IMiS®/wClient Manual

Version 1.1.1805

IMAGING SYSTEMS

Imaging Systems Inc.
Brnciceva 41 G
Ljubljana
Slovenia

TABLE OF CONTENTS

1 PREFACE 8
1.1 About the manual 8
1.2 Target audience 8
1.3 Conventions 8
1.4 Terms and abbreviations 9
2 INTRODUCTION 12
2.1 Features 12
2.2 Versioning and numbering 13
2.3 Functionalities 14
3 TECHNICAL DOCUMENTATION 15
3.1 Client architecture 15
4 USER MANUAL 16
4.1 Login and Logout 16
4.1.1 Cookie Policy 17
4.1.2 Localization 18
4.2 Interface description 18
4.2.1 Classification scheme 21
4.2.2 List of entities 23
4.2.3 Menu functions 25
4.2.4 Command bar 28
4.2.5 Entity information 28
4.3 Actions 37
4.3.1 Entity access 37
4.3.2 Creating an entity 38
4.3.3 Editing entity data 52
4.3.4 Content management 63
4.3.5 Search functions 74
4.3.6 Archiving email messages 87
4.3.7 Acquiring authenticity evidence 93
4.3.8 Deletion of an entity 96
4.4 System attributes 97
4.4.1 General system attributes 98
4.4.2 Email attributes 100
4.4.3 Physical content attributes 100
4.5 Roles 101
5 SYSTEM REQUIREMENTS 101
5.1 Hardware 101
5.1.1 Minimum requirements 102
5.1.2 Recommended hardware 102

2018 © Imaging Systems Inc., All rights reserved.

5.2 Installation requirements 102
5.2.1 Minimum requirements 102
5.2.2 Recommended requirements 103
6 INSTALLATION 103
6.1 Installation procedure 103
6.1.1 Installation settings 103
6.2 Upgrade procedure 104
7 MANAGING PRODUCT 104
8 TROUBLESHOOTING 104
8.1 How to avoid problems 104
8.2 Frequent errors 105

TABLE OF IMAGES

Table of images appearing in the manual

Image 2: Client architecture 15
Image 3: Login on archive 16
Image 4: Log out of the archive 16
Image 5: Cookie Policy 17
Image 6: User interface of the IMiS®/wClient 18
Image 7: Categories in the left view 19
Image 8: A list of entities 19
Image 9: Entity information 20
Image 10: Display of the command bar 20
Image 11: Header of the user interface of the IMiS®/wClient module 21
Image 12: Display of the entity's hierarchical position within the tree structure 21
Image 13: Display of the tree view of the classification scheme in the »Archive« folder 22
Image 14: Selecting the »Directory« folder in the left view 23
Image 15: Selecting the »My entities« folder in the left view 23
Image 16: A list of contained entities of the selected entity 24
Image 17: Selecting the order of displaying the list of entities 24
Image 18: Popup menu in the right part of the header of the user interface 25
Image 19: Display of the window with user details 26
Image 20: Display of the window for changing the user password 26
Image 21: About dialog box 27
Image 22: Selecting the display of entities in a grid 27
Image 23: Command bar above the information of the selected entity 28
Image 24: Tabs containing entity information in the preview/reading mode 29
Image 25: Preview mode display of the »Details« tab 30
Image 26: Reading mode display of the »Details« tab 31

2018 © Imaging Systems Inc., All rights reserved.

Image 27: Drop-down menu on the selected content in the reading mode 32
Image 28: A list of users/groups with access rights to the entity in the preview and reading mode 32
Image 29: A list of effective permissions for the selected user in the preview and reading mode 33
Image 30: Preview and reading mode display of the »Retention« tab 34
Image 31: Dialog box with the information on disposition hold 35
Image 32: Dialog box with the information on retention policy 35
Image 33: The »Activity« tab in the preview and reading mode 36
Image 34: User information 36
Image 35: Display of contained entities. 39
Image 36: Display of creating a new folder 40
Image 37: Entry of required metadata 41
Image 38: Entry of text metadata 41
Image 39: Entry of date and time metadata 41
Image 40: Entry of metadata with predefined values 41
Image 41: Entry of multiple value metadata 42
Image 42: Selecting the type of classification code entry for the class of the contained entity 42
Image 43: Manual entry of a child entity's classification code 43
Image 44: Display of manually entered classification code 43
Image 45: Specifying the security class of a new entity 44
Image 46: Changing the security class of the entity 44
Image 47: Entering the security class of the entity with an inherited value 45
Image 48: Entity information after entering the security class 46
Image 49: Specifying the status of a new entity 47
Image 50: Changing the status of an entity 47
Image 51: Display of the entry of physical content metadata 48
Image 52: Display of the »Retention« tab 49
Image 53: Display of changing retention periods 49
Image 54: Saving a new or modified entity 50
Image 55: Example classification code 50
Image 56: Example creator of entity 51
Image 57: Example date and time an entity was opened 51
Image 58: Example date and time an entity was closed 51
Image 59: Example date and time an entity was created 51
Image 60: Example date and time of last changes to the entity 51
Image 61: Example date and time of last access to the entity 51
Image 62: Example entity identifier 52
Image 63: Attribute values in editing mode 52
Image 64: Entering the values of custom attributes in editing mode 53

2018 © Imaging Systems Inc., All rights reserved.

Image 65: Information on the entity that contains custom attributes 53
Image 66: Display of entering physical content metadata 54
Image 67: Popup menu for selecting the status of the physical content 55
Image 68: »Security« tab in editing mode 56
Image 69: List of users with access rights to the entity 56
Image 70: List of editing permissions 57
Image 71: Popup menu for selecting access rights to a selected metadata 57
Image 72: List of user permissions on the selected metadata 58
Image 73: The »Retention policy« tab in editing mode 59
Image 74: Selecting validity for a specific type of entity 59
Image 75: The record of retention period with the removal option 60
Image 76: The »Disposition hold« tab in editing mode 60
Image 77: The popup menu for selecting the »Status« command 61
Image 78: Selecting the status and giving the reason for the change 61
Image 79: The popup menu for selecting the »Security class« command 62
Image 80: Selecting the security class and giving the reason for the change 62
Image 81: Display of the list of contents in the central view 64
Image 82: The »Content« field for dropping contents 64
Image 83: The added content before saving 64
Image 84: The added content after saving 65
Image 85: Content details in the right view 66
Image 86: An example of the content type of a document 66
Image 87: An example of the date of creating the document content 66
Image 88: An example of the date of modifying the document content 66
Image 89: An example of the date of the last access to the document content 66
Image 90: An example of the document content identifier 67
Image 91: An example of a display of indexed document content 67
Image 92: An example of a display of signed document content 67
Image 93: Opening document content 67
Image 94: The selected content before update 68
Image 95: Selecting the »Update« command in the popup menu 68
Image 96: The selected content after update 69
Image 97: Selecting the »Download« command in the popup menu 69
Image 98: Selecting the »Move« command in the popup menu 70
Image 99: Selecting the target document for moving content 70
Image 100: Content temporarily removed from the document 71
Image 101: Saved document content 71
Image 102: The content on the list before deletion 72
Image 103: The content on the list after deletion 72
Image 104: Selecting the »Queue for Indexing« command 73
Image 105: Successful adding of content for indexing 73

2018 © Imaging Systems Inc., All rights reserved.

Image 106: Selecting the »Queue for Conversion« command....74
Image 107: Successful tagging of content for later conversion....74
Image 108: Entering a search string in the »Search« field....75
Image 109: A full text search result....75
Image 110: Entering a search string in the »Full text search« field....76
Image 111: A wildcard search by using special characters....76
Image 112: Searching using operators....77
Image 113: An example of a search result....78
Image 114: A dialog box for searching by metadata....79
Image 115: An example of a metadata search result....79
Image 116: Use of special characters in a search string....80
Image 117: An example of a result of searching by metadata using special characters....80
Image 118: A dialog box for searching by the metadata »Owner«....81
Image 119: A dialog box for searching by the content description....82
Image 120: Use of special characters in a search string....83
Image 121: Results of searching by the document contents description....84
Image 122: Entering a search string in a combined search....85
Image 123: Results of searching by metadata and the text of the content....85
Image 124: Entering a search string when searching by metadata and the content description....86
Image 125: Results of searching by metadata and the content description....86
Image 126: Entering a search string when searching by the text of the content and the content description....87
Image 127: Displaying the result of searching by the text of the content and the content description....87
Image 128: Preparing the environment for transferring an email message from the email client to the archive....88
Image 129: Dropping the email message to the selected entity....89
Image 130: Viewing and editing the details of an email message before saving....89
Image 131: Displaying a saved email message on the list of entities....91
Image 132: Contents of the email message....91
Image 133: Display of the metadata transferred from the email message....92
Image 134: The popup menu for selecting the »Authenticity evidence« command....93
Image 135: Selecting the folder for saving the directory with the two files containing authenticity evidence....93
Image 136: Example archive information package....94
Image 137: Example evidence record....96
Image 138: Selecting the »Delete« command....96
Image 139: A dialog box for deleting an entity....97
Image 140: An example of the error: Invalid or incorrect password....106
Image 141: An example of an error when saving a new folder....106

2018 © Imaging Systems Inc., All rights reserved.

Image 142: An example of an error when editing a closed document 107
Image 143: An example of an error when opening an entity in editing mode 107

LIST OF TABLES

Below is a list of tables appearing in the manual:

Table 1: Manual font types and their meaning 8
Table 2: Definition of abbreviations 11
Table 3: List of terms used in the manual 12
Table 4: Description of possible attribute properties 98
Table 5: Description of general system attributes 100
Table 6: Description of email attributes 100
Table 7: Description of physical content attributes 101

2018 © Imaging Systems Inc., All rights reserved.

1 PREFACE

This manual describes the operation of the IMiS®/wClient software product and offers advice on the technical and operational aspects of its use.

1.1 About the manual

The manual presents the web client architecture, user interface, range of actions over entities, mechanisms for verifying authenticity, report functionalities and the installation, configuring and management procedures of the IMiS®/wClient.

1.2 Target audience

Information presented by this manual is intended for users with at least intermediate understanding of computer and application use.

1.3 Conventions

The manual employs several font types to convey information. These are explained below:

Font type	**Used to denote**
Regular	basic text, images, tables
regular bold	chapter titles (main chapters 1-6 and subchapters)
Italic	advice, examples, tips, instructions
"inside quotation marks"	titles of selectable functions, files or actions
underlined italic	see specified chapter for more information
Monospace	names of console commands, files, directories, ...
Monospace Bold	user input characters

Table 1: Manual font types and their meaning

2018 © Imaging Systems Inc., All rights reserved.

1.4 Terms and abbreviations

Abbreviations appearing in the text and images of the user manual are explained below

Abbreviation	Description
7ZIP	7-Zip open source file archiver and format (extension ».7z«)
ACL	Access Control List
AFM	Adobe Font Metrics (extension ».afm«)
AIP	Archival Information Package
ANPA	American Newspaper Publishers Association news feed format
ATOM	Atom Syndication Format
BMP	Bitmap image file format (Windows format – extension ».bmp«)
CAD	Computer Aided Design
CHM	CHM Help format (extension ».chm«)
CPIO	cpio file archiver and format (Unix format – extension ».cpio«)
CSV	Comma Separated Value (text file format– extension ».csv«)
DMS	Document Management System
DWG	CAD file format (extension ».dwg«)
ELF	Executable and Linkable Format (Linux, Unix, Mac OS X format)
EML	EML format (RFC 822 archive standard – extension ».eml«)
EPUB	Electronic Publication Format (extension ».epub«)
EXIF	Exchangeable image file format (image metadata format)
FB2	FixtionBook format (electronic book format – extension ».fb2«)
FLV	Flash Video file format (Adobe video format – extension ».flv«)
GB	Gigabyte (information unit of 2^30 or roughly 10^9 bytes)
GHz	Gigahertz (frequency unit of 10^9 hertz)
GIF	Graphics Interchange Format (image format – extension ».gif«)
HDF	Hierarchical Data Format
HTML	HyperText Markup Language
ID	Identifier
IPTC	International Press Telecommunications Council News Feed Format
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
JPEG	Joint Photographic Experts Group format (extension ».jpg«)
LDAP	Lightweight Directory Access Protocol (Internet protocol for accessing directory)

2018 © Imaging Systems Inc., All rights reserved.

Abbreviation	Description
MAT	Matlab data format
MB	Megabyte (information unit of 2^20 or roughly 10^6 bytes)
MBOX	MBox file format (Unix email archive format)
MIDI	Musical Instrument Digital Interface
MIME	Multipurpose Internet Mail Extensions (email standard)
MP3	MP3 format (audio format – extension ».mp3«)
MP4	MP4 format (video and audio format – extension ».mp4«)
NetCDF	Network Common Data Form formats
OGG	OGG format (open source format – extension ».ogg«)
PE	Portable Executable format (Win library and program format)
PDF	Portable Document Format (extension ».pdf«)
PDF/A	Portable Document Format for archiving electronic documents
PKCS7	PCKS #7 Cryptographic Message Syntax Standard
PNG	Portable Network Graphics (image format – extension ».png«)
PSD	Adobe Photoshop file format
PST	Personal Storage Table (email storage format for Windows)
RFC	Request for Comments (technical and organizational document, specification intended for the exchange of opinions on the subject)
RSA	Ronald **R**ivest, Adi **S**hamir, Leonard **A**dleman (public key encryption algorithm)
RSS	Rich Site Summary / Really Simple Syndication
RTF	Rich Text Format
S/MIME	Secure Multipurpose Internet Mail Extensions (secure MIME)
SDRAM	Synchronous Dynamic Random-access Memory
SHA	Secure Hash Algorithm (digital fingerprint algorithm)
SRP-6A	Secure Remote Password revision 6A (an encryption protocol for secure user authentication)
SSL	Secure Socket Layer (collection of cryptographic protocols)
SSO	Single Sign-on (user authentication in independent systems)
TAR	Tape Archive (Unix compression format – extension ».tar«)
TCP/IP	Transmission Control Protocol / Internet Protocol (family of network protocols)

2018 © Imaging Systems Inc., All rights reserved.

Abbreviation	Description
TIFF	Tagged Image File Format (document storage format – extension ».tif«)
TLS	Transport Layer Security
TTF	TrueType Font (Microsoft text format – extension ».ttf«)
WAV	Waveform Audio File Format (Win audio format – extension ».wav«)
W3C	World Wide Web Consortium (organization for the standardization of web techniques)
XML	Extensible Markup Language (language for structuring data in the form of a text file)
XMLDSIG	XML Signature (specification for XML encoding of electronic signatures)
ZIP	ZIP archive file format (standard archiving format – extension ».zip«)

Table 2: Definition of abbreviations

Terms used in the text and images of the manual are explained below.

Term	Description
Attribute	The attribute is the basic cell or container of metadata. It prescribes the rules and framework for the entry, maintenance and storage of metadata values belonging to an entity.
Document	The document is the basic unit of archived content on the IMiS®/ARChive Server, which can store various kinds of digital content (e.g. text, images, video). Documents are usually located inside folders, but they can also be in a class of their own.
Entity	The entity is a container of data and content on the IMiS®/ARChive Server. There are three types of entity: class, folder, and document.
Folder	Folder - a group of entities (contained folders, documents), which round off the content. It represents a dossier of the folder in question (content-related question, topic, task, project, etc.) with all of the corresponding properties and contents. For more information see chapter »Entity types« in the IMiS®/ARChive Server manual.
IMiS®/ARChive Server	IMiS®/ARChive Storage Server (archive server for document storage)
IMiS®/Scan	IMiS®/Scan client (IMiS® application for scanning paper documents)

2018 © Imaging Systems Inc., All rights reserved.

IMiS®/Storage Connector	IMiS®/Storage Connector interface (interface for the transfer of archived objects between applications and archive servers)
IMiS®/View	IMiS®/View client (IMiS® client for viewing scanned documents)
Linux	Various open source operating systems similar to Unix.
Mac OS X	Apple operating system, based on Unix.
Metadata	Metadata represents "information about information" or "data about data" that is the object of storage.
Microsoft .NET Framework	Microsoft environment for the development of web services and other software components.
Microsoft Excel	Standard MS spreadsheet software that can also be used to view CSV files.
Class	The class is the basic constituent part of content organization on the IMiS®/ARChive Server. Classes can store folders or documents, e.g. according to the type or the owner of documents stored inside.
Template	The template prescribes the metadata scheme – the required and allowed attributes for entity creation. Each template contains built-in and predefined system attributes.
Unix	A family of computer operating systems that are based on the original Unix OS developed by Bell Labs.
Windows	Microsoft operating system.
Windows Explorer	The Windows file manager application into which the IMiS®/Client is integrated.

Table 3: List of terms used in the manual

2 INTRODUCTION

2.1 Features

IMiS®/wClient is web client intended for the capture and management of content of electronic origin or content digitalized using scan procedures. The client operates directly with the IMiS®/ARChive Server, which ensures secure long-term storage of documents and archived content along with the corresponding metadata.
Users access the content from any web browser via the web client IMiS®/wClient.

Content is structured by the classification scheme, which sorts materials according to their subject, authority, activity, and the business and expert functions of corresponding personnel within the company.

2018 © Imaging Systems Inc., All rights reserved.

Entities follow a hierarchical order (classes, folders, documents), with practically unlimited sub-levels specified according to need. Each entity in the archive has its own unique classification code.

Secure authentication of a local archive user is enabled via the username and password of the user, registered in the external directory, which is synchronized with the archive server via LDAP. Secure authentication is provided by username and password, along with all the current technological means of protection from unauthorized data access.
Content security is ensured through unique identifiers (ID), which are assigned to each entity and document when it is being stored on the IMiS®/ARChive Server. The identifiers are encrypted and prevent unauthorized access, viewing or deletion.

Managing the users' access rights to entities and metadata is a key concept for ensuring the confidentiality and integrity of archived content, along with appropriate availability.
Users are limited to accessing those entities; they have been authorized to access according to the security class of the document and the security class level of the user, which are both dictated by the access control list (ACL).

The audit log records all instances of server access, along with all the events and changes performed on the server. Throughout its entire life cycle, it is impervious to modification and protected from any interventions, whether authorized or not.

One of the most practical functionalities of the electronic archive is searching by metadata or searching the full text of stored content. Users may perform search functions on the complete archive, or on any selected entity.

The IMiS®/wClient can be connected to many IMiS®/ARChive Servers,
which facilitates the capture and management of electronic content of several separate organizational units on a single location.

2.2 Versioning and numbering

The version of the IMiS®/wClient can be read from the name of the installation package, which appears according to this scheme:

IMiS.wClient.MAJOR.MINOR.RELEASE.BUILD.zip

2018 © Imaging Systems Inc., All rights reserved.

The example of installation package name:

IMiS.wClient.1.1.1805.1.zip

The scheme consists of the name of the IMiS® module (IMiS.Client) and the following elements:

- MAJOR: marks a major/central version of the IMiS® module, which changes least frequently. Changes indicate a new generation of module that introduces major functionality changes compared to the previous version. The identifier has values ranging from 1-n which grow in successive numbers.
- MINOR: marks a minor version of the IMiS® module, which changes more frequently. Changes indicate fixes and minor changes to functionalities, and fixes to the generation of module marked by the MAJOR version. The values range from 1-n, are not always successive and revert back to the base value (1) with each change of the MAJOR version.
- RELEASE: marks the release version. Unlike the other value ranges, the IMiS® module release date follows a YYMM scheme, where MM marks the release month (range 01-12) and YY marks the final two digits of the year.
- BUILD: The identifier in this position indicates the unique serial number of the product build; this number never repeats. If smaller changes are made to the product within a single month, this identifier may change. In this case, all other identifiers remain the same. The range of values is from 1 to n. This number is not continuous and can only increase.

2.3 Functionalities

The basic functionalities of the IMiS®/wClient are as follows:

- Access to any of IMiS®/ARChive Servers from any web browser.
- Secured communication with the IMiS®/ARChive Server via SSL/TLS protocol.
- Secure user authentication (SRP-6A, LDAP).
- Simple user authentication via Single Sign-on (SSO) mode.
- Access to the records according to a predetermined classification scheme.
- Entry and management of the records metadata according to a predetermined attribute scheme.
- Storage of archive materials of electronic origin or digitized using the scanner.
- Streaming-mode access to the records.

2018 © Imaging Systems Inc., All rights reserved.

- Audit log that records every operation performed over the records stored on the archive server (includes date and time, user name, name of computer, type of event, reason for action taken).
- Secure audit log viewing for authorized users.
- Search by metadata and search full text of stored content.
- Management of retention policies and disposition holds for the records.
- Support for IPv4 and IPv6 network communication systems.

3 TECHNICAL DOCUMENTATION

3.1 Client architecture

IMiS®/wClient is the user component of an electronic and physical records management system. The client connects to the web service IMiS®/Storage Connector Services REST, which uses the IMiS®/Storage Connector. The latter can be connected to many IMiS®/ARChive Servers.

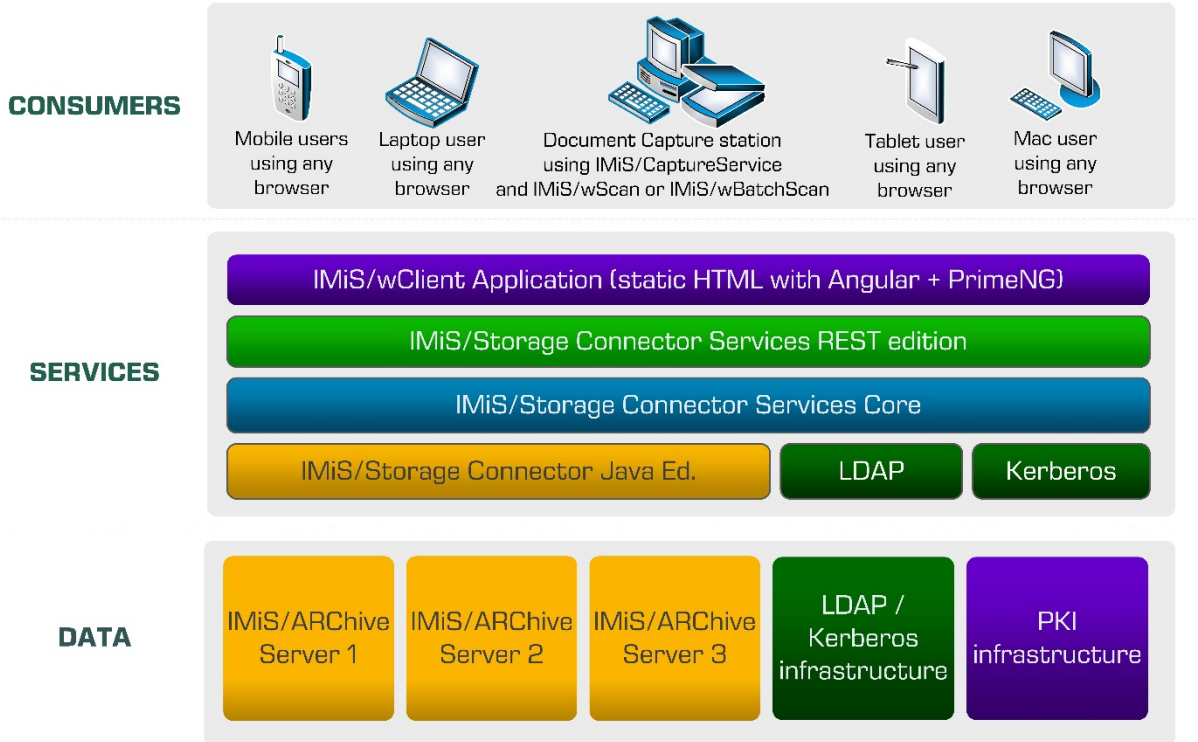

Image 1: Client architecture

2018 © Imaging Systems Inc., All rights reserved.

4 USER MANUAL

4.1 Login and Logout

The user logs in the archive of the IMiS®/ARChive Server via the IMiS®/wClient by first selecting the appropriate archive in the login window.

The user enters his username in the field »Username« and his password in the field »Password«. Confirms login with the »Log in« button.

After a successful login, the central view shows the user a list of root classes in the classification scheme of the selected archive to which the user has access rights.

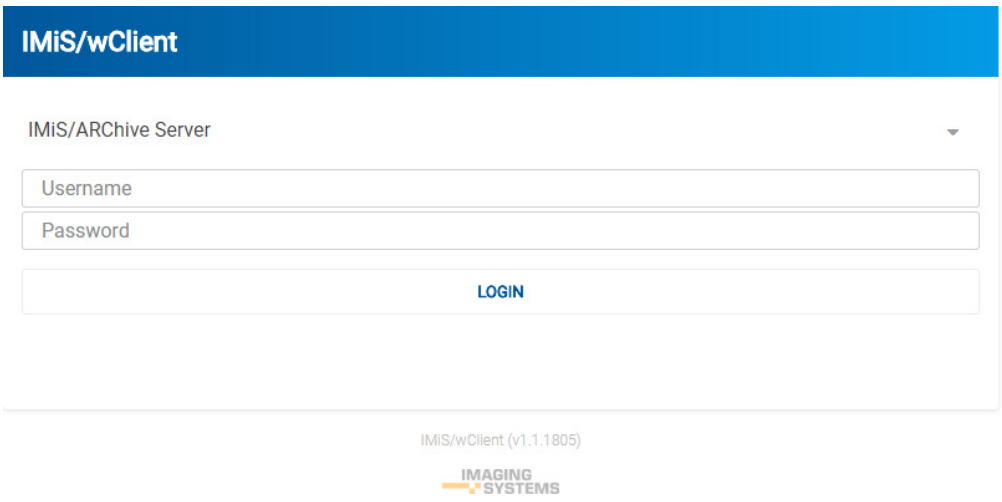

Image 2: Login on archive

Note:

The user can choose only among the archives predefined by the administrator. The administrator is the only one who can remove an archive.

The user logs out of the archive using the »Log out« command in the popup menu.

Access to the popup menu is enabled by clicking the arrow next to the user's name in the top right corner of the user interface.

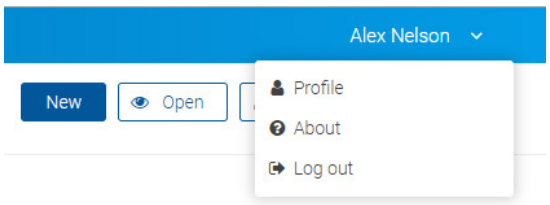

Image 3: Log out of the archive

4.1.1 Cookie Policy

Before first login on the archive and every subsequent login (if cookies have been removed) the user has to agree to the use of cookies.

To ensure proper operation and a better user experience the website uses the following cookies:

- To remember last selected archive
- Current archive user identifier
- Archive token
- Entity handles
- Entity information visibility
- Current locale
- List mode
- Policy agreed
- Classification code visibility
- Description visibility
- Sort field
- Sort field descending.

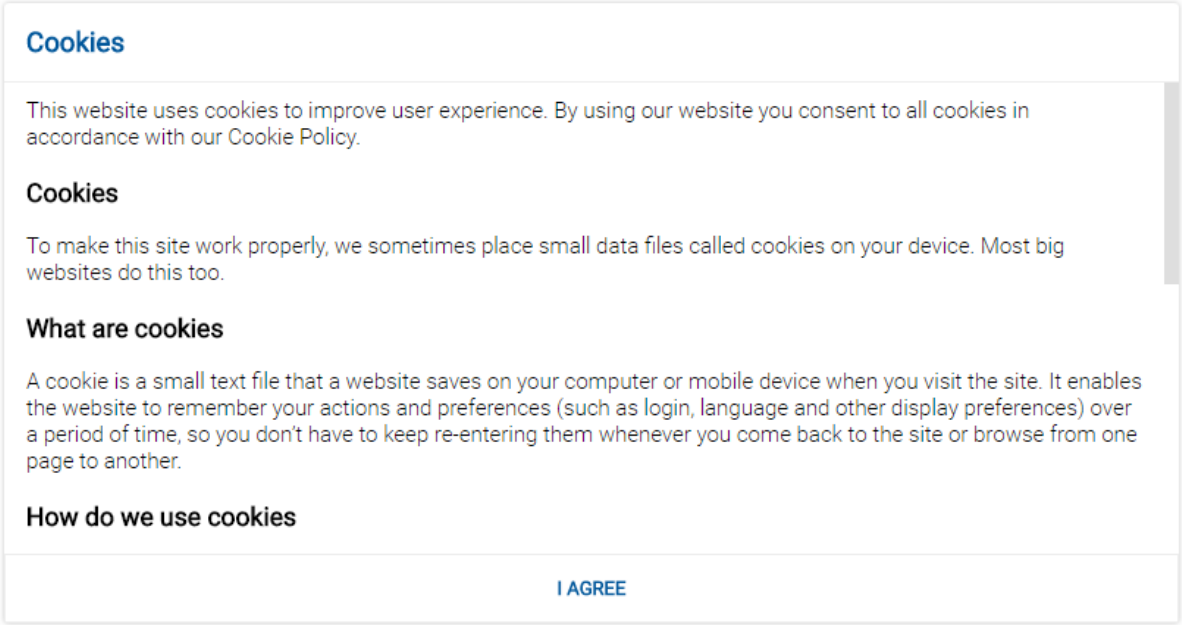

Image 4: Cookie Policy

2018 © Imaging Systems Inc., All rights reserved.

4.1.2 Localization

The user has the option to choose the language of the IMiS®/wClient above the login window. The languages currently supported are:

- English
- Slovene.

4.2 Interface description

The user interface of the IMiS®/wClient is designed in accordance with contemporary design trends. It has preserved the concept of displaying the key data on the archive records, following the example of the desktop client IMiS®/Client.

Therefore, managing the archives and entities of the electronic archive is similar to managing regular folders and files, which makes use simple and familiar. The user interface consists of six (6) main windows described below.

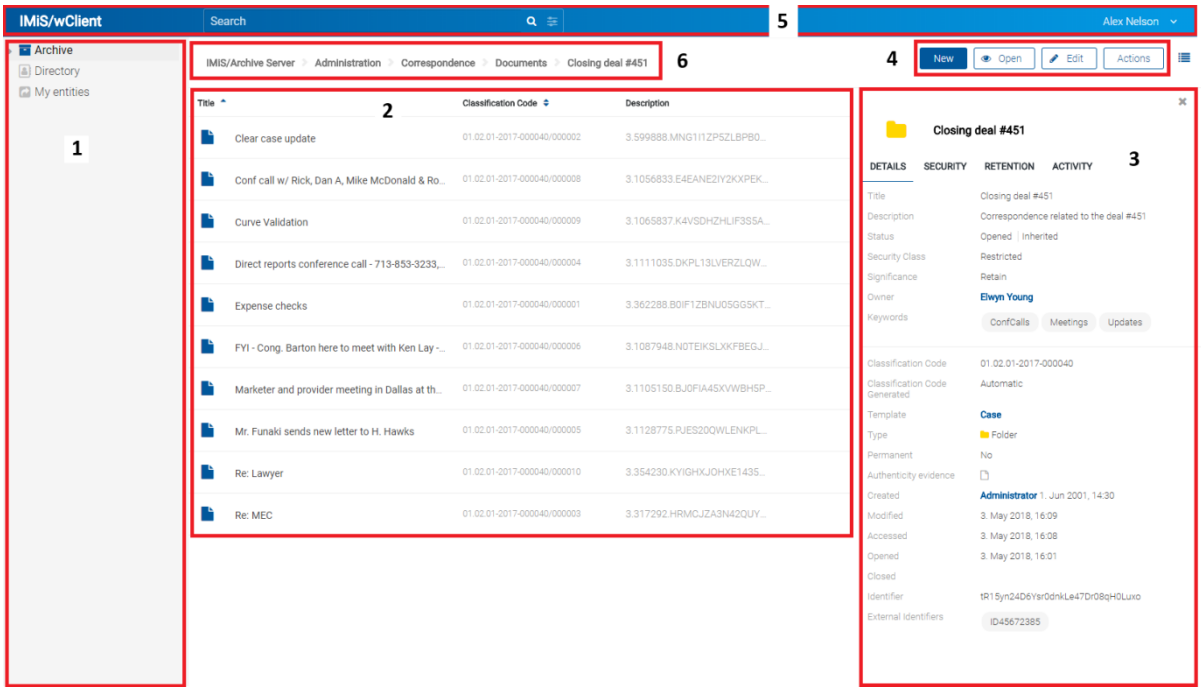

Image 5: User interface of the IMiS®/wClient

The left view of the user interface (number 1 in the image above) contains the following categories:

- Archive: root classes of the classification scheme.
- Directory: the list of users and user groups of the archive.
- My entities: the list of entities, to which the user has accessed.

2018 © Imaging Systems Inc., All rights reserved.

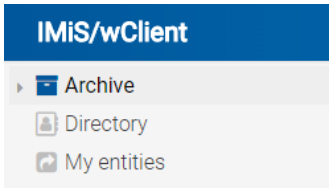

Image 6: Categories in the left view

In the central view of the user interface (number 2 in the image above) is a list of contained entities of the selected archive or class. The archive contains only classes, while the class and folder may contain folders and documents.

