



IMiS[®] /wClient
Manual

Version 1.5.2010

**IMAGING
SYSTEMS**

Imaging Systems Inc.
Brnciceva 41 G
Ljubljana
Slovenia

TABLE OF CONTENTS

1	PREFACE	15
1.1	About the manual.....	15
1.2	Target audience.....	15
1.3	Conventions.....	15
1.4	Terms and abbreviations.....	16
2	INTRODUCTION.....	20
2.1	Features.....	20
2.2	Versioning and numbering.....	21
2.3	Functionalities	22
2.4	New functionalities in this version.....	23
3	TECHNICAL DOCUMENTATION	25
3.1	Client architecture.....	25
3.2	Format of import / export files.....	25
3.2.1	File structure.....	27
3.2.2	List of XML tags and their meaning.....	27
3.2.3	Format of the additional metadata export file.....	45
3.3	Format of the confirmation file during transfer.....	47
4	USER MANUAL.....	48
4.1	Login and Logout.....	48
4.1.1	Cookie Policy.....	48
4.1.2	Localization.....	49
4.1.3	About.....	50
4.1.4	Login.....	50
4.1.5	Logout.....	52
4.2	Interface description.....	53
4.2.1	Classification scheme.....	59
4.2.2	List of entities.....	64
4.2.3	Entity information.....	67
4.2.4	Command bar.....	80
4.2.5	Menu functions.....	81
4.2.6	Search.....	97
4.3	Actions.....	97
4.3.1	Entity access.....	97
4.3.2	Creating an entity.....	99
4.3.3	Editing entity data.....	115
4.3.4	Entity move.....	133
4.3.5	Content management.....	137
4.3.6	Versioning.....	161
4.3.7	Search functions.....	168

4.3.8	Archiving email messages.....	192
4.3.9	Acquiring authenticity evidence.....	199
4.3.10	Reporting.....	203
4.3.11	Bulk document capture.....	225
4.3.12	Import.....	225
4.3.13	Export.....	231
4.3.14	Deletion of an entity.....	240
4.4	System attributes.....	247
4.4.1	General system attributes.....	247
4.4.2	Security class change attributes.....	250
4.4.3	Moved entity attributes.....	250
4.4.4	Deleted entity attributes.....	250
4.4.5	Transferred entity attributes.....	251
4.4.6	Email attributes.....	251
4.4.7	Physical content attributes.....	252
4.4.8	Review process attributes.....	252
4.4.9	Entity attributes in the decision-making process.....	253
4.5	Authenticity.....	254
4.5.1	Digital certificate.....	254
4.5.2	Electronic signature.....	255
4.6	Review process.....	258
4.6.1	Preparation phase.....	259
4.6.2	Decision-making phase.....	267
4.6.3	Implementation phase.....	272
4.6.4	Disposition.....	274
4.6.5	Transfer of entities.....	275
4.6.6	Reviewing and classifying documents.....	283
4.7	Roles.....	287
5	SYSTEM REQUIREMENTS.....	288
5.1	Hardware.....	288
5.1.1	Minimum requirements.....	288
5.1.2	Recommended hardware.....	288
5.2	Installation requirements.....	289
5.2.1	Minimum requirements.....	289
5.2.2	Recommended requirements.....	289
6	INSTALLATION.....	290
6.1	Installation procedure.....	290
6.1.1	Installation settings.....	290
6.2	Upgrade procedure.....	291
7	MANAGING PRODUCT.....	292
8	TROUBLESHOOTING.....	293

8.1	How to avoid problems.....	293
8.2	Frequent errors.....	293

TABLE OF IMAGES

Table of images appearing in the manual

Image 1:	Client architecture.....	25
Image 2:	XPath notation text example	26
Image 3:	Example XSD scheme.....	46
Image 4:	Example additional metadata export file	46
Image 5:	Example of a confirmation file after transfer.....	47
Image 6:	Login on archive.....	48
Image 7:	Cookie Policy	49
Image 8:	Language selection	49
Image 9:	About dialog box.....	50
Image 10:	A list of available archives	51
Image 11:	Logging into the archive	51
Image 12:	Log out of the archive.....	52
Image 13:	User interface of the IMiS®/wClient.....	53
Image 14:	Categories in the left view	54
Image 15:	A list of mixed entity types.....	54
Image 16:	Movable dividing line between the left and central view	55
Image 17:	Entity information.....	56
Image 18:	Display of the command bar	56
Image 19:	Header of the user interface	57
Image 20:	Hierarchical position of the entity within the tree structure.....	57
Image 21:	Narrowing the user interface display.....	58
Image 22:	Access to folders in the left view via the menu	59
Image 23:	Display of folders in the left view of the web client IMiS®/wClient	59
Image 24:	The tree view of the classification scheme in the Archive folder	60
Image 25:	Popup menu in the tree view.....	61
Image 26:	Selecting the entity in the My entities folder in the central view	61
Image 27:	Selecting the Drafts folder in the left view.....	62
Image 28:	The Directory folder in the left view	62
Image 29:	Searching by directory entities.....	63
Image 30:	Results of searching by directory entities	63
Image 31:	User data.....	64
Image 32:	A list of contained entities of the selected entity.....	65
Image 33:	Sorting by entity type.....	65
Image 34:	Limiting the display of a greater number of entities on the list.....	66
Image 35:	Limiting the set of entities displayed on the list with a search.....	66

Image 36: Selecting the order of displaying the list of entities.....	67
Image 37: Tabs containing entity information in the reading mode	68
Image 38: The Details tab in the reading mode	69
Image 39: Custom metadata in the reading mode.....	70
Image 40: Custom metadata in edit mode.....	70
Image 41: Specifying multi-value attributes	71
Image 42: Display and selection of binary values	71
Image 43: The Details tab in reading mode	72
Image 44: References in the Details tab.....	73
Image 45: Email data in the reading mode.....	73
Image 46: Email data in the editing mode.....	73
Image 47: Physical content data in the reading mode.....	74
Image 48: Physical content data in the editing mode.....	74
Image 49: A report on checking the validity of electronic signatures and digital certificates ...	75
Image 50: Retention and disposition hold periods in the »Retention« tab.....	75
Image 51: Information on disposition hold	76
Image 52: Retention policy information.....	76
Image 53: The Security tab for a logged user in the preview mode.....	77
Image 54: A list of directory entities with access rights to the entity in the reading mode.....	78
Image 55: The Activity tab in the preview and reading mode.....	79
Image 56: Information about the user who performed an action on the entity.....	79
Image 57: Command bar above the information of the selected entity.....	81
Image 58: Enabling/disabling the display of entity information.....	81
Image 59: Popup menu in the header of the user interface	82
Image 60: Transition from profile settings to the entity review in the archive.....	82
Image 61: Display of the “Basic” tab	83
Image 62: Editing user details in edit mode.....	84
Image 63: Display of the “Security” tab.....	85
Image 64: Display of the window for changing the user password.....	85
Image 65: Showing the list of user sessions.....	86
Image 66: View of the “Settings” tab.....	87
Image 67: Dialog box for disabling the entry of the reason for performing actions.....	88
Image 68: Showing the basic settings.....	88
Image 69: Setting the parameters in the “IMiS®/wScan” tab.....	89
Image 70: View of the “Search history” tab.....	89
Image 71: Transition from profile settings to the entity review in the archive.....	90
Image 72: Report types	90
Image 73: Setting the display of entities.....	91
Image 74: Entities shown on a list.....	92
Image 75: Entities shown in a grid.....	92
Image 76: Selecting individual entities for move and deletion.....	92

Image 77: Selecting all the loaded entities for move or deletion.....	93
Image 78: Selecting a part of the loaded entities for move or deletion	93
Image 79: Set of actions on selected entities.....	94
Image 80: An example of an entity with a defined value of the Categories attribute	95
Image 81: A categorized Categories view	95
Image 82: A categorized Keywords view	96
Image 83: Display of the columns of the selected attributes of Title and Description	96
Image 84: Modifying a template in editing mode.....	99
Image 85: Creating a root class	100
Image 86: Display of contained entities.....	101
Image 87: Display of creating a new document	102
Image 88: Entry of required metadata	103
Image 89: Entry of text metadata.....	103
Image 90: Entry of date and time metadata	103
Image 91: Displaying the inherited value of the date field of the parent entity	104
Image 92: Entry of metadata with predefined values.....	104
Image 93: Entry of multiple values into a field.....	104
Image 94: Entering multiple values of an attribute.....	105
Image 95: Entering the values of multiple directory entities.....	106
Image 96: Selecting the type of classification code entry for the contained entity	107
Image 97: Manual entry of a child entity's classification code.....	108
Image 98: Display of manually entered classification code	108
Image 99: Specifying the security class of a new entity	108
Image 100: Entity information after entering the security class	109
Image 101: Specifying the status of a new entity	110
Image 102: Display of the entry of physical content metadata.....	111
Image 103: The date of the last change of the Status attribute.....	111
Image 104: Selecting validity for a specific type of entity.....	112
Image 105: Display of the »Retention« tab	112
Image 106: Saving a new or modified entity	113
Image 107: Example classification code	113
Image 108: Example creator of entity.....	114
Image 109: Example date and time an entity was created	114
Image 110: Example date and time of last changes to the entity	114
Image 111: Example date and time of last access to the entity	114
Image 112: Example date and time an entity was opened.....	114
Image 113: Example date and time an entity was closed.....	115
Image 114: Example entity identifier	115
Image 115: Editing of the physical content metadata	116
Image 116: Popup menu for selecting the status of the physical content	116
Image 117: Security tab in editing mode.....	117

Image 118: Searching a directory entity on a list.....	118
Image 119: List of directory entities with access rights to the entity	118
Image 120: Setting the inheritance of access permissions to contained entities	119
Image 121: Setting the temporal validity of access permissions.....	119
Image 122: A list of access permissions for a specific attribute.....	120
Image 123: Popup menu for selecting access rights to a selected metadata	121
Image 124: List of user permissions on the selected metadata.....	122
Image 125: The Retention policy tab in editing mode	123
Image 126: The Disposition hold tab in editing mode	124
Image 127: Selecting the classification code.....	125
Image 128: Selecting the classification code and giving the reason for the change	125
Image 129: The popup menu for selecting the Status command	126
Image 130: Selecting the status.....	126
Image 131: Selecting the status and giving the reason for the change.....	127
Image 132: The popup menu for selecting the Security class command	127
Image 133: Selecting the security class.....	128
Image 134: Selecting the security class and giving the reason for the change	128
Image 135: Selecting the command Share in the popup menu.....	128
Image 136: Displaying the created link to the selected entity	129
Image 137: Copying the link to the selected entity.....	129
Image 138: Notification of copying a link to the clipboard	129
Image 139: Sending a link to the selected entity/content by email	130
Image 140: The popup menu for selecting the New reference command.....	130
Image 141: The dialog box for adding and editing a reference	131
Image 142: Selecting Search for entity« in the New reference dialog box	131
Image 143: Adding the Title and Description in the New reference dialog box	132
Image 144: Removing a reference before saving.....	132
Image 145: A dialog box for selecting an action on the reference.....	133
Image 146: Selecting the Move command via the Actions command in the command bar	133
Image 147: A popup menu on the selected entity for selecting the Move command	134
Image 148: A dialog box for moving an individual entity	134
Image 149: Manually assigning the classification code when moving	135
Image 150: A dialog box for moving multiple entities	135
Image 151: The Content field for adding contents.....	138
Image 152: The added content before saving	138
Image 153: The added content after saving	138
Image 154: Displaying the list of contents in open mode.....	139
Image 155: Displaying the icon Scan for capturing content from a scanner.....	139
Image 156: Integrated window for scanning with IMiS®/wScan.....	140
Image 157: Displaying the document after finishing the scan	141
Image 158: A scanned document added to the list.....	142

Image 159: Content details in the right view	143
Image 160: Changing the description of content	143
Image 161: Popup menu on the selected content in the reading mode.....	144
Image 162: An example of the content type of a document.....	144
Image 163: An example of the date of creating the document content.....	145
Image 164: An example of the date of modifying the document content	145
Image 165: An example of the date of the last access to the document content.....	145
Image 166: An example of the document content identifier.....	145
Image 167: An example of a display of indexed document content	145
Image 168: An example of a display of signed document content.....	145
Image 169: Opening document content	146
Image 170: Opening content by clicking on the content.....	146
Image 171: Loading content.....	146
Image 172: Displaying the menu for selecting and previewing content	147
Image 173: Selecting the menu on the content preview	147
Image 174: WOPI flow chart.....	148
Image 175: Opening MS Office content.....	149
Image 176: Opening audio content.....	149
Image 177: Opening video content.....	149
Image 178: Selecting the Download command in the popup menu.....	150
Image 179: Displaying the progress of the download of content.....	150
Image 180: Displaying the option of selecting actions on downloaded content	150
Image 181: Selecting the Copy command in the popup menu.....	151
Image 182: Copying the content to another document.....	151
Image 183: Information about saving a copy of the content	152
Image 184: Selecting the command Share in the popup menu	152
Image 185: Displaying the created link to the selected content.....	152
Image 186: Notification of copying a link to the clipboard	153
Image 187: Selecting the »Update« command in the popup menu.....	153
Image 188: The selected content after update	153
Image 189: Selecting the Move command in the popup menu.....	154
Image 190: Selecting the target document for moving content.....	154
Image 191: Content temporarily removed from the document.....	155
Image 192: Saved document content.....	155
Image 193: Selecting the target document for moving content to the custom content container	156
Image 194: Content temporarily removed from the document	156
Image 195: Saved document content to the custom content container.....	157
Image 196: The content on the list before deletion.....	157
Image 197: Empty list after deletion.....	157
Image 198: Selecting the Queue for Indexing command	158

Image 199: Successful adding of content for indexing.....	158
Image 200: Selecting the Queue for Conversion command.....	159
Image 201: Successful tagging of content for later conversion.....	159
Image 202: Detaching the selected converted content.....	160
Image 203: Tagging content for detachment.....	160
Image 204: Displaying detached content on the list.....	161
Image 205: Selecting the action New version in the popup menu.....	162
Image 206: Checking out a document version.....	163
Image 207: Information about saving a document version	163
Image 208: Displaying document versions in the set Versions.....	164
Image 209: A popup menu on the document version	164
Image 210: Opening a document version in editing mode.....	165
Image 211: Saving a draft for later editing.....	166
Image 212: A draft of a document version in the Drafts folder.....	166
Image 213: Displaying the draft in the list of versions	167
Image 214: Discarding a document draft with the Discard command.....	167
Image 215: Reviewing a draft before checking it in with the Save command.....	168
Image 216: Search history	169
Image 217: Advanced search settings	170
Image 218: Setting the attributes to define the search conditions	170
Image 219: Displaying the set of attributes for defining the search conditions.....	171
Image 220: Before entering the text of limiting the set of attributes for the search.....	172
Image 221: After entering the text of limiting the set of attributes for the search.....	172
Image 222: Example of limiting the set of attributes for the search	173
Image 223: Entering a search string in the Search field	173
Image 224: Entering a search string in the Full text search field	174
Image 225: Entering text to limit the set of attributes for the search	174
Image 226: Example of limiting the set of attributes for the search	175
Image 227: Limiting the set of attributes for the search via the menu.....	175
Image 228: Search results list showing content versions.....	176
Image 229: A dialog box for searching by metadata	178
Image 230: A dialog box for searching by custom metadata.....	178
Image 231: A dialog box for searching by the metadata Owner.....	179
Image 232: Defining the time range for searching by date	180
Image 233: A dialog box for searching by the content description.....	181
Image 234: Use of special characters in a search string.....	181
Image 235: The search string and the results of searching by actual value.....	183
Image 236: Entering a search string in a combined search	184
Image 237: Result of searching by metadata and the full text of the content.....	184
Image 238: Entering a search string when searching by metadata and the content description	185

Image 239: Result of searching by metadata and the content description	185
Image 240: Entering a search string when searching by the text of the content and the content description	186
Image 241: Displaying the result of searching by the text of the content and the content description	186
Image 242: Entering the search string when searching by a custom attribute	187
Image 243: Entering the search string when searching by a custom attribute	188
Image 244: Selecting an entity in the entity tree	188
Image 245: Selecting a directory entity from a list	189
Image 246: Selecting an entity in the entity tree	189
Image 247: Defining an entity identifier	189
Image 248: Selecting audit log events	190
Image 249: Setting the parameters for searching by audit log events	190
Image 250: Saving audit log events in the CSV format	190
Image 251: Saving audit log events in the XML format	191
Image 252: Result of searching by audit log events	191
Image 253: Selecting information shown in columns	192
Image 254: Preparing the environment for transferring an email message from the email client to the archive	193
Image 255: Dropping the email message to the selected entity	194
Image 256: Viewing and editing the details of an email message before saving	195
Image 257: Displaying a saved email message on the list of entities	196
Image 258: Contents of the email message	197
Image 259: Selecting a template for creating an email message	197
Image 260: Selecting an EML file	197
Image 261: Confirming the selection of an EML file	197
Image 262: Display of the metadata transferred from the email message	199
Image 263: Obtaining authenticity evidence in the Details tab	200
Image 264: Information for the user about saving a directory with authenticity evidence	201
Image 265: A directory with two files containing authenticity evidence	201
Image 266: Example archive information package	202
Image 267: Example evidence record	203
Image 268: Defining the scope of the folders report	204
Image 269: The estimated timeframe for preparing the folders report	204
Image 270: Example folder report	205
Image 271: Defining the scope of the documents report	206
Image 272: Example of documents report	207
Image 273: Defining the scope of the document contents report	207
Image 274: Example of a document contents report	208
Image 275: Defining the scope of the retention report	209
Image 276: Example of a review report	210

Image 277: Selecting the review	210
Image 278: Defining the scope of the review report.....	211
Image 279: Example of a Review report - Properties.....	211
Image 280: Example of a Review report – Retention policy.....	211
Image 281: Example of a retention report - Entities	212
Image 282: Example of a retention report - Repot.....	212
Image 283: Defining the scope of the access report.....	213
Image 284: Example access report on the selected user	215
Image 285: Defining the scope of the classes report.....	215
Image 286: Example of a classification scheme report on the classes.....	216
Image 287: Defining the scope of the classes and folders report.....	216
Image 288: Example of a classification scheme report on the classes and folders	217
Image 289: Defining the scope of the entity report	218
Image 290: Example of the Entities report – Properties.....	219
Image 291: Example of the Entities report –Retention	219
Image 292: Example of the Entities report – Security.....	219
Image 293: Example of the Entities report – Transfer metadata	220
Image 294: Decision before preparing the report	220
Image 295: Example of the Deleted entities report.....	221
Image 296: A print preview for the deleted entities report.....	221
Image 297: Notification on preparing the deleted entities report.....	222
Image 298: Review of information on deleted entities in the CSV format.....	222
Image 299: Defining the scope of the delete queue report.....	223
Image 300: Example of the delete queue report.....	224
Image 301: A print preview for the delete queue report	224
Image 302: Notification on preparing the delete queue report	224
Image 303: Review of information on entities waiting for deletion in the CSV format	225
Image 304: Selecting the compressed file with the imported entities.....	225
Image 305: Displaying an import notification	226
Image 306: Display of the Import folder in the Administration system folder.....	226
Image 307: Set of available actions on the import/export report.....	227
Image 308: Popup menu on a import report.....	228
Image 309: Display of the import report in the Import system folder.....	229
Image 310: Information about the audit log created before the entity import.....	230
Image 311: Notification on the transfer of the audit log created before the entity import.....	230
Image 312: Audit log created before the entity import.....	231
Image 313: Selecting the »Export« command at the level of the entire classification scheme	232
Image 314: Setting the export parameters on the entire archive.....	233
Image 315: Notification about saving a file of exported entities of the entire classification scheme	233

Image 316: Information about the export of the entire classification scheme	233
Image 317: Display of a more detailed notification about the export of the entire classification scheme	234
Image 318: Selecting the Export action on the selected entity.....	234
Image 319: Setting the export of the entity tree via a dialog box	235
Image 320: Implementing the export of the entity tree	235
Image 321: Notification about saving a file of individual exported entities.....	236
Image 322: Information about the export of a part of the classification scheme	236
Image 323: Display of the Export folder in the Administration system folder and the document selected for export	236
Image 324: Set of available actions on the export report.....	237
Image 325: Popup menu on the export report.....	238
Image 326: An example of an error report in the export procedure.....	239
Image 327: Export report.....	239
Image 328: Display of a more detailed notification about the export.....	240
Image 329: Selecting the Delete command	241
Image 330: A dialog box for deleting an individual entity.....	241
Image 331: A dialog box for deleting multiple entities.....	242
Image 332: Selecting a single description for all entities selected for deletion	242
Image 333: Selecting a single description for all selected entities.....	243
Image 334: Marking an entity for later deletion.....	244
Image 335: A list of entities suggested for deletion in the Delete queue list folder.....	244
Image 336: Removing an entity from the delete queue list.....	245
Image 337: Display of the Deleted folder in the Administration system folder	246
Image 338: Popup window containing the result of the document's electronic signature verification.	256
Image 339: Example of a report for a valid electronic signature and valid digital certificate ...	257
Image 340: Example of a valid electronic signature and an expired digital certificate.....	257
Image 341: Example of a valid electronic signature for which the certification authority could not be verified.....	257
Image 342: Example of an invalid electronic signature due to a modification of the document after signing	258
Image 343: The Reviews folder in the left view	259
Image 344: A list of reviews in the review process	259
Image 345: Selecting the review type	260
Image 346: Creating a new Regular review in the preparation phase.....	260
Image 347: Display of Regular review attributes in the review process.....	261
Image 348: Access permissions for Regular review in the Security tab	262
Image 349: Display of the saved Regular review.....	262
Image 350: Entering a search expression in the Ad hoc review.....	264
Image 351: Display of the attributes of the review process in the Ad hoc mode	264

Image 352: Display of a saved ad-hoc review	265
Image 353: Cancellation of the review process using the Discard command.....	265
Image 354: A canceled decision-making phase	266
Image 355: Display of the review in the preparation phase in the Preparing state	266
Image 356: Display of an error which occurred during the preparation phase of the review process.....	267
Image 357: Display of the review pages and documents	268
Image 358: A list of selected entities on a specific review page	268
Image 359: Defining the columns of selected attributes in the popup menu	269
Image 360: Option of viewing an entity from the review	269
Image 361: Adding and modifying attribute values in editing mode	270
Image 362: Modifying the action of an entity in editing mode.....	271
Image 363: Modifying attribute values in the review	271
Image 364: Starting the process of completing the review	272
Image 365: During the process of completing the review.....	273
Image 366: Review execute report.....	273
Image 367: Review completed.....	274
Image 368: A list of disposed entities in the review process	274
Image 369: Display of the list of disposed entities on the review page	275
Image 370: Transfer of entities in the review process.....	276
Image 371: Setting the transfer parameters	276
Image 372: Implementing the transfer process.....	277
Image 373: Transfer notification	277
Image 374: Selecting the confirmation file	278
Image 375: Displaying the confirmation file.....	278
Image 376: Confirmation of entities recorded in the confirmation file.....	278
Image 377: Notification of saving the confirmation file	279
Image 378: A report on the transfer between review entities	280
Image 379: Log files in the transfer report	280
Image 380: An example of an ExportReport.txt report.....	280
Image 381: Manual transfer confirmation for an individual entity	281
Image 382: Transfer confirmation using a confirmation file	282
Image 383: Selecting the confirmation file	282
Image 384: Adding documents to the review	283
Image 385: Adding document metadata	284
Image 386: Adding a document to the review	284
Image 387: Notification about a document added to the review.....	285
Image 388: Reviewing documents.....	286
Image 389: Options of performing actions on entities.....	286
Image 390: An example of the error: Invalid or incorrect password	294
Image 391: An example of an error when saving a new folder	295

Image 392: An example of an error when opening an entity in editing mode	295
Image 393: Example of defining the service key	296

LIST OF TABLES

Below is a list of tables appearing in the manual:

Table 1: Manual font types and their meaning	15
Table 2: Definition of abbreviations.....	18
Table 3: List of terms used in the manual.....	19
Table 4: Terminology explanation	26
Table 5: Lists of XML tags	45
Table 6: Description of possible attribute properties.....	247
Table 7: Description of general system attributes.....	249
Table 8: Description of security class change attributes	250
Table 9: Description of moved entity attributes.....	250
Table 10: Description of deleted entity attributes.....	250
Table 11: Description of moved entity attributes.....	251
Table 12: Description of email attributes.....	251
Table 13: Description of physical content attributes	252
Table 14: Description of review process attributes.....	253
Table 15: Description of entity attributes in the decision-making process.....	253

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)
<i>italic</i>	advice, examples, tips, instructions
"inside quotation marks"	titles of selectable functions, files or actions
<u><i>underlined italic</i></u>	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

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)

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)

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)

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.

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.

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

The example of installation package name:

IMiS.wClient.1.5.2010.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.
- Editing of access permissions for entities, attributes of directory entity type and metadata.
- Entry and management of the records metadata according to a predetermined attribute scheme.
- Content management (capturing, viewing data, saving, previewing, downloading, updating, copying, moving, deleting, tagging for later indexing or conversion).
- Document versioning.
- Storage of archive materials of electronic origin or digitized using the scanner.
- Streaming-mode access to the records.
- 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.
- Sorting of entities according to the values of the categorized attributes (categorized views).
- Establishing of connections between different entities (references).
- Management of retention policies and disposition holds for the records.
- Making reports on folders, documents, document contents, retention, reviews, accesses, the classification scheme, entities, deleted entities, and entities to be deleted.
- Support for IPv4 and IPv6 network communication systems.

2.4 New functionalities in this version

We have implemented the following new functionalities and improvements to the previous certified version 1.4.1910 of the IMiS®/wClient module:

New functionalities:

- Parsing email contents at the server level.
- Searching audit log events using an identifier.
- Adding and moving content to the custom container.
- Showing the audit log created before the entity import.
- Show search history.
- IMiS®/wScan API key and URL settings in the profile settings.
- Showing directory entity aliases.
- Show directory entity membership.
- Show context menu in the tree view.
- Information on user sessions.
- Saving user settings.
- Saving the template categorization.
- Showing the password on the login page.
- Sorting the entity collection by type.
- Preview of Microsoft Office content [Word, Excel, Power Point].
- Searching by entity type.
- Recursive search with a depth setting option.
- Editing the advanced search display.
- Changing the order of attributes after changing the template.
- Making reports.
- Side menu of the preview of PDF and TIFF content.
- Showing the deleted entity type.
- Changed classification code.

Improvements:

- Keyboard use supported in edit mode.
- Limiting the size of collections found by a search.
- Record of the internal entity identifier in the audit log report.
- Preserving the remaining metadata of entities destroyed or transferred.
- Selecting multiple entities simultaneously to be moved and deleted.
- One-time setting of a description of all entities to be deleted.
- Loading a page while showing the entities list.
- Changed Binary property operations.
- Changed mode of loading a user's images.
- Saving the status of the display of sections in the "Details".
- Preview for the Binary-type properties.
- Sorting columns on the list in descending/ascending order.
- Loading content by parts.
- Retrieval of the file type from the extension.
- Improved component for selecting the directory entity.
- Selecting an email template before creating an entity.
- Enhanced dialog box for selecting an entity.
- Downloading the report on saving the review.

Small improvements:

- Enhanced display of the slider.
- Changed display of permissions in the "Security" tab.
- Enhanced user interface.
- Transition from the profile to the classification scheme.
- Disabling the action "Next" until the reason is entered.
- Changed text when displaying larger collections.
- Changed display of the device name in the "Activities" view.
- Framework upgraded to Angular 10 and PrimeNG 10.

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 represents the service level of the interface of the IMiS®/Storage Connector.

The latter can be connected to many IMiS®/ARChive Servers.

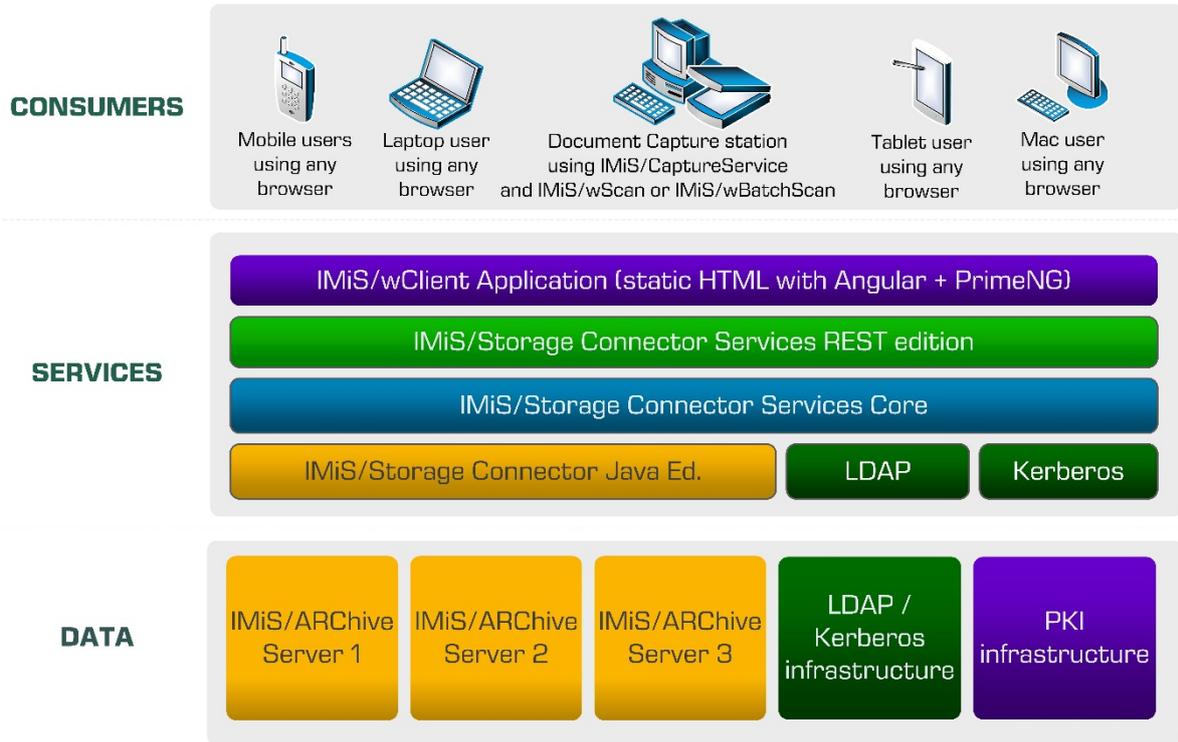


Image 1: Client architecture

3.2 Format of import / export files

The format of the import, export and data transfer files on the IMiS®/ARChive Server is the XML file, structured according to a partly modified Moreq2 scheme.

The differences between XML and Moreq2 schemes are as follows:

- Attributes which are required (mandatory) in the Moreq2 scheme and are not supported by the servers change from required to optional.
- All attributed in the "Custom" part of the XML scheme are newly added.

Moreq2 documentation is thus only a supplemental explanation of the attributes in the data transfer server scheme. Various types of entities (class, folder, document) are each covered by their separate scheme.

Since the schemes are derived from the Moreq2 standard, the following terminology is used:

Item type	Moreq2
Class	Class
Folder	Folder
Item inside folder	Sub-File
Document	Record

Table 4: Terminology explanation

The description of XML tags uses XPath notation for a clearer overview.

Example:

```
<?xml version="1.0"encoding="utf-8"?>
  <Class xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.dlm-network.org/moreq2/1.04.01">
    <Description xmlns="">
    <abstract />
    <classification>
      <classification_code>08</classification_code>
      <fully_qualified_classification_code>08</fully_qualified_classification_code>
    </classification>
    <place />
    <title>Balance sheet Q3 2018 </title>
```

...

Image 2: XPath notation text example

In the above example, the path to a full classification code in XPath notation would be shown by the following description:

/Class/classification/fully_qualified_classification_code.

3.2.1 File structure

Each entity is contained by its own XML file. The filename must be in the following format:

[class|file|sub-file|record]_audit_n.xml (the sequence number is identical to the sequence number of the entity). When importing data, it is important for all files of a given entity to be located in the same directory as the entity file.

The names of remaining files are contained in corresponding XML tags (chapter [List of XML tags and their meaning](#)).

Example: When exporting a class, the file containing the class is named `class_1.xml`, and the audit log file for the class is named `class_1_audit.xml`.

3.2.2 List of XML tags and their meaning

The following section lists the supported tags, along with references to server documentation of the IMiS®/ARChive Server. The meaning of XML tags on the server and their reference to the Moreq2 code is presented in more detail. Every XML document begins with the root node, which describes the type (class, folder, sub-folder, document).

Since the scheme is derived from the Moreq2 scheme, it uses the Moreq2 terminology (Class, File, Sub-File, Record) which is explained in table 4 found above.

For better clarity, the name of the root node in the presentation below is swapped with »<entity_type>«. In case the user is interested in an entity whose type is class, user can replace »/<entity_type>« with »/Class« and only view tags that use »Class: YES«.

/<entity_type>

	Required:	YES	Number:	1
Definition:	Root node			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	Uses entity types according to MOREQ2 standard (Class, File, Sub-File, Record).			
XMLSchema type:	complexType	Reference:	/	MOREQ2 code: /

/<entity_type>/Description/abstract/description

	Required:	NO	Number:	1
Definition:	Entity description			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: NO
Commentary:	Optional short description of the entity. This attribute has no influence on the business logic of the server during operations with entities and is merely an information carrier.			
XMLSchema type:	String	Reference:	sys:Description	MOREQ2 code: M047

/<entity_type>/Description/abstract/keyword

	Required:	NO	Number:	Multiple
Definition:	Keyword			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	Optional keywords that define the entity. This attribute has no influence on the business logic of the server during operations with entities and is merely an information carrier.			
XMLSchema type:	String	Reference:	sys:Keywords	MOREQ2 code: M004

/<entity_type>/Description/abstract/classification/classification_code

	Required:	YES	Number:	1
Definition:	Own classification code			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The own classification code is unique among all entities that are subordinate (child) to the same entity.			
XMLSchema type:	String	Reference:	Classification code	MOREQ2 code: M011

/<entity_type>/Description/abstract/classification/fully_qualified_classification_code

	Required:	YES	Number:	1
Definition:	Full classification code			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The full classification code is unique for the entire archive and consists of the full classification code of the parent entity, and the entity's own classification code.			
XMLSchema type:	String	Reference:	Classification codes	MOREQ2 code: M012

/<entity_type>/Description/copy_recipient/e_mail_address

	Required:	YES	Number:	Multiple
Definition:	Mail address of email copy recipient			
Use:	Class: NO	Folder: NO	Sub-File: NO	Record: YES
Commentary:	Values represent valid email addresses of email copy recipients. They are forwarded by the messaging client, which usually acquires them from the message itself, though the precision of the information depends on the client. Values represent the values of attributes »cc« of the message according to RFC 2822 specification.			
XMLSchema type:	String	Reference:	sys:eml:ToCC	MOREQ2 code: M185

/<entity_type>/Description/copy_recipient/name

	Required:	YES	Number:	Multiple
Definition:	Name of email copy recipient			
Use:	Class: NO	Folder: NO	Sub-File: NO	Record: YES
Commentary:	Values represent names of email copy recipients. They are forwarded by the messaging client, which usually acquires them from the message itself, though the precision of the information depends on the client. Values represent the values of attributes »cc« of the message according to RFC 2822 specification.			
XMLSchema type:	String	Reference:	sys:eml:ToCC	MOREQ2 code: M067

/<entity_type>/Description/date

	Required:	NO	Number:	1
Definition:	Message date			
Use:	Class: NO	Folder: NO	Sub-File: NO	Record: YES
Commentary:	The metadata is acquired from the message itself or entered when adding the message to the document system. It is used only in case of email messages and is filled out with the »sent« date.			
XMLSchema type:	DateTime	Reference:	sys:eml:Date	MOREQ2 code: M065

/<entity_type>/Description/external_identifier/external_system_reference

	Required:	NO	Number:	1
Definition:	Unique message identifier			
Use:	Class: NO	Folder: NO	Sub-File: NO	Record: YES
Commentary:	This value represents the unique external identifier of the email message, assigned by the messaging server upon delivery. The value is forwarded by the messaging client, which usually acquires it from the message itself, though the precision of the information depends on the client. Values represent the values of the attribute »message-id« of the message according to RFC 2822 specification.			
XMLSchema type:	String	Reference:	sys:eml:MessageId	MOREQ2 code: M195

/<entity_type>/Description/place/current_location

	Required:	NO	Number:	1
Definition:	Current location of physical records			
Use:	Class: NO	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The value represents a description of the current location of physical records, when this is not a home location or when physical records is checked out or entrusted to a third party for storage. Enter data that describes the external location of physical records as precisely as possible (address, room, cabinet, folder ...). At the same time, make the appropriate modification of the attribute »prm:Status« into »CheckedOut«.			
XMLSchema type:	String	Reference:	sys:prm:CurrentLocatio n	MOREQ2 code: M086

/<entity_type>/Description/place/home_location

	Required:	NO	Number:	1
Definition:	Home location of physical records			
Use:	Class: NO	Folder: YES	Sub-File: YES	Record: YES
Commentary:	This value represents a description of the home location of physical records. Enter data that precisely describes the in-house location where the physical records is being stored (address, room, cabinet, folder, file ...).			
XMLSchema type:	String	Reference:	sys:prm:HomeLocation	MOREQ2 code: M122

/<entity_type>/Description/recipient/e_mail_address

	Required:	NO	Number:	Multiple
Definition:	Email address of email recipient			
Use:	Class: NO	Folder: NO	Sub-File: NO	Record: YES
Commentary:	Values represent the valid email addresses of email recipients. They are forwarded by the messaging client, which usually acquires them from the message itself, though the precision of the information depends on the client. Values represent the values of attributes »to« of the message according to RFC 2822 specification.			
XMLSchema type:	String	Reference:	sys:eml:To	MOREQ2 code: M186

/<entity_type>/Description/recipient/name

	Required:	NO	Number:	Multiple
Definition:	Name of email recipient			
Use:	Class: NO	Folder: NO	Sub-File: NO	Record: YES
Commentary:	Values represent valid names of email recipients. They are forwarded by the messaging client, which usually acquires them from the message itself, though the precision of the information depends on the client. Values represent the values of the attribute »to« of the message according to RFC 2822 specification.			
XMLSchema type:	String	Reference:	sys:eml:To	MOREQ2 code: M066

/<entity_type>/Description/sender/e_mail_address

	Required:	NO	Number:	Multiple
Definition:	Email address of email sender			
Use:	Class: NO	Folder: NO	Sub-File: NO	Record: YES
Commentary:	This value represents a valid email address of the email sender. It is forwarded by the messaging client, which usually acquires it from the message itself, though the precision of the information depends on the client. The value represents the value of the attribute »from« of the message according to RFC 2822 specification.			
XMLSchema type:	String	Reference:	sys:eml:From	MOREQ2 code: M187

/<entity_type>/Description/sender/name

	Required:	NO	Number:	Multiple
Definition:	Name of the email sender			
Use:	Class: NO	Folder: NO	Sub-File: NO	Record: YES
Commentary:	This value represents the valid name of the email sender. It is forwarded by the messaging client, which usually acquires it from the message itself, though the precision of the information depends on the client. The value represents the value of the attribute »from« of the message according to RFC 2822 specification.			
XMLSchema type:	String	Reference:	sys:eml:From	MOREQ2 code: M075

/<entity_type>/Description/title

	Required:	YES	Number:	1
Definition:	Title of the entity			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The mandatory title of the entity being described.			
XMLSchema type:	String	Reference:	sys:Title	MOREQ2 code: M003

/<entity_type>/Event_history/abstract/reclassification_reason

	Required:	NO	Number:	1
Definition:	Commentary stating the reason for moving (reclassifying) an entity			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:				
XMLSchema type:	String	Reference:	sys:moveReason	MOREQ2 code: M021

/<entity_type>/Event_history/date/checked_in

	Required:	NO	Number:	1
Definition:	Date and time of change of attribute "prm:Status" to "CheckedIn"			
Use:	Class: NO	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The value represents the date and time when the attribute »prm:Status« of the entity in question received the value »CheckedIn«.			
XMLSchema type:	dateTime	Reference:	sys:prm:Status	MOREQ2 code: M093

/<entity_type>/Event_history/date/checked_out

	Required:	NO	Number:	1
Definition:	Date and time of change of attribute »prm:Status« to »CheckedOut«			
Use:	Class: NO	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The value represents the date and time when the attribute »prm:Status« of the entity in question received the value »CheckedOut«.			
XMLSchema type:	dateTime	Reference:	sys:prm:Status	MOREQ2 code: M094

/<entity_type>/Event_history/date/closed

	Required:	NO	Number:	1
Definition:	Date and time of change of attribute »sys:Status« to »Closed«			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The value represents the date and time when the attribute »sys:Status« of the entity in question received the value »Closed«.			
XMLSchema type:	dateTime	Reference:	sys:Closed	MOREQ2 code: M051

/<entity_type>/Event_history/date/created

	Required:	YES	Number:	1
Definition:	Date and time of the entity's creation			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The value represents the date and time when the entity was created.			
XMLSchema type:	dateTime	Reference:	sys:Created	MOREQ2 code: M048

/<entity_type>/Event_history/date/opened

	Required:	YES	Number:	1
Definition:	Date and time of change of attribute »sys:Status« to »Opened«			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The value represents the date and time when the attribute »sys:Status« of the entity in question received the value »Opened« (chapter General system attributes).			
XMLSchema type:	dateTime	Reference:	sys:Opened	MOREQ2 code: M050

/<entity_type>/Event_plan/date/return

	Required:	NO	Number:	1
Definition:	Return date and time of checked out physical record			
Use:	Class: NO	Folder: YES	Sub-File: YES	Record: YES
Commentary:	This value represents the status of physical record according to its current storage location. It is specified/changed in case physical record is checked out or transferred to a thirty party that stores it at a remote location.			
XMLSchema type:	dateTime	Reference:	sys:prm:ReturnDue	MOREQ2 code: M098

/<entity_type>/Event_plan/status/permanent

	Required:	YES	Number:	1
Definition:	States this entity should not be deleted			
Use:	Class: NO	Folder: YES	Sub-File: YES	Record: YES
Commentary:	This value states the entity should not be deleted, neither through an admin request nor in the review process. The value is merely a warning, and the administrator can choose to disregard it at their own discretion. The value »sys:Significance« of the coded entity is »Permanent« or »Vital«.			
XMLSchema type:	Boolean	Reference:	sys:Significance	MOREQ2 code: M031

/<entity_type>/Identity/system_identifier

	Required:	YES	Number:	1
Definition:	Unique system identifier			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	Assigned by the IMiS®/ARChive Server.			
XMLSchema type:	String	Reference:	Internal entity identifier	MOREQ2 code: M020

/<entity_type>/Relation/agent/custodian

	Required:	NO	Number:	1
Definition:	States the current custodian of physical record			
Use:	Class: NO	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The value represents the identity of the current custodian of physical record. When record is stored at a home location (value of the attribute »prm:Status« is »CheckedIn«), this is the person safekeeping the physical record. When it is stored remotely (value of the attribute »prm:Status« is »CheckedOut«), it is the outside person who was entrusted with safekeeping the checked out record.			
XMLSchema type:	String	Reference:	sys:prm:Custodian	MOREQ2 code: M002

/<entity_type>/Relation/agent/owner

	Required:	YES	Number:	1
Definition:	Person who is the current owner of the entity			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The value represents the directory subject (user or group) the entity belongs to (the owner of the entity).			
XMLSchema type:	String	Reference:	sys:Owner	MOREQ2 code: M002

/<entity_type>/Relation/is_child_of

	Required:	YES	Number:	1
Definition:	Full classification code of the parent entity			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:				
XMLSchema type:	String	Reference:	Classification code	MOREQ2 code: M057

/<entity_type>/Relation/retention_and_disposition_schedule

	Required:	YES	Number:	Multiple
Definition:	Unique system identifier of the retention policy			
Use:	Class: YES	Folder: YES	Sub-File: YES	Document: Conditionally
Commentary:	A link to the retention policy is required for the class, folder and document if it is classified directly under the class.			
XMLSchema type:	String	Reference:	Entity binds	MOREQ2 code: M025

/<entity_type>/Relation/disposal_hold

	Required:	NO	Number:	Multiple
Definition:	Unique system identifier of the disposition hold			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:				
XMLSchema type:	String	Reference:	Entity binds	MOREQ2 code: M032

/<entity_type>/Use/status/active

	Required:	YES	Number:	1
Definition:	Entity is active			
Use:	Class: YES	Folder: YES	Sub-File: NO	Record: NO
Commentary:	»true« when the attribute »sys:Status« of the entity in question has the value »Opened« (chapter General system attributes).			
XMLSchema type:	Boolean	Reference:	sys:Status	MOREQ2 code: M019

/<entity_type>/Use/status/physical

	Required:		NO	Number:	1
Definition:	Physical content tag				
Use:	Class: NO		Folder: YES	Sub-File: YES	Record: YES
Commentary:	»true« when this is physical record, »false« or no value when it is not				
XMLSchema type:	Boolean		Reference:	Physical records management attributes	MOREQ2 code: M084

/<entity_type>/Use/status/vital_record

	Required:	YES	Number:	1
Definition:	States this entity is of vital importance to the archive owner			
Use:	Class: NO	Folder: YES	Sub-File: NO	Record: YES
Commentary:	States that this entity is of vital importance. Deleting it by administrator's request or in the review process is prohibited. The entity may also follow a special data safety regime.			
XMLSchema type:	Boolean	Reference:	sys:Significance	MOREQ2 code: M005

/<entity_type>/Use/technical_environment/format

	Required:	NO	Number:	1
Definition:	Contains a description of physical record			
Use:	Class: NO	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The value represents a description of the physical record. Enter a precise description of the physical record, its format, physical carriers, volume ...			
XMLSchema type:	String	Reference:	sys:prm:Description	MOREQ2 code: M092

/<entity_type>/Custom/acl

	Required:	NO	Number:	1
Definition:	List of access rights and metadata on the entity (Access Control List)			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The label »acl« contains data about the list of access rights and metadata on the entity, that are not a part of the Moreq2 specification. Individual entries in the list of access rights are found in the contained »entry« labels.			
XMLScheme type:	complexType	Reference:	ACL	MOREQ2 code: /

/<entity_type>/Custom/acl/entry

	Required:	YES	Number:	Multiple
Definition:	List of access rights and metadata on the entity (Access Control List)			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES

<p>Commentary:</p>	<p>The entry in the list of access rights for an entity does not contain values, but it does contain an XML »user« attribute with the name of the directory's entity, and the following XML attributes that specify which access rights are valid for the directory's entity:</p> <ul style="list-style-type: none"> • type: enumerator of the type of access right (see below). • cr: right to edit access rights list.+- • cse: right to create new child entities. • da: right to delete the entity. • mv: right to move the entity. • ra: right to read the entity. • wa: right to edit the entity. • cre: right to change storage. • csc: right to change security class. • cs: right to change status. • date_from: date of current access control list validity (start / valid from). • date_to: date of current access control list validity (end / valid to). <p>The entry in the list of access rights for the entity's metadata contains an XML »user« attribute with the name of the directory's entity, an XML »property« attribute with the name of the metadata, and the following XML attributes that specify which access rights are valid for the directory's entity:</p> <ul style="list-style-type: none"> • type: enumerator of the type of right (see below). • ca: right to create the value of the entity's metadata. • da: right to delete the value of the entity's metadata. • ra: right to read the value of the entity's metadata. • wa: right to edit the value of the entity's metadata. • date_from: start of validity of the current list of access rights. • date_to: end of validity of the current list of access rights. <p>Description of enumerator values for the type of access right:</p> <ul style="list-style-type: none"> • EXPLICIT_ALLOW: explicit permission. • EXPLICIT_DENY: explicit denial. • INHERITED_ALLOW: inherited permission. • INHERITED_DENY: inherited denial. 				
<p>XMLScheme type:</p>	<p>none</p>	<p>Reference:</p>	<p>ACL</p>	<p>MOREQ2 code:</p>	<p>/</p>

/<entity_type>/Custom/additional_metadata

	Required:	NO	Number:	1
Definition:	User entered metadata			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	User entered metadata necessary for managing the archive. This data is not prescribed by the IMiS®/ARChive Server and is input by the user according to requirements. Additional metadata is intended for export only and is ignored in case of import.			
XMLSchema type:	any	Reference:	ETZ: 3.5.3.8 MOREQ2: 5.3.17	MOREQ2 code: /

/<entity_type>/Custom/audit_trail

	Required:	NO	Number:	1
Definition:	Name of the audit trail file			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The name of the separate file that contains the audit trail. To verify the file's authenticity, an XML attribute »hash_algorithm« of the type »string« which contains the name of the hash algorithm, and the XML attribute »hash« which contains the hash value of the exported audit trail, are added.			
XMLSchema type:	String	Reference:	Audit trail	MOREQ2 code: /

/<entity_type>/Custom/Content

	Required:	NO	Number:	1
Definition:	Container of attached content (files)			
Use:	Class: NO	Folder: NO	Sub-File: NO	Record: YES
Commentary:	The »content« label contains at least one »part« label, which represents exactly one document content and an XML »hash_algorithm« attribute that contains the name of the hash function, which is used when calculating the hash value of the exported content.			
XMLSchema type:	complexType	Reference:	sys:Content	MOREQ2 code: /

/<entity_type>/Custom/content/part

	Required:	NO	Number:	Multi
Definition:	Container of attached content (files)			
Use:	Class: NO	Folder: NO	Sub-File: NO	Record: YES
Commentary:	<p>The »part« label contains the name of a separate file, which contains exactly one exported document content, and the following XML attributes:</p> <ul style="list-style-type: none"> • description: content description • mime: data on content type • extension: extension of the attached content • size: content size • accessed: timestamp of the last access to the content • created: timestamp of the content creation • modified: timestamp of the last change of the content <p>hash: hash value of the content that is used for verifying the authenticity of a separate file.</p>			
XMLSchema type:	String	Reference:	ContentPart	MOREQ2 code: /

/<entity_type>/Custom/email

	Required:	NO	Number:	1
Definition:	Email metadata (names and values)			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The »email« label contains email metadata and the values that are not a part of the Moreq2 specification.			
XMLSchema type:	complexType	Reference:	»eml:« attributes	MOREQ2 code: /

/<entity_type>/Custom/email/subject

	Required:	NO	Number:	1
Definition:	Email subject			
Use:	Class: NO	Folder: NO	Sub-File: NO	Record: YES
Commentary:	The »subject« label contains the subject of the email.			
XMLSchema type:	String	Reference:	sys:eml:Subject	MOREQ2 code: /

/<entity_type>/Custom/email/blind_copy_recipient/e-mail_address

	Required:	NO	Number:	Multi
Definition:	The email address of the hidden recipient of the email copy			
Use:	Class: NO	Folder: NO	Sub-File: NO	Record: YES
Commentary:	The values represent valid email addresses of hidden recipients of the email copies. The values are transmitted by the client and are usually obtained from the email, although the accuracy of this information depends on the client. The values represent the values from the »bcc« attribute of the message according to the RFC 2822 specification.			
XMLSchema type:	String	Reference:	sys:eml:ToBCC	MOREQ2 code: /

/<entity_type>/Custom/email/blind_copy_recipient/name

	Required:	NO	Number:	Multi
Definition:	The name of the hidden recipient of the email copy			
Use:	Class: NO	Folder: NO	Sub-File: NO	Record: YES
Commentary:	The values represent the names of hidden recipients of the email copies. The values are transmitted by the client and are usually obtained from the email, although the accuracy of this information depends on the client. The values represent the values from the »bcc« attribute of the message according to the RFC 2822 specification.			
XMLSchema type:	String	Reference:	sys:eml:ToBCC	MOREQ2 code: /

/<entity_type>/Custom/email/priority

	Required:	NO	Number:	1
Definition:	Contains the priority status when sending email			
Use:	Class: NO	Folder: NO	Sub-File: NO	Record: YES
Commentary:	The »priority« label contains the priority status when sending email.			
XMLSchema type:	String	Reference:	sys:eml:Priority	MOREQ2 code: /

/<entity_type>/Custom/email/signed

	Required:	NO	Number:	1
Definition:	The value indicates whether the email was electronically signed			
Use:	Class: NO	Folder: YES	Sub-File: NO	Record: YES
Commentary:	The »signed« label contains the value that indicates whether the email has been electronically signed.			
XMLSchema type:	Boolean	Reference:	sys:eml:Signed	MOREQ2 code: /

/<entity_type>/Custom/Evidence

	Required:	NO	Number:	1
Definition:	Evidence of entity's authenticity			
Use:	Class: NO	Folder: YES	Sub-File: YES	Record: YES
Commentary:	<p>The value represents an evidence record of the entity's authenticity obtained from the previous ISDM in case of import. In case of export from ISDM, the data is exported into a metadata scheme and a third ISDM can again import it into the attributes of transferred entities. The attribute does not influence the business logic of the server, it serves merely as a carrier of information.</p> <p>Two XML attributes are contained:</p> <ul style="list-style-type: none"> • Hash_algorithm: »string« type containing the name of the hash algorithm. • Hash: hash value of file with the authenticity evidence. <p>The value of the XML tag contains the name of the authenticity evidence file.</p>			
XMLSchema type:	String	Reference:	sys:trf:Evidence	MOREQ2 code: /

/<entity_type>/Custom/physical_identifier

	Required:	NO	Number:	1
Definition:	Identifier of the metadata of physical material			
Use:	Class: NO	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The label »physical_identifier« contains the identifier of the metadata of physical material.			
XMLSchema type:	String	Reference:	Physical content	MOREQ2 code: /

/<entity_type>/Custom/properties

	Required:	NO	Number:	1
Definition:	Other entity attributes together with values			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The »properties« label contains at least one »property« label, which represents the entity attributes together with values that are not a part of the Moreq2 specification.			
XMLSchema type:	complexType	Reference:	Attribute	MOREQ2 code: /

/<entity_type>/Custom/properties/property

	Required:	YES	Number:	Multi
Definition:	Entity attribute together with values			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	<p>The »property« label represents the entity attribute together with values. Every »property« label can have the following XML attributes:</p> <ul style="list-style-type: none"> • »name«, which contains the name of the attribute. • »type«, which contains the type of the attribute in the database. • »value_type«, which represents the type of the attribute with possible values: STRING, STRINGMAX, BINARY. • »hash_algorithm«: contains the name of the hash function that is used for calculating hash value for STRINGMAX or BINARY type attributes and at least one »value« label, which contains either the value of the entity's attribute for STRING type attributes or the name of a separate file for STRINGMAX or BINARY type attributes. 			
XMLSchema type:	complexType	Reference:	Attribute	MOREQ2 code: /

/<entity_type>/Custom/properties/property/value

	Required:	YES	Number:	Multi
Definition:	Value of the entity's attribute			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	<p>The »value« label does not contain XML attributes if the attribute type is STRING (see the »property« label). In this case, the value written in the label is the same as the value of the attribute.</p> <p>If the value of the attribute type is the same as STRINGMAX or BINARY, the value written in the »value« label is the same as the name of the separate file that contains the value of the attribute. In this case, the »value« label contains the XML »hash« attribute that represents the hash value of the file with the attribute content.</p> <p>For BINARY attributes the »value« label also contains the XML »mime« attribute, which contains data on the content type.</p>			
XMLSchema type:	String	Reference:	Attribute	MOREQ2 code: /

/<entity_type>/Custom/retention

	Required:	NO	Number:	1
Definition:	Entity retention policy list			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	<p>The »retention« label contains data on the entity retention policy list that is not a part of the Moreq2 specification. Individual entries in the retention policy list are found in the contained »policy« labels.</p>			
XMLSchema type:	complexType	Reference:	ACL	MOREQ2 code: /

/<entity_type>/Custom/retention/policy

	Required:	YES	Number:	Multi
Definition:	Entity's retention policy			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	The »policy« value represents the entity's retention policy. The value of the label is the same as the identifier of the retention policy. Besides the value, the label has an XML »filter« attribute that represents the retention policy's filter type with the following possible values: CLASS, FOLDER or DOCUMENT and their combinations.			
XMLSchema type:	String	Reference:	ACL	MOREQ2 code: /

/<entity_type>/Custom/template_id

	Required:	YES	Number:	1
Definition:	Unique template ID			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	Unique template identifier on the IMiS®/ARChive Server.			
XMLSchema type:	String	Reference:	Templates	MOREQ2 code: /

/<entity_type>/Custom/transferred_audit_log

	Required:	NO	Number:	1
Definition:	Previously imported audit log			
Use:	Class: YES	Folder: YES	Sub-File: YES	Record: YES
Commentary:	Content of the attribute sys:trf:AuditLog. The attribute is created only upon import to the IMiS®/ARChive Server.			
XMLSchema type:	String	Reference:	sys:trf:AuditLog	MOREQ2 code: /

/RDS/Description/abstract/description

	Required:	NO	Number:	1
Definition:	Longer description of the retention policy or disposition hold.			
Commentary:				
XMLScheme type:	String	Reference:	sys:ret:pol:DetailedDescription	MOREQ2 code: M043

/RDS/Description/mandate

	Required:	NO	Number:	Multiple
Definition:	Authorizations, which set the rights of the retention policy.			
Commentary:	Name of the file in the file system which stores the authorization in electronic form. Only the retention policy has authorizations.			
XMLScheme type:	String	Reference:	sys:Content	MOREQ2 code: M030

/RDS/Description/abstract/reason

	Required:	NO	Number:	1
Definition:	Reason for creating a retention policy or disposition hold.			
Commentary:				
XMLScheme type:	String	Reference:	sys:ret:hold:Reasonsys:ret:pol:Reason	MOREQ2 code: M015

/RDS/Description/title

	Required:	YES	Number:	1
Definition:	Title of the retention policy or disposition hold.			
Commentary:				
XMLScheme type:	String	Reference:	sys>Title	MOREQ2 code: M015

/RDS/Event_plan/event_type/disposition_action

	Required:	YES	Number:	1
Definition:	Default action of the retention policy in the implementation phase of the review process.			
Commentary:	Valid values: <ul style="list-style-type: none"> • Dispose: the default action of the retention policy is the disposition of entities. • Permanent: the default action of the retention policy is the permanent retention of entities. • Transfer: the default action of the retention policy is the transfer of entities to another system and their disposition after confirmation of successful transfer. • Review: the default action of the retention policy is to leave the entity for the next review process. 			
XMLScheme type:	String	Reference:	sys:ret:pol:Action	MOREQ2 code: M014

/RDS/Identity/system_identifier/disposal_hold

	Required:	YES	Number:	1
Definition:	Unique system identifier of the disposition hold.			
Commentary:	Set by IMiS®/ARChive Server.			
XMLScheme type:	String	Reference:	Internal entity identifier	MOREQ2 code: M137

/RDS/Identity/system_identifier/retention_and_disposition_schedule

	Required:	YES	Number:	1
Definition:	Unique system identifier of the retention policy.			
Commentary:	Set by IMiS®/ARChive Server.			
XMLScheme type:	String	Reference:	Internal entity identifier	MOREQ2 code: M008

/RDS/Use/status/inheritance

	Required:	NO	Number:	1
Definition:	Specifies whether the retention policy can be inherited by entities.			
Commentary:	The IMiS®/ARChive Server specifies that all retention policies are inherited. The value is always TRUE.			
XMLScheme type:	String	Reference:	Internal entity identifier	MOREQ2 code: M197

Table 5: Lists of XML tags

3.2.3 Format of the additional metadata export file

The additional (user entered) metadata export file is used for the particular requirements of the archiving process. Upon export, each entity may optionally be added additional metadata which is not part of the archived entity's own metadata.

The additional metadata is prepared by the archivist, using a premade XML file.

This metadata is not within the framework of the client or server's business logic.

The format of the file is prescribed with the following XSD scheme:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="http://www.dlm-network.org/moreq2/1.04.01"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:moreq2="http://www.dlm-network.org/moreq2/1.04.01"
elementFormDefault="unqualified" attributeFormDefault="unqualified" version="1.04.01">
  <xs:element name="AdditionalMetadataRoot">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Entity" minOccurs="0" maxOccurs="unbounded">
          <xs:complexType>
            <xs:sequence>
              <xs:any processContents="skip" maxOccurs="unbounded"/>
            </xs:sequence>
            <xs:attribute name="classification_code" type="xs:string"/>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

Image 3: Example XSD scheme

For each entity to be added user metadata during export, the archivist enters, in an XML file under the root node with the name »AdditionalMetadataRoot« (prescribed by the Moreq2 scheme), an »Entity« node with the attribute of the entity's classification code. During export, the content of this node is copied into the export XML file of the entity.

```
<moreq2:AdditionalMetadataRoot xmlns:moreq2="http://www.dlm-network.org/moreq2/1.04.01">
  <Entity classification_code="03.01">
    <!-- add custom XML node entries -->
    <A>Metadata A</A>
  </Entity>
  <Entity classification_code="03.01/00001">
    ...
  </Entity>
</moreq2:AdditionalMetadataRoot>
```

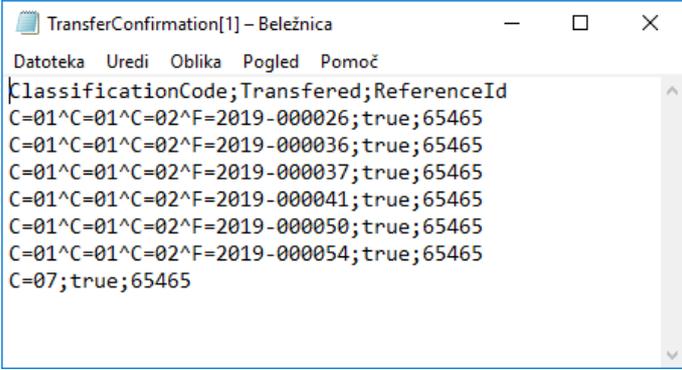
Image 4: Example additional metadata export file

3.3 Format of the confirmation file during transfer

The format of the confirmation file is a text file containing comma separated values; abbreviation: CSV.

Each record contains the following values:

- Classification code of the transferred entity.
- Confirmation value («true» – if the entity has been successfully transferred to a third archive system).
- Reference to the transferred entity in the third archive system.



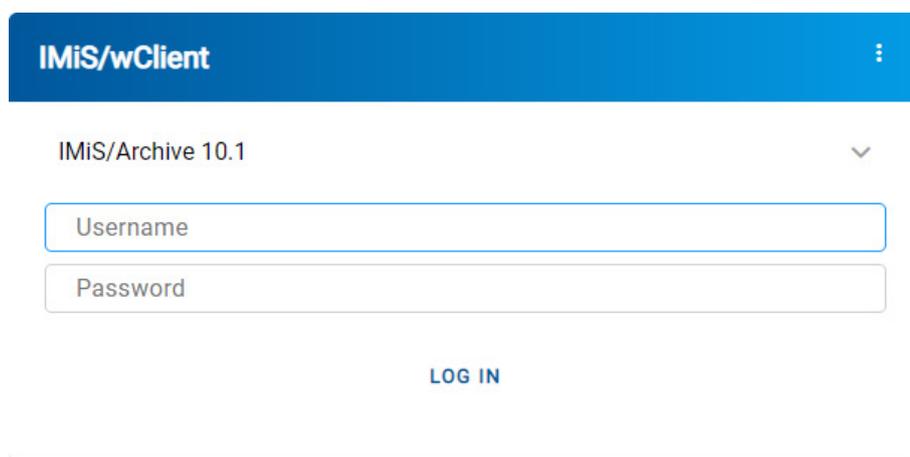
```
TransferConfirmation[1] – Beležnica
Datoteka Uredi Oblika Pogled Pomož
ClassificationCode;Transferred;ReferenceId
C=01^C=01^C=02^F=2019-000026;true;65465
C=01^C=01^C=02^F=2019-000036;true;65465
C=01^C=01^C=02^F=2019-000037;true;65465
C=01^C=01^C=02^F=2019-000041;true;65465
C=01^C=01^C=02^F=2019-000050;true;65465
C=01^C=01^C=02^F=2019-000054;true;65465
C=07;true;65465
```

Image 5: Example of a confirmation file after transfer

4 USER MANUAL

4.1 Login and Logout

The user accesses the IMiS®/wClient application via a web browser (Google Chrome, Mozilla Firefox, MS Edge, ...) by entering the URL of IMiS®/wClient in the title bar. A login window appears in which the user can log into the IMiS®/ARCHive Server.



IMiS/wClient (v1.5.2010.5)



Image 6: Login on 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.

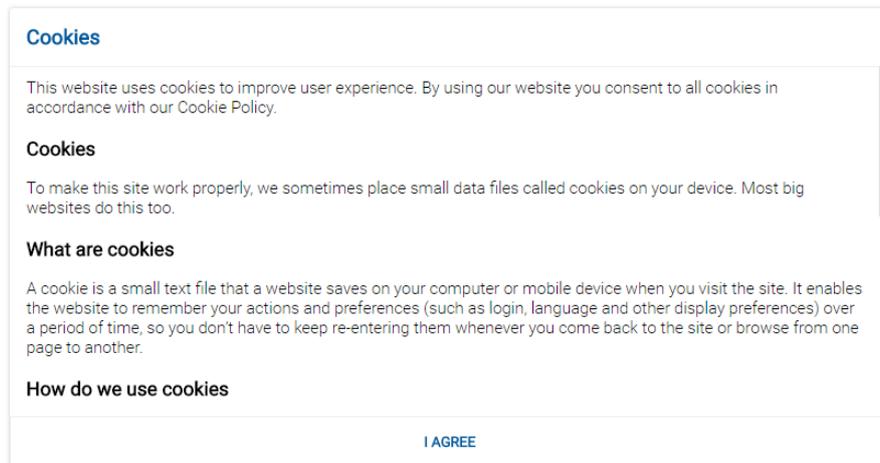


Image 7: Cookie Policy

4.1.2 Localization

In the top right corner of the login window the user can choose the language of the IMiS®/wClient application from a list by clicking on the icon .

In agreement with the application developer Imaging Systems Inc., the language selection can be expanded as desired.

The languages currently supported are:

- English
- Slovene.

