborative workflows with the minimum amount of effort.
3 MediaSeal Encryptor Client

3.1 Encryptor Client Overview

MediaSeal Encryptor is a client application that is used to protect content using MediaSeal encryption technologies. MediaSeal Encryptor Client can protect content using 1 Factor, Multi Factor or Server + Multi Factor authentication.

These authentication methods include password, iLok and Server authentication. Access to protected content can be managed dynamically within MediaSeal Encryptor Client when content is protected using Server + Multi Factor (password, iLok and Server) Authentication. The MediaSeal Encryptor Client enables you to instantly control access to content using MediaSeal Encryptor Client’s built-in Access Control Lists.

Different authentication strategies can also be used to protect content for use in isolated or restricted environments by using 1 factor (password) or Multi factor (password and iLok) authentication.

MediaSeal Encryptor Client provides solutions to seamlessly integrate protecting content into your existing workflows by utilising features such as template driven and batch encoding.
3.2 Licensing

MediaSeal Encryptor Client needs 2 licenses to work, a MediaSeal Encryptor Client license and a MediaSeal Studio License. The MediaSeal Encryptor Client license is managed using iLok technologies.

You will need an iLok account.

As part of the MediaSeal registration process, you will be asked to enter your existing iLok account details or create a new iLok account.

A MediaSeal Encryptor license will be deposited to your iLok account.

As part of the MediaSeal Encryptor Client configuration, you will be asked to enter your iLok account details. Once entered this will enable you to activate your license and allocate the license to a physical iLok or to a specific computer. Please see the Activate iLok Section on how to configure.

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

iLok Website
https://www.ilok.com

You will need a 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, alternatively by the owner of the studio.
3.3 **MediaSeal Client Support**

For MediaSeal Encryptor Client 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.

3.3.1 **MediaSeal Support Portal**

MediaSeal Support Portal

https://mediaseal.fortiumtech.com

3.3.2 **MediaSeal Email Support**

MediaSeal Support Email

mailto:support@mediaseal.com
4 Version Compatibility

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

For the latest version compatibility, please visit the MediaSeal Support Portal.
5 System Requirements

5.1 Hardware Requirements

Most modern computers can run MediaSeal Encryptor Client.

5.1.1.1 Recommended Hardware Specification

- Processor: Dual Core Intel / AMD processor (or Above)
- Memory: 4 Gb RAM (or Above)
- Storage: 1 Gb free space (or Above) + additional space as needed for content files

5.2 Supported Operating Systems

MediaSeal is supported on a wide range of operating systems and versions.

For the latest information on supported operating systems please visit the link below.

MediaSeal Supported Operating Systems
6 ADDITIONAL REQUIREMENTS

6.1 MediaSeal Account

You will need to register a MediaSeal Account to use the MediaSeal Encryptor Client.

You should have received an email invite from noreply@mediaseal.com. Simply follow the instructions in the email and fill in the online form.

To obtain an invitation please contact your content owner.

6.2 MediaSeal Encryptor Client Software

Links to download MediaSeal Encryptor Client software will be sent to your email address once you have completed the MediaSeal Registration.

Download the software that corresponds with your Operating System (OS).

6.3 Permissions to Install Software

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

7.1 INSTALLATION ON WINDOWS

*MediaSeal Encryptor Client will require you to restart the machine after installation.*

*Please save and close any open files before proceeding.*

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

Once installation is completed, go to the *Encryptor License Activation* section for configuring MediaSeal Encryptor Client.
7.2 Installation on MacOS

MediaSeal Encryptor Client will require you to restart the machine after installation. Please save and close any open files before proceeding.

- Download the software using the links provided in the email
- Open or extract the contents of the compressed file to locate the installer files inside the compressed folder.
- Locate and launch MediaSealEncryptor.dmg and follow the on-screen instructions.