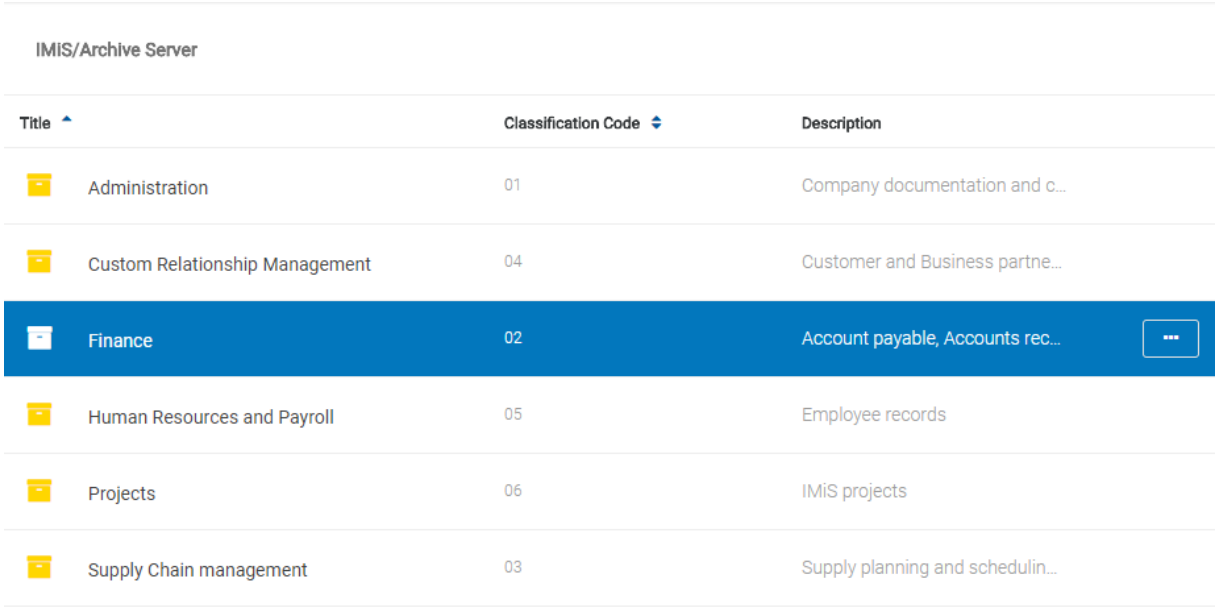

Image 7: A list of entities

The contained entities are shown below the bar with the titles of the common attributes. The »Title« is shown by default. If the user has also selected the »Classification code« and »Description« in the settings, the view also shows information on the selected entity. More on the central view in the chapter List of entities.

The right view of the user interface (number 3 in the image above) contains tabs which show different types of information on the selected entity. When viewing publicly accessible entity data, the user is generally provided public metadata on the entity in the »Details« tab and shown the user's effective rights on the entity in the »Security« tab.

2018 © Imaging Systems Inc., All rights reserved.

Users with rights have access to the display of selected retention periods and disposition holds in the »Retention« tab and of the audit log for the selected entity in the »Activity« tab.
If the user does not have the appropriate rights, the tabs are not shown.

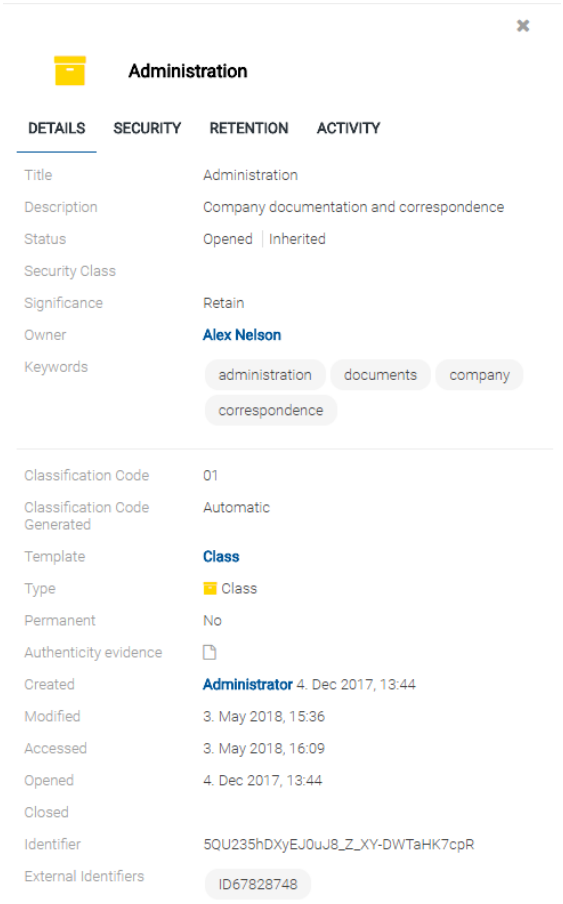

Image 8: Entity information

Note:
The default setting of the IMiS®/wClient is to always show information on the entity and content.

The command bar (number 4 in the image above) contains commands and actions.
They depend on the type and status of the element selected in the classification scheme or of the entity selected from the list of entities, and on the user's rights and role.
More on the command bar in the chapter Command bar.

Image 9: Display of the command bar

2018 © Imaging Systems Inc., All rights reserved.

Note:

If the »Archive« folder is selected, only the button for creating root classes is enabled in the command bar.

The header of the user interface (number 5 in the image above) contains:

- information on the title of the program module (IMiS®/wClient).
- a field for entering the search string with the option of selecting the search scope.
- information on the user's profile and the program module.

Image 10: Header of the user interface of the IMiS®/wClient module

To enable quicker access to entities, the user is provided a hierarchical view of the entity's position within the tree structure (number 6 in the image above) above the central view of the user interface. It enables quick access to the parent entities.

Image 11: Display of the entity's hierarchical position within the tree structure

4.2.1 Classification scheme

After logging in to the web client IMiS®/wClient, the user is shown the folders of the selected archive, a list of root entities, and basic information on the archive.

By selecting the »Archive« category in the left view, the user is shown a list of the archive's root classes.

Note:

By clicking on the arrow in front of the selected class, the user is shown a list of contained classes.

The default server setting specifies a hierarchy with a maximum of five (5) class levels.

2018 © Imaging Systems Inc., All rights reserved.

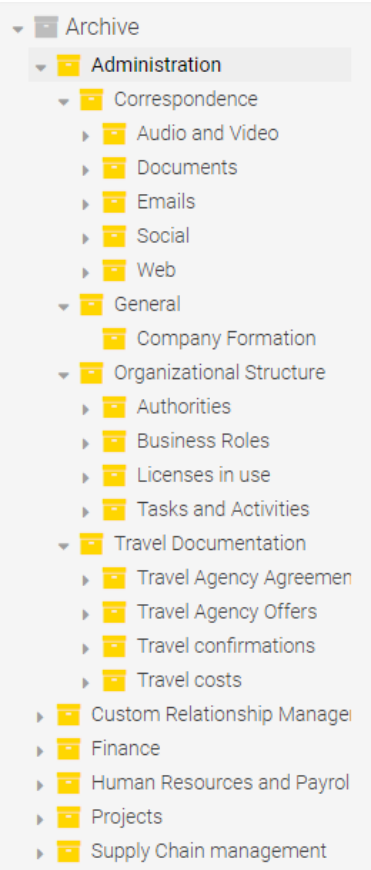

Image 12: Display of the tree view of the classification scheme in the »Archive« folder

The IMiS®/ARChive Server does not limit the number of the archive's root classes nor the number of contained classes, folders or documents in an individual class or folder.

Note:
By configuring the server, the user can limit the number of levels for classes and folders in the classification scheme.

By selecting the »Directory« category in the left view, the user is shown a list of users or groups in the central view. By selecting the »Details« command in the user record, the right view shows the user data.

2018 © Imaging Systems Inc., All rights reserved.

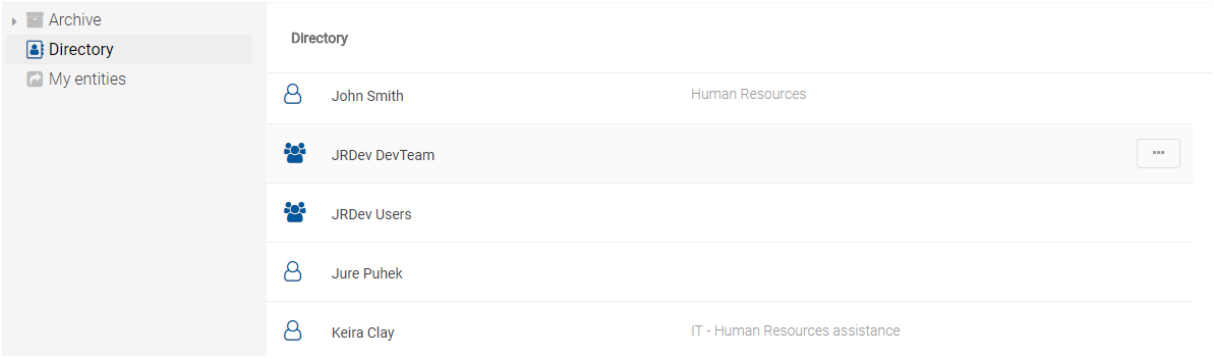

Image 13: Selecting the »Directory« folder in the left view

By selecting the »My entities« category in the left view, the user is shown a list of entities owned by the current user in the central view.

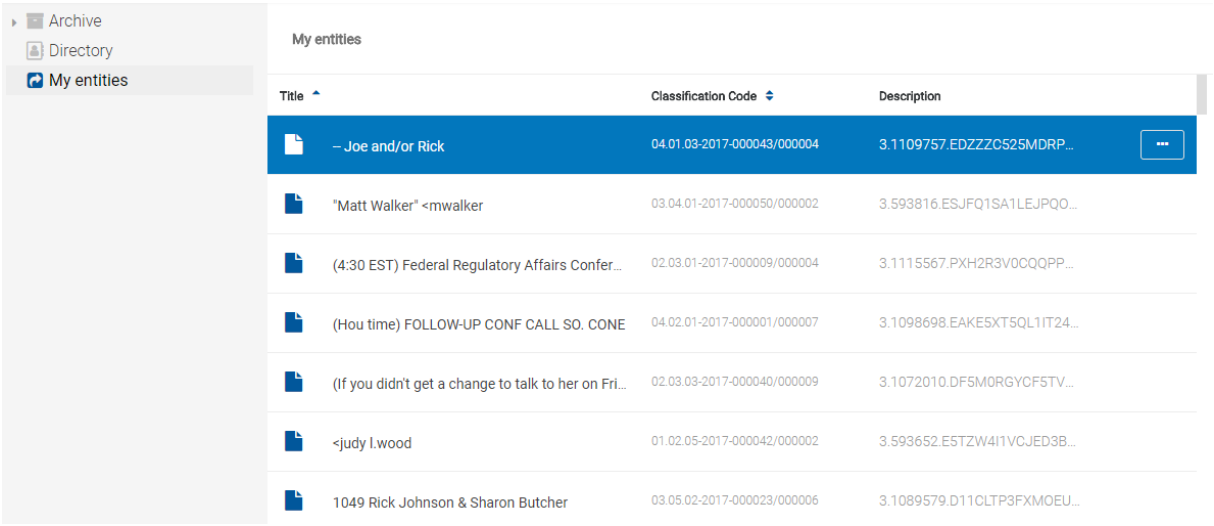

Image 14: Selecting the »My entities« folder in the left view

4.2.2 List of entities

A list of contained entities (classes, folders or documents) of the selected class is located in the central view of the user interface. The contained entities are shown below the bar with the titles of the common attributes of the contained entities.

The order of the shown attributes is predefined and is as follows:

1) Title
2) Classification code
3) Description

2018 © Imaging Systems Inc., All rights reserved.

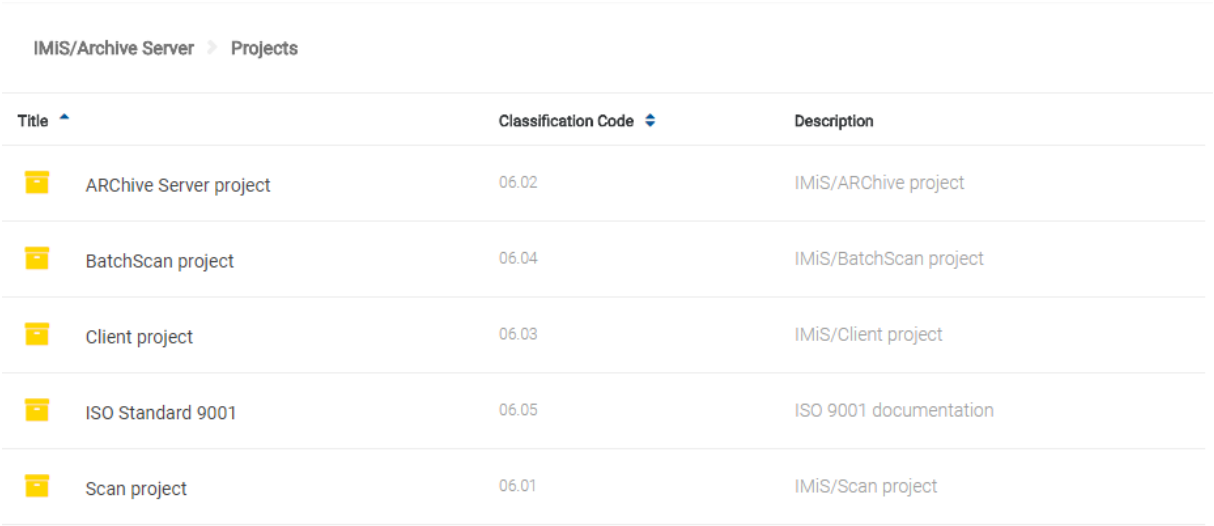

Image 15: A list of contained entities of the selected entity

The user can add or remove the columns of the selected attribute »Classification code« and/or »Description« with the icon in the command bar. The »Title« attribute is always present and cannot be removed from the list of entities.

More information on the set of available options when selecting the icon in the command bar is given in the chapter Menu functions.

By selecting the arrow or title of the column of the selected attribute, the user specifies the order of the entities shown.

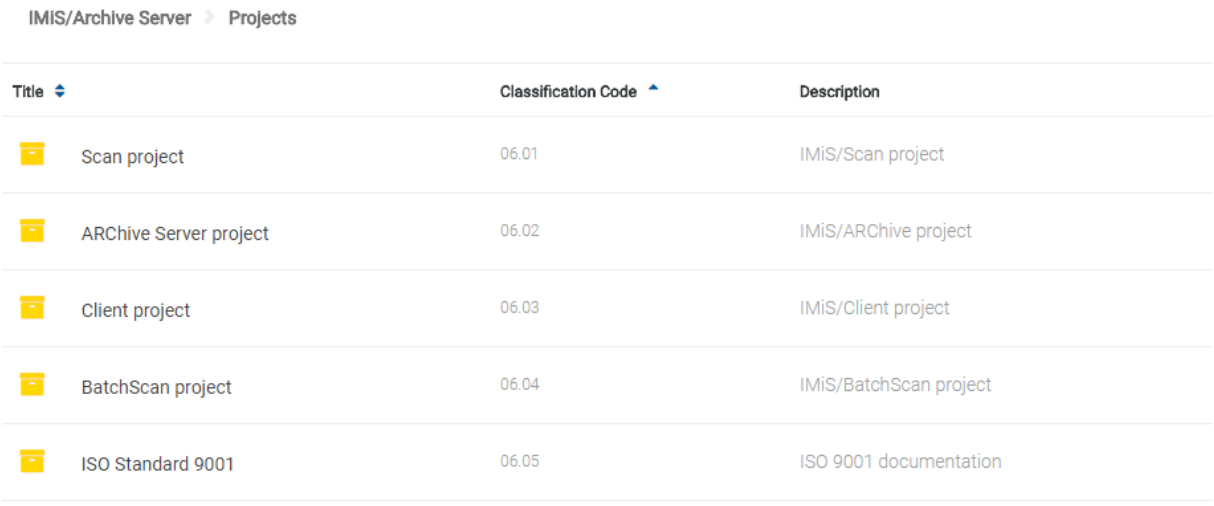

Image 16: Selecting the order of displaying the list of entities

2018 © Imaging Systems Inc., All rights reserved.

Note:

The setting of displayed attributes applies to the selected browser at the level of the entire archive for all entities shown on the list of contained entities.

Type:

In order to preserve a clear classification scheme and limit the moving of entities, users are advised AGAINST classifying documents directly into classes but always in folders.

4.2.3 Menu functions

After login on the selected archive, the following commands of the IMiS®/wClient become available by clicking on the arrow next to the user's name in the top right popup menu:

- Profile: information about the user.
- About: information about the IMiS®/wClient and license agreement.
- Log out: after logging out of the selected archive, a dialog box appears for the user to log in to the selected archive.

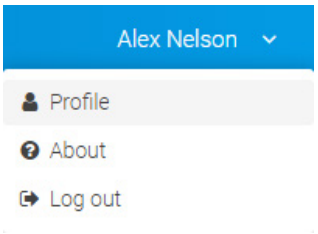

Image 17: Popup menu in the right part of the header of the user interface

4.2.3.1 Profile

By clicking on »User profile«, a notification window opens, showing the following user details:

- Description: a short description of the user.
- Type: type of user (user, group).
- First name: the first name of the user.
- Last name: the last name of the user.
- Email: the email address of the user.
- Security class level: the security class level of the user.
- Identifier: the unique identifier of the user.

2018 © Imaging Systems Inc., All rights reserved.

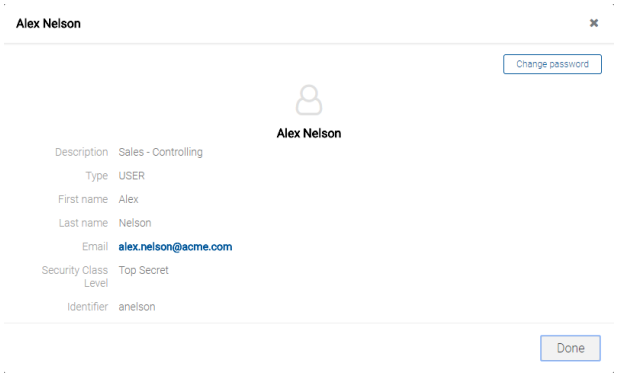

Image 18: Display of the window with user details

By clicking on the »Change password« button in the top right of the window, the user is shown a dialog box for entering the existing and new user password.

The user confirms the change of password with the »Change password« button.

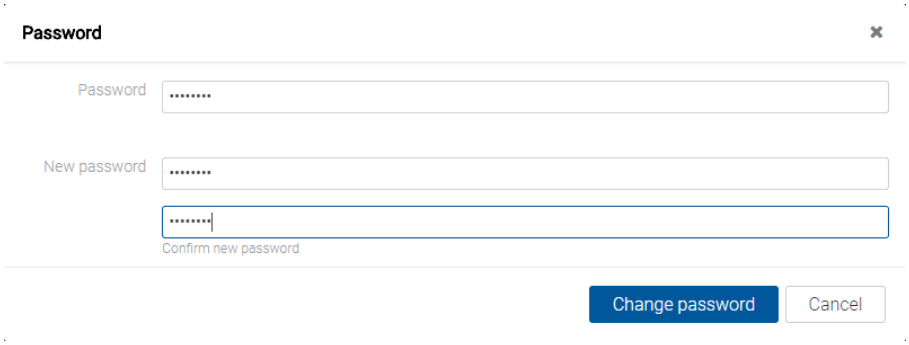

Image 19: Display of the window for changing the user password

4.2.3.2 About

By selecting the »About« command, the user is shown a new window with the following information:

- IMiS® module name.
- IMiS® module version.
- Archive name and version.
- IMiS®/StorageConnector Services REST version.
- License Agreement.
- Notices and Trademarks.

2018 © Imaging Systems Inc., All rights reserved.

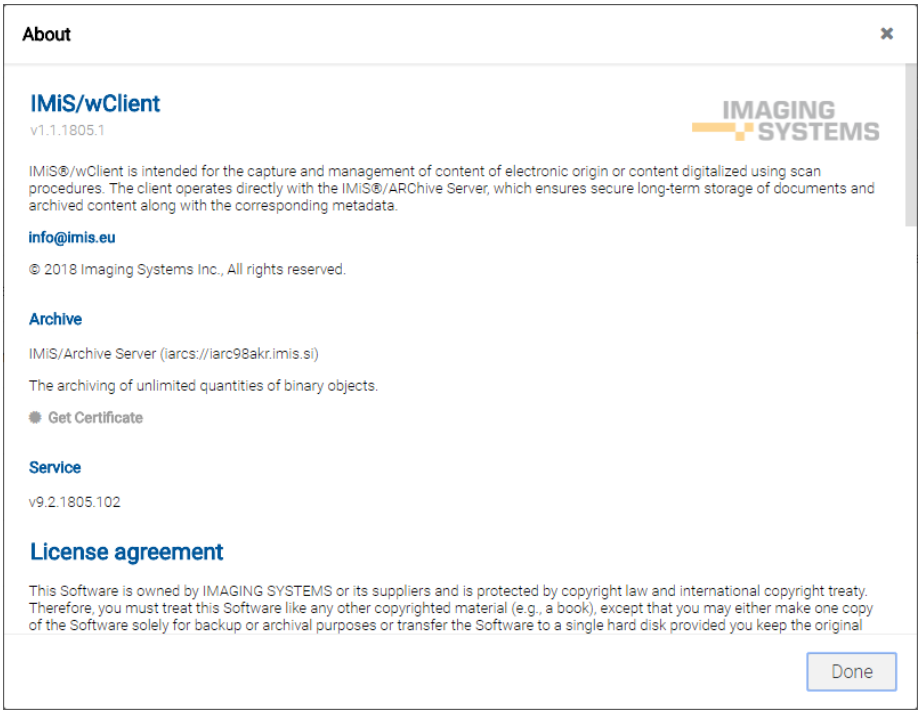

Image 20: About dialog box

4.2.3.3 Log out

By selecting the »Log out« command, the user logs out of the archive. A login window appears for logging in to the archive. For more information see chapter Login and logout.

4.2.3.4 Display of entities

By selecting the icon to the right of the command bar, the user can choose the display mode for the list of entities. The default mode is »List«, where the entities are shown in a list. The user can also choose a graphic display, where the entities are shown in a grid.
By selecting »Classification code« and/or »Description«, the user can add or remove the columns of the selected attribute.

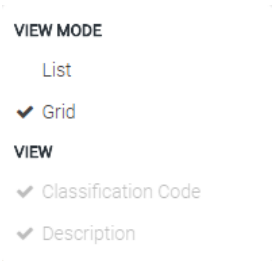

Image 21: Selecting the display of entities in a grid

4.2.3.5 Search

Located above the central view in the header of the user interface is the »Search« field.
It enables the user to search by the metadata of selected entities and to search by the entire text of the content of documents over the entire archive.
For more information on search options see chapter Search functions.

4.2.4 Command bar

After the user logs in to the selected archive, the following commands appear in the command bar above the information on the selected entity:

- New: creates a new root class or contained entity.
- Open: opens the selected entity in the reading mode.
- Edit: opens the selected entity in the editing mode.
- »Actions«: contains commands for performing various operations on the selected entity:
  - »Status«: enables the user to edit the status of the entity via a dialog box, which also offers the option to enter the reasons for the changes performed.
  - »Security class«: enables the user to change the entity's security class via a dialog box, which requires the user to enter the reasons for the change performed.
  - »Authenticity evidence«: enables the user to retrieve authenticity evidence for the selected entity.
  - »Move«: enables the user to move the selected entity around the classification scheme of the archive.
  - Delete: deletes the selected entity.

Image 22: Command bar above the information of the selected entity

4.2.5 Entity information

Information about the selected entity is found in the right view of the IMiS®/wClient user interface. The tabs are shown below the title of the entity.

Previewing the selected entity will display those tabs and content which are publicly accessible to the user. When a selected entity is open in the reading mode, the tabs are adapted according to the effective permissions of the user.

2018 © Imaging Systems Inc., All rights reserved.

In general, data on the selected entity is classified into the tabs.

The tabs are always shown, either in the preview mode for a selected entity or when the selected entity is open in reading mode. By selecting the entity editing mode, a new window opens, containing the attributes whose values can be changed by the user.

Potential exceptions and supplements are given below for each tab:

- »Details« tab: contains system metadata that may be edited, and the predefined metadata of the entity. In the reading mode the tabs show all the data for which the user has the read permission.
- »Security« tab: contains an overview of the effective permissions of groups and users for the selected entity. A user with the »Change permissions« effective permission is enabled the editing of explicit access rights for a selected entity user or group that has predefined effective permissions on the entity.
- »Retention« tab: contains the settings for the selected retention periods and the selected disposition holds. A user with the »Change retention« effective permission is enabled the editing of retention and disposition hold periods.
- »Activity Log« tab: contains the audit log for the selected entity.
  A user with the »AuditLogQuery« role is enabled to review the audit log data.

Image 23: Tabs containing entity information in the preview/reading mode

The tabs are available in the following modes of displaying information on the selected entity:

- Preview
- Open.

2018 © Imaging Systems Inc., All rights reserved.

4.2.5.1 The »Details« tab

The »Details« tab contains a list of the metadata of the selected entity.

The first column gives the titles of attributes, while the second column displays their values.

The »Details« tab contains general and system metadata for the selected entity. Unlike the general metadata, which are publicly accessible and can be edited and changed by the user, the system metadata are read-only. For more information see chapter General system attributes.

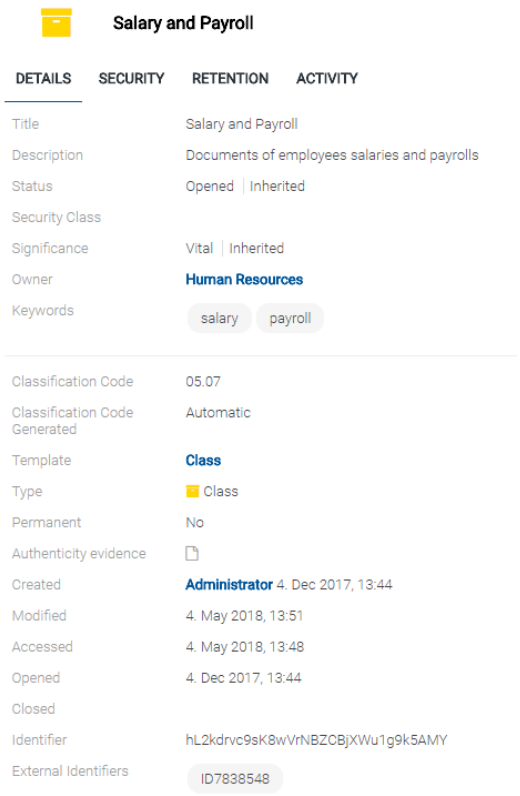

Image 24: Preview mode display of the »Details« tab

In reading mode (Open) the user is shown the following metadata in addition to the general and system metadata:

- Email: contains email metadata. This group is only available for documents that originate from an email template. For more information on email metadata see chapter Email attributes.
- Physical properties: contains physical content metadata.
- Custom: contains custom-entered metadata of the entity.

2018 © Imaging Systems Inc., All rights reserved.

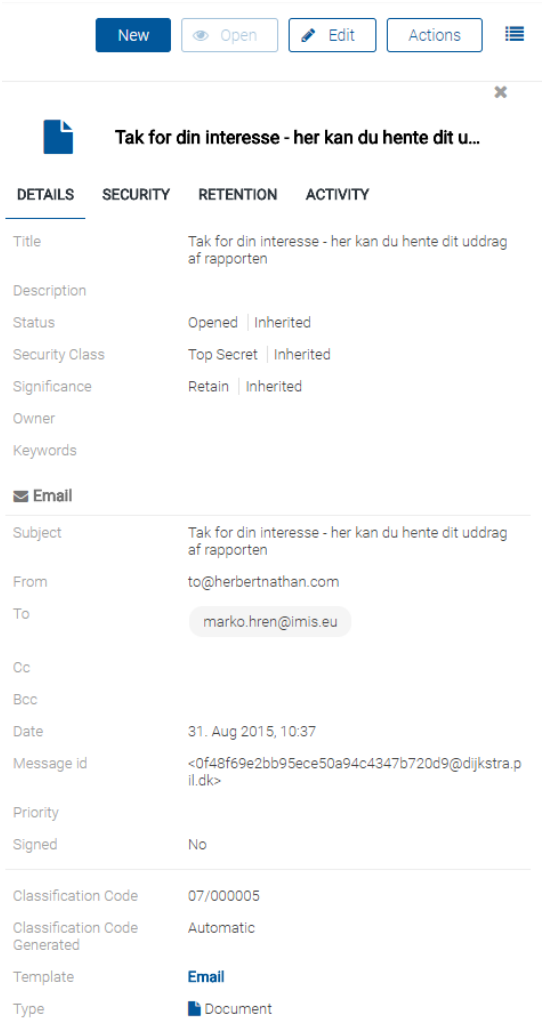

Image 25: Reading mode display of the »Details« tab

By selecting the content from the list in the central view, the following options are available to the user in the popup menu in reading mode (Open):

- Preview: opening content in the preview mode.
- Download: downloading the content to a computer or device.
- Details: displaying information on the content. These details can be displayed if they were not displayed previously.
- Manage: tagging the content for executing specific actions.
  - Queue for Indexing: the selected content is tagged for later indexing.
  - Queue for Conversion: the selected content is tagged for later conversion.

For more information on managing the content see chapter Content management.

2018 © Imaging Systems Inc., All rights reserved.

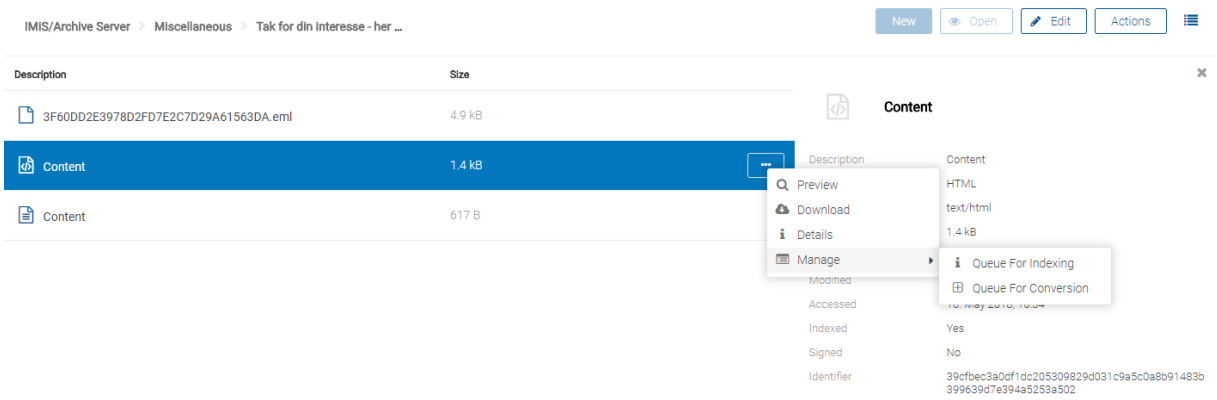

Image 26: Drop-down menu on the selected content in the reading mode

4.2.5.2 The »Security« tab

The »Security« tab is intended for reviewing the access control list (ACL) or the list of explicit permissions of groups or users on the entity and its metadata.

In the preview or reading mode the user is shown a list of groups or users that have been granted at least one explicit permission on the selected entity in the access control list (ACL).

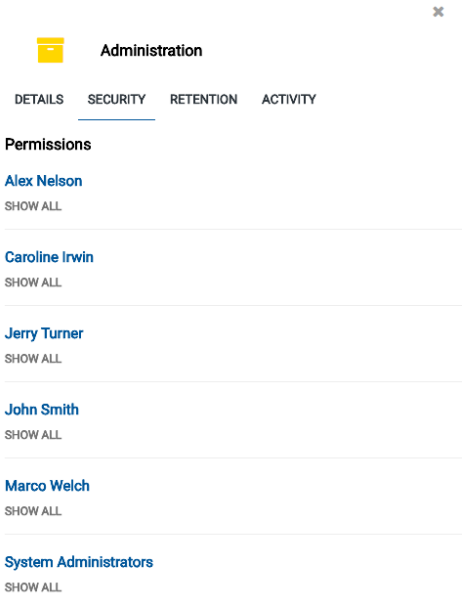

Image 27: A list of users/groups with access rights to the entity in the preview and reading mode

By expanding the display (Show all) under the title of the user or group, the list shows the current status of »Effective permissions« for the selected entity.

2018 © Imaging Systems Inc., All rights reserved.