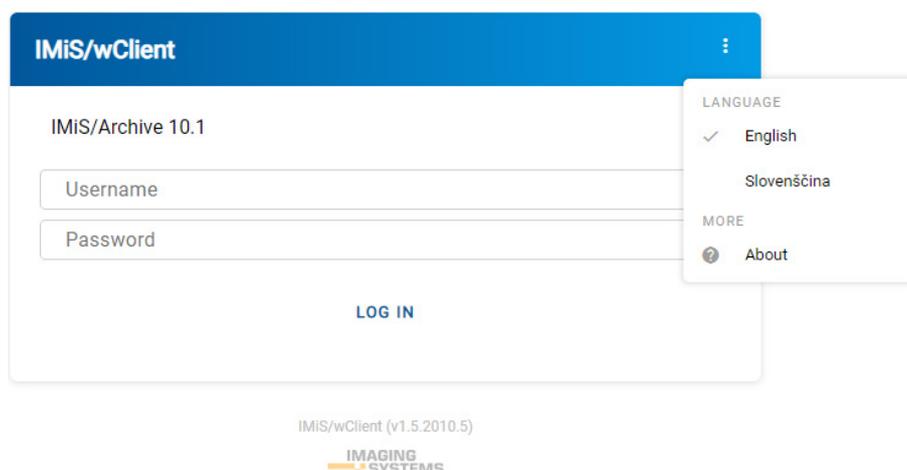


Image 8: Language selection

4.1.3 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®/Storage Connector Services REST version.
- License Agreement.
- Notices and Trademarks.

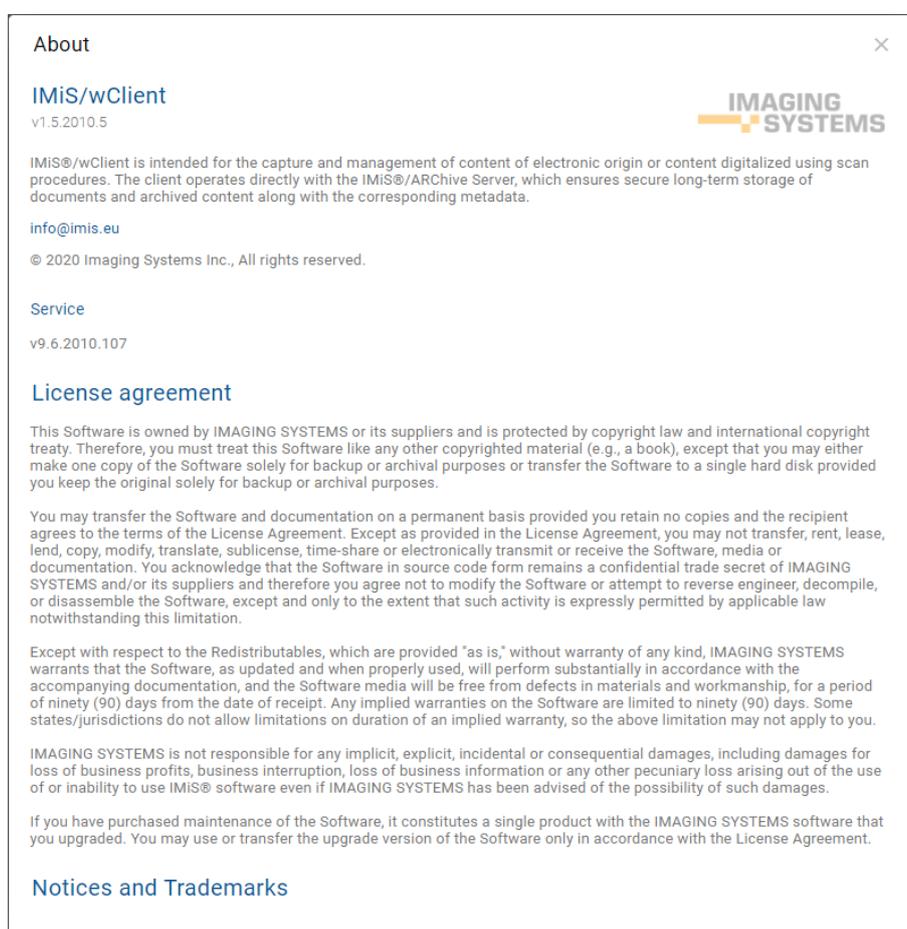


Image 9: About dialog box

4.1.4 Login

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

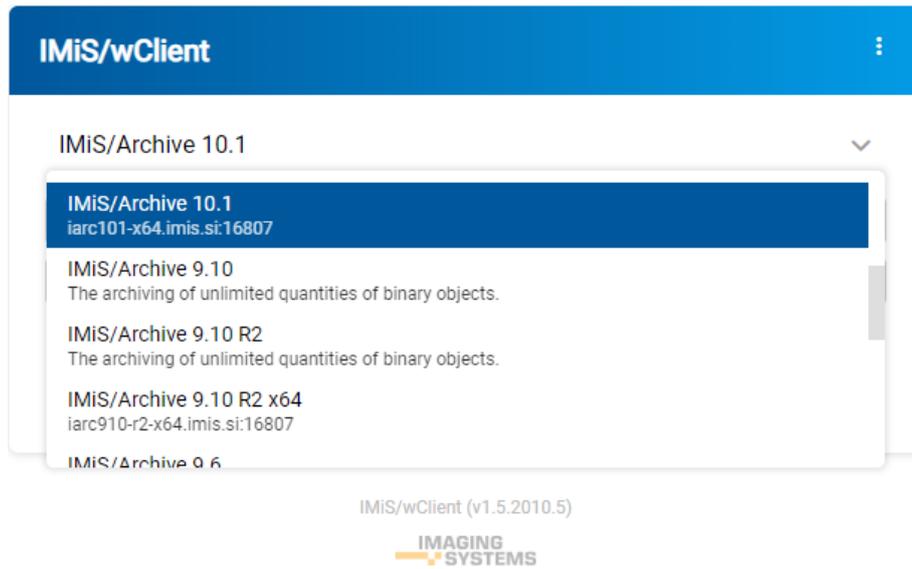


Image 10: A list of available archives

Note:

The user can choose only among the archives predefined by the administrator. The user selects the archive from a list by clicking on the arrow in the top right area of the login window. The administrator is the only one who can remove an archive.

The username that the administrator enters in the field "Username" is case insensitive. For faster selection in the case of a prior login, the username is shown below the field for entering the username.

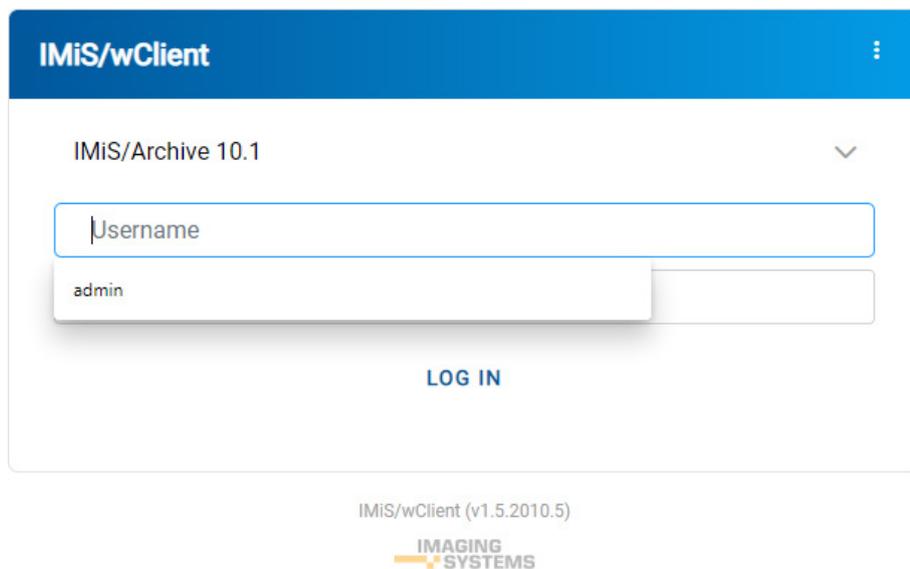


Image 11: Logging into the archive

After entering at least one character of the password, the logged-on user is shown the icon

. By selecting the icon, the user is shown the password characters.

The icon  next to the input field for entering the password enables displaying the password only when the display button is active (Mousedown). The user confirms login with the »Log in« button.

The user can log into multiple archive servers in multiple browser tabs.

When displaying the login page after the user has logged out, the user session remains open.

If the browser is refreshed, the user stays logged into the last archive server.

If the archive identifier does not match the URL after the browser has been refreshed, the login page is shown.

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.

4.1.5 Logout

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.

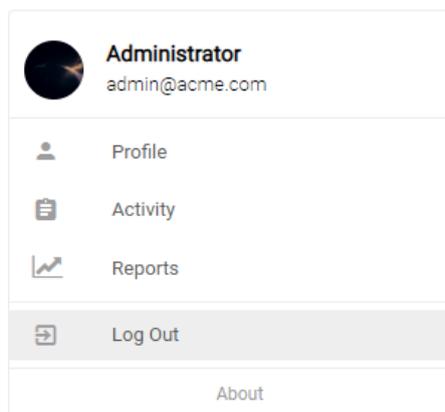


Image 12: Log out of the archive

4.2 Interface description

The user interface of the IMiS®/wClient is designed in accordance with contemporary design trends. 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.

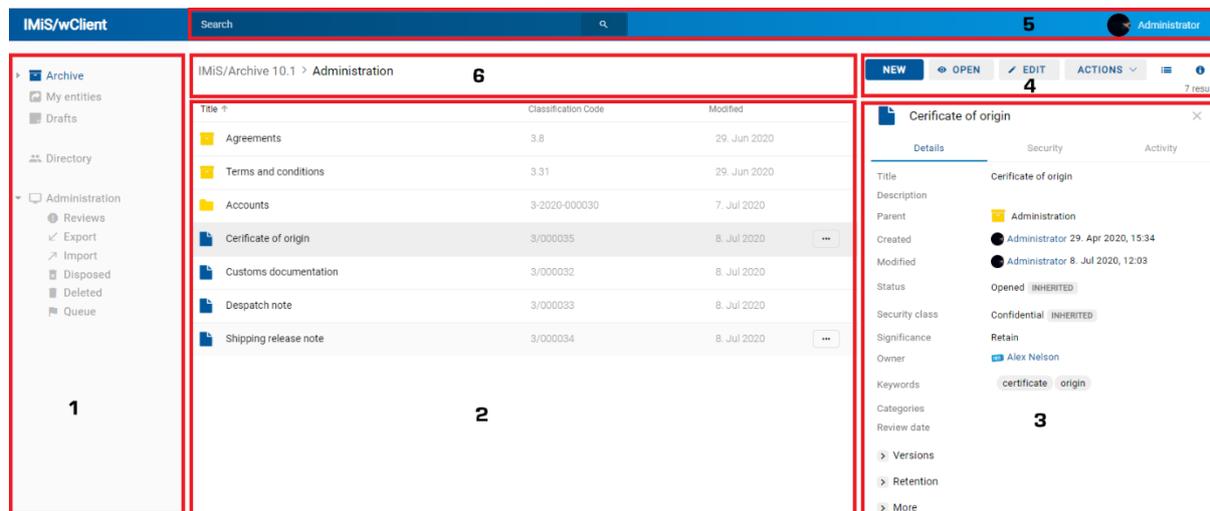


Image 13: User interface of the IMiS®/wClient

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

- Archive
- My entities
- Drafts
- Directory
- Administration.

For more information see chapter [Classification scheme](#).

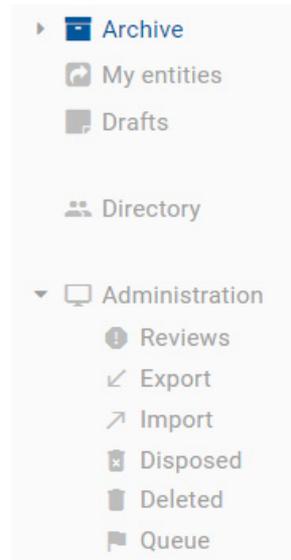


Image 14: Categories in the left view

In the central view of the user interface (number 2 in the image above) is a list of contained directory entities or the selected archive/entity. At the first level, the user can only create classes under the archive's root. The settings of the IMiS®/wAdmin administration web interface allow mixed entity types (classes, folders or documents) at the remaining levels. The mixing of entity types is enabled at the same level under the same parent entity.

Note: The user with permission can enable mixed entity types by checking *Allow Mixed Entity Types* in the section *Administration* in the basic view in the folder *Home* of the IMiS®/wAdmin administration web interface. Mixed entity types are not allowed at the first level of the classification scheme (root entities).

IMiS/Archive 10.1

Title ↑	Classification Co...	Description	Modified
Administration	3	Documents, Ad...	16. Sep 2020
Development	14	Technical know...	29. Jun 2020
Distribution	5	The process of ...	29. Jun 2020
Legacy object containers	99	Class holding L...	15. Jun 2013
Maintenance	8	Actions require...	14. Aug 2020
Other	16		20. Sep 2020
Production	1	Production doc...	20. Sep 2020

Image 15: A list of mixed entity types

The contained entities are shown below the bar with the titles of the common attributes.

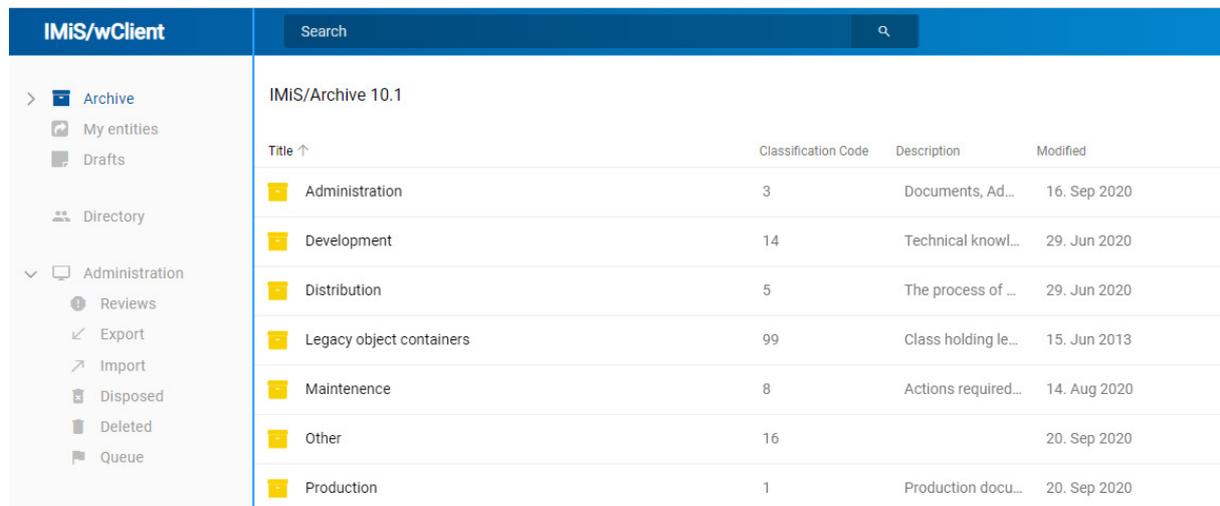
The »Title« is shown by default. More on the central view in the chapter [List of entities](#).

Note: When displaying a greater number of entities, loading all the entities simultaneously would greatly slow down the web client. That is why the user can load (directory) entities by pages.

After showing the first 50 entities, the slider stops halfway; by moving the slider all the way down, 50 new (directory) entities are added.

The user can set the spacing between the left and central view by moving the dividing line.

This setting applies while the user is logged into the archive.



Title ↑	Classification Code	Description	Modified
Administration	3	Documents, Ad...	16. Sep 2020
Development	14	Technical knowl...	29. Jun 2020
Distribution	5	The process of ...	29. Jun 2020
Legacy object containers	99	Class holding le...	15. Jun 2013
Maintenance	8	Actions required...	14. Aug 2020
Other	16		20. Sep 2020
Production	1	Production docu...	20. Sep 2020

Image 16: Movable dividing line between the left and central view

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.

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

For more information see the chapter [Entity information](#) and [Entity access](#).

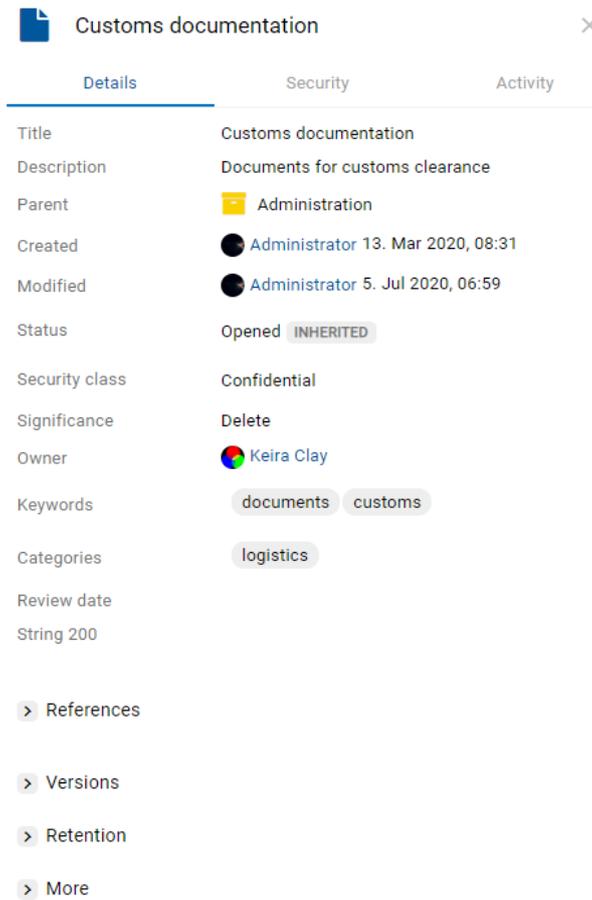


Image 17: Entity information

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.

For more information see the chapter [Command bar](#).



Image 18: Display of the command bar

Note:

If the Archive folder is selected, only the button for creating root classes (New) 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 application (IMiS®/wClient).
- A field for entering the search string with the option of selecting the search scope.
For more information see chapter [Search](#).
- Information on the user's profile and the program module.
For more information see chapter [Menu functions](#).



Image 19: Header of the user interface

To enable quicker access to parent 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. By selecting the title of the parent entity, the user is shown a list of child entities in the central view.

IMIS/Archive Server > Custom Relationship Man... > Invoicing and Crediting > Invoices > Takok 2018

Image 20: Hierarchical position of the entity within the tree structure

The user has the option of narrowing the user interface display by dragging the right edge to the left.

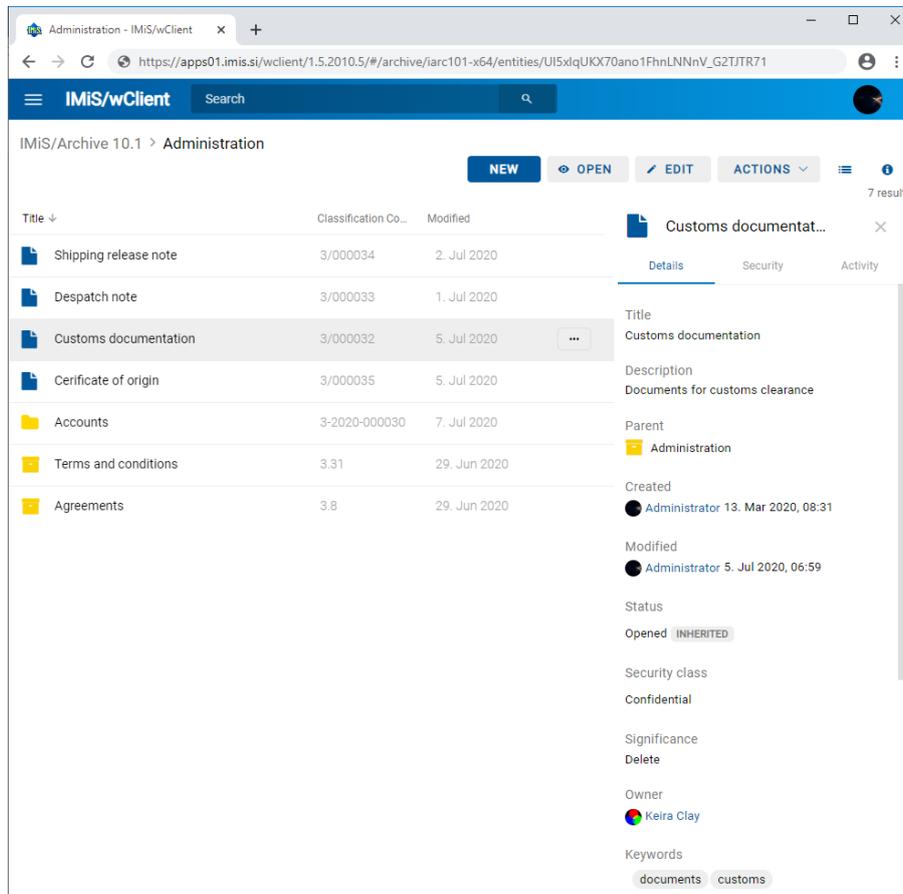


Image 21: Narrowing the user interface display

By narrowing the user interface display, the left view with the classification scheme, list of directory entities and administration folders is moved to the menu. The user accesses the menu via the icon .

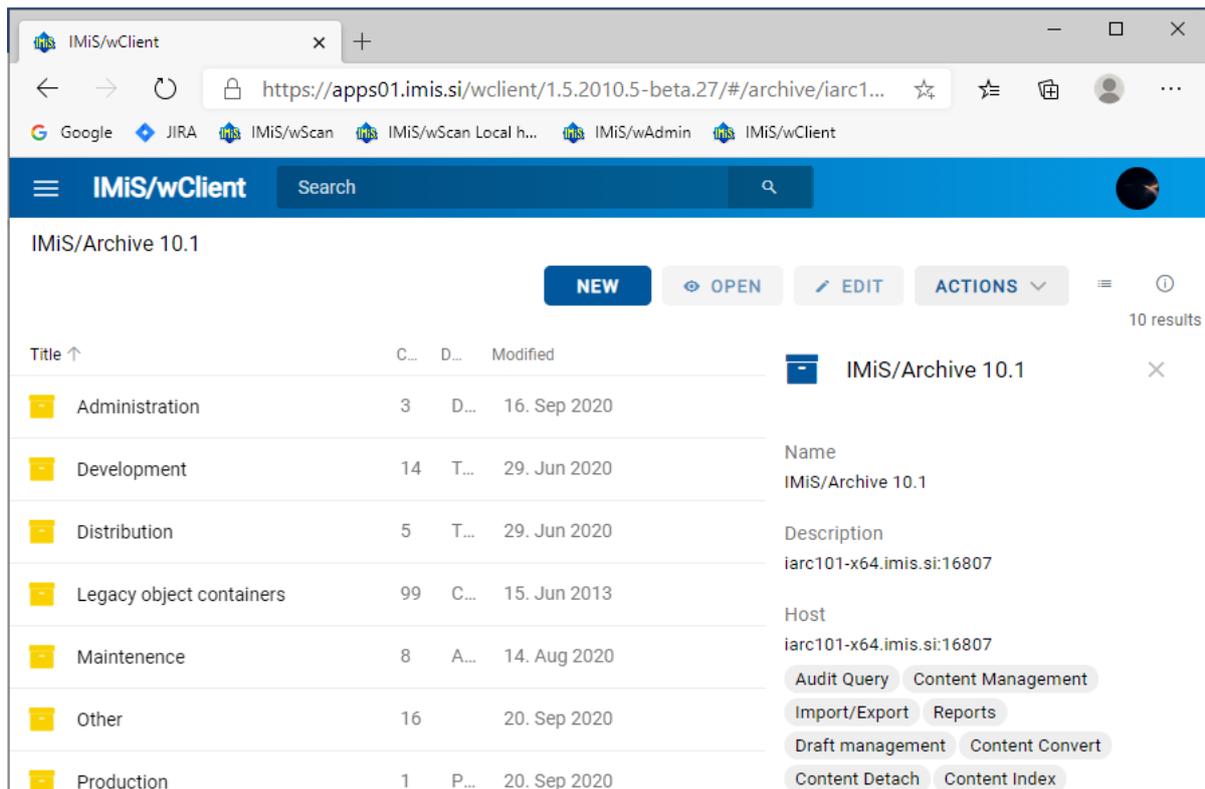


Image 22: Access to folders in the left view via the menu

4.2.1 Classification scheme

In the left view of the IMiS®/wClient, the user is shown the following categories:

- Archive: root classes in the classification scheme.
- My entities: a list of entities accessed by the user.
- Drafts: drafts of document versions.
- Directory: a list of archive users.
- Administration: a system folder with subfolders.

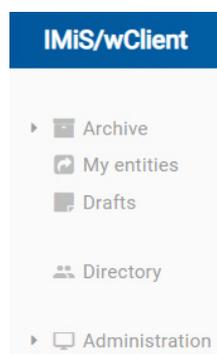


Image 23: Display of folders in the left view of the web client IMiS®/wClient

4.2.1.1 The Archive folder

By selecting the Archive folder in the left view, the user is shown a list of archive root classes. By clicking on the arrow in front of the selected class, the user is shown a list of contained classes.

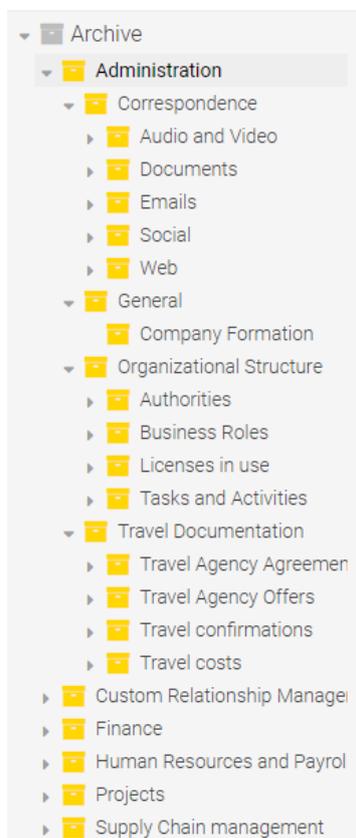


Image 24: The tree view of the classification scheme in the Archive folder

By right-clicking over the selected entity, the user opens a popup menu and performs the following actions:

- New: creates a new entity under the selected entity.
- Open: opens the selected entity in reading mode.
- Edit: opens the selected entity in editing mode.
- Share: copies the link to the selected entity and shares it with other users.
- Delete: deletes the selected entity.

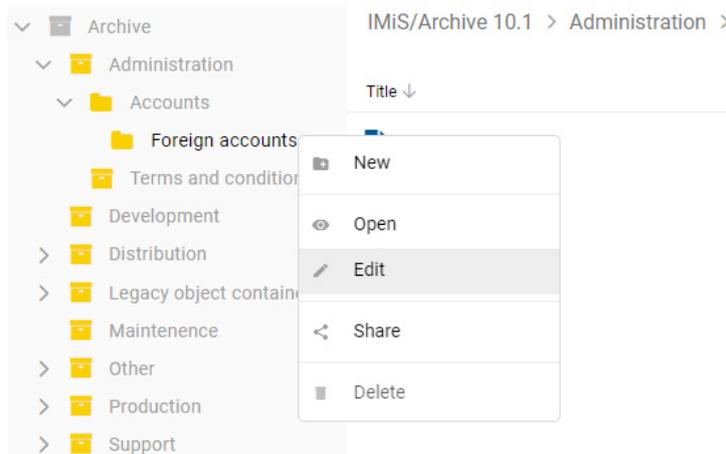


Image 25: Popup menu in the tree view

Note:

By clicking on the arrow in front of the selected class, the user is shown a list of contained classes. By configuring the server, the user can limit the number of levels for classes and folders in the classification scheme. The default setting specifies a hierarchy with a maximum of three (3) class levels.

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.

4.2.1.2 The My entities folder

By selecting the Directory folder in the left view, the user is shown a list of entities, whose owner is the current user, in the central view.

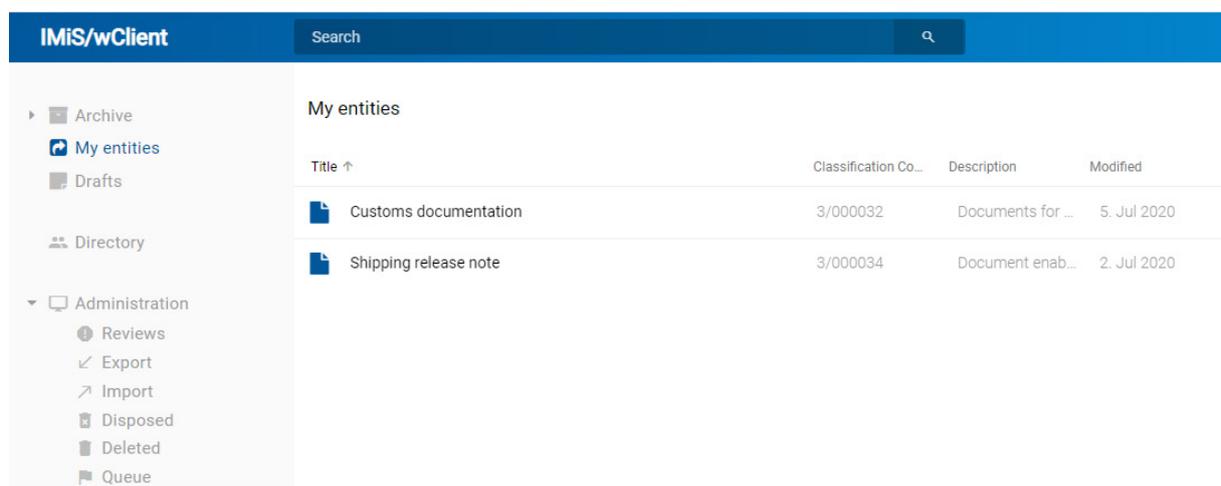


Image 26: Selecting the entity in the My entities folder in the central view

4.2.1.3 The Drafts folder

By selecting the Drafts folder in the left view, the user is shown a list of entity version drafts, to which the current user has access, in the central view.

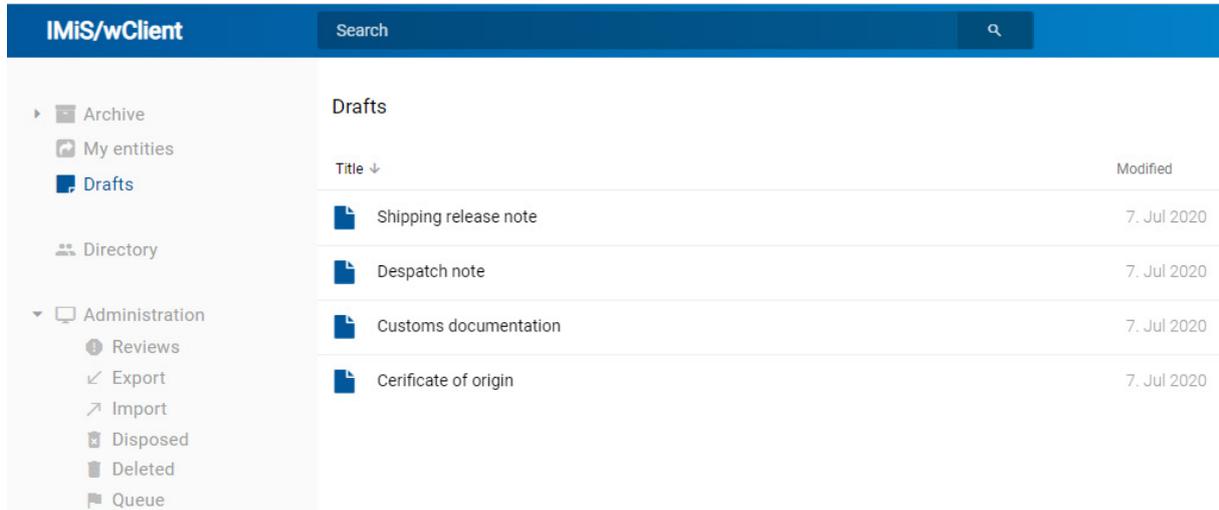


Image 27: Selecting the Drafts folder in the left view

4.2.1.4 The Directory folder

By selecting the Directory folder in the left view, the user is shown a list of directory entities (users or groups) in the central view.

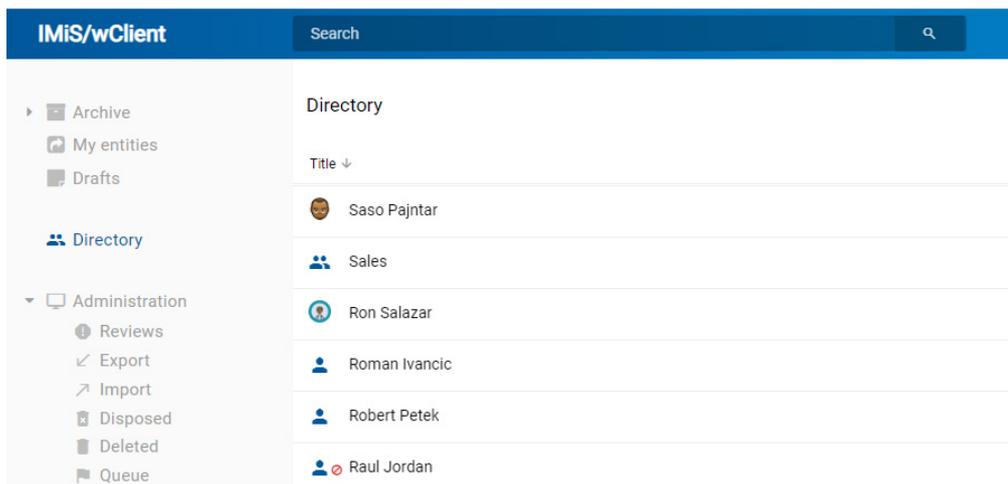


Image 28: The Directory folder in the left view

In the event of a greater number of directory entities, the user can search by the text entered in the search box (title, first name, last name, email, description) and select the directory entity in the popup menu below the text.

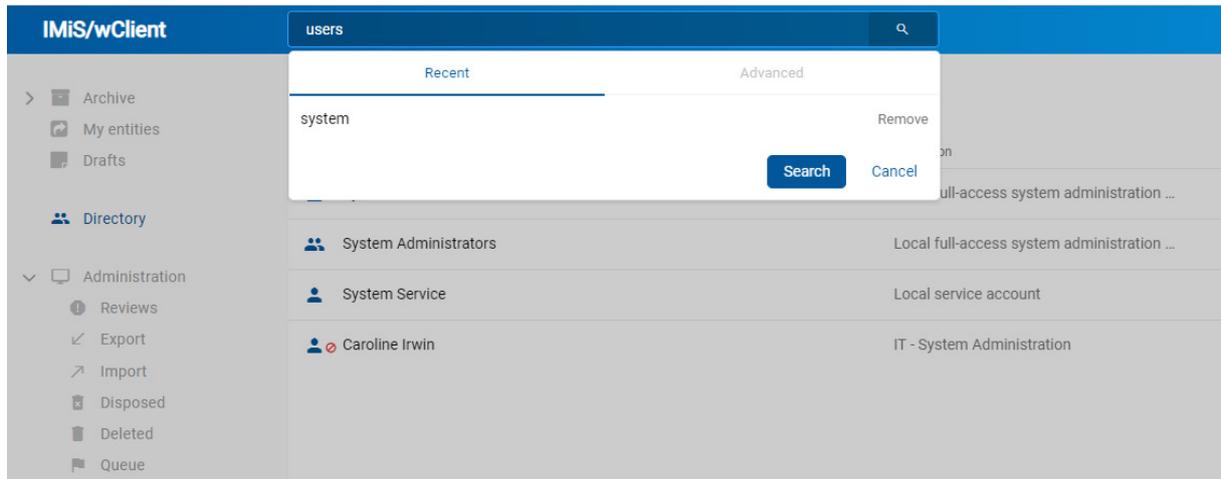


Image 29: Searching by directory entities

The search results are shown on pages with the option of being edited by title in ascending or descending order.

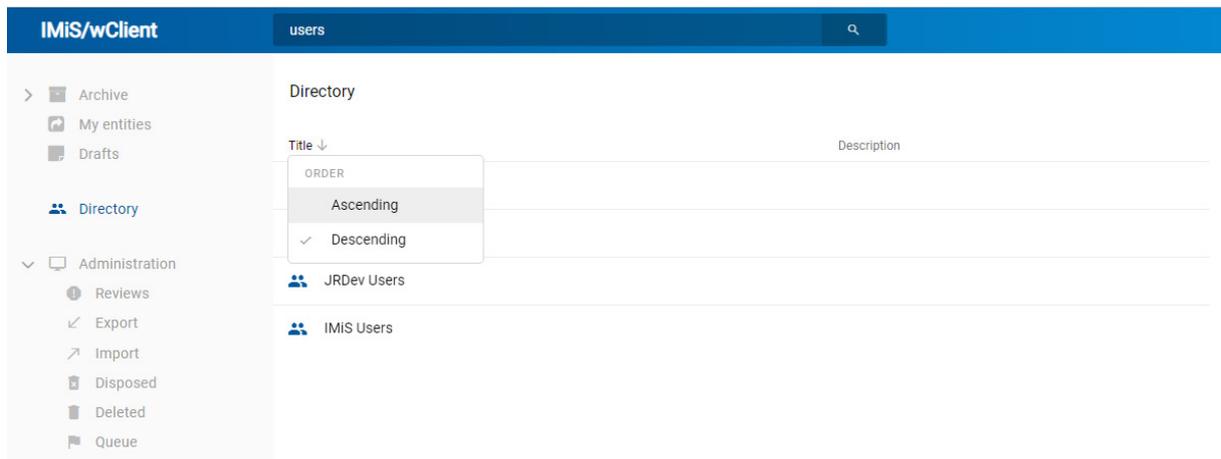


Image 30: Results of searching by directory entities

The right view provides the directory entity information.

The screenshot shows the user data view in the IMiS/wClient interface. The left pane displays a directory list with columns for Title and Description. The right pane shows a detailed view for user 'Ron Salazar'.

Title ↓	Description
Ron Salazar	Sales - IT support
Marco Welch	Sales

Ron Salazar

Description	Sales - IT support
Type	User
First name	Ron
Last name	Salazar
Email	ron.salazar@acme.com
Security class level	Restricted
Created	System Administrator 1. Jan 0001, 01:22
Modified	Administrator 23. Jul 2020, 15:29
Aliases	
Member of groups	Everyone Users IT Sales
Identifier	rsalazar

Image 31: User data

4.2.1.5 The Administration folder

The folder Administration is available to the user in the left view with a default display of subfolders:

- Reviews: a list of reviews in the review process.
For more information see chapter [Review process](#).
- Export: a list of entity exports containing reports.
For more information see chapter [Export](#).
- Import: a list of entity imports containing reports.
For more information see the chapter [Import](#).
- Trash: a list of deleted entities. This folder contains the following subfolders:
 - Disposed: a list of entities disposed of during the review process.
 - Deleted: a list of deleted entities.
 - Queue: a list of entities waiting for deletion.

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
4. Modified.

If the user has also selected the Classification code, Description and Modified in the settings, in addition to the “Title”, the view also shows information on the selected entity.

IMiS/Archive Server > Supply Chain management

Title ▲	Classification Code	Description	Modified
[-] Maintenance	03.06		13/9/2018
[-] Manufacturing	03.04		22/8/2018
[-] Planning and Control	03.01		22/8/2018
[-] Procurement	03.03		22/8/2018
[-] Production	03.07	Production docu...	27/9/2018
[-] Quality Management	03.05		22/8/2018
[-] Work Organization	03.02		22/8/2018

Image 32: A list of contained entities of the selected entity

By selecting the arrow next to the title of the common attributes column, the logged-on user is shown the entities in descending or ascending order. Similarly, by selecting the title a menu appears with the options “Ascending” and “Descending”. The entities on the list are sorted first by entity type and then by title.

IMiS/Archive 10.1 > Administration

Title ↑	Classification Code	Modified
ORDER	Conditions	10. Mar 2020
[-] Ascending		
[-] Descending		
[-] Folder 1	3-2020-000001	12. Mar 2020
[-] Folder 2	3-2020-000002	20. Mar 2020
[-] Audio	3/000016	10. Mar 2020
[-] Danes je lep sončen dan	3/000026	26. Mar 2020

Image 33: Sorting by entity type

Sorting in ascending or descending order is also possible for “Classification code” and “Modified”.

Note: The user can select entities from the list using arrow keys on the keyboard (up/left, down/right).

If the contained entity contains a greater number of entities than specified in the settings, the user is shown the notification Entity collection contains XXX entities and is too large to be displayed automatically.

For more information on setting the number of entities shown on the list see chapter [Installation settings](#).

IMIS/Archive 10.1 > Development

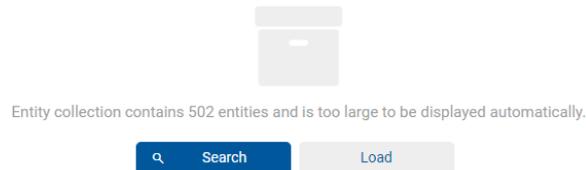


Image 34: Limiting the display of a greater number of entities on the list

The user has two options:

- The user can limit the set of entities displayed on the list with a search (the recommended choice).
- The user loads the entities and displays them on the list.

If the user selects the action Search, a dialog box appears for entering the search string.

For more information on limiting the set of attributes for a search, see chapter [Full text search](#).

Image 35: Limiting the set of entities displayed on the list with a search

If the user selects the action Load, the entities are loaded and displayed on the list.

The user add or remove the columns of the selected attribute Classification code, Description and Modified with the icon  in the command bar. The Title column is always present and cannot be removed.

For more information on the entity display options see chapter [Menu functions](#).

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

IMiS/Archive 10.1 > Administration

Title	Classification Co...	Description	Modified
 Despatch notes			ent se... 15. Sep 2020
 Shipping release note			t ena... 15. Sep 2020
 Invoices	3/000042		15. Sep 2020
 Terms and conditions	3.31	A set of regulat...	11. Sep 2020
 Accounts	3-IS	Accounts recei...	20. Sep 2020
 Certificate of origin	3/IS-CC-027		17. Sep 2020

ORDER
 Ascending
 Descending

Image 36: Selecting the order of displaying the list of entities

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.

Tip:

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 Entity information

Information about the selected entity is found in the right view of the IMiS®/wClient user interface. The tabs are available in the following modes of displaying information on the selected entity:

- Preview: a display of tabs and their contents which are publicly accessible to the user.
- Open: a display of tabs according to the user's effective permissions.
- Edit: a dialog box opens with the attributes whose values can be modified.

Details	Security	Activity
Title	Administration	
Description		
Parent	IMiS/Archive 10.1	
Created	Administrator 19. Feb 2020, 13:17	
Modified	Marko Hren 20. May 2020, 15:16	
Status	Opened	
Security class	Confidential	
Significance	Permanent	
Owner	Marko Hren	
Keywords	key1	
Review date	5. Apr 2017, 08:11	

Image 37: Tabs containing entity information in the reading mode

4.2.3.1 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.

4.2.3.1.1 General metadata

The Details tab contains general and general metadata for the selected entity.

By selecting the name in front of a given set, the user is shown the remaining entity details.

For more information see chapter [General system attributes](#).

The screenshot shows the 'SpaceX' entity details in reading mode. At the top, there are buttons for 'NEW', 'OPEN', 'EDIT', and 'ACTIONS'. Below the entity name 'SpaceX', there are three tabs: 'Details' (selected), 'Security', and 'Activity'. The 'Details' tab contains the following information:

Field	Value
Title	SpaceX
Description	SpaceX project description
Parent	Administration
Created	Administrator 11. Mar 2020, 11:25
Modified	Administrator 30. Apr 2020, 11:54
Status	Opened INHERITED
Security class	Confidential
Significance	Retain
Owner	Alex Nelson
Keywords	space project
Categories	projects

Image 38: The Details tab in the reading mode

Note: The user profile settings save the open/closed status for: "Reference", "Versions", "Retention", "Email", "Physical properties", "Save log" and "More".

4.2.3.1.2 Custom metadata

If using a suitable template, the user with the appropriate rights can predefine the Custom metadata when creating or editing an entity.

They are available to the user in open mode in the Details tab.

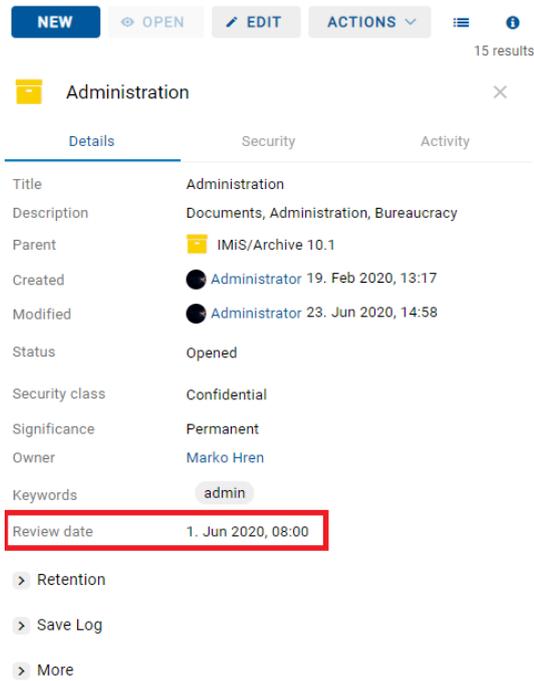


Image 39: Custom metadata in the reading mode

In edit mode the user has the option of editing Custom metadata.

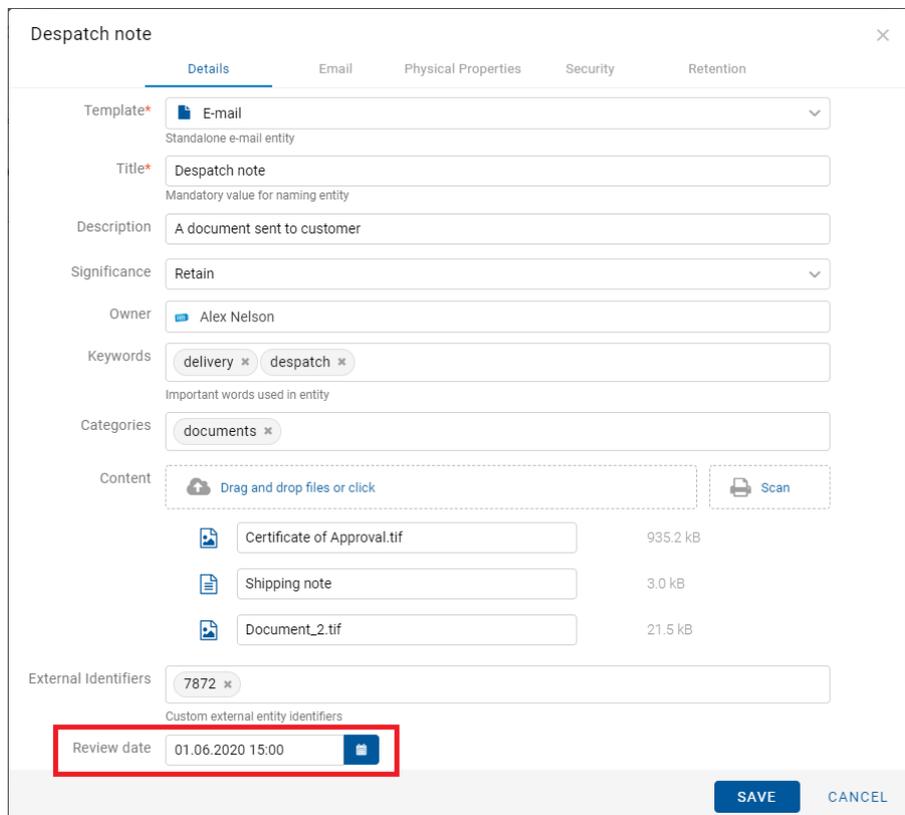


Image 40: Custom metadata in edit mode

Note: The attributes in the template, which is predefined by the user with permission, can be multi-value.

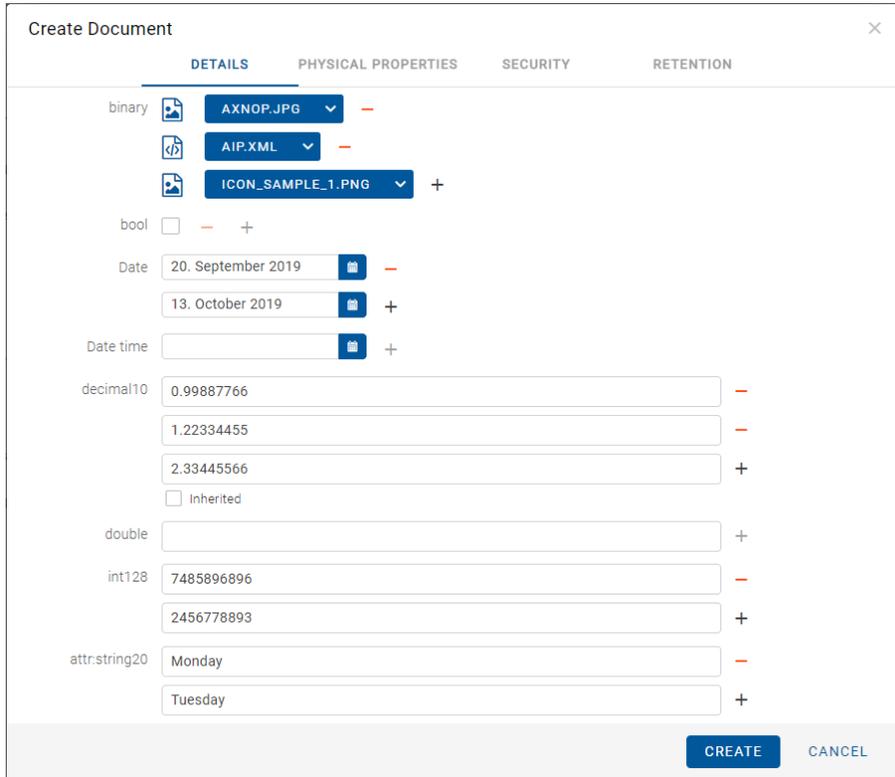


Image 41: Specifying multi-value attributes

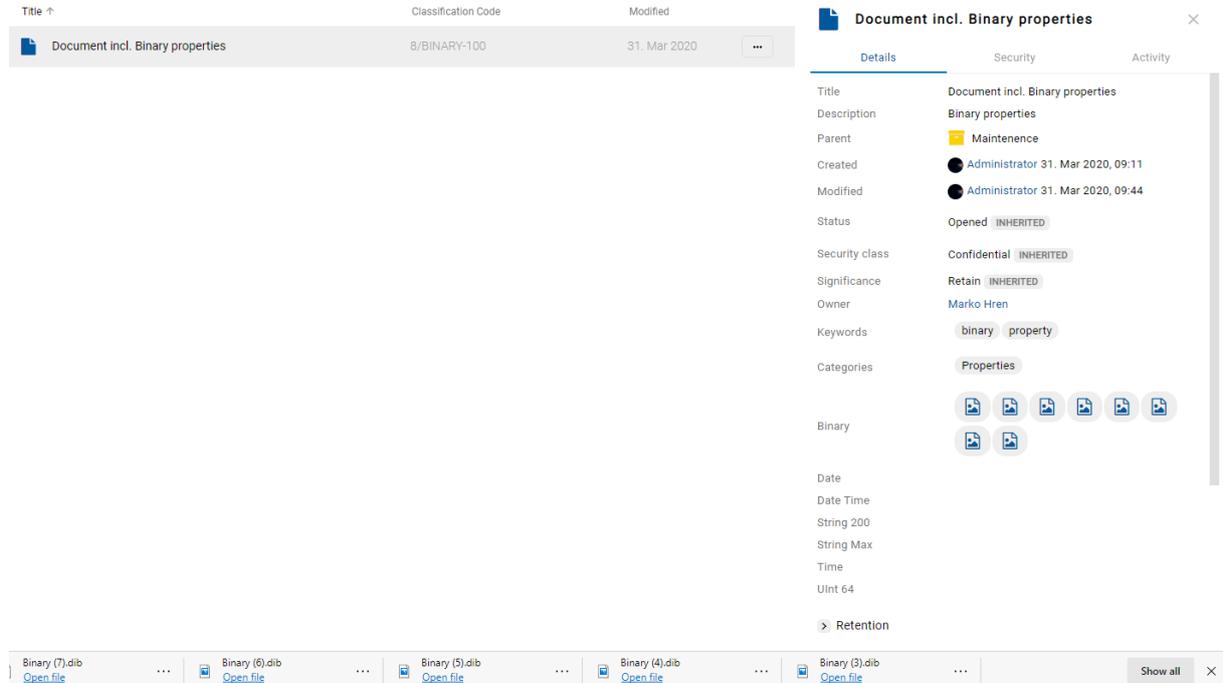


Image 42: Display and selection of binary values

4.2.3.1.3 System metadata

Unlike the general metadata, which are publicly accessible and can be edited and changed by the user, the system metadata are read-only. The user can access them by selecting the arrow in front of the »More« record.

For more information see chapter [General system attributes](#).

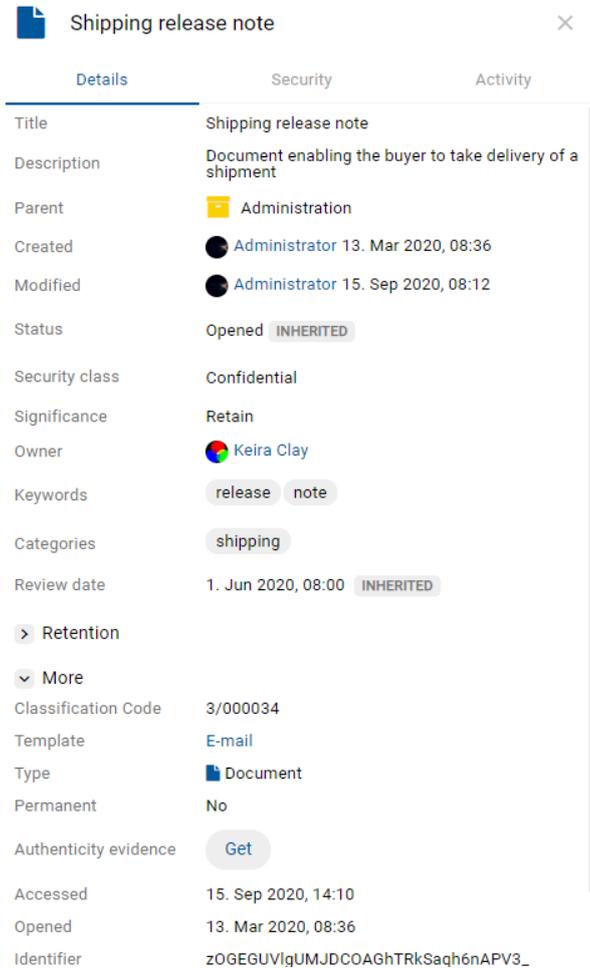


Image 43: The Details tab in reading mode

4.2.3.1.4 Reference

The user with the effective Change references permission can add new references, edit and delete them.

In the References set the user is shown the references to other entities by clicking on the arrow in front of the name in open mode.



Image 44: References in the Details tab

For more information on editing a reference see chapter [Adding and editing references](#).

4.2.3.1.5 Email

In the Email set the user is shown the email metadata by clicking on the arrow in front of the name in the reading mode (Open). Only the documents created based on the email template are shown.

For more information see chapter [Email attributes](#).



Image 45: Email data in the reading mode

In edit mode the user has the option to review email metadata but not to edit them.



Image 46: Email data in the editing mode

4.2.3.1.6 Physical content

The Physical properties set is available to the user only if the value of at least one attribute has been defined. By clicking on the arrow in front of the name in open mode, the user is shown the physical content metadata.

For more information see chapter [Physical content attributes](#).

Physical properties	
Identifier	ID435
Description	Building 4, Floor 2nd, Room 5, Cabinet 2, Shelf 1
Status	CheckedOut ,26. Sep 2018, 11:47
Home location	Brnčičeva 41G
Current location	Dunajska cesta 56
Custodian	Alex Nelson
Return due	28. Sep 2018

Image 47: Physical content data in the reading mode

In edit mode the user has the option of editing all metadata.

Information about a new payment transaction ×

DETAILS EMAIL PHYSICAL PROPERTIES SECURITY RETENTION

Identifier

Description

Status ▼
Status change 26. Sep 2018, 11:47

Home location

Current location

Custodian

Return due

Image 48: Physical content data in the editing mode

4.2.3.1.7 Save log

After checking the validity of electronic signatures and digital certificates upon capture, a Save log is created. The user can review it in the open mode by selecting the arrow in front of the Save log closed set.

For more information see chapter [Checking the validity of the digital certificate](#).

```

Save Log
<?xml version="1.0"?>
<iarc:commitlog xmlns:iarc="http://www.imis.si/imisarc/com
=====
Verifying Go-To-Market report.pdf [bcee4e037007d8e95c9fbb6
Signature status: VALID
Signing certificate subject: '/C=SI/ST=Slovenija/OU=indivi
Signing certificate issuer: '/C=SI/O=Republika Slovenija/
Valid from: '2017-09-28T13:03:03Z'
Valid to: '2022-09-28T13:33:03Z'
=====
Digital signature verification ended: 2018-10-19T07:32:04.
MIIEjCCAvKAgAwIBAgINAjCud3YAAAAAVx3QbzANBgkqhkiG9w0BAQsFAI
CQYDVQQGEwJTSTECMBoGA1UEChMTUmVudWJsawthIFNsb3Zlbn1qYTEXME
YRMOVkfUu0ktMTc2NTk5NTcxFjAUBGNVBAMTDVNIJLVRSVVNUIFJvb3QwHk
NDI1MDczODE3WhcNMzcwMjI1MDgwODE3WjBcMQswCQYDVQQGEwJTSTECME
ChMTUmVudWJsawthIFNsb3Zlbn1qYTEXMBUGA1UEYRMOVkfUu0ktMTc2NT
FjAUBGNVBAMTDVNIJLVRSVVNUIFJvb3QwggGiMA0GC5qGSIB3DQEBAAQAA4
ggGKAoIBgQDTy5wtwuAwQ2UxJP9LsDjzqVPXNdHbt0uTtHKN8cuV01Mrd:
PgIG3a9wFaGqzxGHimZ7y8wdcERCj6zK5sNbJ75No44Qv25UdAhwi1Poy:
IN1L6KwEdawY1YKLG+EgJAdGqwx1NKbni3XuqdmRKRvtby1FwtbiYAGx86
P4w+CPZTK3uiyUwhRIGAZppgOhvEvgzMMBB/ETV4SuaboZZTnJTMEcYETk
4a+MHDx8uZM33/1dPdZrD5dsRM1ZZ1twb/8EG/f1acNdwXj+vafZzC+in:
PHXyJ5eYLj4yd1Ndb2rsCJhWAE3KKYgn55gXpuQvEZDuP5t2MBm1iRrNH
W01I005MvQF7bj5A6tHCCkKTZ8MmLz8HW8+v4x3o0uJ14YSRP/VmAP2qM6

```

Image 49: A report on checking the validity of electronic signatures and digital certificates

4.2.3.1.8 Retention

A user with the »Change retention« effective permission is enabled the adding and editing of retention and disposition hold periods.

In the Retention set the user is shown the settings for the selected retention and disposition hold periods in the preview or reading mode by clicking on the arrow in front of the name.



Image 50: Retention and disposition hold periods in 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.

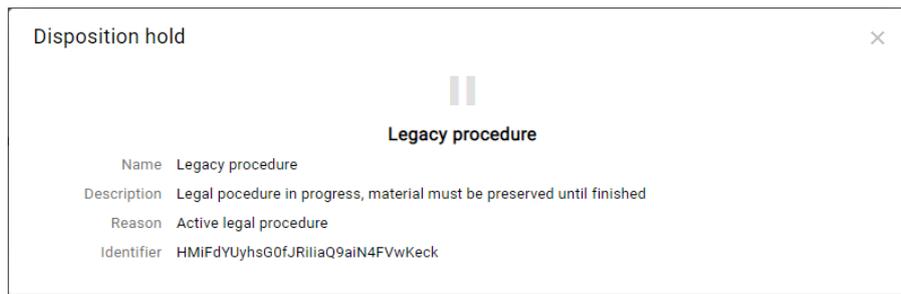


Image 51: Information on disposition hold

By clicking on an individual 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.
- Mandates: mandates for an individual retention policy.

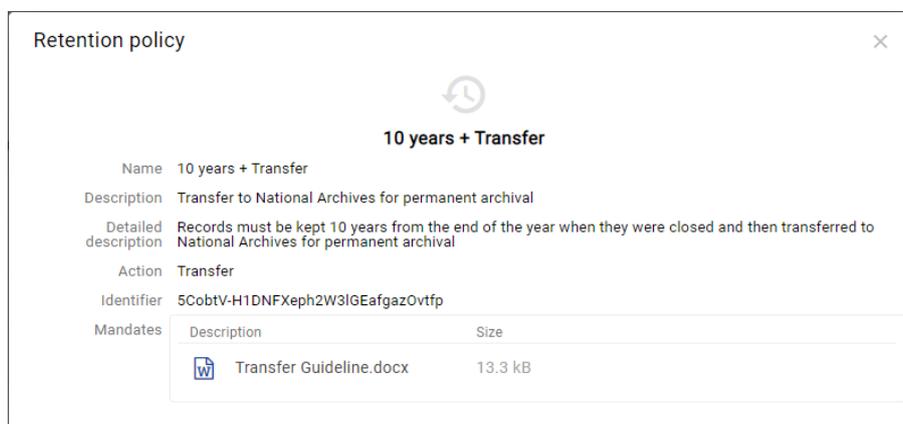


Image 52: Retention policy information

By selecting the command Get, the content opens for the user in the viewer.

For more information on editing retention and disposition hold periods see chapter

[Editing retention policies.](#)

4.2.3.2 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.

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

- Read: permission to read data on the selected entity (view metadata and content files).
- Write: permission to edit entity data (write metadata and add content files).
- Move: permission to move the entity within the classification scheme.
- Delete: permission to delete entity data (delete metadata and remove content files).
- Create entities: permission to create sub-entities inside the selected entity.
- Change permissions: permission to change the effective permissions of other users on the selected entity.
- Change security class: permission to change the security class of the selected entity.
- Change status: permission to change the status of a selected entity.
- Change retention: permission to read and change the content of »Retention« tab.
- Create references: permission to create a reference to another reference.

In the preview mode the user is shown a list of the access control list (ACL) for the logged user.

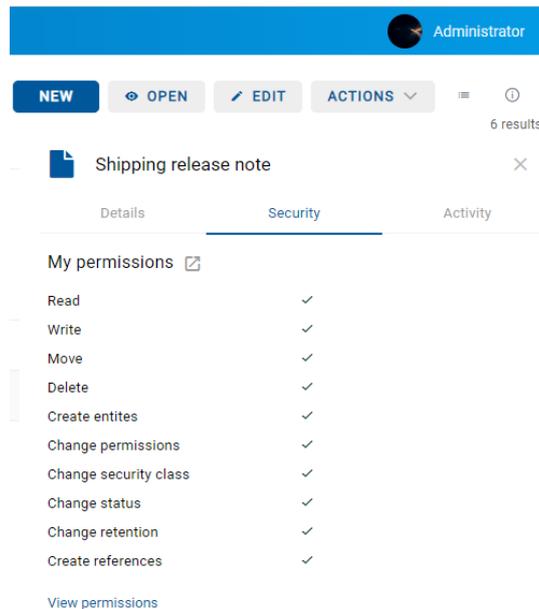


Image 53: The Security tab for a logged user in the preview mode

By selecting View permissions below the list of access permissions, when in read-only mode the user is shown a list of all directory entities that have been granted at least one explicit permission on the selected entity in the access control list (ACL).

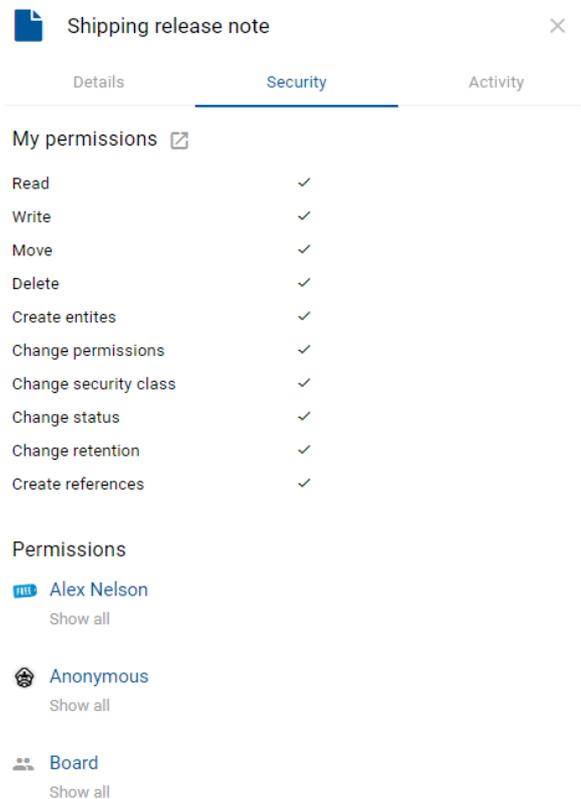


Image 54: A list of directory entities with access rights to the entity in the reading mode

By selecting "Show all", the current status of effective permissions for the selected user is shown.

4.2.3.3 The Activity tab

The Activity tab shows the audit log for the selected entity. This tab is shown to the user with the AuditLogQuery role.

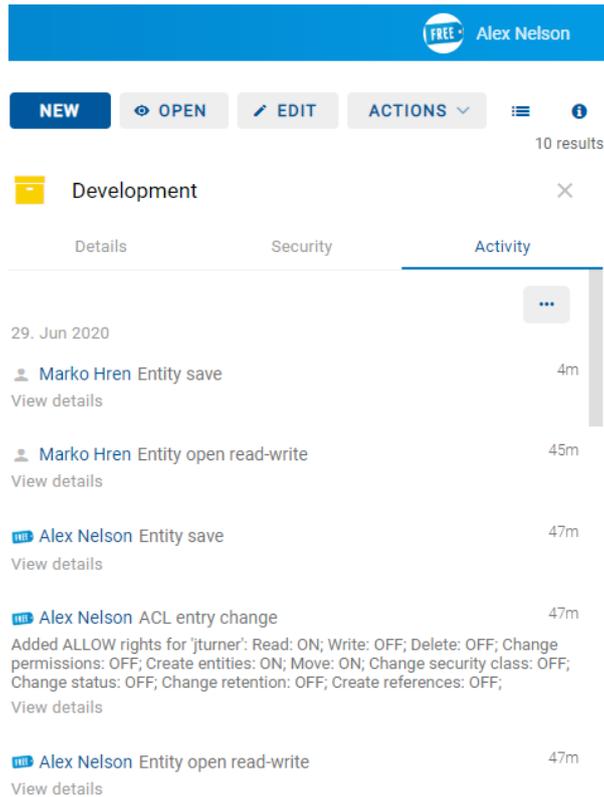


Image 55: The Activity tab in the preview and reading mode

The audit log records the following information:

- User: the 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.
- Event type: a type of event that was performed on the selected entity.