Once installation is completed, go to the Encryptor License Activation section for configuring MediaSeal Encryptor Client.
8 ENCRYPTOR LICENSE ACTIVATION

8.1 ACTIVATE iLOK LICENSE

The first time MediaSeal Encryptor Client is launched it will request you to activate your iLok license.
For support visit: mediaseal.fortiumtech.com

You will be prompted to enter your iLok account credentials.

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

Forgotten iLok Credentials?

If you have forgotten your iLok account credentials:

- Click Forgot Password or User ID?

This will take you to https://www.ilok.com/#/recover to recover your iLok credentials.
Once you have entered your iLok Credentials, a screen will display the license available to activate.

You will need to Select the MediaSeal Encryptor license

- Click on MediaSeal Encryptor License
- Click Next

Continue to **Activation Location Section**

**No MediaSeal Encryptor License?**

*If you do not have a MediaSeal Encryptor license available:*

The license may already be allocated. Please use iLok license Manager to de-allocate your MediaSeal Encryptor license back to your iLok account.

Alternatively, please contact the MediaSeal Support Team.

MediaSeal Support Team

**support@mediaseal.com**
8.2 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

8.2.1 Allocate License to Physical iLok

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

8.2.2 Allocate License to Computer

Allocating the MediaSeal Encryptor Client license to a specific computer restricts protecting content from that specific computer. It should be used only 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
### 9.2 Additional Studio Licenses

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

To manage additional studio licenses:

- Start MediaSeal Encryptor Client
- Click on Manage Studio Licenses
- In the dialog window, enter Your Studio License in the Add New Studio License input field
- Click Add Studio License
The initial MediaSeal Encryptor Client login screen allows you to select which studio to login to.

To select the studio and login:

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

For login accounts and studio licenses to studios other than your own, please contact the studio owner.
You can logout MediaSeal Encryptor Client using the logout link.

To logout:

- **Click the Logout link**

You can only work on 1 studio at a time, to login to another studio, first logout the current studio and then login to the other studio.

To quit the application instead of logging out, click the Quit link on the bottom left.
12 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
- In the dialog window, edit your details as required.
- Click Ok
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. 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.
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.

Above the home tab on the left, indicates which Zone Endpoint you are connected to. See the Zone Endpoints section for more information.
14.1 Global Settings

14.1.1 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 \texttt{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
14.1.2 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.

*Primary Email Addresses* is the setting used to configure which email addresses will receive alerts of suspicious activity.

To test your settings, click the Test button.

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

The security tab allows you to set thresholds for Red and Amber Alert threats (suspicious activities). It also allows setting the required minimum complexity for passwords.

To modify the Thresholds and Password Complexity

- Move the Slider to the required value

**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.

**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.

**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.
14.2 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.
14.2.1 Zone Connectivity Test

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

To Test a Zone Endpoint:

- Click the zone to check and click Check, alternatively click Check All
- The results will be displayed in the dialog box

14.2.2 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

14.2.3 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
**15 Zone Endpoints**

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](https://gs.cloud.mediaseal.com) which acts as a proxy and redirects communication to the correct Studio Server automatically.

However, it may be required that you 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, you can also configure MediaSeal Encryptor Client to use a proxy for communication if required.
15.1 Manage Zone Endpoints

By default, the Zone Endpoint is set to MediaSeal Global Services https://gs.cloud.mediaseal.com.

Add New Zone Endpoint

- Click on Settings Tab
- Click Manage Zone Endpoints
- Click Add Zones
- Enter Zone Name in Zone
- Enter EndpointAddress (*see note)
- Tick Local (*see note) if required.
- Click Add

Zone Endpoint addresses can be either a hostname, fully qualified domain name or IP address.

e.g. https://mystudioserver:443

Local

Local should only be set when communicating directly with a studio server.