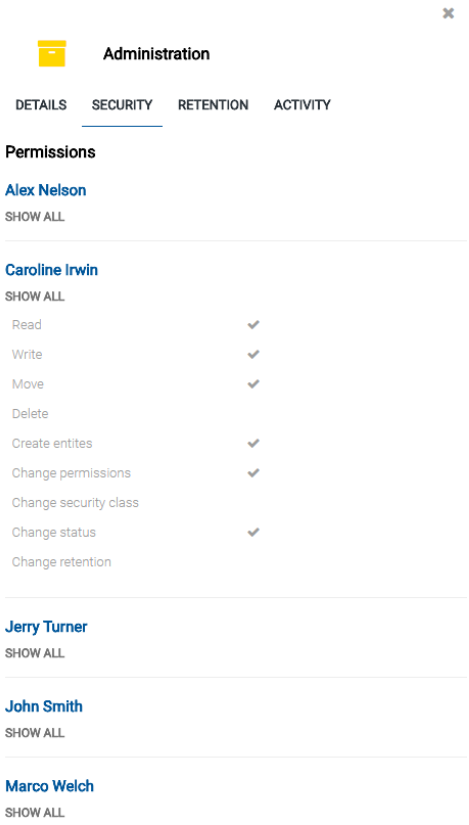

Image 28: A list of effective permissions for the selected user in the preview and reading mode

The list of permissions granted to the user (on the selected entity) consists of the following permissions:

- Read: the user has permission to read data on the selected entity (view metadata and content files).
- Write: the user has permission to edit entity data (write metadata and add content files).
- Move: the user has permission to move the entity within the classification scheme.
- Delete: the user has permission to delete entity data (delete metadata and remove content files).
- Create entities: the user has permission to create sub-entities inside the selected entity.
- Change permissions: the user has permission to change the effective permissions of other users on the selected entity.
- Change security class: the user has permission to change the security class of the selected entity.

2018 © Imaging Systems Inc., All rights reserved.

- Change status: the user has the permission to change the status of a selected entity.
- Change retention: the user has the permission to read and change the content of »Retention« tab.

4.2.5.3 The »Retention« tab

The »Retention« tab is intended for reviewing and editing retention and disposition hold periods for a selected entity.

In the preview or reading mode the user is shown a list of the retention and disposition hold periods which apply to a specific entity.

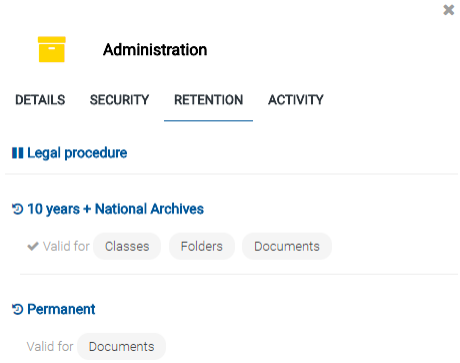

Image 29: Preview and reading mode display of the »Retention« tab

By clicking on the disposition hold title, a notification window opens, containing the following information:

- Name: unique name of the disposition hold.
- Description: a short description of the disposition hold.
- Reason: the reason for creating a disposition hold.
- Identifier: unique identifier of the disposition hold.

2018 © Imaging Systems Inc., All rights reserved.

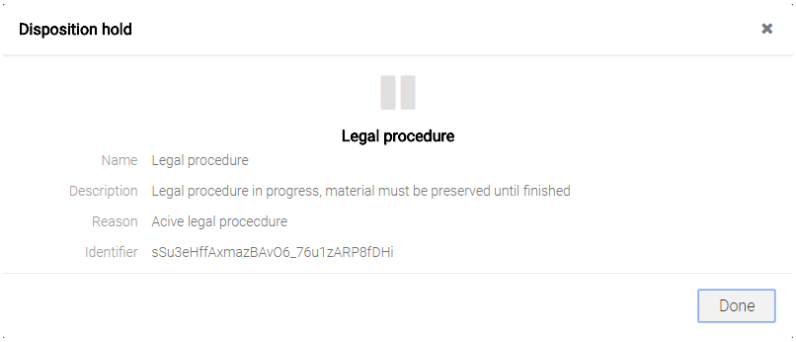

Image 30: Dialog box with the information on disposition hold

By clicking on the retention policy title, a notification window opens, containing the following information:

- Name: unique name of the retention policy.
- Description: short description of the retention policy.
- Detailed description: detailed description of the retention policy.
- Action: the default action from the list of actions for entity.
- Identifier: unique identifier of the retention policy.

The user closes the notification window by selecting the »Done« button.

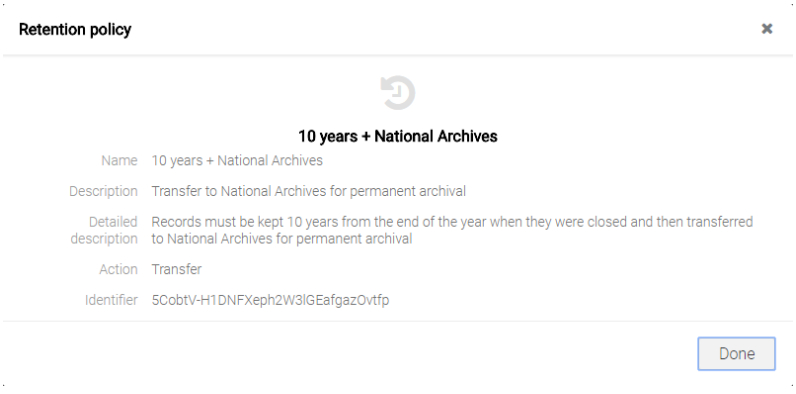

Image 31: Dialog box with the information on retention policy

2018 © Imaging Systems Inc., All rights reserved.

4.2.5.4 The »Activity« tab

The »Activity« tab shows the audit log for the selected entity.

Image 32: The »Activity« tab in the preview and reading mode

The audit log records the following information:

- User: name of the user who performed an action on the selected entity.

  By clicking on the user's name, a notification window opens, showing user information.

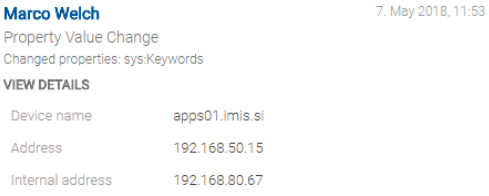

Image 33: User information

- Time: time when an action was performed on the selected entity.
- Event type: type of event that was performed on the selected entity.
- Address: the network address from where the command to perform the action on the selected entity came from.

2018 © Imaging Systems Inc., All rights reserved.

- Internal address: IP address, which is set by opening a new session with the REST service.
- Device name: name of device, from where the command to perform the action on the selected entity came from.

4.3 Actions

This chapter describes the actions of the IMiS®/wClient on the selected archive:

- User login and logout from the archive.
- Access to records on the archive.
- Changing of record properties.
- Managing the contents.
- Archiving of email messages.
- Management of physical records metadata.
- Moving and deleting of records.
- Search by metadata and search full text of archived records.
- Status changes.
- Security class changes.
- Authenticity evidence retrieval.
- Audit log search.

4.3.1 Entity access

Access to the entity in the classification scheme depends on the security class of the entities, the user's security class level, and the user's access right.

For more information on security classes see chapter Access in the IMiS®/ARChive Server user manual. For changing the security class of the entities see chapter Changing the security class.

When logging into the selected archive, the root classes of the archive to which the user has the »Read« access right are read from the IMiS®/ARChive Server.

The user is shown the root classes in the »Archive« folder in the left view and in the list of contained entities in the central view.

2018 © Imaging Systems Inc., All rights reserved.

By selecting a root class, the tabs in the right view (entity information) show only the publicly accessible information on the class. For more on the content of tabs see chapter Entity information.

By selecting the »Open« command in the command bar, all of the data to which the user has read permissions are read from the server. The same applies to the access to entities contained in the archive's root classes.

A user with the »Write« permission on the selected entity can select the »Edit« command in the command bar. The same data are shown in the tabs as when selecting the »Open« command. The user can edit and change the values of attributes that are not tagged on the server as read-only. For more information see chapter Editing entity data.

4.3.2 Creating an entity

The user can create entities in the IMiS®/wClient, if he has the »Create entities« right on the selected class or folder.

For faster capturing and classifying of entities to appropriate places in the classification scheme, it is recommended that users separate (organize) the documents by type before capture.

Separation is performed by classifying documents into the appropriate templates in the classification scheme. Each template has predefined attributes, which are set by the administrator in the settings of the IMiS®/ARChive Server. The user must enter the mandatory attributes before saving.

Example: When creating entities, it is advisable that entities contain only a single type of subordinate entity. Thus, classes should contain only documents or only folders. Mixing different types of entities in the same hierarchy level is not allowed according to the Moreq2 standard (Ref. 3.1.25).

4.3.2.1 Creating a new entity

The »Create entities« permission enables the user to add new root classes and contained entities under the selected entity.

2018 © Imaging Systems Inc., All rights reserved.

4.3.2.1.1 Creating a root class

By selecting the »Archive« folder in the left view, the user can add a new root class to the entities list. The user does that by selecting the »New« command in the command bar, entering the values of attributes, and confirming »Create«.

4.3.2.1.2 Creating a contained entity

In the classification scheme (left view) or in the entities list (central view) the user selects the entity into which he wants to classify a new class, folder or document. The user does that by selecting the »New« command in the command bar, same as when creating a root class.

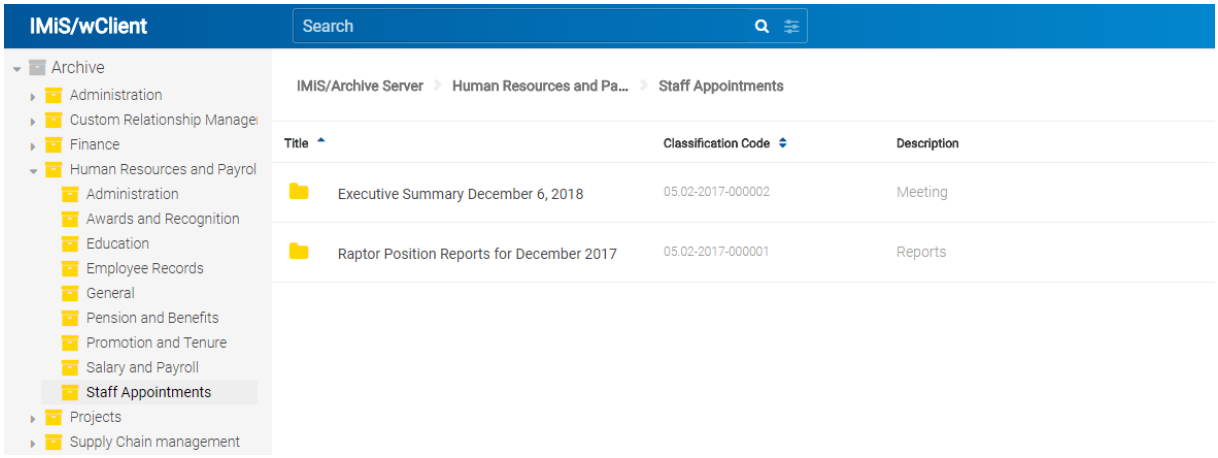

Image 34: Display of contained entities.

After selecting the class in the central view and selecting the »New« command in the command bar, a dialog box appears with the following attributes:

- Parent: the name of the parent entity. This attribute is read-only.
- Template: a set of available templates for creating allowed entities and classifying them under the selected class or folder. The attribute value is mandatory.
- Type: the type of the entity. This attribute is read-only.
- Title: name of the entity. The attribute value is mandatory.
- Description: short description of the entity.
- Status: the status of the entity.
- Security class: a set of available entity security classes based on the entity's position in the classification scheme.
- Significance: a set of available entity significances.

2018 © Imaging Systems Inc., All rights reserved.

- Owner: A directory (user or group) entity that is responsible for the selected entity (owner).
- Keywords: entity-related keywords. This attribute can have multiple values.
- External identifiers: a list of the unique external identifier of the entity on the server.
- Classification code generated: selecting the type of classification code entry for the contained entities of the parent class.

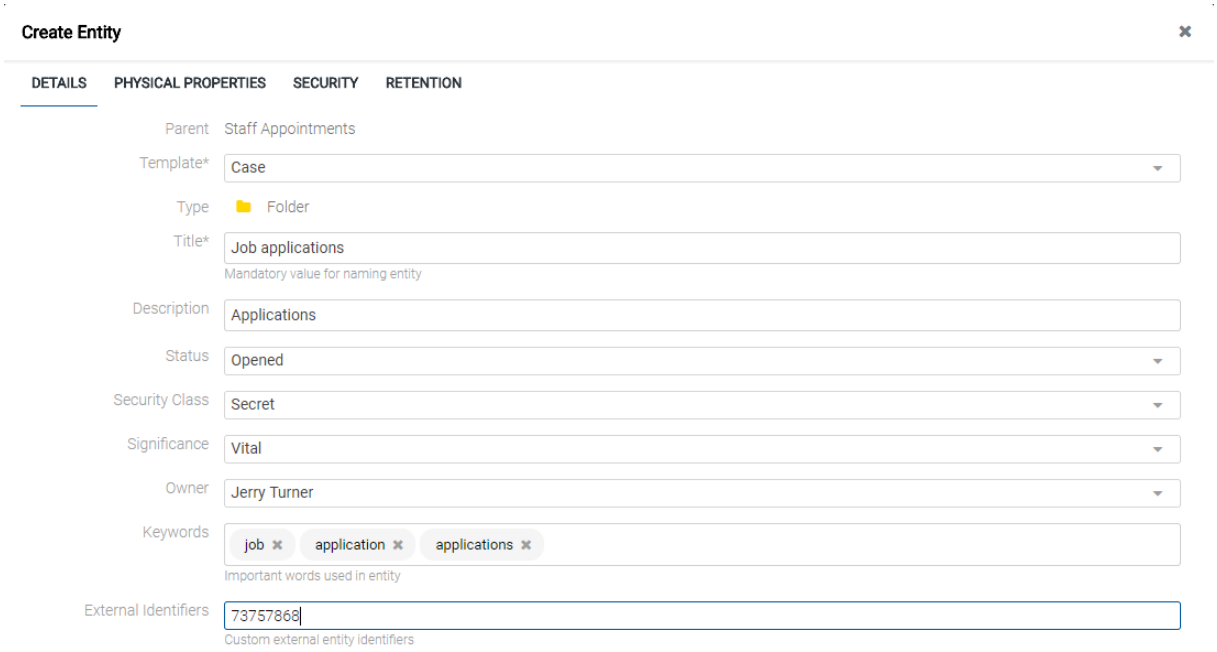

Image 35: Display of creating a new folder

Troubleshooting: the most frequent issues when creating a new entity are:

- *Entity with the template you selected cannot be created inside the selected entity.*
- *User does not have permission to create new entities inside the selected entity.*

4.3.2.2 Entering entity metadata

The »Details« tab in the »Create entity« dialog box contains a list of all attributes of the class, folder or document, which can be entered by the user.

The attributes that are marked (an asterisk is added to the title of the attribute) are required. They must be entered before saving.

2018 © Imaging Systems Inc., All rights reserved.

Image 36: Entry of required metadata

Attribute entry fields are as follows:

- Text field where the user inputs any string of characters.

Image 37: Entry of text metadata

- Date field where the user inputs the date, or selects one from the date and time selection popup window.

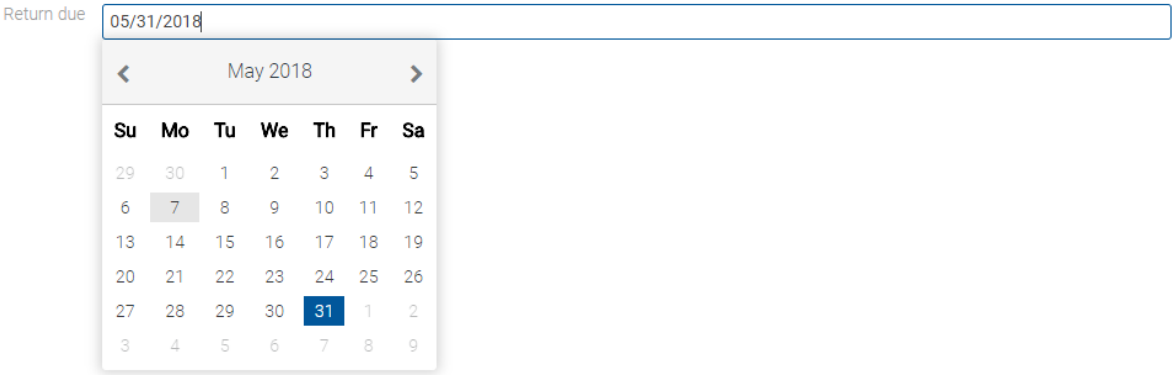

Image 38: Entry of date and time metadata

- A pick list with predefined values, one of which is selected by the user.

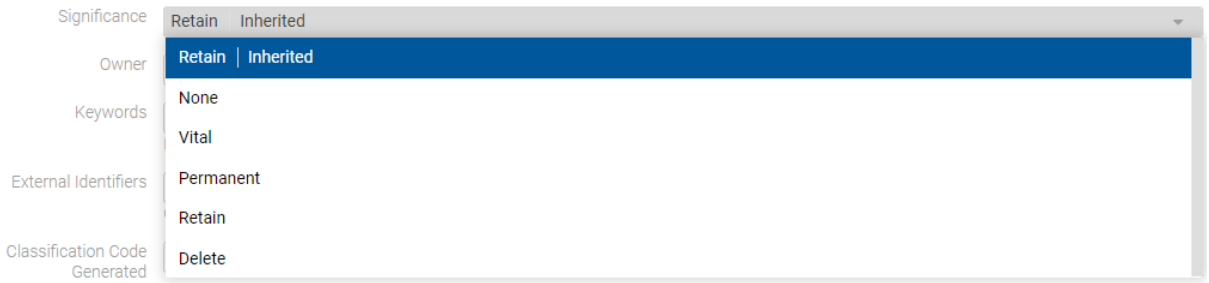

Image 39: Entry of metadata with predefined values

2018 © Imaging Systems Inc., All rights reserved.

- A multiple value field where the user inputs any desired text values, separated by using the »TAB« key. In the multiple value display field, the individual values are separated by spaces. The user has the option of removing individual keywords by clicking on the cross next to the word.
- A multiple value field where the user inputs any desired text values, separated by using the »Enter« key. In the multiple value display field, the individual values are separated by spaces.

Image 40: Entry of multiple value metadata

After entering all of the required and desired attribute values in the »Details« tab, the user continues by entering the values in the remaining tabs.

4.3.2.3 Entry of the classification code

The entry of the classification code for new entities depends on the selected type of classification code generation of the parent class. This type is selected in the »Details« tab in the preview or reading mode. The drop-down list of the field »Child classification code generation« allows the user to set the entry type for the selected class:

- Automatic: where classification codes of child entities are generated automatically by the IMiS®/ARChive Server. These classification codes appear as successive numbers, with each new child entity increasing the number by one.
- Manual: where classification codes of child entities must be entered manually. This classification code may be any combination of letters and numbers, providing it is unique inside the entire parent class.

Image 41: Selecting the type of classification code entry for the class of the contained entity

If the parent class settings dictate the manual entry of classification codes for all new child entities, the user must enter them manually. The user only enters the relative part of the classification code, and the full classification code is then created from the parent entity's own classification code and the code input by the user.

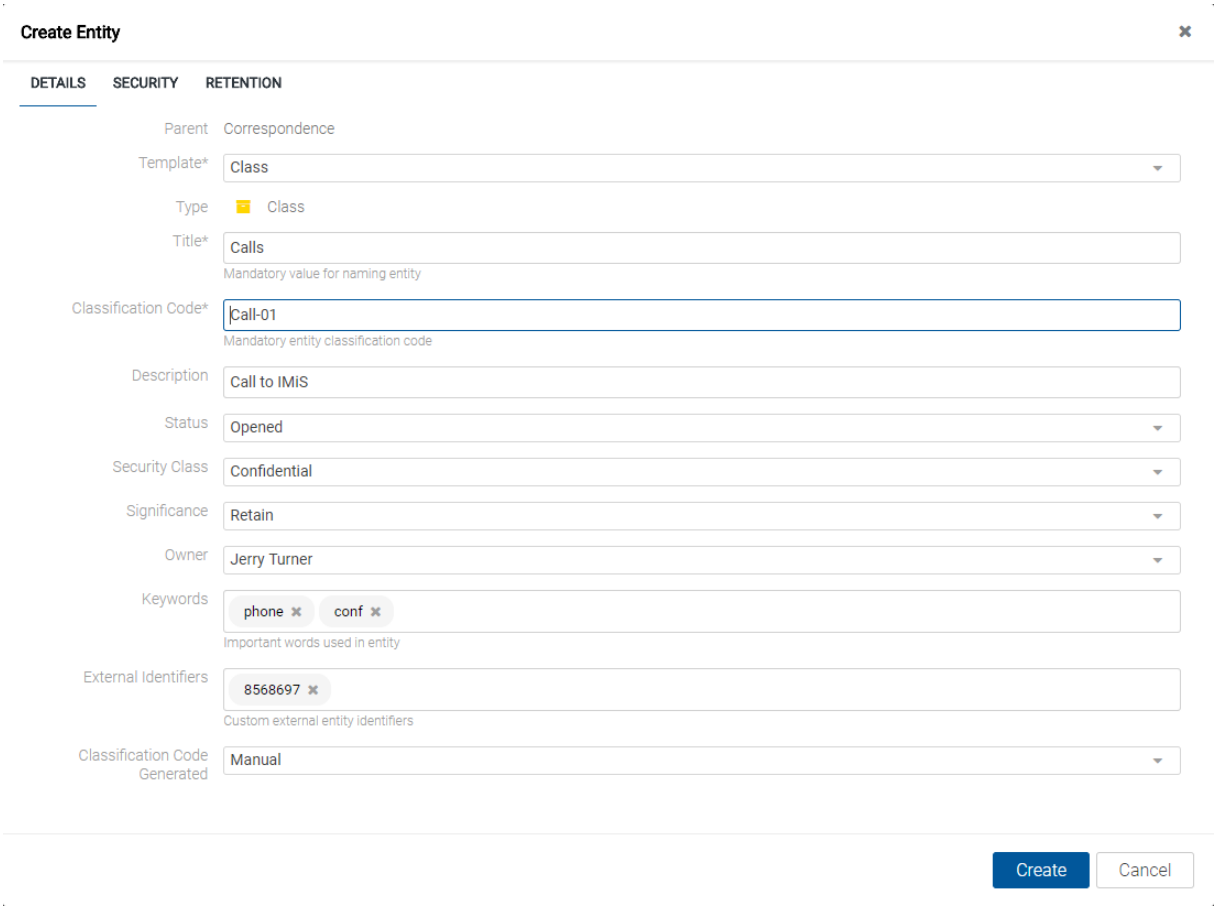

Image 42: Manual entry of a child entity's classification code

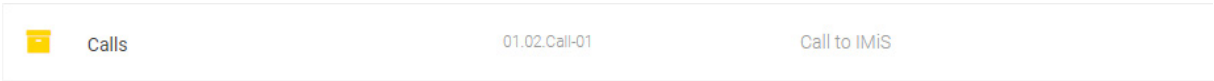

Image 43: Display of manually entered classification code

Example: Inside a class with the classification code »01.02«, the user creates a new folder for which user manually input »Call-01« as the relative part of the classification code. When the folder is saved to the IMiS®/ARChive Server, its full classification code will be »01.02.Call-01«.

2018 © Imaging Systems Inc., All rights reserved.

4.3.2.4 Setting an entity's security class

This setting hides entities from users whose security class level is not high enough to access them. The user with the »Create entities« permission can specify a new »Security class« for new entities in the »Details« tab in the »Create entity« dialog box.

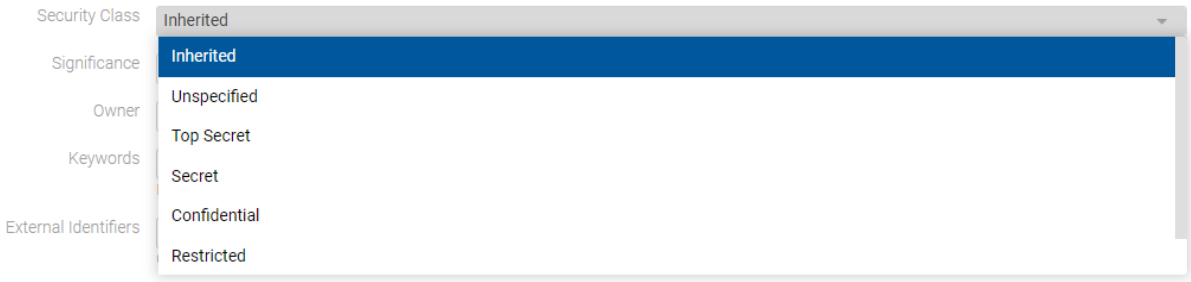

Image 44: Specifying the security class of a new entity

When the entity has been created, the user can change the security class by selecting the commands »Actions« in the command bar and »Security class« in the popup menu.
A dialog box opens for selecting the value of the »Security class« attribute and the reason for the action, which is a required data.

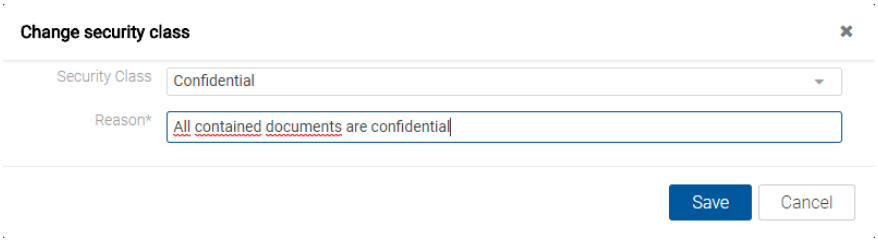

Image 45: Changing the security class of the entity

Security classes are predefined, and range from lowest to highest as follows:

- »Inherited«: means the security class is implicitly inherited from the parent entity. In case of root classes, the inherited security class value is empty.
- »Unclassified«: means access to this entity is not limited.
- »Restricted«: means the entity is an internal matter. It may only be accessed by users with a clearance level »Restricted« or higher.
- »Confidential«: means the entity is considered confidential. It may only be accessed by users with a clearance level »Confidential« or higher.

2018 © Imaging Systems Inc., All rights reserved.

- »Secret«: means the entity is considered secret. It may only be accessed by users with a clearance level »Secret« or higher.
- »Top Secret«: means the entity is considered top secret. It may only be accessed by users with a »Top Secret« clearance level.

The pick list only displays values that are lower or equal to the clearance level of the user. When the security class of the parent entities is not set or when at least one parent entity has a specified security class, then in addition to the values that are lower or equal to the clearance level of the user, the pick list also displays the inherited value, marked by the suffix [Inherited].

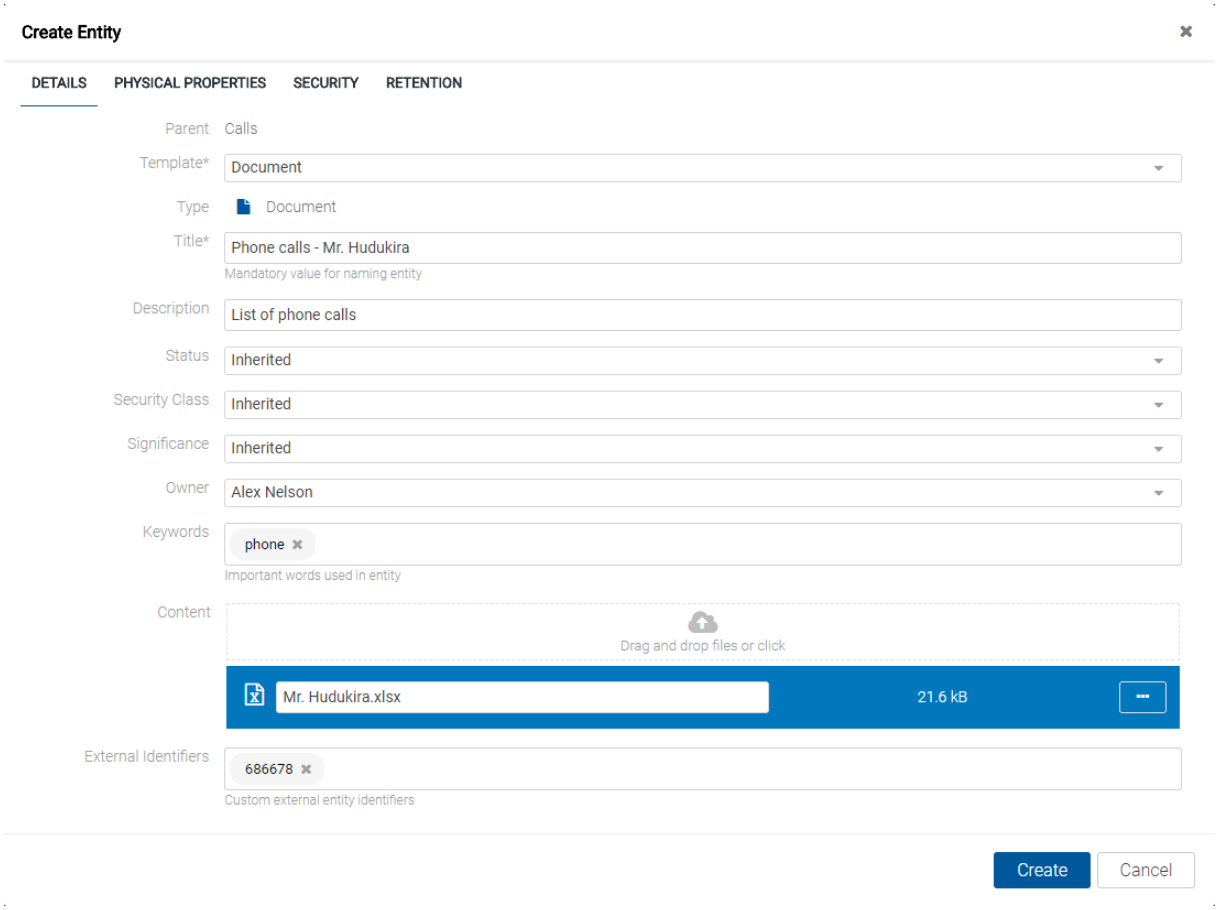

Image 46: Entering the security class of the entity with an inherited value

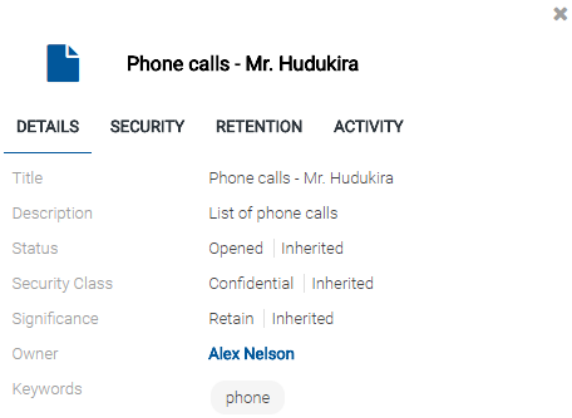

Image 47: Entity information after entering the security class

When a new entity has been saved, users can no longer modify the »Security class« metadata using the »Details« tab but only by using the »Security class« action. In doing so, they must give the reason for changing the entity's security class. The user accesses the »Security class« action by selecting the »Actions« button in the command bar.

For more information on setting an entity's security class see chapter Changing the security class.

2018 © Imaging Systems Inc., All rights reserved.

4.3.2.5 Entering the status of an entity

The user with the »Create entities« permission can specify the »Status« of new entities in the »Details« tab in the »Create entity« dialog box.

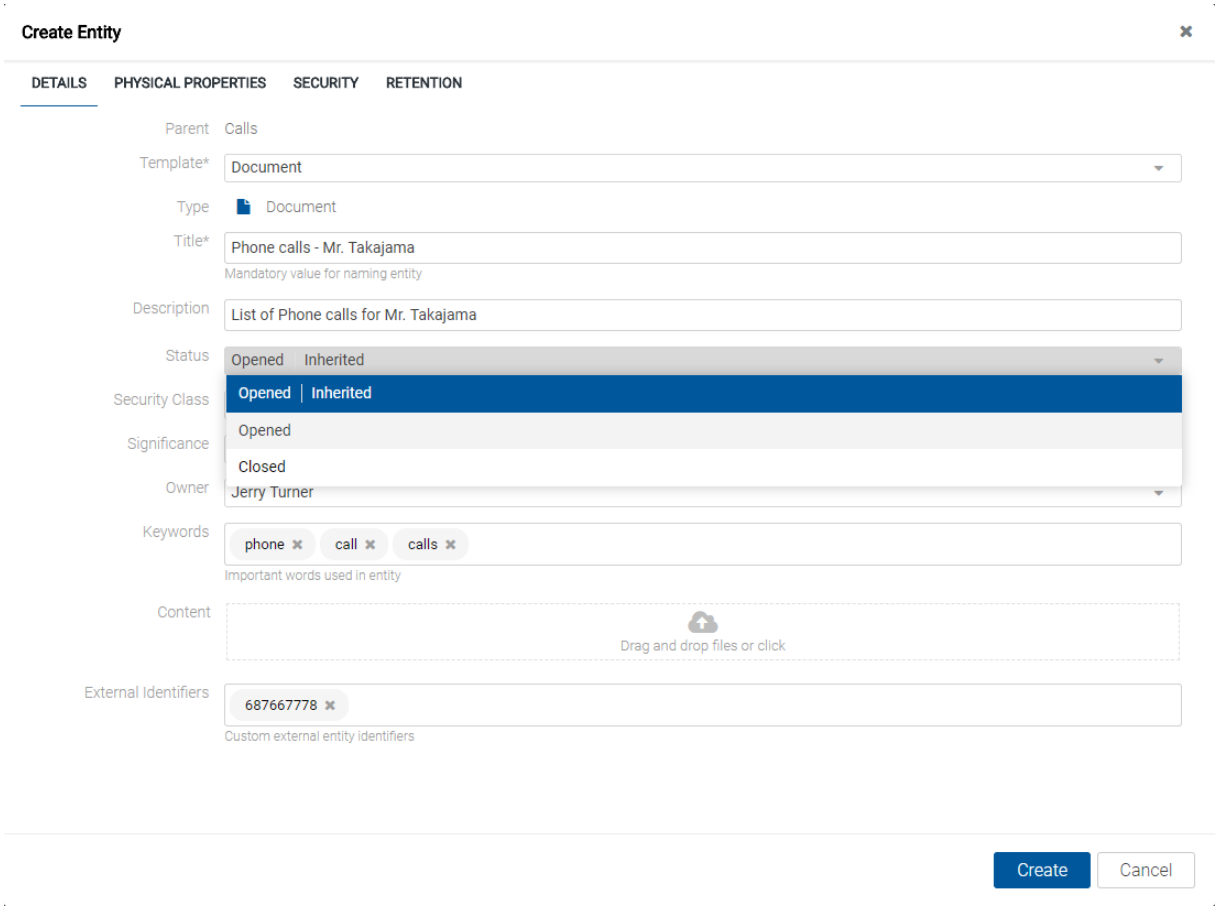

Image 48: Specifying the status of a new entity

When the entity has been created, the user can change the status by selecting the commands »Actions« in the command bar and »Status« in the popup menu.