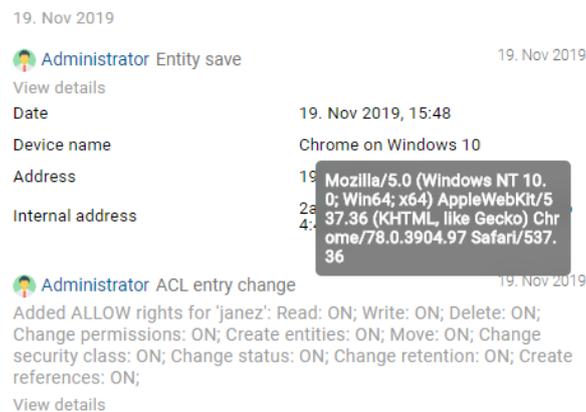


Image 56: Information about the user who performed an action on the entity

- **Date:** a time when an action was performed on the selected entity.
- **Device name:** the name of device, from where the command to perform the action on the selected entity came from.
- **Address:** the network address from where the command to perform the action on the selected entity came from.
- **Internal address:** IP address, which is set by opening a new session with the REST service.

When choosing the »Export« command in the right upper button, a popup menu appears with the possible audit log export formats for the selected entity. The supported formats are CSV and XML.

After selecting the format, the user is shown a notification in the bottom left corner about the downloaded content.

In the popup menu the user has the option of selecting actions. By selecting the action “Open”, the user has the option of saving the audit log to the file system.

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:** edits the status of the entity via a dialog box, which also offers the option to enter the reasons for the changes performed.
 - **Security class:** changes the entity's security class via a dialog box, which requires the user to enter the reasons for the change performed.
 - **Share:** copying the link to the selected entity to be shared with other users.
 - **New reference:** adding a connection to another entity in the classification scheme via a dialog box. For more information see chapter [The Details tab](#).
 - **New version:** creating a new version of the selected document in the classification scheme via a dialog box. For more information see chapter [Versioning](#).
 - **Classification code:** changes the classification code of the selected entity.

- Move: moves the selected entity around the classification scheme of the archive.
- Delete: deletes the selected entity.
- Import: imports the selected entities to the archive.
- Export: exports the selected entities of the archive.

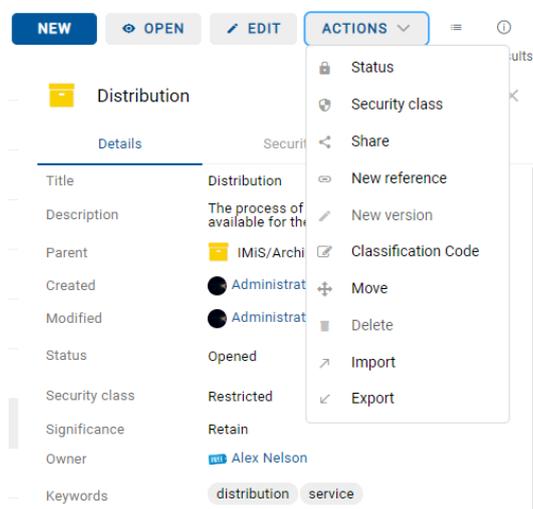


Image 57: Command bar above the information of the selected entity

Below the command bar is the search results counter. It displays the number of entities on the list in the central view.

To the right of the icon for the entity display mode, the user can close or open the right view with entity information by selecting the icon .



Image 58: Enabling/disabling the display of entity information

4.2.5 Menu functions

By selecting the user's name or icon, the following commands are available in the popup menu:

- Profile: information about the user.
- Activity: information about audit log events for the selected user and entity.
- Reports: reports on document contents, retention periods, reviews, access permissions, classification schemes, entities, deleted entities and entities waiting for deletion.

- Log out: log out from the application. After logging out of the selected archive, a dialog box appears for the user to log in again to the selected archive.
- About: information about the application.

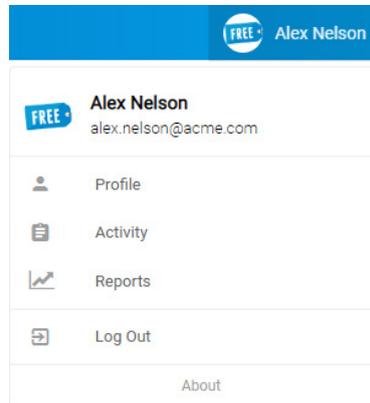


Image 59: Popup menu in the header of the user interface

4.2.5.1 User information

By selecting on Profile, a dialog window opens, showing the following sections:

- Details
- Security
- Settings
- Search History

Note: The user leaves the profile settings by selecting the name of the IMiS®/wClient application or archive (e.g. IMiS/ARChive 10.1).



Image 60: Transition from profile settings to the entity review in the archive

4.2.5.1.1 The Details tab

The “Details” tab contains the following information on the logged-on user:

- 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.
- The modified value is shown after 15 minutes or after logging out and logging back in. The administrator has a special value (1) which is not mapped to the text.
- Created: the user that created the directory entity and the date and time of creating the directory entity.
- Modified: the user that last edited the directory entity and the date and time of the last change to the directory entity.
- Aliases: alternative names of the directory entity with which the directory entity can access the archive.
- Member of groups: view of the list of groups of which a specific user is a member.
- Type: a directory entity type (user, group).
- Identifier: the unique identifier of the user.

IMIS/Archive 10.1

Alex Nelson [Edit](#)

Details Security Settings Search History

First name	Alex
Last name	Nelson
Description	Sales - Controlling
Email	alex.nelson@acme.com
Security class level	13369344
Created	System Administrator 1. Jan 0001, 01:22
Modified	Administrator 12. Mar 2020, 10:58
Aliases	alex@acme.com an@acme.com nelson@acme.com
Member of groups	Everyone Users Controlling Board
Type	User
Identifier	anelson

Image 61: Display of the “Basic” tab

By selecting the action “Edit”, the user edits information in the “Basic” tab.

The user has the following icon (avatar) management options:

- Change avatar: selecting a new image file from the file system. The change becomes effective as soon as the file selection is confirmed.
- Remove avatar: removal of the existing image. The change is executed immediately. After the removal it is replaced by the default image.

IMIS/Archive 10.1

Alex Nelson

Details Security Settings Search History

Change avatar Remove avatar

First name

Last name

Description

Email

Security class level Restricted

Created System Administrator 1. Jan 0001, 01:22

Modified Administrator 16. Jun 2020, 15:39

Aliases alex@acme.com an@acme.com nelson@acme.com

Member of groups Everyone

Type User

Identifier anelson

Image 62: Editing user details in edit mode

Note: For more information on setting editing permissions see chapter “[Server Configuration](#)” / “[Authentication](#)” in the *IMiS®/ARChive Server Manual*.

4.2.5.1.2 The Security tab

The “Security” tab is used to manage the “Password” and review the “Session history”.

IMiS/Archive 10.1

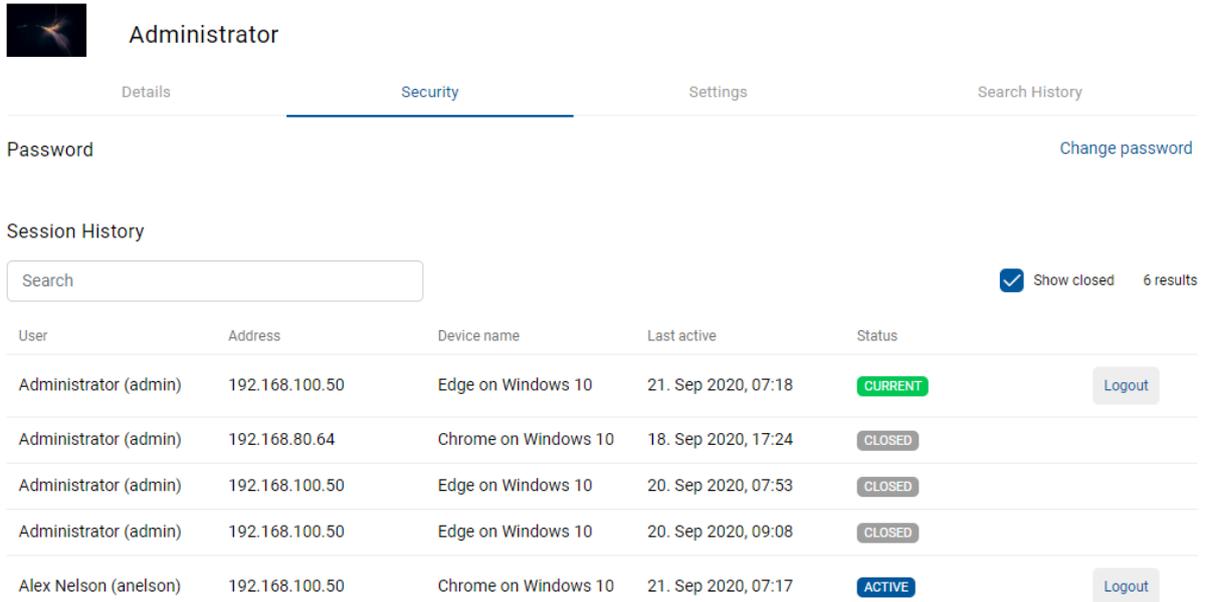


Image 63: Display of the “Security” tab

Note: By unchecking the parameter “Show closed”, the list shows only active sessions. On the right, the user can see the displayed sessions counter.

Password

By selecting the action “Change password”, the user is shown a dialog box for entering the current password and the new password, which the user must confirm. The user confirms the final change of password by selecting the command “Change password”.

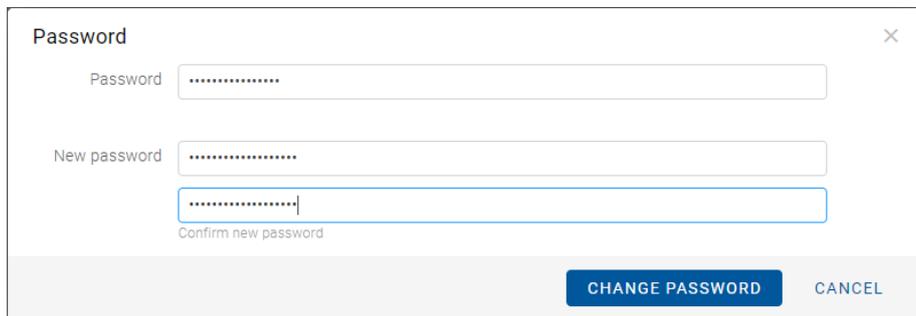


Image 64: Display of the window for changing the user password

Session history

A logged-on user can view the history of their own user sessions.

The user with permission (administrator) can view the sessions of all users.

The following information is provided to the user on the list:

- User: the name of the user who created the session.
- Address: the network address from where the request to create a session came.
- Device name: the name of the device from where the request to create a session came.
- Last active: the date and time of the user's last activity within a specific session.
- Status: status of the session. The available options are:
 - Closed: the session is closed.
 - Active: another user's active session.
 - Current: the current user's active session.

By selecting the action "Logout", the logged-on user can close the current session, while the user with permission (administrator) can close the active session of another user.

To make searching for attributes on a list easier, the user with permission can use the browser. By entering at least two characters of the search string, the user narrows the scope of the search results displayed on the list.

IMiS/Archive 10.1

Alex Nelson Edit

Details **Security** Settings Search History

Password Change password

Session History

Search Show closed 2 result

User	Address	Device name	Last active	Status	
Alex Nelson (anelson)	192.168.100.50	Edge on Windows 10	21. Sep 2020, 07:24	CURRENT	Logout
Alex Nelson (anelson)	192.168.100.50	Chrome on Windows 10	21. Sep 2020, 07:17	ACTIVE	Logout

Image 65: Showing the list of user sessions

4.2.5.1.3 The Settings tab

The “Settings” tab is used to manage the view of entities and set the parameters for connecting to the IMiS®/wScan scanning module.

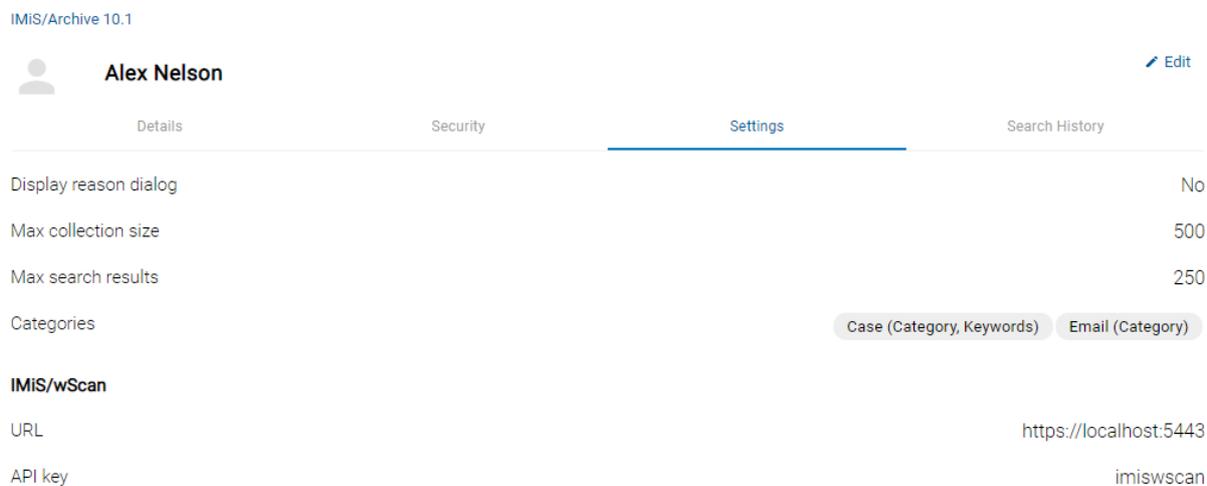


Image 66: View of the “Settings” tab

Under the settings of the view of entities, the logged-on user can set the following attribute parameters and values:

- Display reason dialog
By checking the parameter, the user enables the display of the dialog box for entering the reason for performing the action.

The dialog box shows an additional field for the user to (optionally) enter the reason before performing any of the following actions:

- Creating an entity (dialog box, input field).
- Modifying a template (dialog box).
- Opening an entity (dialog box).
- Editing an entity (dialog box).
- Creating a new version of the entity (dialog box, input field).
- Adding an entity to the queue for indexing or conversion (dialog box).

The user can disable the entry of the reason when first entering the reason for performing the action. The setting applies to any subsequent execution of the above-mentioned actions.



The dialog box titled "Entity create" has a close button (X) in the top right corner. It contains two "Reason" labels, each followed by a text input field. The first input field contains the text "Reason to create an entity". The second "Reason" label is followed by a checked checkbox and the text "Display reason dialog". At the bottom right, there are two buttons: "NEXT" and "CANCEL".

Image 67: Dialog box for disabling the entry of the reason for performing actions

- Max collection size

By defining the attribute value, the user limits the number of entities shown on the list. The default value is defined in the settings (assets/settings.json).

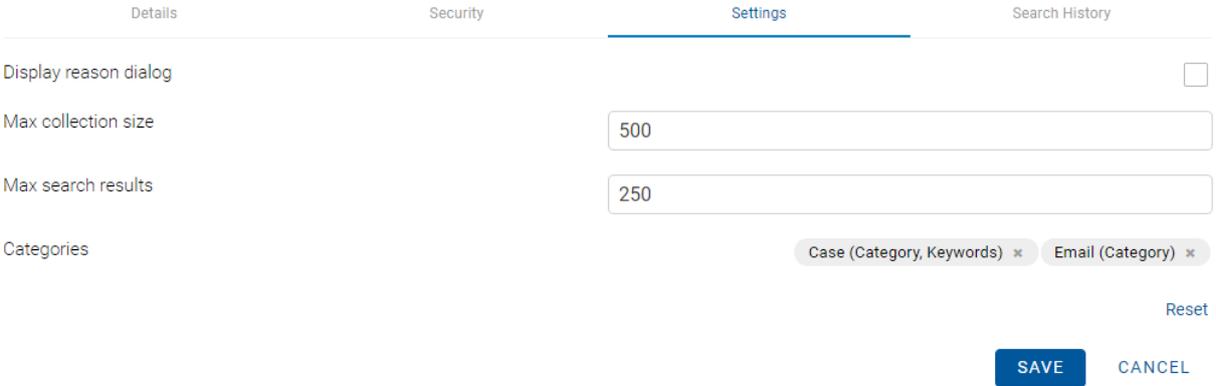
- Max search results

By defining the attribute value, the user limits the number of entity search results shown on the list. The default value is defined in the settings (assets/settings.json).

- Categories

If the user selects a categorized Keywords view (sys:Keywords or sys:Category) in the entity view mode, the categorization settings are saved for the template under which the categorization was performed.

For more information on categorized views see chapter [View mode](#).



The settings page has four tabs: "Details", "Security", "Settings" (active), and "Search History". Under the "Settings" tab, there are four rows of settings:

- "Display reason dialog" with an unchecked checkbox.
- "Max collection size" with a text input field containing "500".
- "Max search results" with a text input field containing "250".
- "Categories" with two category tags: "Case (Category, Keywords) x" and "Email (Category) x".

At the bottom right, there is a "Reset" link, a "SAVE" button, and a "CANCEL" button.

Image 68: Showing the basic settings

The action "Reset" enables the user to restore the original status and set the default value.

IMiS®/wScan

While defining the parameters for connecting the IMiS®/wClient web client with the IMiS®/wScan scanning module, the user can set the following attribute values:

- URL: Address of the IMiS®/Storage Connector Services REST
- API key: Security key preventing unauthorized use of the API.

IMiS/wScan

URL

API key

Reset

SAVE CANCEL

Image 69: Setting the parameters in the “IMiS®/wScan” tab

The action “Reset” enables the user to restore the original status and set the default value.

Note: Before capturing scanned documents, the settings of the service address (URL) and the security key (API key) must be coordinated with the settings of the IMiS®/Capture Service in the “Security” tab.

4.2.5.1.4 The Search history tab

The “Search history” tab is used to view the last searches performed by the logged-on user.

IMiS/Archive 10.1

Administrator [Edit](#)

Details Security Settings **Search History**

Clear all

content:customs* manufacturing*	3. Jul 2020, 11:59	Remove
title:despatch* content:shipping*	2. Jul 2020, 10:05	Remove
owner:kclay manufacturing	2. Jul 2020, 09:32	Remove
title:sun* owner:marko maxDepth:2	5. Jun 2020, 08:00	Remove
raw:[sys:Status]=2	4. Jun 2020, 12:30	Remove

Image 70: View of the “Search history” tab

The user can remove the search result record by selecting the action “Remove”.

4.2.5.2 Information about audit log events

By selecting the command “Activity”, the user is shown information about audit log events for the selected user and entity. More information on the Activity action is available to the user in the chapter [Searching audit log events](#).

Note: The user leaves the view of information on audit log events by selecting the name of the application IMiS®/wClient or archive (e.g. IMiS/ARChive 10.1).

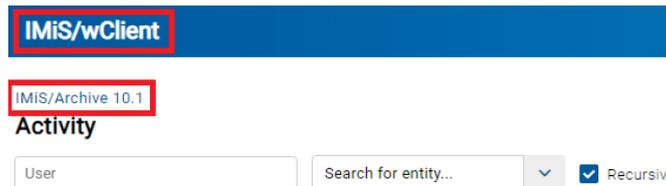


Image 71: Transition from profile settings to the entity review in the archive

4.2.5.3 Reports

The IMiS®/wClient enables users with a Reports role on the server to create reports on the IMiS®/ARChive Server. Logged-on user can create report on folders, documents, document contents, retention, reviews, user access, entities, classification scheme

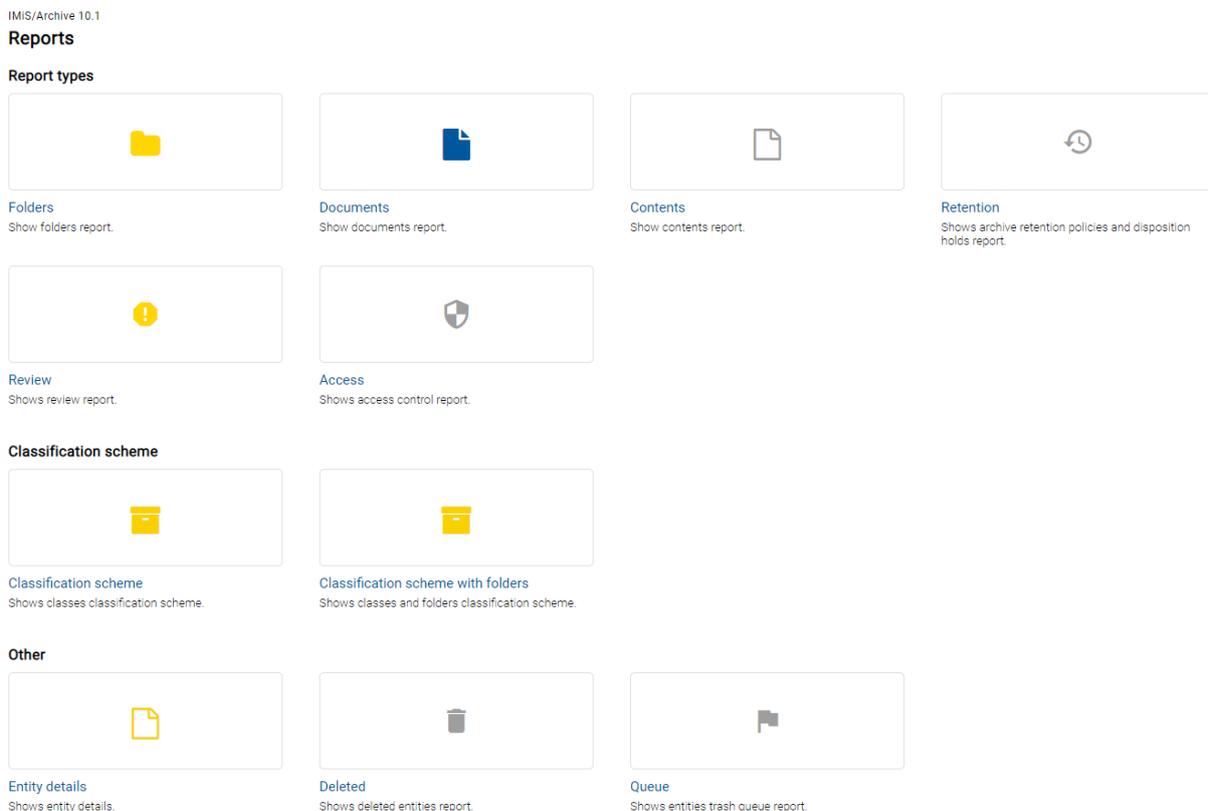


Image 72: Report types

For more information on specific report see chapter [Reporting](#).

4.2.5.4 Logout

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](#).

4.2.5.5 About

By selecting the “About” command, the user is shown information about the application and licensing terms. More information on the About command is available to the user in the chapter [About](#).

4.2.5.6 Display of entities

By selecting the icon  to the right of the command bar, the user can define the display mode for the list of entities.

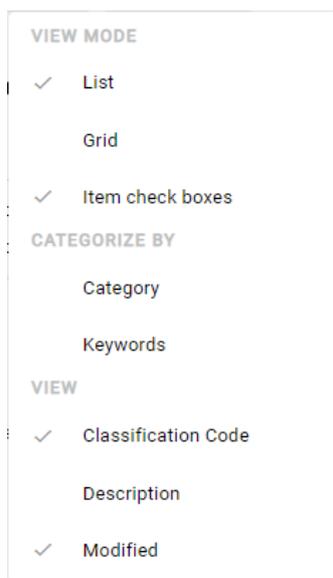


Image 73: Setting the display of entities

4.2.5.6.1 View mode

In the View mode, the user defines how the entities are displayed in the central view and marks entities for performing actions. The available options are:

- List
- Grid
- Item check boxes.

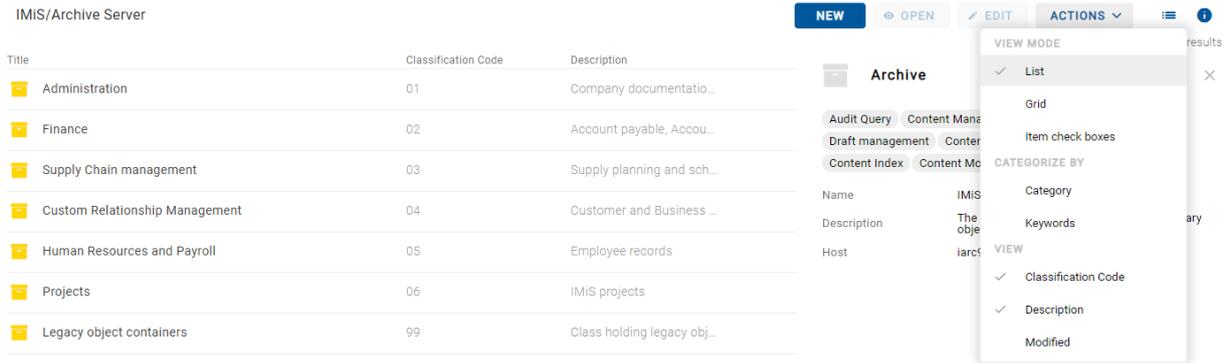


Image 74: Entities shown on a list



Image 75: Entities shown in a grid

By selecting the option Item check boxes in the menu, the user can mark the individual entities which will be moved or deleted in the next step. The user can also do that by holding down the Ctrl key on the keyboard and selecting the entity, or by selecting the entity and pressing the Space key.

The command bar displays the number of entities selected (X Items Selected).

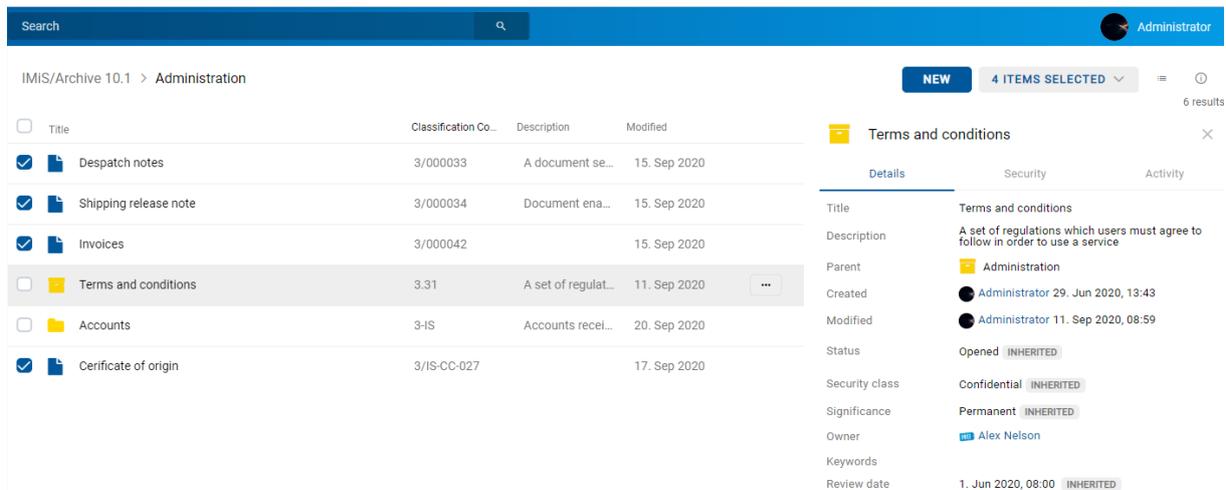


Image 76: Selecting individual entities for move and deletion

The user can select all the displayed entities at once. The user does that by checking the checkbox left of the “Title” column.

By doing so, the user selects all the loaded entities, but not the entire collection.

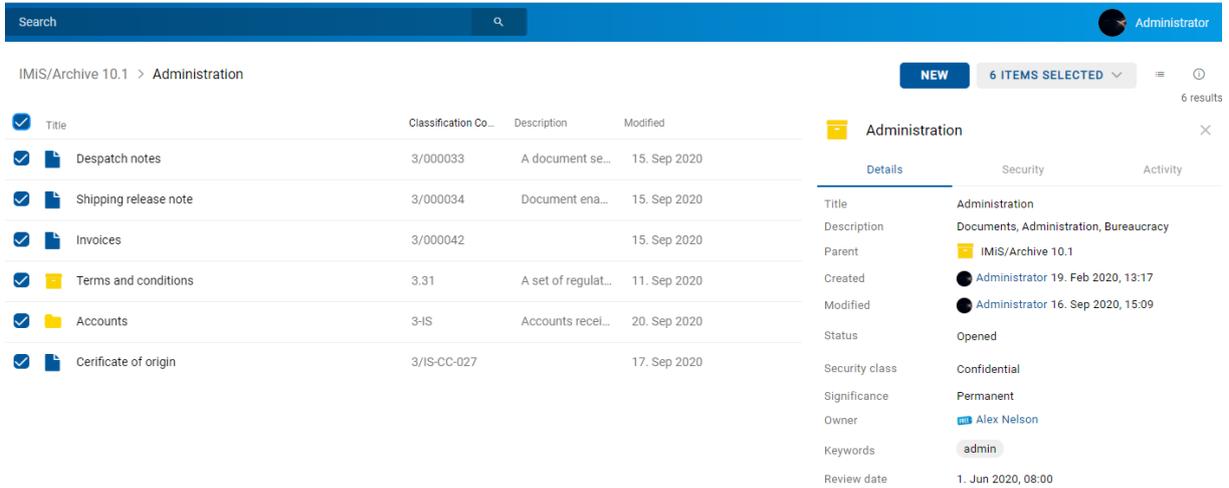


Image 77: Selecting all the loaded entities for move or deletion

The user can select only a part of the displayed entities. The user does that by first selecting the entity from the list. The user then selects another entity by simultaneously holding down the Shift key on the keyboard.

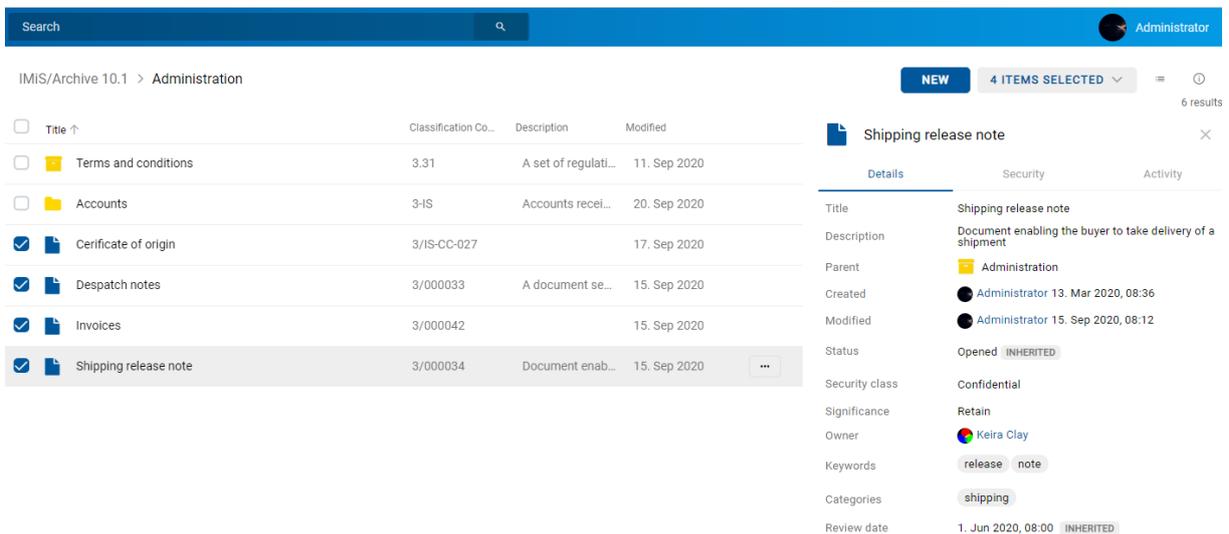


Image 78: Selecting a part of the loaded entities for move or deletion

By selecting the arrow next to the number of entities selected, a menu opens with the following options:

- Move
- Delete
- Deselect all.

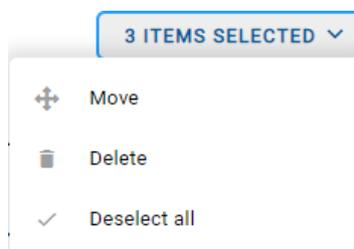


Image 79: Set of actions on selected entities

The procedure of moving multiple entities is the same as the procedure of moving a single entity. For more information see chapter [Entity move](#).

Likewise, the procedure of deleting multiple entities is the same as the procedure of deleting a single entity. For more information see chapter [Deletion of an entity](#).

4.2.5.6.2 Categorization

In the Categorize by set the user defines how the entities are classified in the central view. Categorization enables a view of entities belonging to the same category at the same hierarchical level.

Two categorization options are available:

- Category
- Keywords.

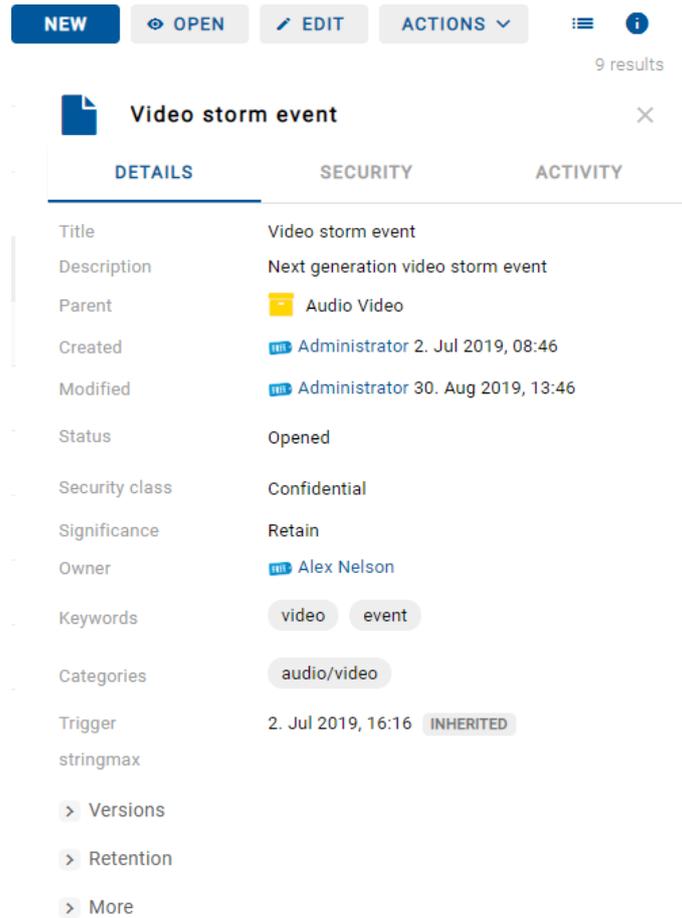


Image 80: An example of an entity with a defined value of the Categories attribute

If the value of the Categories attribute has been defined, the central view shows the user a list of entities classified into the same category at a specific hierarchical level.

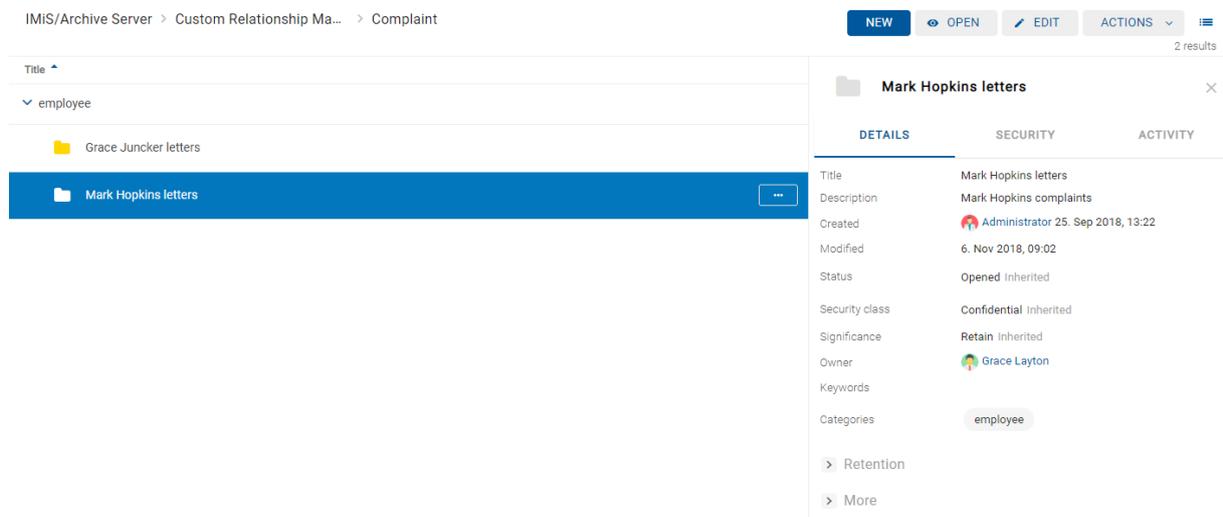


Image 81: A categorized Categories view

If the value of the Keywords attribute has been defined, the central view shows the user a list of entities with the same keyword at a specific hierarchical level.

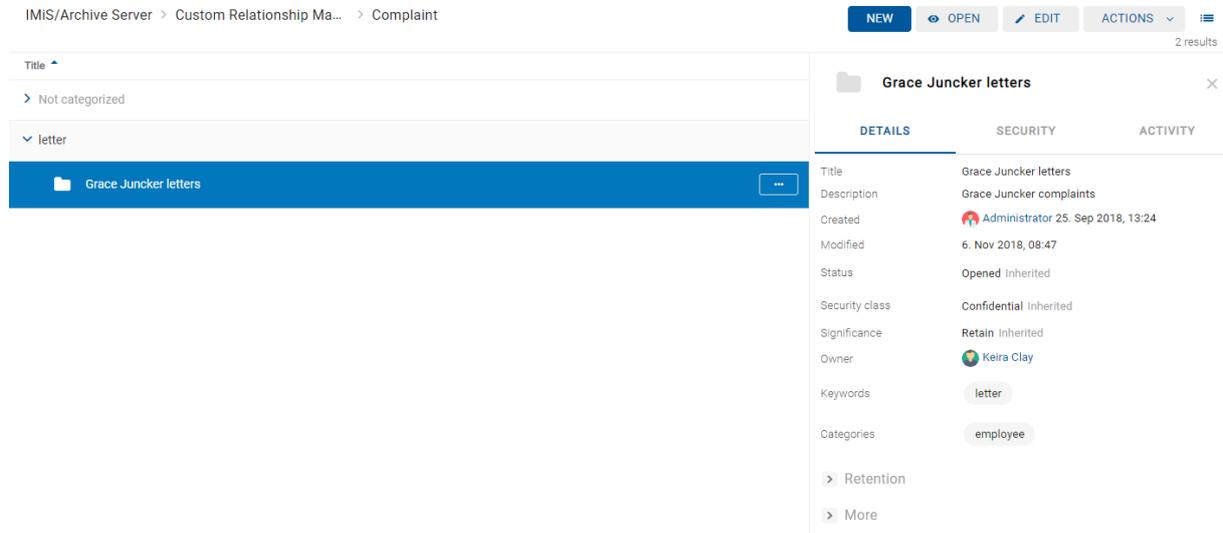


Image 82: A categorized Keywords view

4.2.5.6.3 View

In the View set the user defines which columns of the selected attributes will be displayed in the central view. The user can add or remove the following columns of the selected attributes:

- Classification code
- Description
- Modified.

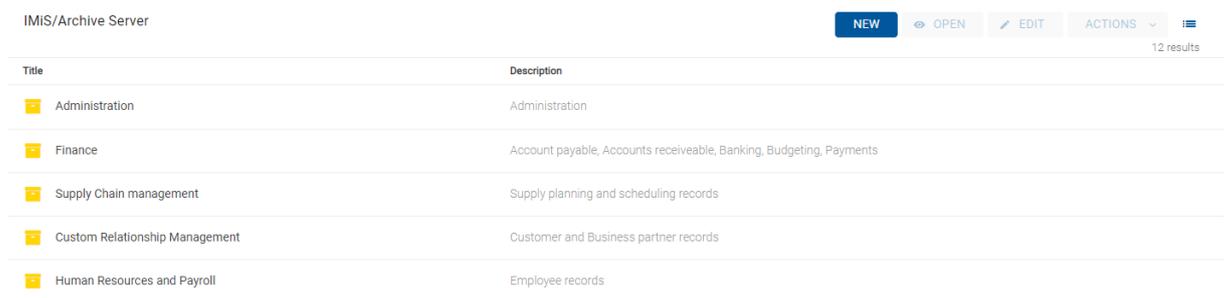


Image 83: Display of the columns of the selected attributes of Title and Description

4.2.6 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](#).

4.3 Actions

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

- [Entity access](#)
- [Creating an entity](#)
- [Editing entity data](#)
- [Entity move](#)
- [Content management](#)
- [Versioning](#)
- [Search functions](#)
- [Archiving email messages](#)
- [Acquiring authenticity evidence](#)
- [Import](#)
- [Export](#)
- [Deleting an entity](#).

4.3.1 Entity access

Access to the entity in the classification scheme depends on the:

- Security class of the entities.
- User's security class level.
- User's access right.

4.3.1.1 Security class of the entities

This setting in the entity details specifies the set of available entity security classes based on the entity's position in the classification scheme.

For more information on security classes see chapter [Access](#) in the [IMiS®/ARChive Server user manual](#). Changing the security class of the entities is described in greater detail in the chapter [Changing the security class](#).

4.3.1.2 User's security class level

In the settings of the IMiS®/wAdmin administration web interface in the »Directory« folder, the user with permission specifies the »Security class level«.

This setting specifies the security class level of the content which the user is allowed to review. The user can review only the content whose security level is lower than or equal to the user's.

4.3.1.3 User's access right

In the settings of the IMiS®/wAdmin administration web interface in the Access control folder, the user with permission specifies the access permissions for each directory entity, which applies to a specific archive volume.

Under the settings, the user also specifies whether the permissions are inherited by the contained entities (Propagated) and whether the user can log in on behalf of a delegated user (Delegate context).

For more information on access rights see chapter [The Security tab](#).

When logging into the selected archive, the root classes of the archive to which the user has the Read 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.

By selecting a root class, the tabs in the right view, where the entity information is located, 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 root classes and sub-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.

Documents 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.

The user has the option of modifying the template when editing an entity. By selecting the field with the values of the attribute Template, the list shows the available templates of the same type.

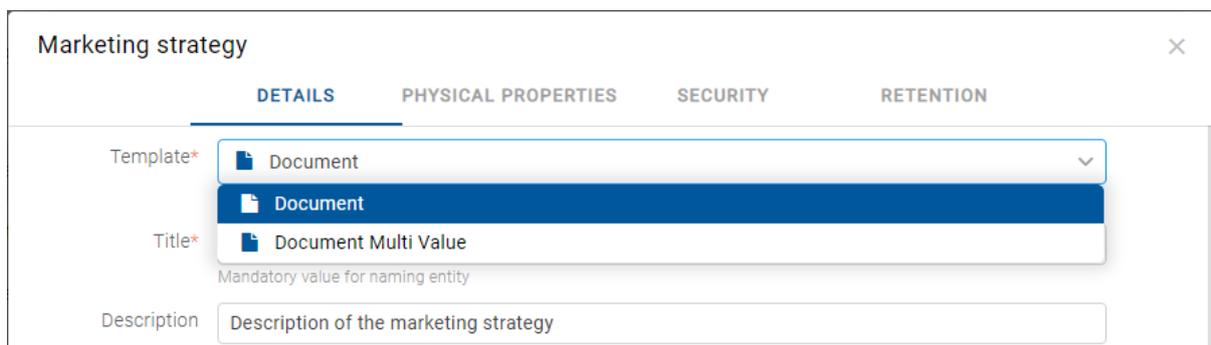


Image 84: Modifying a template in editing mode

For more information on templates see chapter [Templates](#) in the [IMiS®/ARChive Server Manual](#).

4.3.2.1 Creating a new entity

Besides the Create entities permission, the user has to have the Change retention permission to create new entities.

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, selecting the relevant template from the list, entering the values of attributes, defining the retention policy and confirming Create.

The screenshot shows the 'Create Class' dialog box with the following fields and values:

- Parent: IMIS/Archive 10.1
- Template*: Class
- Title*: Manufacturing
- Description: Manufacturing documents
- Status: INHERITED
- Security class: INHERITED
- Significance: Vital
- Owner: Alex Nelson
- Keywords: production, products, industry
- External Identifiers: manufacturing
- Review date: 01.09.2010 10:24
- Classification Code: Manual (optional)

Buttons at the bottom: Create another, **Create**, Cancel

Image 85: Creating a root class

4.3.2.1.2 Creating subentity

In the classification scheme in the left view or in the entities list in the 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 and selecting the relevant template from the list, same as when creating a root class.

IMiS/Archive 10.1 > Administration

Title ↑	Classification Co...	Description	Modified
Terms and conditions	3.31	A set of regulat...	11. Sep 2020
Accounts	3-IS	Accounts recei...	20. Sep 2020
Certificate of origin	3/IS-CC-027		17. Sep 2020
Despatch notes	3/000033	A document se...	15. Sep 2020
Invoices	3/000042		15. Sep 2020
Shipping release note	3/000034	Document ena...	15. Sep 2020

NEW OPEN EDIT ACTIONS

- Class
- Folder
- Document
- E-mail
- Document01
- Custom document
- Autonomous Custom Email

Status: **Opened** ✓

Security class: Confidential

Significance: Permanent

Owner: Alex Nelson

Keywords: admin

Review date: 1. Jun 2020, 08:00

Image 86: Display of contained entities.

The user is shown a dialog box with the relevant tabs and set of attributes based on the selected template. In the Details tab the following attributes are available to the user:

- 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.
- Title: name of the entity. The attribute value is mandatory.
- Classification code: the classification code of the created entity in the classification scheme.
- 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.
- Owner: a directory entity (user or group) entity that is responsible for the selected entity (owner).

***Note:** The user can search by the text entered in the search box and select a directory entity in the popup menu below the text. The search is performed if at least 2 characters have been entered. Only the directory entities matching the search criteria will be displayed (5 at the most). The user can select them using the keys ↑ and ↓ and confirm the selection by clicking on the selected entity in the popup menu below or by using the key Enter ↵.*

- Keywords: entity-related keywords. This attribute can have multiple values.
- Categories: the entity view mode.
- Content: document contents. This attribute is available only for document-type entities.
- External identifiers: a list of the unique external identifier of the entity on the server.
- Classification code generated: the type of classification code entry for the contained entities of the parent class.
- Custom attributes: additional custom attributes. The selection of attributes depends on the selected template.

The user can specify whether the value of the custom attribute is inherited from a parent entity. By checking the box of the custom attribute »Inherited« and saving the entity (Save), the value(s) is (are) transferred from the parent entity.

Image 87: Display of creating a new document

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 order of attributes on the list is defined by the order of the template attributes.

The following can be edited in the web administration interface IMiS®/wAdmin.

For more information see chapter [The Template folder in the IMiS®/ARCHive Server Manual](#).

Required attributes are marked with an asterisk and must be entered before saving.

Title*
Mandatory value for naming entity

Image 88: Entry of required metadata

Attribute entry fields are as follows:

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

Description

Image 89: Entry of text metadata

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

Status	< June 2020 >
Security class	Su Mo Tu We Th Fr Sa
Significance	31 1 2 3 4 5 6
Owner	7 8 9 10 11 12 13
Keywords	14 15 16 17 18 19 20
Categories	21 22 23 24 25 26 27
External Identifiers	28 29 30 1 2 3 4
	^ 08 : 00 ^
	Today Clear
Review date	<input type="text" value="01.06.2020 08:00"/> <input type="button" value="📅"/>
	<input type="checkbox"/> Inherited
	<small>The review date log</small>

Image 90: Entry of date and time metadata

In the event of a contained entity, the user is shown the inherited value in the date field. By unchecking the default setting »Inherited«, the user can enter the date or select it from the popup window for setting the date and time.

Review date 01.06.2020 08:00

Inherited
The review date log

Image 91: Displaying the inherited value of the date field of the parent entity

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

Significance Retain

Owner INHERITED

Keywords None
Vital

Categories Permanent

External Identifiers Retain
Custom external entity identifiers

Image 92: Entry of metadata with predefined values

- A field for entering multiple desired text values, separated by using the Enter 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.

Keywords document note letter company

Important words used in entity

Image 93: Entry of multiple values into a field

- A field for selecting multiple values of an attribute. This feature is supported in the following types of attributes: Binary, Boolean, Decimal, Double, Int, Date, Date time, Time and Picklist. For each attribute, the user has the option of adding values with the icon » + « or removing them with the icon » - «.

The screenshot shows the 'Create Document' dialog box with the following details:

- Owner:** Alex Nelson
- Keywords:** office, documents, phonecalls
- Categories:** administration
- Content:** Certificate.tif (36.9 kB)
- Custom Content:** Company Overview.pdf (86.5 kB)
- External Identifiers:** 5623
- Binary:** mib.bin, efsys.bin, bootfix.bin
- Date Time:** 20.09.2050 12:58

At the bottom right, there is a checkbox for 'Create another', a 'Create' button, and a 'Cancel' button.

Image 94: Entering multiple values of an attribute

- A field for selecting multiple values of a directory entity. This feature is supported in the attribute type Directory entity. By entering the text value into the field, the user limits the set of the searched directory entities. For each directory entity, the user has the option of adding with the icon » + « or removing with the icon » - «.

The screenshot shows a 'Create Document' dialog box with a 'DETAILS' tab selected. The dialog is divided into several sections:

- Editors:** A list of five users: Alex Nelson, Jerry Turner, John Smith, Keira Clay, and Marco Welch. Each user has a minus sign (-) or plus sign (+) to the right of their name.
- binary:** A list of four PDF files: PDF #1.PDF, PDF #2.PDF, PDF #3.PDF, and PDF #4.PDF. Each file has a minus sign (-) or plus sign (+) to the right of its name.
- bool:** A checkbox with a minus sign (-) and a plus sign (+) to its right.
- double:** A text input field with a plus sign (+) to its right.
- attr:label:** A text input field with a plus sign (+) to its right.
- time:** A text input field with a calendar icon and a plus sign (+) to its right.
- attr:uint64:** A text input field with a plus sign (+) to its right.
- Reason:** A text input field.

At the bottom right of the dialog, there are two buttons: 'CREATE' and 'CANCEL'.

Image 95: Entering the values of multiple directory entities

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 or folder.

In the preview or open mode, the information about the classification code of an existing entity is in the Details tab in the set More.

In the editing mode, the drop-down list of the field Child classification code generation allows the user to set the entry type for the selected class or folder:

- Automatic: Entity numbering is automatic. The classification code of child entity is 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: Entity numbering is manual. The classification code of child class or folder entity must be entered manually by the user. This classification code may be any combination of letters and numbers, providing it is unique inside the entire parent class.
- »Manual (Optional)«: Entity numbering is flexible.

If the user manually sets the classification code, the server first checks whether the code is duplicate. If it is, it rejects it with an error. If the user does not manually set the classification code, the server assigns it automatically.



Image 96: Selecting the type of classification code entry for the contained entity

In the event of a manual entry of the classification code, the user only enters the relative (own) 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.

Example: (see below) Inside a class with the classification code 03.04, the user creates a new folder for which user manually input IS-EXP-1000 as the relative part of the classification code. When the folder is saved to the IMiS®/ARChive Server, its full classification code will be 03.04.IS-EXP-1000.

Image 97: Manual entry of a child entity's classification code

IMiS/Archive 10.1 > Administration

Title	Classification Co...	Description	Modified ↓
Export	3/IS-EXP-1000	Export docume...	21. Sep 2020

Image 98: Display of manually entered classification code

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 99: Specifying the security class of a new entity

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

- **Inherited:** The security class is implicitly inherited from the parent entity. In case of root classes, the inherited security class value is empty.
- **Unspecified:** Access to this entity is not specified.
- **Restricted:** The entity is an internal matter. It may only be accessed by users with a clearance level Restricted or higher.
- **Confidential:** The entity is considered confidential. It may only be accessed by users with a clearance level Confidential or higher.
- **Secret:** The entity is considered secret. It may only be accessed by users with a clearance level Secret or higher.
- **Top Secret:** The entity is considered top secret. It may only be accessed by users with a Top Secret clearance level.

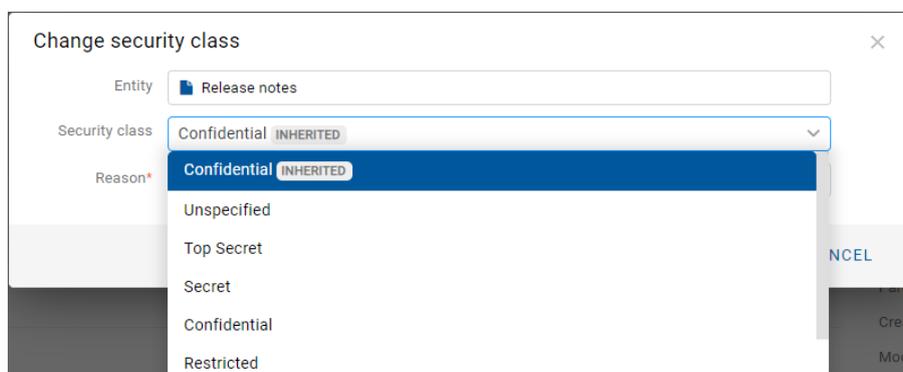


Image 100: Entity information after entering the security class

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.

The user can choose from predefined values for the status of an entity:

- **Inherited:** the status of the entity is implicitly inherited from the parent entity. In the case of root classes, it matches the status Opened.
- **Opened:** the status of the entity changes explicitly to Opened.
- **Closed:** the status of the entity changes explicitly to Closed.

The screenshot shows the 'Create Document' dialog box with the following details:

- Parent:** wClient project
- Template*:** Document (Standalone document entity)
- Title*:** Development strategy (Mandatory value for naming entity)
- Description:** Total transformation through a right-the-time approach
- Status:** Opened INHERITED
- Security class:** Opened INHERITED
- Significance:** Opened, Closed
- Owner:** Alex Nelson
- Keywords:** development, strategy (Important words used in entity)
- Categories:** development
- Content:** Drag and drop files or click
- External Identifiers:** Custom external entity identifiers

Buttons: CREATE, CANCEL

Image 101: Specifying the status of a new entity

4.3.2.6 Entry of physical content metadata

In the case of a document- or folder-type entity, information about the physical content is also available to the user in addition to the above-mentioned information when in open or edit mode.

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 is possible upon capture/import, or later when the content is already stored in electronic form.

By selecting the Physical Content tab in the editing mode, a list of attributes, referring to the description of physical content, appears.

The screenshot shows a 'Create Document' window with a close button (X) in the top right. The window has four tabs: 'DETAILS', 'PHYSICAL PROPERTIES' (which is selected and underlined), 'SECURITY', and 'RETENTION'. Below the tabs are several input fields:

- Identifier: ID534
- Description: Building 4, Floor 2nd, Room 5, Cabinet 2, Shelf 1
- Status: CheckedOut (with a dropdown arrow)
- Home location: Brodway street 1070, Manhattan, New York
- Current location: Denver street 500, Denver, Colorado
- Custodian: John Cusac
- Return due: 31.12.2019 (with a calendar icon)

Image 102: 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](#).

The screenshot shows a 'Status' dropdown menu with 'CheckedOut' selected. Below the dropdown, the text 'Status change 19. Sep 2019, 09:06' is displayed.

Image 103: The date of the last change of the Status attribute

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.

Only a user with the Change retention permission can add retention and disposition hold periods. The user adds retention and disposition hold periods by selecting the command Add 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.

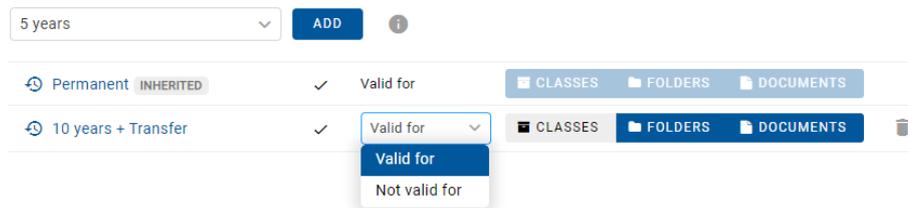


Image 104: Selecting validity for a specific type of entity

After creating an entity, the effective retention periods are ticked in front of the information about the validity of individual types of entities.

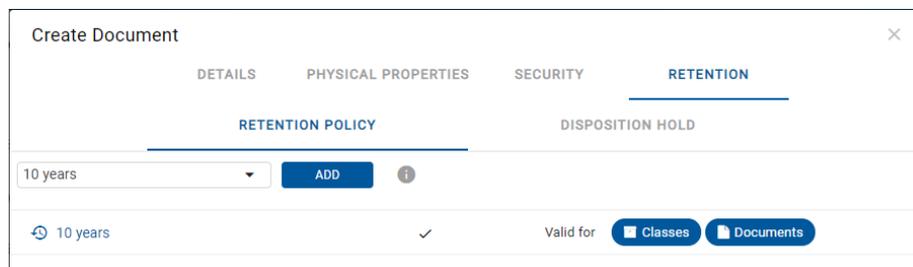


Image 105: Display of the »Retention« tab

4.3.2.8 Saving an entity

Before saving an entity, 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 Create command in the bottom part of the dialog window.

Image 106: 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.

Classification Code 13/IS-EXP-500

Image 107: 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.

Owner

 Ron Salazar

Image 108: Example creator of entity

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

Created

 Keira Clay 27. Sep 2018, 14:49

Image 109: 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.

Modified

27. Sep 2018, 14:49

Image 110: 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.

Accessed

27. Sep 2018, 14:49

Image 111: Example date and time of last access to the entity

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

Opened

27. Sep 2018, 14:49

Image 112: Example date and time an entity was opened

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

Closed 27. Sep 2018, 15:01

Image 113: Example date and time an entity was closed

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

Identifier Jjgoyu4LBNJkT0HSu9aMalwQt-IYIuzH

Image 114: 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.

A dialog box opens with the attributes and their values.

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 attribute values.

The selection of attributes is defined by the selected template.

For more information on the set of editing metadata see chapter [Creating subentity](#).

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](#).

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.

Image 115: Editing of the 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.

Image 116: Popup menu for selecting the status of the physical content

4.3.3.4 Editing access rights

The user with the Change permissions permission can edit the access control list (ACL) for the entity or a selected metadata for a directory entity (user, group, attribute of directory entity type). The list shows only those directory entities 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.

4.3.3.4.1 Editing access rights for an entity

By selecting the Edit button in the command bar, a dialog box opens showing effective permissions on the entity for the selected directory entity or the given directory entity contained in the mentioned attribute of the directory entity type.

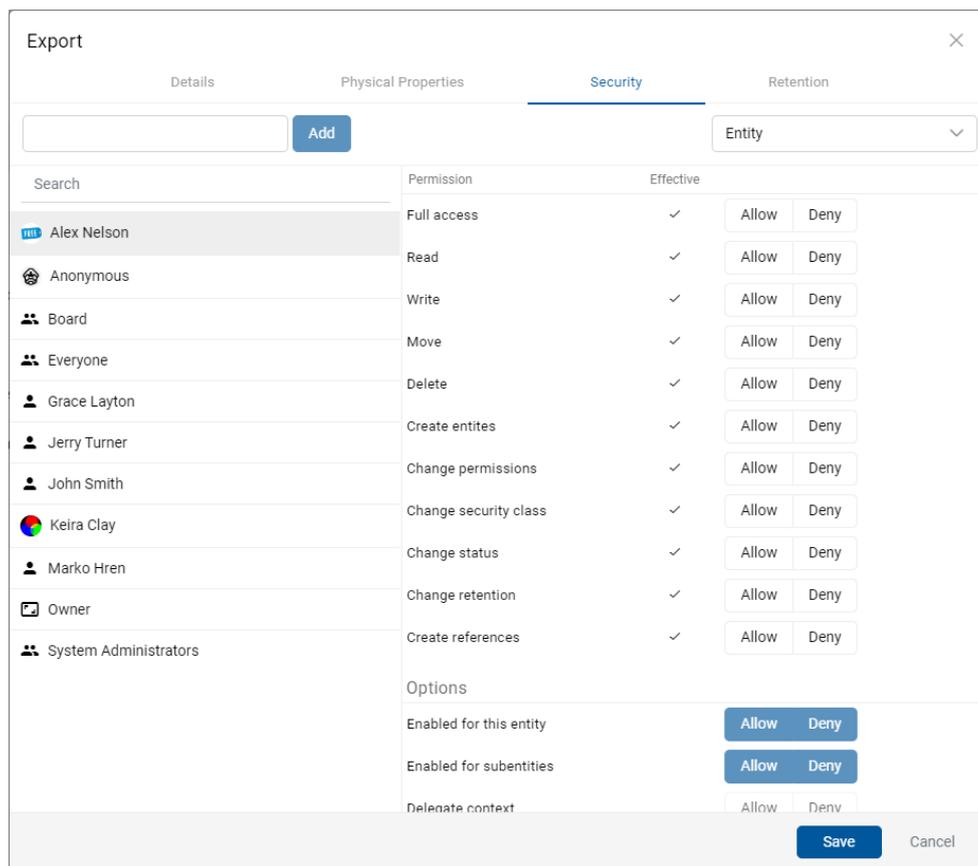


Image 117: Security tab in editing mode

The left part of the view contains a list of directory entities with access rights to the entity. In the event of a greater number of directory entities, search is enabled via a search box.

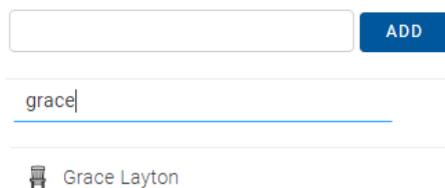


Image 118: Searching a directory entity on a list

If a specific group, user or an attribute of directory entity type, 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.

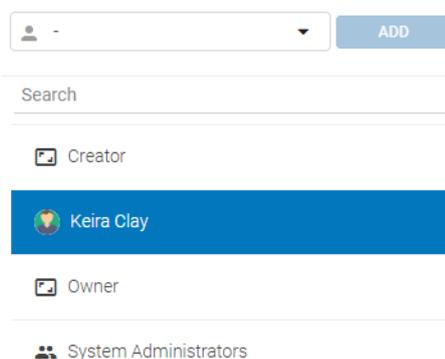


Image 119: List of directory entities with access rights to the entity

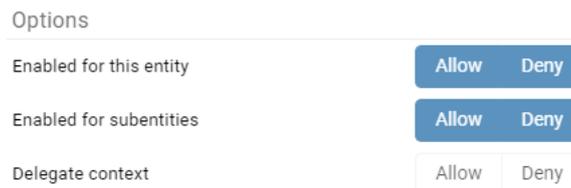
In the right part of the view a list of entity editing permissions is shown in the section Permissions, for the selected directory entity or an attribute of directory entity type.

The Effective column shows the current state of effective permissions for the selected group or user over the entity.

To the right of the column Effective permissions, the user selects Allow to add an explicit permission, or Deny to revoke a permission. The user can specify explicit permissions for any registered directory entity or an attribute of directory entity type.

In the section Options with a tick the user enables the options for access permissions in the context of Allow or Deny:

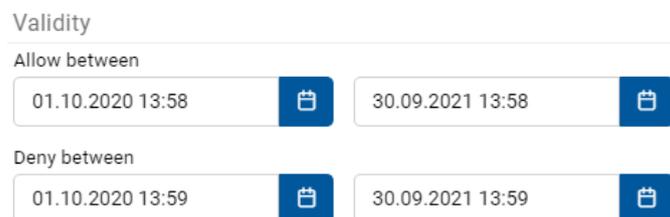
- Enabled for this entity: the permissions are enabled on the current entity.
- Enabled for subentities: enables the inheritance of permissions on contained entities.
- Delegate context: the access permissions apply to the user who will log in on behalf of a delegated user.



Options	
Enabled for this entity	Allow Deny
Enabled for subentities	Allow Deny
Delegate context	Allow Deny

Image 120: Setting the inheritance of access permissions to contained entities

In the section Validity the user sets a time limit on the validity of entity access permissions for the selected directory entity or for the given directory entity contained in the mentioned attribute of the directory entity type. The user does so by setting the temporal validity of access permissions (Valid from and Valid to) in the date field.



Validity	
Allow between	
01.10.2020 13:58	30.09.2021 13:58
Deny between	
01.10.2020 13:59	30.09.2021 13:59

Image 121: Setting the temporal validity of access permissions

In the case of the directory entity type attributes, the permission is effective for the respective value in the mentioned attribute in the context of the entity in question. Therefore, a permission does not have the same effect on all child entities, but rather sets the permission for all users and/or user groups mentioned in the value of the attribute to which the access permission refers. Permissions have no effect on system directory entities.

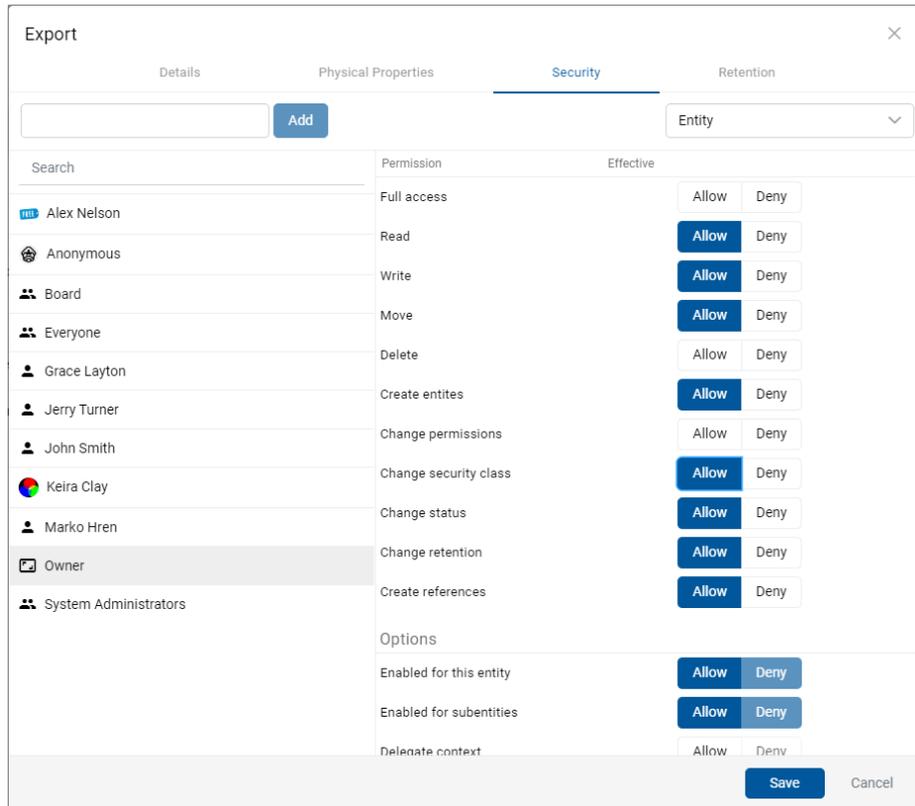


Image 122: A list of access permissions for a specific attribute

4.3.3.4.2 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.