Only 1 of the zones can be marked local. The Default Zone (MediaSeal Global Services) cannot be marked Local
**Edit Zone**

To edit the Zone Endpoint:

- Click on the Zone to edit in the list, highlighting the Zone
- Click Edit
- Amend Zone details as required
- Click Change

**Restore Default Zone**

To set the default Zone Endpoint:

- Click Default Zones

**Remove Zone**

To Remove a Zone Endpoint:

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

**Remove All Zone Endpoints**

To remove all Zone Endpoints:

- Click Remove All
15.2 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

In the dialog box shown enter your proxy server details. (If you do not know the proxy server details, please contact your System Administrator for assistance)

- Click Save
Encryptor Users are those users you wish to allow to login to the Studio Server using the MediaSeal Encryptor Client. You can manage these users through the Encryptor Users section.
16.1 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 (see note*)
- Click Ok

*By default, new accounts are not Active, to make the account active click on the active checkbox. Alternatively see the Activate Encryptor User Section.

16.2 Edit Encryptor User

To edit an Encryptor User:

- Click the user account in the list so the user account is highlighted.
- Click Edit
- Modify the required fields.
- Click Ok
16.3 **DELETE ENCRYPTOR USER**

To delete an Encryptor User:

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

![Delete Encryptor User](image)

16.4 **ACTIVATE ENCRYPTOR USER**

To activate an Encryptor User:

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

16.5 **DEACTIVATE ENCRYPTOR USER**

To deactivate an Encryptor User:

- Check the tick box of the Encryptor User account to deactivate
- Click *Deactivate*
Encryptor groups allow you to group together Encryptor Users Accounts. Within each group you can set application permissions and recipient permissions.

In addition, you can add manage group memberships
17.1 Create Encryptor Group

To create an Encryptor Group:

- Click on New
- Enter Name and Description.
- Tick Active (see note*)
- Click Ok

*By default, new accounts are not Active, to make the account active click on the active checkbox. Alternatively see the Activate Encryptor User Section.

17.2 Edit Encryptor Group

To edit an Encryptor Group:

- Click the group in the list, so the group is highlighted.
- Click Edit
- Modify the required fields.
- Click Ok
17.3 **Delete Encryptor Group**

To delete an Encryptor Group:

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

17.4 **Activate Encryptor Group**

To activate an Encryptor Group:

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

17.5 **Deactivate Encryptor Group**

To deactivate an Encryptor Group:

- Check the tick box of the Encryptor Group to deactivate
- Click *Deactivate*
17.6 Manage Encryptor Group Memberships

To manage an Encryptor Group:

- Click the group in the list, so the group is highlighted.
- Click Edit
- Click the Members Tab
- Tick the Members you wish to add
- Untick the Members you wish to remove
- Click Ok
## 17.7 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 listing of application permission controls.

To set Application Permissions:

- Click the group in the list, so the group is highlighted.
- Click *Edit*
- Click the *Application Permissions Tab*
- Select the relevant Tab