A dialog box opens for selecting the value of the »Status« attribute and the reason for the action, which is a required data.

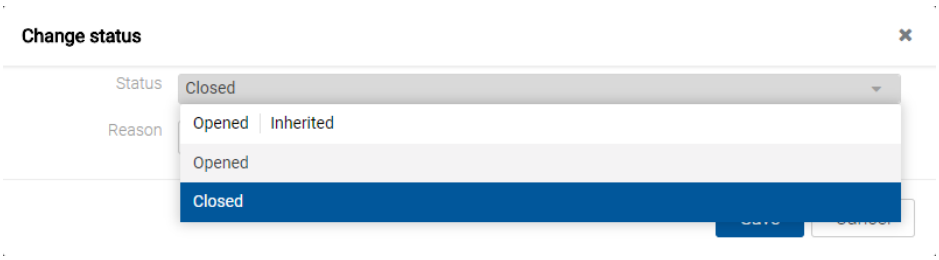

Image 49: Changing the status of an entity

2018 © Imaging Systems Inc., All rights reserved.

4.3.2.6 Entry of physical content metadata

When capturing physical content into its electronic form, users may add metadata that describes the physical location of the stored content, in addition to other types of metadata. The location metadata is optional. Entry of physical content metadata for a folder or document is possible upon capture / import, or later when the content is already stored in electronic form.

By selecting the folder or document, a dialog box opens in editing mode, containing the following tabs: »Details«, »Physical Properties«, »Security« and »Retention« and the attributes whose values the user can select, input or change.

By selecting the »Physical Content« tab, a list of all attributes, referring to the description of entity-related physical content, appears.

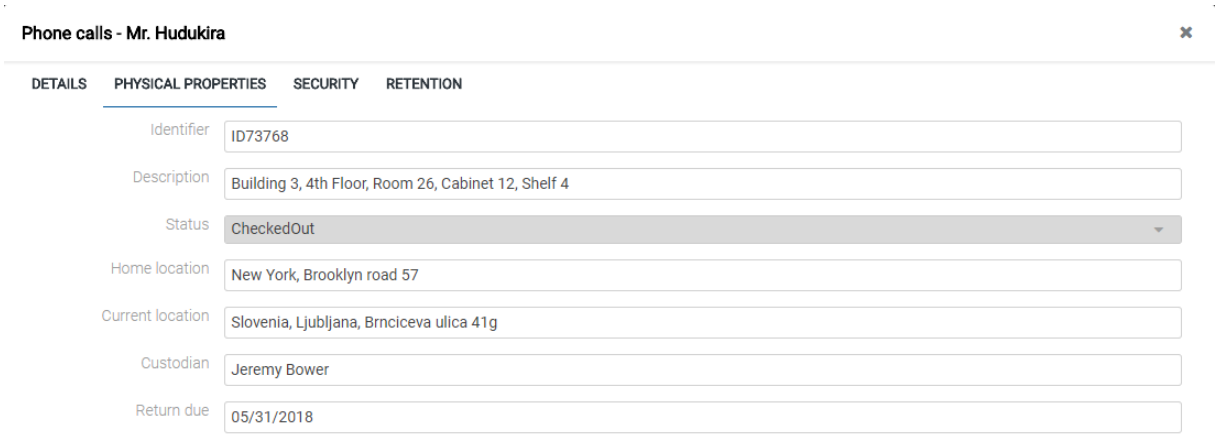

Image 50: Display of the entry of physical content metadata

The user can specify all of the attribute values except for »Date of status change«, which is automatically filled in with the date of the last change of the »Status« attribute.
When capturing physical content, set the »Status« to the »CheckedIn« value.
For more information on physical content attribute description see chapter Physical content attributes.

4.3.2.7 Specifying retention periods

A condition for successfully saving new entities is the existence of effective retention periods on the entity. This condition applies to all types of entities, except for documents in a folder for which retention periods cannot be specified.

2018 © Imaging Systems Inc., All rights reserved.

The presence of effective retention periods can be checked by the user in the »Retention« tab. On the list the effective retention periods are ticked in front of the information on the validity of individual entity types. If the entity does not have an effective retention period, one must be specified.

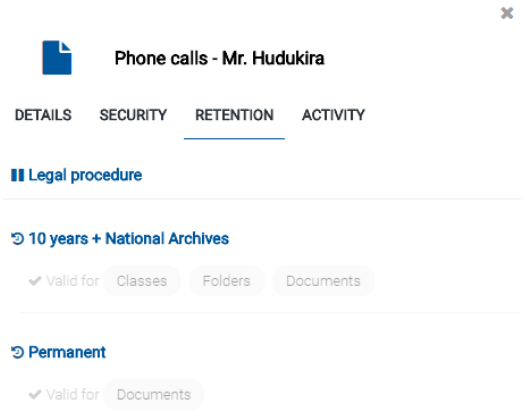

Image 51: Display of the »Retention« tab

The user with the »Change retention« permission can add or remove retention periods by selecting the »Edit« command in the »Retention« tab. For more information on changing retention see chapter The »Retention« tab.

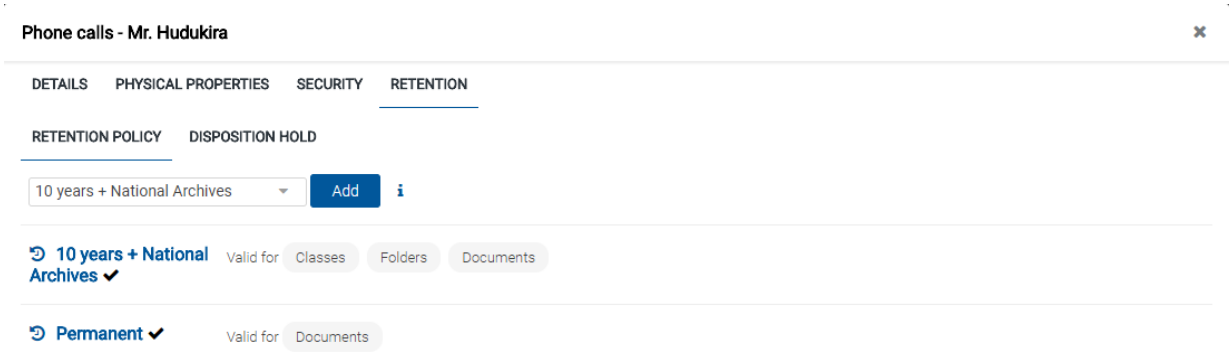

Image 52: Display of changing retention periods

4.3.2.8 Saving an entity

Before saving the user has to enter all of the mandatory metadata and specify an effective retention period. The user saves the entity to the IMiS®/ARChive Server by selecting the »Save« command in the bottom part of the user interface.

2018 © Imaging Systems Inc., All rights reserved.

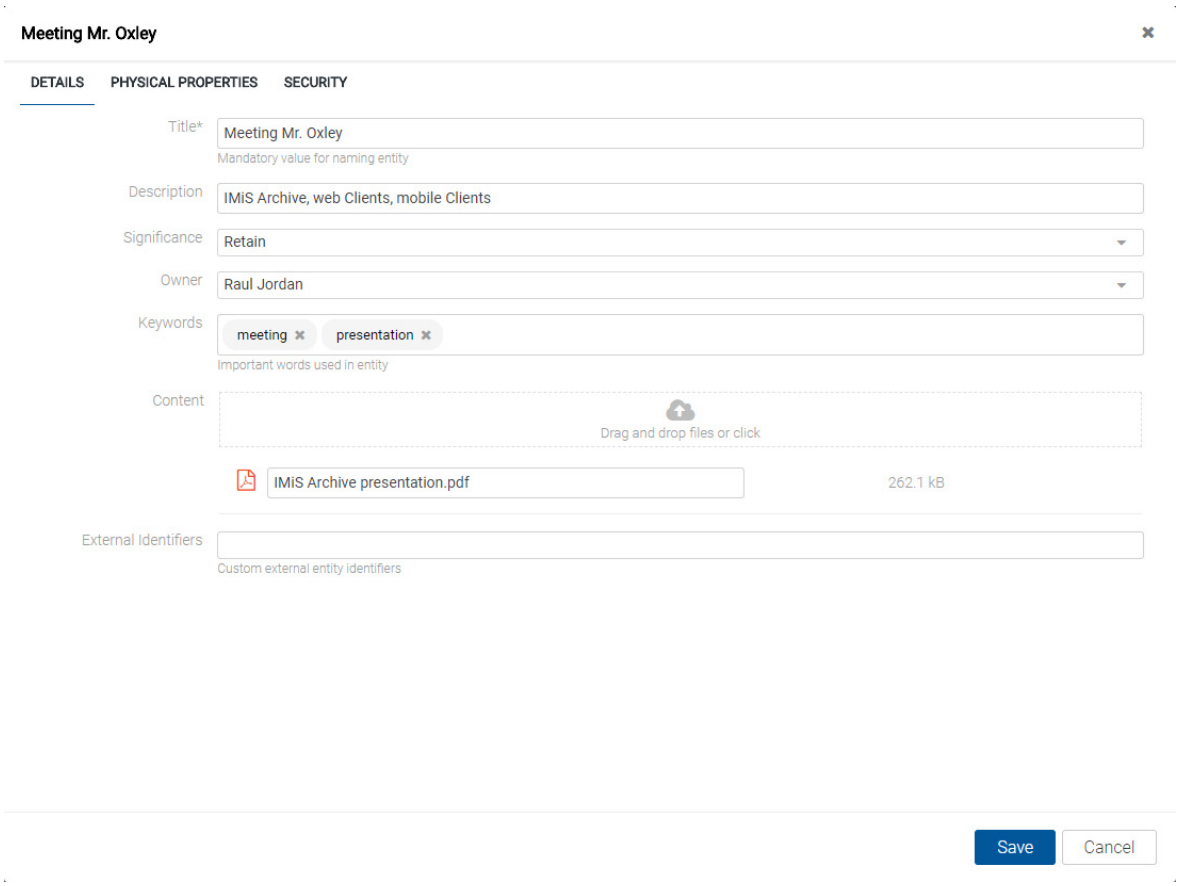

Image 53: Saving a new or modified entity

Troubleshooting:

Most frequent errors when saving:

- *The value of a mandatory attribute was not specified.*
- *The entered attribute value does not correspond to the limitations prescribed by the attribute.*

When saving an entity to the IMiS®/ARChive Server, the following metadata is automatically recorded into the entity:

- »Classification code«: according to the classification of the entity in the classification scheme, the server creates a unique string of characters.

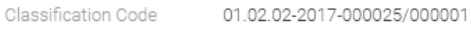

Image 54: Example classification code

- »Creator«: the user who created the entity; meaning the user who was logged in during the session when the entity was created. This metadata never changes.

2018 © Imaging Systems Inc., All rights reserved.

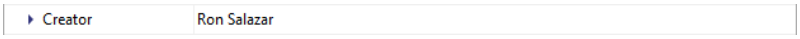

Image 55: Example creator of entity

- »Opened«: records the date and time the »Status« attribute was saved with the »Opened« value.

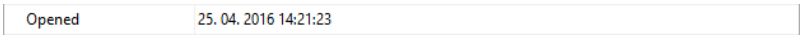

Image 56: Example date and time an entity was opened

- »Closed«: records the date and time the »Status« attribute was saved with the »Closed« value.

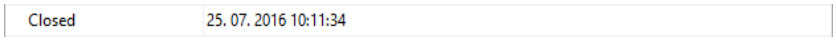

Image 57: Example date and time an entity was closed

- »Created«: records the date and time the entity was created on the server. This metadata never changes.

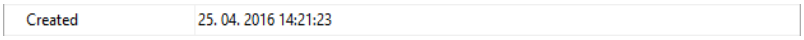

Image 58: Example date and time an entity was created

- »Modified«: records the date and time of the last change to any of the attributes or the content of the entity. This metadata changes every time the entity is saved.

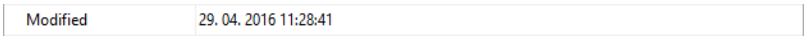

Image 59: Example date and time of last changes to the entity

- »Accessed«: records the date and time the entity was last opened in the reading mode or the editing mode. This metadata changes whenever a user accesses or edits the entity.

Image 60: Example date and time of last access to the entity

2018 © Imaging Systems Inc., All rights reserved.

- »Identifier«: the entity's unique identifier on the server. This metadata never changes.

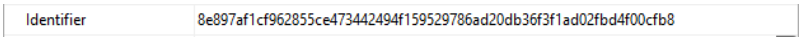

Image 61: Example entity identifier

4.3.3 Editing entity data

Changing data about an entity in the IMiS®/wClient includes editing metadata and modifying content. A user can only change entity data when user have the »Write« permission on the entity. To edit the selected entity, use the »Edit« command in the command bar.

The user edits the selected entity using the »Edit« command in the command bar.
To the right of the attribute title is a field in which the user can change the attribute value.
The value can be text, date, logical or one of the predefined values, which may be multiple.

4.3.3.1 Editing entity metadata

In the »Details« tab the user can edit the following attribute values:

- Title: title of the folder or document being described. Attribute value is mandatory.
- Description: short description of the entity.
- Significance: significance rating of the entity.
- Owner: a directory entity (user or group) that is responsible for the selected entity.
- Keywords: keywords related to the entity. Attribute can have multiple values.
- External identifiers: a list of the entity's unique external identifiers on the server.

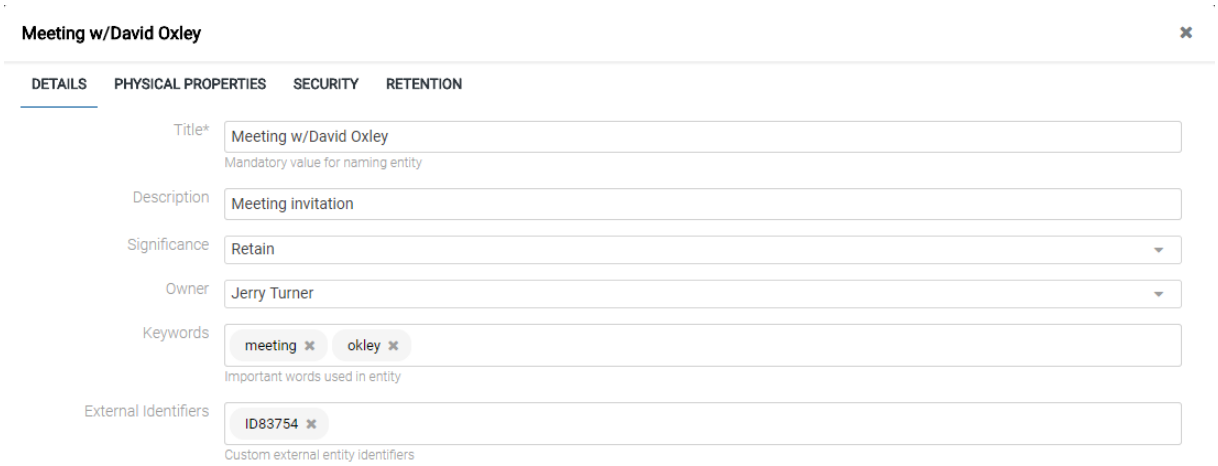

Image 62: Attribute values in editing mode

In addition to the above-mentioned attributes, the user can also edit custom attributes, which are predefined by the template.

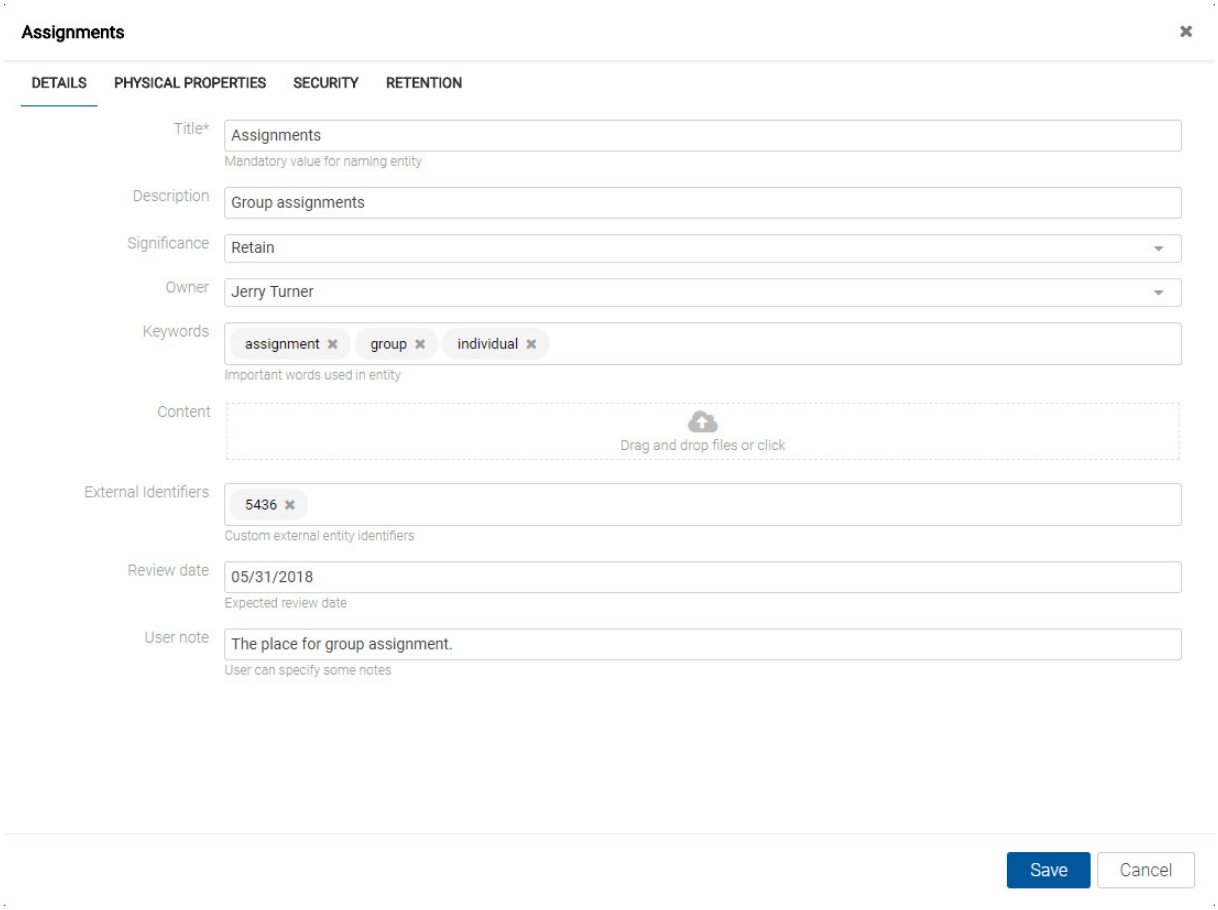

Image 63: Entering the values of custom attributes in editing mode

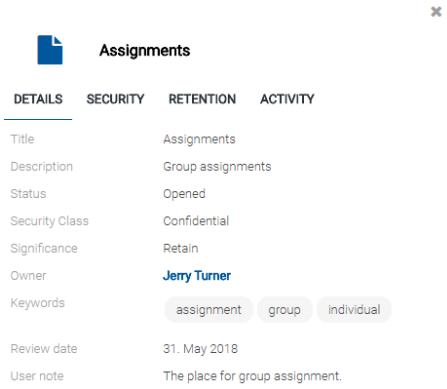

Image 64: Information on the entity that contains custom attributes

2018 © Imaging Systems Inc., All rights reserved.

4.3.3.2 Editing content

In the »Details« tab the user edits document contents.

For more information on editing contents see chapter Content management.

4.3.3.3 Editing physical content metadata

In the »Physical Content« tab the user edits the metadata referring to the location of the physical content. The metadata are not mandatory for archiving physical content.

Physical content metadata can be entered for a folder or document. For more information on editing physical content metadata see chapter Physical content attributes.

Image 65: Display of entering physical content metadata

By changing the value of the »Status« attribute and saving the entity, the »Status Change« is written below the value field. »Status Change« is automatically filled in with the date of the last change of the »Status« field.

The user can change the value of the »Status« attribute to »CheckedIn« when checking in physical content or to »CheckedOut« when checking out physical content.

The user can edit the following values of physical content attributes:

- Identifier: unique identifier of the physical content.
- Description: description of the physical content.
- Status: the current status of the physical content.
- Home location: the home location of the document's physical content.
- Current location: the current location of the document's physical content.
- Return due: return date and time of checked out physical content.

2018 © Imaging Systems Inc., All rights reserved.

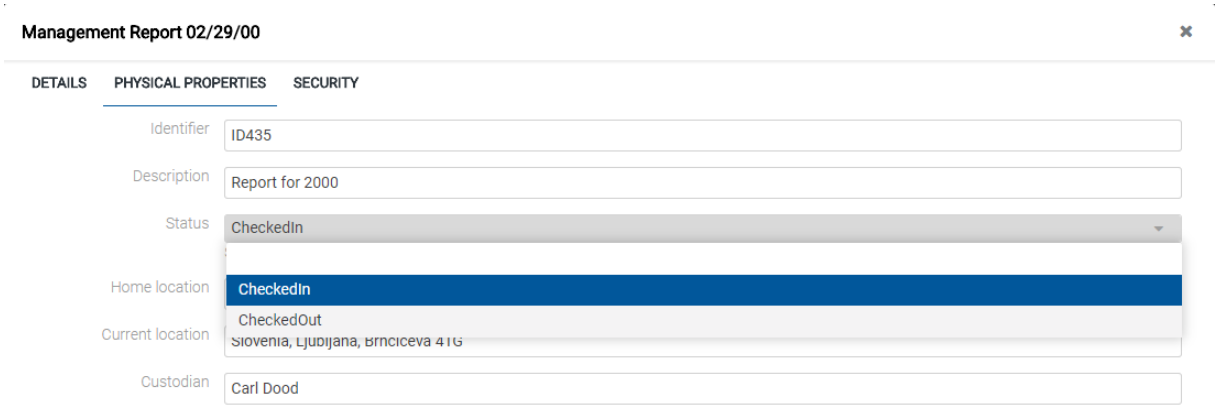

Image 66: Popup menu for selecting the status of the physical content

4.3.3.4 Editing access rights for an entity

The user with the »Change permissions« permission can edit the access control list (ACL) for the entity or a selected metadata for a specific user or group. The list shows only those users and groups that have been granted at least one explicit permission on the selected entity.

The »Permissions« field is located above the list of editing permissions. The default value is »Entity«, with which the access control list (ACL) is associated.

By selecting the »Edit« button in the command bar, a dialog box opens showing effective permissions on the entity for the selected user.

2018 © Imaging Systems Inc., All rights reserved.

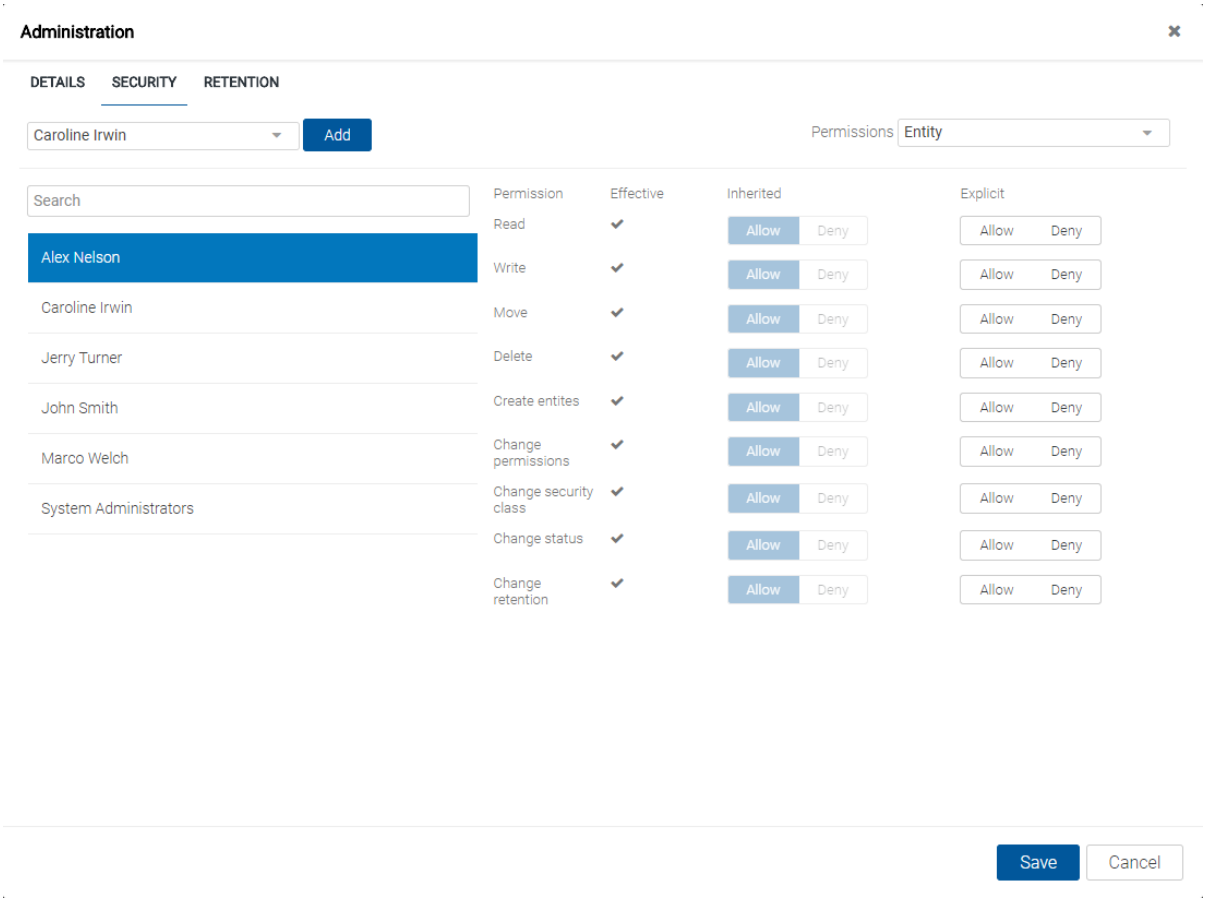

Image 67: »Security« tab in editing mode

The left part of the view contains a list of users with access rights to the entity.

In the event of a greater number of users, search is enabled via a search box. If a specific group or user that is registered on the IMiS®/ARChive Server is not mentioned on the list, the user with permission can select and add them using the »Add« button.

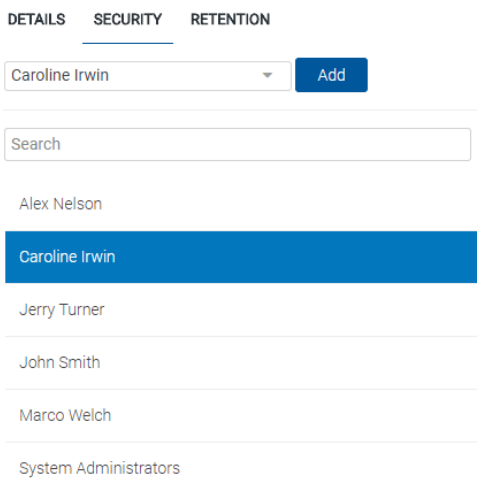

Image 68: List of users with access rights to the entity

2018 © Imaging Systems Inc., All rights reserved.

In the right part of the view a list of entity editing permissions is shown for the selected user. In the »Explicit« column the user selects »Allow« to add an explicit permission, or »Deny« to revoke a permission. The user can specify explicit permissions for any group or user that is registered on the IMiS®/ARChive Server.

Image 69: List of editing permissions

4.3.3.5 Editing access rights for metadata

The »Permissions« field is located above the list of editing permissions.

Instead of the »Entity« default value, the user can select one of the metadata with which the access control list (ACL) is associated.

In the left view the user selects the group or user to which it wants to grant access rights to a selected metadata. The user adds it to the list using the »Add« button.

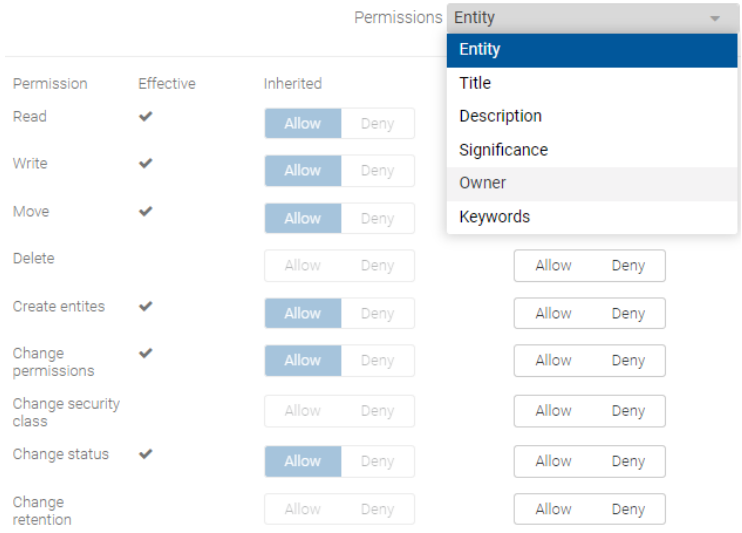

Image 70: Popup menu for selecting access rights to a selected metadata

The left part of the view contains a list of users with access rights to the selected metadata. In the event of a greater number of users, search is enabled via a search box.
In the right part of the view a list of metadata editing permissions is shown for the selected user. In the »Explicit« column the user selects »Allow« to add an explicit permission, or »Deny« to revoke a permission.

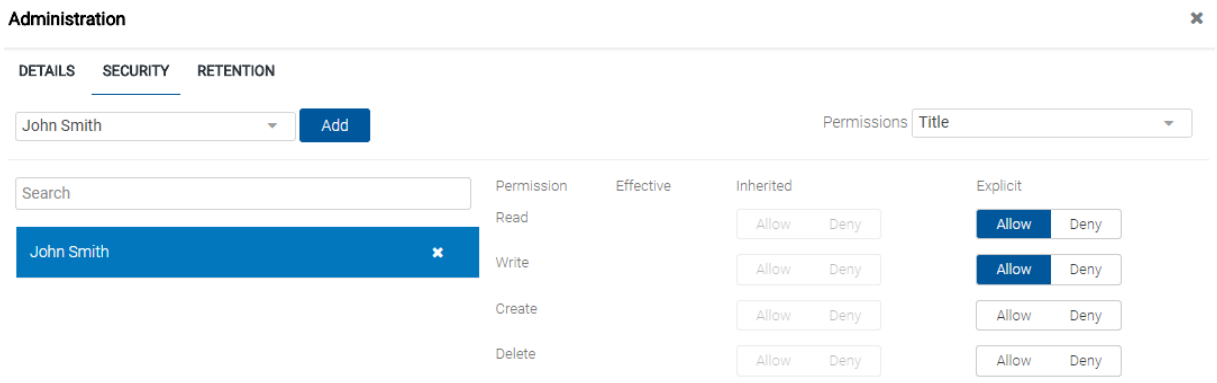

Image 71: List of user permissions on the selected metadata

The list of user permissions on the selected metadata of the entity consists of the following access rights:

- »Read«: the user has permission to read the value of the selected metadata of the entity.
- »Write«: the user has permission to edit the value of the selected metadata of the entity.
- »Create«: the user has permission to create the value of the selected metadata of the entity.
- »Delete«: the user has permission to delete the value of the selected metadata of the entity.

The user confirms the changes to the explicit permissions with the »Save« command or cancels them with the »Cancel« button.

4.3.3.6 Editing retention policies

The user with the »Change retention« permission can edit the retention periods and disposition holds of the selected entity by selecting the »Edit« command.

2018 © Imaging Systems Inc., All rights reserved.

A new window opens containing the tabs:

- Retention policy: entity retention policy list.
- Disposition hold: entity disposition hold list.

In the central part of the view of the contained »Retention policy« tab is a list of retention periods for the selected entity. The user can edit only the explicit retention periods.
The inherited retention periods cannot be edited.