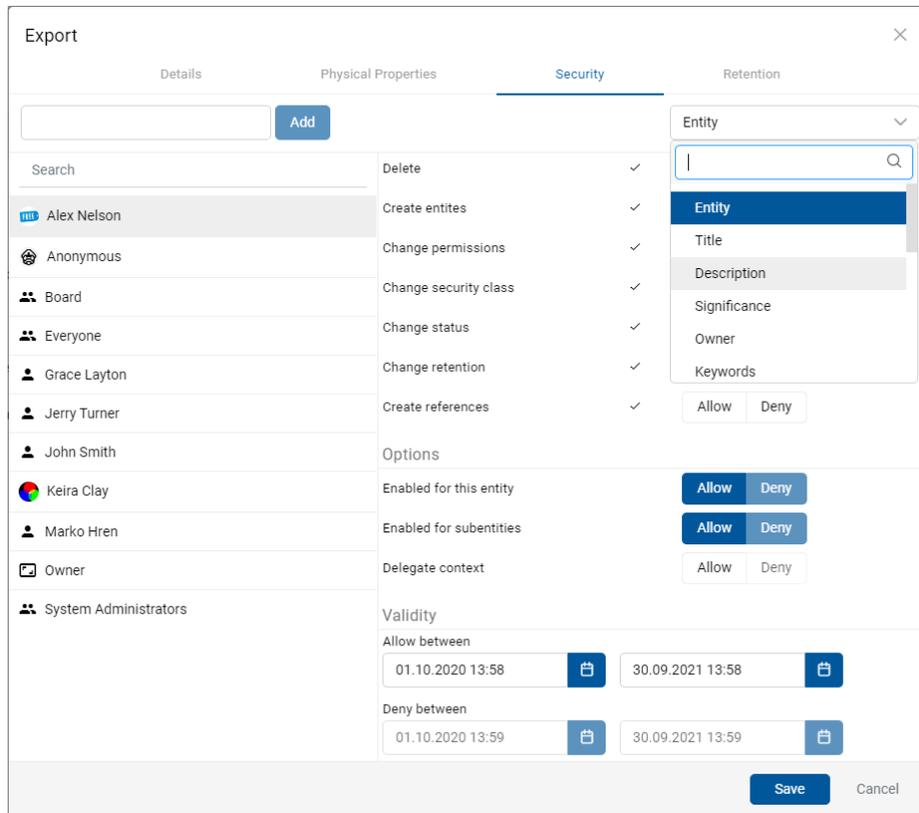


Image 123: Popup menu for selecting access rights to a selected metadata

The left part of the view contains a list of users with access rights to the selected metadata. User selects a directory entity to which it wants to grant access rights. In the event of a greater number of directory entities, search is enabled via a search box.

The user adds it to the list using the Add button.

In the right part of the view a list of metadata editing permissions is shown for the selected directory entity.

To the right of the column Effective permissions, the user selects Allow to add an explicit permission, or Deny to revoke a permission.

In the section Options with a tick the user enables the options for access permissions in the context of Allow or Deny:

- Enabled for this entity: the permissions are enabled on the current entity.
- Enabled for subentities: enables the inheritance of permissions on contained entities.
- Delegate context: the access permissions apply to the user who will log in on behalf of a delegated user.

In the section Validity the user sets a time limit on the validity of metadata access permissions for the selected directory entity or for the given directory entity contained in the mentioned attribute of the directory entity type. The user does so by setting the temporal validity of access permissions (Valid from and Valid to) in the date field.

The screenshot shows the 'Export' dialog box with the 'Security' tab selected. The user 'Alex Nelson' is selected, and the attribute 'Description' is chosen. The permissions are listed as follows:

Permission	Effective	Explicit
Full access	Allow	Deny
Read	Allow	Deny
Write	Allow	Deny
Create	Allow	Deny
Delete	Allow	Deny

Options:

Enabled for this entity	Allow	Deny
Enabled for subentities	Allow	Deny
Delegate context	Allow	Deny

Validity:

Allow between: Valid from [] Valid to []

Deny between: Valid from [] Valid to []

Buttons: Save, Cancel

Image 124: 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.

4.3.3.5 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.

A new window opens containing the tabs:

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

In the central 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.

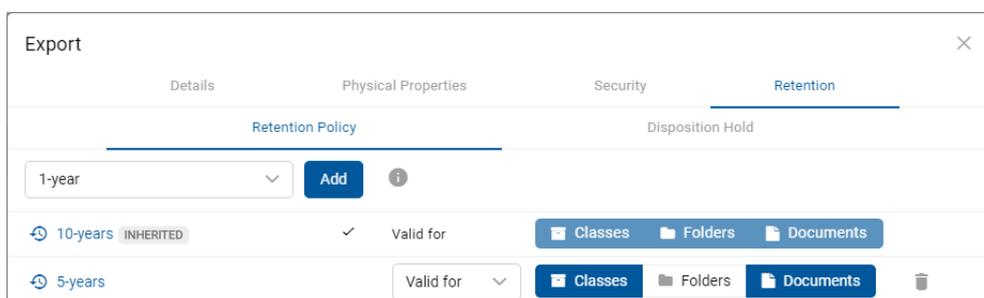


Image 125: The Retention policy tab in editing mode

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

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

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

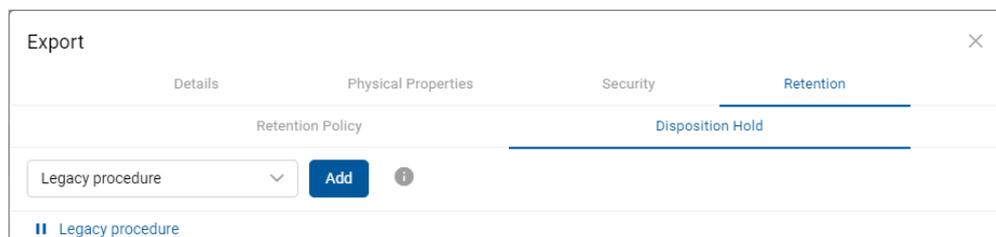


Image 126: The Disposition hold tab in editing mode

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 icon  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.

4.3.3.6 Changing the classification code of an entity

The user can change the relative entity classification code even after assigning the classification code on entity creation. The classification code can be changed only on entities where the classification code of their parent entity has been set to "Manual" or "Optional". For more information on setting the parent classification code see chapter [Entry of the classification code](#).

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

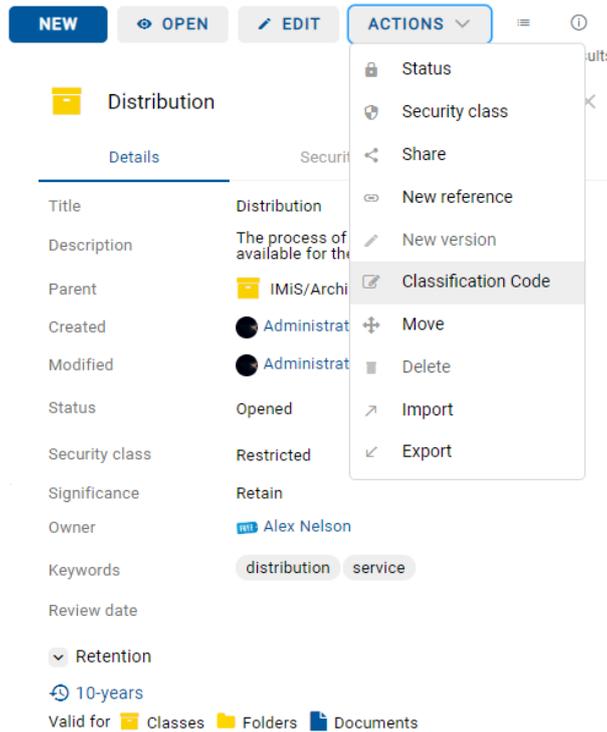


Image 127: Selecting the classification code

In the Change classification code dialog box in the Classification code field the user enters the new relative entity classification code.

The user writes a reason for the classification code change in the Reason to change field.

The change of classification code for the selected entity is confirmed using the Save button.



Image 128: Selecting the classification code and giving the reason for the change

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.

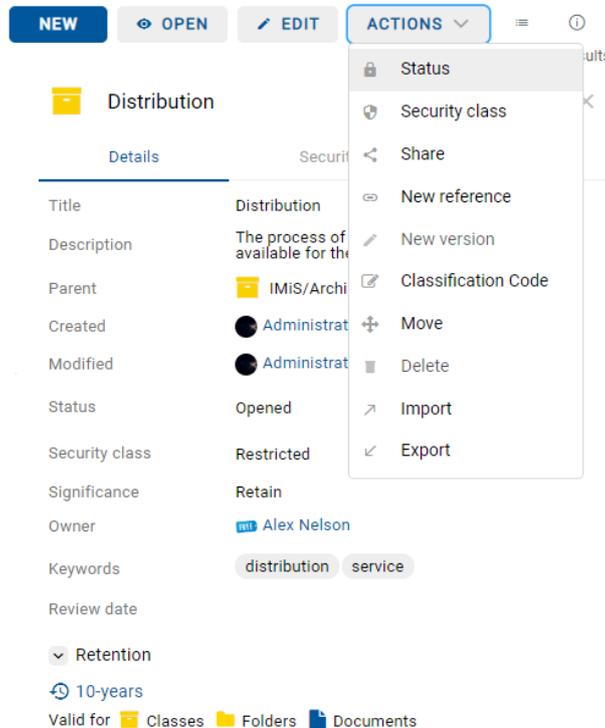


Image 129: The popup menu for selecting the Status command

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

For more information on the set of predefined values for the entity's status see chapter [Entering the status of an entity](#).

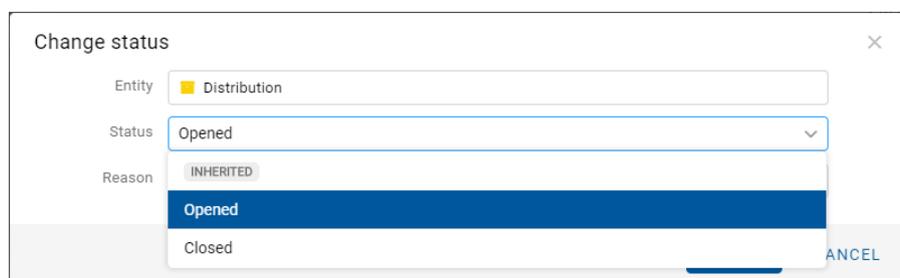


Image 130: Selecting the status

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 131: 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.

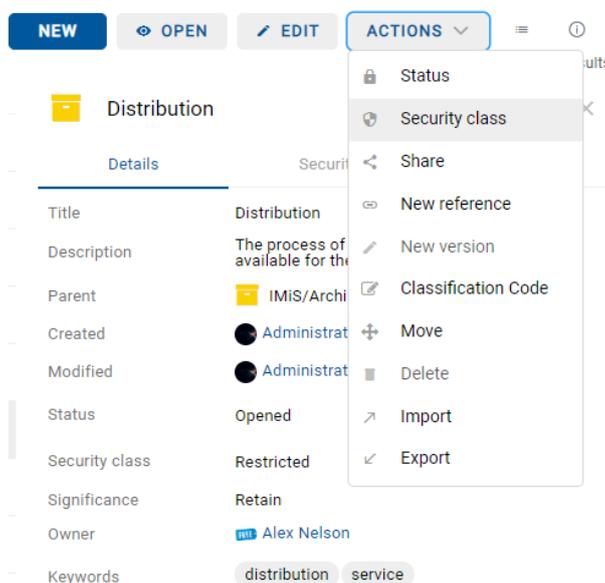


Image 132: The popup menu for selecting the Security class command

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

For more information on the set of predefined values for the entity's security class see chapter [Setting an entity's security class](#).

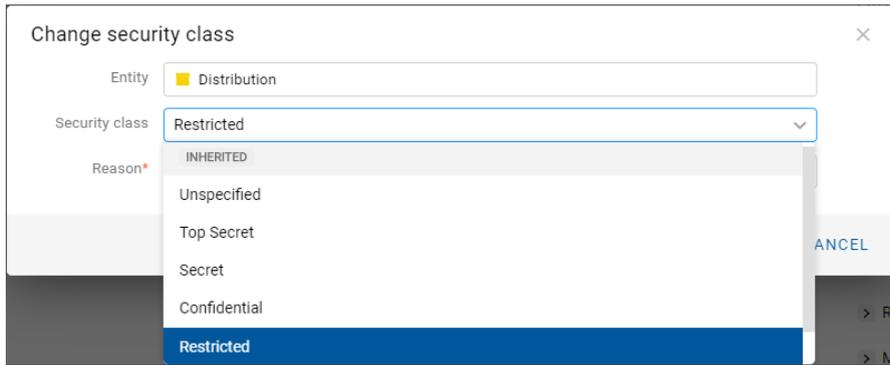


Image 133: Selecting the security class

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.

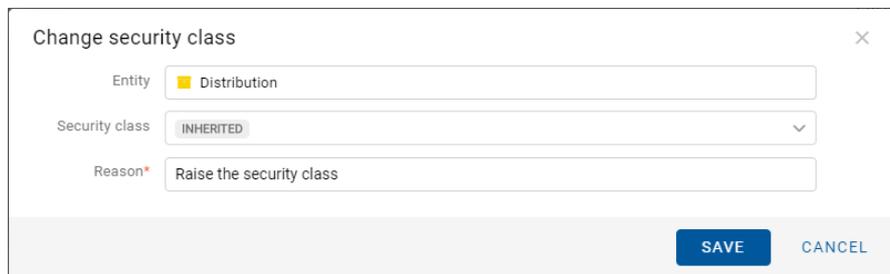


Image 134: Selecting the security class and giving the reason for the change

4.3.3.9 Sharing an entity

An entity can be shared by a user with the Read permission.

The user creates a copy of the link to the entity and saves it to the clipboard.

In open mode, the user selects the entity. By selecting the popup menu on the marked entity, the user selects the command Share.

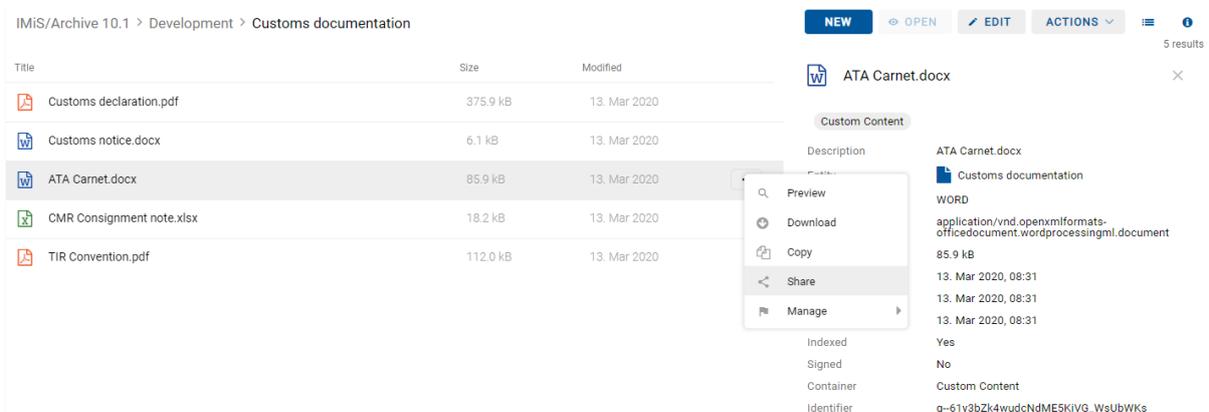


Image 135: Selecting the command Share in the popup menu

A dialog box opens containing the created link to the selected entity or content.

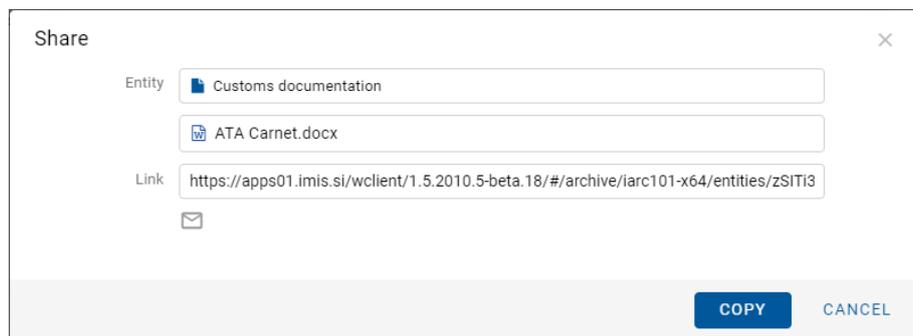


Image 136: Displaying the created link to the selected entity

By clicking on the field, the user can select the full text of the displayed link. Selecting the email icon opens a window for a new email message in the default application. The button Copy copies the link the same as using a right click and Copy over highlighted text or Ctrl+C over highlighted text.

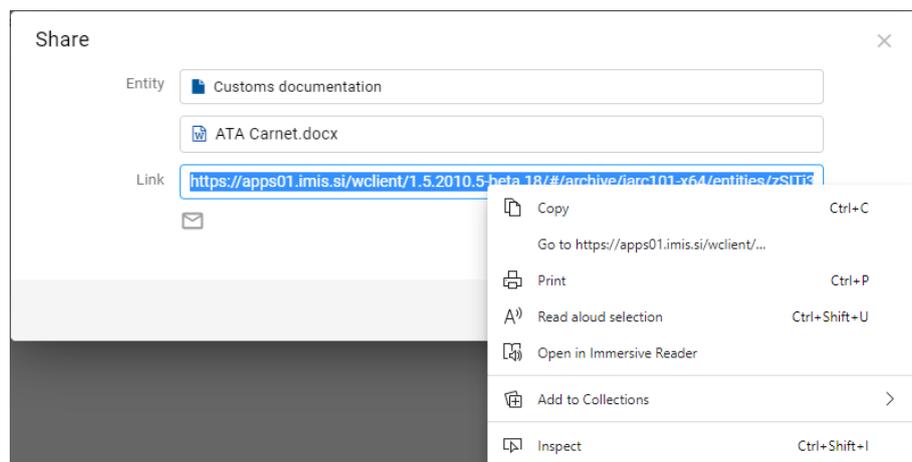


Image 137: Copying the link to the selected entity

By confirming the action Copy, the link to the entity is copied to the clipboard.



Image 138: Notification of copying a link to the clipboard

By selecting the icon , the user is shown the email content in the default messaging client with a link to the entity/content.

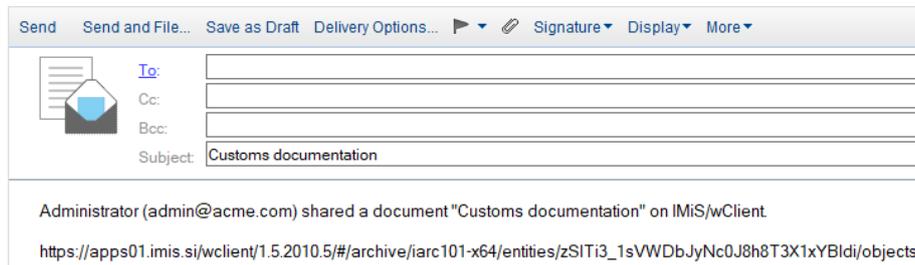


Image 139: Sending a link to the selected entity/content by email

By clicking the link, the email recipient is shown a login window of the IMiS®/wClient. After login, the user is shown the selected entity/content in the preview mode.

4.3.3.10 Adding and editing references

References enable a user to establish connections between entities and instantly move to other entities in the classification scheme.

To add references on an entity the user must have the Create reference permission.

The user can add a reference on existing entities by selecting the Actions command in the command bar and New reference in the popup menu.

Note: Functionality is supported in IMiS/ARChive Server version 9.9 or higher.

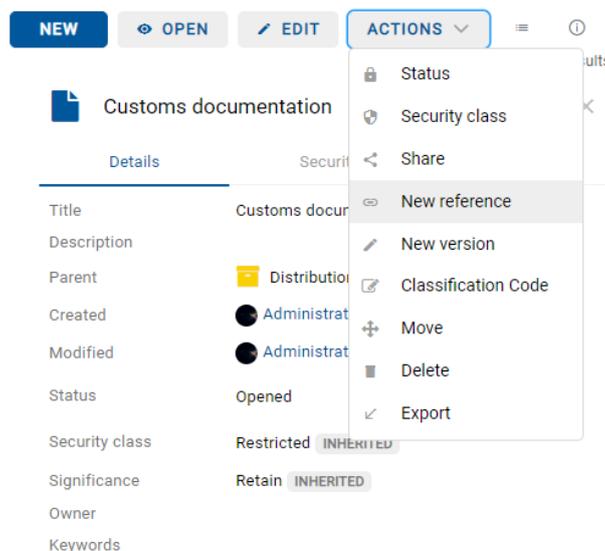


Image 140: The popup menu for selecting the New reference command

The user is shown a dialog box for adding a reference.

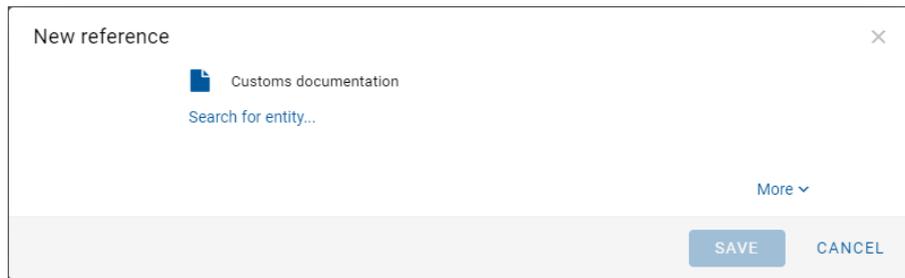


Image 141: The dialog box for adding and editing a reference

By selecting Search for entity, an entity tree opens for the user in the dialog box.

By confirming the selection of the relevant entity (Add), the user establishes a reference between the entities.

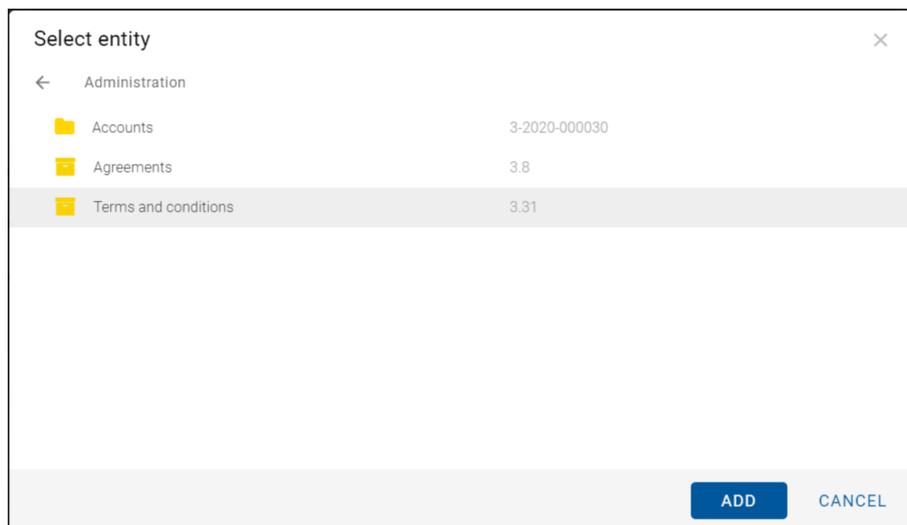


Image 142: Selecting Search for entity« in the New reference dialog box

By selecting More in the dialog box, the user is shown two fields for entering the values of the attributes Title and Description of the reference.

The two attributes are not mandatory. If their values are empty, the fields stay hidden.

The title of the reference is simply the name of the reference, if there is no reference title and there is only one entity in the reference. If there is more than one entity in the reference, they are shown below the title of the reference.

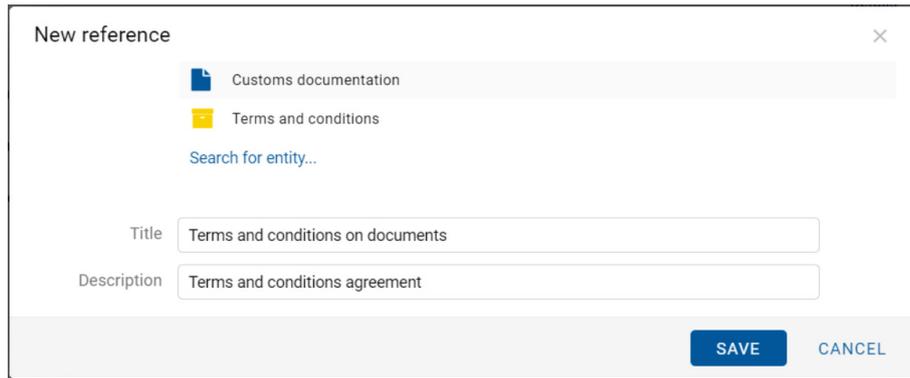


Image 143: Adding the Title and Description in the New reference dialog box

The reference can be removed by selecting the icon  at the end of the record of each reference.

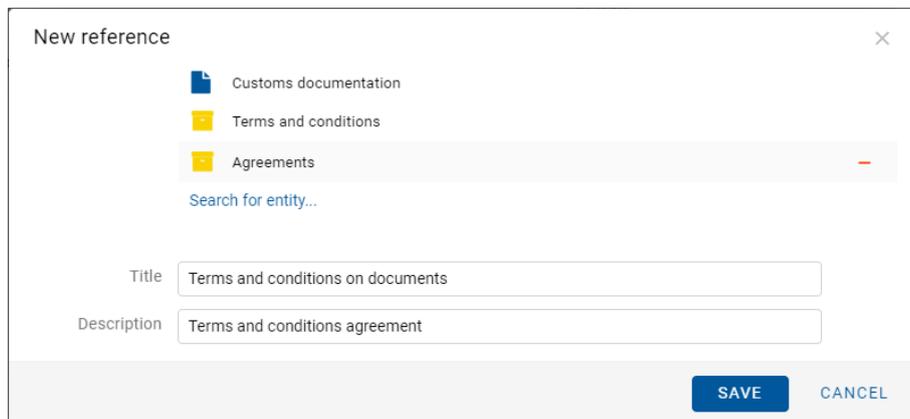


Image 144: Removing a reference before saving

Note: Saving is enabled in the dialog for editing a reference if at least 2 entities are displayed. A reference with a single entity cannot be saved.

References between entities are visible to the user in the set References in the Details tab in the right view. The user can edit the reference in the preview mode or in the open mode by selecting the icon  at the end of the reference record.

One exception is a document classified under a folder, in which case the set References is visible only in open mode.

By selecting the Edit command, the user can edit existing references or add new ones.

By selecting the Delete command, the user removes the reference from the list.

The user cannot delete an entity that contains a reference which the user is editing.

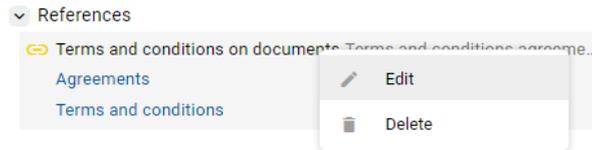


Image 145: A dialog box for selecting an action on the reference

4.3.4 Entity move

The IMiS®/wClient enables the movement of entities across the classification scheme.

To move entities, a user requires the following permissions:

- Move: on the entity he is moving.
- Delete: on the entity he is moving.
- Create entities: on the newly selected parent entity or root class.

To begin moving single or multiple entities within the classification scheme, select the entity you wish to move, and then the Move command, which is available via:

- Actions command in the command bar.
- popup menu on the entity chosen from the list of contained entities.

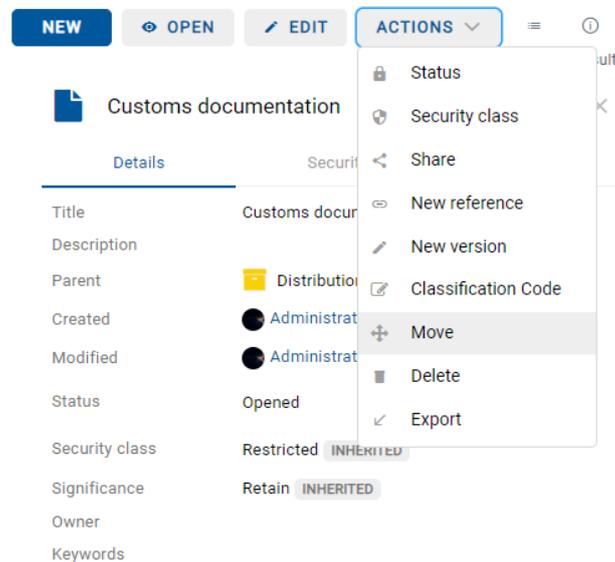


Image 146: Selecting the Move command via the Actions command in the command bar

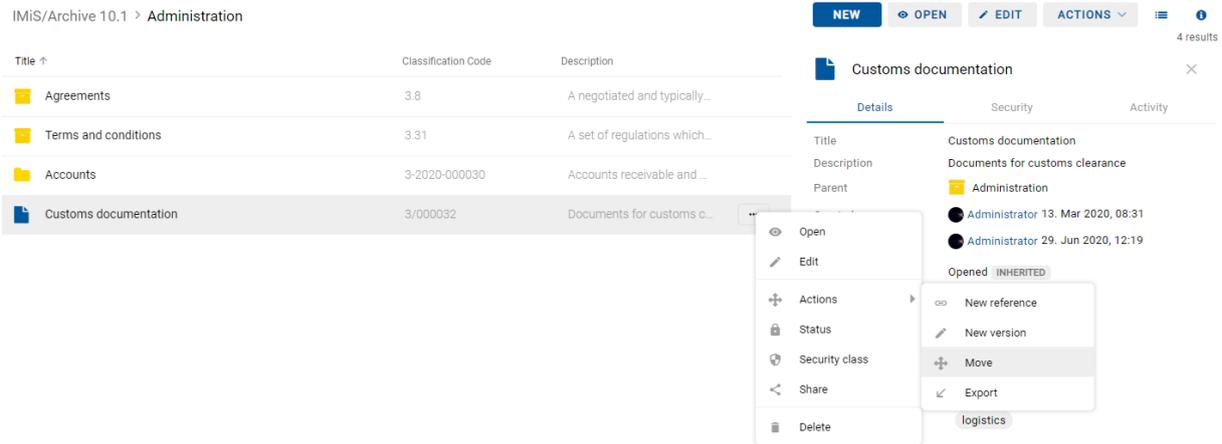


Image 147: A popup menu on the selected entity for selecting the Move command

When selecting the Move command, user will receive the Move dialog box, where he selects new parent entity from the list of entities, and the Reason field to enter the reason for the move. The move of the entity is confirmed using the Move button.

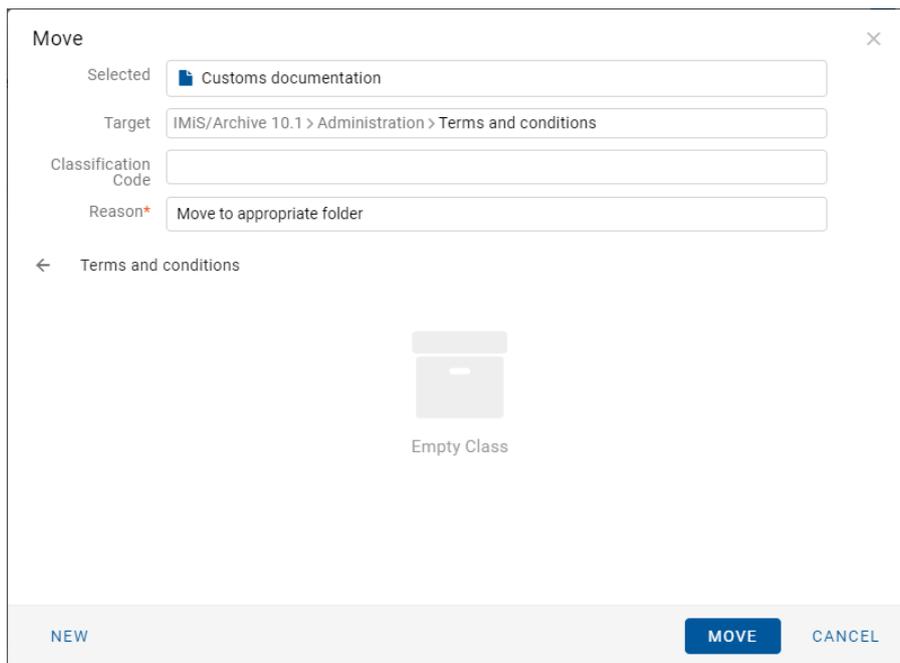


Image 148: A dialog box for moving an individual entity

The user can manually set a new classification code for the entity when moving it. In the dialog box for moving, the user enters the new classification code in the field for entering the value of the attribute Classification code.

The 'Move' dialog box contains the following fields:

- Selected:** Customs documentation
- Target:** IMIS/Archive 10.1 > Administration > Terms and conditions
- Classification Code:** IS-ADMIN-2020/001
- Reason*:** Move to appropriate folder

Image 149: Manually assigning the classification code when moving

If multiple entities are being moved, the user marks the entities and selects the action Move in the menu.

In the dialog box, the user specifies the reason for the move and selects the entity to which the selected entities will be moved.

The 'Move' dialog box shows multiple entities selected and a list of target folders:

- Selected:** Shipping release note, Despatch note, Customs documentation
- Target:** IMIS/Archive 10.1 > Administration > Terms and conditions
- Reason*:** Move to appropriate folder

Below the fields is a list of folders under 'Administration':

Folder Name	Classification Code
Accounts	3-2020-000030
Agreements	3.8
Customs documentation	3/000032
Despatch note	3/000033
Shipping release note	3/000034
Terms and conditions	3.31

At the bottom of the dialog are three buttons: NEW, MOVE, and CANCEL.

Image 150: A dialog box for moving multiple entities

Before the move, the user can create a new entity by selecting the command New in the dialog box. For more information see chapter [Creating a new entity](#).

The classification code serves as a unique locator of the entity within the classification scheme. It consists of the relative (own) classification codes of the entities.

When moving, the following rules for renumbering the classification code apply depending on the manual, manual (optional) or automatic setting of the entity classification code in the moving entity tree:

- The entities in the moving entity tree, which are located directly under the entity with a manual or manual (optional) setting of classification codes, are not renumbered; all other entities are renumbered if the counter context enables it (automatic creation of a classification code on the entity to which the entity tree is moving).
- Moving an entity with a manually or manually (optional) set classification code under an entity which is set to automatically create a classification code causes that entity to be renumbered; the implementation mentioned in point 1 applies to all other contained entities.
- Moving an entity with a manually, manually (optional) or automatically set classification code under an entity which is set to manually assign a classification code is not possible, if a contained entity exists that has the same partial classification code as the source entity. If the move is possible, the entity tree is moved. Due to an invalid counter context (manual setting of the classification code), the renumbering is not performed for any contained entity.

Note:

The following rules apply to the user when moving:

- *The user can move all entities, regardless of whether they are closed or opened.*
- *The user cannot move documents which are classified directly under a class under folders.*
The user likewise cannot move documents which are classified under folders directly into a class.

4.3.5 Content management

This chapter describes the following actions over document contents:

- [Capturing content](#)
- [Content details](#)
- [Saving content](#)
- [Content preview](#)
- [Downloading content](#)
- [Content update](#)
- [Copying content](#)
- [Moving content](#)
- [Deleting content](#)
- [Indexing content](#)
- [Content conversion.](#)

4.3.5.1 Capturing content

The user captures the content of documents by using the:

- File system command, by selecting the specific content.
- Scanner and the enabled services of IMiS®/Capture Service.

4.3.5.1.1 Capturing content from the file system

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, if they exist. In the case of a new document the list is empty. In editing mode, the contents are displayed below the field for adding contents.



Image 151: The Content field for adding contents

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 152: 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.

For more information see chapter [Saving an entity](#).

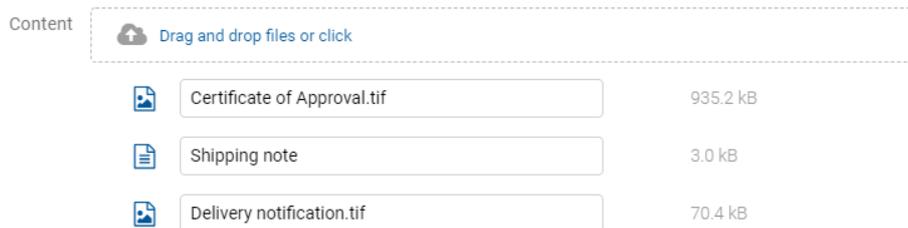


Image 153: The added content after saving

The contents are shown below the bar with the titles of the common attributes in open mode. Description and Size are shown by default.

The user can add or remove the column of selected attributes Modified via the icon  in the command bar.

Note:

Attaching contents is possible only in the Document entity type.

IMiS/Archive 10.1 > Administration > Despatch note

Title	Size	Modified
 Certificate of Approval.tif	935.2 kB	12. Mar 2020
 Shipping note	3.0 kB	13. Mar 2020
 Delivery notification.tif	70.4 kB	30. Jun 2020

Image 154: Displaying the list of contents in open mode

4.3.5.1.2 Capturing content from a scanner

If a suitable service key record has been defined in the settings of the IMiS®/Capture Service and the user profile in the IMiS®/wClient, the icon “Scan” appears in the field for adding contents.

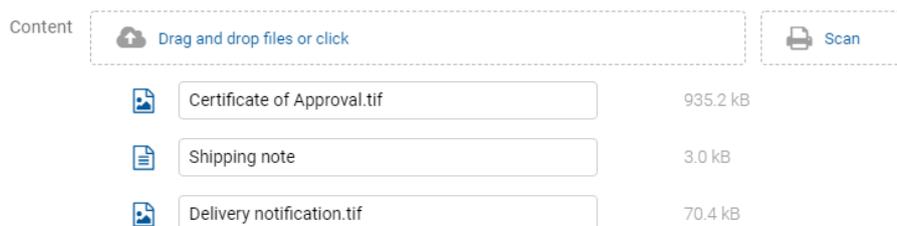


Image 155: Displaying the icon Scan for capturing content from a scanner

Note: If the icon “Scan” is not shown, check the settings:

- of the service key in the “Security” tab of the IMiS®/Capture Service.
For more information see chapter [Security settings in IMiS®/wScan Manual](#).
- of the service and security key address in the IMiS®/wScan section in the “Settings” tab.
For more information see chapter [The Details tab](#).

By selecting the icon Scan, the user is shown an integrated window for scanning using the IMiS®/wScan program module.

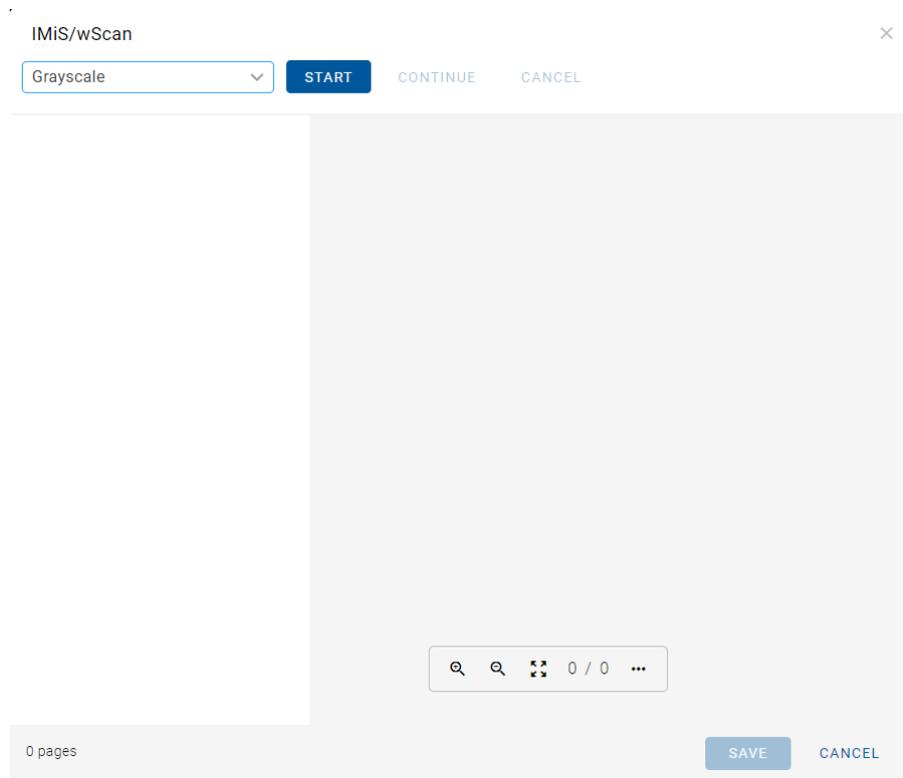


Image 156: Integrated window for scanning with IMiS®/wScan

Note:

If the user has connected or turned on the scanner cable later and the command Start is still disabled, we recommend restarting IMiS®/Capture Service with the command Restart Service.

By selecting the Start command, the scanning of documents is executed. The user receives a report with the basic scanning information.

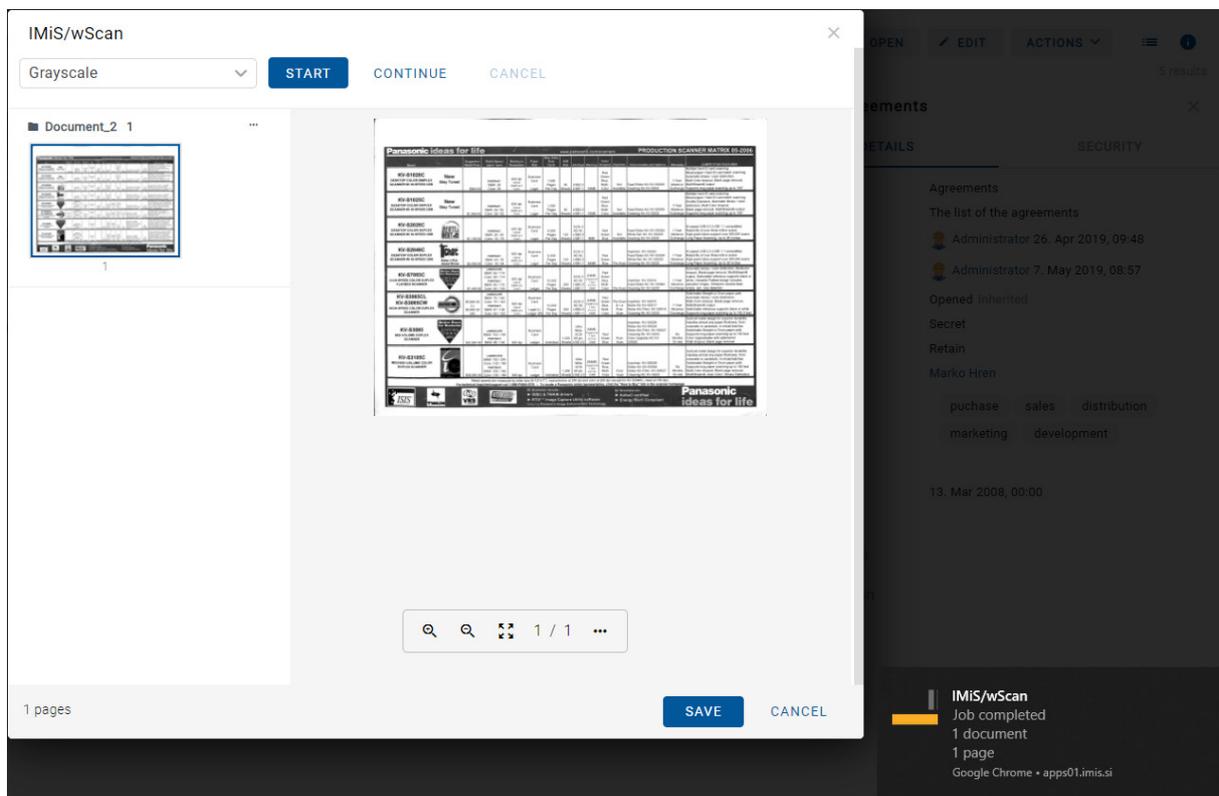


Image 157: Displaying the document after finishing the scan

After finishing the scan, the user adds the scanned document to the list of content pages. By selecting the popup menu on the view of thumbnails of the scanned document, the user can choose from the following options:

- Download: download an individual page in the PNG format.
- Insert before: Continues scanning before the selected page.
- Insert after: Continues scanning after the selected page.
- Rotate right: rotates page to the right.
- Rotate left: rotates page to the left.
- Delete: deletes an individual page.
- Properties: content properties (this functionality is currently not supported).

By selecting the Save command, the user saves the scanned content to the IMiS®/ARChive Server.

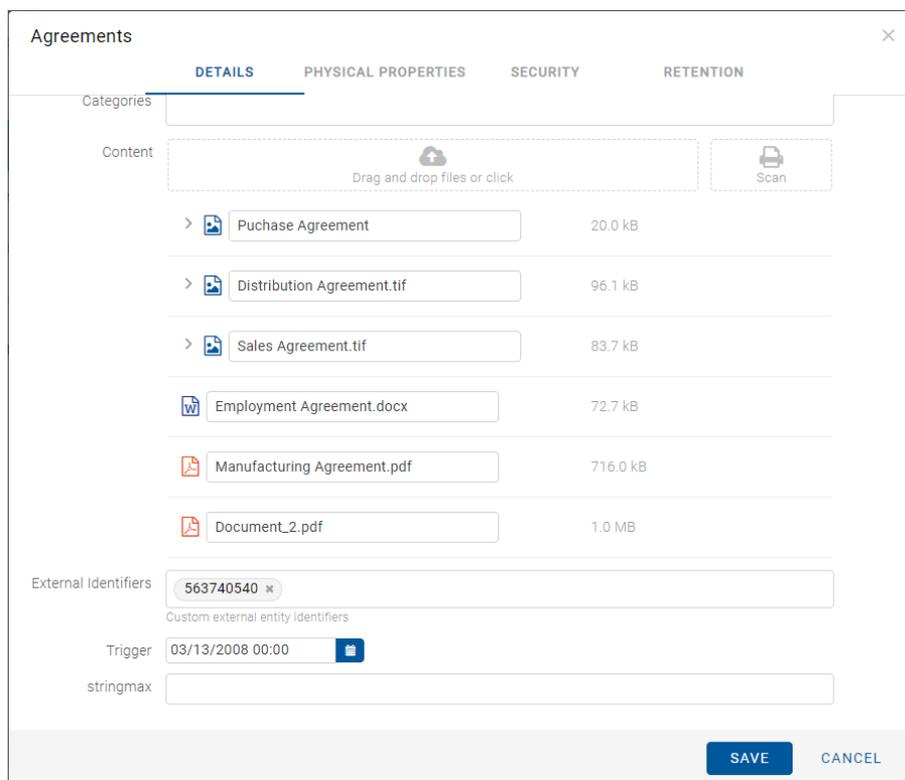


Image 158: A scanned document added to the list

For more information on setting IMiS®/Capture Service see chapter [Application integration in the IMiS®/wScan Manual](#).

Note: The scanning settings are located in the Settings tab or in the configuration settings.json under scan.apiKey and scan.url.

Troubleshooting: Most frequent issues when capturing content:

- The file does not exist.
- Wrong MIME type of file.

4.3.5.2 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.
- Entity: the title of the entity.
- 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.

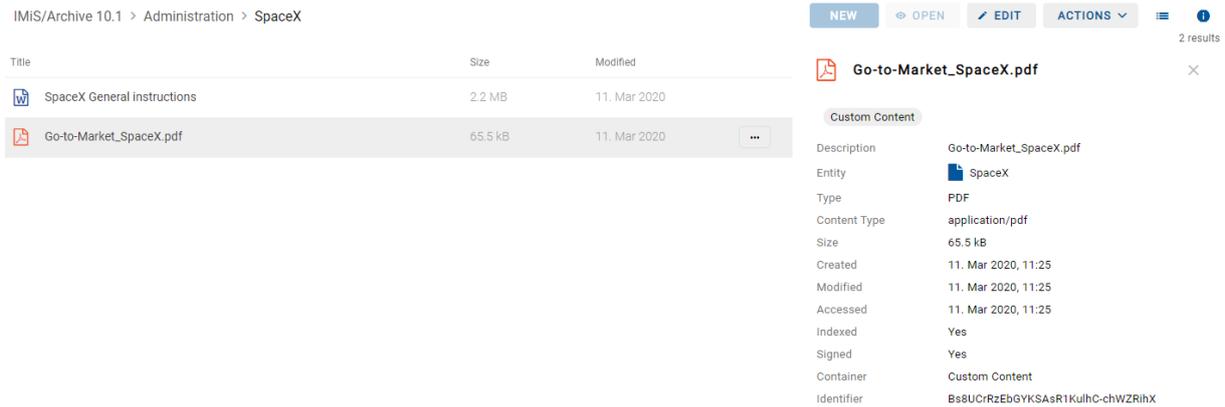


Image 159: Content details in the right view

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



Image 160: Changing the description of content in editing mode

Note: Depending on the template settings in the IMiS®/ARChive Server administrative interface, the logged-on user also has the option of saving content to the "Custom content container". For more information see the chapter [Moving content](#).

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.
- Copy: copying content to another document.
- Details: displaying information on the content. These details are displayed if they were not displayed yet.
- 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.

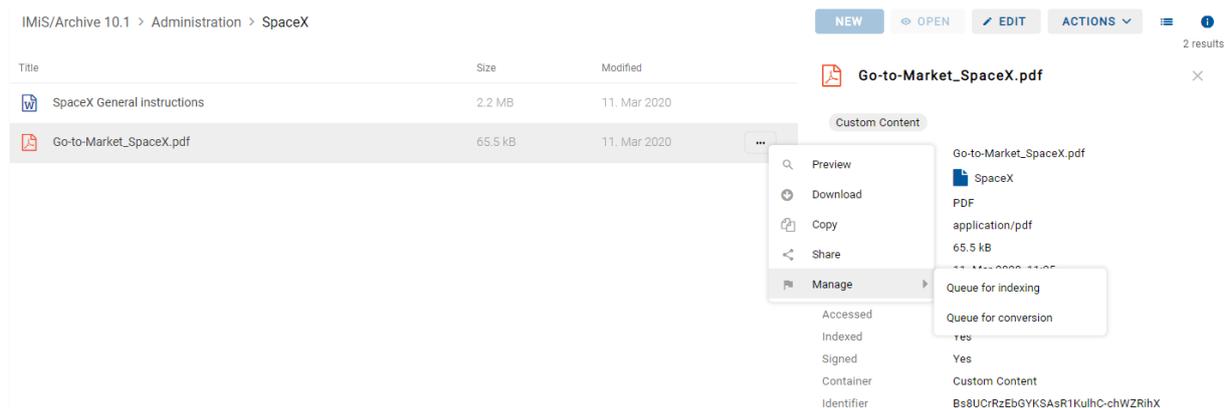


Image 161: Popup menu on the selected content in the reading mode

4.3.5.3 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).

Content Type application/pdf

Image 162: 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.

Created 10. Mar 2020, 08:25

Image 163: 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.

Modified 30. Jun 2020, 13:34

Image 164: 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.

Accessed 30. Jun 2020, 13:34

Image 165: An example of the date of the last access to the document content

- **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.

Identifier UhwTMq4NrM0qw7HjhmVy2s6Z6VGe58kA

Image 166: An example of the document content identifier

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

Indexed Yes

Image 167: An example of a display of indexed document content

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

Signed No

Image 168: An example of a display of signed document content

4.3.5.4 Content preview

The content can be previewed by a user with the Read permission.

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

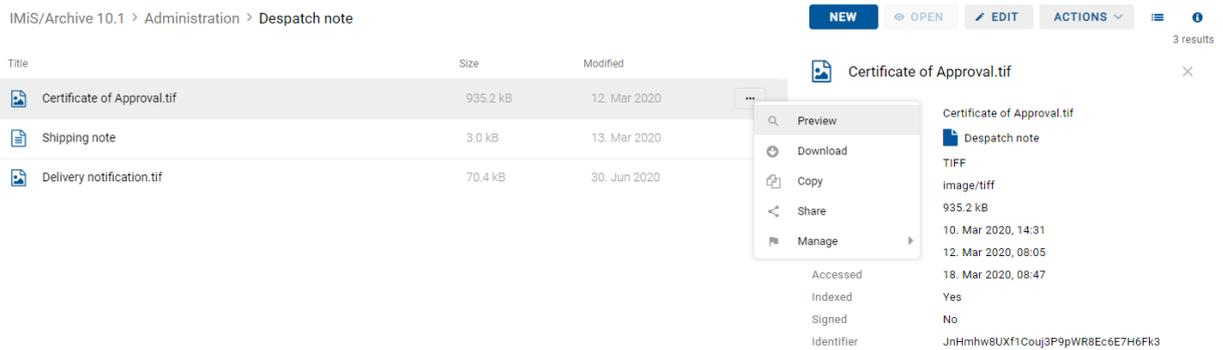


Image 169: Opening document content

An alternative option is that the user simply clicks on the content record.

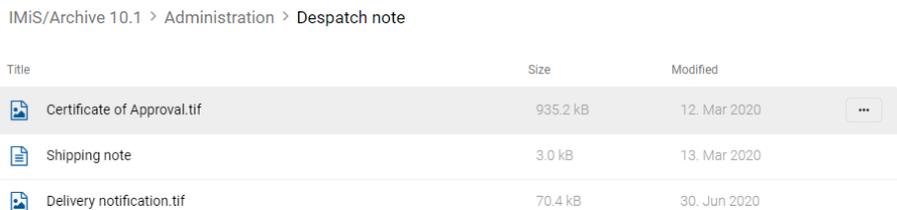


Image 170: Opening content by clicking on the content

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.

For more information on downloading content see chapter [Downloading content](#).

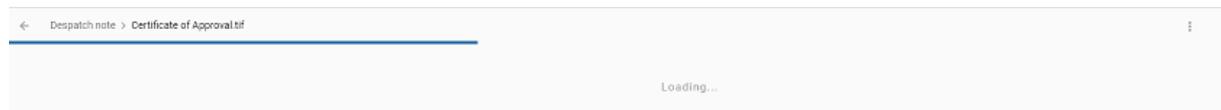


Image 171: Loading content

By selecting the content preview, in the case of multiple contents a menu appears at the bottom for selecting and displaying contents under a specific entity. The user switches between contents by clicking on the title of each content or using the left/right keys on the keyboard.

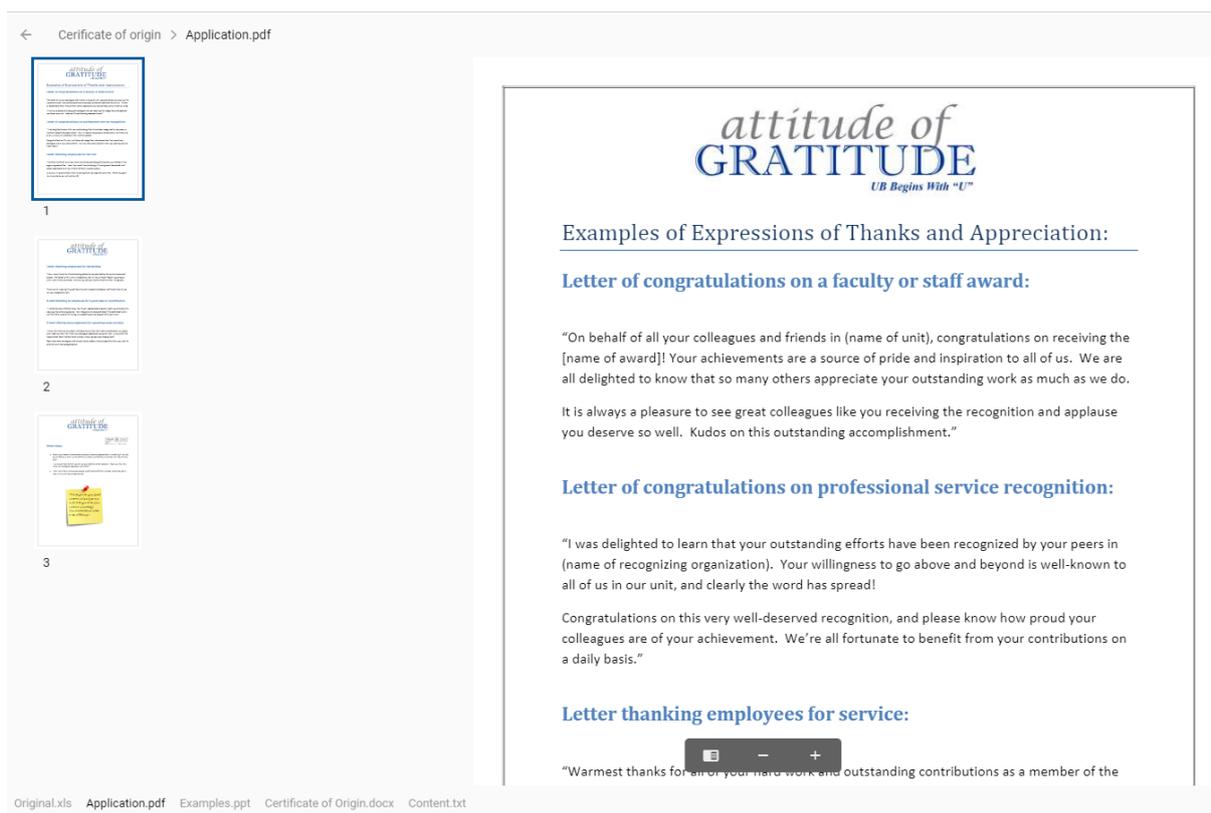


Image 172: Displaying the menu for selecting and previewing content

For easier and faster searching by the pages of the contents of PDF/A and TIFF formats, the user can use the side menu with the thumbnails of document pages.

Located on the displayed content pages is a menu for zooming in or out of the displayed content and the side menu view.

By selecting the top right menu, the user can perform the following:

- Download: downloading the content to a computer or device.
- Share: copies the link to the selected content and shares it with other users.

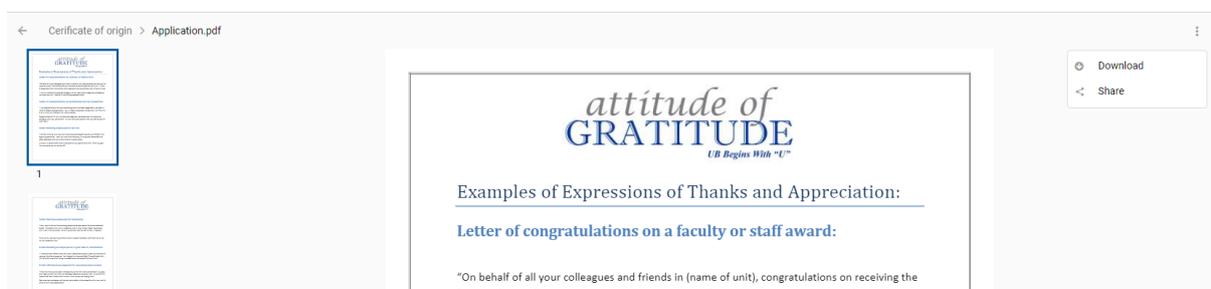


Image 173: Selecting the menu on the content preview

The user has the option of previewing content with the link *archive/:archive/entities/:id/view* with the parameters index and id.

Example 1: Link with the parameter id

<https://apps01.imis.si/wclient/1.5.2010.5/#/archive/iarc101-x64/entities/BMtozc348swzj1NCSyWXEaUH44UD65j4/view?id=Qgi2oGjJOdcwztmOBE7slvULSbamjyh&ver=4/OBJECTS>

Example 2: Link with the parameter index 1

<https://apps01.imis.si/wclient/1.5.2010.5/#/archive/iarc101-x64/entities/BMtozc348swzj1NCSyWXEaUH44UD65j4/view?id=Qgi2oGjJOdcwztmOBE7slvULSbamjyh&ver=4/OBJECTS/VIEW?INDEX=1>

Example 3: Link without parameters, which opens the first object

<https://apps01.imis.si/wclient/1.5.2010.5/#/archive/iarc101-x64/entities/BMtozc348swzj1NCSyWXEaUH44UD65j4/view?id=Qgi2oGjJOdcwztmOBE7slvULSbamjyh&ver=4/VIEW>

IMiS®/wClient and IMiS®/Storage Connector Services REST use the Web Application Open Platform Interface (WOPI) protocol for integration with Office Online. It defines the mode of interaction between the WOPI server (IMiS®/Storage Connector Services REST) and Office Online. In the settings (assets/settings.json) the addresses of the Office Online server must be defined in order to be able to preview Word, Excel and PowerPoint contents.

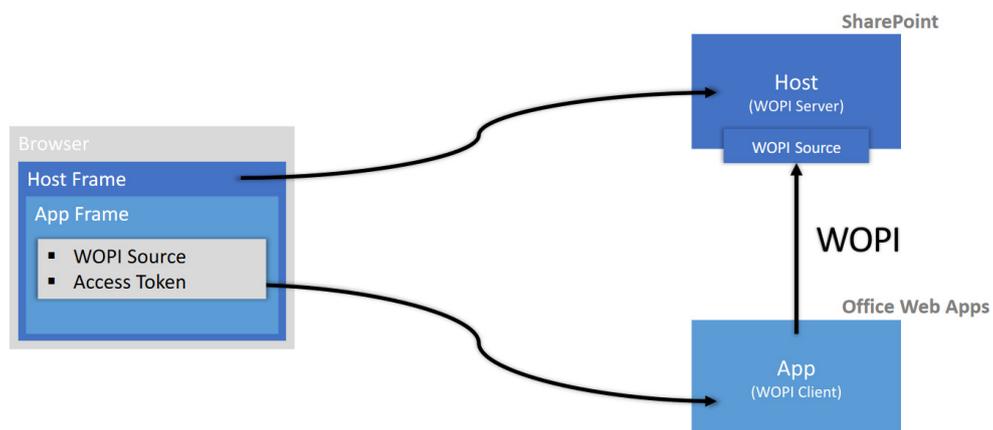


Image 174: WOPI flow chart

It enables the user to preview Word, Excel and PowerPoint contents.



Image 175: Opening MS Office content

In the context of the content formats which are supported on the IMiS®/ARChive Server and can be described with IANA-registered content types (MIME type; see chapter [Capturing content](#)), the user can play the following audio and video contents in streaming mode:

- Audio (wav, ogg, mpeg)

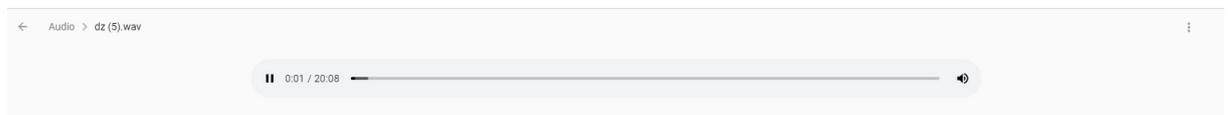


Image 176: Opening audio content

- Video (mp4, webm, ogg)



Image 177: Opening video content

***Note:** Previewing audio and video contents is possible if the content has been optimized for online viewing.*

4.3.5.5 Downloading content

The content can be downloaded by a user with the Read permission.

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.

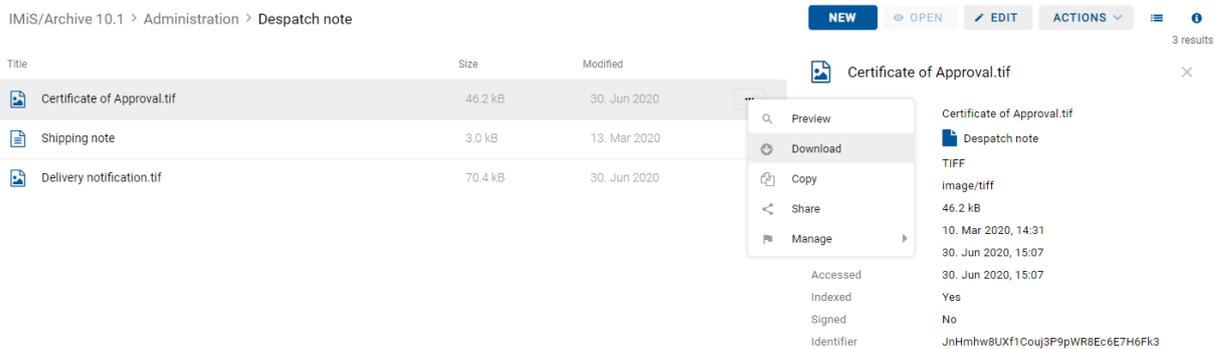


Image 178: Selecting the Download command in the popup menu

In the bottom left corner the user is shown the progress of the download of content and the Cancel option.

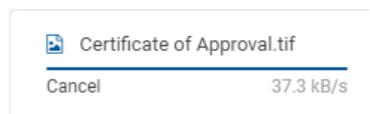


Image 179: Displaying the progress of the download of content

By selecting the popup menu on the notification about downloaded content, the user has the option of selecting actions.

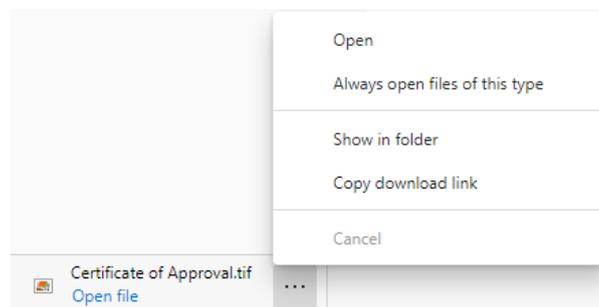


Image 180: Displaying the option of selecting actions on downloaded content

4.3.5.6 Copying content

Copying content can be performed by the user with the Write right.