**ALLOW PERMISSION:**

- Tick the relevant permission

**DENY PERMISSION:**

- Untick the relevant permission

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

---

**MediaSeal Encryptor Client Manual 3.9.2**

02 October 2019
17.7.1 Permission Controls

<table>
<thead>
<tr>
<th>Jobs / Titles</th>
<th>Function</th>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jobs</td>
<td>View</td>
<td>View Jobs</td>
<td></td>
</tr>
<tr>
<td>Jobs</td>
<td>Create</td>
<td>Create Jobs</td>
<td></td>
</tr>
<tr>
<td>Jobs</td>
<td>Edit</td>
<td>Edit Jobs</td>
<td></td>
</tr>
<tr>
<td>Jobs</td>
<td>Archive</td>
<td>Archive Jobs</td>
<td></td>
</tr>
<tr>
<td>Jobs</td>
<td>Copy</td>
<td>Duplicate Jobs</td>
<td></td>
</tr>
<tr>
<td>Jobs</td>
<td>Modify</td>
<td>Modify Existing Jobs</td>
<td></td>
</tr>
<tr>
<td>Titles</td>
<td>View</td>
<td>View Titles</td>
<td></td>
</tr>
<tr>
<td>Titles</td>
<td>Create</td>
<td>Create Titles</td>
<td></td>
</tr>
<tr>
<td>Titles</td>
<td>Edit</td>
<td>Edit Titles</td>
<td></td>
</tr>
<tr>
<td>Titles</td>
<td>Archive</td>
<td>Archive Titles</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encryptor</th>
<th>Function</th>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryptor Users</td>
<td>View</td>
<td>View Encryptor Users</td>
<td></td>
</tr>
<tr>
<td>Encryptor Users</td>
<td>Create</td>
<td>Create Encryptor Users</td>
<td></td>
</tr>
<tr>
<td>Encryptor Users</td>
<td>Edit</td>
<td>Edit Encryptor Users</td>
<td></td>
</tr>
<tr>
<td>Encryptor Users</td>
<td>Activate</td>
<td>Activate Encryptor Users</td>
<td></td>
</tr>
<tr>
<td>Encryptor Groups</td>
<td>Create</td>
<td>Create Encryptor Groups</td>
<td></td>
</tr>
<tr>
<td>Encryptor Groups</td>
<td>Modify</td>
<td>Modify Encryptor Groups</td>
<td></td>
</tr>
<tr>
<td>Encryptor Groups</td>
<td>View</td>
<td>View Encryptor Groups</td>
<td></td>
</tr>
<tr>
<td>Encryptor Groups</td>
<td>Activate</td>
<td>Activate Encryptor Groups</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Decryptor</th>
<th>Function</th>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decryptor Users</td>
<td>View</td>
<td>View Decryptor Users</td>
<td></td>
</tr>
<tr>
<td>Decryptor Users</td>
<td>Create</td>
<td>Add Decryptor Users</td>
<td></td>
</tr>
</tbody>
</table>
### Decryptor Groups

<table>
<thead>
<tr>
<th>Function</th>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decryptor Users</td>
<td>Edit</td>
<td>Edit Decryptor Users</td>
</tr>
<tr>
<td>Decryptor Groups</td>
<td>View</td>
<td>View Decryptor Groups</td>
</tr>
<tr>
<td>Decryptor Groups</td>
<td>Create</td>
<td>Create Decryptor Groups</td>
</tr>
<tr>
<td>Decryptor Groups</td>
<td>Edit</td>
<td>Edit Decryptor Groups</td>
</tr>
<tr>
<td>Decryptor Departments</td>
<td>View</td>
<td>View Decryptor Departments</td>
</tr>
<tr>
<td>Decryptor Departments</td>
<td>Create</td>
<td>Create Decryptor Departments</td>
</tr>
<tr>
<td>Decryptor Departments</td>
<td>Edit</td>
<td>Edit Decryptor Departments</td>
</tr>
</tbody>
</table>

### Settings

<table>
<thead>
<tr>
<th>Function</th>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Settings</td>
<td>Edit</td>
<td>Edit Local Settings</td>
</tr>
<tr>
<td>Global Settings</td>
<td>Edit</td>
<td>Edit Global Settings</td>
</tr>
<tr>
<td>Personal Details</td>
<td>Edit</td>
<td>Edit Personal Details</td>
</tr>
</tbody>
</table>

### Reporting

<table>
<thead>
<tr>
<th>Function</th>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting</td>
<td>View</td>
<td>View Audit Reports</td>
</tr>
<tr>
<td>Reporting</td>
<td>Export</td>
<td>Export Audit Reports</td>
</tr>
</tbody>
</table>
17.8 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

To Add User:

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

To Remove User:

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

To Remove All Users:

- Click Remove All
- Click Ok
18 Decryptor Users

Every person who uses MediaSeal Decryptor Client will sign up for a MediaSeal Account. In order to protect content for that person, it is necessary to import that person into your Studio Server via MediaSeal Encryptor Client.

18.1 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 Decryptor 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
TO ADD A DECRYPTOR USER

- Tick the Decryptor User

TO REMOVE A DECRYPTOR USER

- Untick the Decryptor User

  - Click Save

To clear the search field and retrieve all users, click the clear button.