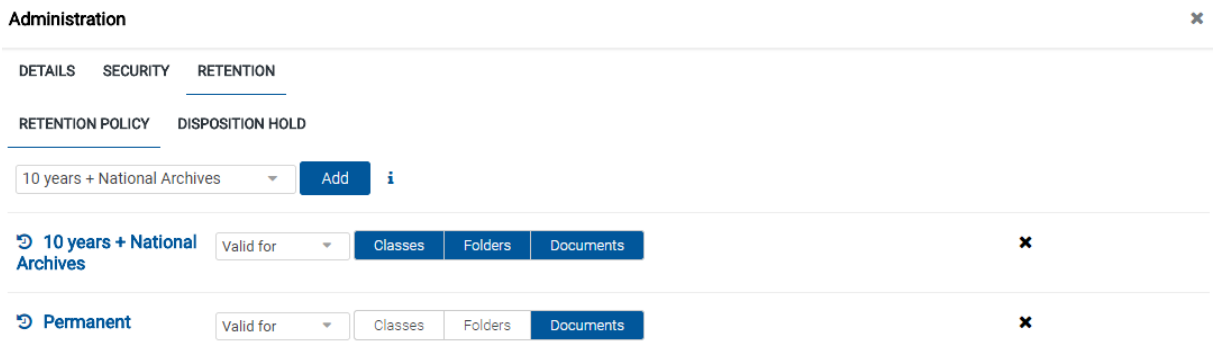

Image 72: The »Retention policy« tab in editing mode

If the retention period is not given on the list, the user can select and add it using the »Add« button in the top part of the view.

For each retention period the user specifies the validity and type of entity to which it refers:

- Classes: the retention period is valid for all classes under and including the selected entity.
- Folders: the retention period is valid for all folders under and including the selected entity.
- Documents: the retention period is valid for all documents under the selected entity.

The retention period can be valid for or not valid for a specific type of entity.

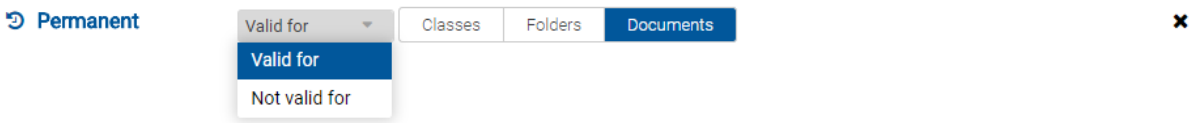

Image 73: Selecting validity for a specific type of entity

2018 © Imaging Systems Inc., All rights reserved.

The user can remove explicit retention periods from the list by clicking on the cross at the end of the record of an individual retention period.

Image 74: The record of retention period with the removal option

The user confirms the changes to the retention periods with the »Save« command or cancels them by selecting the »Cancel« command.

In the central part of the view of the contained »Disposition hold« tab is a list of disposition holds for the selected entity.

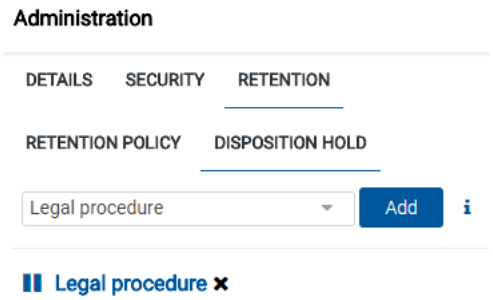

Image 75: The »Disposition hold« tab in editing mode

If the disposition hold is not given on the list, the user can select and add it using the »Add« button in the top part of the view.

The user can remove disposition holds from the list by clicking on the cross at the end of the record of an individual disposition hold.

The user confirms the changes to the disposition holds with the »Save« command or cancels them by selecting the »Cancel« command.

4.3.3.7 Changing the status of an entity

For changing the status of an entity, the user has to have the »Change status« permission on the entity. The user can change the current status on existing entities by selecting the »Actions« command in the command bar and the »Status« action in the popup menu.

2018 © Imaging Systems Inc., All rights reserved.

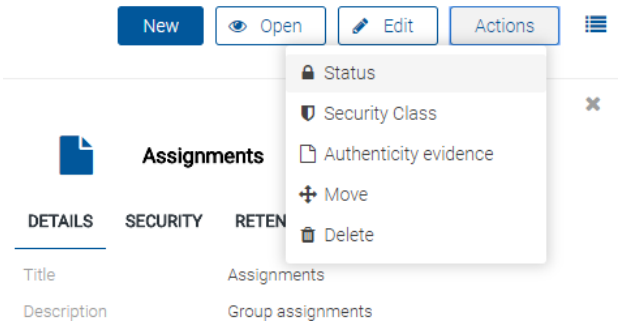

Image 76: The popup menu for selecting the »Status« command

In the »Change status« dialog box in the »Status« field the user selects the desired status from the drop-down menu.

The following predefined status values are possible:

- »Inherited«: the status of the entity is implicitly inherited from the parent entity.
  In the case of root classes, this status is equal to »Opened«.
- »Opened«: the status of the entity becomes explicitly »Opened«.
- »Closed«: the status of the entity becomes explicitly »Closed«.

The user writes a reason for the status change in the »Reason to change« field.

The change of status for the selected entity is confirmed using the »Save« button.

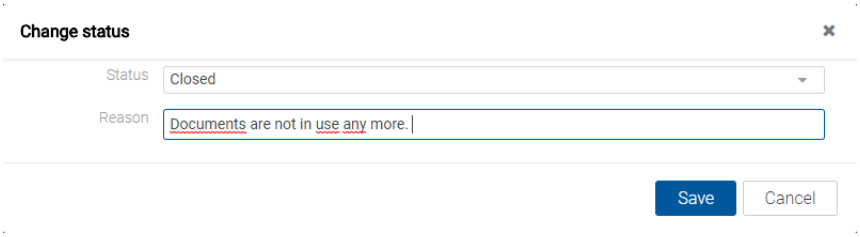

Image 77: Selecting the status and giving the reason for the change

4.3.3.8 Changing the security class

To change an entity's security class, the user must have the »Change security class« access right on the entity.

The user can change the current security class on existing entities by selecting the »Actions« command in the command bar and »Security class« in the popup menu.

2018 © Imaging Systems Inc., All rights reserved.

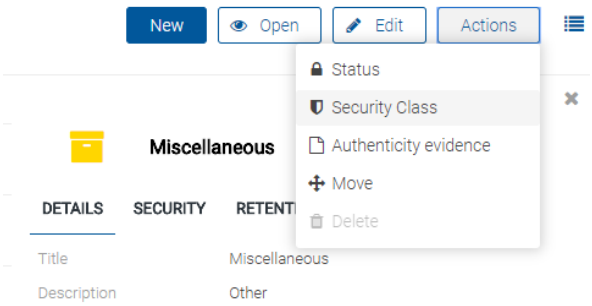

Image 78: The popup menu for selecting the »Security class« command

In the »Change security class« dialog box in the »Security class« field the user selects the desired security class from the drop-down menu.

The following predefined values are available (listed from lowest to highest):

- »Inherited«: the entity's security class is implicitly inherited from the parent entity. In case of root classes, the security class value is removed.
- »Unclassified«: access to the entity is not limited.
- »Restricted«: the entity is an internal matter. It can only be accessed by users with a clearance level »Restricted« or higher.
- »Confidential«: the entity is confidential. It can only be accessed by users with a clearance level »Confidential« or higher.
- »Secret«: the entity is considered secret. It can only be accessed by users with a clearance level »Secret« or higher.
- »Top Secret«: the entity is considered top secret. It can only be accessed by users with the »Top Secret« clearance level.

The user enters the reason for the change of security class into the »Reason to change« field. The change is confirmed by clicking the »Save« button.

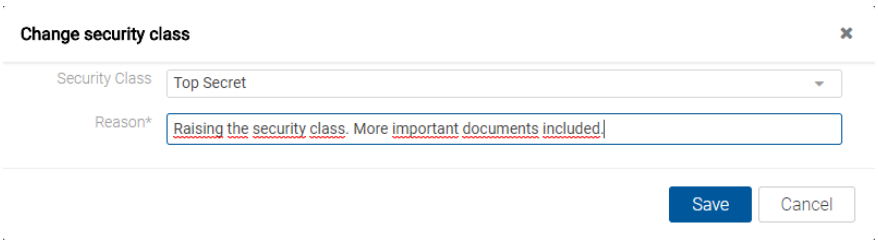

Image 79: Selecting the security class and giving the reason for the change

2018 © Imaging Systems Inc., All rights reserved.

4.3.4 Content management

This chapter describes the following actions over document contents:

- Capturing content.
- Reviewing information on the content.
- Saving content.
- Previewing content.
- Updating content.
- Downloading content.
- Moving content.
- Deleting content.
- Indexing content.
- Converting content.

4.3.4.1 Capturing content

The IMiS®/wClient enables the capture of those content, that are supported by the IMiS®/ARChive Server and can be described using the IANA-registered content type (MIME type).

The format of the file is recognized from the file's extension. If the file extension is wrong, it is possible the recognized format will also be wrong.

Example:

- *Long-term content storage formats (TIFF, PDF/A).*
- *Formats related to email (e.g. EML, VCF).*
- *Various text, image and graphics formats (e.g. TXT, JPG, DWG).*
- *Microsoft Office formats (e.g. DOCX, XLSX, PPTX).*
- *Webpage file formats (e.g. HTML, XML).*
- *Compression formats (e.g. ZIP, TGZ).*
- *Audio-video formats (e.g. AVI, MP4).*
- *...*

By selecting a document, the user is shown a list of contents in the central view.

In the case of a new document the list is empty. The contents are shown below the bar with the titles of the common attributes. »Description« and »Size« are shown by default.

2018 © Imaging Systems Inc., All rights reserved.

Note:

Attaching contents is possible only in the Document entity type.

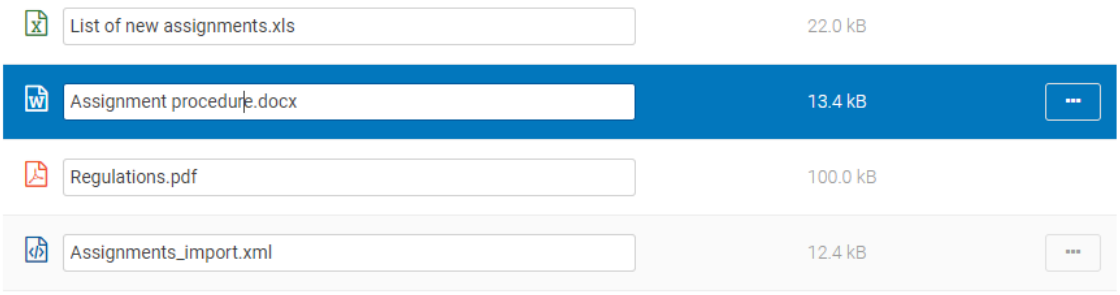

Image 80: Display of the list of contents in the central view

The user adds contents by first selecting the »Edit« button in the command bar.
This opens a dialog box with entity details, in which the user drops content in the »Content« field using the »Drag and drop« mode or clicks it on the list.

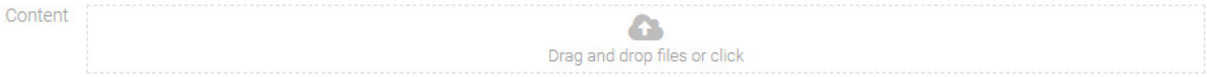

Image 81: The »Content« field for dropping contents

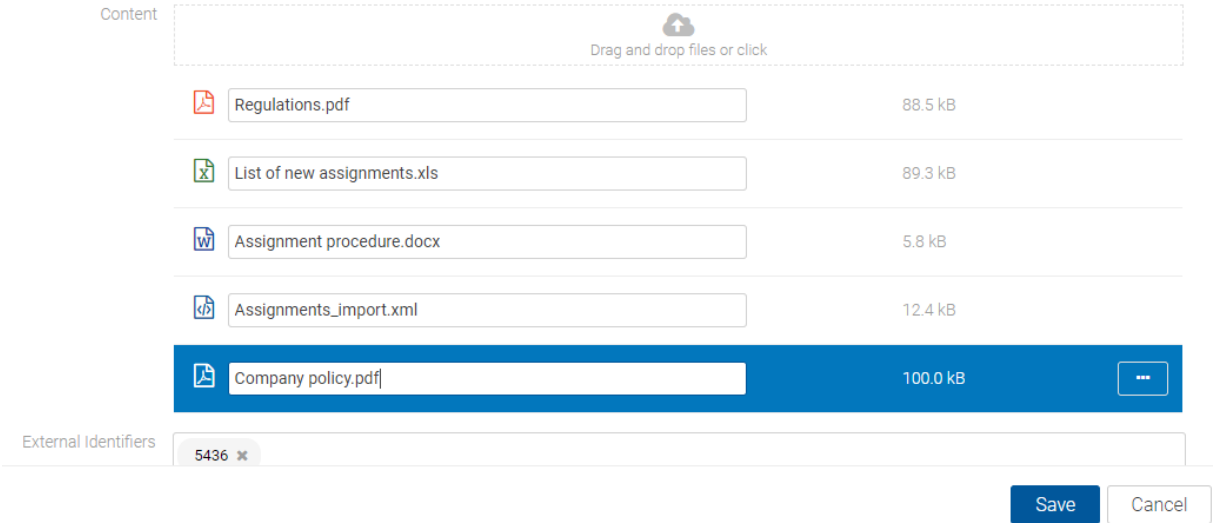

Image 82: The added content before saving

After confirmation the contents are added to the list under the »Content« field. After the user has finished capturing contents, the document can be saved (see chapter Saving an entity).

2018 © Imaging Systems Inc., All rights reserved.

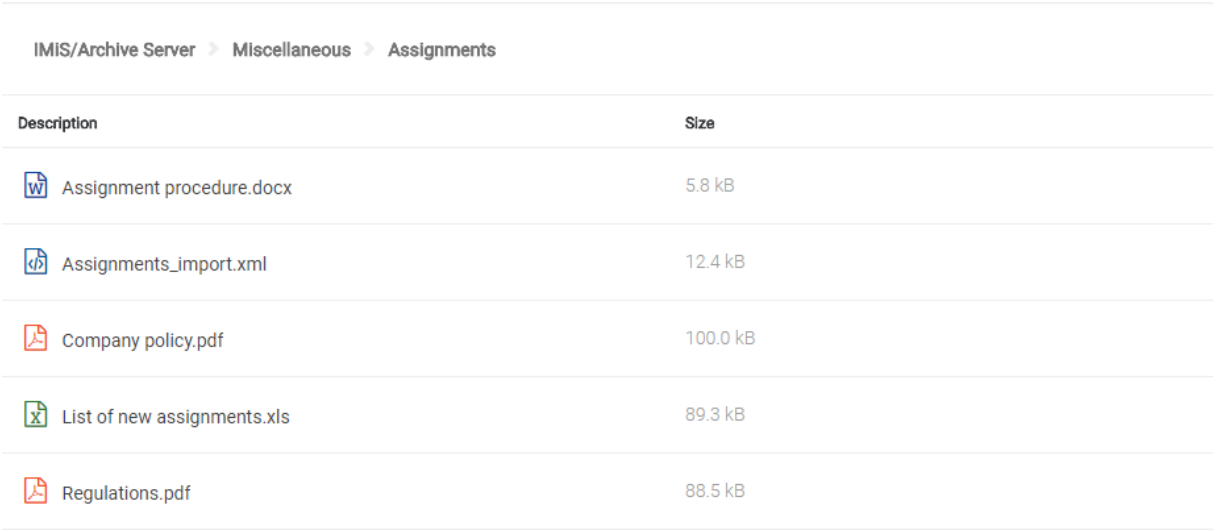

Image 83: The added content after saving

4.3.4.2 Content details

The entity content details provide certain information to the user which is otherwise not shown in the list of contents. If the details are not shown in the right view by default, the user can access them by selecting the »Details« command in the popup menu on the tagged content.

Besides the list of contents, the user is also shown the following entity content details in the right view:

- Description: Content description.
- Type: Content type.
- Content type: MIME content type.
- Size: Content size in kB.
- Created: Timestamp of the content creation.
- Modified: Timestamp of the last change of the content.
- Accessed: Timestamp of the last access to the content.
- Indexed: states whether the content is indexed.
- Signed: a value that registers if the email message was electronically signed.
- Identifier: unique identifier of the content.

Of all the displayed data the user can change only the description of the content when in entity editing mode.

2018 © Imaging Systems Inc., All rights reserved.

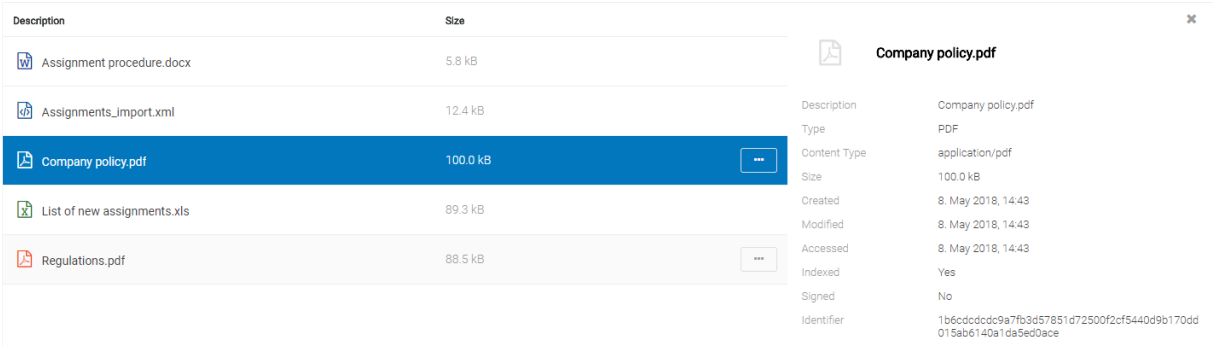

Image 84: Content details in the right view

4.3.4.3 Saving content

When saving document content to the IMiS®/ARChive Server, the following attribute values are automatically recorded into the entity:

- Content type: the type of the content output format (MIME type).

Image 85: An example of the content type of a document

- Created: the date the document content was created on the server. As long as the content exists, the attribute value does not change.

Image 86: An example of the date of creating the document content

- Modified: the date the user changed the document content. As long as the document content exists, the attribute value changes with each change of content.

Image 87: An example of the date of modifying the document content

- Accessed: the date and time the document content was last opened in reading mode or in editing mode. As long as the content exists, the attribute value changes each time the user opens or modifies the content.

Image 88: An example of the date of the last access to the document content

2018 © Imaging Systems Inc., All rights reserved.

- Identifier: The unique identifier of the content of the document saved on the server. As long as the content exists, the attribute value does not change.

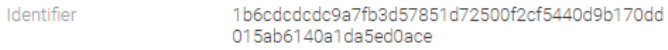

Image 89: An example of the document content identifier

- Indexed: A value that shows whether the document content is indexed.

Image 90: An example of a display of indexed document content

- Signed: A value that shows whether the document content is electronically signed.

Image 91: An example of a display of signed document content

4.3.4.4 Content preview

The user opens the document content by selecting »Preview« in the popup menu on the tagged content in the document reading mode (»Open«).

Certain contents are opened directly in the browser's viewer; if that is not possible, the contents are downloaded and opened with an external viewer.

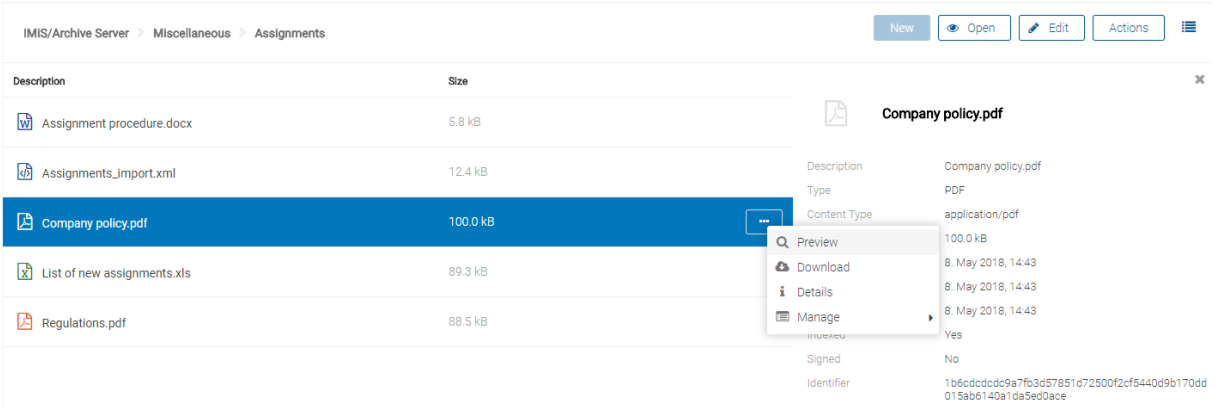

Image 92: Opening document content

4.3.4.5 Content update

The user has the option of updating saved content. In editing mode, the user selects the document content. In the popup menu the user selects the »Update« command.

This opens a dialog box for selecting the content which will replace the existing content.

If the user does not change the title of the content, it is preserved.

The user confirms the change to the entity with the »Save« command or cancels it with the »Cancel« command.

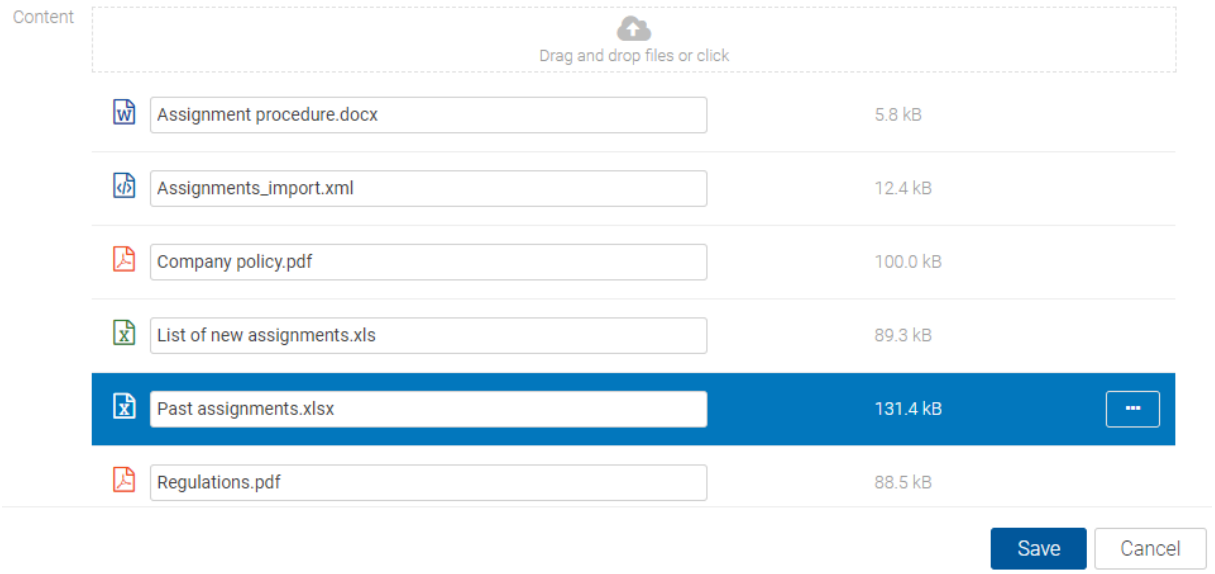

Image 93: The selected content before update

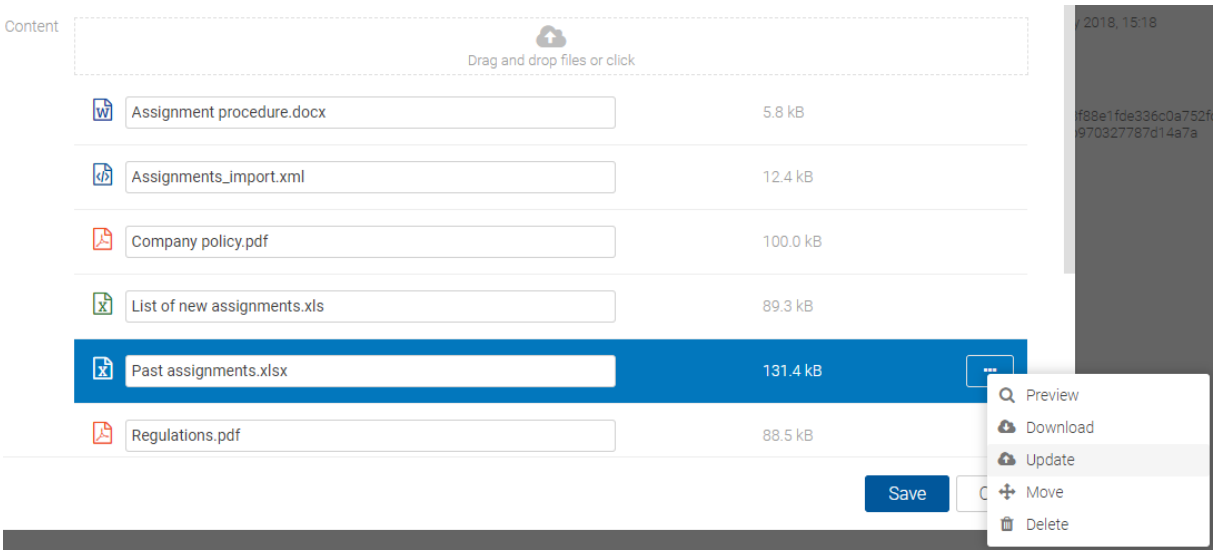

Image 94: Selecting the »Update« command in the popup menu

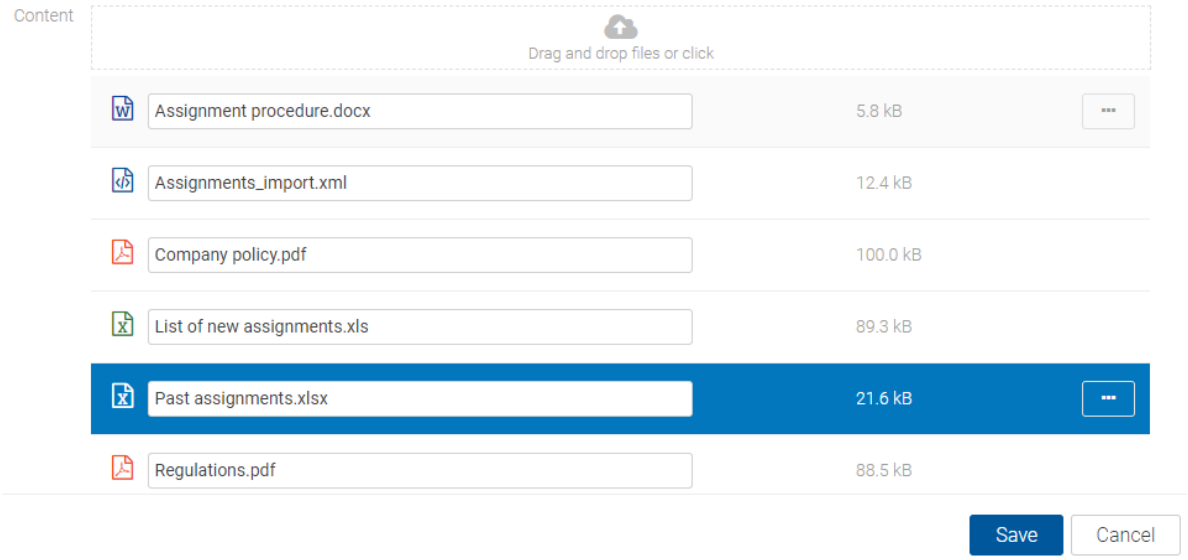

Image 95: The selected content after update

4.3.4.6 Downloading content

By selecting the »Download« command in the popup menu on the tagged content in the document reading mode (»Open«), the user downloads the content to the device. The content is saved in the selected location on the device.

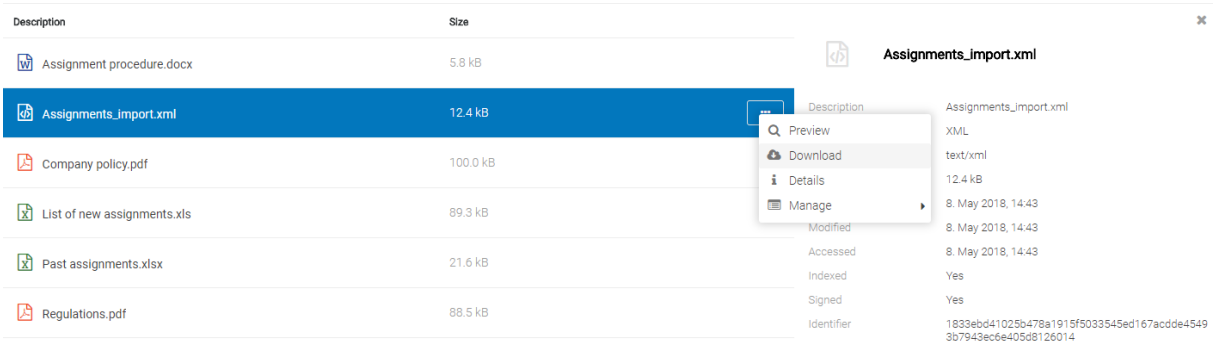

Image 96: Selecting the »Download« command in the popup menu

4.3.4.7 Moving content

Moving content from one entity to another can be performed by any user with the »Write« right. The user selects the content in the Edit mode.

By selecting the popup menu on the tagged content, the user selects the »Move« command.

2018 © Imaging Systems Inc., All rights reserved.

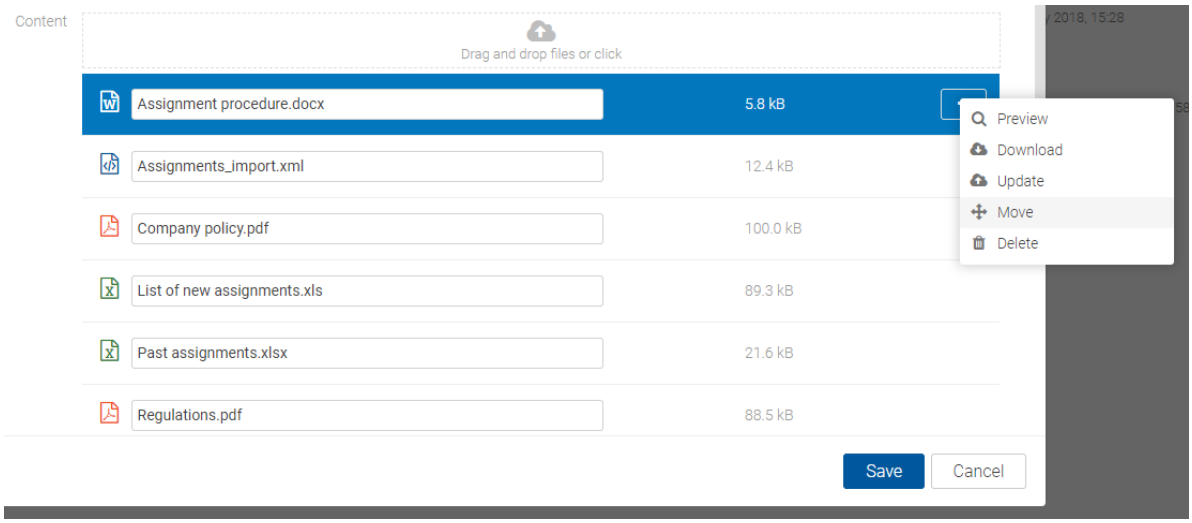

Image 97: Selecting the »Move« command in the popup menu

This opens a dialog box for selecting the target document in the classification scheme.

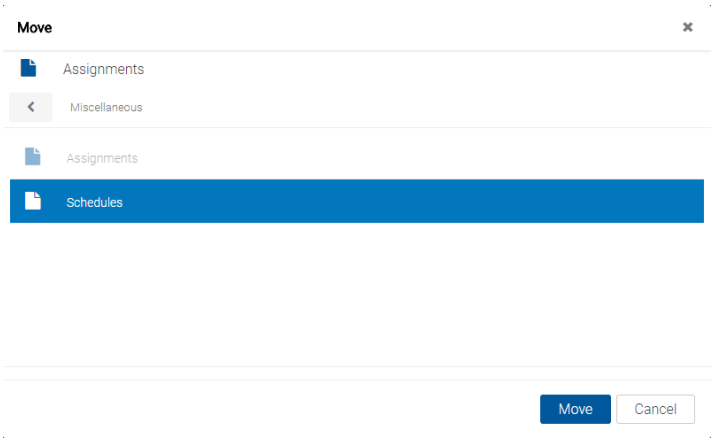

Image 98: Selecting the target document for moving content

By confirming the selection with the Move command, the content is temporarily removed from the content list.

2018 © Imaging Systems Inc., All rights reserved.