The user makes a copy of the entity's content and copies it to another document-type entity.

The user selects the content in the Open mode. By selecting the popup menu on the tagged content, the user selects the Copy command.

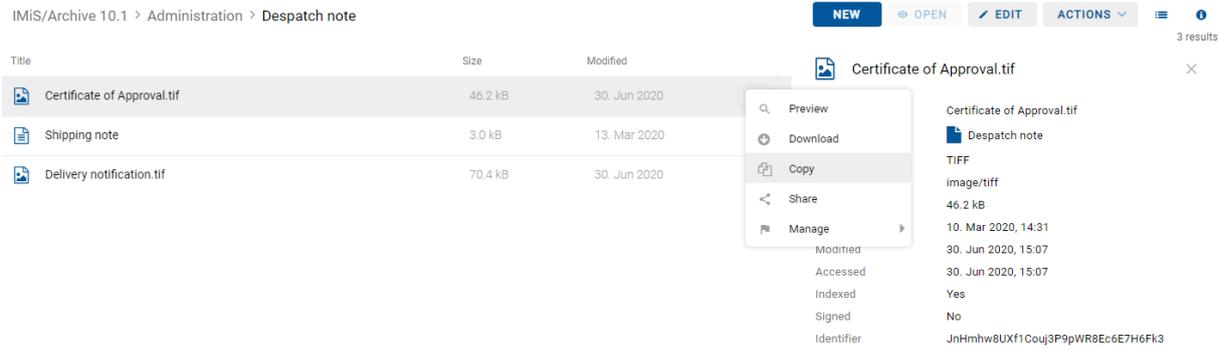


Image 181: Selecting the Copy command in the popup menu

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

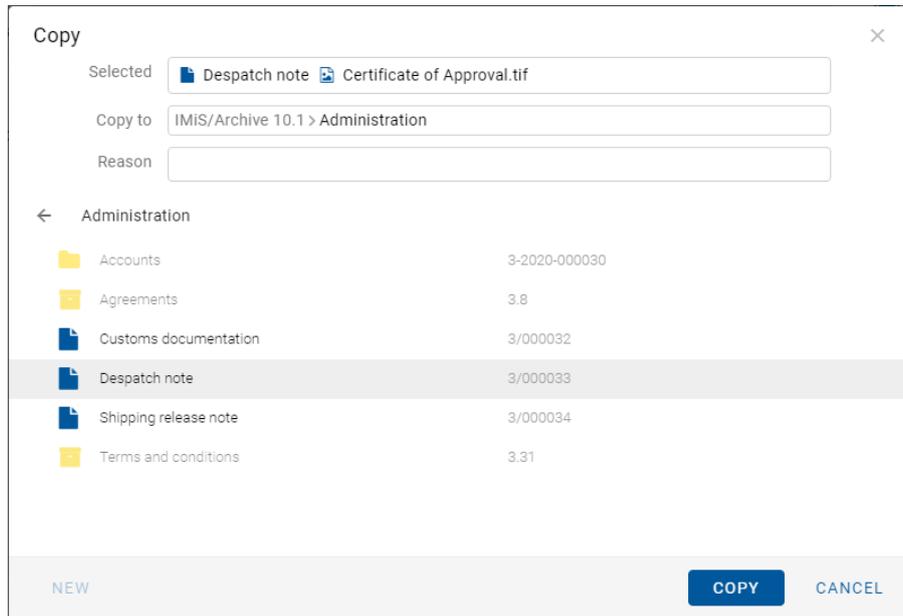


Image 182: Copying the content to another document

After confirming the Copy command, a copy of the content is saved to the selected document. The user is informed of saving a copy of the content.

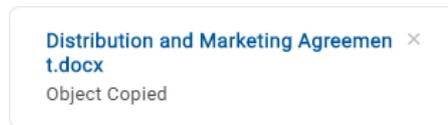


Image 183: Information about saving a copy of the content

4.3.5.7 Sharing content

The content can be shared by a user with the »Read« permission.

The user creates a copy of the link to the entity's content and saves it to the clipboard.

In open mode, the user selects the content. By selecting the popup menu on the tagged content, the user selects the command Share.

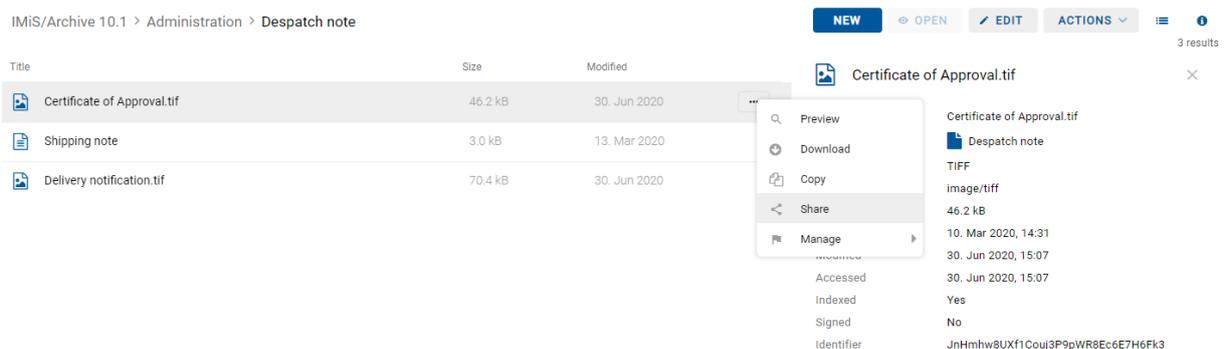


Image 184: Selecting the command Share in the popup menu

A dialog box opens containing the created link to the selected content.

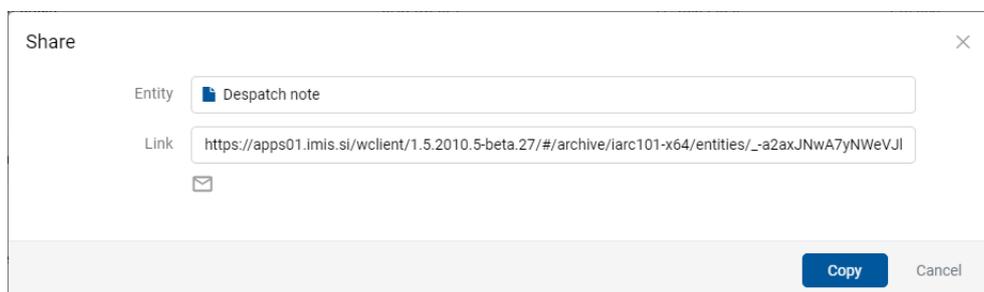


Image 185: Displaying the created link to the selected content

By confirming the action Copy, the link to the content is copied to the clipboard.

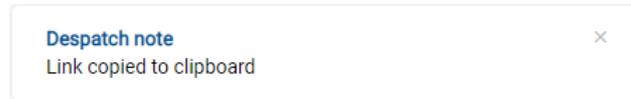


Image 186: Notification of copying a link to the clipboard

4.3.5.8 Content update

Content update can be performed by the user with the Write right.

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.

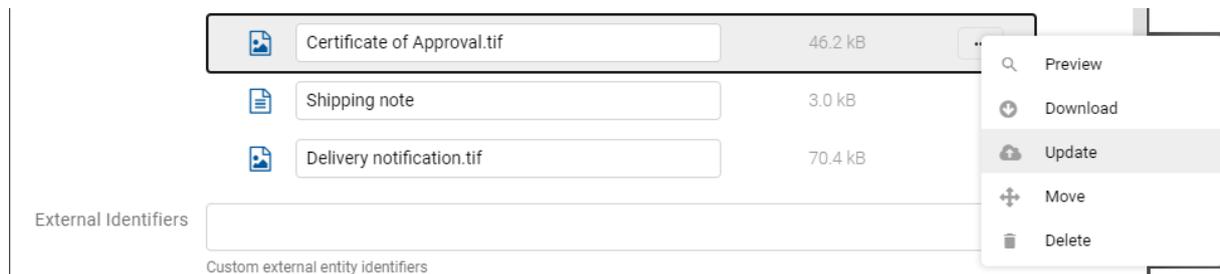


Image 187: Selecting the »Update« command in the popup menu

IMiS/Archive 10.1 > Administration > Despatch note

Title	Size	Modified
 Certificate of Approval.tif	62.5 kB	1. Jul 2020
 Shipping note	3.0 kB	13. Mar 2020
 Delivery notification.tif	70.4 kB	30. Jun 2020

Image 188: The selected content after update

4.3.5.9 Moving content

Moving content from one entity to another can be performed by the user with the Write right. The user selects the content in the editing mode. In the popup menu on the tagged content, the user selects the Move command.

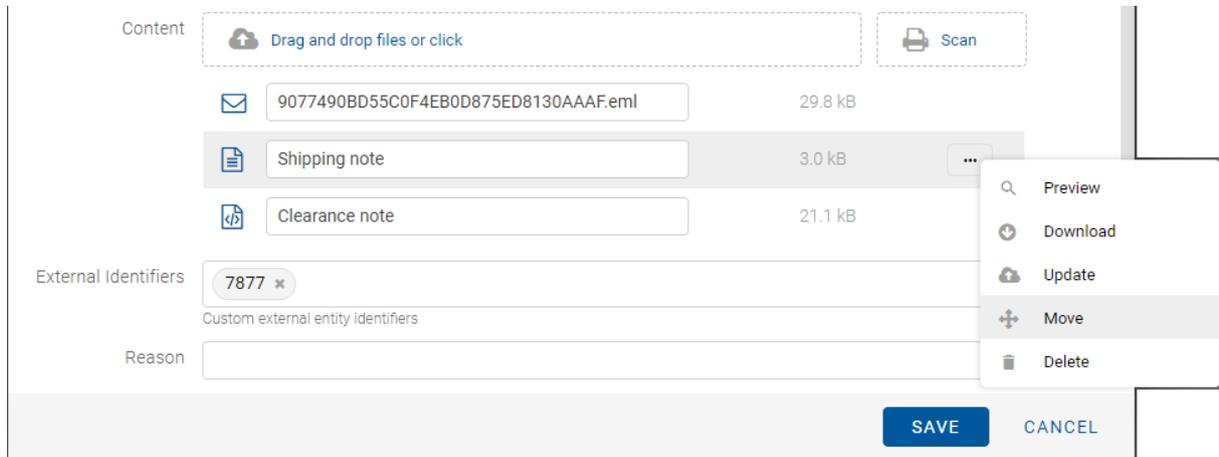


Image 189: Selecting the Move command in the popup menu

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

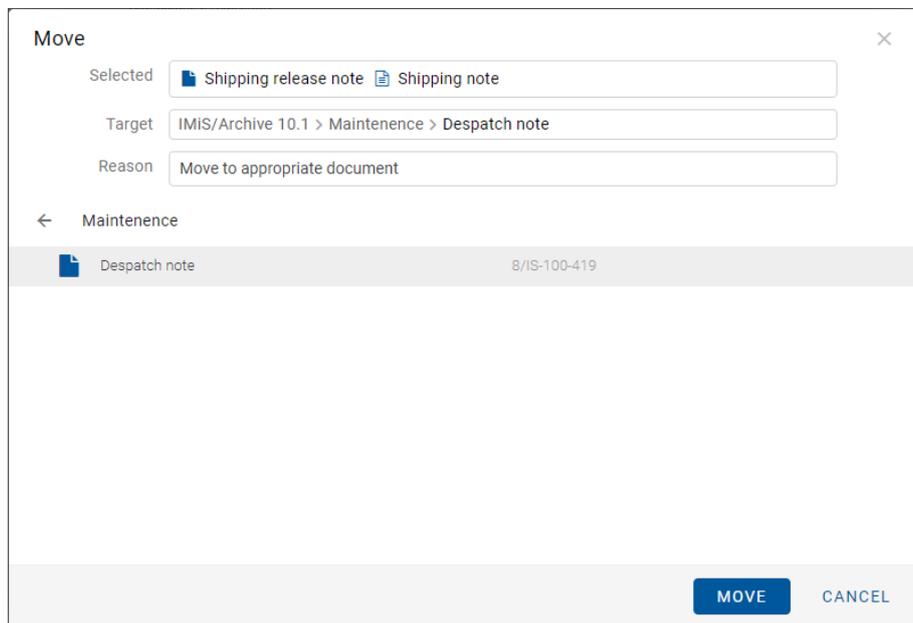


Image 190: Selecting the target document for moving content

By confirming the selection with the Move command, the content is tagged to move.

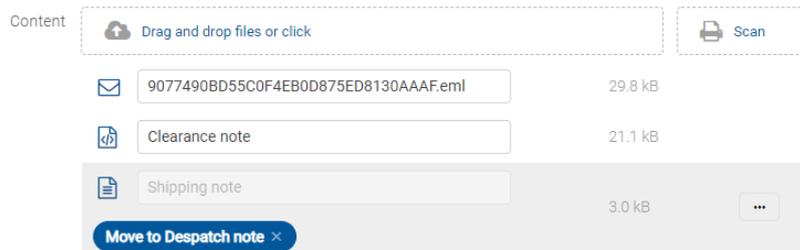


Image 191: Content temporarily removed from the document

Content move is not performed until after saving changes.

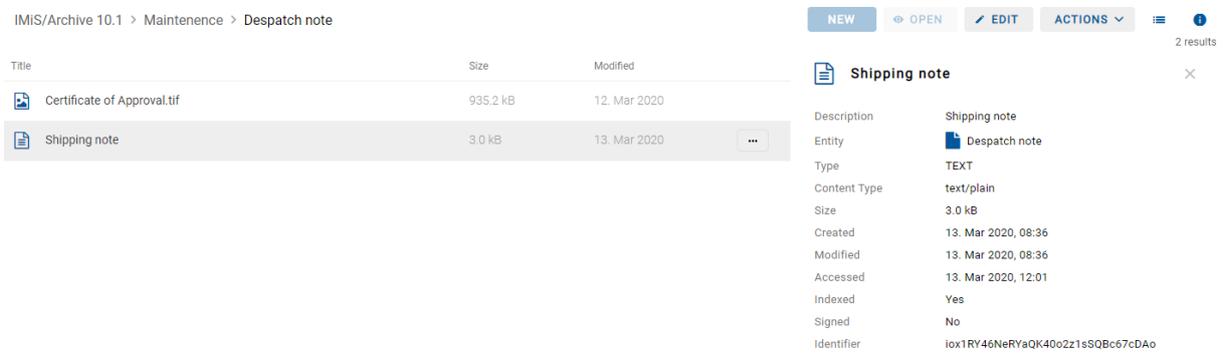


Image 192: Saved document content

The logged-on user can also move content to the “Custom content container”. When selecting the target document for moving content, an additional “Container” attribute is shown if the template contains an attribute of the File type.

The user selects accordingly from the set of values.

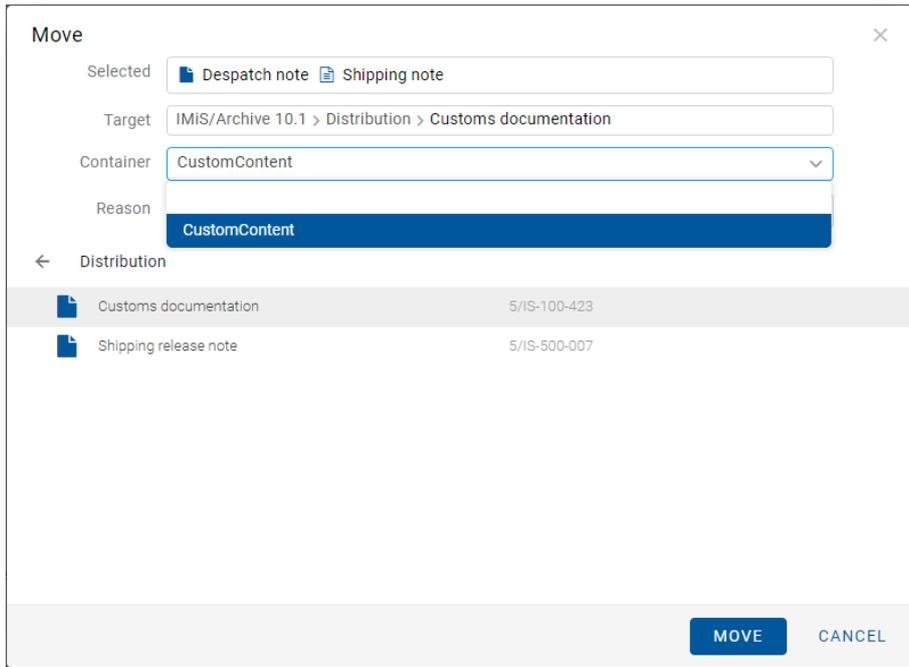


Image 193: Selecting the target document for moving content to the custom content container

By confirming the selection with the Move command, the content is tagged to move to the custom content container.

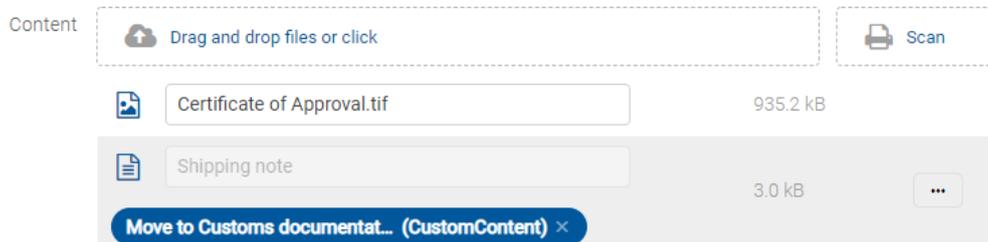


Image 194: Content temporarily removed from the document

Content move to the custom content container is not performed until after saving changes.

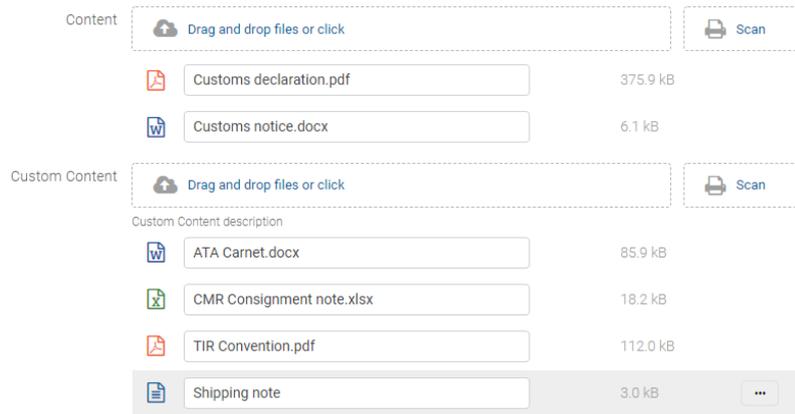


Image 195: Saved document content to the custom content container

4.3.5.10 Deleting content

Deleting content can be performed by the user with the Write right.

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.

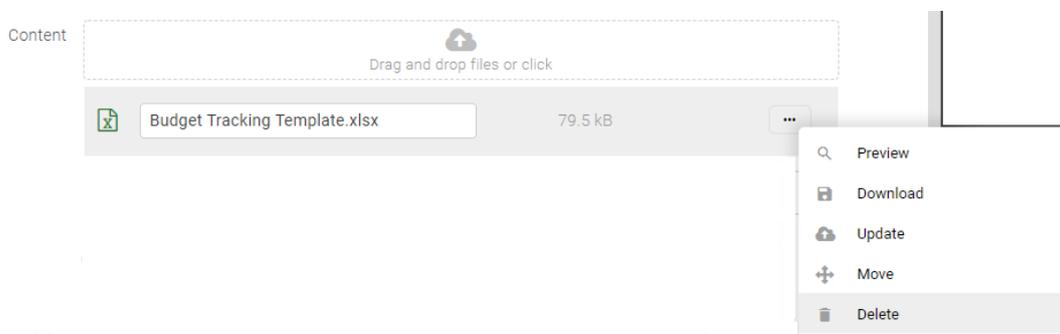


Image 196: The content on the list before deletion

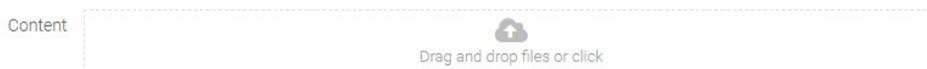


Image 197: Empty list after deletion

4.3.5.11 Indexing content

The manual tagging of content for indexing can be performed by the user with the ContentManagement role.

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.

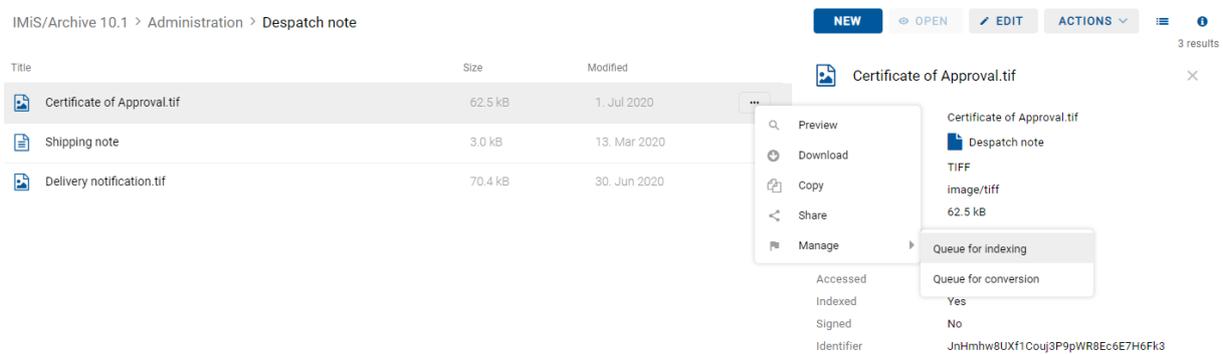


Image 198: Selecting the Queue for Indexing command



Image 199: Successful adding of content for indexing

4.3.5.12 Content conversion

The IMiS®/ARChive Server enables automatic content conversion. All newly added content is automatically converted to a long-term storage format after being stored according to the period setting in the server configuration (PDF/A, TIFF).

Example: A content created in Microsoft Word that is attached to the document must be converted into the PDF/A file type to ensure long-term storage.

For better visibility, the converted content is displayed in a tree. Content can also be multi-level and enable a view of the conversion history. 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.

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.

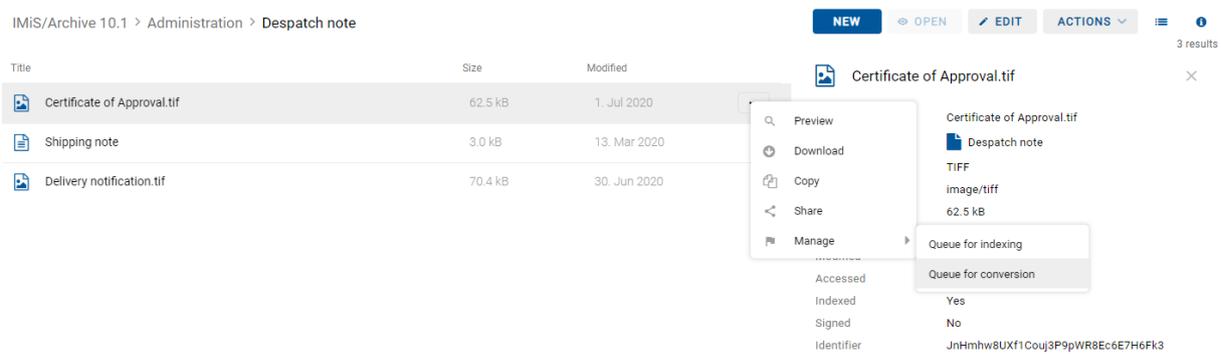


Image 200: Selecting the Queue for Conversion command

The user is informed of successfully tagging the content for later conversion.



Image 201: Successful tagging of content for later conversion

4.3.5.13 Detaching content

In edit mode the user has the option of detaching the selected converted content.

The user with the Write permission can perform the detachment.

In edit mode the user selects the content. In the popup menu the user selects the Detach command.

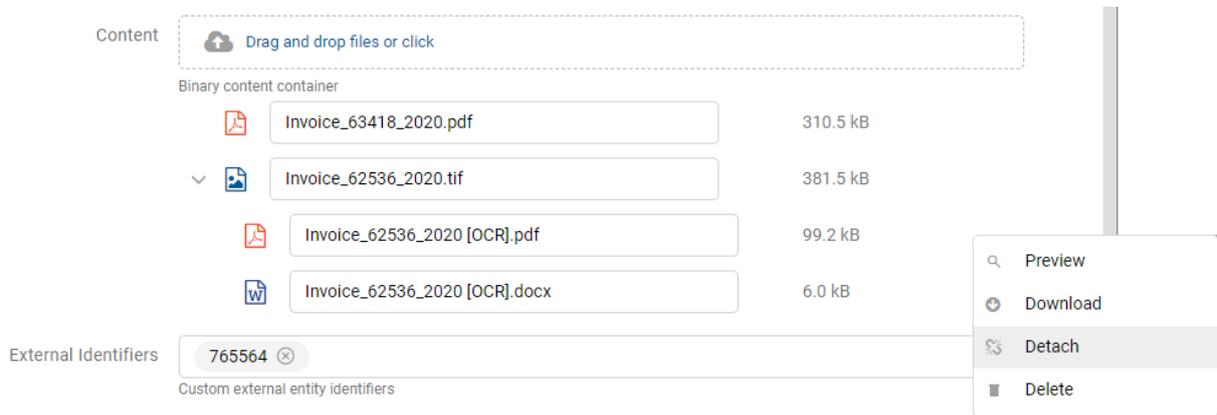


Image 202: Detaching the selected converted content

The detachment is not executed until confirmed with the Save command.

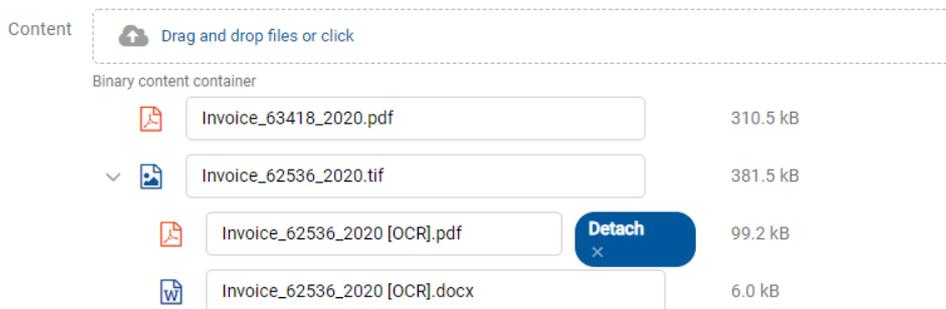


Image 203: Tagging content for detachment

After confirming the detachment of converted content, the selected content is classified under the last content on the list.



Image 204: Displaying detached content on the list

Warning: Removal of source content is possible only after a prior removal of all interpretations of the content. While removing content at individual levels, the entity must be saved.

4.3.6 Versioning

The user is enabled the versioning of the values of document attributes. The properties that have been modified in individual document versions can be reviewed only on templates that enable versioning. The basic condition is that the template attribute has been marked as “versionable”.

This functionality is supported in IMiS®/ARChive Server version 9.9 or higher.

For more information see chapter [Versioning in the IMiS®/ARChive Server Manual](#).

4.3.6.1 Creating new version

By selecting the action “New version” in the popup menu on the “Actions” button in the command bar or on the document selected from a list, the user is shown a dialog box with the relevant tabs and set of attributes.

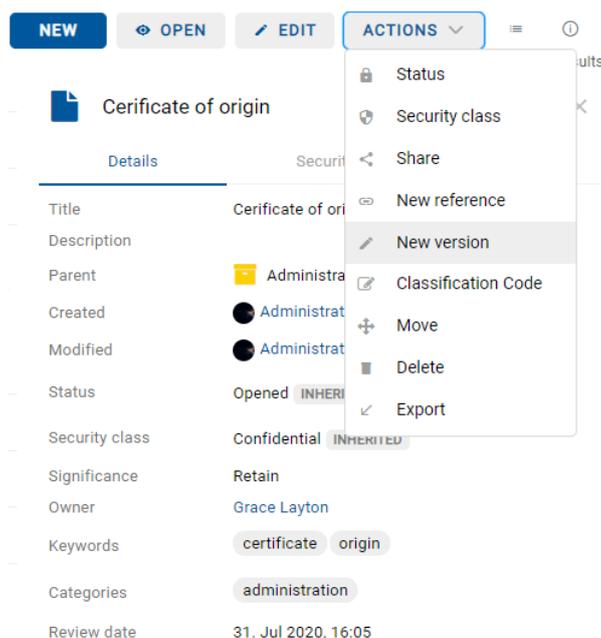


Image 205: Selecting the action New version in the popup menu

In the Details tab the following attributes are available to the user:

- Version: selecting a document version. The available options are:
 - Major: signifies major changes to the document.
 - Minor: signifies minor changes to the document.
 - 3rd level: signifies minimum changes to the document.
 - 4th level: signifies the smallest changes to the document.
 - Overwrite: overwrites the existing document version.
- Comment: a comment to the document version.
- Title: the name of the document. This attribute is mandatory.
- Description: a short description of the document.
- Significance: a set of available document significances.
- Owner: the directory entity (user or group) that is responsible for the selected document version (owner).
- Keywords: document-related keywords. This attribute can have multiple values.
- Categories: a collection of document categories.
- Content: document contents.
- External identifiers: a list of the unique external identifier of the document version on the server.

Certificate of origin

Details Security Retention

Version: Major

Comment: Major

Title*: 3rd level

Description: Overwrite

Owner: Administrator

Keywords: certificate, origin

Categories: administration

Content: Drag and drop files or click

Binary content container

Original.xls	30.5 kB
Application.pdf	514.8 kB
Examples.ppt	1.7 MB
Certificate of Origin.docx	13.8 kB

Save Save Draft Discard Cancel

Image 206: Checking out a document version

The user confirms the checking out of a new document version with the Save command or cancels it with the Cancel button.

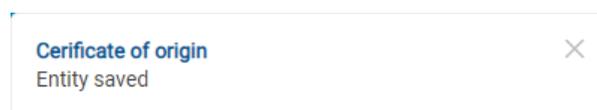


Image 207: Information about saving a document version

Note: While creating a document version, the source document is available to other users only in read-only mode.

4.3.6.2 Reviewing a document version

In the preview mode and open mode, the user can review document versions in the set Versions in the Details tab in the right view.



Image 208: Displaying document versions in the set Versions

Note: The last saved document version is placed at the top of the view. The selected document version is marked in blue.

4.3.6.3 Editing document version

The user can edit only the values of attributes to which he has the appropriate access rights.

By selecting the icon  on the document version record, the user can choose from the following options in the popup menu:

- Open: opens the selected document version in the reading mode.
- Edit: opens the selected document version in the editing mode.
- New version: creates a new version of the document via a dialog box.
- Delete: deletes a document version.

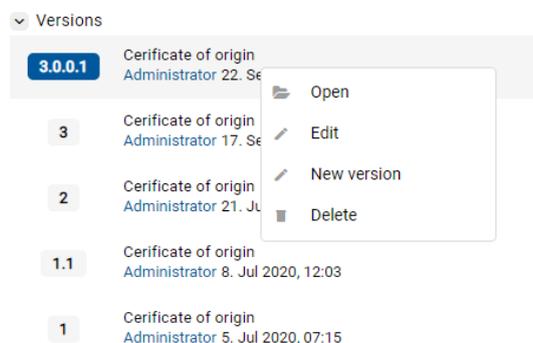


Image 209: A popup menu on the document version

In edit mode the user can change the attribute values.

Certificate of origin

Details Physical Properties Security Retention

Template* Document
Standalone document entity

Title* Certificate of origin
Mandatory value for naming entity

Description

Significance Retain

Owner Grace Layton

Keywords certificate origin
Important words used in entity

Categories administration

Content
Drag and drop files or click

Binary content container

Original.xls	30.5 kB
Application.pdf	514.8 kB
Examples.ppt	1.7 MB
Certificate of Origin.docx	13.8 kB
Content.txt	3.0 kB

Save Cancel

Image 210: Opening a document version in editing mode

Note: When editing the document version, the values of attributes with the property Versionable will apply only to this version. By changing the values of attributes that do not have this property, the changed values will be saved in all previous versions of the document.

The user can delete an individual version of the document or the versioned document by removing every single version.

4.3.6.4 Creating draft

If the user wants to check in a document version at a later time, he can save it temporarily with the command Save as draft.

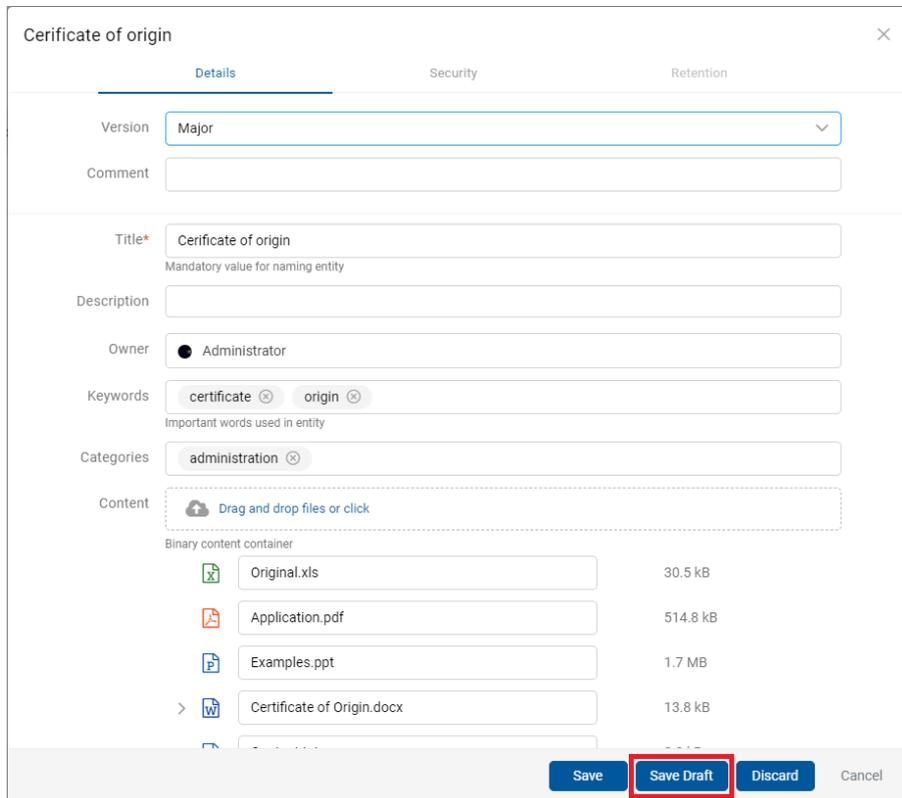


Image 211: Saving a draft for later editing

By selecting the Drafts folder, the left view shows a list of drafts of document versions. The user can review information about the selected document version with the Open command, edit the document draft with the Edit command and remove the draft with the Discard command.

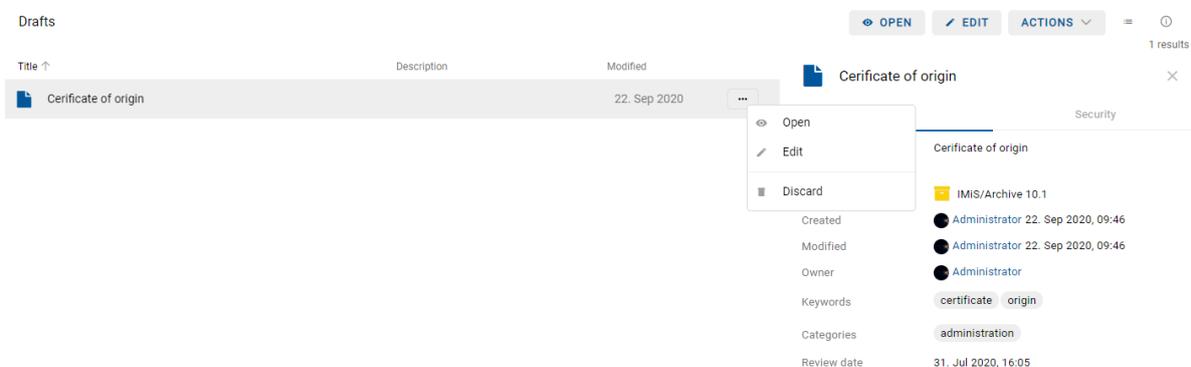


Image 212: A draft of a document version in the Drafts folder

Note: by selecting the  icon, the user defines which columns will be displayed in the review of deleted entities. The user can check or uncheck Description and Modified. The Title of the draft is mandatory.

The created draft is recorded in the list of versions in the section Versions in the display of entity information. The user has the option of opening, editing and discarding the draft.

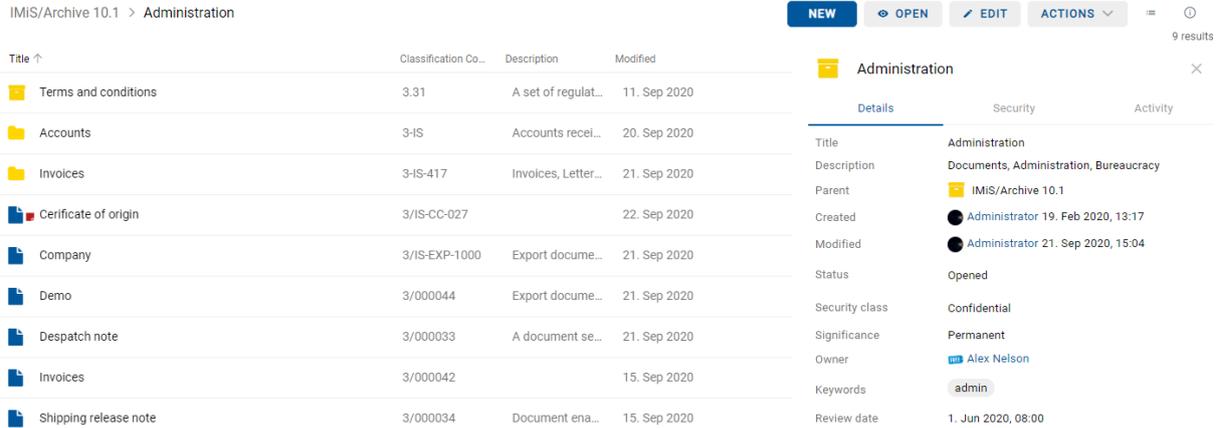


Image 213: Displaying the draft in the list of versions

4.3.6.5 Discarding draft

The user can discard a document draft with the Discard command, thus destroying it.

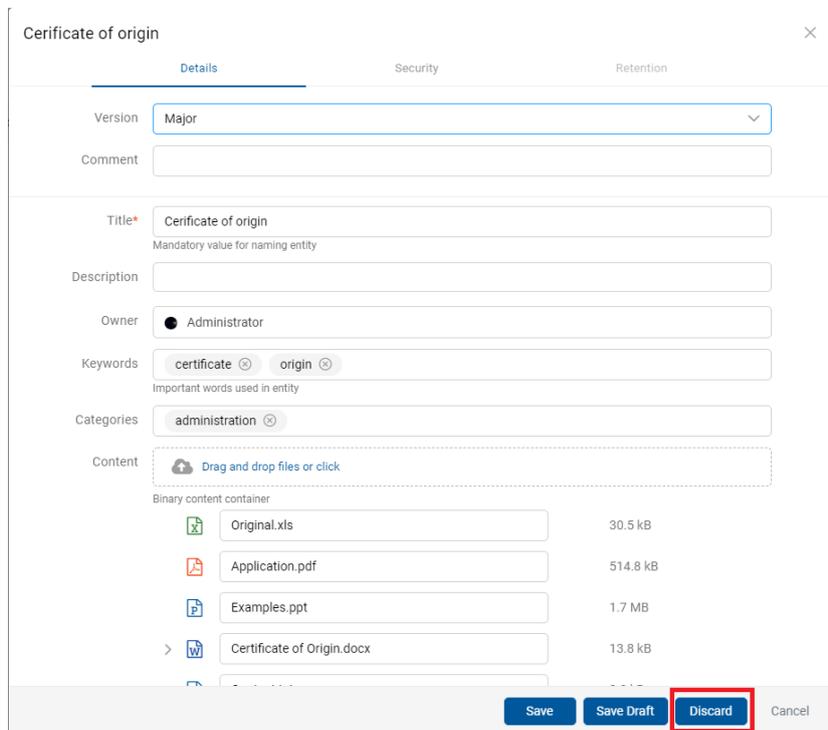


Image 214: Discarding a document draft with the Discard command

4.3.6.6 Checking in draft

The user checks in a version of a document saved in the Drafts folder by selecting the Save command in the bottom command bar.

Image 215: Reviewing a draft before checking it in with the Save command

After checking in the draft, the user is redirected to the display of the parent document, a version of which was created by checking in the draft.

4.3.7 Search functions

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

- Metadata of the class, folder and document.
- Actual value of the content metadata.
- 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:

- Recent
- Advanced.

Recent

If the user has previously performed searches, the search history is shown by selecting the search box in the section “Recent”. The list contains only the last 5 searches, while older searches are saved to the user profile (chapter [The Search history tab](#)).

The user has the option of deleting the search history with "Remove".

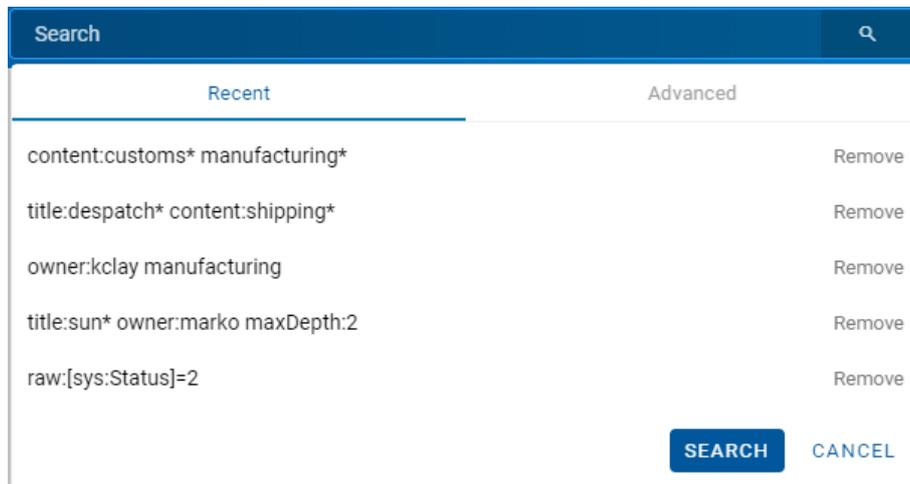


Image 216: Search history

Advanced

The user performs a new search by first selecting the search box. By entering values in the relevant boxes in the section “Advanced” in the dialog box, the user defines the search conditions. The search begins by selecting the action “Search”.

If the user first selects one of the last 5 searches in the section “Recent” and then the section “Advanced”, the search conditions for the selected search appear. These can be modified or supplemented if need be.

Image 217: Advanced search settings

By selecting the icon , a dialog box opens for setting the attributes for defining the search conditions. In the menu, the user is offered both the system attributes and the custom attributes.

Attribute	Visibility
Scope	<input checked="" type="checkbox"/>
Recursive	<input checked="" type="checkbox"/>
Max depth	<input type="checkbox"/>
Full text search	<input checked="" type="checkbox"/>
Title	<input checked="" type="checkbox"/>
Include	<input checked="" type="checkbox"/>
Owner	<input checked="" type="checkbox"/>
Keywords	<input checked="" type="checkbox"/>
Date modified	<input checked="" type="checkbox"/>
Content description	<input checked="" type="checkbox"/>
Review date	<input checked="" type="checkbox"/>
String Max	<input type="checkbox"/>
String 200	<input type="checkbox"/>
Covid	<input type="checkbox"/>
Date Time	<input type="checkbox"/>
Date	<input type="checkbox"/>
Time	<input type="checkbox"/>
UInt 64	<input type="checkbox"/>

Image 218: Setting the attributes to define the search conditions

By moving the icon  in front of the title of the attribute for defining the search conditions up or down, the user defines the sequence of the display of attributes in the search dialog box.

By confirming the selection (“Save”), the display settings are saved to the user profile and the set of displayed attributes for defining the search conditions is adjusted accordingly. The user selects “Reset” for the default display settings. By selecting the icon  or the “Cancel” button, the settings are not saved.

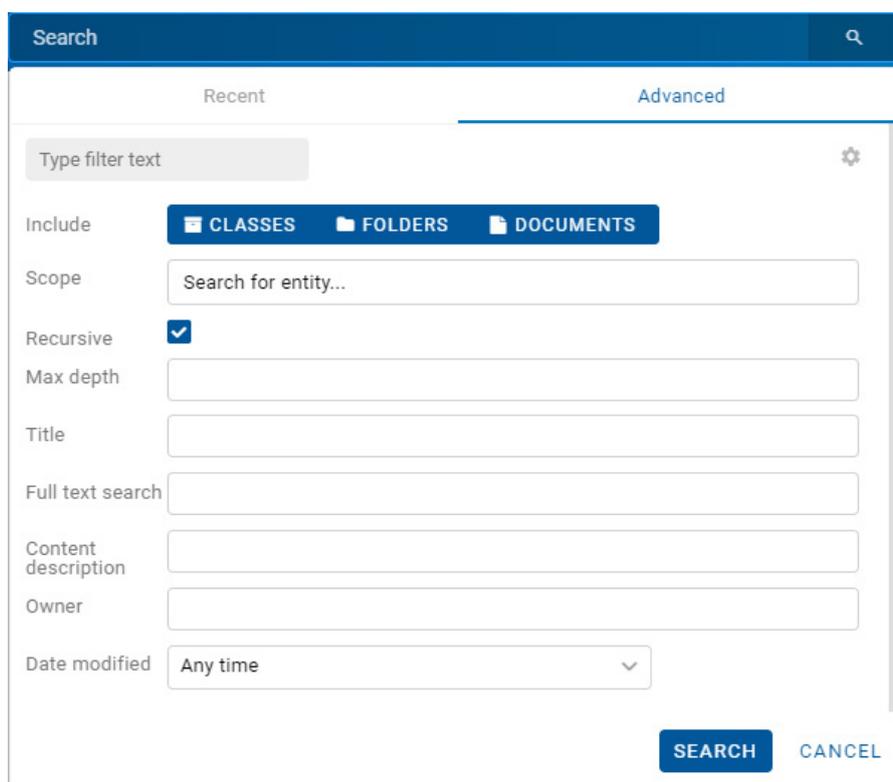


Image 219: Displaying the set of attributes for defining the search conditions

The user has the option of filtering the attributes for defining the search conditions. By entering text in the Type filter text field, the set of displayed attributes is limited accordingly.

***Example 1:** The user previously searched by the value of the attribute Full text search = STATE DEPARTMENT. The user enters the search string “sc” in the Type filter entity field. The set of attributes which will be searched is limited to attributes with titles containing the search string “sc”. Additionally, the set of attributes for the search also contains the attribute Full text search with the value STATE DEPARTMENT.*

Search [magnifying glass icon]

Recent | **Advanced**

Type filter text [input field] [gear icon]

Include: [CLASSES] [FOLDERS] [DOCUMENTS]

Scope: [Development x]

Recursive:

Max depth: [4]

Title: [input field]

Full text search: [state department]

Content description: [input field]

Owner: [Alex Nelson]

Date modified: [Any time v]

[SEARCH] [CANCEL]

Image 220: Before entering the text of limiting the set of attributes for the search

Search [magnifying glass icon]

Recent | **Advanced**

sc [input field] [gear icon]

Scope: [Development x]

Recursive:

Max depth: [4]

Full text search: [state department]

Content description: [input field]

Owner: [Alex Nelson]

[SEARCH] [CANCEL]

Image 221: After entering the text of limiting the set of attributes for the search

Example 2: Building on the previous example, the user removes the value *GENUINE* from the field for entering the value of the attribute *Full text search*. The user reenters the search string “*sc*” in the *Type filter entity* field and performs the search. The set of displayed attributes which will be searched is additionally limited to attributes with titles containing the search string “*sc*”.



Image 222: Example of limiting the set of attributes for the search

4.3.7.1 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 or “Enter” on the keyboard.

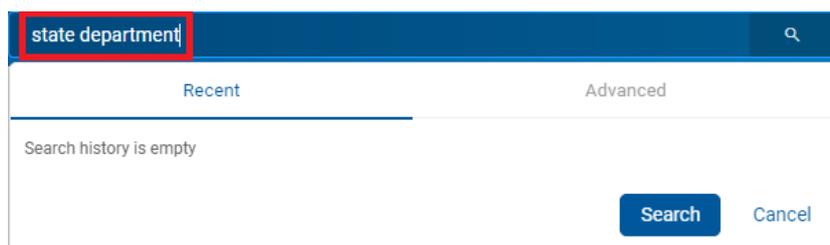


Image 223: Entering a search string in the Search field

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

The screenshot shows the 'Search' dialog box with the 'Advanced' tab selected. At the top, there are tabs for 'Recent' and 'Advanced'. Below them is a 'Type filter text' field with a gear icon. The main search area includes:

- 'Scope' field with placeholder text 'Search for entity...'
- 'Recursive' checkbox which is checked.
- 'Max depth' empty text input field.
- 'Full text search' field containing the text 'state department', which is highlighted with a red rectangular border.
- 'Title' empty text input field.
- 'Include' section with three buttons: 'CLASSES', 'FOLDERS' (which is selected and highlighted in blue), and 'DOCUMENTS'.
- 'Owner' field showing a user icon and the name 'Grace Layton'.
- 'Keywords' empty text input field.
- Below the 'Keywords' field, the text 'Important words used in entity' is displayed.
- At the bottom right, there are two buttons: 'SEARCH' and 'CANCEL'.

Image 224: Entering a search string in the Full text search field

The user has the option of filtering the attributes whose values will be used for the search. By entering text in the Type filter entity field, the set of displayed attributes is limited accordingly.

This screenshot shows the same 'Search' dialog box, but with the 'Type filter text' field at the top containing the letter 's'. The 'Full text search' field is now empty. The 'Recursive' checkbox is still checked. The 'Include' section remains the same with 'FOLDERS' selected. The 'Owner' field still shows 'Grace Layton'. The 'Keywords' field is empty. The 'Important words used in entity' text is still present. The 'SEARCH' and 'CANCEL' buttons are at the bottom right.

Image 225: Entering text to limit the set of attributes for the search

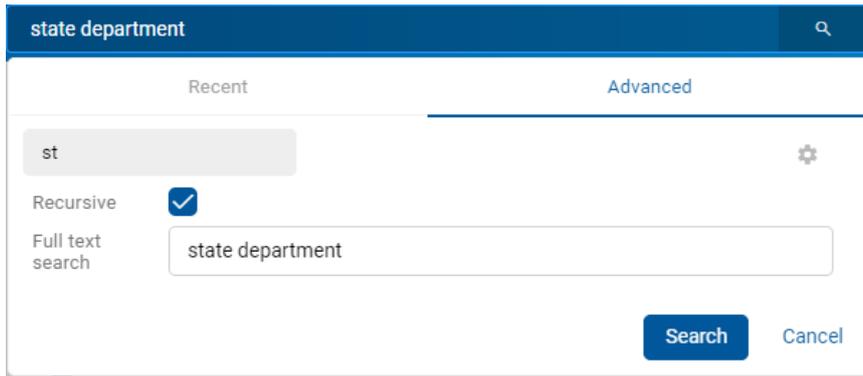


Image 226: Example of limiting the set of attributes for the search

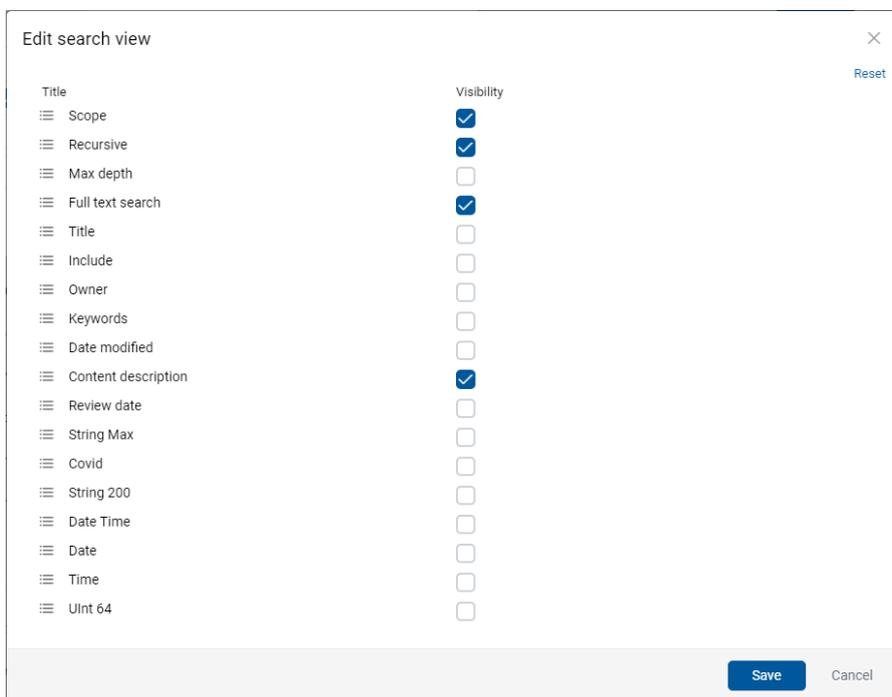


Image 227: Limiting the set of attributes for the search via the menu

After confirming the search, the user is shown the search results list in the central view.

For each document containing content with the search string all versions of the content are shown with their titles, content type and icon.

By selecting the title (version) of the content, the document opens and shows the contents in preview mode.

IMIS/Archive 10.1		
Title ↑	Classification Code	Modified
Certificate of origin	3/IS-CC-027	22. Sep 2020
Examples.ppt		
Certificate of Origin.docx		
Certificate of Origin.pdf		
Contracts	5/000174	9. Oct 2020
1 data (2).pdf		
1.1 data (2).pdf		
1.2 Slovenian_distributor.pdf		
1 Sample Contracts (1).pdf		
1.1 Sample Contracts (1).pdf		
1.2 Sample Contract.pdf		

Image 228: Search results list showing content versions

The user can create a search string from one or multiple simple search conditions. When searching by the full text of the document content, an exact match to the metadata value is not necessary. For more information on searching by partial values see chapter [Wildcard search](#).

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.
- 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).

4.3.7.2 Searching by Metadata

The user can search by metadata by first selecting the field for entering the search string in the header of the user interface. In the “Search” dialog box in the section “Advanced”, the user has the following fields available:

- Scope: the entity under which the search will be implemented.
- Recursive: checking this parameter means that the search is implemented on the selected entity and on all contained entities. On the contrary, by unchecking this parameter, the user limits the search to the selected entity and the 1st level of contained entities.
- Max depth: the numerical value defines the maximum search depth.

Example: Setting the value “Search depth = 2” means that the search will be performed up to and including level 2 of the selected entity tree.

- Full text search: searching by the text of the content.
- Include: the type of entity for which the search will be performed. All entity types – documents, folders and classes are set by default. If all types or none are selected in the search dialog box, all entities are searched.
- Title: name of the entity.
- Owner: owner of the entity.
- Keywords: keywords related to the entity.
- Date modified: date of the last entity modification.

Image 229: A dialog box for searching by metadata

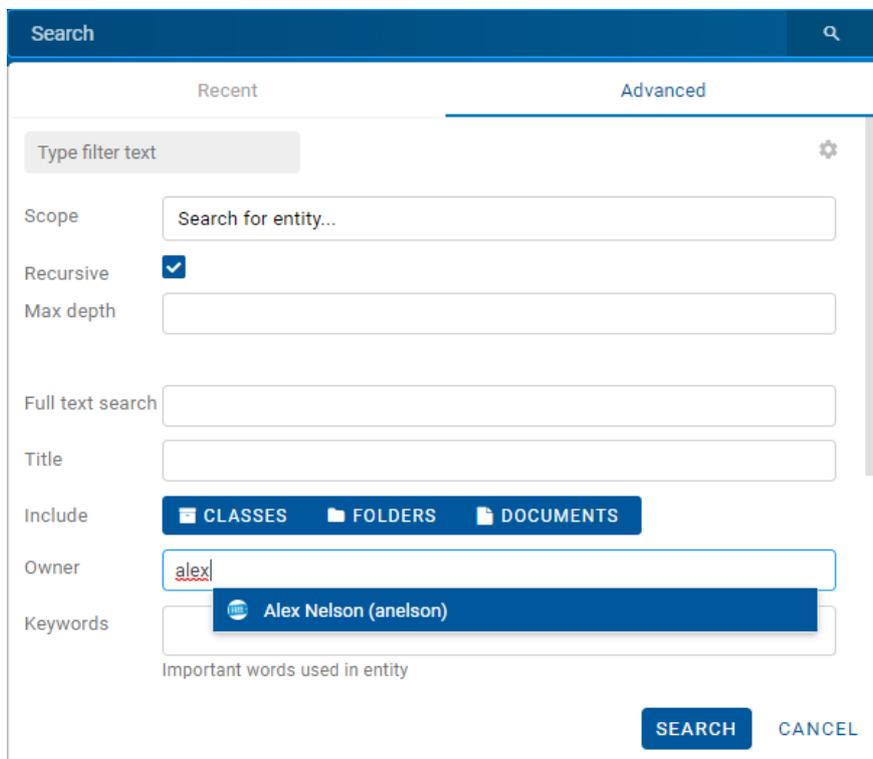
Besides the above-mentioned attributes, the user can also search by Custom attributes. The set comprises the attributes which are used in at least one entity.

Image 230: A dialog box for searching by custom metadata

When choosing text metadata, the value must be entered. When searching text metadata, the value does not have to be identical. For more information on searching by partial values see chapter [Wildcard search](#).

When searching metadata whose value is represented by the name of an IMiS®/ARChive Server user (for example the metadata Owner) 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. To start the search, it is enough to enter two characters from the search string.



The image shows a 'Search' dialog box with the following fields and options:

- Scope:** Search for entity...
- Recursive:**
- Max depth:** (empty text box)
- Full text search:** (empty text box)
- Title:** (empty text box)
- Include:** CLASSES, FOLDERS, DOCUMENTS
- Owner:** alex
- Keywords:** Alex Nelson (anelson)

Buttons: SEARCH, CANCEL

Image 231: A dialog box for searching by the metadata Owner

When searching by date, the user selects the icon  or field for defining the value. From the list, the user selects the appropriate date and time of the start and/or end of date validity.

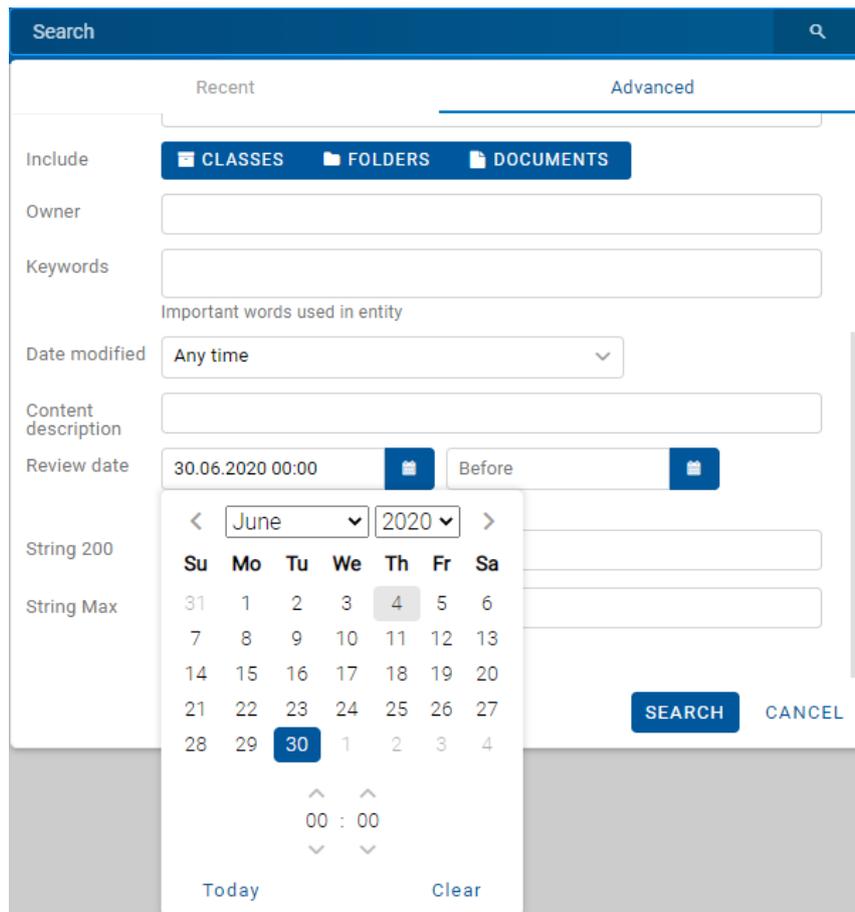


Image 232: Defining the time range for searching by date

4.3.7.3 Searching by Content descriptions

The user searches by the document content by first selecting the field for entering the search string in the header of the user interface. In the “Search” dialog box in the section “Advanced”, the user enters the search string into the Content description field.

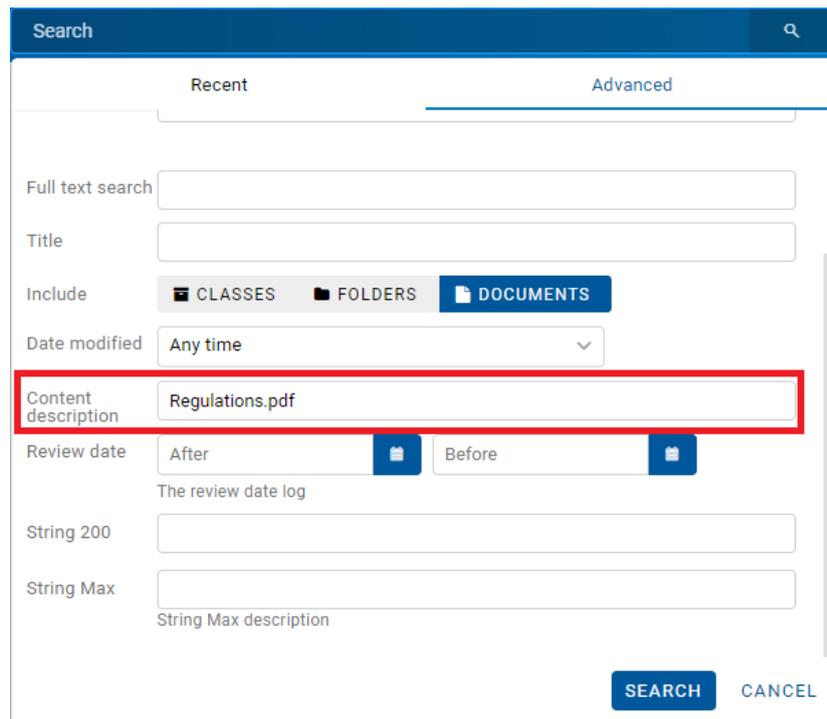


Image 233: A dialog box for searching by the content description

4.3.7.4 Wildcard search

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.

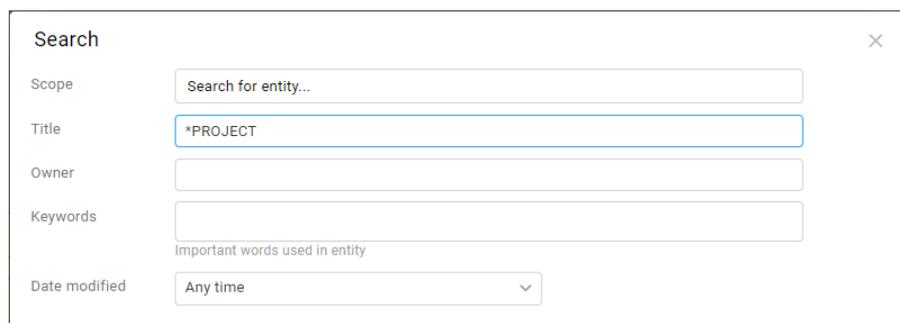


Image 234: Use of special characters in a search string

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"

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, ...)

The search result is shown in the central view of the user interface.

4.3.7.5 Searching by actual value

The user searches by actual value by entering the search string in the search box in the header of the user interface. The search string can consist of one or multiple simple search conditions, beginning with the string “raw:”.

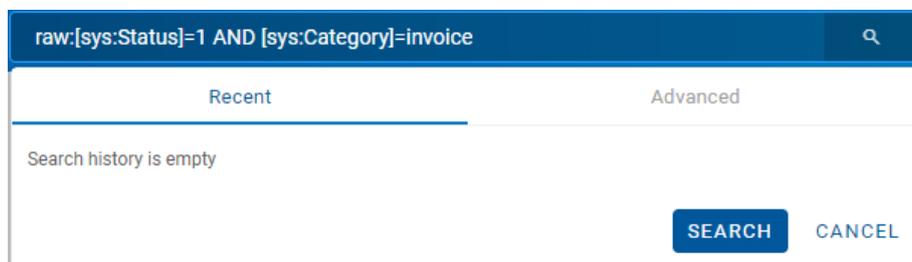


Image 235: The search string and the results of searching by actual value

4.3.7.6 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 the title of the document content by first selecting the field for entering the search string in the header of the user interface. In the “Search” dialog box in the section “Advanced”, the user enters the search strings into the relevant fields.

Note:

The combined search takes the logical operator AND into account.

4.3.7.6.1 Combined search by Metadata and Full text search

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

The screenshot shows the 'Advanced' search tab in the IMiS application. The search bar at the top contains 'owner:kclay manufacturing'. Below the search bar, there are several filter options: 'Type filter text' (empty), 'Scope' (Administration), 'Recursive' (checked), 'Full text search' (manufacturing), 'Title' (empty), 'Owner' (Keira Clay), 'Date modified' (Any time), 'Content description' (empty), and 'Date Time' (After/Before). The 'Full text search' and 'Owner' fields are highlighted with red boxes. At the bottom right, there are 'SEARCH' and 'CANCEL' buttons.

Image 236: Entering a search string in a combined search

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. Full text search = manufacturing).