18.2 DELETE DECRYPTOR USERS

To delete Decryptor Users from your Studio:

- Click on the Decryptor Users Section
- Tick the Decryptor Users to remove
- Click Delete button
18.3 Activate Decryptor User

To Activate a Decryptor Users from your Studio

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

18.4 Deactivate Decryptor User

To Deactivate a Decryptor Users from your Studio

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

You can group Decryptor users in 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 for allowing and revoking permissions when using Server authentication.

19.1 Create Decryptor Group

To create a new Decryptor Group:

- Click on the Decryptor Groups section
- Click New
- Enter a Name and Description
- Click Ok
19.2 Edit Decryptor Group

To edit an Decryptor Group:

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

19.3 Manage Members of an 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
**20 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 for allowing and revoking permissions when using Server authentication.

**20.1 Create Decryptor Department**

To create a new Decryptor Department:

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

**20.2 Edit Decryptor Department**

To edit an Decryptor Department:

- Click the department in the list, so the department is highlighted.
- Click *Edit*
- Modify the required fields.
- Click *Ok*
20.3 Manage Members of a Decryptor Department

To add members to a Decryptor Department:

- Click the department in the list, so the department is highlighted.
- Click Edit
- Tick the Decryptor Users you wish to Add
- Untick the Decryptor Users you wish to Remove
- Click Ok
21 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.

21.1 Create Title

To create a Title:

- Click on the Titles Section
- Click on New
- Enter Name and Description.
- Verify Active (see note to deactivate*)
- Click Ok

*By default, new titles are Active, to make the new title de-active untick the active checkbox. Alternatively see the Deactivate Title section
21.2 Edit Title

To edit a Title:

- Click the title in the list, so the title is highlighted.
- Click Edit
- Modify the required fields.
- Click Ok

21.3 Delete Title

To delete a Title:

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

21.4 Activate Title

To activate a Title:

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

To deactivate a Title:

- Check the checkbox of the Title to deactivate
- Click Deactivate
- Click Yes to confirm deactivating the Title
21.6 Manage Title Permissions

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

- Click the title in the list, so the title is highlighted.
- Click Edit

Add User or Group

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

To Remove User or Group

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

- Click *Remove All*

- Click *Ok*
22 Jobs

The jobs section is the main work activity section where MediaSeal Content Protection jobs and templates can be created.

22.1 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.

Search

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

To search:

- Type in the search box
**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. Use the **Show My Jobs Only**, **Show My Templates Only** or **Show My Archive Jobs** checkbox respectively.

### 22.2 Create Job

#### 22.2.1 Description Tab

To create a new Job:

- **Click the Jobs section**
- **Click New**
- **In the Description Tab enter the required details**
- **Click Next**
Please see the **Authentication Types** section for more information on authentication types.

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

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

### 22.2.1.1 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.

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Factor Level</th>
<th>MediaSeal Authentication</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Factor Authentication</td>
<td>Password Only</td>
<td>MediaSeal Decryptor Client</td>
<td></td>
</tr>
</tbody>
</table>
22.2.1.2 **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.*

*Please note* Using the Secure Playback option requires a Key-Server update and Decryptor clients to be running version 3.8.1 or above.

22.2.1.3 **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.

22.2.1.4 **Advanced Options**
22.2.1.4.1 Re-Authenticate Every [x] Hours

This allows the content 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.

22.2.1.4.2 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.*

**22.2.2 Source Tab**

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

To add source files:

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

To add source folders:
22.2.2.1 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.

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.*

22.2.3 Destination Tab

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

*Please note: The source content will remain unaffected and will not be removed or modified*

To select a new destination:

- Click Choose New
- Select an output folder
To select the most recent output destination:

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

To use source directory:

- Click Use Source

To remove recent output destinations:

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

To manually create a folder:

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

### 22.2.4 Viewers Tab

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

To add the User, Group or Department

- Click on the Name in the left column
To remove the User, Group or Department

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

To Remove all Users, Groups and Departments

- Click Remove All

### 22.2.5 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.

To edit content controls:

- Tick the default, user, group or department to modify
- Click Edit
- Modify fields as required.
22.2.6 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 content owner of the file.