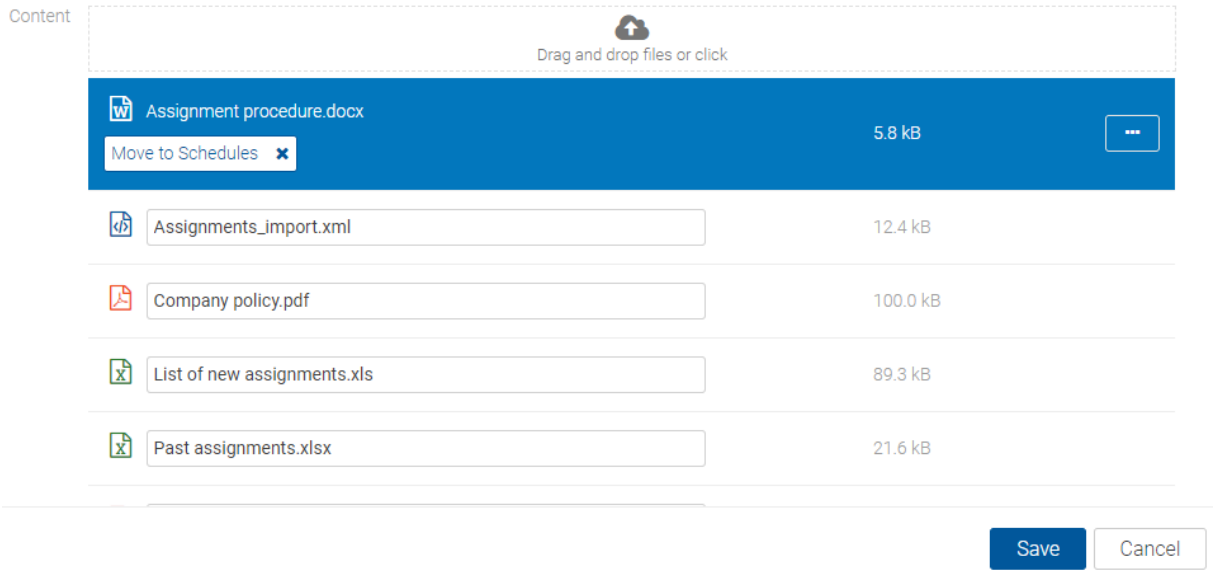

Image 99: Content temporarily removed from the document

Content migration is not performed until after saving changes.

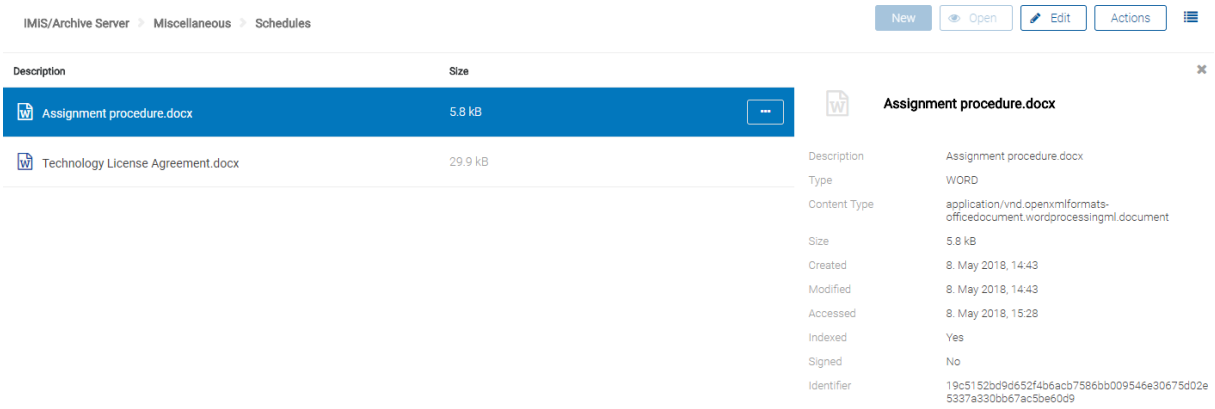

Image 100: Saved document content

4.3.4.8 Deleting content

The user removes document content by first selecting the document content in Edit mode.

In the popup menu the user selects the »Delete« command.

The content is removed from the list.

The user confirms the change to the entity with the »Save« command or cancels it with the »Cancel« command.

2018 © Imaging Systems Inc., All rights reserved.

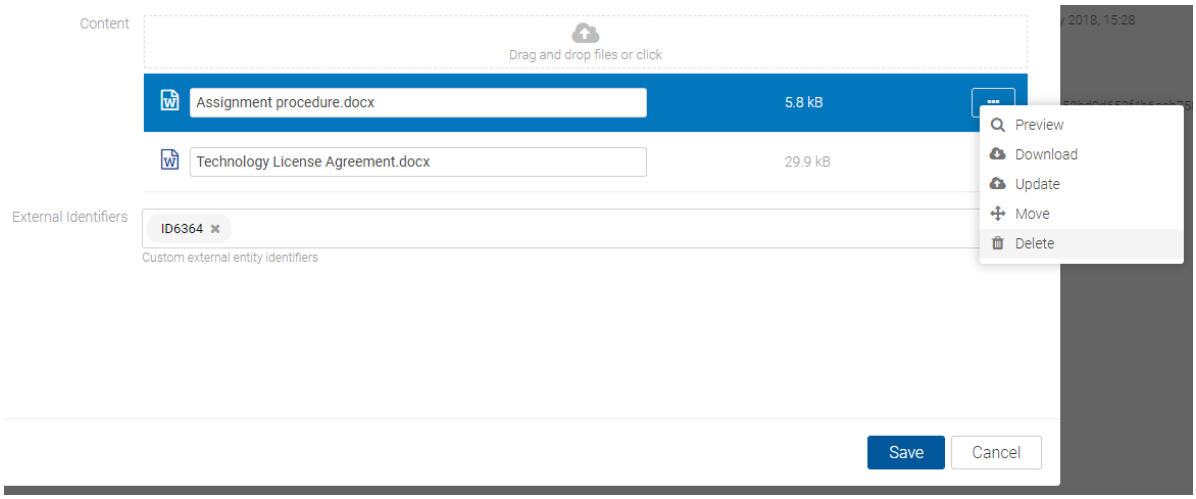

Image 101: The content on the list before deletion

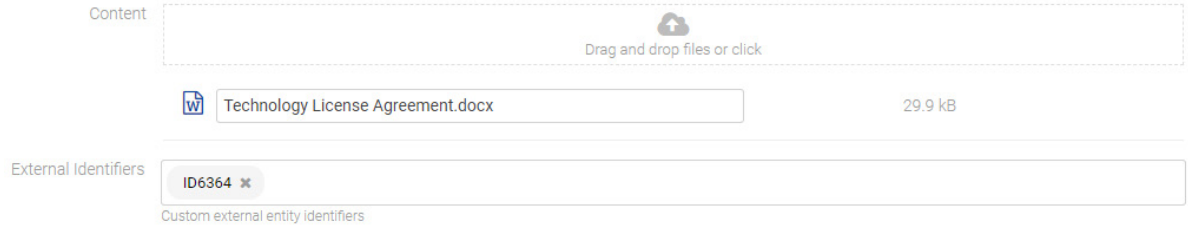

Image 102: The content on the list after deletion

4.3.4.9 Indexing content

By selecting the popup menu on the tagged content in the document reading mode (»Open«), the user can select the »Manage« command. By confirming the »Queue for Indexing« command, the selected content is tagged for later indexing.

The indexing of content can be done automatically with the appropriate settings on the IMiS®/ARChive Server or manually for an individual content within the interval specified in the server settings. For the manual tagging of content for indexing the user must have the »ContentManagement« role.

2018 © Imaging Systems Inc., All rights reserved.

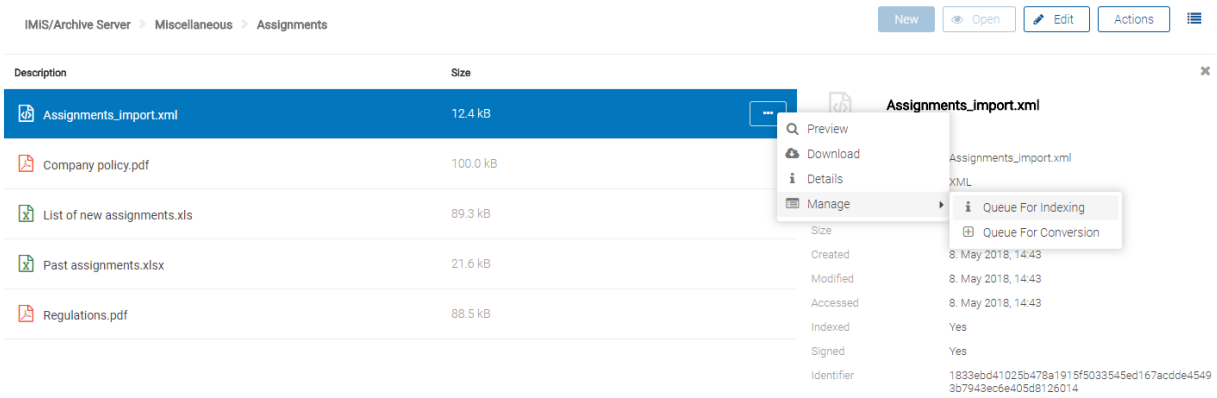

Image 103: Selecting the »Queue for Indexing« command

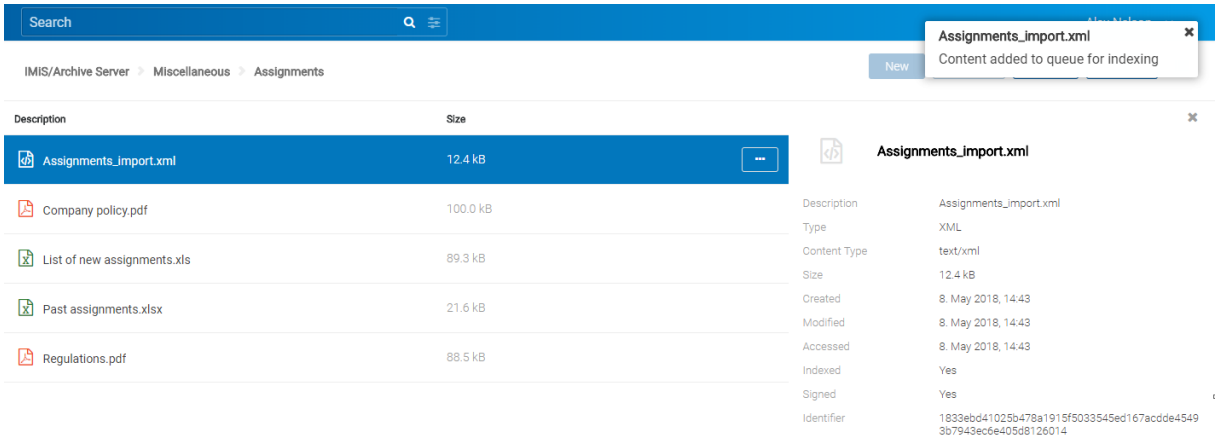

Image 104: Successful adding of content for indexing

4.3.4.10 Content conversion

By selecting the popup menu on the tagged content in the document reading mode (»Open«), the user can select the »Manage« command. By confirming the »Queue for Conversion« command, the selected content is tagged for later conversion.

The conversion of content can be done automatically with the appropriate settings on the IMiS®/ARChive Server or manually for an individual content within the interval specified in the server settings. For the manual tagging of content for conversion the user must have the »ContentManagement« role.

2018 © Imaging Systems Inc., All rights reserved.

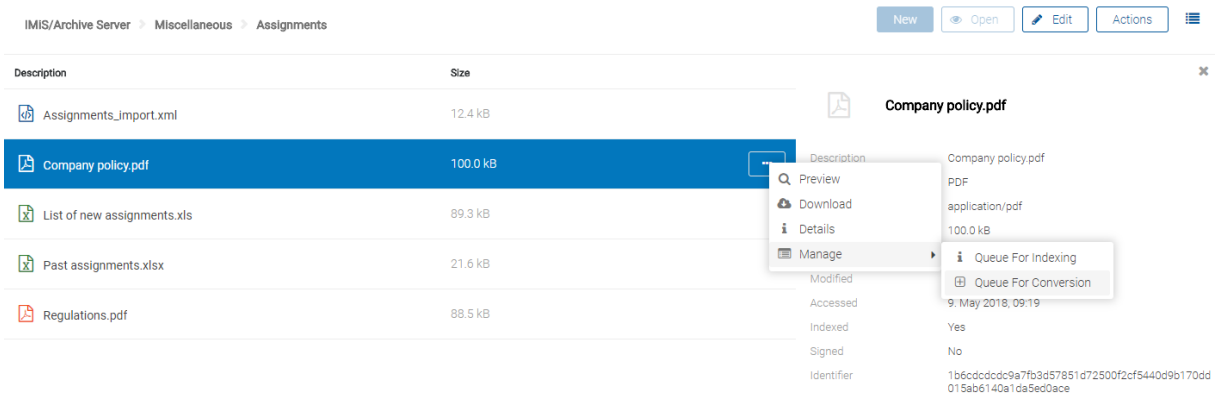

Image 105: Selecting the »Queue for Conversion« command

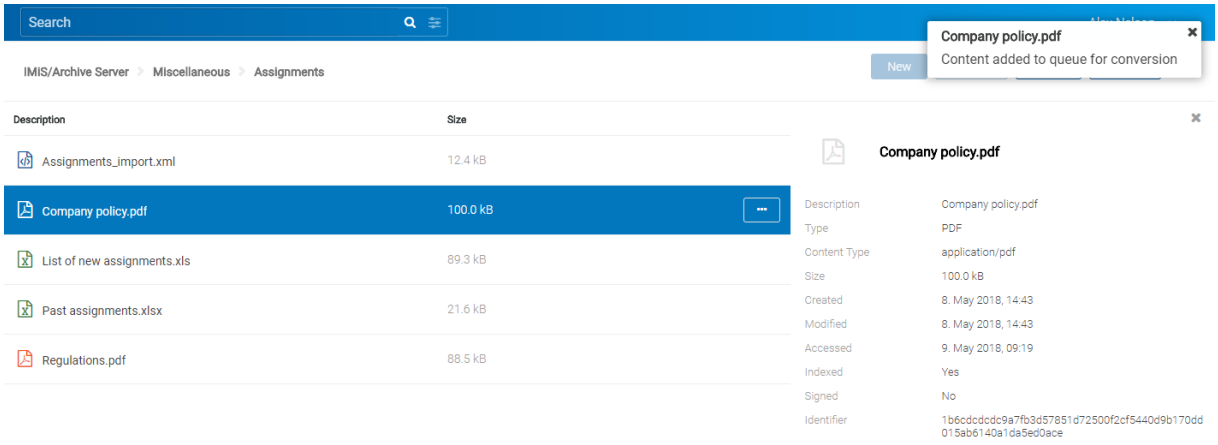

Image 106: Successful tagging of content for later conversion

4.3.5 Search functions

The IMiS®/ARChive Server enables users to search by:

- Metadata of the class, folder and document.
- Full text of the content attached to the document.
- Title of content contained by the document.
- Metadata and full text of content, simultaneously.

Users may only search entities they are authorized to access. Search functions are available for the selected entity, or the entire server archive.

The search engine is made up of two sets which refer to: conditions for searching by metadata, by content descriptions, and by the full text of document contents.

2018 © Imaging Systems Inc., All rights reserved.

4.3.5.1 Full text search

The user begins searching the full text of the content by entering a search string in the »Search« field in the header of the user interface. The user confirms it by selecting the icons, which denote a search.

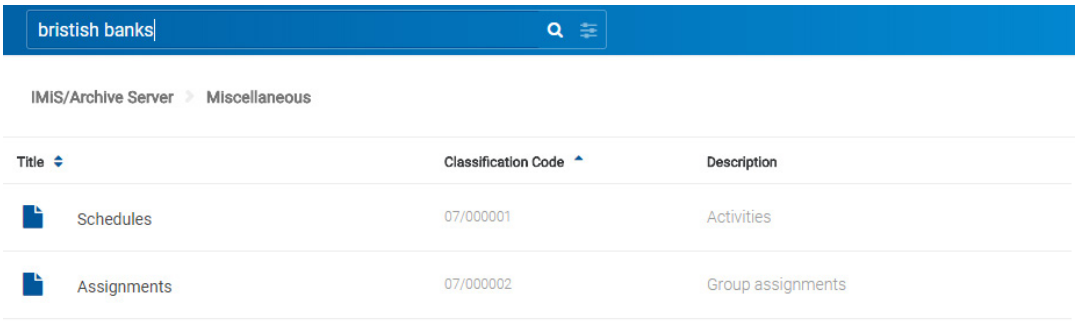

Image 107: Entering a search string in the »Search« field

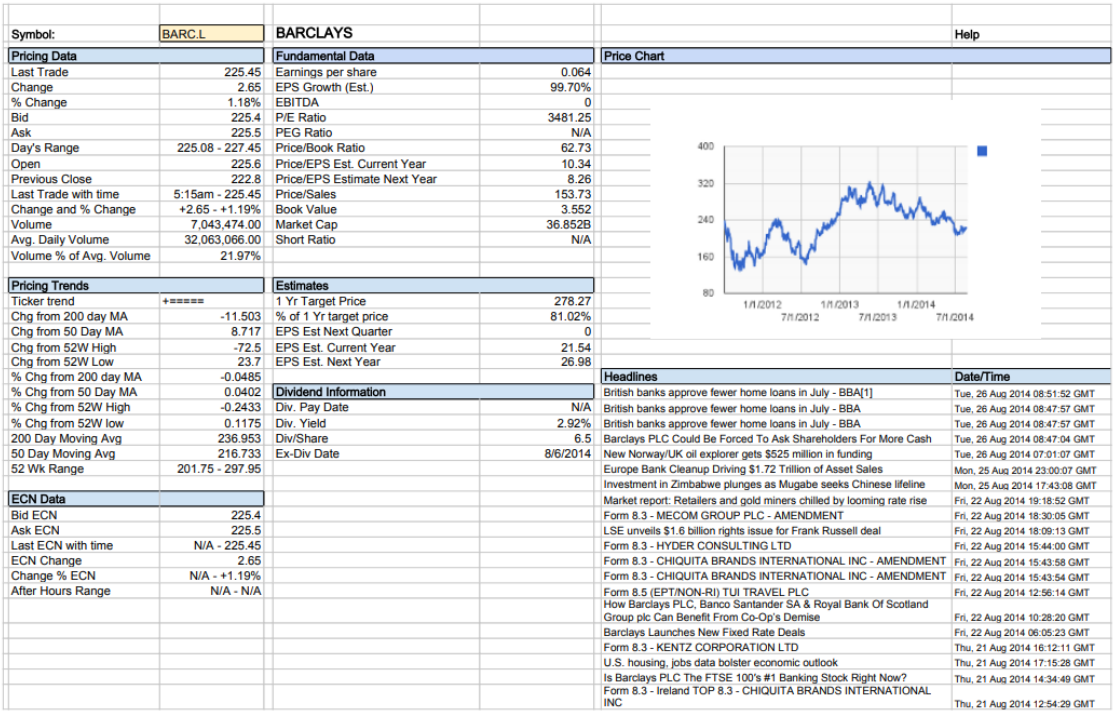

Image 108: A full text search result

An alternative way of searching the full text of the content is by selecting the icon in the header of the user interface and entering the search string in the »Full text search« field in the »Search« dialog box.

2018 © Imaging Systems Inc., All rights reserved.

The user can create a search string from one or multiple simple search conditions.

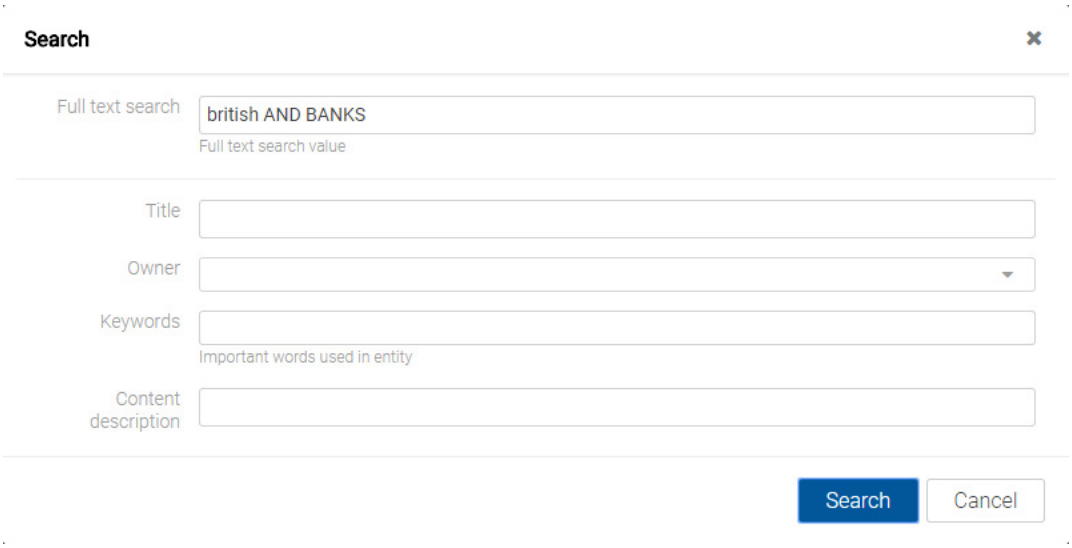

Image 109: Entering a search string in the »Full text search« field

The full text search is case insensitive and searches only by the text file formats from which the IMiS®/ARChive Server can extract the text.
The user can also perform a wildcard search by using the special characters »*« and »?« in the search string.

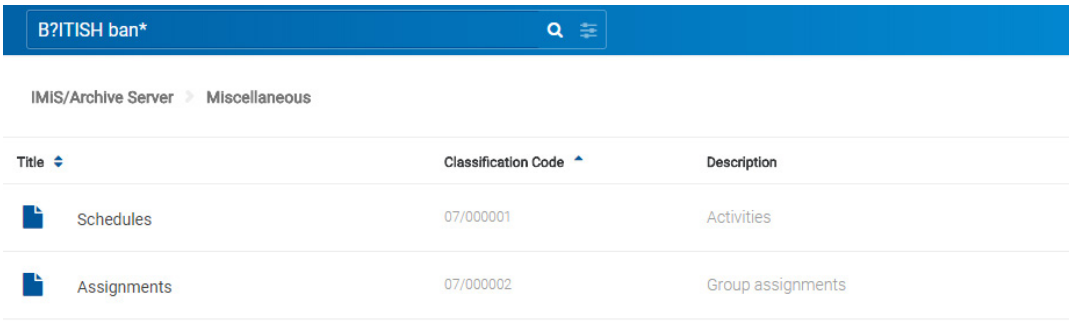

Image 110: A wildcard search by using special characters

Besides values and special characters, the user can also use »Operator« in the search string. It is about the logical operators for chaining simple search conditions into complex search conditions. The available operators are the logical inclusive (AND), the logical interchangeable (OR), and the logical mutually exclusive (XOR).

2018 © Imaging Systems Inc., All rights reserved.

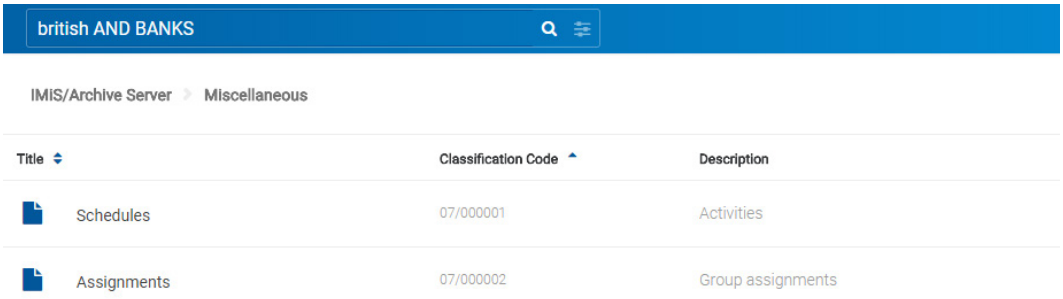

Image 111: Searching using operators

Examples:

A user is searching for entities in the full text of the content. Based on the search string:

- ****test*** *returns an error. Such syntax is not allowed.*
- ***te*st*** *finds all document contents with words beginning with »te« and ending with »st« (i.e. telephonist, terrorist, ...).*
- ***te?t*** *finds all document contents in which the third letter of the word is unknown (i.e. test, text, ...).*
- ***test**** *finds all document contents with the word »test« (i.e. tests, testing, ...).*
- ***test result*** *finds all document contents with words »test« or »result«.*
  The rule is that if there are no logical operators between the words, operator OR will be used.
- ***test AND result*** *finds all document contents with words »test« and »result«. Logical operators must be written in uppercase.*
- ***»test result«*** *finds all document contents with words »test result« written in succession.*
- ***»test result*«*** *finds all document contents with words »test result« written in succession, with the possibility that the second word can also be longer (i.e. results, resultados, ...)*

Formats supported by the full text search function are:

- HTML, XML and similar formats.
- Microsoft Office, OpenOffice and iWork formats.
- RTF format.
- PDF format.
- Text formats.
- Audio format metadata (metadata of WAV, MIDI, MP3, MP4, OGG).
- Image format metadata (metadata of BMP, GIF, PNG, PSD; EXIF for JPEG, TIFF).
- Video format metadata (metadata of FLV, MP4).
- Email formats (PST, MBOX, EML).
- PKCS7 formats.

2018 © Imaging Systems Inc., All rights reserved.

- Electronic publication formats (EPUB, FB2).
- Web feed and news formats (RSS, ATOM, IPTC, ANPA).
- DWG format.
- CHM format.
- Font formats (TTF, AFM).
- Scientific formats (HDF, NETCDF, MAT).
- Program and library formats (ELF, PE).
- Compression formats (TAR, CPIO, ZIP, 7ZIP).

The search result is shown in the central view of the user interface. It contains only the list of entities or contents to which the user has access.

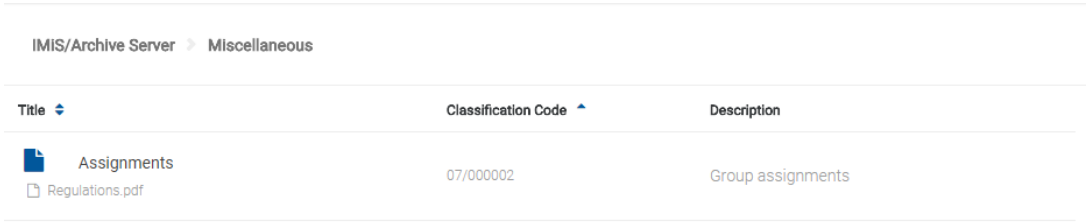

Image 112: An example of a search result

4.3.5.2 Search by metadata

The user can search by metadata by selecting the icon in the header of the user interface and selecting the values from the list, or by entering a search string in the following fields in the »Search« dialog box:

- Title: name of the entity.
- Owner: owner of the entity.
- Keywords: keywords related to the entity.

Creates a search string from one or multiple simple search conditions.

2018 © Imaging Systems Inc., All rights reserved.

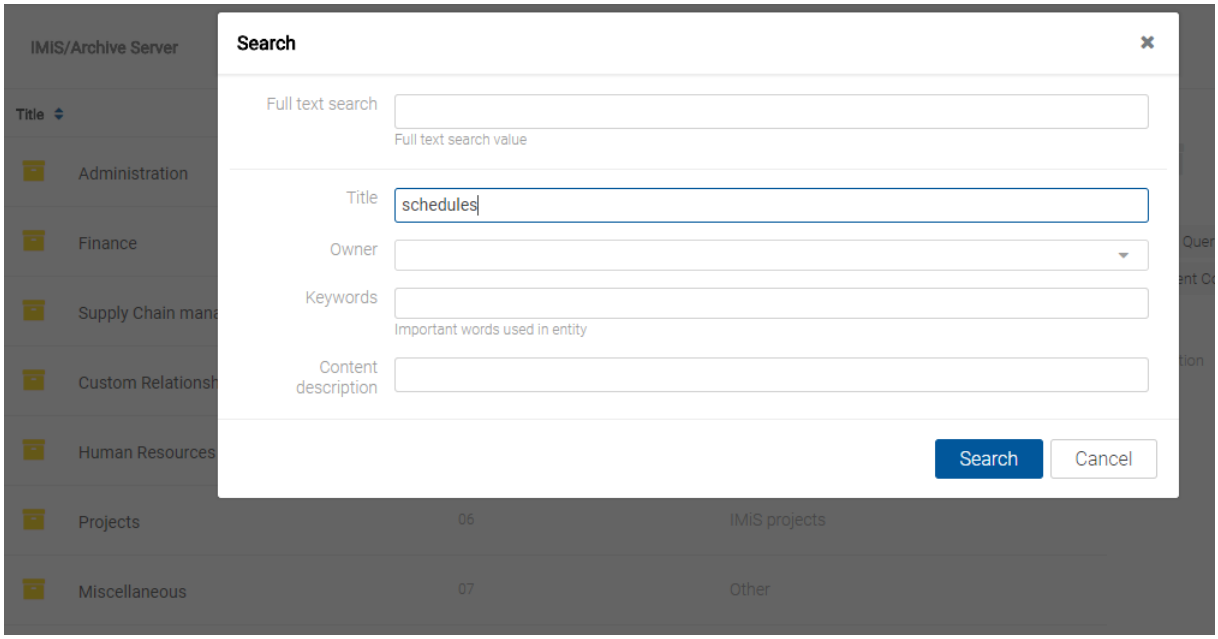

Image 113: A dialog box for searching by metadata

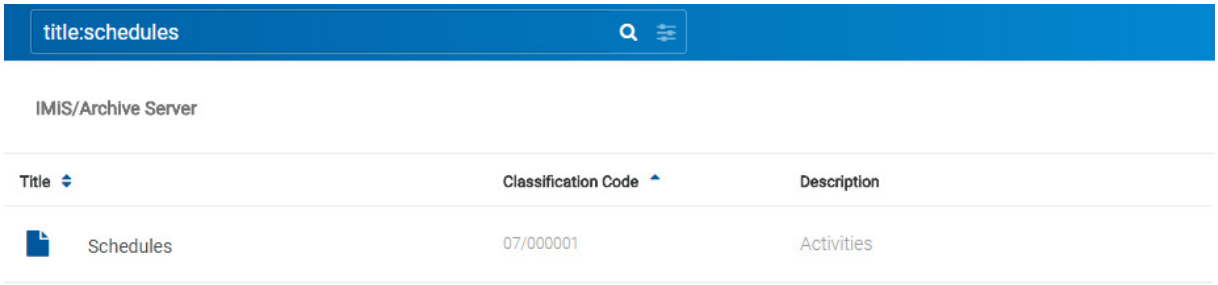

Image 114: An example of a metadata search result

When choosing text metadata, the search value must be text. When searching text metadata, the value does not have to be exactly identical. The IMiS®/wClient also allow you to perform a »Wildcard search« by using special characters in the search string:

- »*« means zero or more characters of any kind
- »?« means any character.

2018 © Imaging Systems Inc., All rights reserved.

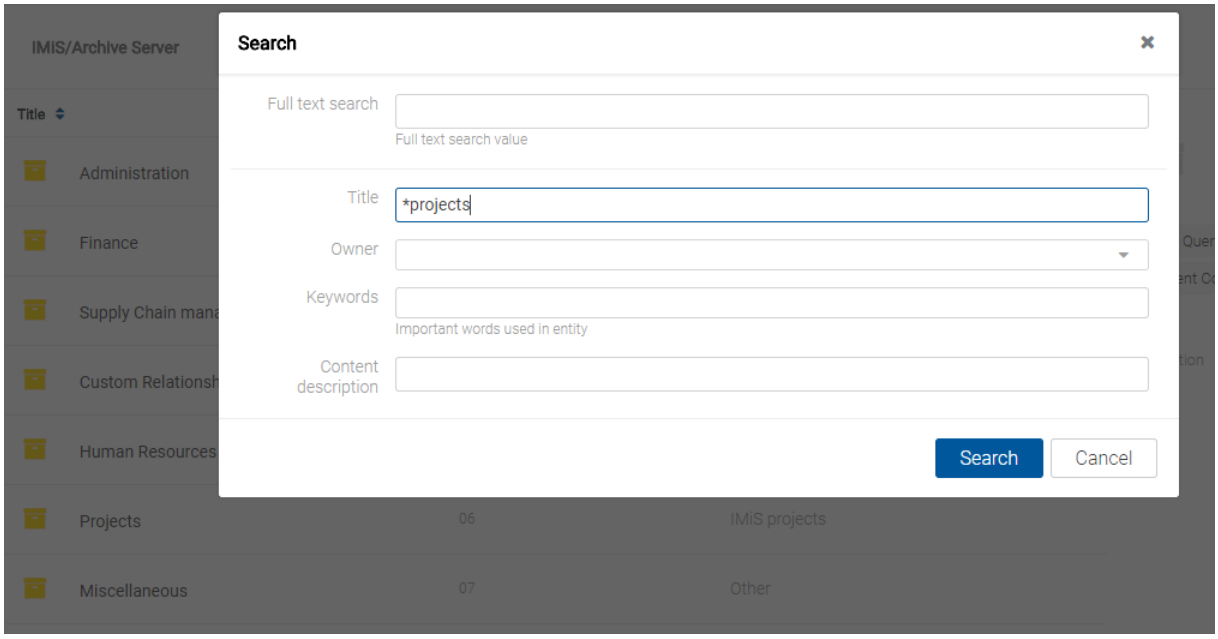

Image 115: Use of special characters in a search string

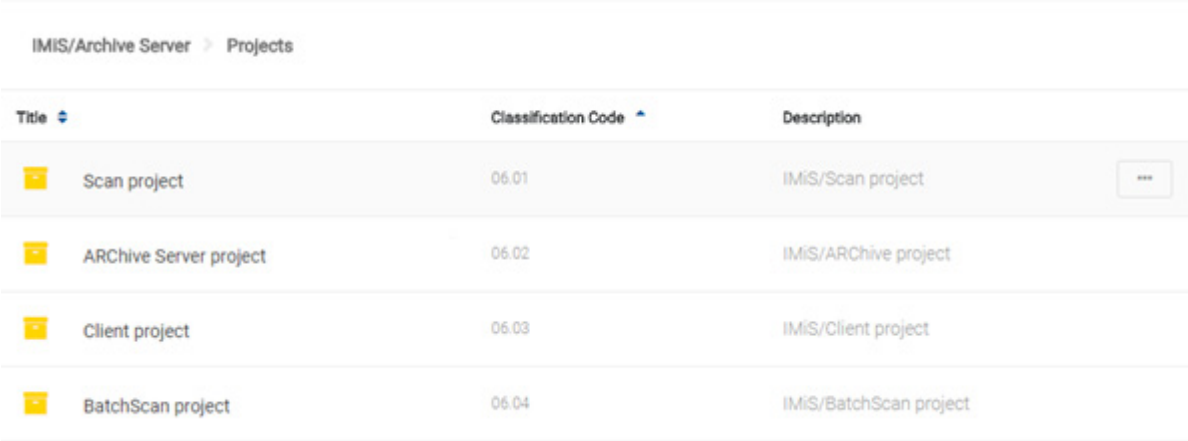

Image 116: An example of a result of searching by metadata using special characters

Note:

The user does not have to pay attention to the use of small and capital letters, because the search is case insensitive.