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

IMiS/Archive 10.1 > Administration

Title ↑	Classification Code	Modified
 Customs documentation	3/000032	2. Jul 2020
 Customs declaration.pdf		

Image 237: Result of searching by metadata and the full text of the content

4.3.7.6.2 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 = despatch*) and whose content descriptions also contain the searched text (e.g. shipping*).

The screenshot shows the search interface with the search string `title:despatch* content:shipping*` entered in the search bar. The interface is in the 'Advanced' search mode. The search criteria are as follows:

- Scope: Administration
- Recursive:
- Full text search: (empty)
- Title: despatch*
- Owner: (empty)
- Date modified: Any time
- Content description: shipping*
- Date Time: After (Before is also available)

Buttons for 'SEARCH' and 'CANCEL' are visible at the bottom right.

Image 238: Entering a search string when searching by metadata and the content description

The screenshot shows the search results for the query `title:despatch* content:shipping*`. The results are displayed in a table under the path 'IMiS/Archive 10.1 > Administration'.

Title ↑	Classification Code	Modified
Despatch note	3/000033	1. Jul 2020
Shipping note		

Image 239: Result of searching by metadata and the content description

4.3.7.6.3 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. Content descriptions = customs*) and whose content also contains the searched text (e.g. Full text search = manufacturing).

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

The screenshot shows the 'Search' interface with the 'Advanced' tab selected. The search criteria are as follows:

- Scope: Administration
- Recursive:
- Full text search: manufacturing*
- Title: (empty)
- Owner: (empty)
- Date modified: Any time
- Content description: customs*
- Date Time: After

Buttons for 'SEARCH' and 'CANCEL' are visible at the bottom right.

Image 240: Entering a search string when searching by the text of the content and the content description

The search results are displayed under the breadcrumb 'IMiS/Archive 10.1 > Administration'. The search criteria 'content:customs* manufacturing*' are shown at the top. The results are as follows:

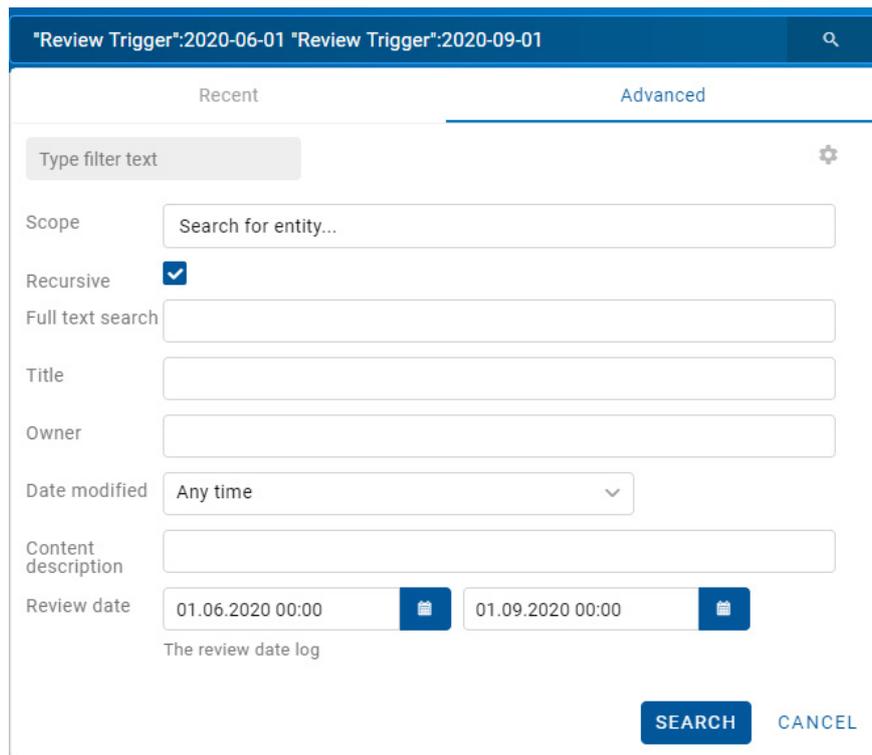
Title ↑	Classification Code	Modified
Customs documentation	3/000032	2. Jul 2020
Customs declaration.pdf		
Customs notice.docx		

Image 241: Displaying the result of searching by the text of the content and the content description

4.3.7.6.4 Search by Custom metadata

The user performs a combined search by the title of the document content by first selecting the field for entering the search string in the header of the user interface.

The user searches by custom metadata by first selecting the field for entering the search string in the header of the user interface. In the “Search” dialog box in the section “Advanced”, the user enters the search string into the selected custom field.



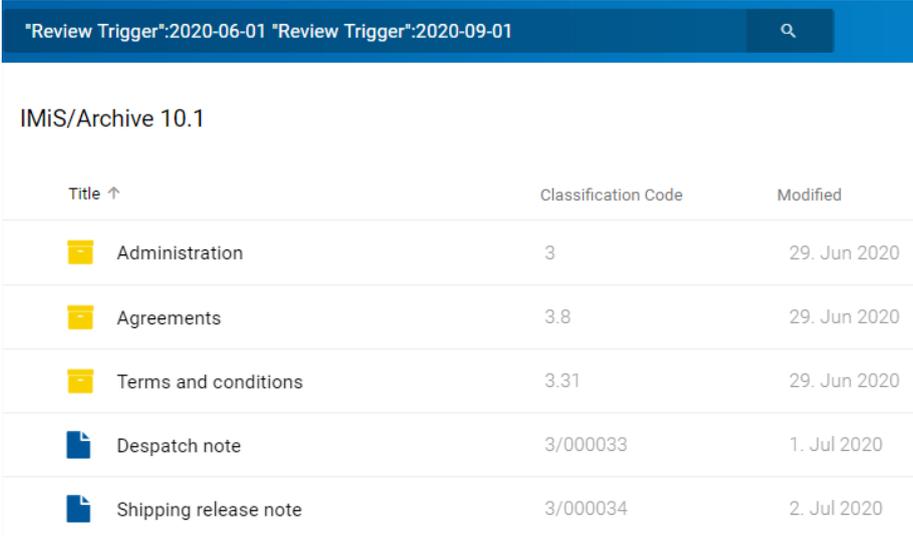
The screenshot displays the 'Advanced' search dialog box. At the top, there are two tabs: 'Recent' and 'Advanced', with 'Advanced' being the active tab. Below the tabs is a search bar with the placeholder text 'Type filter text'. The main area contains several search criteria:

- Scope:** A text input field with the placeholder 'Search for entity...'.
- Recursive:** A checked checkbox.
- Full text search:** A text input field.
- Title:** A text input field.
- Owner:** A text input field.
- Date modified:** A dropdown menu currently set to 'Any time'.
- Content description:** A text input field.
- Review date:** Two date range inputs. The first is '01.06.2020 00:00' and the second is '01.09.2020 00:00'. Both have calendar icons to their right. Below these is the text 'The review date log'.

At the bottom right, there are two buttons: 'SEARCH' and 'CANCEL'.

Image 242: Entering the search string when searching by a custom attribute

The search result is all the documents whose date values of the custom attribute “Review date” is between June 1st and September 1st



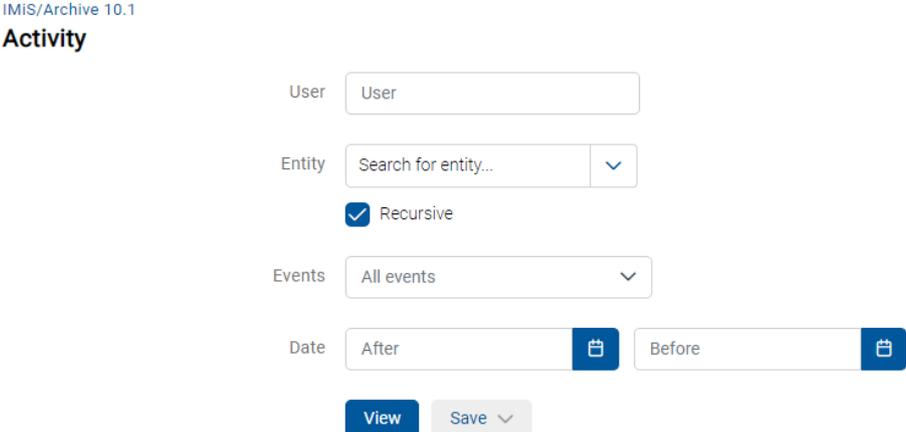
The screenshot shows a search bar with the string: "Review Trigger":2020-06-01 "Review Trigger":2020-09-01. Below the search bar, the results are displayed under the heading "IMiS/Archive 10.1". The results are in a table with columns: Title, Classification Code, and Modified.

Title ↑	Classification Code	Modified
 Administration	3	29. Jun 2020
 Agreements	3.8	29. Jun 2020
 Terms and conditions	3.31	29. Jun 2020
 Despatch note	3/000033	1. Jul 2020
 Shipping release note	3/000034	2. Jul 2020

Image 243: Entering the search string when searching by a custom attribute

4.3.7.7 Searching Audit log events

By selecting the action Activity, a dialog box opens for searching for information on audit log events.



The screenshot shows the "Activity" search dialog box. It includes the following fields and options:

- User: User
- Entity: Search for entity... (dropdown menu)
- Recursive
- Events: All events (dropdown menu)
- Date: After (calendar icon) Before (calendar icon)
- Buttons: View, Save (dropdown arrow)

Image 244: Selecting an entity in the entity tree

The user can specify the following settings:

- User: by entering the search string, the user selects the directory entity from the list to display information on selected audit log events.



Image 245: Selecting a directory entity from a list

- Entity: the user can select or define one of the following search modes based on which the information on selected audit log events will be shown:
 - Browse mode: selects an entity in the entity tree.

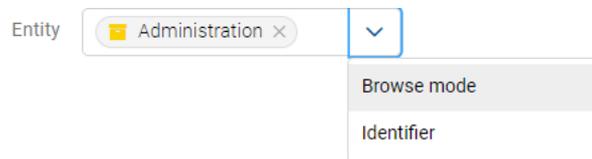


Image 246: Selecting an entity in the entity tree

- Identifier: defines a unique entity identifier on the server.

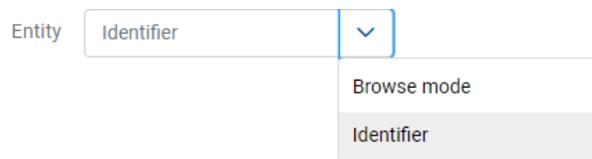


Image 247: Defining an entity identifier

- Recursive: checking this parameter means that the search is implemented on the selected entity and on all contained entities. On the contrary, by unchecking this parameter, the user limits the search to the selected entity and the first level of sub-entities.

- Events: selecting the audit log events for which the information will be displayed.

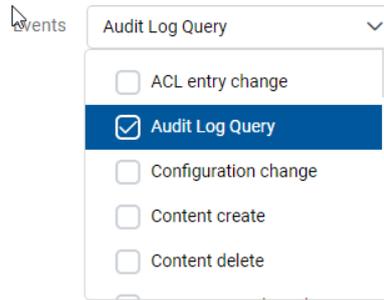


Image 248: Selecting audit log events

- After: start of the time period for displaying information on audit log events.
- Before: end of the time period for displaying information on audit log events.

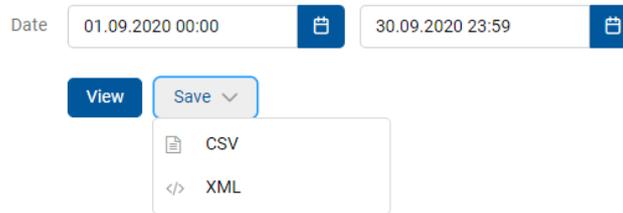


Image 249: Setting the parameters for searching by audit log events

By selecting the action View, a list of audit log events that match the search criteria is shown by pages.

By selecting the action Save, a popup menu appears with the possible formats (CSV, XML) for saving information on audit log events.

	A	B	C	D	E	F	G	H	I	J
1	Sequence Time	User	Address	Computer	InternalAddress	Id	ClassificationCode	Event Type	EventDetails	
2	11 2020-04-01T09:00:24Z	anelson	127.0.0.1	SERVER		RSURRqVPiU7y7_zbaLvA471ogfUly1m	C=3* C=8	ENTITY_REVIEWED	Retention policy conflict. No default reason available.	
3	10 2020-04-01T09:00:24Z	anelson	127.0.0.1	SERVER		XB8d_bpjVjUoGxaD_0jm06OIdI-R2fk1	C=3* F=2020-000030	ENTITY_REVIEWED	Retention policy conflict. No default reason available.	
4	9 2020-04-01T09:00:24Z	anelson	127.0.0.1	SERVER		ijddH_jP2Tbdj@hQMIrEeLSP4A2SKDr	C=3* F=2020-000030* D=000001	ENTITY_REVIEWED	Retention policy conflict. No default reason available.	
5	8 2020-03-19T13:27:48Z	anelson	192.168.50.15	Mozilla/5.0	2a01:260:4086:1282:100::b	_oGEGUVjglUjMjDCOAGhTrkSqhénAPV3_	C=3* D=000034	ENTITY_OPEN_READ_ONLY		
6	7 2020-03-19T13:27:28Z	anelson	192.168.50.15	Mozilla/5.0	2a01:260:4086:1282:100::b	_-92axjNwA7yNwVeVjI9q1XgFqQKWCEn	C=3* D=000033	ENTITY_OPEN_READ_ONLY		
7	6 2020-03-17T15:00:13Z	anelson	192.168.50.15	Mozilla/5.0	2a01:260:4086:1282:100::c	RSURRqVPiU7y7_zbaLvA471ogfUly1m	C=3* C=8	ENTITY_OPEN_READ_WRITE		
8	5 2020-03-17T07:55:31Z	anelson	192.168.50.15	Mozilla/5.0	192.168.100.51	UISxlqUKX70ano1FhnLNnV_G2TjTR71	C=3	ENTITY_SAVE		
9	4 2020-03-17T07:55:31Z	anelson	192.168.50.15	Mozilla/5.0	192.168.100.51	UISxlqUKX70ano1FhnLNnV_G2TjTR71	C=3	PROPERTY_VALUE_CHANGE	Changed properties: sys:Externalids	
10	3 2020-03-17T07:55:20Z	anelson	192.168.50.15	Mozilla/5.0	192.168.100.51	UISxlqUKX70ano1FhnLNnV_G2TjTR71	C=3	ENTITY_OPEN_READ_WRITE		
11	2 2020-03-12T14:12:03Z	anelson	192.168.50.15	Mozilla/5.0	2a01:260:4086:1282:100::5	XB8d_bpjVjUoGxaD_0jm06OIdI-R2fk1	C=3* F=2020-000030	ENTITY_SAVE		
12	1 2020-03-12T14:12:03Z	anelson	192.168.50.15	Mozilla/5.0	2a01:260:4086:1282:100::5	XB8d_bpjVjUoGxaD_0jm06OIdI-R2fk1	C=3* F=2020-000030	PROPERTY_VALUE_CHANGE	Changed properties: sys:Category, sys:Keywords	
13	0 2020-03-12T14:11:33Z	anelson	192.168.50.15	Mozilla/5.0	2a01:260:4086:1282:100::5	XB8d_bpjVjUoGxaD_0jm06OIdI-R2fk1	C=3* F=2020-000030	ENTITY_OPEN_READ_WRITE		

Image 250: Saving audit log events in the CSV format

```
<?xml version="1.0" encoding="UTF-8"?>
<auditlog.query.resultset xsi:schemaLocation="http://www.imis.si/imisarc http://www.imis.si/imisarc/auditlog.xsd" xmlns="http://www.imis.si/imisarc" xmlns:xsi="http://
<sessions>
  <!--Audit query sessions.-->
  <session id="1098" closureReason="0" address="192.168.50.15" internal_address="2a01:260:4086:1282:100::5" dateTimeOpened="2020-03-12T09:10:12Z" username="anelson"
  <session id="1196" closureReason="0" address="192.168.50.15" internal_address="192.168.100.51" dateTimeOpened="2020-03-17T06:01:08Z" username="anelson" computerNa
  <session id="1222" closureReason="0" address="192.168.50.15" internal_address="2a01:260:4086:1282:100::c" dateTimeOpened="2020-03-17T14:44:31Z" username="anelson"
  <session id="1357" closureReason="0" address="192.168.50.15" internal_address="2a01:260:4086:1282:100::b" dateTimeOpened="2020-03-19T13:26:57Z" username="anelson"
  <session id="1954" closureReason="0" address="127.0.0.1" dateTimeOpened="2020-04-01T09:00:24Z" username="anelson" computerName="SERVER"/>
</sessions>
<events>
  <!--Audit query events.-->
  <!--Sort compare function is QuerySorter::CompareSESS_TS-->
  <event sessionId="1098" type="3" seq="0" dateTime="2020-03-12T14:11:33Z" classificationCode="C=3^F=2020-000030" context="XB8d_bpJvJuoGxaD_0jm060IDi-R2fk1"/>
  <event sessionId="1098" type="9" seq="1" dateTime="2020-03-12T14:12:03Z" classificationCode="C=3^F=2020-000030" context="XB8d_bpJvJuoGxaD_0jm060IDi-R2fk1" message
  <event sessionId="1098" type="4" seq="2" dateTime="2020-03-12T14:12:03Z" classificationCode="C=3^F=2020-000030" context="XB8d_bpJvJuoGxaD_0jm060IDi-R2fk1"/>
  <event sessionId="1196" type="3" seq="3" dateTime="2020-03-17T07:55:20Z" classificationCode="C=3" context="UI5xIqUKX70ano1FhnLNlnV_G2TJTR71"/>
  <event sessionId="1196" type="9" seq="4" dateTime="2020-03-17T07:55:31Z" classificationCode="C=3" context="UI5xIqUKX70ano1FhnLNlnV_G2TJTR71" message="Changed prop
  <event sessionId="1196" type="4" seq="5" dateTime="2020-03-17T07:55:31Z" classificationCode="C=3" context="UI5xIqUKX70ano1FhnLNlnV_G2TJTR71" message="get"/>
  <event sessionId="1222" type="3" seq="6" dateTime="2020-03-17T15:00:13Z" classificationCode="C=3^C=8" context="RSUtRqVpti7y7_zbalvA147logFuLy1m"/>
  <event sessionId="1357" type="2" seq="7" dateTime="2020-03-19T13:27:28Z" classificationCode="C=3^D=000033" context="_a2axJNuA7yNlveVJ19qIXgFqQKQwCen"/>
  <event sessionId="1357" type="2" seq="8" dateTime="2020-03-19T13:27:48Z" classificationCode="C=3^D=000034" context="z0GEGUV1gUMJDCOAghTRkSaghnAPV3_"/>
  <event sessionId="1954" type="26" seq="9" dateTime="2020-04-01T09:00:24Z" classificationCode="C=3^F=2020-000030^D=000001" context="ijddh_1P2Tbdj6hQMItToEzLSP4A2SKC
  <event sessionId="1954" type="26" seq="10" dateTime="2020-04-01T09:00:24Z" classificationCode="C=3^F=2020-000030" context="XB8d_bpJvJuoGxaD_0jm060IDi-R2fk1" messa
  <event sessionId="1954" type="26" seq="11" dateTime="2020-04-01T09:00:24Z" classificationCode="C=3^C=8" context="RSUtRqVpti7y7_zbalvA147logFuLy1m" message="Retent
</events>
```

Image 251: Saving audit log events in the XML format

The number of events and users for each day in the selected time period is shown in graphs.



Title	Details	Identifier	Classification Code	User	Delegate	Version	Device name	Address	Internal address	Date ↓
Entity reviewed	Retention policy conflic t. No default reason available	RSURqVPI7y7_zbalvAJ47logFuLy1m	3.8	Alex Nelson			SERVER	127.0.0.1		1. Apr 2020, 11:00
Entity reviewed	Retention policy conflic t. No default reason available	XB8d_bpJvJuoGxaD_0jm060IDi-R2fk1	3-2020-000030	Alex Nelson			SERVER	127.0.0.1		1. Apr 2020, 11:00
Entity reviewed	Retention policy conflic t. No default reason available	ijddh_1P2Tbdj6hQMItToEzLSP4A2SKC	3-2020-000030/000001	Alex Nelson			SERVER	127.0.0.1		1. Apr 2020, 11:00
Entity open read-only		z0GEGUV1gUMJDCOAghTRkSaghnAPV3_	3/000034	Alex Nelson			Edge on Windows 10	192.168.50.15	2a01:260:4086:1282:100::b	19. Mar 2020, 14:27

Image 252: Result of searching by audit log events

By selecting the icon the user defines which information will be shown in the columns.

In the top right part of the view, a popup menu appears with the following options:

- Identifier: unique identifier of the entity on the IMiS®/ARCHive Server.
- Classification code: the entity classification code for displaying information on audit log events.
- User: the name of the selected user for displaying information on audit log events.
- Delegate: a user presented as a person authorized by another user in the authentication process and who executed an operation on that user's behalf.
- Version: the entity version for which data on selected audit log events will be displayed. If it is not a document, the value is empty.

- Device name: the name of the device from where the request to perform an action on the selected entity came.
- Address: the network address from where the request to perform an action on the selected entity came.
- Internal address: the IP address, which is set by opening a new session.

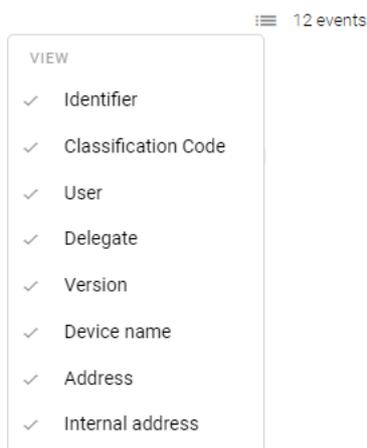


Image 253: Selecting information shown in columns

4.3.8 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.
- Creating and saving email messages based on the template “Email”.

To enable capture, the server must be configured with at least one template that contains email message attributes [Email attributes](#).

4.3.8.1 Capturing received and sent emails

The user can capture a received or sent email directly from the messaging client (MS Outlook, HCL Notes, etc.) and save it to the classification scheme of IMiS®/Archive Server.

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.

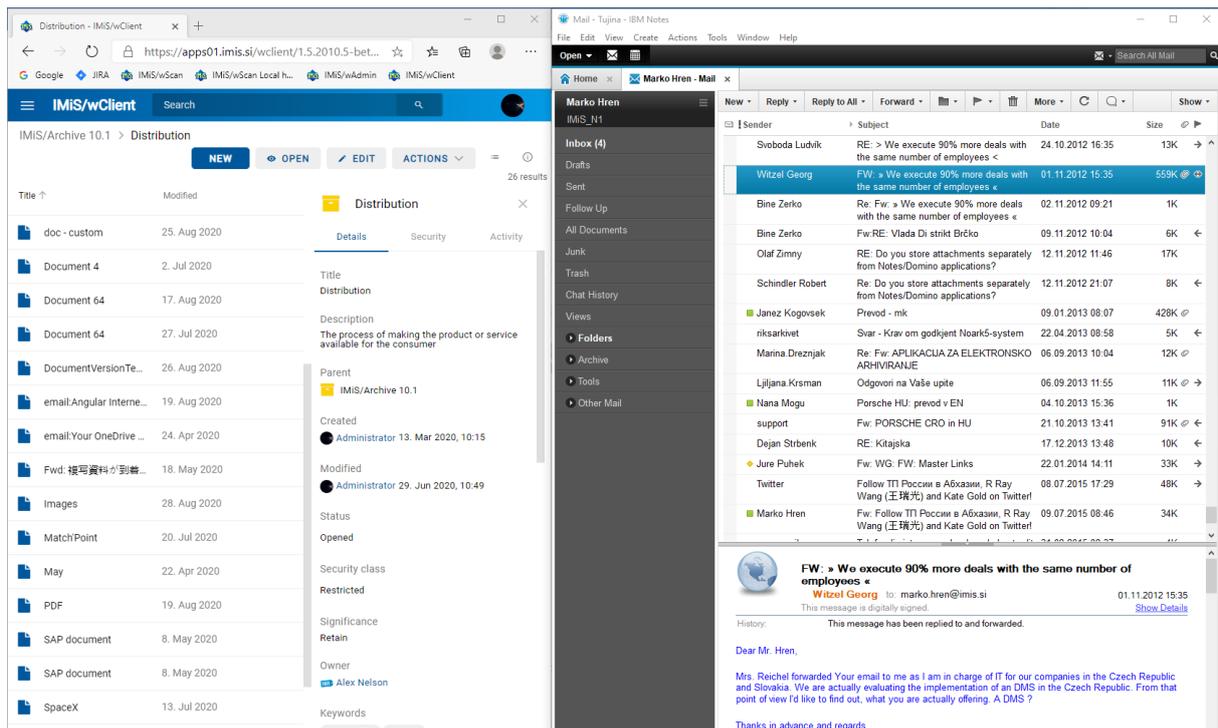


Image 254: Preparing the environment for transferring an email message from the email client to the archive

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 and drags them to the selected class or folder in the classification scheme in 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.

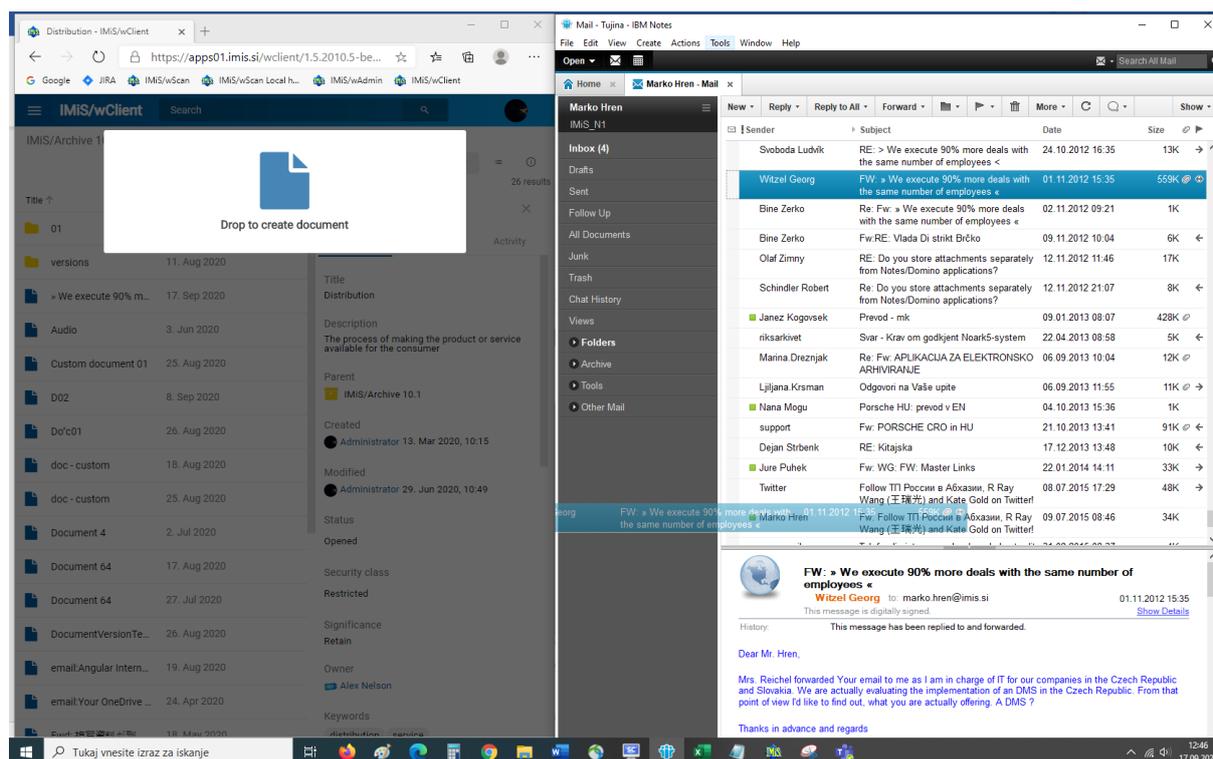


Image 255: Dropping the email message to the selected entity

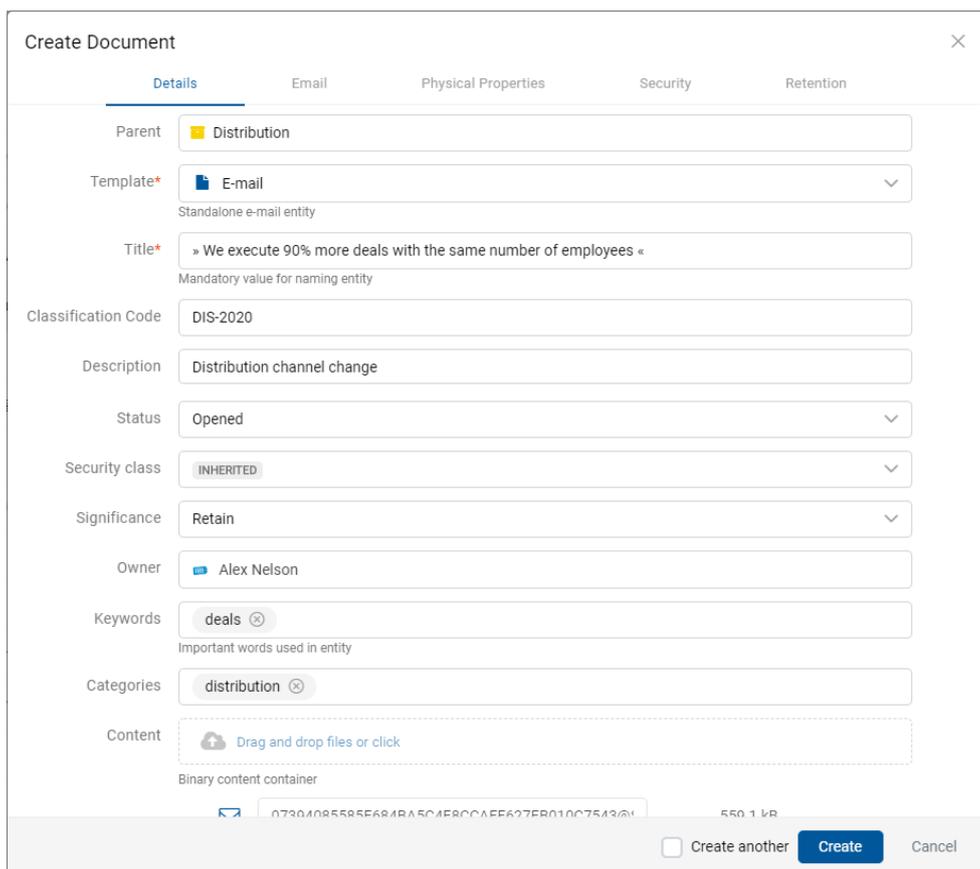
After releasing the mouse button, a dialog box opens for viewing and editing the details of the email message.

4.3.8.1.1 Editing email message data

In the Details tab the user can view or edit the following metadata of the email message:

- 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.
- Title: name of the folder or document described. Attribute value is mandatory.
- Classification code: a manually assigned classification code for the selected entity in the classification scheme.
- Description: Short description of the entity.
- Status: the 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.
- Categories: the entity view mode.
- Content: the content of the email message and attachment, each in its own content. This attribute is read-only.
- External identifiers: a list of the entity's unique external identifiers on the server.



The screenshot shows the 'Create Document' dialog box with the 'Details' tab selected. The form contains the following fields and values:

- Parent: Distribution
- Template*: E-mail (Standalone e-mail entity)
- Title*: » We execute 90% more deals with the same number of employees « (Mandatory value for naming entity)
- Classification Code: DIS-2020
- Description: Distribution channel change
- Status: Opened
- Security class: INHERITED
- Significance: Retain
- Owner: Alex Nelson
- Keywords: deals (Important words used in entity)
- Categories: distribution
- Content: Binary content container (550.1 kB)

At the bottom of the dialog, there is a checkbox for 'Create another', a 'Create' button, and a 'Cancel' button.

Image 256: Viewing and editing the details of an email message before saving

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.

If the user wants to create a new entity immediately after creating the entity (email message) in the classification scheme, the user can do so by checking the parameter “Create another”.

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.

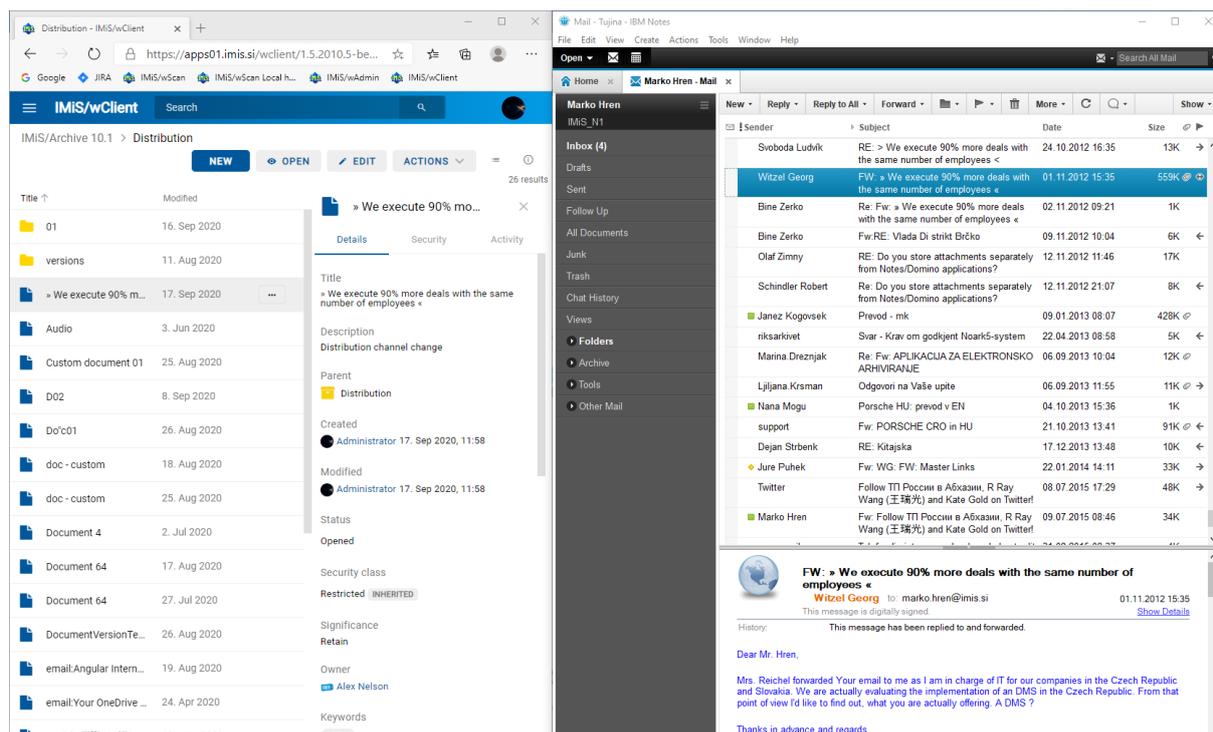


Image 257: Displaying a saved email message on the list of entities

In the Details tab, the user can see all the content that was saved together with the email message in the editing mode. In the Content field the original email message in the EML format and the recognized email attachments are created. Adding new contents is disabled, as is the execution of actions on the contents shown on the list.

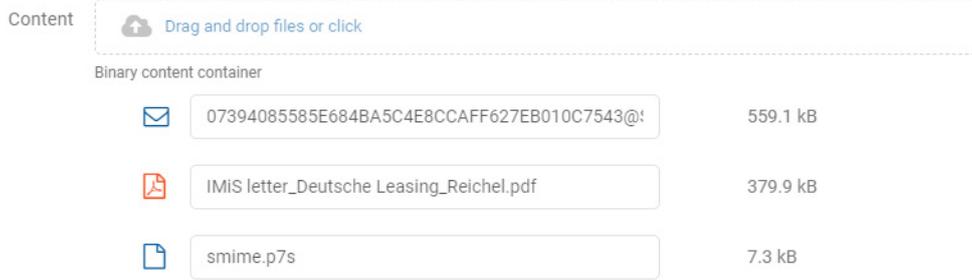


Image 258: Contents of the email message

4.3.8.2 Creating email messages

A user can create an email message by selecting the relevant template from the set of available templates.

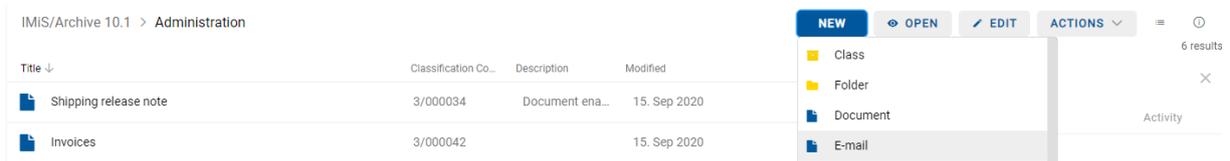


Image 259: Selecting a template for creating an email message

The user selects a file in the EML format from the file system.

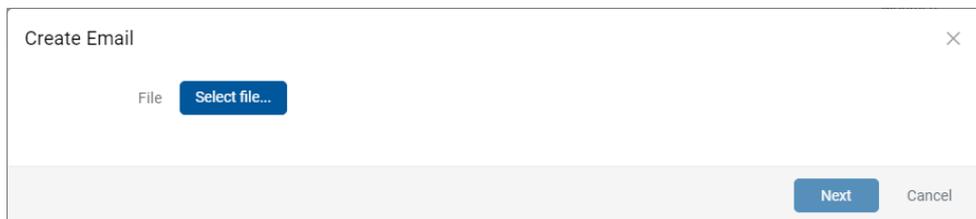


Image 260: Selecting an EML file

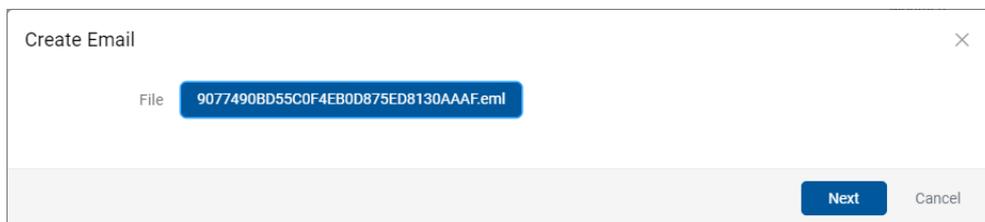


Image 261: Confirming the selection of an EML file

After selecting the action “Next”, the user is shown the email message data, which the user can then review and edit the next entity metadata.

For more information see chapter [Editing email message data](#).

4.3.8.3 Functionality description

After viewing and confirming the email message with the Create button, the content of the email message is parsed at the level of IMiS®/ARChive Server (version 10.1.2010 or above) and is copied to the appropriate 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 and is visible to the user in the Email tab:

- 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.

The Date and Sender email metadata are mandatory.

If one of these is not successfully captured, the message will not be saved.

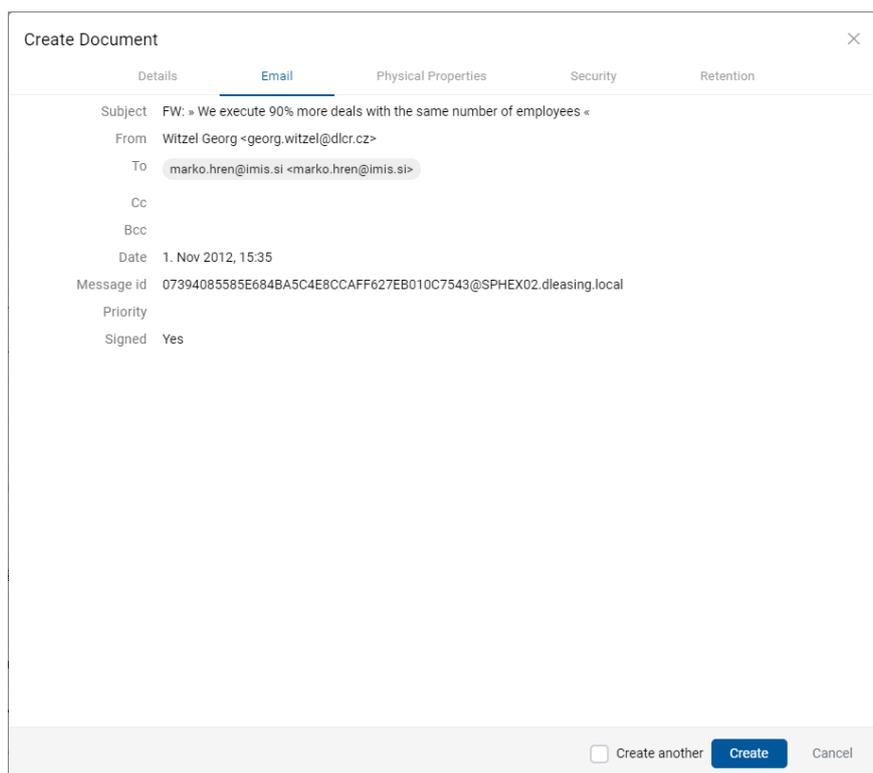


Image 262: Display of the metadata transferred from the email message

In the Physical Content tab the user can add information about the physical content.

In the Security tab the user with the Change permissions permission can change the access permissions of directory entities (users, groups, attributes).

Warning:

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

4.3.9 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 chapter [Rules in the IMiS®/ARChive Server Manual](#).

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

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.

In case authenticity evidence for the selected entity already exists on the archive, the user can obtain authenticity evidence also by selecting the icon **GET** in the set More of the Details tab in the right view.

The screenshot shows the 'Certificate of origin' details in the 'Details' tab. The 'Authenticity evidence' section is highlighted with a red box, and the 'Get' button next to it is also highlighted. The interface includes a top navigation bar with buttons for 'NEW', 'OPEN', 'EDIT', and 'ACTIONS'. The main content area displays various metadata fields for the certificate, including title, description, parent, creation and modification dates, status, security class, significance, owner, keywords, categories, review date, versions, retention, and more. The 'More' section includes fields for Classification Code, Template, Type, and Permanent status. The 'Authenticity evidence' section shows a 'Get' button and a table with columns for 'Opened' and 'Identifier'.

Opened	Identifier
29. Apr 2020, 15:34	BMtozc348swzj1NCsyWXEaUH44UD65j4

Image 263: Obtaining authenticity evidence in the Details tab

The notification bar in the bottom part of the user interface shows the information about saving a file with authenticity evidence.

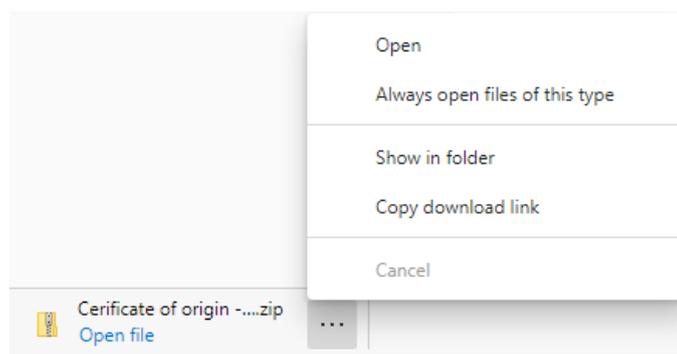


Image 264: Information for the user about saving a directory with authenticity evidence

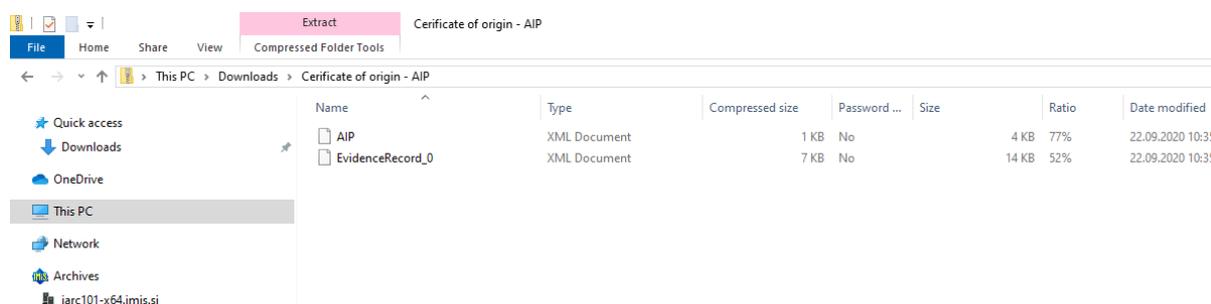


Image 265: A directory with two files containing authenticity evidence

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...T5irp0T+SrJMp+VE=</ds:DigestValue>
  </aip:ContentValue>
</aip:Content>
</aip:AIP>

```

Image 266: Example archive information package

```

<?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>RiHMqrrhGATA/fDYJVO2IVg4ftw=</DigestValue>
<DigestValue>dawWHxN2luddA70+NGHYNd3ApG8=</DigestValue>
</Sequence>
<Sequence Order="2">
<DigestValue>vqBEIqW7kGPUaFB/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>j8bwhFukHoD6jcmzgEZtXDF/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-13ED106F54C2C33ED42000000000007BD7">
<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/XIbNsA=</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>
</dsig:Signature>
</TimeStampToken>
<CryptographicInformationList>
<CryptographicInformation Order="1"
Type="CERT">MIIEHDCCAwSgBAGlE...z9Oz6gk/2vorAfGEhuB9nBxVeoQp</CryptographicInformation>
<CryptographicInformation Order="2"
Type="CRL">MIISKTCCECAQEwDQYJ...pYO2SYQMkw819LR9I/Y0Fg</CryptographicInformation>
</CryptographicInformationList>
</TimeStamp>
</ArchiveTimeStamp>
</ArchiveTimeStampChain>
</ArchiveTimeStampSequence>
</EvidenceRecord>

```

Image 267: Example evidence record

4.3.10 Reporting

The user can make reports on:

- [folders](#)
- [documents](#)
- [contents](#)
- [retention](#)
- [reviews](#)
- [access](#)
- [classification scheme](#)
- [entities](#)
- [deleted entities](#)
- [entities waiting for deletion.](#)

4.3.10.1 The Folder report

A folder report contains information about all the folders inside the selected archive, class or folder. The user creates it by selecting the icon  or the action “Folders” in the “Report types” section.

By selecting the root of the archive or selected entity, the user defines the scope of the report. By checking of the “Recursive” parameter, the user defines that the report includes the selected entity, and all contained entities. On the contrary, by unchecking this parameter, the user limits the search to the selected entity and the first level of sub-entities.

The report will list all folders for the user throughout the archive or under the selected entity. After selecting the action “Next”, the report is prepared.

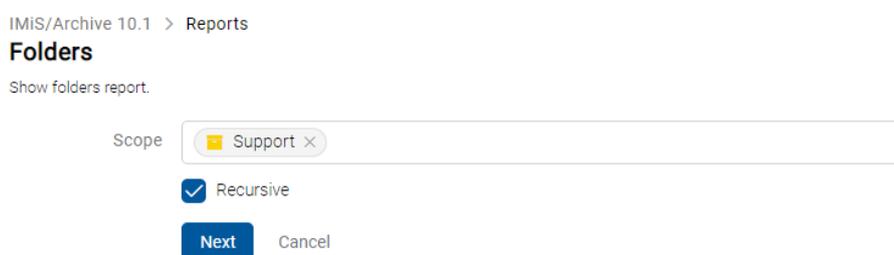


Image 268: Defining the scope of the folders report

Note: In the case of a longer report the user is first shown the notification “Preparing report”, followed by an indicative timeframe for preparing the report.



Image 269: The estimated timeframe for preparing the folders report

The report header provides the following information to the user:

- Scope: the scope of the report.
- Classification code: the classification code of the selected entity in the classification scheme.
- Number of folders: the number of folders included.

Information about folders is listed in the following columns:

- **Classification code:** the classification code of the folder in the classification scheme.
- **Title:** the title of the folder.
- **Template:** the name of the template, on which the folder was created.
- **Status:** the current status of the folder in the context of the archive.
Status dictates whether certain actions on the folder are allowed or not.
- **Significance:** the significance of the folder in the context of the archive.
- **Security class:** the security class of the folder or document. Security class is used for hiding entities from users, that do not have access rights to the entities set by the Security clearance level.
- **Current location:** the current location of the folder's physical content.
- **Home location:** the home location of the folder's physical content.
- **Number of entities:** represents the number of all contained entities.

IMiS/Archive 10.1 > Reports

Folders

Show folders report.

[PRINT](#) [EXPORT](#)

Scope:	Accounts
Classification Code:	3-2020-000030
Number of folders:	1

Classification Code ↑	Title	Template	Status	Significance	Security class	Current location	Home location	Number of subtities
3-2020-000030	Accounts	Folder	Opened	Delete	Confidential	Current location	Home location	3

Image 270: Example folder report

4.3.10.2 The Document report

A document report contains information about all the documents contained inside a selected archive, class or folder. The user creates it by selecting the icon  or the action “Documents” in the “Report types” section.

By selecting the root of the archive or selected entity, the user defines the scope of the report. By checking of the “Recursive” parameter, the user defines that the report includes the selected entity, and all contained entities. On the contrary, by unchecking this parameter, the user limits the search to the selected entity and the first level of sub-entities.

The report will list all documents for the user throughout the archive or under the selected entity. After selecting the action “Next”, the report is prepared.

IMIS/Archive 10.1 > Reports

Documents

Show documents report.

Scope

NEXT CANCEL

Image 271: Defining the scope of the documents report

The report header provides the following information to the user:

- Scope: the scope of the report.
- Classification code: the classification code of the selected entity in the classification scheme.
- Number of documents: the number of documents contained.
- Documents size: the total size of documents (KB/MB/GB).
- Number of errors: the total number of errors found (this field is shown if at least one error occurs).

Information about documents is listed in the following columns:

- Classification code: the classification code of the document in the classification scheme.
- Title: the title of the document.
- Template: the name of the template, on which the document was created.
- Status: the current status of the document in the context of the archive. Status dictates whether certain actions on the documents are allowed or not.
- Significance: the significance of the document in the context of the archive.
- Security class: the security class of the entity. It is used to hide entities from users whose security class does not provide them with access to entities.
- Current location: the current location of the document's physical content.
- Home location: the home location of the document's physical content.
- Number of contents: the total number of content(s) in the documents.
- Size: the total size of the content(s) in the document.

IMiS/Archive 10.1 > Reports

Documents

Show documents report.

[PRINT](#)

Scope:	Administration
Classification Code:	3
Number of documents:	16
Documents size:	632.2 MB
Number of errors:	2

Classification Code	Title	Template	Status	Significance	Security class	Current location	Home location	Number of contents	Size
3/000015	Video	Document	Opened	Permanent	Confidential			3	160.4 MB
3/000016	Audio	Document	Opened	Permanent	Confidential			9	338.0 MB
3/000018	Document 4	Document	Opened		Secret	current	home	2	114.9 MB
3/000019	email:Your OneDrive has been unfrozen	E-mail	Opened	Permanent	Confidential			3	66.4 kB
3/000020	email:Angular Internet Explorer	E-mail	Opened	Retain	Confidential			1	2.9 kB
▲ 3/000021	Document 64	Document01	Opened	Permanent	Secret			0	0 B
Server reported an error processing request (Reason: code=ERR_IAS_ERROR, message=Invalid date part (invalid day range).)									
3/000022	SpaceX	Document01	Opened	Retain	Confidential			2	2.2 MB

Image 272: Example of documents report

Note: In the event of errors, an entity error notification is shown below a given entity. All errors that are created if the entity fails to open are logged.

4.3.10.3 The Contents report

The content report contains information about all the files attached to the documents inside the selected archive, class or folder. The user creates it by selecting the icon  or the action “Contents” in the “Report types” section.

By selecting the root of the archive or selected entity, the user defines the scope of the report. By checking of the “Recursive” parameter, the user defines that the report includes the selected entity, and all contained entities. On the contrary, by unchecking this parameter, the user limits the search to the selected entity and the first level of sub-entities.

The report will list all content(s) in the all documents for the user throughout the archive or under the selected entity. After selecting the action “Next”, the report is prepared.

IMiS/Archive 10.1 > Reports

Contents

Show contents report.

Scope

Recursive

[Next](#) [Cancel](#)

Image 273: Defining the scope of the document contents report

The report header provides the following information to the user:

- Scope: the scope of the report.
- Classification code: the classification code of the selected entity in the classification scheme.
- Number of documents: the number of documents contained.
- Documents size: the total size of documents (KB/MB/GB).
- Number of contents: the total number of content(s) in the documents.
- Number of errors: the total number of errors found (this field is shown if at least one error occurs).

Information about document contents is listed in the following columns:

- Classification code: the classification code of the document in the classification scheme.
- Title: the title of the document.
- Template: the name of the template, on which the document was created.
- Content description: a description of content (files) attached to a document.
- Content type: the types of content (files) attached to a document.
- Size: the sizes of content (files) attached to a document.

IMiS/Archive 10.1 > Reports

Contents

Show contents report.

[PRINT](#)

Scope:	Administration
Classification Code:	3
Number of documents:	16
Documents size:	632.2 MB
Number of contents:	52
Number of errors:	2

Classification Code	Title	Template	Content description	Content Type	Size
3/000015	Video	Document	Resolution.webm	video/webm	127.4 MB
3/000015	Video	Document	Tehnicna_dokumentacija_2014.pdf	application/pdf	33.0 MB
3/000015	Video	Document	icon_sample_5.png	image/png	1.2 kB
3/000016	Audio	Document	dz.wav	audio/wav	110.6 MB

Image 274: Example of a document contents report

4.3.10.4 The Retention report

The retention report contains information on retention periods and disposition holds on all entities under the selected archive, class or folder. The user creates it by selecting the icon



or the action "Retention" in the "Report types" section.

By selecting the root of the archive or selected entity, the user defines the scope of the report. By checking of the “Recursive” parameter, the user defines that the report includes the selected entity, and all contained entities. On the contrary, by unchecking this parameter, the user limits the search to the selected entity and the first level of sub-entities.

The report will list all content(s) in the all documents for the user throughout the archive or under the selected entity. After selecting the action “Next”, the report is prepared.

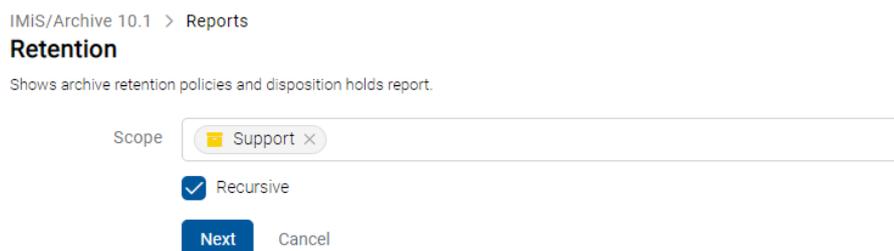


Image 275: Defining the scope of the retention report

The report header provides the following information to the user:

- Scope: the scope of the report.
- Classification code: the classification code of the selected entity in the classification scheme.
- Number of classes: the number of classes contained.
- Number of folders: the number of folders contained.
- Number of documents: the number of documents contained.

Information on retention is listed in the following columns:

- Classification code: the classification code of the entity in the classification scheme.
- Title: the title of the entity being described.
- Type: contains the type of the entity being described.
- Template: the name of the template, on which the entity was created.
- Policy: represents the type of entry (retention policy or disposition hold).
- Name: the name of the retention policy or disposition hold.
- Reason: the reason for the retention policy or disposition hold.
- Description: a description of the retention policy or disposition hold.

IMiS/Archive 10.1 > Reports

Retention

Shows archive retention policies and disposition holds report.

PRINT

Scope:	Support
Classification Code:	15
Number of classes:	3
Number of folders:	1
Number of documents:	4

Classification Code	Title	Type	Template	Policy	Name	Reason	Description
15	Support	Class	Class	Retention policy	5-years	Dispose after 5 years retention	Dispose after 5 years retention
15.C-1	Education	Class	Class	Retention policy	5-years	Dispose after 5 years retention	Dispose after 5 years retention

Image 276: Example of a review report

4.3.10.5 The Review report

The review report contains information on reviews. The user creates it by selecting the icon  or the action “Review” in the “Report types” section.

By selecting the review, the user defines the scope of the report.

By checking of the “Recursive” parameter, the user defines that the report includes the selected entity, and all contained entities. On the contrary, by unchecking this parameter, the user limits the search to the selected entity and the first level of sub-entities.

The report will list all reviews for the user throughout the archive or under the selected entity. After selecting the action “Next”, the report is prepared.

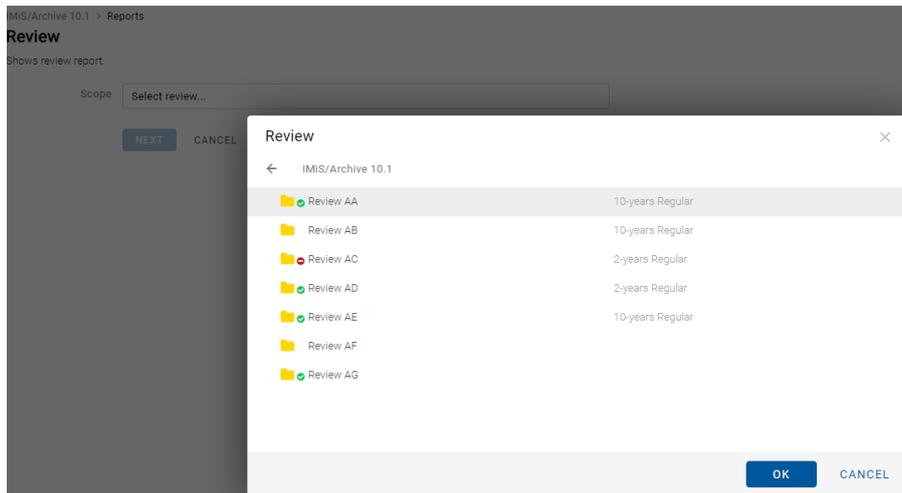


Image 277: Selecting the review

IMiS/Archive 10.1 > Reports

Review

Shows review report.

Scope

NEXT CANCEL

Image 278: Defining the scope of the review report

The report header provides the following information to the user:

- Review: the title of the review.
- Entities: the number of entities in the selected review.

Information on reviews are listed in the following sections and columns:

The Details section

- Property: the review properties.
- Value: the value of the review properties.

Details

Property	Value
Title	Review AD
Scope	Administration
Scope Classification Code	3
Description	2-years Regular
Status	Closed
Owner	John Smith (jsmith [DELETED 20005])
Creator	Administrator (admin)

Image 279: Example of a Review report - Properties

The Retention policy section

- Title: the name of the retention policy.
- Reason: the reason for the retention policy.
- Description: a description of the retention policy.

Retention policy

Name	Reason	Description
2-years	Dispose after 2 years retention	Dispose after 2 years retention

Image 280: Example of a Review report – Retention policy

4.3.10.6 The Access report

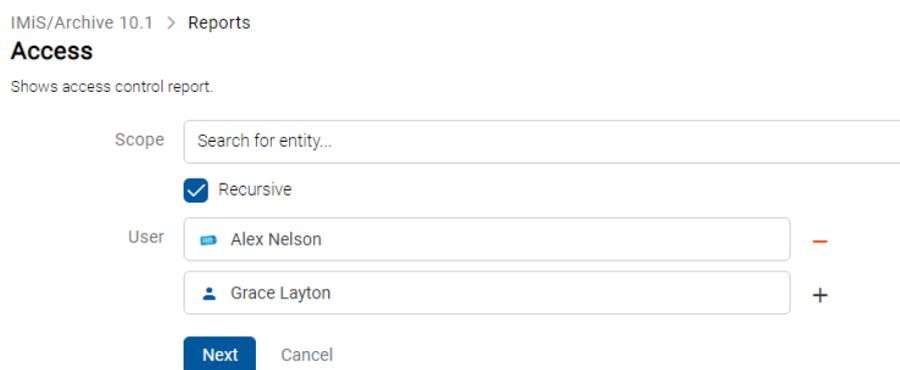
The access report contains information about the access rights / permissions of users on all the folders and documents inside a selected archive, class or folder, to which the archive users have access. The user creates it by selecting the icon  or the action “Access” in the “Report types” section.

By selecting the archive's root or selected entity, the user defines the scope of the report. By checking of the “Recursive” parameter, the user defines that the report includes the selected entity, and all contained entities. On the contrary, by unchecking this parameter, the user limits the search to the selected entity and the first level of sub-entities.

Select the “User” from the list.

If you wish to create an entity access report on all the users of the archive, leave the field with the label “All users” blank. Otherwise, select one or more users from the list (“Select user”).

The report will list all access rights for the user throughout the archive or under the selected entity. After selecting the action “Next”, the report is prepared.



IMiS/Archive 10.1 > Reports

Access

Shows access control report.

Scope

Recursive

User -

+

Image 283: Defining the scope of the access report

The report header provides the following information to the user:

- Scope: the scope of the report.
- Classification code: the classification code of the selected entity in the classification scheme.
- Number of classes: the number of classes contained.
- Number of folders: the number of folders contained.
- Number of documents: the number of documents contained.

Information on the users' rights on individual folders and documents is listed in the following columns:

- Classification code: the classification code of the entity in the classification scheme.
- Title: the title of the entity.
- Type: the type of the entity being described.
- Template: the name of the template, on which the document was created.
- Status: the status of the entity in the context of the archive.
Status dictates whether certain actions on the document are allowed or not.
- Significance: the significance of the entity in the context of the archive.
- Security class: the security class of the entity. Security classes are used to hide entities from users whose clearance level is not high enough to access them.
- Current location: the current location of the entity's physical content.
- Home location: the home location of the entity's physical content.
- User: the name of the user the report is on.
- Read: this value tells if the user has access right to read entities.
- Write: this value tells if the user has access right to edit entities.
- Delete: this value tells if the user has access right to delete entities.
- Move: this value tells if the user has access right to move entities.
- Create entities: this value tells if the user has access right to create entities.
- Change permissions: this value tells if the user has access right to change permissions.
- Change security class: this value tells if the user has access right to change security class.
- Change status: this value tells if the user has access right to change status.
- Change retention: this value tells if the user has access right to change retention.
- Create references: this value tells if the user has access right to create a reference to another reference.

IMiS/Archive 10.1 > Reports

Access

Shows access control report.

[PRINT](#) [EXPORT](#)

Scope:	Customs documentation
Classification Code:	3/000032
Number of classes:	0
Number of folders:	0
Number of documents:	1

Classification Code	Title	Type	Template	Status	Significance	Security class	Current location	Home location	User	Read	Write	Delete	Move	Create entities	Change permissions	Change security class	Change status	Change retention	Create references	
3/000032	Customs documentation	Document	Custom document	Opened	Delete	Confidential			3KDCDevelopment (3KDCDevelopment)											
3/000032	Customs documentation	Document	Custom document	Opened	Delete	Confidential			Anonymous (Anonymous)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Image 284: Example access report on the selected user

4.3.10.7 The Classification scheme report

A classification scheme report contains information about all the classes inside the selected archive or class. The user creates it by selecting the icon  or the action “Classification scheme” or “Classification scheme with folders” in the “Classification scheme” section.

Classes in the classification scheme

By selecting the archive's root or selected entity, the user defines the scope of the report. The report will list all classes for the user throughout the archive or under the selected entity. After selecting the action “Next”, the report is prepared.

IMiS/Archive 10.1 > Reports

Classification scheme

Shows classes classification scheme.

Scope

[NEXT](#) [CANCEL](#)

Image 285: Defining the scope of the classes report

The report header provides the following information to the user:

- Scope: the scope of the report.
- Classification code: the classification code of the selected entity in the classification scheme.
- Number of classes: the number of classes contained.

Information on individual classes are listed in the following columns:

- **Classification code:** the classification code of the class in the classification scheme.
- **Title:** the title of the class being described.
- **Created:** the date the entity was created on the server.

IMiS/Archive 10.1 > Reports
Classification scheme
 Shows classes classification scheme.

[PRINT](#)

Scope:	Administration
Classification Code:	3
Number of classes:	2

Classification Code	Title	Created
3	Administration	19. Feb 2020, 13:17
3.8	Agreements and Terms & Conditions	13. Nov 2018, 13:26

Image 286: Example of a classification scheme report on the classes

Classes and folders in the classification scheme

By selecting the archive's root or selected entity, the user defines the scope of the report. The report will list all classes and folders for the user throughout the archive or under the selected entity. After selecting the action “Next”, the report is prepared.

IMiS/Archive 10.1 > Reports

Classification scheme with folders

Shows classes and folders classification scheme.

Scope

[NEXT](#) [CANCEL](#)

Image 287: Defining the scope of the classes and folders report

The report header provides the following information to the user:

- **Scope:** the scope of the report.
- **Classification code:** the classification code of the selected entity in the classification scheme.
- **Number of classes:** the number of classes contained.
- **Number of folders:** the number of folders contained.

Information on individual classes and folders are listed in the following columns:

- **Classification code:** the classification code of the class or folder in the classification scheme.
- **Title:** the title of the class or folder being described.
- **Type:** the type of the entity being described.
- **Created:** the date the entity was created on the server.

IMiS/Archive 10.1 > Reports
Classification scheme with folders
 Shows classes and folders classification scheme.

Print Export

Scope:	Administration
Classification Code:	3
Number of classes:	3
Number of folders:	2

Classification Code ↑	Title	Type	Created
3	Administration	Class	19. Feb 2020, 13:17
3.31	Terms and conditions	Class	29. Jun 2020, 13:48
3.8	AgreementsAgreementsAgreementsAgreementsAgreementsAgreementsAgreementsAgreements	Class	13. Nov 2018, 13:26
3-2020-000030	Accounts	Folder	19. Feb 2020, 13:20
3-2020-000030-00004	Folder 1	Folder	16. Jul 2020, 16:29

Image 288: Example of a classification scheme report on the classes and folders

4.3.10.8 The Entity report

The entity report contains selected entity data. The user creates it by selecting the icon  or the action “Entity details” in the “Other” section.

By selecting the entity, the user defines the scope of the report.

The user can limit the displayed data set with the settings of the following fields and/or parameters:

- **Version:** entity version.
- **Content:** content of documents or emails.
- **Security:** collection of access permissions for directory entities and entity properties.
- **Physical content:** metadata and location of the physical content.
For more information on physical content see chapter [Physical content](#).
- **Email:** email information. Available only for documents created using the template “Email”.
For more information see chapter [Email](#).
- **Retention:** information on retention periods and disposition holds.
For more information see chapter [Retention](#).

- Save log: information on checking the validity of electronic signatures and digital certificates upon capture. For more information see chapter [Save log](#).
- Transfer metadata: information on the transfer of physical content (and the audit log).
- Custom metadata: additional metadata shown based on the type of template. For more information see chapter [Custom metadata](#).

After selecting the action “Next”, the report is prepared.

IMIS/Archive 10.1 > Reports
Entity details
Shows entity details.

Scope: Administration x

Version: [dropdown arrow]

- Content
- Security
- Physical properties
- Email
- Retention
- Save Log
- Transfer metadata
- Review date

Next Cancel

Image 289: Defining the scope of the entity report

Information on entity are listed in the following columns:

- Classification code: the classification code of the entity in the classification scheme.
- Template: the name of the template.
- Status: the current status of the entity.
- Significance: the significance of the entity.
- Security class: the security class of the entity.
- Current location: the current location of the document's physical content.
- Home location: the home location of the document's physical content.
- Number of contents: the total number of content(s) in the documents.
- Size: sizes of content (files) attached to a document.

IMiS/Archive 10.1 > Reports

Entity details

Shows entity details.

[Print](#)

Administration

Property	Type	Value
Classification Code	STRING200	3
Title	STRING200	Administration
Description	STRING200	Documents, Administration, Bureaucracy
Permanent	BOOL	No
Status	UINT32	Opened
Opened	DATE_TIME	19. Feb 2020, 13:17
Closed	DATE_TIME	
Security class	UINT32	Confidential
Significance	UINT32	Permanent

Image 290: Example of the Entities report – Properties

Retention

Name	Reason	Description
10-years	Dispose after 10 years retention	Dispose after 10 years retention
5-years	Dispose after 5 years retention	Dispose after 5 years retention
2-years	Dispose after 2 years retention	Dispose after 2 years retention

Disposition holds

Name	Reason	Description
Legacy procedure	Active legal procedure	Legal procedure in progress, material must be preserved until finished

Image 291: Example of the Entities report –Retention

Security

Name	Type	Permission	Read	Write	Delete	Move	Create entities	Change permissions	Change security class	Change status	Change retention	Create references	Valid from	Valid to
anelson	USER	Allow	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
anelson	USER	Allow, Inherited	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Anonymous	USER	Allow, Inherited	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
board [DELETE D 10004]	GROUP	Allow, Inherited	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
sys:Everyone	GROUP	Allow	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
sys:Everyone	GROUP	Allow, Inherited												
glayton	USER	Allow, Inherited	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
jturner	USER	Allow, Inherited	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
jsmith [DELETE D 20005]	USER	Allow, Inherited	✓	✓										
kclay	USER	Allow, Inherited	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
marko	USER	Allow, Inherited	✓	✓	✓									
sys:Owner	ATTRIBUTE	Allow	✓	✓			✓	✓						
sys:Owner	ATTRIBUTE	Allow, Inherited	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
sys:Administrators	GROUP	Allow, Inherited	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		

Security / DateTime

Name	Type	Permission	Read	Write	Create	Delete	Valid from	Valid to
glayton	USER	Allow, Inherited	✓	✓	✓	✓		

Security / evaluation

Name	Type	Permission	Read	Write	Create	Delete	Valid from	Valid to
jturner	USER	Allow, Inherited	✓	✓	✓	✓		

Image 292: Example of the Entities report – Security

Transfer metadata

Property	Type	Value
Classification Code	STRING100	0
Transfer date	DATE_TIME	10. Mar 2020, 08:25
Transfer system identifier	STRING100	5910_UZK30JTL9evjy0CaFRDAa5-BmM

Transfer audit log