To set the contact details:

- Complete Contact Name and Contact Number

22.2.7 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.

To save as a template:

- Tick Save as Template checkbox
IF THE FOLLOWING MESSAGE IS DisplayED:

Creating Job.....

Success:
You are now ready to start the encryption process. The "Save as Template" check box enables you to save the job as a template.

• You can click Start Job

IF THE FOLLOWING MESSAGE IS DisplayED:

Creating Job.....

Error:
You cannot proceed with the encryption as there is a problem in one of the previous steps. Please go back to the 'Description' tab and click 'Next' through all of the stages to find what was missed.

• Please check each of the tabs for any missing elements.

22.3 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:
FOCUS SUPPORT VISIT: mediaseal.fortiumtech.com

- Click the Job in the list, highlighting the job to duplicate
- Click Duplicate
- Set Source and Destination
- Amend details as Required
- Click Start Job

22.4 Edit Job

You can edit an existing job, this allows you to make changes to the job including change passwords, assign or revoke permissions when using server authentication and modify content controls.

**Not all fields can be modified**

To edit a job:

- Click the Job in the list, highlighting the job to duplicate
- Click Edit
- Amend details as Required
- Click Update Job from the Summary Tab
22.5 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.

To edit a job:

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

22.6 Archive Job

Jobs that cannot be deleted, or jobs that are no longer relevant can be archived.

To archive a job:

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

The job will be moved and accessible in the Archived Jobs Tab

To un-archive a job:
22.7 Delete Job

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

To delete a job:

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

23.1 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.

To create a template:

- Click the Jobs Section
- Click Templates Tab
- Click New Template
- Enter the required configuration
- Click Save
23.2 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.

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
23.3 EXPORT TEMPLATE

The export template is primarily 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.

To export a template:

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

For information on using the Job XML Template, please see the Command Line section.
23.4 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.

To create a shortcut:

- Click the template in the list, highlighting the template
- 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.

23.5 Delete Template

To delete a template:

To edit a job:

- Click the Job in the list, highlighting the job to duplicate
- Click Delete
**24 Verify**

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.

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.
25 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)

To upload audit logs:

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

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

Accurate Decryptor User Audit Data is dependent on either Server + Multi Factor Authentication (Password, iLok and Server), or Uploading MediaSeal Decryptor Client User Audit Data. See the **Uploading Audit Logs** section for more information on uploading MediaSeal Decryptor Client user 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.
### 26.1 Viewing Audit Data

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

To view audit data:

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

#### Audit Types:

<table>
<thead>
<tr>
<th>Decryptor User Audit Types</th>
<th>Audit Type:</th>
<th>Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attempted to access a file</td>
<td>An attempt was made to access a file</td>
<td></td>
</tr>
<tr>
<td>Was denied access to a file</td>
<td>Access to a file was denied</td>
<td></td>
</tr>
<tr>
<td>Was granted access to a file</td>
<td>Access to a file was granted</td>
<td></td>
</tr>
<tr>
<td>Save file having open assets</td>
<td>A file was saved whilst protected content was open</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encryptor User Audit Types</th>
<th>Audit Type:</th>
<th>Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attempted to login</td>
<td>An attempt was made to login</td>
<td></td>
</tr>
<tr>
<td>Was denied a login</td>
<td>Login attempt was denied</td>
<td></td>
</tr>
<tr>
<td>Was granted a login</td>
<td>Login attempt was successful</td>
<td></td>
</tr>
<tr>
<td>Created a new entry</td>
<td>A new entity was created</td>
<td></td>
</tr>
<tr>
<td>Updated an existing entity</td>
<td>An entity was updated</td>
<td></td>
</tr>
<tr>
<td>Deleted an existing entity</td>
<td>An entity was deleted</td>
<td></td>
</tr>
</tbody>
</table>

#### 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.

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.