2018 © Imaging Systems Inc., All rights reserved.

Example:

If the user is searching entities by the »Title« metadata, the search string:

- *»a*« searches for entities whose title starts with the letter »a«. For example, producing: »aa«, »Administration«, »authorization«, »A-test« and »Auto Service«.*
- *»*traffic*« searches for entities that have a string of characters »traffic« in the title*
  For example: »traffic light«, »havy traffic«, »road traffic jam «.
- *»*en« searches for entities whose title ends with a string of characters »en«.*
  For instance: »then«, »when«, »hen«, »maiden«.
- *»d?b« searches for entities whose title has a specified first and third letter (in this case »d« and »b«), while the second letter and all other letters can be random.*
  For example, producing: »debate«, »Debit«, »dab« or »dubious claims«.

This does not work when searching metadata whose value is represented by the name of a IMiS®/ARChive Server user (for example the metadata »Owner«).

For these values, the search string must be identical to the value of the metadata.

Instead of manually entering the title of the owner into the search string, the user selects it from the set of available users.

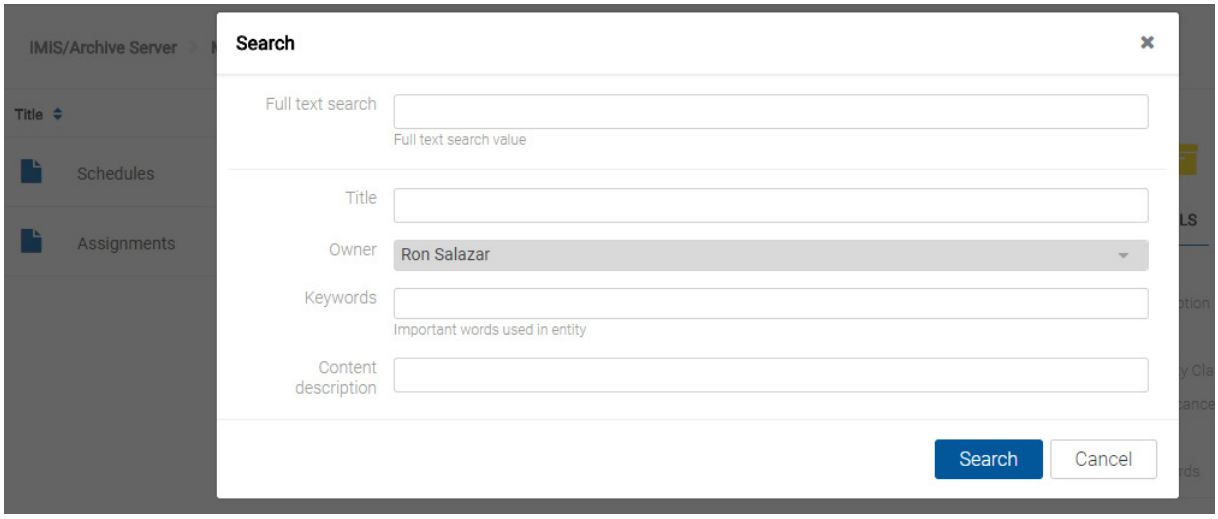

Image 117: A dialog box for searching by the metadata »Owner«

Type:

To make the archive clearer, the administrator should, if possible, recommend a standard structure for naming entities and metadata (upper and lower case, abbreviations…) saved to the server.

2018 © Imaging Systems Inc., All rights reserved.

4.3.5.3 Search by content descriptions

The user searches by the document content description by selecting the icon in the header of the user interface and entering the search string into the »Content description« field in the »Search« dialog box.

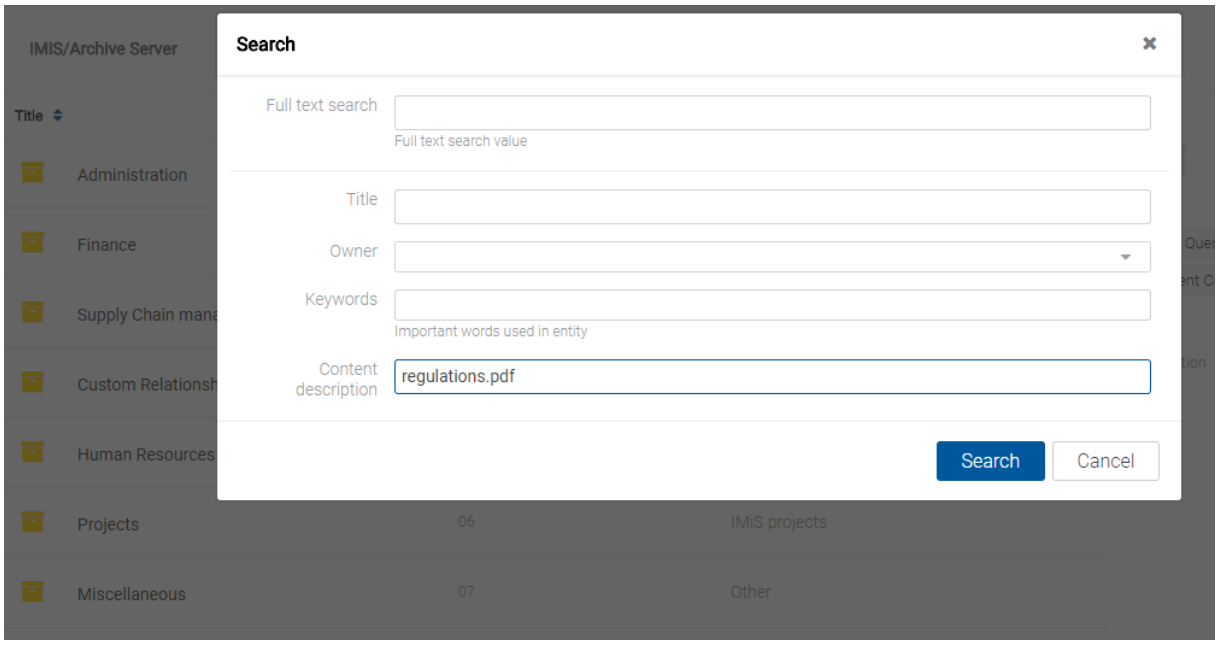

Image 118: A dialog box for searching by the content description

The IMiS®/wClient can perform a »wildcard search« by using special characters in the search string:

- »*« means zero or more characters of any kind.
- »?« means any character.

2018 © Imaging Systems Inc., All rights reserved.

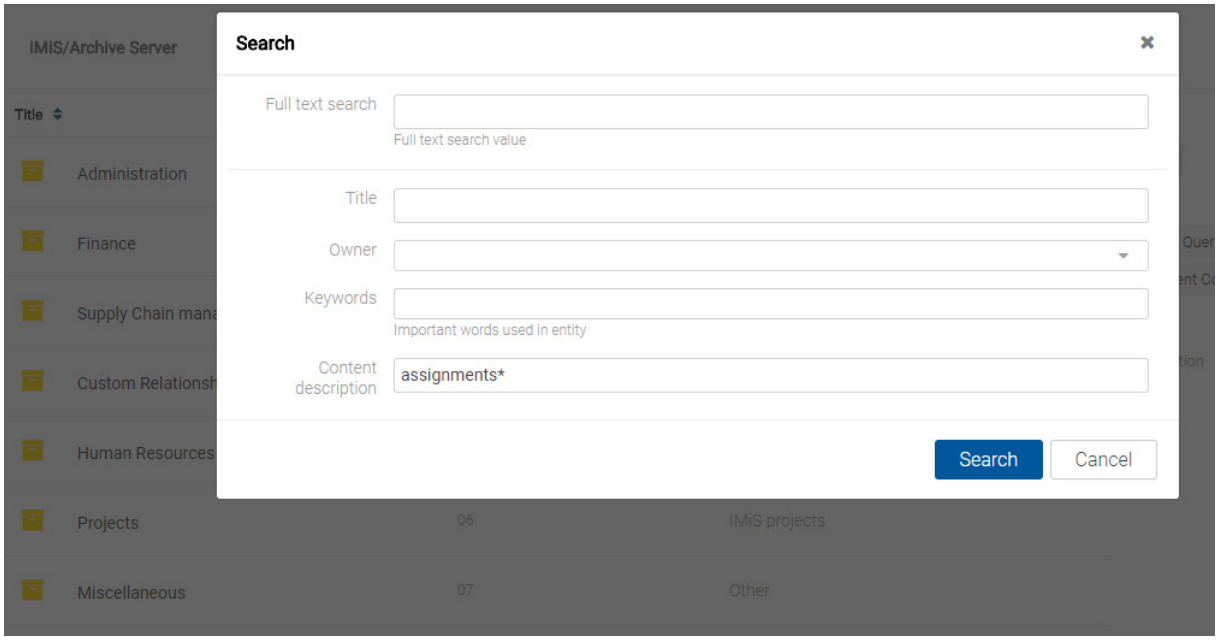

Image 119: Use of special characters in a search string

The user does not have to pay attention to the use of small and capital letters, because the search by the content description is case insensitive.

Example:

If the user is searching entities by the content descriptions, the search string:

- *»a*« searches for entities containing contents whose titles begin with the letter »a«.*
  For example, producing: »aa«, »Administration«, »authorization«, »A-test« and »Auto Service«.
- *»*traffic*« searches for entities containing contents whose titles contain the »traffic« character string.*
  For example: »traffic light«, »havy traffic«, »road traffic jam «.
- *»*en« searches for entities containing contents whose titles end with the »en« character string.*
  For instance: »then«, »when«, »hen«, »maiden«.
- *»d?b« searches for entities containing contents whose titles have a specific first and third letter (in this case »d« and »b«), while the second letter and all other letters can be random.*
  For example, producing: »debate«, »Debit«, »dab« or »dubious claims«.

2018 © Imaging Systems Inc., All rights reserved.

In the central view the user is shown the search results.

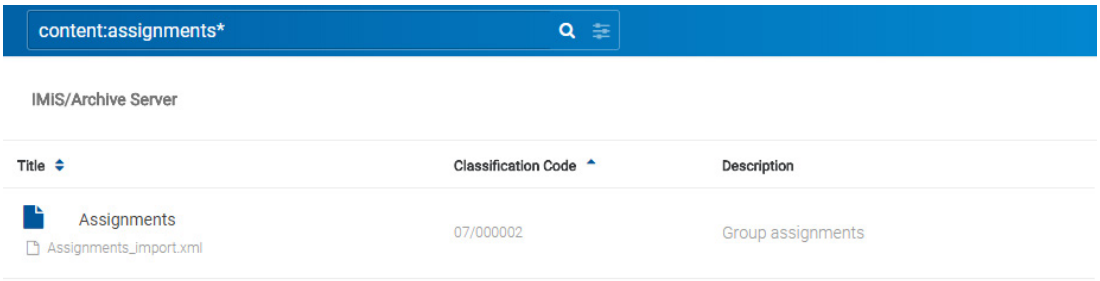

Image 120: Results of searching by the document contents description

4.3.5.4 Combined search

The user can also perform the following combinations of searches:

- By metadata and the full text of the content.
- By metadata and the content description.
- By the full text of the content and the content description.

The user performs a combined search by selecting the icon in the header of the user interface and entering the search strings into the relevant fields, or by selecting the value of the attribute »Owner« from the list in the »Search« dialog box.

Note:

The combined search takes the logical operator »AND« into account.

4.3.5.4.1 Combined search by metadata and full text search

The user can simultaneously search by metadata and by the full text of the content.

The search result is all documents containing the searched metadata (e.g. Owner = Keira Clay) and whose content also contains the searched text (e.g. exclusive).

The searched text can contain one or multiple simple search conditions.

2018 © Imaging Systems Inc., All rights reserved.

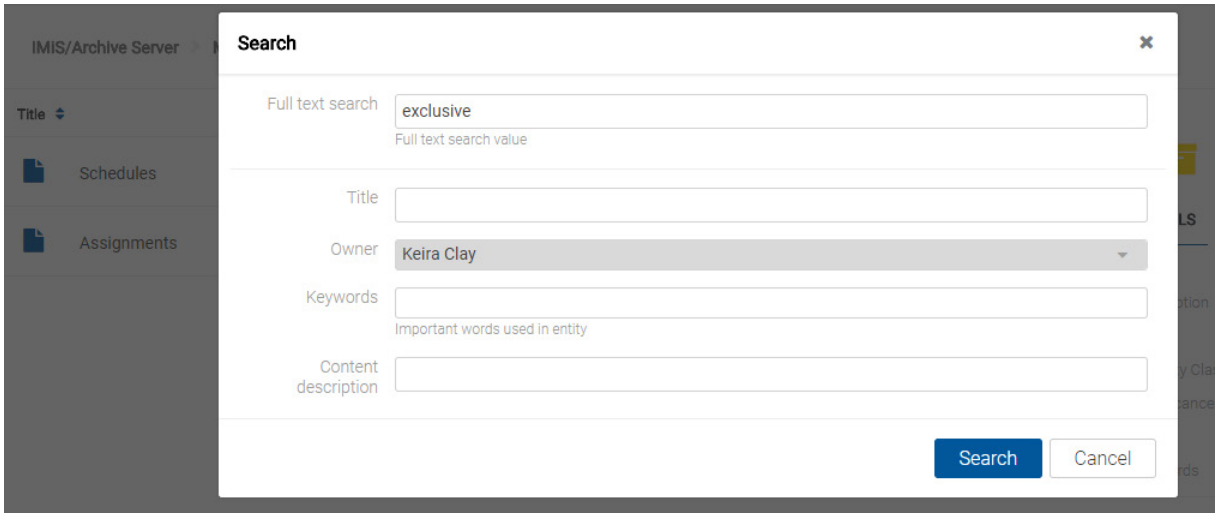

Image 121: Entering a search string in a combined search

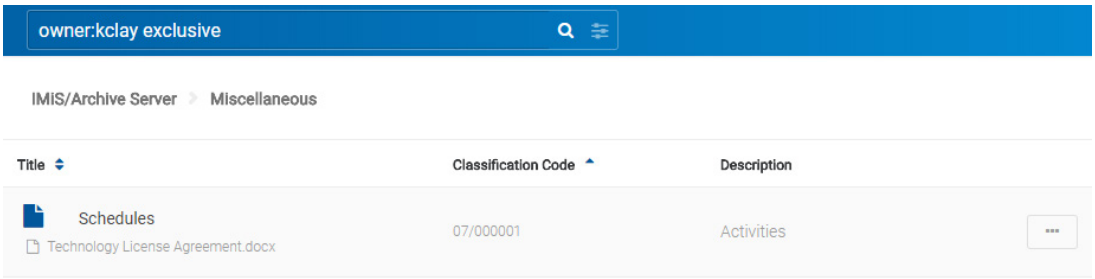

Image 122: Results of searching by metadata and the text of the content

4.3.5.4.2 Combined search by metadata and content descriptions

The user can simultaneously search by metadata and by the content description.

The search result is all documents containing the searched metadata (e.g. Title = meeting) and whose content descriptions also contain the searched text (e.g. IMiS).

2018 © Imaging Systems Inc., All rights reserved.

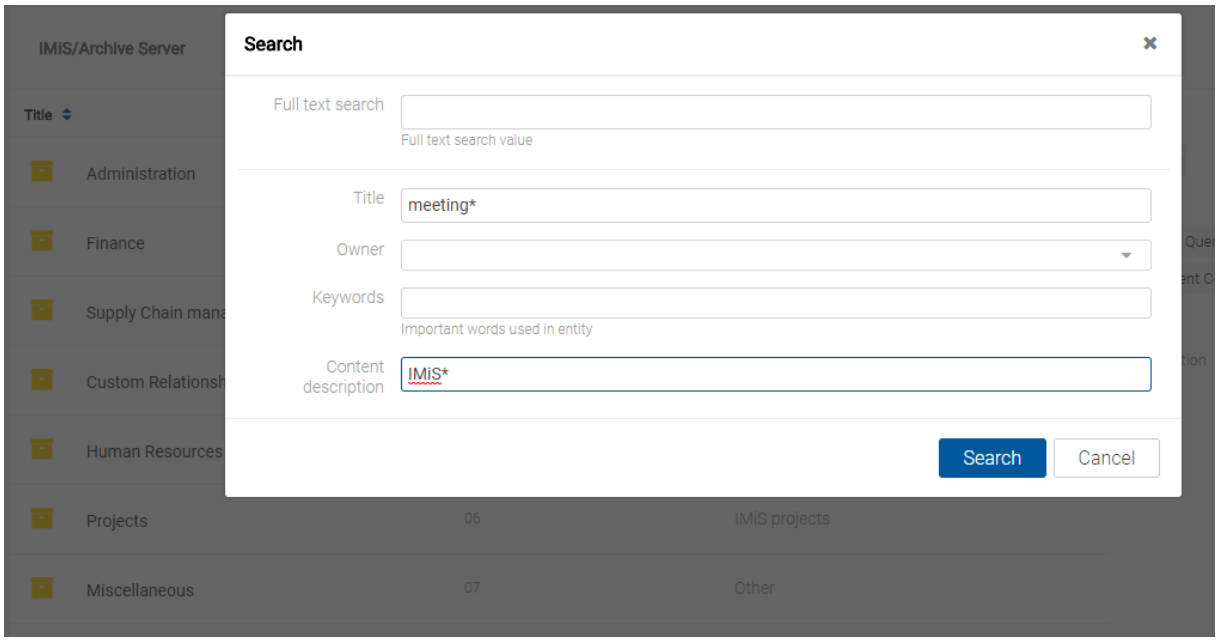

Image 123: Entering a search string when searching by metadata and the content description

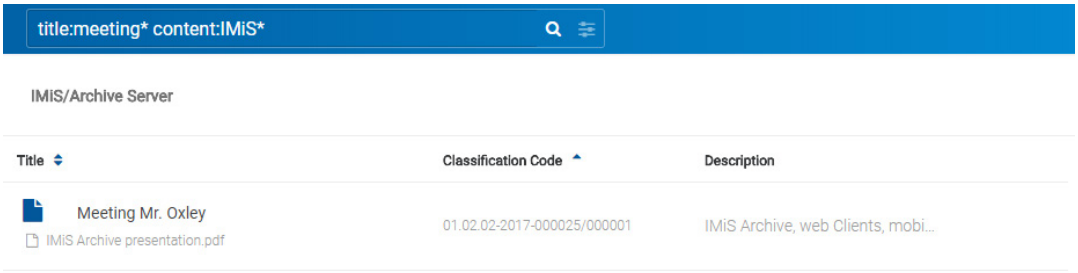

Image 124: Results of searching by metadata and the content description

4.3.5.4.3 Combined search by content descriptions and full text search

The user can simultaneously search by the content description and by the full text of the content.

The search result is all documents containing a specific search string in the content description (e.g. IMiS) and whose content also contains the searched text (e.g. china).

The searched text can contain one or multiple simple search conditions.

2018 © Imaging Systems Inc., All rights reserved.

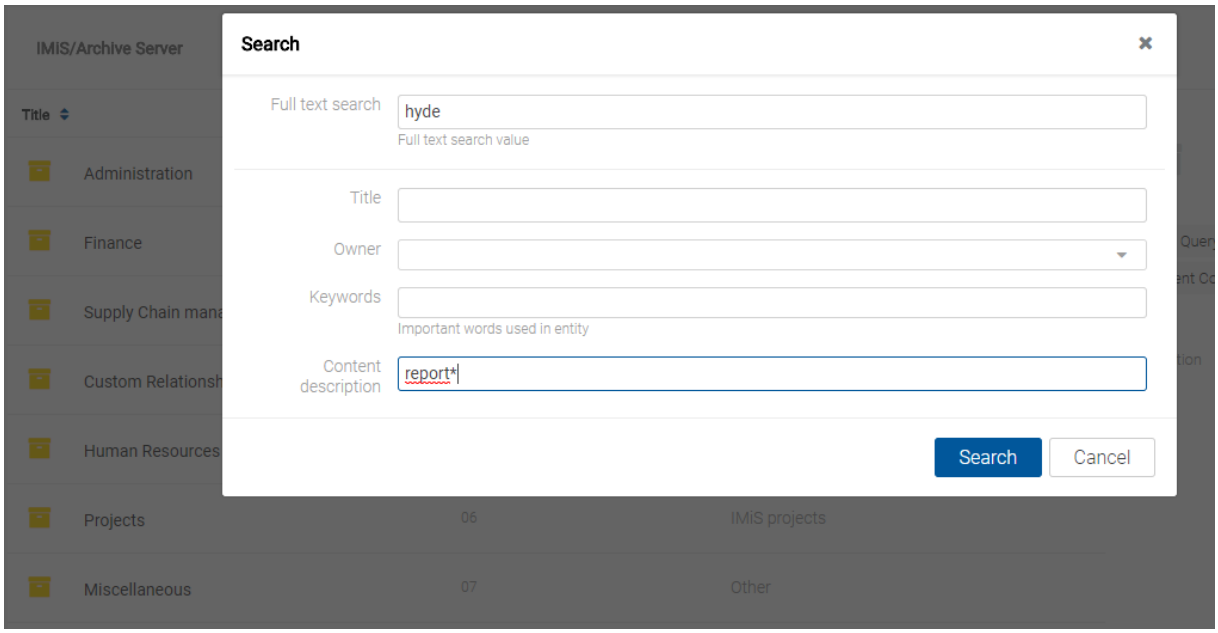

Image 125: Entering a search string when searching by the text of the content and the content description

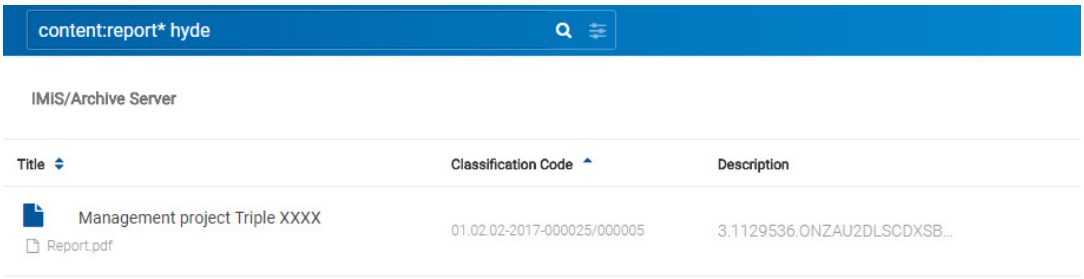

Image 126: Displaying the result of searching by the text of the content and the content description

4.3.6 Archiving email messages

The IMiS®/wClient enables users to capture the received and sent email messages with corresponding metadata and attachments, depending on the IMiS®/ARChive Server settings. To enable capture, the server must be configured with at least one template that contains email message attributes Email attributes.

2018 © Imaging Systems Inc., All rights reserved.

4.3.6.1 Email archiving procedure

The user captures email messages by using the »Drag and drop« functionality.

The user marks one or several email messages, including their attachments, in the email client (MS Outlook, IBM Notes etc.) and »drags« them to the selected class or folder in the classification scheme in the IMiS®/wClient.

The user arranges the IMiS®/wClient and email client windows so that they are both visible on screen. By holding down the left mouse button, the user drags the selected email messages to the central view of the IMiS®/wClient.

If a window appears notifying user that he can drop the selected email message, this means that a popup window for creating an entity will appear when the email message is dropped. If the email is recognized successfully and it is possible to create entities with a template that enables email, the »Email« tab will be shown.

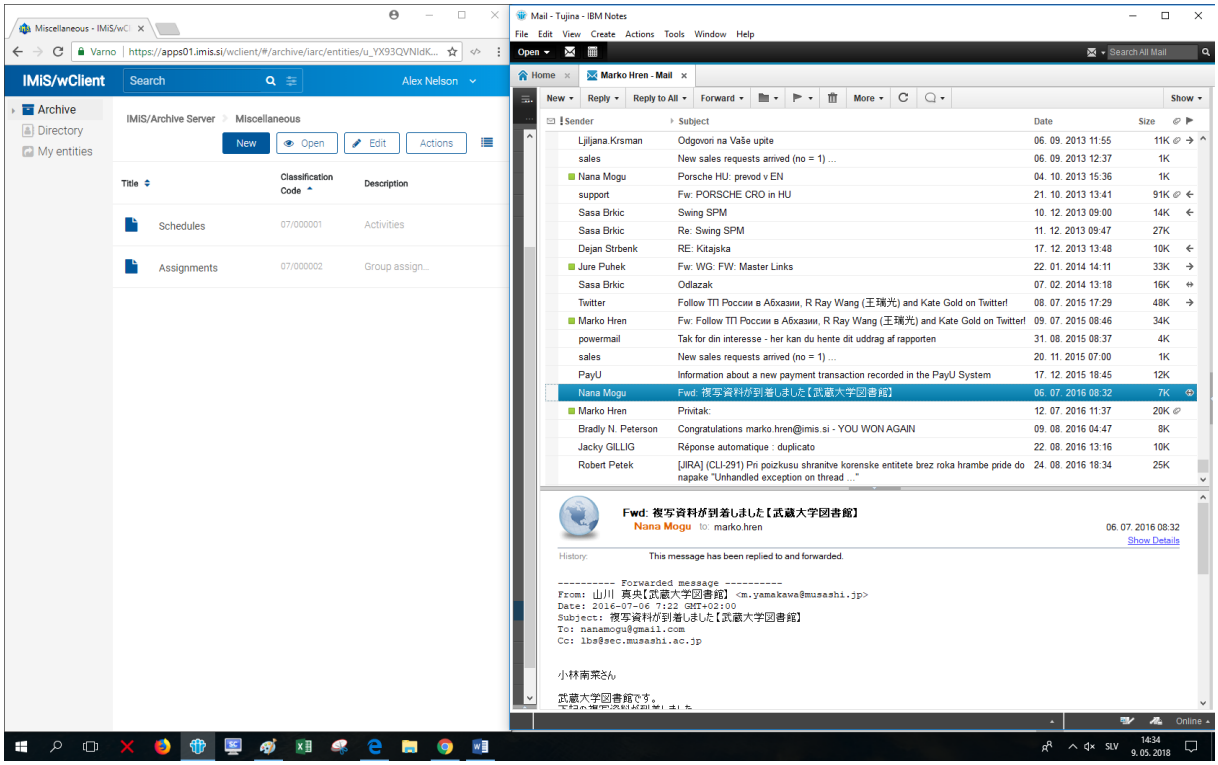

Image 127: Preparing the environment for transferring an email message from the email client to the archive

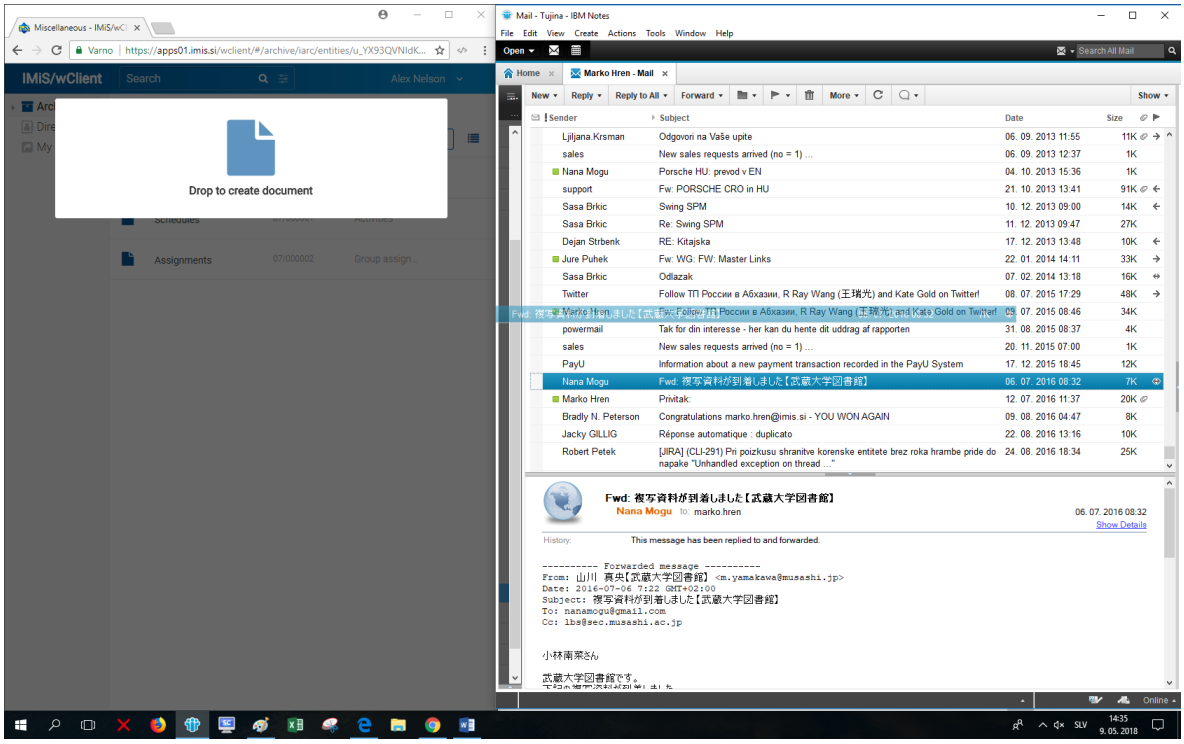

Image 128: Dropping the email message to the selected entity

After releasing the mouse button, a dialog box opens for viewing and editing the details of the email message.

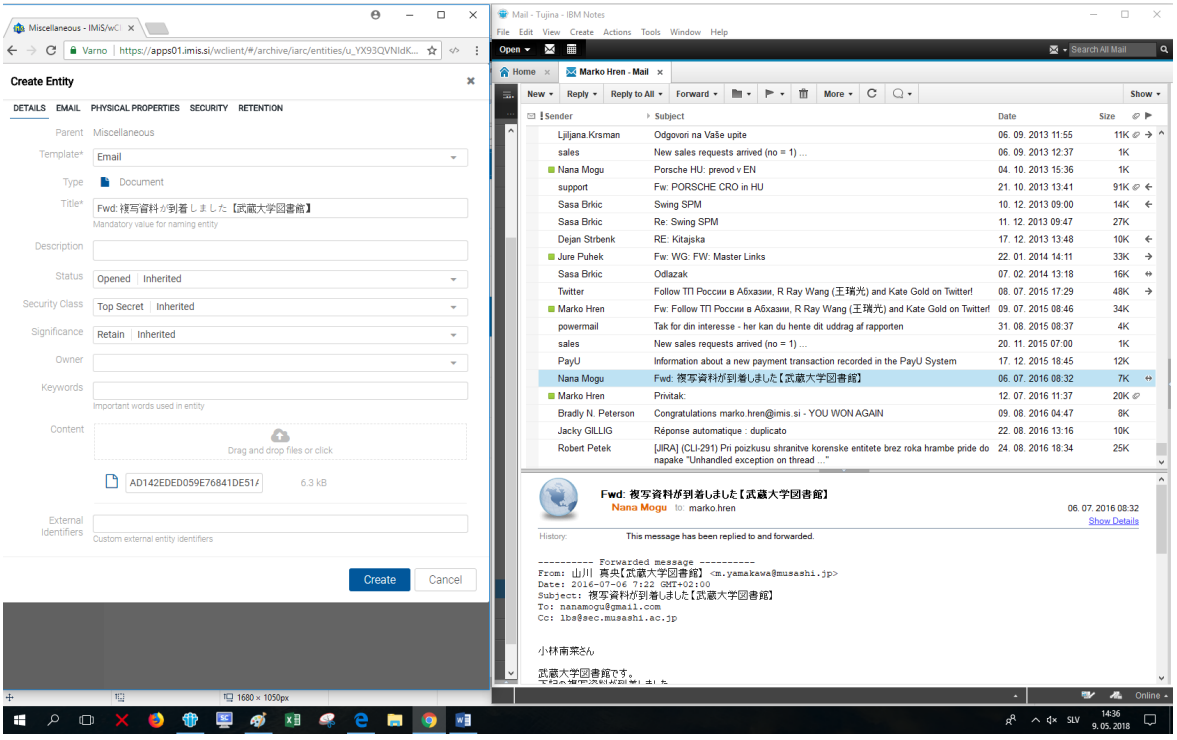

Image 129: Viewing and editing the details of an email message before saving

2018 © Imaging Systems Inc., All rights reserved.