```
<?xml version="1.0" encoding="UTF-8"?>
<auditlog query/resultset/isi/schemaLocations="http://www.imis.si/misarc/http://www.imis.si/misarc/auditlog.xsd" xmlns="http://www.imis.si/misarc" xmlns: xsi="http://www.w3.org/2001/XMLSchema-instance">
<session id="53" closureReasons="0" address="192.168.80.64" internal_address="1" dateTimeOpened="2020-02-19T10:16:32Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.106 Safari/537.36"/>
<session id="139" closureReasons="0" address="192.168.80.64" internal_address="1" dateTimeOpened="2020-02-21T14:32:59Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.106 Safari/537.36"/>
<session id="179" closureReasons="0" address="192.168.80.64" internal_address="1" dateTimeOpened="2020-02-25T08:58:53Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.116 Safari/537.36"/>
<session id="271" closureReasons="0" address="192.168.80.15" internal_address="200126040861280760a10c6e4670b6" dateTimeOpened="2020-02-28T13:52:43Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36"/>
<session id="328" closureReasons="0" address="192.168.50.15" internal_address="1" dateTimeOpened="2020-02-27T15:35:47Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36"/>
<session id="359" closureReasons="0" address="192.168.80.64" internal_address="1" dateTimeOpened="2020-02-28T14:29:59Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36"/>
<session id="357" closureReasons="0" address="192.168.80.64" internal_address="1" dateTimeOpened="2020-02-28T13:57:51Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36"/>
<session id="358" closureReasons="0" address="192.168.80.64" internal_address="1" dateTimeOpened="2020-02-28T13:57:52Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36"/>
<session id="404" closureReasons="0" address="192.168.80.64" internal_address="1" dateTimeOpened="2020-02-28T15:48:58Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36"/>
<session id="405" closureReasons="0" address="192.168.80.64" internal_address="1" dateTimeOpened="2020-02-28T15:48:58Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36"/>
<session id="415" closureReasons="0" address="192.168.50.15" internal_address="1" dateTimeOpened="2020-03-03T09:43:27Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.109 Safari/537.36"/>
</session>
</auditlog>
```

Image 293: Example of the Entities report – Transfer metadata

4.3.10.9 The Deleted entities report

The deleted entities report contains information on entities deleted throughout the archive.

The user creates it by selecting the icon  or the action “Deleted” in the “Other” section.

After selecting the action “Next”, the report is prepared.



Image 294: Decision before preparing the report

The report header provides the following information to the user:

- Scope: the scope of the report.
- Size: the number of all deleted entities.
- Number of classes: the number of classes contained.
- Number of folders: the number of folders contained.
- Number of Documents: the number of documents contained.

Information on entity are listed in the following columns:

- Classification code: the classification code of the deleted entity in the classification scheme.
- Title: The title of the deleted entity being described.
- Type: the type of the deleted entity being described.
- Description: a short description of the deleted entity.
- Agent: the user who executed the delete action.
- Deleted: the date and time of deleting the entity from the archive server.

IMIS/Archive 10.1 > Reports

Deleted

Shows deleted entities report.

[Print](#) [Export](#)

Scope:	IMIS/Archive 10.1
Size:	425
Number of classes:	235
Number of folders:	16
Number of documents:	174

Classification Code	Title	Type	Description	Agent	Deleted
0	Administration	Class	-	Administrator (admin)	10. Mar 2020, 10:31
0.10	Class 5	Class	-	Administrator (admin)	10. Mar 2020, 10:15
0.11	Class 6	Class	-	Administrator (admin)	10. Mar 2020, 10:15
0.12	Class 7	Class	-	Administrator (admin)	10. Mar 2020, 10:15
0.16	Categories	Class	-	Administrator (admin)	10. Mar 2020, 10:31
0.16.6	Class 1	Class	-	Administrator (admin)	10. Mar 2020, 10:30
0.16/000001	1	Document	-	Administrator (admin)	10. Mar 2020, 10:30
0.16/000002	2	Document	-	Administrator (admin)	10. Mar 2020, 10:30

Image 295: Example of the Deleted entities report

By selecting the action “Print”, the user is shown a print preview for the deleted entities report. The user prints the report by selecting the action “Print” or cancels it by selecting the action “Cancel”.

Print
Total: 12 sheets of paper

Printer
KONICA MINOLTA bizhub C3110(E)F1

Copies
1

Layout
 Portrait
 Landscape

Pages
 All
e.g. 1-5, 8, 11-13

Colour
Black and white

[More settings](#)

[Print using system dialogue \(Ctrl-Shift+P\)](#)

[Print](#) [Cancel](#)

08/09/2020 Deleted - Reports - IMIS/wClient

Deleted

Scope:	IMIS/Archive 10.1
Size:	425
Number of classes:	235
Number of folders:	16
Number of documents:	174

Classification Code	Title	Type	Description	Agent	Deleted
0	Administration	Class	-	Administrator (admin)	10. Mar 2020, 10:31
0.10	Class 5	Class	-	Administrator (admin)	10. Mar 2020, 10:15
0.11	Class 6	Class	-	Administrator (admin)	10. Mar 2020, 10:15
0.12	Class 7	Class	-	Administrator (admin)	10. Mar 2020, 10:15
0.16	Categories	Class	-	Administrator (admin)	10. Mar 2020, 10:31
0.16.6	Class 1	Class	-	Administrator (admin)	10. Mar 2020, 10:30
0.16/000001	1	Document	-	Administrator (admin)	10. Mar 2020, 10:30
0.16/000002	2	Document	-	Administrator (admin)	10. Mar 2020, 10:30
0.16/000003	3	Document	-	Administrator (admin)	10. Mar 2020, 10:30
0.16/000004	4 1111111111111111 22 222222 333333333333 33333333333333333333 33333333333333333333	Document	-	Administrator (admin)	10. Mar 2020, 10:30
0.16/000005	No category	Document	-	Administrator (admin)	10. Mar 2020, 10:30
0.16/000007	1-1	Document	-	Administrator (admin)	10. Mar 2020, 10:30
0.16/000008	1-2	Document	-	Administrator (admin)	10. Mar 2020, 10:30
0.18	Agreements and Terms & Conditions	Class	-	Administrator (admin)	10. Mar 2020, 10:31
0.18.0	Finance	Class	Account payable, Accounts receivable, Banking, Budgeting, Payments	Administrator (admin)	10. Mar 2020, 10:30
0.18.0.0	Accounts Payable	Class	-	Administrator (admin)	10. Mar 2020, 10:27
0.18.0.0.0	Incoming Invoices	Class	-	Administrator (admin)	10. Mar 2020, 10:26
0.18.0.0.1	Credit Notes	Class	-	Administrator (admin)	10. Mar 2020, 10:26
0.18.0.1	Accounts Receivable	Class	-	Administrator (admin)	10. Mar 2020, 10:27
0.18.0.1.0	Outgoing Invoices	Class	-	Administrator (admin)	10. Mar 2020, 10:27
0.18.0.1.1	Balance Sheet	Class	-	Administrator (admin)	10. Mar 2020, 10:27
0.18.0.2	Banking	Class	-	Administrator (admin)	10. Mar 2020, 10:28

Image 296: A print preview for the deleted entities report

By selecting the action “Export”, a popup menu appears with the possible format (CSV) for saving data on deleted entities. After selecting the CSV format, the user is shown a notification on preparing the deleted entities report.



Image 297: Notification on preparing the deleted entities report

After selecting the action “Open”, the information on deleted entities is shown.

	A	B	C	D	E
1	ClassificationCode	Title	Description	Agent	Deleted
2	0.18	Agreements and Terms & Conditions	.	admin	2020-03-10T09:31:12.093Z
3	0.18.0	Finance	Account payable, Accounts receivable, Banking, Budgeting, Payments	admin	2020-03-10T09:30:26.880Z
4	0.18.0.0	Accounts Payable	.	admin	2020-03-10T09:27:37.266Z
5	0.18.0.0.0	Incomming Invoices	.	admin	2020-03-10T09:26:54.445Z
6	0.18.0.0.1	Credit Notes	.	admin	2020-03-10T09:26:54.409Z
7	0.18.0.1	Accounts Receivable	.	admin	2020-03-10T09:27:37.300Z
8	0.18.0.1.0	Outgoing Invoices	.	admin	2020-03-10T09:27:18.477Z
9	0.18.0.1.1	Balance Sheet	.	admin	2020-03-10T09:27:18.437Z
10	0.18.0.2	Banking	.	admin	2020-03-10T09:28:56.591Z
11	0.18.0.2.0	Domestic Accounts	.	admin	2020-03-10T09:27:54.318Z
12	0.18.0.2.1	Foreign Accounts	.	admin	2020-03-10T09:28:37.149Z
13	0.18.0.2.1.0	Class 91	.	admin	2020-03-10T09:28:27.873Z
14	0.18.0.2.2	Bank Statements	.	admin	2020-03-10T09:27:54.284Z
15	0.18.0.3	Budgeting	.	admin	2020-03-10T09:30:12.246Z
16	0.18.0.3.0	Budgets	.	admin	2020-03-10T09:29:39.944Z
17	0.18.0.3.1	Projects	.	admin	2020-03-10T09:29:40.012Z
18	0.18.0.3.2	Expenses	.	admin	2020-03-10T09:29:39.979Z
19	0.18.0.3.3	Reports	.	admin	2020-03-10T09:29:40.054Z
20	0.18.0.4	Payments	.	admin	2020-03-10T09:30:12.280Z
21	0.18.0.4.0	Cash Management	.	admin	2020-03-10T09:29:57.887Z
22	0.18.0.4.1	Cheques	.	admin	2020-03-10T09:29:57.923Z

Image 298: Review of information on deleted entities in the CSV format

4.3.10.10 The Delete queue report

The delete queue report contains information on entities placed on the delete queue list.

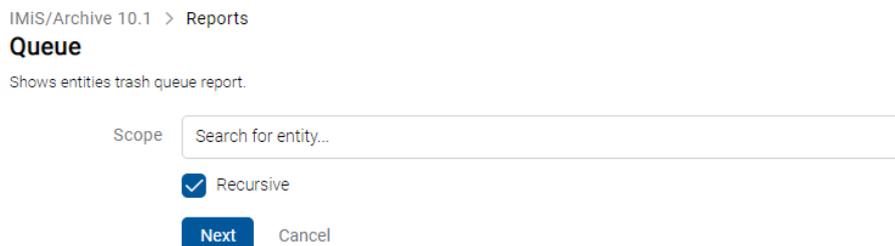
The user creates it by selecting the icon  or the action “Queue” in the “Other” section.

After selecting the action “Next”, the report is prepared.

By selecting the root of the archive (leaving the field blank) or selected entity, the user defines the scope of the report.

By checking of the “Recursive” parameter, the user defines that the report includes the selected entity, and all contained entities. On the contrary, by unchecking this parameter, the user limits the search to the selected entity and the first level of sub-entities.

After selecting the action “Next”, the report is prepared.



IMiS/Archive 10.1 > Reports

Queue

Shows entities trash queue report.

Scope

Recursive

Image 299: Defining the scope of the delete queue report

The report header provides the following information to the user:

- Scope: the scope of the report.
- Classification code: the classification code of the selected entity in the classification scheme.
- Number of classes: the number of classes contained.
- Number of folders: the number of folders contained.
- Number of documents: the number of documents contained.

Information on the entities waiting for deletion are listed in the following columns:

- Classification code: the classification code of the class in the classification scheme.
- Type: the type of the entity being described.
- Template: the name of the template used to create the entity.
- Status: the status of the entity in the context of the archive owner.
- Security class: the security class of the entity. It is used to hide entities from users whose security class does not provide them with access to entities.
- 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 throughout the entity's existence.
- Owner: a directory entity (user or group) entity that is responsible for the selected entity (owner).

IMiS/Archive 10.1 > Reports

Queue

Shows entities trash queue report.

[PRINT](#)
[EXPORT](#)

Scope:	IMiS/Archive 10.1
Classification Code:	
Number of classes:	1
Number of folders:	1
Number of documents:	1

Classification Code	Title	Type	Template	Status	Significance	Security class	Creator	Owner
15.C-1	Education	Class	Class	Opened	Delete	Confidential	Administrator (admin)	Marko Hren (marko)
3/000032	Customs documentation	Document	Custom document	Opened	Delete	Confidential	Administrator (admin)	Keira Clay (kclay)
9-2020-000030	Accounts	Folder	Folder	Opened	Delete	Confidential	Administrator (admin)	Human Resources (hr)

Image 300: Example of the delete queue report

By selecting the action “Print”, the user is shown a print preview for the deleted entities report. The user prints the report by selecting the action “Print” or cancels it by selecting the action “Cancel”.

Image 301: A print preview for the delete queue report

By selecting the action “Export”, a popup menu appears with the possible format (CSV) for saving data on the entities waiting for deletion. After selecting the CSV format, the user is shown a notification on preparing the deletion queue report.

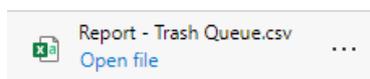


Image 302: Notification on preparing the delete queue report

After selecting the action “Open”, the information on the entities waiting for deletion is shown.

	A	B	C	D	E	F	G	H	I
1	ClassificationCode	Title	Type	Template	Status	Significance	SecurityClass	Creator	Owner
2	15.C-1	Education	CLASS	Class	Opened	Delete	Confidential	admin	marko
3	3/000032	Customs documentation	DOCUMENT	Custom Document	Opened	Delete	Confidential	admin	kclay
4	3-2020-000030	Accounts	FOLDER	Case	Opened	Delete	Confidential	admin	hr

Image 303: Review of information on entities waiting for deletion in the CSV format

4.3.11 Bulk document capture

Bulk capture is the action of importing a large number of documents without the need for the user to oversee each individual capturing procedure. Bulk capture in the IMiS®/wClient is performed using the “Import” action. By preparing the content correctly before you import it, you can decrease the possibility of encountering errors during the bulk capture procedure. Entities that experience errors during bulk capture are not imported and must be captured manually by the user. For more information on the bulk capture procedure see chapter [Import](#).

4.3.12 Import

The IMiS®/wClient enables the import of entities to the IMiS®/ARChive Server together with their metadata on Audit log and Authenticity evidence if they exist. The entities imported by a user with the ImportExport role have to be compressed (.zip) and prepared in the prescribed XML format.

For more information on roles see chapter [Access in the IMiS®/ARChive Server Manual](#).

Import may be performed into the root class of the classification scheme or into any chosen class or folder. After selecting the action »Import« in the Actions dropdown menu in the command bar or on a given entity, a window opens for selecting the compressed file for entity import (Select file).

Image 304: Selecting the compressed file with the imported entities

Confirming the action **Import** starts the entity import.

After the import process is completed, the bottom right part of the view shows an import notification.



Image 305: Displaying an import notification

Each import action on the IMiS®/ARChive Server is logged in the Import folder contained in the Administration system folder in the left view. This folder can only be accessed by users who have been assigned the Reports role and the appropriate rights to import logs.

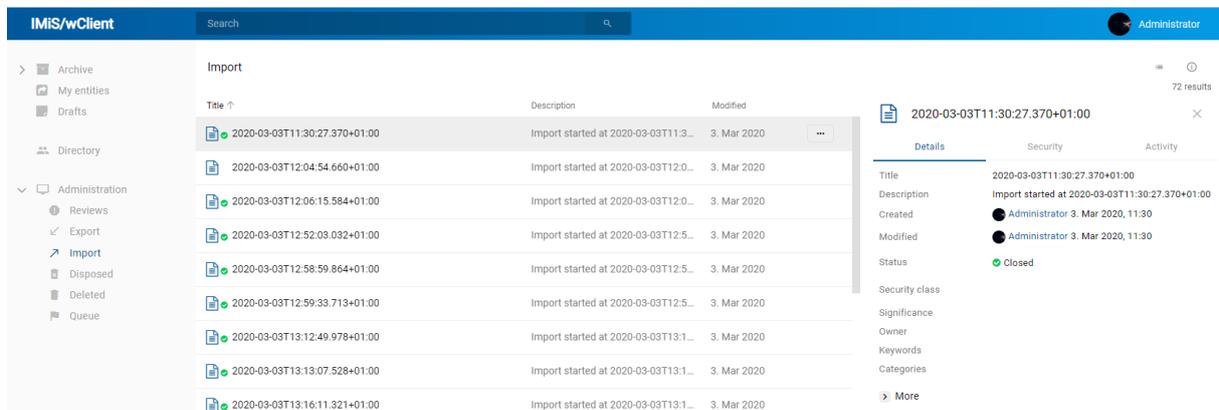


Image 306: Display of the Import folder in the Administration system folder

The IMiS®/wClient enables the review of imported entities on the IMiS®/ARChive Server, including import data. The imported entities reviewed by the user are prepared in the prescribed XML format.

For more information on the file format for import and the file structure see chapter [Format of the import / export file](#).

After creation is completed, the import report is given the status **Closed**. The user can open the report and perform the following actions:

- **Open:** opens the selected import report in reading mode.
- **Edit:** opens the selected entity in editing mode. Enables adding the import report metadata, and modifying and removing the report, metadata and contents.

- **Actions:** contains commands for various actions on the selected entity:
 - **New reference:** adding a connection to another report or entity in the classification scheme via a dialog box. For more information see chapter [Reference](#).
 - **Move:** moving the import report within the classification scheme on the archive.
 - **Export:** exporting the selected report from the archive.
- **Status:** modifying the status of the import report via a dialog box which enables giving the reason for the change.
- **Security class:** modifying the security class of the import report via a dialog box, which requires the user to give the reason for the change.
- **Share:** copying the link to the selected entity to be shared with other users.
- **Delete:** deleting the selected import report.

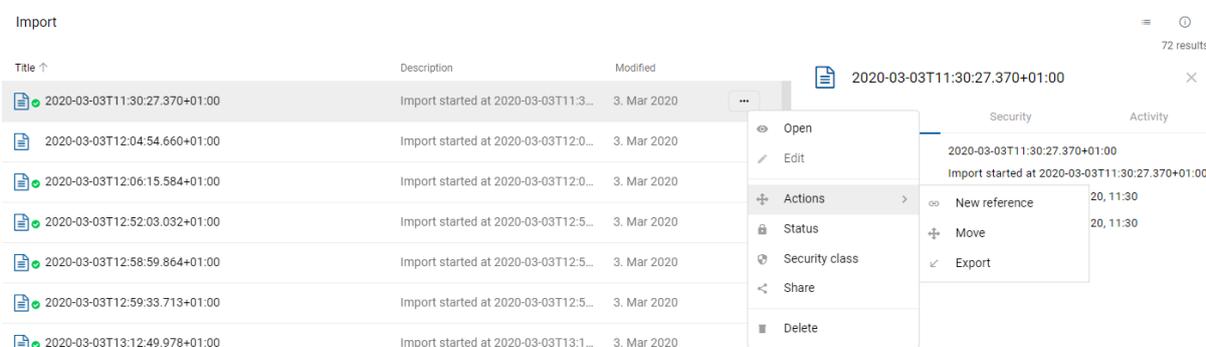


Image 307: Set of available actions on the import/export report

By selecting the popup menu on the import report, the user can choose from the following options:

- **Preview:** For more information on content preview see chapter [Content preview](#).
- **Download:** For more information on downloading content see chapter [Downloading content](#).
- **Copy:** copying the content to another document.
- **Share:** copying the link to the selected entity to be shared with other users.
- **Manage:**
 - **Queue for Indexing.** For more information on indexing content see chapter [Indexing content](#).
 - **Queue for Conversion.** For more information on content conversion see chapter [Content conversion](#).

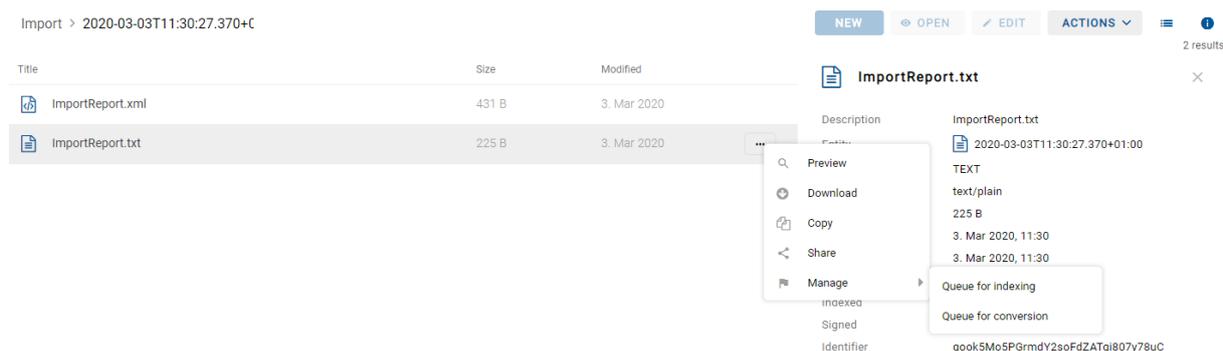


Image 308: Popup menu on a import report

4.3.12.1 Import procedure

At the start of the import procedure, the IMiS®/WClient creates a new document in the folder Import located in the »Administration« system folder. This document contains a report of the import to the archive server.

The title of the document is identical to the date and time of import, in ISO format.

The status of the document is Opened.

During import, the import document is completed with the following three log files:

- ImportReport.xml: XML file that contains:
 - import success rate statistics
 - list of failed import attempts (including the classification codes)
 - list of successfully imported files (including the hash values and full classification codes).
- ImportReport.txt: contains a report for each successfully or unsuccessfully imported entity.
- ErrorReport.txt: contains a report for each failed import attempt including the reason for the import error.

When all entities from the list are imported, the file ImportReport.xml is digitally signed with the selected digital certificate according to the XMLDSIG standard. This ensures that the report's authenticity can be verified.

The status of the document then changes to Closed.

If there is an error while the document is being completed, the import document remains in the system class in its raw form and has the status Open.

If there is an error during the import of an entity on the import list, the sub-entities it contains will not be imported. In case a sub-entity encounters an error, the other sub-entities will still be imported, providing the import of the parent entity was successful.

The screenshot displays the 'Import' system folder. On the left, a table lists two files: 'ImportReport.xml' (431 B, 3. Mar 2020) and 'ImportReport.txt' (225 B, 3. Mar 2020). On the right, a detailed view for the file '2020-03-03T11:30:27.370+01:00' is shown. The 'Details' tab is active, displaying the following information:

Attribute	Value
Title	2020-03-03T11:30:27.370+01:00
Description	Import started at 2020-03-03T11:30:27.370+01:00
Created	Administrator 3. Mar 2020, 11:30
Modified	Administrator 3. Mar 2020, 11:30
Status	Closed
Security class	
Significance	
Owner	
Keywords	
Categories	
Save Log	
More	
Classification Code	sys.Logs.Import/0000000001
Template	Log
Type	Document
Permanent	No
Accessed	13. Mar 2020, 14:37
Opened	6. Mar 2020, 09:01
Closed	13. Mar 2020, 14:37
Identifier	t1tuy-Hc_u647qKLSiYEdUj8eV1Zeduf
External Identifiers	

Image 309: Display of the import report in the Import system folder

By selecting the value of the attribute "Get" in the imported entity data ("Transfer audit log") in open mode, the logged-on user is shown a notification in the bottom bar on the audit log created before importing the entity in the .bin format.

NEW OPEN EDIT ACTIONS 2 results

Despatch note

Details Security Activity

Modified Administrator 13. Mar 2020, 15:11

Status Opened

Security class Confidential

Significance Retain INHERITED

Owner Alex Nelson

Keywords despatch note

Categories distribution logistics

> Email

> Retention

> Save Log

More

Classification Code 5/000003

Template E-mail

Type Document

Permanent No

Accessed 13. Mar 2020, 15:11

Opened 10. Mar 2020, 14:31

Identifier oXixJXGRs-bMMFqMEzBAQqHaA_Yp-B6l

External Identifiers

Transfer date 13. Mar 2020, 14:48

Transfer audit log GET

Transfer system identifier _-a2axJNwA7yNWeVJl9q1XgFqQKQWCEn

Image 310: Information about the audit log created before the entity import

Despatch note - Tran....bin

[Open file](#)

Image 311: Notification on the transfer of the audit log created before the entity import

By opening the file in a suitable application (e.g. Notepad), the user can view the audit log created before the entity import.

```

[>xml version="1.0" encoding="UTF-8">
<auditlog.query.resultset xsi:schemaLocation="http://www.imis.si/imisarc http://www.imis.si/imisarc/auditlog.xsd" xmlns="http://www.imis.si/imisarc" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<sessions>
<!--Audit query sessions.-->
<session id="990" closureReason="0" address="192.168.50.15" internal_address="192.168.80.67" dateTimeOpened="2020-03-10T13:11:59Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0; Win64; x64)
<session id="989" closureReason="0" address="192.168.50.15" internal_address="192.168.80.67" dateTimeOpened="2020-03-10T13:11:43Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0; Win64; x64)
<session id="1041" closureReason="0" address="192.168.80.64" internal_address=":" dateTimeOpened="2020-03-11T09:19:30Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
<session id="1028" closureReason="0" address="192.168.50.15" internal_address="192.168.80.67" dateTimeOpened="2020-03-11T08:02:54Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0; Win64; x64)
<session id="1084" closureReason="0" address="192.168.50.15" internal_address="2a01:260:4086:1282:100::5" dateTimeOpened="2020-03-12T06:37:43Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0
<session id="1082" closureReason="0" address="192.168.50.15" internal_address="2a01:260:4086:1282:100::5" dateTimeOpened="2020-03-12T06:32:11Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0
<session id="1083" closureReason="0" address="192.168.50.15" internal_address="2a01:260:4086:1282:100::5" dateTimeOpened="2020-03-12T06:37:21Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0
<session id="1087" closureReason="0" address="192.168.50.15" internal_address="2a01:260:4086:1282:100::5" dateTimeOpened="2020-03-12T07:27:50Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0
<session id="1085" closureReason="0" address="192.168.50.15" internal_address="2a01:260:4086:1282:100::5" dateTimeOpened="2020-03-12T07:20:54Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0
<session id="1090" closureReason="0" address="192.168.50.15" internal_address="2a01:260:4086:1282:100::8" dateTimeOpened="2020-03-12T08:04:30Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0
<session id="1089" closureReason="0" address="192.168.50.15" internal_address="2a01:260:4086:1282:100::8" dateTimeOpened="2020-03-12T07:53:47Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0
<session id="1088" closureReason="0" address="192.168.50.15" internal_address="2a01:260:4086:1282:100::8" dateTimeOpened="2020-03-12T07:53:43Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0
<session id="1134" closureReason="0" address="192.168.50.15" internal_address="2a01:260:4086:1282:100::4" dateTimeOpened="2020-03-13T09:35:50Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0
<session id="1135" closureReason="0" address="192.168.50.15" internal_address="2a01:260:4086:1282:100::4" dateTimeOpened="2020-03-13T09:35:50Z" username="admin" computerName="Mozilla/5.0 (Windows NT 10.0
</sessions>
<events>
<!--Audit query events.-->
<!--Sort compare function is QuerySorter::CompareOBJ TS-->
<event sessionId="1134" type="3" seq="76" dateTime="2020-03-13T10:16:55Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn/">
<event sessionId="1134" type="3" seq="77" dateTime="2020-03-13T10:25:34Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn" message="Changed properties: sys:Description, sy
<event sessionId="1134" type="4" seq="78" dateTime="2020-03-13T10:25:34Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn/">
<event sessionId="1134" type="12" seq="79" dateTime="2020-03-13T10:27:00Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn" message="Security Class change occurred from 'U
<event sessionId="1134" type="5" seq="80" dateTime="2020-03-13T10:27:27Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn" message="Full classification code: 'C-2-D-000000B
;cat1"]; [sys:eml:MessageId:&quot;81;OF00A238E;D6B7EC9B-0MC1258527;004801A1-C1258527;00485071@localdomain&quot;]; [sys:eml:Date:&quot;2020-03-10T14:10:23Z&quot;]; [sys:eml:From:&quot;yesna.zunko@imis
<event sessionId="1135" type="2" seq="82" dateTime="2020-03-13T10:43:50Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn/">
<event sessionId="1135" type="2" seq="81" dateTime="2020-03-13T10:43:43Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn" message="Full classification code: 'C-5-D-IS-100
-10T13:31:04;7872&quot;]; [sys:Modified:&quot;2020-03-13T10:25:34;0282&quot;]; [sys:Accessed:&quot;2020-03-13T10:44:57;1452&quot;]; [sys:ModifiedBy:&quot;admin&quot;]; [sys:Category:&quot;cat1&quot;]; [sys:eml:Me
<event sessionId="1135" type="3" seq="85" dateTime="2020-03-13T10:45:07Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn/">
<event sessionId="1135" type="22" seq="86" dateTime="2020-03-13T10:45:56Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn" message="Certificate of Approval.tif [Jnhmh8UX
<event sessionId="1135" type="4" seq="87" dateTime="2020-03-13T10:45:56Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn/">
<event sessionId="1134" type="2" seq="88" dateTime="2020-03-13T10:45:56Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn/">
<event sessionId="1134" type="3" seq="89" dateTime="2020-03-13T11:22:30Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn" message="Move appropriate document"/>
<event sessionId="1134" type="16" seq="90" dateTime="2020-03-13T11:22:30Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn" message="Content Shipping note [iox1R4V6MeRYaQK
<event sessionId="1135" type="2" seq="91" dateTime="2020-03-13T11:24:03Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn/">
<event sessionId="1135" type="3" seq="92" dateTime="2020-03-13T11:40:40Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn/">
<event sessionId="1135" type="3" seq="93" dateTime="2020-03-13T11:40:54Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn/">
<event sessionId="1135" type="16" seq="94" dateTime="2020-03-13T11:58:01Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn" message="Content Shipping note [iox1R4V6MeRYaQK
<event sessionId="1135" type="4" seq="95" dateTime="2020-03-13T11:58:01Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn/">
<event sessionId="1134" type="2" seq="96" dateTime="2020-03-13T11:58:02Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn/">
<event sessionId="1135" type="17" seq="97" dateTime="2020-03-13T11:58:05Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn" message="Certificate of Approval.tif [Jnhmh8UX
<event sessionId="1135" type="2" seq="98" dateTime="2020-03-13T11:58:15Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn/">
<event sessionId="1134" type="2" seq="99" dateTime="2020-03-13T12:56:15Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn/">
<event sessionId="1135" type="3" seq="100" dateTime="2020-03-13T13:01:15Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn/">
<event sessionId="1135" type="16" seq="101" dateTime="2020-03-13T13:01:15Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn" message="Content Shipping note [iox1R4V6MeRYaQ
<event sessionId="1135" type="2" seq="102" dateTime="2020-03-13T13:28:42Z" classificationCode="C-8-D-IS-100-419" context="._a2axJNwA7yMwV19qIXgFqQKQKcEn/">
</events>
</auditlog.query.resultset>

```

Image 312: Audit log created before the entity import

4.3.13 Export

Users who have the ImportExport role can export the complete classification scheme or any of its individual parts. Each entity is exported with all its metadata and content, while export of the audit log and additional metadata is optional. User-added metadata is not part of the entity's own metadata and is employed only for the purposes of the archiving procedure.

For more information on the export file format and file structure see chapter [Format of the import / export files](#).

For more information on server roles see chapter [Access in the IMiS®/ARCHive Server Manual](#).

4.3.13.1 Exporting the entire classification scheme

The user begins the procedure of exporting the entire classification scheme by selecting the Actions command in the command bar and the Export action in the popup menu before selecting the root class.

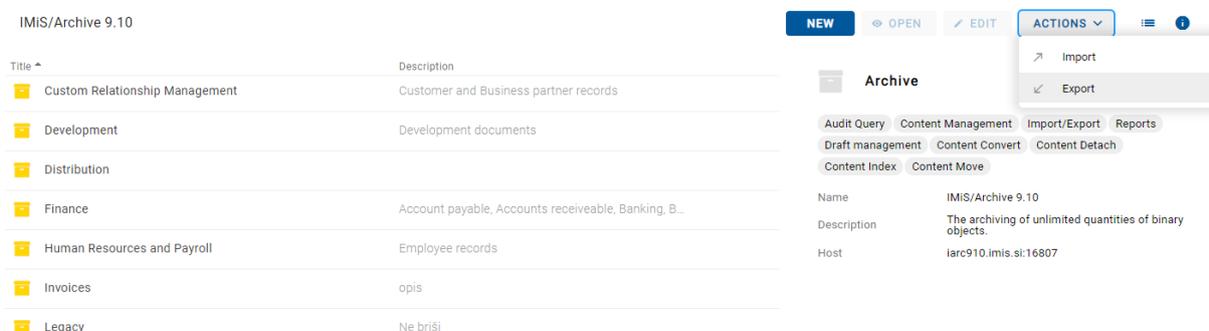


Image 313: Selecting the »Export« command at the level of the entire classification scheme

Opens a dialog box for setting the following export parameters:

- Scope: the user checks whether they want to perform an export on the entity currently selected in the classification scheme.
- Option: selecting additional export options:
 - Recursive
 - Export parents.
- Include: the user can include or exclude the following export settings:
 - Entity type: classes folders, documents.
 - Activity: the audit log of the individual exported entity.
 - Authenticity evidence: evidence on the entity's authenticity, if entity authenticity evidence has been created on the archive.
- Select metadata file: additional metadata from the XML file, which will be included in the export. For a description of the structure of the additional metadata file see chapter [Format of the additional metadata export file](#).

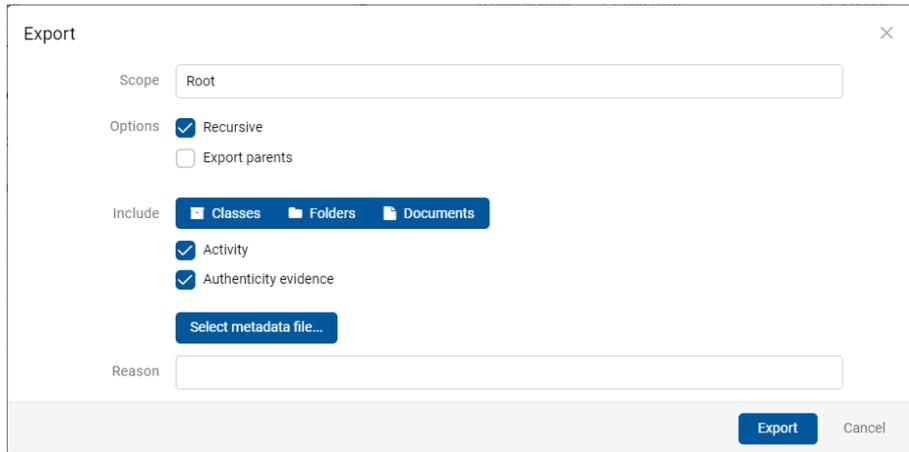


Image 314: Setting the export parameters on the entire archive

After completing the export of the entire classification scheme, the user is shown a notification in the bottom bar about saving the export file (IMiS_Archive Server.zip).

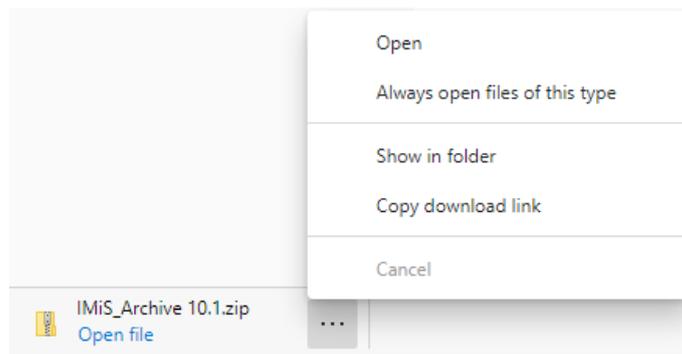


Image 315: Notification about saving a file of exported entities of the entire classification scheme

By selecting the Open command, export reports open for the user.

This PC > Downloads > IMiS_Archive 10.1							
Name	Type	Compressed size	Password protected	Size	Ratio	Date modified	
ExportData	File folder					3.07.2020 08:58	
ExportReport	Text Document	13 KB	No	121 KB	90%	3.07.2020 09:51	
ExportReport	XML Document	58 KB	No	248 KB	77%	3.07.2020 09:51	

Image 316: Information about the export of the entire classification scheme

By selecting the ExportReport, the user is shown a more detailed notification about the export.

```
Exporting scope: '3', subject: 'admin', recursive: true, exportParents: false, classes: true, folders: true, documents: true, auditLog: true, evidence: true

2020-09-22T16:08:56.827+0200 - Exported Class '3' into file ExportData/class_1.xml
2020-09-22T16:08:57.254+0200 - Exported Document '3/000033' into file ExportData/document_1.xml
2020-09-22T16:08:57.397+0200 - Exported Document '3/000034' into file ExportData/document_2.xml
2020-09-22T16:08:58.005+0200 - Exported Document '3/000042' into file ExportData/document_3.xml
2020-09-22T16:08:58.379+0200 - Exported Document '3/000044' into file ExportData/document_4.xml
2020-09-22T16:08:58.444+0200 - Exported Class '3.31' into file ExportData/class_2.xml
2020-09-22T16:08:58.578+0200 - Exported Document '3.31/000001' into file ExportData/document_5.xml
2020-09-22T16:08:58.679+0200 - Exported Folder '3-IS' into file ExportData/folder_1.xml
2020-09-22T16:08:59.094+0200 - Exported Document '3-IS/000002' into file ExportData/document_6.xml
2020-09-22T16:08:59.223+0200 - Exported Document '3-IS/000003' into file ExportData/document_7.xml
2020-09-22T16:08:59.314+0200 - Exported Folder '3-IS-IS' into file ExportData/folder_2.xml
2020-09-22T16:08:59.493+0200 - Exported Document '3-IS-IS/000001' into file ExportData/document_8.xml
2020-09-22T16:08:59.630+0200 - Exported Document '3-IS-IS-212' into file ExportData/document_9.xml
2020-09-22T16:08:59.735+0200 - Exported Document '3-IS-IS-514' into file ExportData/document_10.xml
2020-09-22T16:08:59.854+0200 - Exported Document '3-IS-IS-632' into file ExportData/document_11.xml
2020-09-22T16:09:00.093+0200 - Exported Document '3-IS-IS-710' into file ExportData/document_12.xml
2020-09-22T16:09:00.161+0200 - Exported Document '3-IS/Social-2020' into file ExportData/document_13.xml
2020-09-22T16:09:00.495+0200 - Exported Folder '3-IS-417' into file ExportData/folder_3.xml
2020-09-22T16:09:00.874+0200 - Exported Document '3-IS-CC-027' into file ExportData/document_14.xml
2020-09-22T16:09:00.874+0200 - Exported Document '3-IS-EXP-1000' into file ExportData/document_15.xml

Class entities: OK(2) Fail(0)
Folder entities: OK(3) Fail(0)
Document entities: OK(15) Fail(0)
```

Image 317: Display of a more detailed notification about the export of the entire classification scheme

4.3.13.2 Exporting of the classification scheme

The procedure of exporting an individual part of the classification scheme begins by selecting an entity in the classification scheme or from the list of entities.

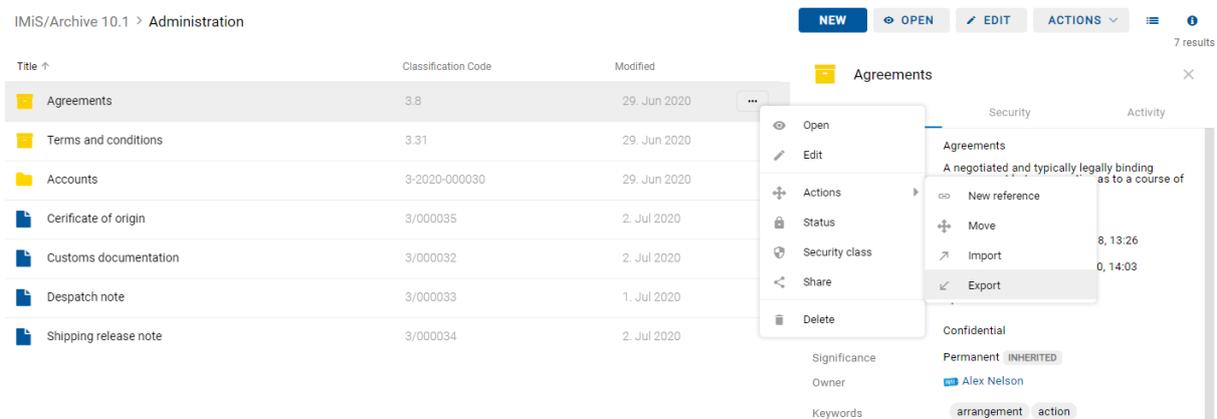


Image 318: Selecting the Export action on the selected entity

After selecting the Actions command in the command bar and the Export action in the popup menu, the user is shown a dialog box for setting the export parameters.

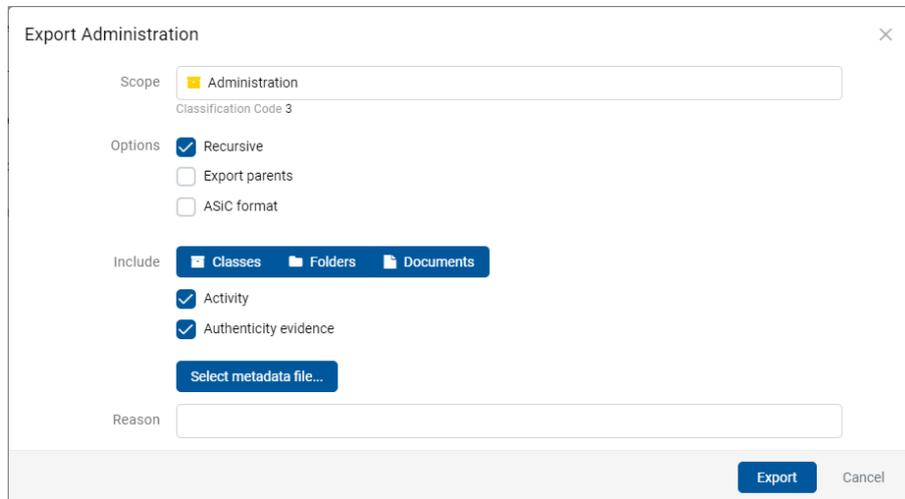


Image 319: Setting the export of the entity tree via a dialog box

In the Options section, in addition to the export settings described in chapter [Exporting the entire classification scheme](#), the user is also provided the following:

- **ASiC format:** interoperable forms of content export with the associated authenticity evidence. Export in the ASiC format enables only the export of a single selected entity. The ASiC format is in the “Extended” form, where multiple evidence is possible for the exported contents. The basic information is available at https://en.wikipedia.org/wiki/Associated_Signature_Containers.

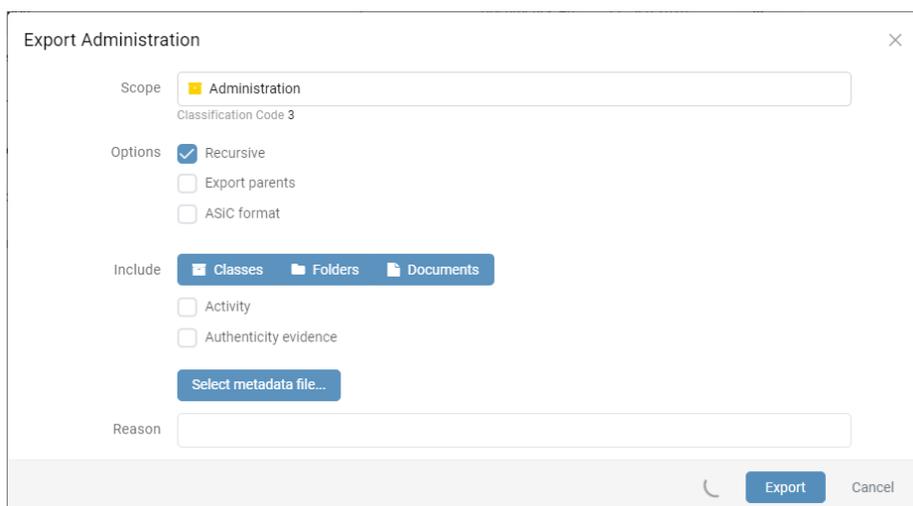


Image 320: Implementing the export of the entity tree

The entities are exported in the XML format to the default directory Downloads. The user can access the export details from the notification bar by selecting the action Open in the popup menu.

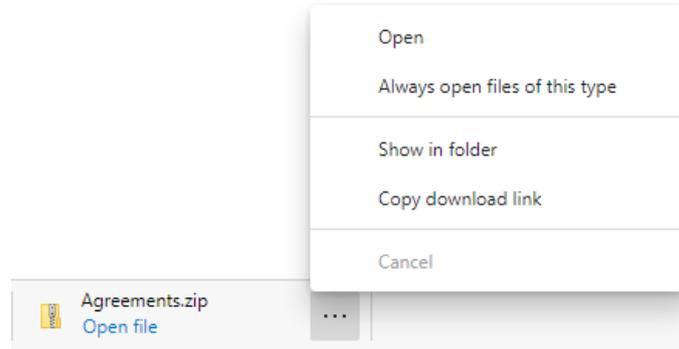


Image 321: Notification about saving a file of individual exported entities

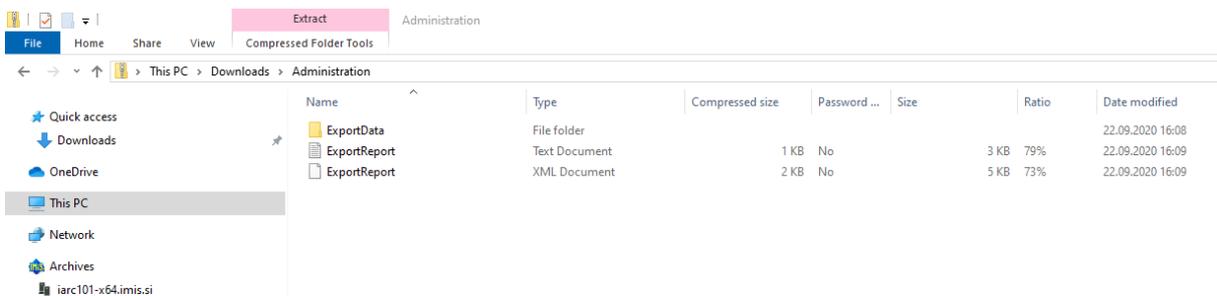


Image 322: Information about the export of a part of the classification scheme

Every export action from the IMiS®/ARChive Server is recorded in the Export folder located in the Administration system folder.

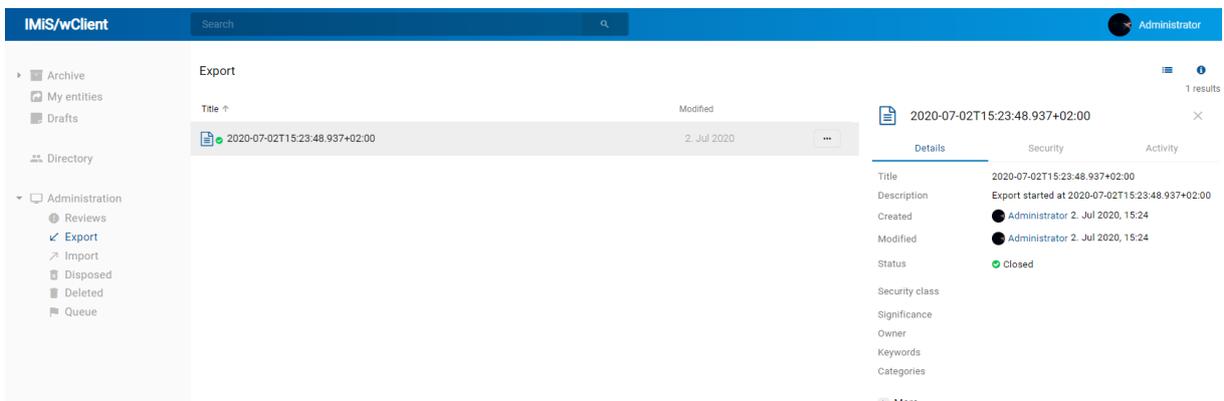


Image 323: Display of the Export folder in the Administration system folder and the document selected for export

The IMiS®/wClient enables the review of exported entities on the IMiS®/ARCHIVE Server, including export data. The exported entities reviewed by the user are prepared in the prescribed XML format.

For more information on the file format for export and the file structure see chapter [Format of the import / export file](#).

After creation is completed, the export report is given the status Closed. The user can open the report and perform the following actions:

- Open: opens the selected export report in reading mode.
- Edit: opens the selected entity in editing mode. Enables adding the export report metadata, and modifying and removing the report, metadata and contents.
- Actions: contains commands for various actions on the selected entity:
 - New reference: adding a connection to another report or entity in the classification scheme via a dialog box. For more information see chapter [Reference](#).
 - Move: moving the export report within the classification scheme on the archive.
 - Export: exporting the selected report from the archive.
- Status: modifying the status of the export report via a dialog box which enables giving the reason for the change.
- Security class: modifying the security class of the export report via a dialog box, which requires the user to give the reason for the change.
- Share: copying the link to the selected entity to be shared with other users.
- Delete: deleting the selected export report.

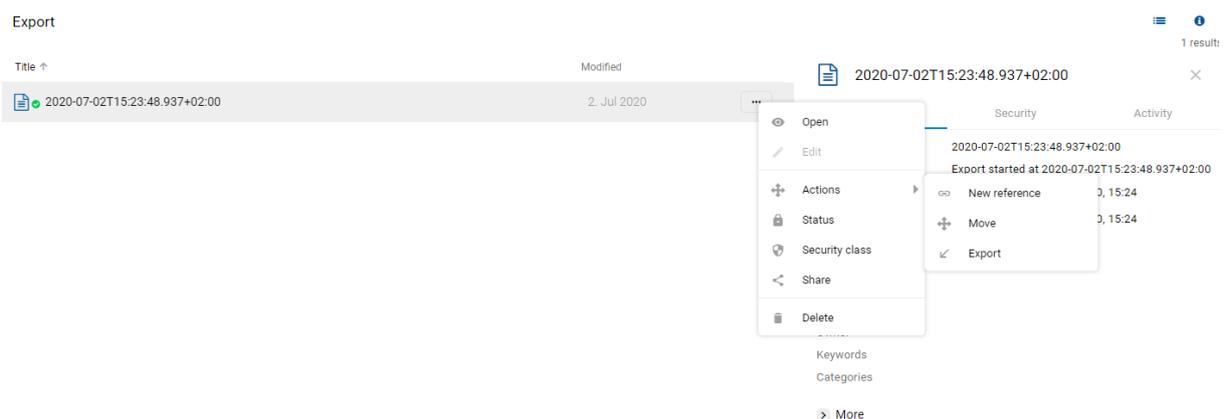


Image 324: Set of available actions on the export report

By selecting the popup menu on the export report, the user can choose from the following options:

- Preview: For more information on content preview see chapter [Content preview](#).
- Download: For more information on downloading content see chapter [Downloading content](#).
- Copy: copying the content to another document.
- Share: copying the link to the selected export report to be shared with other users.
- Manage:
 - Queue for Indexing. For more information on indexing content see chapter [Indexing content](#).
 - Queue for Conversion. For more information on content conversion see chapter [Content conversion](#).

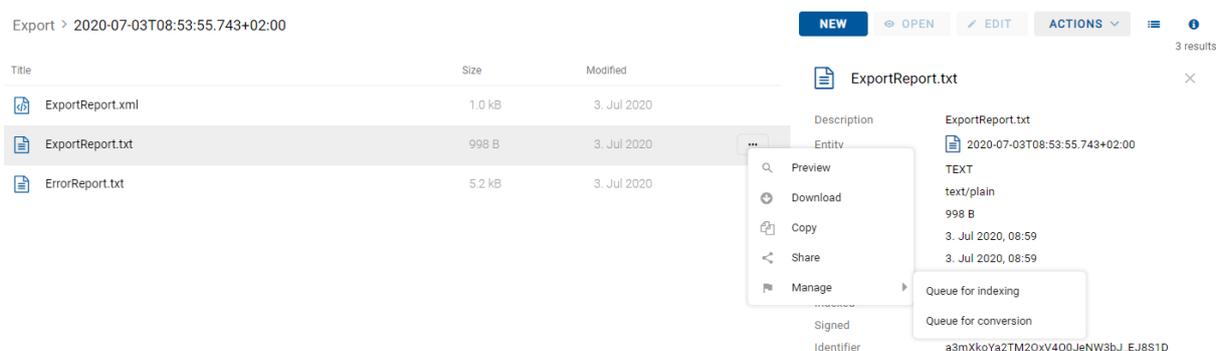


Image 325: Popup menu on the export report

4.3.13.3 Export procedure

At the start of the export procedure, the IMiS®/wClient creates a new document in the folder Export located in the Administration system folder. This document contains a report on the export from the archive server.

The title of the document is identical to the date and time of export, in ISO format. The status of the document is Opened.

During exporting, the export document is completed with the following two or three log files:

- ExportReport.xml: XML file that contains:
 - Statistics of successfully and unsuccessfully exported entities.
 - List of failed export attempts (including the classification codes).
 - List of successfully exported files (including hash values and full classification codes).

- **ExportReport.txt:** which contains a report for each successfully or unsuccessfully exported entity.
- **ExportReport_ERROR.txt:** which contains a report for each failed export attempt, including the error received.

```

← 2020-07-03T08:53:55.743+02:00 > ErrorReport.txt
1 2020-07-03T08:59:04.922+02:00 - ERROR: Unable to export '1/000121' content part 'Ho_27p2kZLI60-XKOETp66vS4Lskgde'. Error java.net.SocketException: Connection reset Exception class org.apache.catalina.connector.CI
2 at com.imis.storageconnector.services.utils.Utils.write(Utils.java:123)
3 at com.imis.storageconnector.services.utils.Utils.write(Utils.java:114)
4 at com.imis.storageconnector.services.app.EntityExport.exportContentPart(EntityExport.java:458)
5 at com.imis.storageconnector.services.app.EntityExport.exportEntity(EntityExport.java:729)
6 at com.imis.storageconnector.services.app.EntityExport.exportAllSubEntities(EntityExport.java:259)
7 at com.imis.storageconnector.services.app.EntityExport.exportAllSubEntities(EntityExport.java:262)
8 at com.imis.storageconnector.services.app.EntityExport.exportEntities(EntityExport.java:385)
9 at com.imis.storageconnector.services.app.EntityExport.build(EntityExport.java:929)
10 at com.imis.storageconnector.services.io.rest.resource.ArchiveResource$4.write(ArchiveResource.java:2871)
11 Caused by: Exception class java.net.SocketException: Connection reset
12 at com.imis.storageconnector.services.utils.Utils.write(Utils.java:123)
13 at com.imis.storageconnector.services.utils.Utils.write(Utils.java:114)
14 at com.imis.storageconnector.services.app.EntityExport.exportContentPart(EntityExport.java:458)
15 at com.imis.storageconnector.services.app.EntityExport.exportEntity(EntityExport.java:729)
16 at com.imis.storageconnector.services.app.EntityExport.exportAllSubEntities(EntityExport.java:259)
17 at com.imis.storageconnector.services.app.EntityExport.exportAllSubEntities(EntityExport.java:262)
18 at com.imis.storageconnector.services.app.EntityExport.exportEntities(EntityExport.java:385)
19 at com.imis.storageconnector.services.app.EntityExport.build(EntityExport.java:929)
20 at com.imis.storageconnector.services.io.rest.resource.ArchiveResource$4.write(ArchiveResource.java:2871)
21 2020-07-03T08:59:04.926+02:00 - ERROR: Unable to export '1/000121' content part 'Ho_27p2kZLI60-XKOETp66vS4Lskgde'. Error java.net.SocketException: Broken pipe (Write failed) Exception class org.apache.catalina.co
22 at com.imis.storageconnector.services.app.EntityExport.exportContentPart(EntityExport.java:467)

```

Image 326: An example of an error report in the export procedure

The status of the document then changes to Closed.

If there is an error while the export document is being completed, it will remain in the system class in its raw form and with an Open status.

If there is an error during the export of an entity queued for export, the sub-entities it contains will not be exported. In case a sub-entity encounters an error during import, the other sub-entities will still be exported, providing the export of the parent entity was successful.

Export > 2020-07-03T08:53:55.743+02:00

Title	Size	Modified
ExportReport.xml	1.0 kB	3. Jul 2020
ExportReport.txt	998 B	3. Jul 2020
ErrorReport.txt	5.2 kB	3. Jul 2020

2020-07-03T08:53:55.743+02:00

Details	Security	Activity
Title	2020-07-03T08:53:55.743+02:00	
Description	Export started at 2020-07-03T08:53:55.743+02:00	
Created	Administrator 3. Jul 2020, 08:59	
Modified	Administrator 3. Jul 2020, 08:59	
Status	Closed	
Security class		
Significance		
Owner		
Keywords		
Categories		
Save Log		
More		

Image 327: Export report

By selecting the ExportReport, the user is shown a more detailed notification about the export.