<table>
<thead>
<tr>
<th>Decryptor User Filters</th>
<th>Filter Type:</th>
<th>Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>The name of the file</td>
<td></td>
</tr>
<tr>
<td>File Id</td>
<td>The File Id of the file</td>
<td></td>
</tr>
<tr>
<td>Machine Name</td>
<td>The hostname of the machine</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the machine</td>
<td></td>
</tr>
<tr>
<td>MAC Address</td>
<td>The network MAC Address of the machine</td>
<td></td>
</tr>
<tr>
<td>Host User Name</td>
<td>The username used on the machine</td>
<td></td>
</tr>
</tbody>
</table>
26.2 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.
27 Command Line

27.1 Command Line Options

The MediaSeal Encryptor Client Command line switches offer the ability to run the MediaSeal Encryptor Client using the command line.

You must have administrative permissions to run Encryptor from the Command Line

You can display the help by passing the command line switch –help or -h to the Decryptor Client

- Type Encryptor --help

Please note the help menu does not show for the Windows platform
### Options:

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-?, -h, --help</td>
<td>Displays this help.</td>
</tr>
<tr>
<td>-c, --commandline &lt;jobXmlFile&gt;</td>
<td>Job Template XML File</td>
</tr>
<tr>
<td>-l, --list</td>
<td>Get a list of groups and studio users for the job template file.</td>
</tr>
<tr>
<td>-u, --username &lt;username&gt;</td>
<td>Username</td>
</tr>
<tr>
<td>-p, --password &lt;password&gt;</td>
<td>Password</td>
</tr>
<tr>
<td>-o, --output &lt;OutputStatusFile&gt;</td>
<td>Operation status file output</td>
</tr>
<tr>
<td>-s, --screenoutput</td>
<td>Display output on Screen Dialog</td>
</tr>
<tr>
<td>--id, --templateid &lt;templateid&gt;</td>
<td>Commandline run template id</td>
</tr>
<tr>
<td>--n, --templatejobname &lt;templatejobname&gt;</td>
<td>Commandline run job name</td>
</tr>
<tr>
<td>--opath, --outputpath &lt;opath&gt;</td>
<td>Commandline run output path</td>
</tr>
<tr>
<td>-q, --autoquit</td>
<td>Commandline to automatically quit on complete</td>
</tr>
<tr>
<td>-m, --allow-multiple-instances</td>
<td>Allow multiple instances of the Encryptor</td>
</tr>
</tbody>
</table>

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

#### 27.1.1 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.

#### 27.1.2 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.
27.1.3 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.

27.1.4 Multiple Instances

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

27.1.5 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.
27.1.6 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.

27.1.7 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.

27.1.8 Command Line Encryptor (Windows)

An example of running MediaSeal Encryptor Client command line:

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

27.1.9 Command Line Encryptor (MacOS)

An example of running MediaSeal Encryptor Client command line:
Command Line Error Codes

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

<table>
<thead>
<tr>
<th>Result Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Success</td>
</tr>
<tr>
<td>1</td>
<td>Command line parameter error</td>
</tr>
<tr>
<td>2</td>
<td>Connection error</td>
</tr>
<tr>
<td>3</td>
<td>Login error</td>
</tr>
<tr>
<td>4</td>
<td>Error opening or reading task file</td>
</tr>
<tr>
<td>5</td>
<td>Error opening or updating status file</td>
</tr>
<tr>
<td>6</td>
<td>Error during encryption process</td>
</tr>
</tbody>
</table>

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 the following command to view the result of the last operation:

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

**Windows**

- Type `echo %errorlevel%` and hit Enter
MacOS

- Type `echo $?` and hit Enter

27.2 Command Line XML Files

27.2.1 Create Job Using XML Template File

XML configuration files are a convenient method of passing template information to the Encryptor command line. To create a job from the command line using an XML Template file:

- Export the template to a file to get the basic template xml

To export a template to an xml file, please see the Export Template section. See below for an example of an exported template:

```xml
<EncryptionJob>
  <CreateJobData>
    <JobName></JobName>
    <OutputDirectoryPath></OutputDirectoryPath>
    <SourceFilePathList/>
    <TemplateId>1</TemplateId>
  </CreateJobData>
</EncryptionJob>
```
Modify the XML File: first, enter a job name `<JobName>new job</JobName>`

Enter an output directory `<OutputDirectoryPath>c:\output</OutputDirectoryPath>`

To encrypt a single file, add the full path of the file
`<SourceFilePathList>C:/the/path/to/the/input.avi</SourceFilePathList>`

To encrypt multiple files, add each file as a list item `<SourceFilePathList>`
`<listitem>C:/path/to/file1.mov</listitem> <listitem>C:/path/to/file2.avi</listitem> </SourceFilePathList>`

```xml
<?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>
```

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

```
START /WAIT "C:\Program Files (x86)\MediaSeal\Encryptor\Encryptor.exe" -c C:/Users/testuser/testinput.xml -u user1 -p password -o C:/Users/testuser/testStatus.xml
```
An example of running the command on macOS from terminal, assuming the application bundle is in /Applications, you can use the following syntax:

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

### 27.2.2 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.

If the --output (-o) option was specified:

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

**N.B.**

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.

The status file is XML with the following format:
<xml version="1.0" encoding="UTF-8"?>
<Status>
  <StatusFileData>
    <DataRate>20</DataRate>
    <FileBeingEncrypted>C:/Users/Public/Videos/Sample Videos/testfile1.avi</FileBeingEncrypted>
    <LogEntry>
      <listItem>Starting job processing: Thu 6. Feb 15:18:41 2014</listItem>
      <listItem>initialising log</listItem>
      <listItem>Starting encryption of 1 files</listItem>
      <listItem>Starting encryption of file: C:/Videos/Sample Videos/commandline/b2465feb-c54d-43c6-abc4-384e563e6590-testfile1.avi</listItem>
      <listItem>Finished encrypting file</listItem>
      <listItem>Finished encryption of all file(s)</listItem>
    </LogEntry>
    <TaskProgress>100</TaskProgress>
    <TotalProgress>100</TotalProgress>
  </StatusFileData>
</Status>

**If the --output ( -o ) command line option was 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.
27.2.3 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 the changes. e.g. Encryptor.exe -c changeusers.xml -u user1 -p password

- Using the template below, modify the GroupId, UserId and OperationType as required.

Supported Operation Types: [ADD] [REMOVE]

```xml
<?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>
```
27.3 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

27.3.1 Drag and Drop File Protection (Windows)

To create a shortcut on Windows:

- On the Desktop right click and Select New, Shortcut
- Click Browse and select Encryptor.exe from the MediaSeal Encryptor Client installation directory
- Append the required commands e.g. "C:\Program Files (x86)\MediaSeal\Encryptor\Encryptor.exe" -u myusername -p mypassword –screenoutput –autoquit –templateid 34 –templatejobname Test1 –output c:\Users\User1\n- Click Next, type a Name for the shortcut, then click Finish

If you drag and drop files onto this shortcut, it will run a job to protect the files.
27.3.2 Drag and Drop File Protection (MacOS)

To create an Automator Task on MacOS:

- 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 e.g.

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

- Select File, Save.
If you drag and drop files onto this Automator, it will run a job to protect the files.
28 Troubleshooting

28.1 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.

(Beware of copying and pasting passwords as they may include additional hidden characters)

28.2 Advanced Troubleshooting

For advanced troubleshooting, the latest information and tutorials, please visit the MediaSeal Support Portal. If you still require further assistance, please email the MediaSeal Support Team support@mediaseal.com

MediaSeal Support Portal
https://mediaseal.fortiumtech.com