In the »Details« tab the user can view or edit the following metadata:

- Parent: the title of the parent entity. This attribute is read only.
- Template: a set of available templates for creating allowed entities and classifying them under the selected class or folder. This attribute is mandatory.
- Type: the type of the entity described. This attribute is read only.
- Title: name of the folder or document described. Attribute value is mandatory.
- Description: Short description of the entity.
- Status: current status of the entity.
- Security class: a set of available entity security classes based on the entity's position in the classification scheme.
- Significance: significance rating of the entity.
- »Owner«: a directory (user or group) entity that is responsible for the selected entity.
- Keywords: keywords related to the entity. Attribute can have multiple values.
- External identifiers: a list of the entity's unique external identifiers on the server.

In addition to the above-mentioned attributes, the user can also edit the so-called »Custom attributes«, which are predefined by the template.

When the selected email message is moved to the IMiS®/wClient, the value of the »Title« attribute is automatically transferred to the »Content« field, and contents containing email details are created. If the email contains additional contents, they too are transferred. After confirming the entry and selection of attribute values with the »Create« button, the selected messages are automatically transferred to the desired location in the classification scheme together with their metadata and content and are saved to the IMiS®/ARChive Server.

2018 © Imaging Systems Inc., All rights reserved.

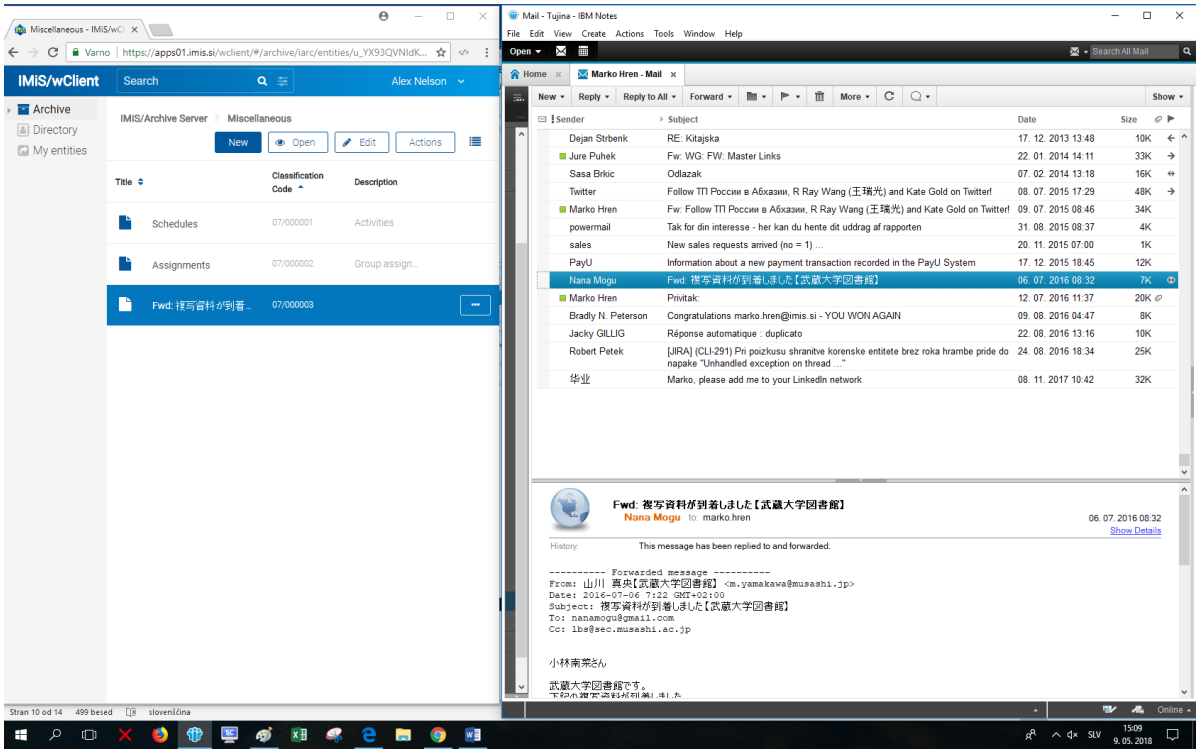

Image 130: Displaying a saved email message on the list of entities

In the »Details« tab, the user can see all the content that was saved together with the email message. In the »Content« field the original email message in the EML format and the recognized email attachments are created.

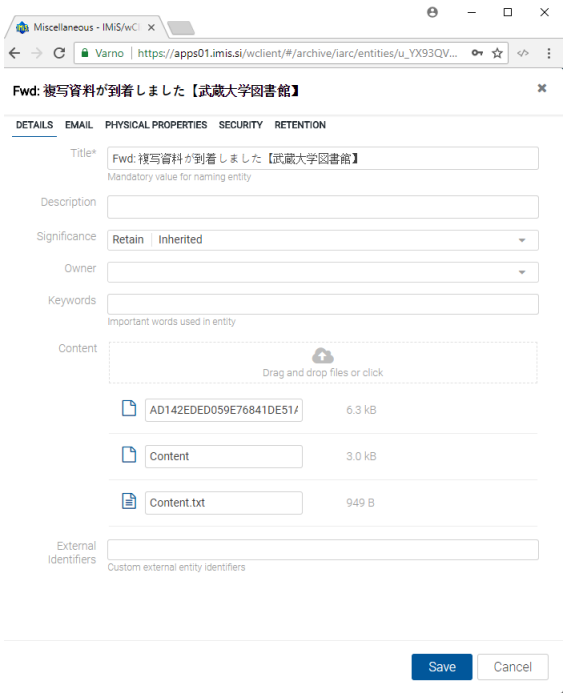

Image 131: Contents of the email message

2018 © Imaging Systems Inc., All rights reserved.

4.3.6.2 Functionality description

After viewing and confirming the email message with the »Create« button, the selected email messages are copied to the specified location in the classification scheme,
in the form of an EML file. For each email message, the IMiS®/wClient creates a new document containing the original message, the metadata and any captured content.

The following metadata (when present) is automatically extracted from the email message:

- »Subject«: the subject of the message.
- »From«: email address of the sender.
- »To«: email addresses of recipients.
- »CC«: email addresses of the carbon copy recipients.
- »BCC«: email addresses of hidden recipients.
- »Date«: the date and time the message was sent or received.
- »Message Id«: automatically generated message identifier.
- »Priority«: priority status of the email.
- »Signed«: a value that registers if the email message was electronically signed.

In this process, the »Date« and »Sender« email metadata are mandatory.
If one of these is not successfully captured, the message will not be saved.

Image 132: Display of the metadata transferred from the email message

Warning:

E-mail messages can't be saved if the selected template includes »Required« custom attribute.

4.3.7 Acquiring authenticity evidence

Authenticity evidence is created on the IMiS®/ARChive Server for the entities, whose properties correspond to at least one rule for generating proofs and have at least one metadata or content that is intended for generating proofs.

For additional information on rules for generating and renewing proofs see the IMiS®/ARChive Server user manual chapter 3.6.7 Rules.

Evidence is created in packets, according to predetermined time intervals.

In case authenticity evidence for the selected entity already exists on the archive, the user can retrieve it by using the »Action« command and »Authenticity evidence« command.

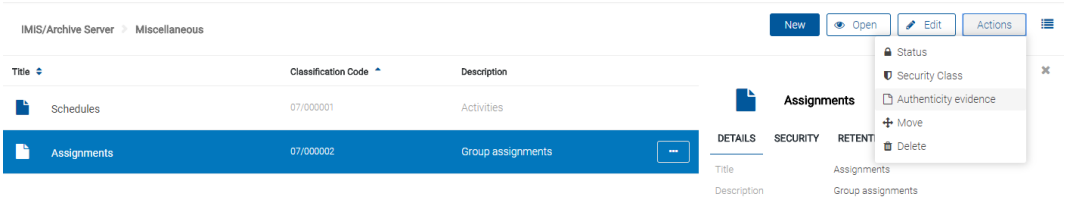

Image 133: The popup menu for selecting the »Authenticity evidence« command

The user is shown a dialog box for selecting the folder to which he will save the directory with the two files containing authenticity evidence. The user saves them by confirming the »Save« button.

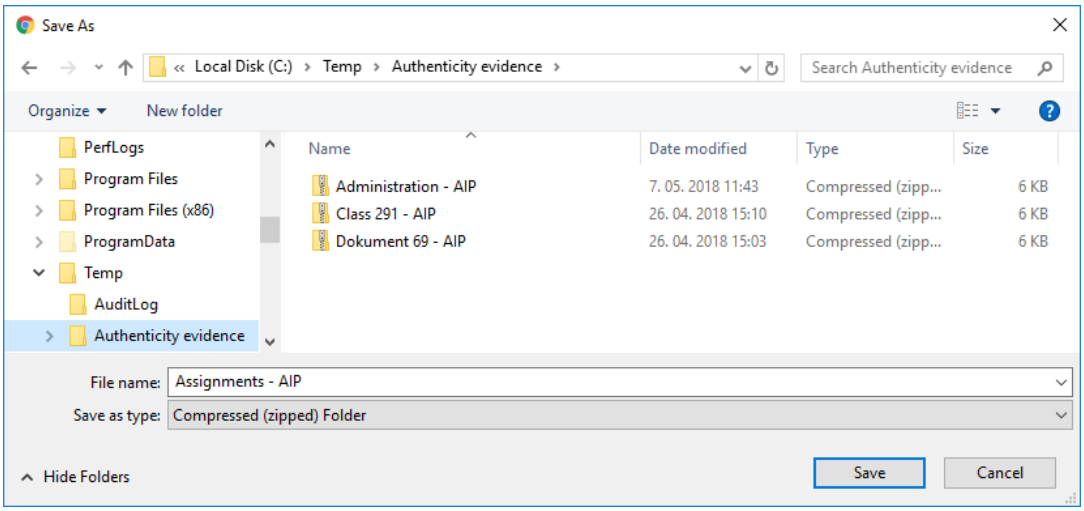

Image 134: Selecting the folder for saving the directory with the two files containing authenticity evidence

The authenticity evidence includes these two file types:

- »AIP.xml«: XML file that contains the »Archival Information Package – AIP«, which is a summary of the entity's metadata and content subject to the authenticity verification procedure.
- »EvidenceRecord X.xml«: one or more XML files that contain the evidence record of the entity according to the »Evidence Record Syntax – ERS« standard, which prescribes a system for ensuring the authenticity of long-term archived content. The »X« in the name of the file means the successive number of the record.

```
<?xml version="1.0" encoding="UTF-8"?>
<aip:AIP xmlns:aip="http://www.imis.eu/imisarc/aip"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <aip:Header Version="1">
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
    </aip:Header>
    <aip:Attribute Id="sys:Closed" Type="16">
        <aip:Value>2014-03-31T16:23:50.401+02:00</aip:Value>
    </aip:Attribute>
    <aip:Attribute Id="sys:Opened" Type="16">
        <aip:Value>2014-03-31T16:23:47.094+02:00</aip:Value>
    </aip:Attribute>
    <aip:Attribute Id="sys:Status" Type="18">
        <aip:Value>Closed</aip:Value>
    </aip:Attribute>
    <aip:Content Id="sys:Content">
        <aip:ContentValue>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>ONPJp3qfSkFm...T5irpOT+SrJMp+VE=</ds:DigestValue>
        </aip:ContentValue>
    </aip:Content>
</aip:AIP>
```

Image 135: Example archive information package

Warning:

Depending on the settings of the IMiS®/ARChive Server, authenticity evidence is created in certain intervals. The default setting is 5 minutes. The evidence thus becomes available when this time period has elapsed.

2018 © Imaging Systems Inc., All rights reserved.

```
<?xml version="1.0" encoding="UTF-8"?>
<EvidenceRecord xmlns="http://www.setcce.org/schemas/ers" Version="1.0">
<ArchiveTimeStampSequence>
<ArchiveTimeStampChain Order="1">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<ArchiveTimeStamp Order="1">
<HashTree>
<Sequence Order="1">
<DigestValue>RiHMqrhrGATA/fDYJVO2lVg4fTw=</DigestValue>
<DigestValue>dawWHxN2luddA7O+NGHYNd3ApG8=</DigestValue>
</Sequence>
<Sequence Order="2">
<DigestValue>vqBElqW7kGPUaFB/g6tfUFWwylE=</DigestValue>
</Sequence>
</HashTree>
<TimeStamp>
<TimeStampToken Type="XMLENTRUST">
<dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Id="TimeStampToken">
<dsig:SignedInfo>
<dsig:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<dsig:Reference URI="#TimeStampInfo-13ED106F54C2C33ED420000000000007BD7">
<dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<dsig:DigestValue>fWwSCkW04udY+/kvwMgL59scG3k=</dsig:DigestValue>
</dsig:Reference>
<dsig:Reference URI="#TimeStampAuthority">
<dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<dsig:DigestValue>j8bwhFukHoD6jcjmzgEZtXDF/ko=</dsig:DigestValue>
</dsig:Reference>
</dsig:SignedInfo>
<dsig:SignatureValue>J5Vmm9HR9gYzPouh... ELWNov32qUw==
</dsig:SignatureValue>
<dsig:KeyInfo Id="TimeStampAuthority">
<dsig:X509Data>
<dsig:X509Certificate>MIIFYDCCBEi...InphHBlzxEkFU3</dsig:X509Certificate>
</dsig:X509Data>
</dsig:KeyInfo>
<dsig:Object Id="TimeStampInfo-13ED106F54C2C33ED420000000000007BD7">
<ts:TimeStampInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:ts="http://www.entrust.com/schemas/timestamp-protocol-20020207">
<ts:Policy id="http://www.si-tsa.si/dokumenti/SI-TSA-politika-za-casovni-zig-1.pdf"/>
<ts:Digest>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>kKsYK3bWkp5Zc/wbgssA/XlbNsA=</ds:DigestValue>
</ts:Digest>
<ts:SerialNumber>108487637460...6624147310345175</ts:SerialNumber>
<ts:CreationTime>2014-04-02T09:45:00.093Z</ts:CreationTime>
<ts:Nonce>7949411139179750976</ts:Nonce>
</ts:TimeStampInfo>
</dsig:Object>
```


2018 © Imaging Systems Inc., All rights reserved.

```
</dsig:Signature>
</TimeStampToken>
<CryptographicInformationList>
<CryptographicInformation Order="1"
Type="CERT">MIIEHDCCAwSgBAgIE...z9Oz6gk/2vorAfGEhuB9nBxVeoQp</CryptographicInformation>
<CryptographicInformation Order="2"
Type="CRL">MIISKTCCERECAQEwDQYJ....pYO2SYQMkw819LR9I/YOFg</CryptographicInformation>
</CryptographicInformationList>
</TimeStamp>
</ArchiveTimeStamp>
</ArchiveTimeStampChain>
</ArchiveTimeStampSequence>
</EvidenceRecord>
```

Image 136: Example evidence record

4.3.8 Deletion of an entity

The IMiS®/wClient enables immediate deletion of an entity from the classification scheme.

4.3.8.1 Immediate deletion of an entity

To execute a delete action, the user must have the »Delete« right on the selected entity.

For displaying the effective rights of a user see chapter Entity information.

Prior to deletion, the user has to make sure the classes or folders he is about to delete do not contain entities.

Entities namely cannot be deleted. The same is valid for all closed entities (the value of the »Status« attribute is »Closed«).

The user can delete an entity by selecting the »Actions« command in the command bar and »Delete« in the popup menu.

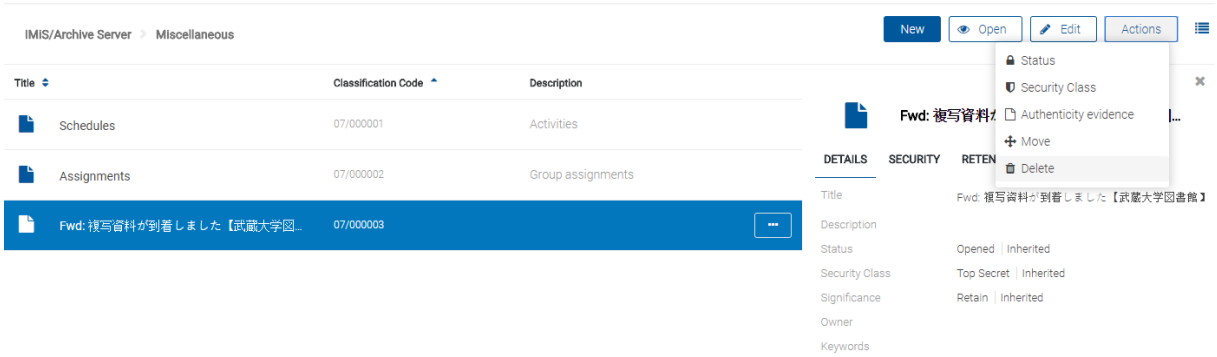

Image 137: Selecting the »Delete« command

A dialog box opens for giving the »Reason to delete« and the »Description«, which are required.

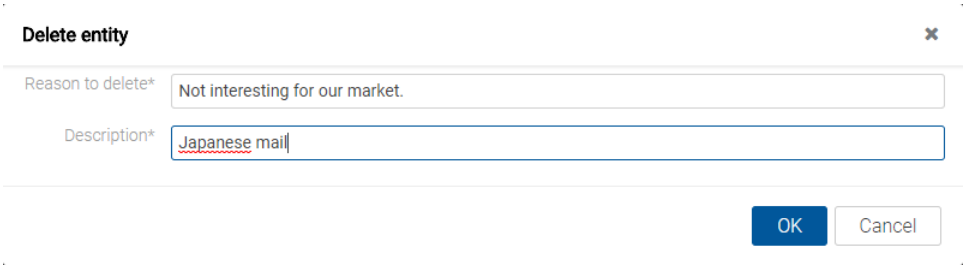

Image 138: A dialog box for deleting an entity

After both values have been entered, the »OK« command is enabled. The user can either confirm the deletion or cancel it by selecting the »Cancel« command.

4.4 System attributes

System attributes are predefined. On the IMiS®/ARChive Server they are specified by the attribute scheme and have prescribed properties.

Attributes can be:

- Publicly accessible: The attribute is accessible to all users no matter what access rights and roles they have.
- Required: The attribute value has to be input before the entity can be saved.
- Read-only: Attributes can be read but not edited.

Attributes can have multiple values, pick list values, and any combination of possible properties. Attribute values can also be inherited. The table below describes the possible attribute properties.

Name of attribute property	Description
Public	Attribute is publicly accessible to all users.
Required	Attribute value is mandatory.
Unique	Attribute value must be unique.
ReadOnly	Attribute value cannot be changed.
MultiValue	Attribute has multiple values.
PickList	Attribute must have one of the values from the pick list.
Searchable	Attribute is searchable.
Inherited	Attribute values are inherited from the parent entity.

2018 © Imaging Systems Inc., All rights reserved.

Name of attribute property	Description
AppendOnly	Attribute values may only be appended.
IncludeInAIP	Attribute values are part of the archive information package.

Table 4: Description of possible attribute properties

In addition to limitations that specify attribute properties, certain other system limitations also apply. For example, some attributes are only available for specific types of entities, and some only for entities in a specific location in the classification scheme, or after a specific action has been executed (e.g. transfer)

All the system attributes of the IMiS®/ARChive Server are described below.

4.4.1 General system attributes

The general system attributes of an entity consist of various attributes such as »Title«, »Description« and »Classification code«. They contain mandatory as well as optional attributes. Most attributes are available for all entities. The exceptions are »Status«, »Opened date« and »Closed date«, which are present for classes, folders, and those documents that are located directly under a class. Attribute »Significance« is available for folders and documents only.

The table below lists and describes all the general system attributes.

Name	Description
Classification code	Contains the entity's classification code within the classification scheme. The classification code is generated automatically on the archive server. *Example: The classification code 01-2014-00004/00001 represents document 00001, located inside folder 2014-00004, located inside class 01. The classification code is a publicly accessible type of metadata.*
Title	Saves/contains the title of the entity. The title is a required, public metadata that enables search.
Description	Saves/contains a short description of the entity. The description is a public metadata.
Status	Saves/contains the status of the entity. The status is a required metadata for all entities that are either classes, folders, or documents directly under classes. It is a public metadata that enables search. The possible values are: • »Opened«: the entity can be edited by a user with the appropriate effective access rights (the right to write) • »Closed«: the entity cannot be edited.

2018 © Imaging Systems Inc., All rights reserved.

Name	Description
Opened date	Contains the date and time the status of the entity was changed to »Opened«. The opened date is public metadata, is read-only and enables search.
Closed date	Contains the date and time the status of the entity was changed to »Closed«. The closed date is public metadata, is read-only and enables search.
Significance	Saves/contains the significance rating of the entity. Significance is a required metadata for folders and documents. It is public metadata that enables search. The possible values are: • »Vital«: entity is vital. • »Permanent«: entity is permanent. • »Retain«: entity should be retained. • »Delete«: entity is queued for deletion.
Security class	Saves/contains the security class of the entity. The security class is optional metadata for all new entities. Once it is set, it cannot be modified without stating a reason for change. The security class is a public metadata that enables inheriting and enables search. The possible predefined values are: • »Unclassified«: entity is freely accessible. • »Restricted«: entity is of an internal nature. Can only be accessed by users with clearance level »Restricted« or higher. • »Confidential«: entity is confidential. Can only be accessed by users with clearance level »Confidential« or higher. • »Secret«: entity is secret. Can only be accessed by users with clearance level »Secret« or higher. • »Top Secret«: entity is top secret. Can only be accessed by users with clearance level »Top Secret«.
Creator	Contains the creator of the entity (name of user who created it). The value is set when an entity is created on the IMiS®/ARChive Server and cannot be changed. The creator is a public metadata, is read-only and enables search.
Owner	Saves/contains the owner of the entity. The value of the attribute is selected from among the currently registered users of the archive server. The owner is a public metadata that enables search.
Keywords	Saves/contains keywords related to the entity. This attribute can have multiple values and is a public metadata that enables search.

2018 © Imaging Systems Inc., All rights reserved.

Name	Description
External Ids	Saves/contains external identifiers of the entity. This attribute can have multiple unique values and is a public metadata that enables search. *Warning: When entering values, keywords should be separated using the »Enter« key or the semicolon character (;).*
Save log	Contains a report on the verification of the electronic signature for digitally signed content. This attribute can have multiple, added values. It is a public metadata that enables search

Table 5: Description of general system attributes

4.4.2 Email attributes

Email attributes are only available for documents that have been created using an email template. Email attributes store information about the email such as the sender, recipients, and sent date.

Name	Description
Message Id	Contains the automatically generated message identifier.
From	Contains the address of the sender. This metadata is mandatory.
To	Contains the addresses of the email's recipients.
CC	Contains the addresses of the email's CC recipients.
BCC	Contains the addresses of the email's hidden recipients.
Subject	Contains the subject of the email message.
Priority	Contains the email priority status.
Signed	Contains a value that registers if the email was electronically signed.
Date	Contains the date and time the email was sent. This metadata is mandatory.

Table 6: Description of email attributes

4.4.3 Physical content attributes

Physical content attributes are only available for documents. The existence of physical content is specified by the unique physical content identifier. The physical content has a home location, which changes when it is checked out. The change of location is saved in the »status« attribute.

2018 © Imaging Systems Inc., All rights reserved.

Name	Description
Identifier	Contains the unique identifier of the physical content.
Description	Contains a short description of the physical content.
Status	Contains the current status of the physical content. Possible values are: - »CheckedIn«: the physical content is stored at its home location. - »CheckedOut«: the physical content has been sent to another location.
Status change date	Contains the date and time of the physical content's last status change.
Home location	Contains the home location of the physical content.
Current location	Contains the current location of the physical content.
Custodian	Contains the name of the physical content's custodian.
Return date	Contains the expected return date of checked out content.

Table 7: Description of physical content attributes

4.5 Roles

A server role is a set of access rights that allow users to execute specific operations on the IMiS®/ARChive Server. An appropriately authorized user can grant the following roles to other users or groups:

- »AuditLogQuery«: allows access to the audit log.
  Users with an »AuditLogQuery« role see the Activity tab in the entity information overview and can access the audit trail through this tab.
- »Content management«: The role enables the user to tag content for indexing or conversion.

5 SYSTEM REQUIREMENTS

System requirements are divided into client requirements and the IMiS®/wClient requirements.

5.1 Hardware

Most current workstations and computers should be able to run the IMiS®/wClient.
The workstations and computers being sold on the market today meet the client requirements of the IMiS®/wClient. It needs few resources to operate and works in all of the popular web browsers on Windows, macOS and other operating systems.

2018 © Imaging Systems Inc., All rights reserved.

5.1.1 Minimum requirements

- Browsers:
  - Chrome ≥ 66.0.3359
  - Firefox ≥ 60.0.1
  - Edge ≥ 42.17134
  - Safari ≥ 11.1
  - Internet Explorer 11 ≥ 11.0.10240.16384.
- Size of available work memory should be about 512 MB larger than the operating system's memory requirements.
- TCP/IP network access (IPv4 or IPv6).

5.1.2 Recommended hardware

- Browsers:
  - Chrome ≥ 66.0.3359
  - Firefox ≥ 60.0.1
  - Edge ≥ 42.17134
  - Safari ≥ 11.1
- Size of available work memory should be about 1 GB larger than the operating system's memory requirements.
- TCP/IP network access (IPv4 or IPv6).

5.2 Installation requirements

Most current servers should be able to run the IMiS®/wClient.

It needs the IMiS®/Storage Connector Services REST to operate.

5.2.1 Minimum requirements

- IMiS®/StorageConnector Services REST 9.2.1805.102;
- Minimum free disk capacity for installing the IMiS®/wClient is 6GB.
- TCP/IP network access (IPv4 or IPv6).

2018 © Imaging Systems Inc., All rights reserved.

5.2.2 Recommended requirements

- IMiS®/StorageConnector Services REST 9.2.1805.102;
- prostor na disku ≥ 6 MB;
- Minimum free disk capacity for installing the IMiS®/wClient is 6GB.
- TCP/IP network access (IPv4 or IPv6).

6 INSTALLATION

Below is a description of the installation procedure for the IMiS®/wClient. It can be performed by a user with the appropriate rights (Administrator). The installation is conducted step-by-step and is the same for everyone.

6.1 Installation procedure

The IMiS®/wClient must be installed in an environment that satisfies minimum requirements. The user must have rights on the server on which he is installing the client. The installation package is extracted to a directory on the server selected by the administrator.

Procedure:

1. The administrator extracts the installation package to a directory on the server.
2. He sets the settings.json.

6.1.1 Installation settings

For successful installation the address to the IMiS®/StorageConnector Services REST must be entered into the »assets/settings.json« as the »url« property.

Example of the setttings.json:

```
{
  "url": "https://apps.imis.eu/scsvc",
  "requestTimeout": 240000
}
```

url	String	Address of the IMiS®/StorageConnector Services REST.
requestTimeout	Integer	The timeout of an individual request to the service in *ms* (optional). The default value is 120000.

2018 © Imaging Systems Inc., All rights reserved.

6.2 Upgrade procedure

1. The administrator copies the current »assets/settings.json« to a temporary directory.
2. Deletes the directory containing the IMiS®/wClient.
3. Extracts the installation package to the directory.
4. Replaces the settings.json from the temporary directory.

7 MANAGING PRODUCT

The IMiS®/wClient can be managed by a user with the appropriate rights (e.g. administrator).

The user must first log in to access the archive.
For more information on logging in/out see chapter Login and logout.

The user stops the IMiS®/wClient by logging out and closing the tab/window of the web browser.

8 TROUBLESHOOTING

Users of the IMiS®/wClient must know how to handle the product correctly and are advised to follow instructions provided by documentation. If you encounter issues or errors, it is important to follow proper procedures. The first thing that is advised is to contact the IT expert or system administrator of your company.

Administrators are advised to troubleshoot errors with the help of the appropriate manual. If you cannot discover the cause of the issue or find the appropriate fix, feel free to contact IMiS® software support and we'll be glad to offer assistance. Be advised that a layperson's interference can make things worse and further destabilize the system.

8.1 How to avoid problems

Regular updating of the IMiS®/wClient is essential to keep issues at a minimum.
Every new version of IMiS® software fixes known bugs and errors.

2018 © Imaging Systems Inc., All rights reserved.

If you want to make sure things run smoothly, a highly recommended choice is our optional maintenance contract. A valid maintenance contract will protect you from serious errors or system outage. Several kinds of maintenance contracts are available:

- Primary, where the developer takes over the complete process of system maintenance.
- Secondary, where the developer fixes serious or less frequent errors, while users and their IT service perform regular maintenance and troubleshooting.

Maintenance contracts can be tailored to the specific needs of IMiS® software users.
Ask for a deal and we'll be happy to assist you.

8.2 Frequent errors

This chapter describes errors that may be frequently encountered while using the IMiS®/wClient. Each error is paired with the possible reasons and the steps that should allow you to fix it.

Error when accessing an archive

Likely cause: There was an error in establishing a connection with the IMiS®/ARChive Server, which can be due to:

- Wrong IP address.
- Invalid network port.
- Firewall on the client, or on the network between the client and the server, that prevents communication between the client and the server.

Solution: First, check the validity of the IP address and the network port. If that's not the cause, check if communication between the client and the server is open and reconfigure any firewalls as necessary.

»Invalid Username or password«

Likely cause: Invalid username or password.

Solution: Check whether the username and password have been entered correctly (e.g. use of capital/small letters, without initial or end spaces, etc.).
If that does not solve the problem, notify the administrator who will check whether a user with that name is actually registered on the IMiS®/ARChive Server.

2018 © Imaging Systems Inc., All rights reserved.

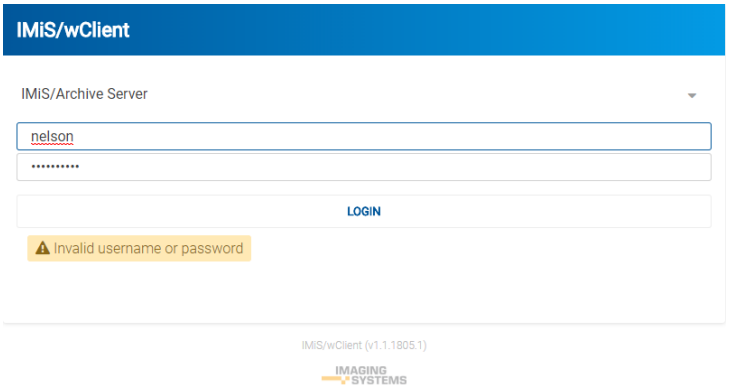

Image 139: An example of the error: Invalid or incorrect password

»Entity cannot be created since Classification Code generator is not defined for its hierarchy depth.«

Likely cause: Creating a folder in the classification scheme at a too low level.

When saving a new folder, a classification code is automatically generated, however, the classification code generator on the IMiS®/ARChive Server supports the generation only to a certain level in the classification scheme, and not beyond it.

Solution: Creating a folder at a higher level, which is still supported by the classification code generator on the server.

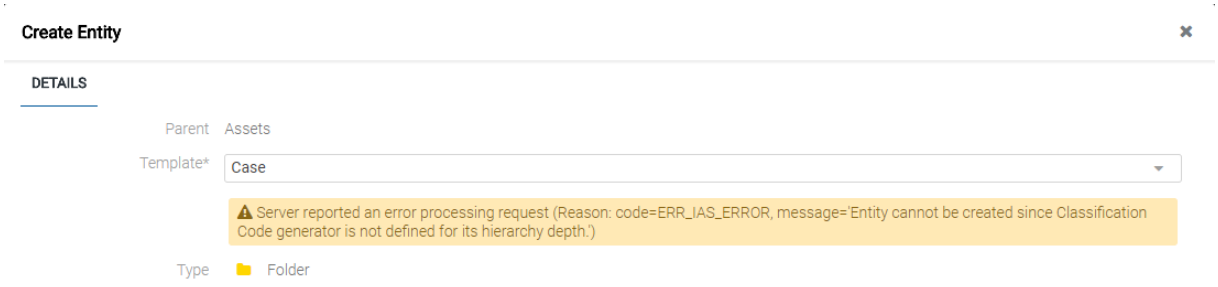

Image 140: An example of an error when saving a new folder

»Closed entities cannot be edited. «

Likely cause: An attempt to open a closed entity in editing mode.

The entity's status is »Closed«. Closed entities cannot be edited.

Solution: Dismiss the editing of the closed entity or change the entity's status to Opened via the popup menu on the document or the »Actions« button in the command bar.

2018 © Imaging Systems Inc., All rights reserved.

Image 141: An example of an error when editing a closed document

»[Class, Folder, Document] <classification code> cannot be edited.«

Likely cause: The entity is already open in editing mode on another computer.

Solution: Wait until the other user finishes editing and then open the entity once again.

Image 142: An example of an error when opening an entity in editing mode

2018 © Imaging Systems Inc., All rights reserved.