```
← 2020-07-03T14:38:53.125+02:00 > ExportReport.txt
1 Exporting scope:'3', subject:'admin', recursive:true, exportParents:false, classes:true, folders:true, documents:true, auditLog:true, evidence:true
2
3 2020-07-03T14:38:53.289+0200 - Exported Class '3' into file ExportData/class_1.xml
4 2020-07-03T14:38:53.609+0200 - Exported Document '3/000032' into file ExportData/document_1.xml
5 2020-07-03T14:38:53.799+0200 - Exported Document '3/000033' into file ExportData/document_2.xml
6 2020-07-03T14:38:53.936+0200 - Exported Document '3/000034' into file ExportData/document_3.xml
7 2020-07-03T14:38:54.034+0200 - Exported Document '3/000035' into file ExportData/document_4.xml
8 2020-07-03T14:38:54.135+0200 - Exported Folder '3-2020-000030' into file ExportData/folder_1.xml
9 2020-07-03T14:38:54.291+0200 - Exported Document '3-2020-000030/000001' into file ExportData/document_5.xml
10 2020-07-03T14:38:54.552+0200 - Exported Document '3-2020-000030/000002' into file ExportData/document_6.xml
11 2020-07-03T14:38:54.659+0200 - Exported Document '3-2020-000030/000003' into file ExportData/document_7.xml
12 2020-07-03T14:38:54.725+0200 - Exported Class '3.31' into file ExportData/class_2.xml
13 2020-07-03T14:38:54.819+0200 - Exported Class '3.8' into file ExportData/class_3.xml
14
15 Class entities: OK(3) Fail(0)
16 Folder entities: OK(1) Fail(0)
17 Document entities: OK(7) Fail(0)
18
```

Image 328: Display of a more detailed notification about the export

***Warning:** The user can export different entities into the selected export folder several times, without having to delete previous export files. When saving exported entities into the selected folder, the previous export files are overwritten.*

4.3.14 Deletion of an entity

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

To learn how to check the effective rights of a user see chapter [Entity information](#).

The IMiS®/wClient enables two ways of removing an entity from the classification scheme:

- Immediate deletion.
- Marking an entity for later deletion (delete queue).

4.3.14.1 Immediate deletion of an entity

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.

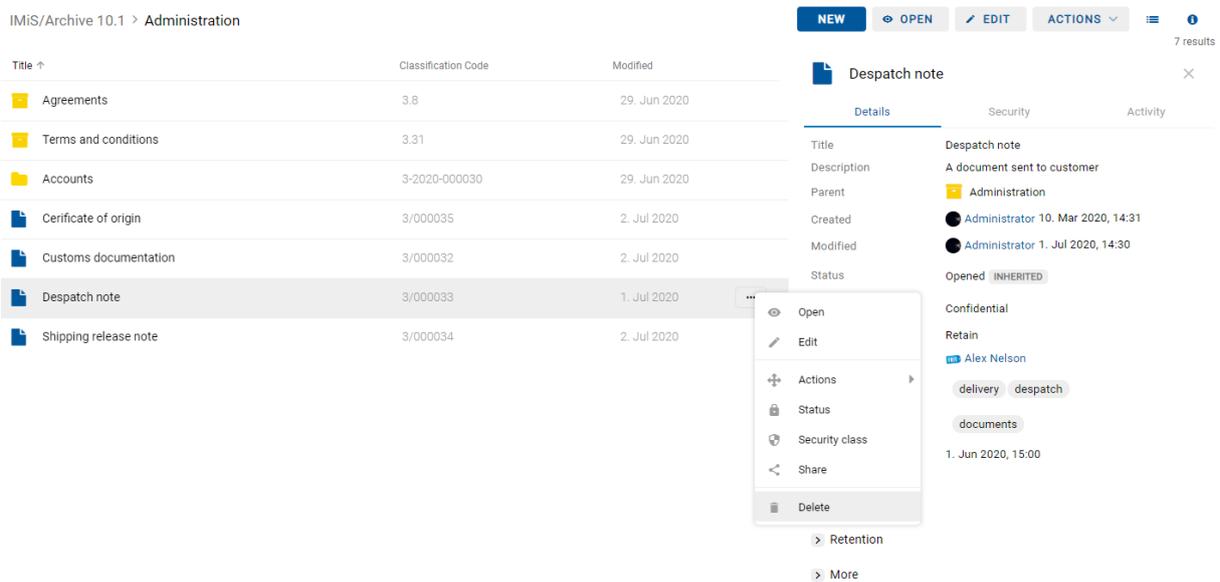


Image 329: Selecting the Delete command

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

The screenshot shows a 'Delete' dialog box with the following fields:

- Entity: Despatch note
- Classification Code: 3/000033
- Description*: A document sent to customers
- Reason to delete*: Obsolete

Buttons: Delete, Cancel

Image 330: A dialog box for deleting an individual entity

When deleting multiple entities simultaneously, the user marks the entities and in the menu on one of the entities selects the action Delete. In the dialog box the user gives the reason for the deletion and the potentially missing entity description for each entity.

Delete 2 entities [X]

Entity:

Classification Code:

Description*:

Entity:

Classification Code:

Description*:

Reason to delete*:

[DELETE] [CANCEL]

Image 331: A dialog box for deleting multiple entities

The user has the option of defining a single description for all selected entities (“Description for all entities”). The user does that by checking the checkbox.

Delete [X]

Description for all entities

Entity:

Classification Code:

Entity:

Classification Code:

Entity:

Classification Code:

Entity:

Classification Code:

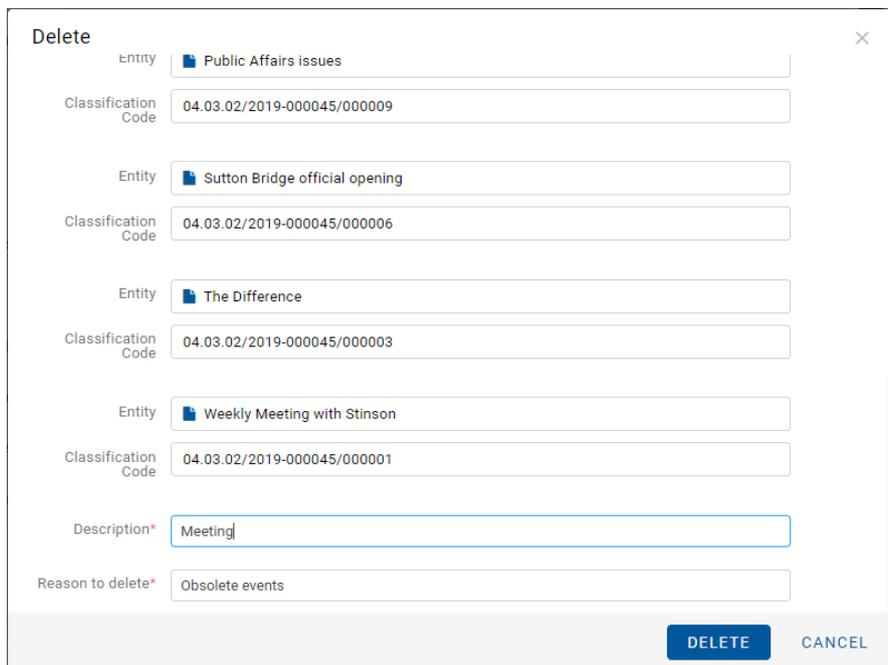
Description*:

Reason to delete*:

[DELETE] [CANCEL]

Image 332: Selecting a single description for all entities selected for deletion

Before confirming the deletion, the user defines a single description for all selected entities (“Description”) and the “Reason to delete”.



The screenshot shows a 'Delete' dialog box with a close button (X) in the top right corner. It contains the following fields:

- Entity: Public Affairs issues
- Classification Code: 04.03.02/2019-000045/000009
- Entity: Sutton Bridge official opening
- Classification Code: 04.03.02/2019-000045/000006
- Entity: The Difference
- Classification Code: 04.03.02/2019-000045/000003
- Entity: Weekly Meeting with Stinson
- Classification Code: 04.03.02/2019-000045/000001
- Description*: Meeting
- Reason to delete*: Obsolete events

At the bottom right, there are two buttons: 'DELETE' and 'CANCEL'.

Image 333: Selecting a single description for all selected entities

After the reason for the deletion has been entered, the command OK, or Delete in the case of deleting multiple entities, is enabled.

4.3.14.2 Marking an entity for later deletion

If the user has the Write access right on the entity but does not have the Delete access right, user is able to mark the entity for later deletion. For the display of a user's current effective access rights see chapter [The Security tab](#).

All types of entities can be marked for later deletion. The procedure is as follows:

1. User finds and selects the entity he wishes to mark for later deletion.
2. By choosing the Edit command, the selected entity is opened in editing mode.
3. In the first tab Details, select the Significance attribute. Change the value of this attribute to Delete in the pick list of possible attribute values.
4. When the value of the Significance attribute is changed, save the entity using the Save command. The new value Delete is then stored to the server.

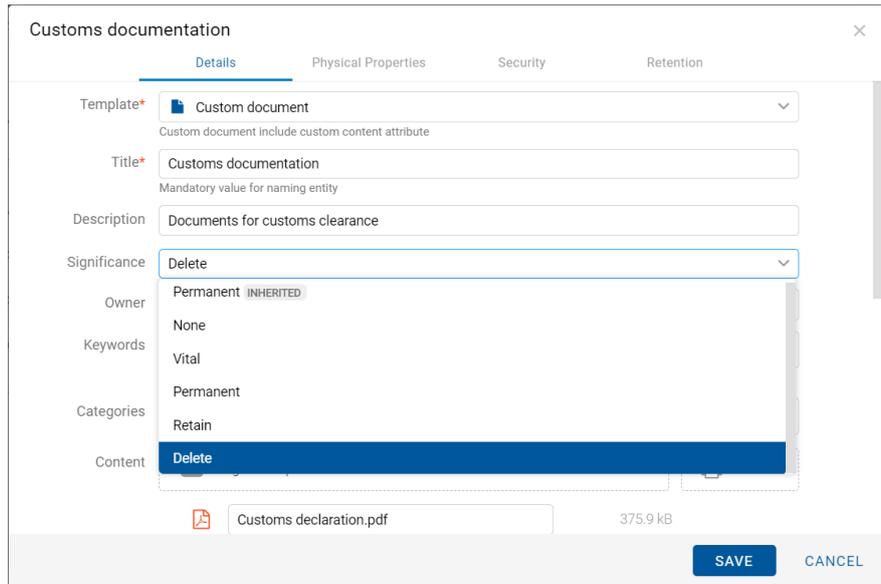


Image 334: Marking an entity for later deletion

4.3.14.3 Managing the delete queue

Entities whose Significance attribute is set to Delete appear in the list of entities waiting for deletion. This list is found in the Queue folder in the Trash folder in the Administration« system folder.

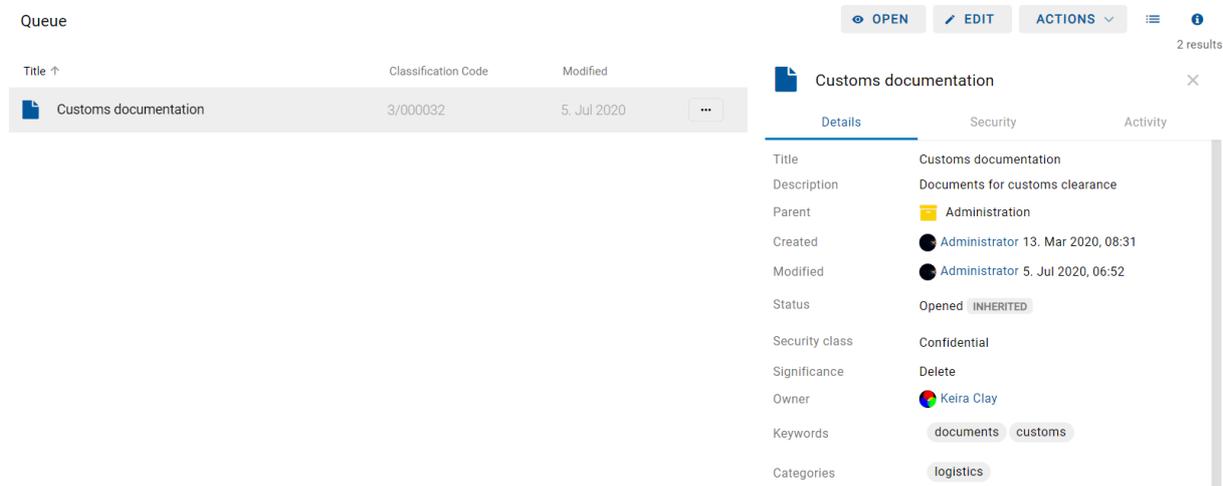


Image 335: A list of entities suggested for deletion in the Delete queue list folder

By selecting the Queue folder, the central view shows all the entities that were marked for deletion by various users.

Besides the title of the entity, the central view also shows the user information about the classification code, description and the last modified date.

A user is responsible for checking the exact content of the entities and making the final decision whether or not to delete them. If deletion is warranted, the entity is deleted by choosing the Delete command in the popup menu on the entity selected from the list. For more information on deletion procedure see chapter [Immediate deletion of an entity](#).

If a user decides the entity should not be deleted, user can remove it from the delete queue. This is done by changing the Significance attribute of the entity to a value other than the Delete value.

The procedure for removing an entity from the delete queue list is as follows:

1. A user selects the entity to remove from the list.
2. By choosing the Edit command in the top command bar, the selected entity is opened in editing mode.
3. In the first tab Details, the user selects the Significance attribute.
4. The value of this attribute has to be changed from Delete to a different value in the pick list of possible values.
5. When the value is changed, the entity is saved using the Save command.

The new value of the Significance attribute is stored to the server.

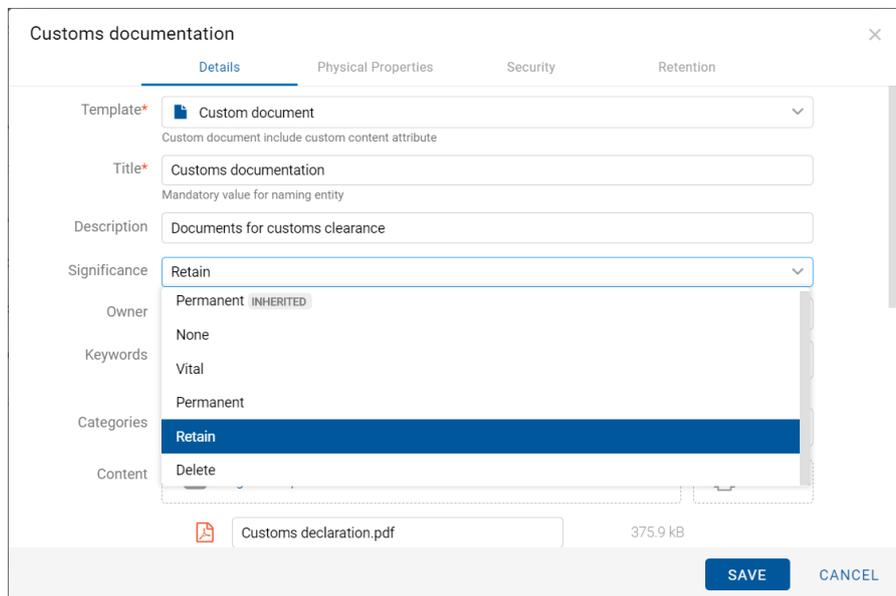


Image 336: Removing an entity from the delete queue list

Once you refresh the delete queue list, the entity will no longer appear there. You can still find it in its old location in the classification scheme.

4.3.14.4 Deleted entities

Each entity deleted by the user is located in its basic form in the Deleted subfolder of the Trash folder in the Administration system folder.

By selecting the Trash folder, the central view will display all the deleted entities.

The list of deleted entities shows the following entity information:

- Title: the title of the deleted entity.
- Classification code: the classification code of the deleted entity.
- Deleted: the date and time of deleting the entity from the archive server.
- Description: a required description of the deleted entity. If an entity had no description before deletion, the delete action requires the input of a description.

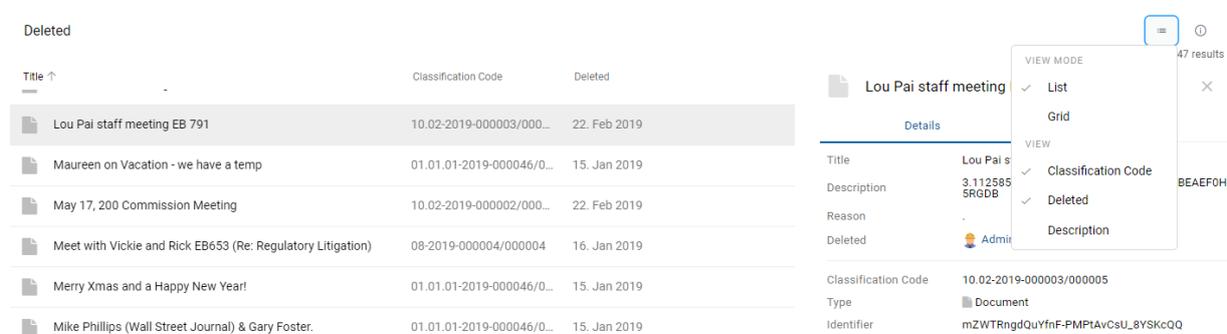


Image 337: Display of the Deleted folder in the Administration system folder

Note: by selecting the  icon, the user defines which columns will be displayed in the review of deleted entities.

The user can check or uncheck Classification code, Deleted and Description. The Title of the draft is mandatory.

The title, description and classification code are the only attributes still preserved when an entity has been deleted. All other metadata of the entity is erased and replaced with the following attributes:

- Reason: the reason for deletion as it was input by the user when removing the entity.
- Deleted: the name of the user who deleted the entity and the date and time of entity deletion.
- Identifier: unique identifier of the deleted entity.

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 or 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.
AppendOnly	Attribute values may only be appended.
IncludeInAIP	Attribute values are part of the archive information package.
Full text indexed	Attribute values are indexed.

Table 6: 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. The table below lists and describes all the general system attributes.

Name	Description
Classification code	<p>Contains the entity's classification code within the classification scheme. The classification code is generated automatically on the archive server.</p> <p><i>Example: The classification code 01-2019-00004/00001 represents document 00001, located inside folder 2019-00004, located inside class 01. The classification code is a publicly accessible type of metadata.</i></p>
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	<p>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.</p> <p>The possible values are:</p> <ul style="list-style-type: none"> • 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.
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	<p>Saves/contains the significance rating of the entity. Significance is a required metadata for folders and documents. It is public metadata that enables search.</p> <p>The possible values are:</p> <ul style="list-style-type: none"> • Vital: entity is vital. • Permanent: entity is permanent. • Retain: entity should be retained. • Delete: entity is queued for deletion.

Security class	<p>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.</p> <p>The possible predefined values are:</p> <ul style="list-style-type: none"> • 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	<p>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.</p>
Owner	<p>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.</p>
Keywords	<p>Saves/contains keywords related to the entity. This attribute can have multiple values and is a public metadata that enables search.</p>
External Ids	<p>Saves/contains external identifiers of the entity. This attribute can have multiple unique values and is a public metadata that enables search.</p> <p><i><u>Warning:</u> When entering values, keywords should be separated using the Enter key or the semicolon character (;).</i></p>
Save log	<p>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</p>

Table 7: Description of general system attributes

4.4.2 Security class change attributes

Security class change attributes are created by the IMiS®/ARChive Server when an entity's security class is changed. They store the agent of the change, the reason and date of the change, and the value before and after the security class change.

Name	Description
Agent	Contains the agent (user who changed the entity's security class).
Reason	Contains the reason for the security class change.
Modified date	Contains the date and time the security class was changed.
Before change	Contains the security class value prior to the change.
After change	Contains the security class value after the change.

Table 8: Description of security class change attributes

4.4.3 Moved entity attributes

Moved entity attributes are created by the server when an entity is moved. They store the agent of the move, the reason and the date.

Name	Description
Agent	Contains the agent of the move.
Reason	Contains the reason for the move.
Moved date	Contains the date and time the entity was moved.

Table 9: Description of moved entity attributes

4.4.4 Deleted entity attributes

Deleted entity attributes are created by the server when an entity is deleted. They store the agent of deletion, the classification code, the reason for the deletion and its date.

Name	Description
Agent	Contains the agent of the delete action.
Classification code	Contains the classification code of the deleted entity.
Reason	Contains the reason for the entity's deletion.
Deleted date	Contains the date and time the entity was deleted.

Table 10: Description of deleted entity attributes

4.4.5 Transferred entity attributes

Transferred entity attributes are created by the server when an entity is imported.

They store the system identifier, the classification code of the transferred entity, the audit log and the date of import.

Name	Description
System Id	Contains the unique system identifier of the transferred entity.
Classification code	Contains the classification code of the transferred entity.
Audit log	Contains the audit log of the transferred entity.
Imported date	Contains the date and time the entity was transferred.

Table 11: Description of moved entity attributes

4.4.6 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 12: Description of email attributes

4.4.7 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.

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: <ul style="list-style-type: none"> - 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 13: Description of physical content attributes

4.4.8 Review process attributes

Review process attributes are available only during review processes.

Name	Description
Members	Users who perform review process.
Action	By selecting one of the valid values, you influence the review process. Valid values: <ul style="list-style-type: none"> • Reviewing: the value represents the action of reviewing entities in the review process and does not influence the server. • Complete: the value represents the action of completing the review process on the server. • Discard: the value represents the action of canceling the review process on the server.
Comments	Optional attribute which is used for entering various comments, explanations and other information that is in any way connected with the review process.
Message	Short error description entered by IMiS®/ARChive Server. In the event of an error during the preparation or implementation phase of the review process. Also recorded in the attribute is the successful completion of the review process.

Name	Description
State	<p>This value is set by IMiS®/ARCHive Server during the review process.</p> <p>Valid values:</p> <ul style="list-style-type: none"> • Unknown: this value represents an invalid state of the review process. • Created: this value is set by the server when the user creates a new review. • Preparing: this value is set by the server during the content creation phase for the review process. • InReview: this value is set by the server after successfully creating the entities for the review process. • Completing: this value is set by the server when beginning of the review process. • Completed: this value is set by the server after successfully implementing the review process. • Discarded: this value is set by the server after successfully canceling the review process. • Failed: this value is set by the server if an irreparable error occurred during implementation or cancellation.
Scope	<p>Represents the classification code of the entity under which the preparation phase of the review process will be implemented. If this value is not present, the preparation is implemented on the entire archive.</p>
Query	<p>This value represents the query which will/has captured entities for the review processes. This value is set if the Ad hoc function was selected for creating the process.</p>

Table 14: Description of review process attributes

4.4.9 Entity attributes in the decision-making process

Decision-making entity attributes are available only to the entity undergoing the process.

Name	Description
Classification code	Contains the entity classification code in the classification scheme.
Title	Title of the selected entity.
Action	Contains the action which will be implemented over the selected entity during the execution process. This value is copied from the effective retention policy.
Reason	Contains the reasons for the action to be implemented over the entities. This value is copied from the effective retention policy.
Comment	Contains a random comment which is entered during the transfer process.
Transferred	<p>This attribute value states whether the entity transfer was successful or not.</p> <p>Valid values: "true" or "false".</p>
Transfer id	Contains a value that represents a reference to the transferred entity.

Table 15: Description of entity attributes in the decision-making process

4.5 Authenticity

The IMiS®/wClient ensures the authenticity of stored electronic records for the lifelong duration of storage.

4.5.1 Digital certificate

The digital certificate and the private key are issued by a trusted Certificate Authority (CA) that manages the certificates. The certificate contains information that uniquely identifies the person who owns it. In addition to the private key disclosed only to the holder, it also contains a certified copy of the public key, which is used by third parties to verify the authenticity of content electronically signed using the certificate.

The public key and electronic signature authenticate the identity of the private key's holder.

Qualified digital certificates are used for:

- Secure internet communication using the SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols.
- Secure email traffic using the S/MIME (Secure Multipurpose Internet Mail Extensions) protocol.
- Encryption and decryption of data in electronic form.
- Digital signing of data in electronic form, and the verification of the key holder's identity.
- Services or applications that require the use of qualified digital certificates.
- Safe deletion of data in electronic form.

4.5.1.1 Checking the validity of the digital certificate

Each time it saves an electronically signed content in the PDF/A, TIFF or XML formats or an email message in the EML format, the IMiS®/ARChive Server automatically checks the validity of the digital certificate using the Certificate Revocation List (CRL) of the issuing authority.

During the validity checking procedure, the IMiS®/ARChive Server sends the serial number of the certificate to the trusted authority's digital certificate server. The server, which frequently updates certificate revocation lists, then sends electronically signed information about the certificate's status to the user.

4.5.1.2 Revocation of the digital certificate

A trusted certificate authority can revoke their certificate(s), making them invalid.

The authority's digital certificate server contains lists of active and revoked certificates.

The Certificate Revocation List (CRL), based on the X.509 standard, shows a list of certificates (ID code, date and time of revocation) that were revoked by the authority before having expired.

4.5.2 Electronic signature

Electronic signatures are based on asymmetrical cryptography. Users signs content with their own private key. The private key is only accessible to a particular user and is saved in their digital certificate, protected by a password. The password is set by the user upon installation and can also be changed later.

The public key is accessible to anyone, and the trusted certificate authority (CA) guarantees it belongs to a particular organization. Anyone can verify the organization's digital signature by processing it with the corresponding public key.

The electronic signature proves the authenticity and integrity of a signed document. It enables recognition of the signer, confirms the content has not been modified, and provides a link between the signer and the signed content.

Any change to the content of a document or its metadata will make the signature invalid.

4.5.2.1 Process of electronic signing

Using the electronic signature, the user integrates data from the digital certificate with the content of the document. On the basis of a hash algorithm, the complete content of the document is transformed into a unique string of data (digital fingerprint), which is encrypted with the user's private key. The private key is stored in the digital certificate or in a separate private key storage location, depending on the settings.

The digital fingerprint is integrated with the content of the document along with information about the digital certificate and the corresponding public key, but not the private key.

Note: The IMiS®/wClient does not (yet) enable the electronic signing of TIFF and PDF/A-type files.

4.5.2.2 Verifying the validity of the electronic signature

The recipient of a signed document uses the signer's public key to verify the validity of the document. The public key is found in the signer's digital certificate, which is also stored in the signed document. If the signature is valid, this confirms the document was saved by the signer and was not modified since then. The validation procedure also checks the validity of the signer's digital certificate.

The IMiS®/wClient enables the verification of electronic signatures during document capture or when documents are being saved. The entire procedure is performed on the IMiS®/ARChive Server for the document formats PDF/A, TIFF, XML, and for EML email messages.

The server then communicates the verification results to the client.

The verification message is displayed as a popup window in the bottom part of UI.

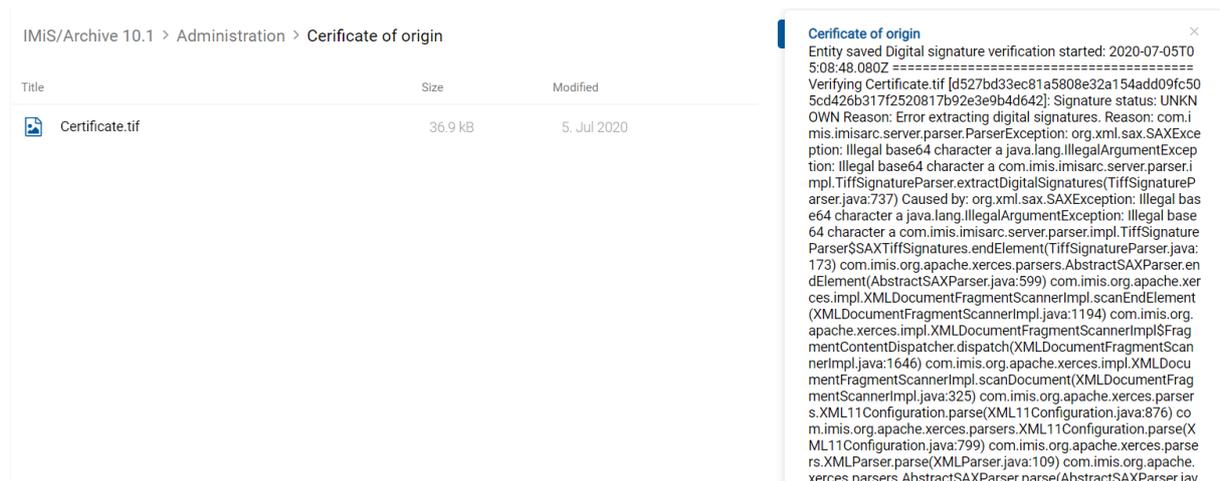


Image 338: Popup window containing the result of the document's electronic signature verification.

The popup window automatically closes after a few seconds. The signature is automatically verified when a document is being archived to the server. The archive server also saves documents with invalid electronic signatures.



Image 339: Example of a report for a valid electronic signature and valid digital certificate

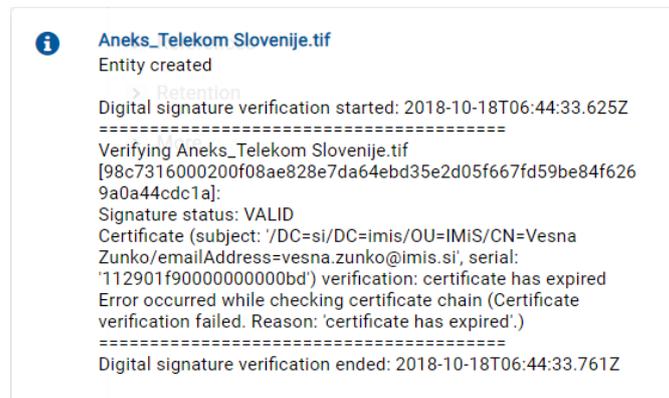


Image 340: Example of a valid electronic signature and an expired digital certificate

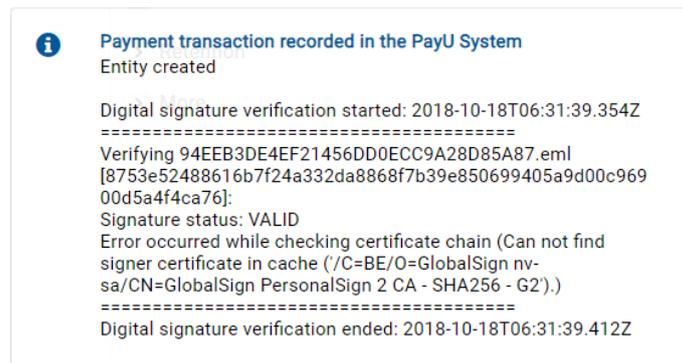


Image 341: Example of a valid electronic signature for which the certification authority could not be verified.

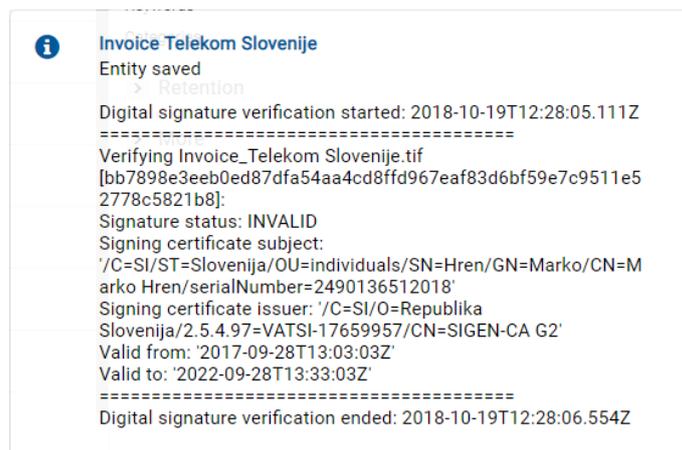


Image 342: Example of an invalid electronic signature due to a modification of the document after signing.

4.6 Review process

Each entity in the classification scheme has its own life span. Each class, folder or document classified directly under a class must have at least one retention period set, which specifies the time frame for the retention of an individual entity in the archive.

In addition to the time frame, the retention policy also contains the default action which will be implemented in the review process. This action can be changed by the team members during a controlled and planned process of implementation the transfer, disposition or permanent retention of the content.

IMiS®/wClient enables the user to:

- Prepare the review process.
- Review and select entities during the decision-making process.
- Implement the review process.
- Transfer selected entities.
- Review the content of documents.
- Review the selected retention periods.
- Transfer save log.

All activities in the review process are implemented in the “Reviews” folder, classified under the Administration system folder.

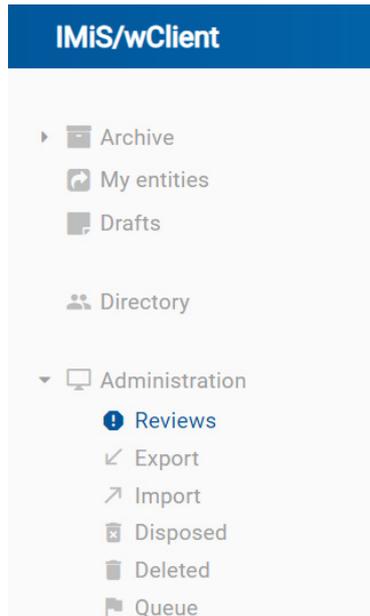


Image 343: The Reviews folder in the left view

The review process can be implemented by users with the Read access rights, which grants them access to the Reviews folder. Creating reviews is enabled for users with the Create entities right.

4.6.1 Preparation phase

In the left view, the user selects the Administration system folder in which the Reviews folder is located. By selecting the folder, the central view shows the already prepared Reviews, if any.

Title	Description	Modified
Review P4 July 2019	Ad-hoc Review [owner=anelso...	23/9/2019
Review A8 June 2019	10-years Regular Review with ...	23/9/2019
Review 2-years D6 May 2019	2-years Regular Review	23/9/2019
Review K12 April 2019	3-years Regular Review	23/9/2019
Review G-3 March 2019	10-years Regular review G3	23/9/2019

Name	Description
IMIS/Archive 9.10	The archiving of unlimited quantities of binary objects.
Host	iarc910.imis.si:16807

Image 344: A list of reviews in the review process

By selecting the New command, a pop-up menu appears, where the user selects the:

- Type
- Retention policy
- Scope
- Reason.

4.6.1.1 Review types

The user can choose the following two modes for creating a review of selected entities:

- Regular: Preparation of review based on selected retention periods.
- Ad hoc: Preparation of review based on the query provided. It is used when transferring entities to a third archive.

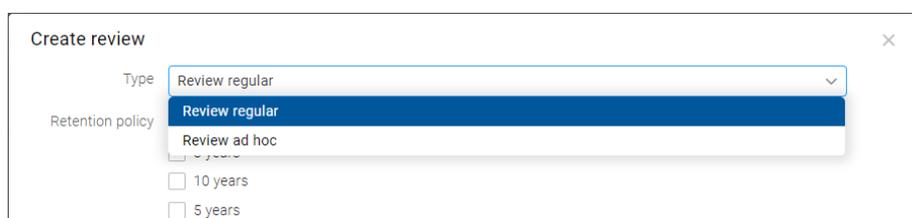


Image 345: Selecting the review type

4.6.1.1.1 Regular review

When selecting the default value Regular review, the user also selects the:

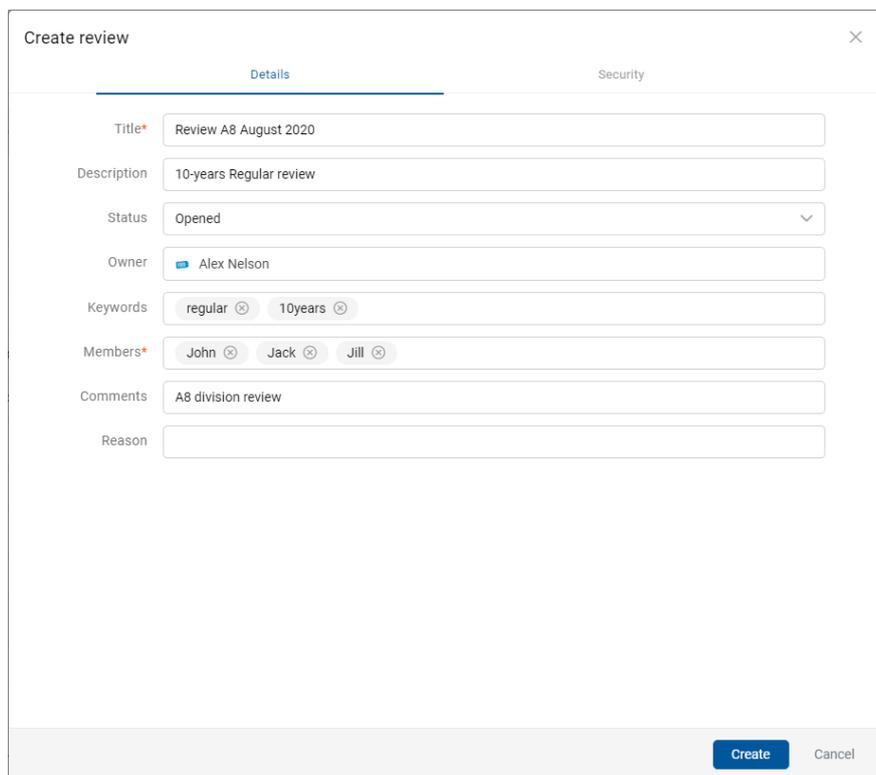
- Retention policy: a list of retention periods for the review process.



Image 346: Creating a new Regular review in the preparation phase

- Scope: selecting the entire archive or entity under which the review will be implemented.
- Reason: the reason for creating the review.

After confirmation with the Next command, the user is shown the attributes of a new review in the review process in the Details tab.



The screenshot shows a 'Create review' dialog box with two tabs: 'Details' (active) and 'Security'. The 'Details' tab contains the following fields:

- Title*: Review A8 August 2020
- Description: 10-years Regular review
- Status: Opened (dropdown menu)
- Owner: Alex Nelson
- Keywords: regular, 10years
- Members*: John, Jack, Jill
- Comments: A8 division review
- Reason: (empty field)

At the bottom right of the dialog, there are 'Create' and 'Cancel' buttons.

Image 347: Display of Regular review attributes in the review process

In the Security tab the user with the appropriate rights defines the access permissions for users, groups and attributes of the directory entity type. For more information on defining access permissions see chapter [Entity access](#).

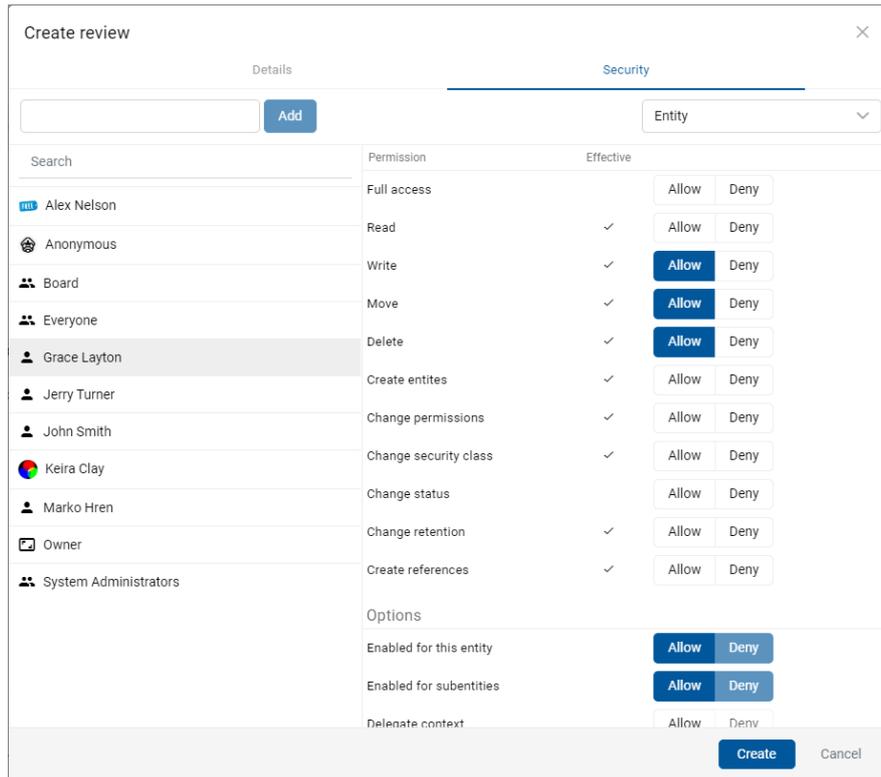


Image 348: Access permissions for Regular review in the Security tab

After entering the metadata, the user saves the review to IMiS®/ARCHive Server by selecting the action Create.

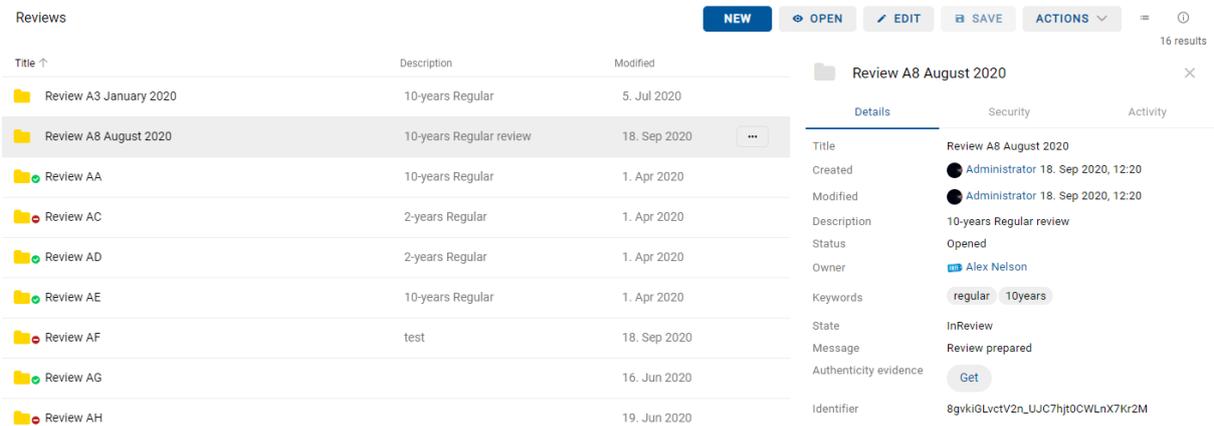


Image 349: Display of the saved Regular review

The Details tab contains the following information on review:

- Title: the title of the review.
- Created: the user that created the review and the date and time of creating the review.
- Modified: the user that last edited the review and the date and time of the last change to the review.
- Description: a short description of the review.
- Status: the status of the review.
- Owner: a directory (user or group) entity that is responsible for the selected review.
- Keywords: keywords related to the review. Attribute can have multiple values.
- State: the state of the review.
- Message: a message to the user regarding the review process.
- Authenticity evidence: obtaining authenticity evidence of the selected review. In case authenticity evidence for the selected entity already exists on the archive, the user can obtain authenticity evidence by selecting the icon  in the Details tab in the right view. For more information see chapter [Acquiring the authenticity evidence](#).
- Identifier: the identifier of the review.

The entities imported by a user with the ImportExport role have to be compressed (.zip) and prepared in the prescribed XML format.

4.6.1.1.2 Ad-hoc review

After selecting the Ad hoc command, the following fields for entering the value of the attribute Expression appears to the user:

- Expression: query based on which a list of selected entities will be created.
- Scope: selecting the entire archive or entity under which the custom review will be implemented.
- Reason: the reason for creating the custom review.

Create review [X]

Type: Review ad hoc

Expression: [sys:owner]='*anelson*

Scope: Administration

Reason: Review under Administration root class for selected directory entity only

NEXT CANCEL

Image 350: Entering a search expression in the Ad hoc review

After confirmation by clicking on the Next button, a dialog window shows the tabs of a new review in the ad-hoc review process.

The Attributes tab contains the list of all process attributes which can be entered by the user. For more information on entering metadata see chapter [Entering entity metadata](#).

Create review [X]

DETAILS SECURITY

Title*: Review U9 August 2019

Description: Ad-hoc Review [owner=anelson]

Status: Opened

Owner: Alex Nelson

Keywords: adhoc owner

Members*: Jerry Roger Albert

Comments:

Reason: Review under Administration root class for selected directory entity only

CREATE CANCEL

Image 351: Display of the attributes of the review process in the Ad hoc mode

By creation of the review, two attributes are mandatory: Title and Members performing the entity review.

As in a regular review, the user with the appropriate rights defines the access permissions for users, groups and attributes in the Security tab.

After entering the metadata, the user saves the review to IMiS®/ARChive Server by selecting the action Create.

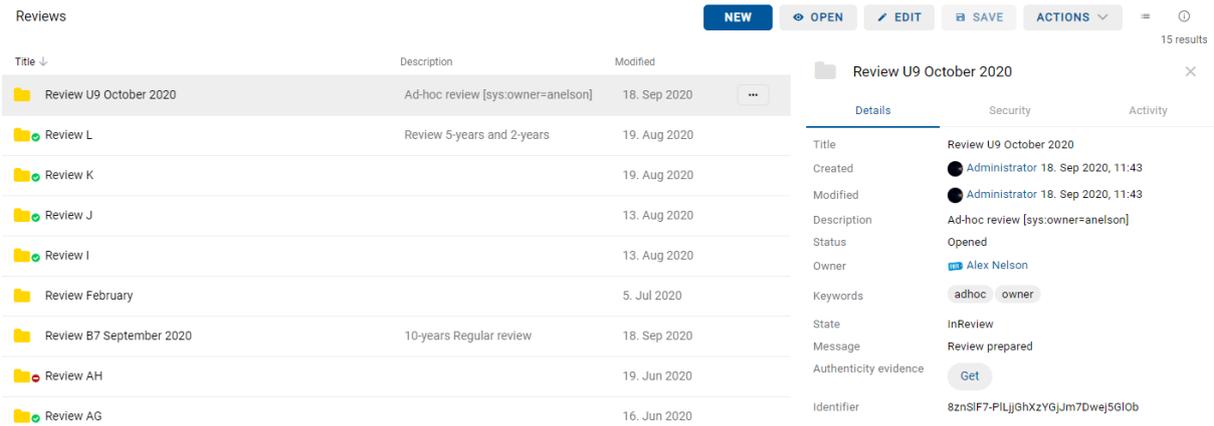


Image 352: Display of a saved ad-hoc review

This starts the transfer of all entered metadata to IMiS®/ARChive Server. After the review has been saved, it is queued for preparation.

Problems: The most common problem during saving is that the value of the mandatory attribute has not been entered.

Problems: The most common problem when creating a new review in the review process is that the user does not have the access right to create new reviews.

4.6.1.2 Canceling the review process

The review process can be discarded by team members at any time with the Discard command. They do that by selecting the Actions command in the command bar and the Discard action in the popup menu.

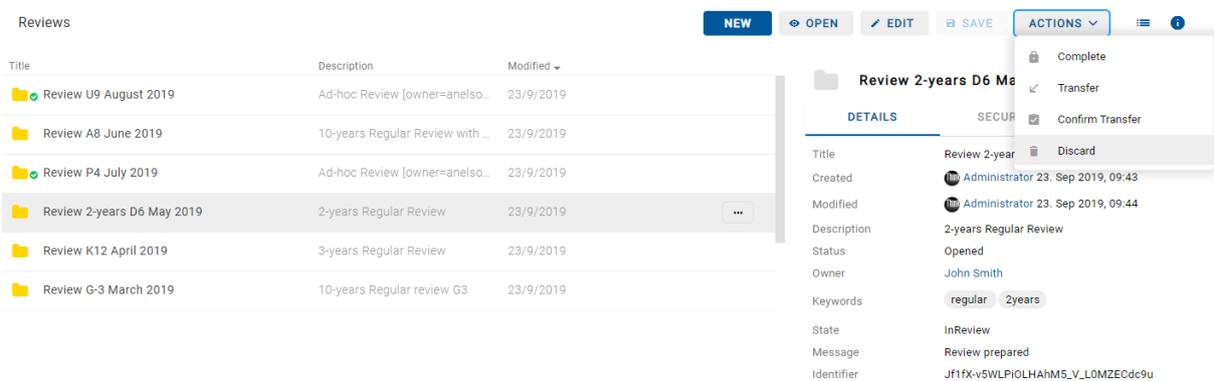


Image 353: Cancellation of the review process using the Discard command

After discarding the review process, the IMiS®/ARChive Server:

- Changes the value of the State attribute to Discarded.
- Changes the value of the Status attribute to Closed.
- It is entered into the Message attribute that the review process has been discarded by the user. In this case the entire review process must be recreated.

The screenshot shows the 'Reviews' section of the IMiS®/wClient interface. A table lists several reviews, including 'Review 2-years D6 May 2019'. The details panel for this review shows the following information:

Review 2-years D6 May 2019		
DETAILS	SECURITY	ACTIVITY
Title	Review 2-years D6 May 2019	
Created	Administrator 23. Sep 2019, 09:43	
Modified	Administrator 23. Sep 2019, 11:03	
Description	2-years Regular Review	
Status	Closed	
Owner	John Smith	
Keywords	regular 2years	
State	Discarded	
Message	Review discarded	
Identifier	Jf1fX-v5WLPiOLHAH5_V_L0MZECdc9u	

Image 354: A canceled decision-making phase

4.6.1.3 Entity preparation phase

The phase of preparing a list of entities begins when IMiS®/ARChive Server detects that entities are queued for review. The list only shows those entities which meet the condition of the selected retention periods. Other criteria are considered in the process.

For more information see chapter [Filtering process in the IMiS®/ARChive Server Manual](#).

While the review process is in the preparation phase, it cannot be modified.

During that time, its State attribute shows the Preparing value.

The screenshot shows the 'Reviews' section of the IMiS®/wClient interface. A table lists several reviews, including 'Review S2 September 2019'. The details panel for this review shows the following information:

Review S2 September 2019		
DETAILS	SECURITY	ACTIVITY
Title	Review S2 September 2019	
Created	Administrator 23. Sep 2019, 11:14	
Modified	Administrator 23. Sep 2019, 11:14	
Description	Regular review 5-years	
Status	Opened	
Owner	Alex Nelson	
Keywords	regular 5years	
State	Preparing	
Message		
Identifier	LVS3hFCUzILZu4GzrO_hgThxqg2rWS7	

Image 355: Display of the review in the preparation phase in the Preparing state

Once IMiS®/ARChive Server finishes preparing a list of entities, the value of the State attribute changes to InReview. The preparation of a review is completed and awaits the decision-making phase.

The entity placed on the list remains on that list even if its retention period is modified after the list was prepared.

During the preparation phase of the review process an error can occur for various reasons. In the event of an error, the review process is automatically cancelled. Such a process does not contain entities on its list and cannot be prepared again. Such a list also cannot be edited.

The following attributes change their values:

- The value of the Status attribute changes to Closed.
- The value of the State attribute changes to Failed.
- The cause of the cancellation is recorded into the Message attribute.

The screenshot displays the 'Reviews' section of the IMiS wClient interface. On the left, a table lists several reviews with columns for Title, Description, and Modified date. The review 'Review U9 August 2019' is highlighted. On the right, a detailed view for this review is shown, including fields for Title, Created, Modified, Description, Status, Owner, Keywords, State, Message, and Identifier. The 'Status' is 'Closed' and the 'State' is 'Failed'. The 'Message' field contains the error: 'Unable to locate metadata attribute named 'sys.owner''. The 'Identifier' is 'LAzL1365apxgWLWdbiescqg7C8ZEnpSJ'.

Title	Description	Modified
Review 2-years D6 May 2019	2-years Regular Review	23/9/2019
Review U9 August 2019	Ad-hoc Review [owner=anelso...]	23/9/2019
Review A8 June 2019	10-years Regular Review with ...	23/9/2019
Review P4 July 2019	Ad-hoc Review [owner=anelso...]	23/9/2019
Review K12 April 2019	3-years Regular Review	23/9/2019
Review G-3 March 2019	10-years Regular review G3	23/9/2019

Review U9 August 2019	
DETAILS	SECURITY
Title	Review U9 August 2019
Created	Administrator 23. Sep 2019, 10:57
Modified	Administrator 23. Sep 2019, 10:57
Description	Ad-hoc Review [owner=anelson]
Status	Closed
Owner	Alex Nelson
Keywords	adhoc owner
State	Failed
Message	Unable to locate metadata attribute named 'sys.owner'.
Identifier	LAzL1365apxgWLWdbiescqg7C8ZEnpSJ

Image 356: Display of an error which occurred during the preparation phase of the review process

4.6.2 Decision-making phase

By selecting the folder, the central view shows all of the reviews created. By selecting the appropriate review, review pages are shown along with the associated documents, which are the object of the review process.

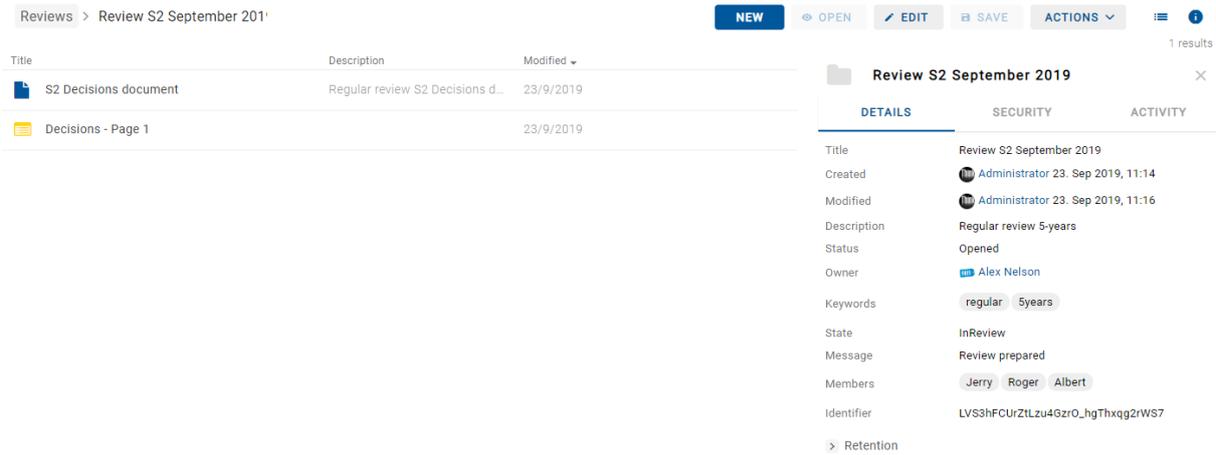


Image 357: Display of the review pages and documents

In the review the following data is visible for each page:

- Sequential title of the review page in the Title line.
- Short description of the review page in the Description line.
- Date of last page modification in the Modified line.

Each page contains the final number of entities. The default value is 2,000 entities.

By clicking on the selected page, the central view shows a list of selected entities.

A feature of this list is a display of the action which will be executed for each entity after the entire review process is completed.

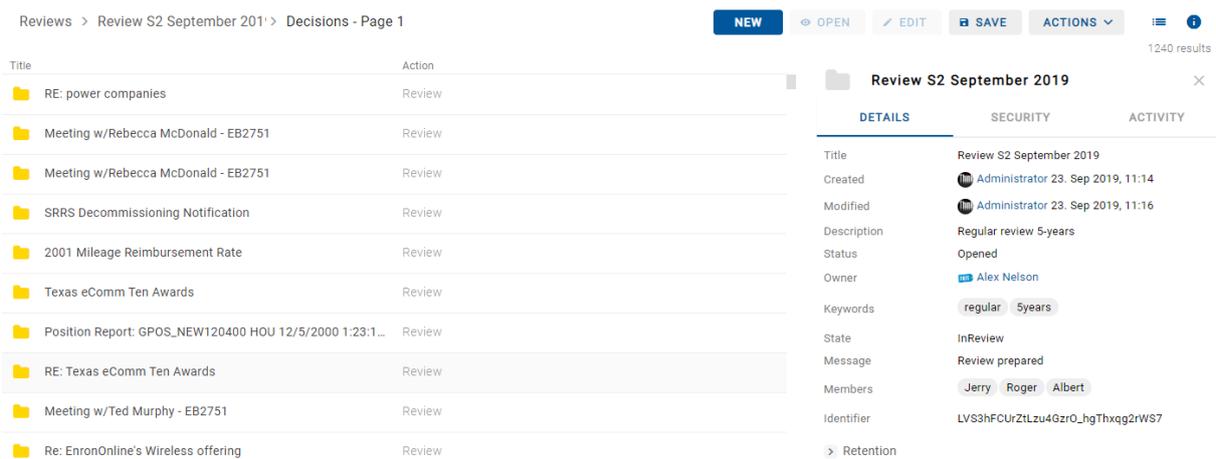


Image 358: A list of selected entities on a specific review page

By selecting the icon  to the right of the command bar, the user can define which columns of the selected attributes will be shown on the list of selected entities in the central view. The user can add or remove: Action, Reason and Comment.

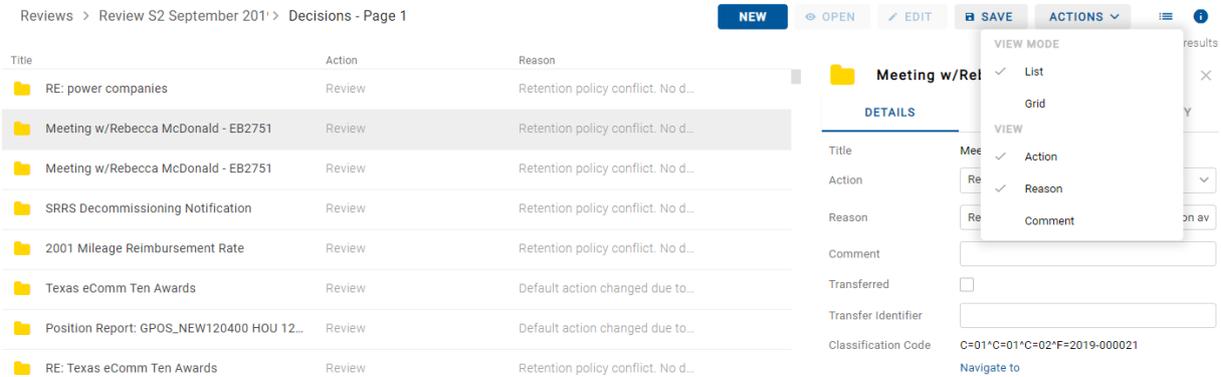


Image 359: Defining the columns of selected attributes in the popup menu

An entity which is included on the list of an individual review page has the following tabs:

- Details: a list of the metadata of the selected entity.
- Security: a review of the effective permissions of directory entities for the selected entity.
- Activity: audit log records for the selected entity.

By clicking on the Navigate to button in the right view, the selected entity is shown in the classification scheme.

The user can return to the review by selecting the back arrow in the browser.

Classification Code C=01*C=01*C=02*F=2019-000021
[Navigate to](#)

Image 360: Option of viewing an entity from the review

4.6.2.1 Modification of the attribute values in the review

If team members decide that the actions of certain entities must be modified in the review process, they can do so with the Edit command.

For more information on attributes see chapter Attributes in the review process.

In the right view, the user can modify the following attributes:

- Action
- Reason
- Comment
- Transferred
- Transfer identifier.

The screenshot shows a web interface for editing an entity. The title is 'Meeting w/Rebecca McDonald...'. The 'DETAILS' tab is selected, showing the following fields:

Attribute	Value
Title	Meeting w/Rebecca McDonald - EB2751
Action	Review (dropdown menu)
Reason	Retention policy conflict. No default reason av (text input)
Comment	(empty text input)
Transferred	<input type="checkbox"/>
Transfer Identifier	(empty text input)
Classification Code	C=01^C=01^C=02^F=2019-000021 Navigate to

Image 361: Adding and modifying attribute values in editing mode

Action

The default value of the »Action« attribute is set by the retention policy in the server's configuration. In the event that the entity undergoing the transfer process has several retention policies which contradict one another, the default value of this attribute is InReview. Such an entity requires a decision from team members on the type of action.

If team members decide that the actions of certain entities must be modified, they can perform one of the following actions:

- **Dispose:** the entity will be disposed of after the process is completed.
- **Permanent:** the entity will never again be selected in the review process. It has been marked for permanent retention.
- **Review:** an action which does not modify the entity's life span. The entity can be selected in the next transfer process.
- **Transfer:** after confirming the transfer and successfully completing the transfer process, the entity will be disposed of.

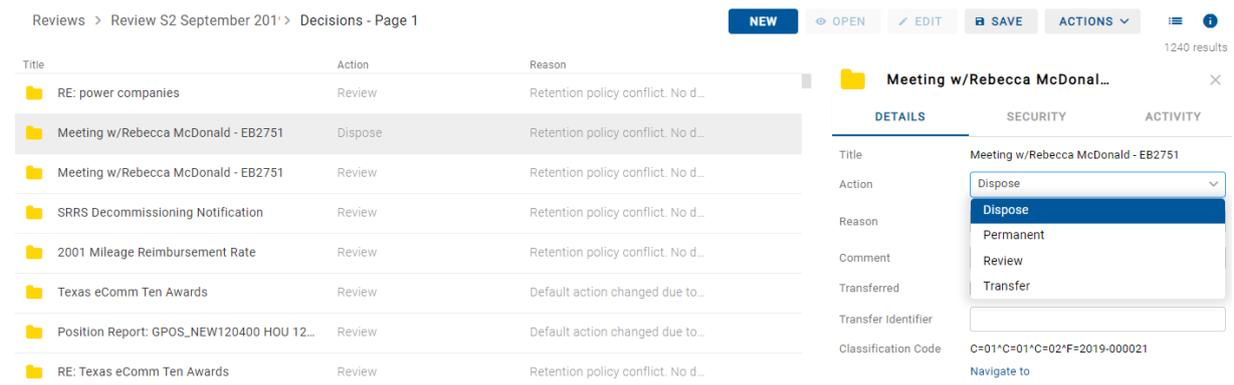


Image 362: Modifying the action of an entity in editing mode

Reason

Every time the »Action« attribute is modified it is recommended that team members also record the reason for the modification in the Reason attribute.

Comment

In the decision-making phase the team members can comment on their decisions.

Transferred

Team members must specify for each entity on the list whether it has been transferred. They do so by ticking the box.

Transfer identifier

If they wish, the team members can also enter a reference to the transferred entity by entering the value of the Transfer identifier attribute.

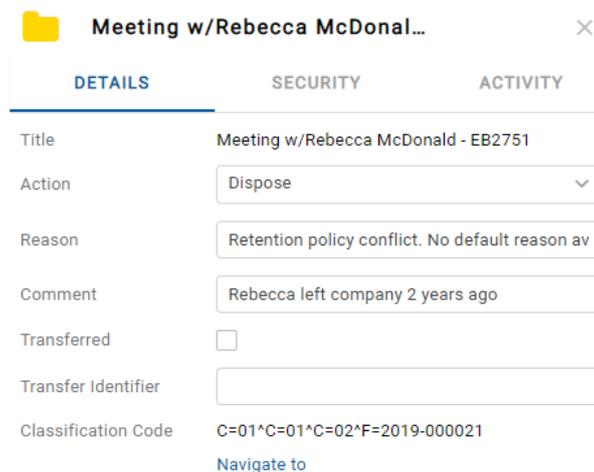


Image 363: Modifying attribute values in the review

After completion, the team members select the Finish command in the top command bar and then by clicking on the Save button save all confirmations to IMiS®/ARChive Server.

After completing the review of entities on the list, they can apply all the modifications by clicking on the Save button or cancel them by returning to the list of reviews.

Modifications of entities are not saved to IMiS®/ARChive Server until the user saves the review page. After saving, the list of reviews reappears. The team members can start working on the next review.

4.6.2.2 Canceling the decision-making process

The review process can be cancelled by team members selecting the Actions command and the Discard operation in the popup menu.

For more information on canceling the review process see chapter [Canceling the review process](#).

4.6.3 Implementation phase

The decision-making phase is followed by the implementation phase. Team members complete the review by selecting Actions command and the Complete operation in the popup menu.

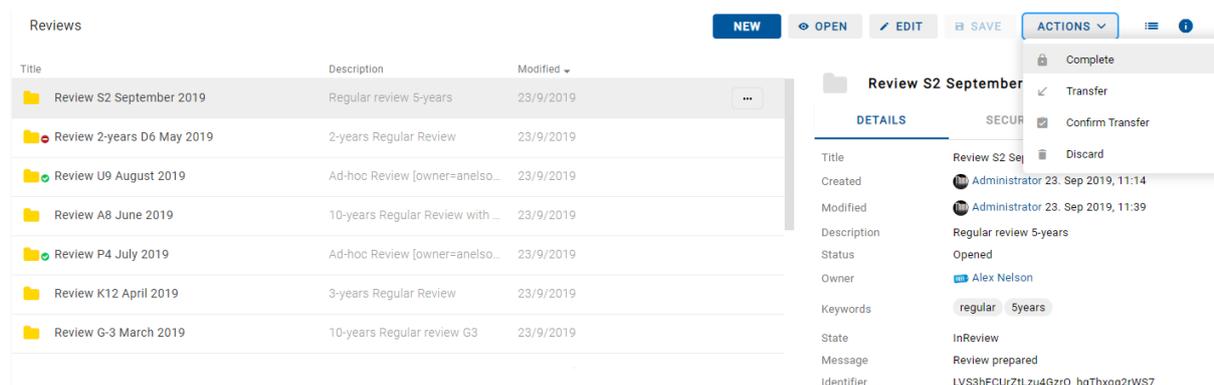


Image 364: Starting the process of completing the review

IMiS®/ARChive Server implements the review process of the disposition, transfer and permanent retention of entities.

Reviews > Review S2 September 201

Title	Description	Modified
S2 Decisions document	Regular review S2 Decisions d...	23/9/2019
Review execute report		23/9/2019
Decisions - Page 1		23/9/2019

Review execute report

DETAILS SECURITY ACTIVITY

Title: Review execute report

Description:

Created: Administrator 23. Sep 2019, 11:44

Modified: Administrator 23. Sep 2019, 11:44

Status:

Security class:

Significance:

Owner:

Keywords:

Categories:

> More

Image 365: During the process of completing the review

It automatically creates a review execute report on the implementation phase and files it among the review contents. For more information see chapter [Reviewing and classifying documents](#).

Reviews > Review S2 September 201

Title	Description	Modified
S2 Decisions document	Regular review S2 Decisions d...	23/9/2019
Review execute report		23/9/2019
Decisions - Page 1		23/9/2019

Review execute report

DETAILS SECURITY ACTIVITY

Title: Review execute report

Description:

Created: Administrator 23. Sep 2019, 11:44

Modified: Administrator 23. Sep 2019, 11:44

Status:

Security class:

Significance:

Owner:

Keywords:

Categories:

> More

Image 366: Review execute report

This action completes the review process, which cannot be modified or implemented. The value of the Status attribute changes to Closed and the value of the Stat« attribute to Completed.

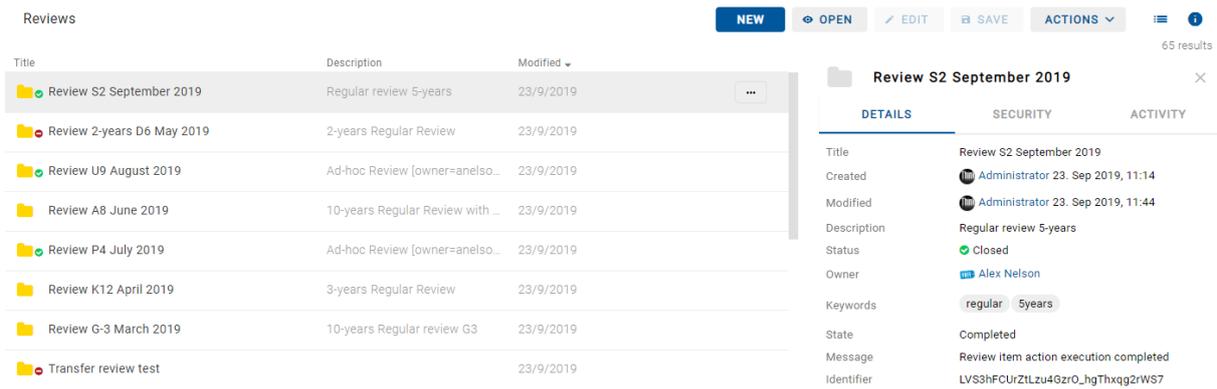


Image 367: Review completed

In the event of an error during the review process:

- An error description is recorded in the Message attribute.
- The value of the State attribute changes to Failed.
- The value of the Status attribute changes to Closed.

In this case the entire review process must be recreated.

4.6.4 Disposition

Each entity which was disposed of during the implementation phase of the review process is located in its raw form in the Disposed folder in the Trash folder, which is located in the Administration system folder.

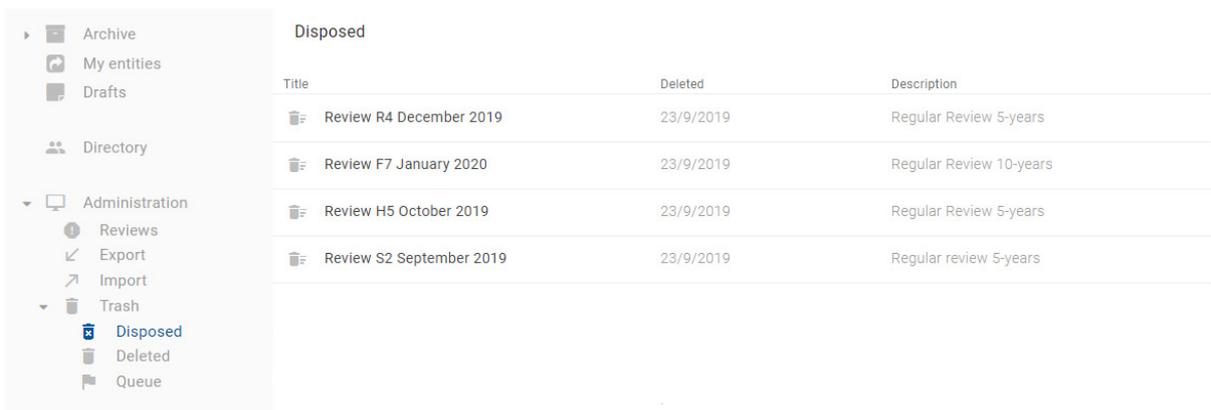
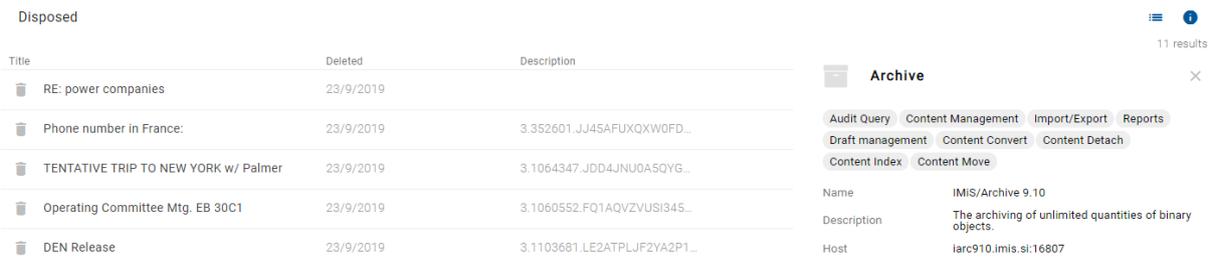


Image 368: A list of disposed entities in the review process

By selecting the Disposed folder, the central view shows all of the review processes during which at least one entity was disposed of. By clicking on an individual review page, a list of disposed entities appears, where the following entity information are shown only:

- Title: the title of the disposed entity.
- Classification code: the classification code of the disposed entity.
- Description: a description of the disposed entity.
- Modified: the date of last change.



Title	Deleted	Description
RE: power companies	23/9/2019	
Phone number in France:	23/9/2019	3.352601.JJ45AFUXQXW0FD...
TENTATIVE TRIP TO NEW YORK w/ Palmer	23/9/2019	3.1064347.JDD4.JNU0A5QYG...
Operating Committee Mtg. EB 30C1	23/9/2019	3.1060552.FQ1AQVZVUSI345...
DEN Release	23/9/2019	3.1103681.LE2ATPLJF2YA2P1...

Image 369: Display of the list of disposed entities on the review page

The Title, Classification code and Description of entity are the only attributes still preserved when an entity has been disposed of. All other entity metadata is erased and replaced with the following attributes:

- Reason: The reason for the disposition of the entity, which was entered by the user during the review process.
- Deleted: The date and time of the disposition of the entity.
- Identifier: Unique user identifier.

4.6.5 Transfer of entities

If the review process was also intended for the transfer of entities from IMiS®/ARChive Server, this action must be executed prior to completing the process.

The transfer action is executed with two separate processes:

- Exporting from IMiS®/ARChive Server to the file system.
- Confirmation of the transfer of entities to a third archive.

4.6.5.1 Exporting to a file system

The user executes the transfer of entities in the selected review selecting the Actions command and the Transfer operation in the popup menu.

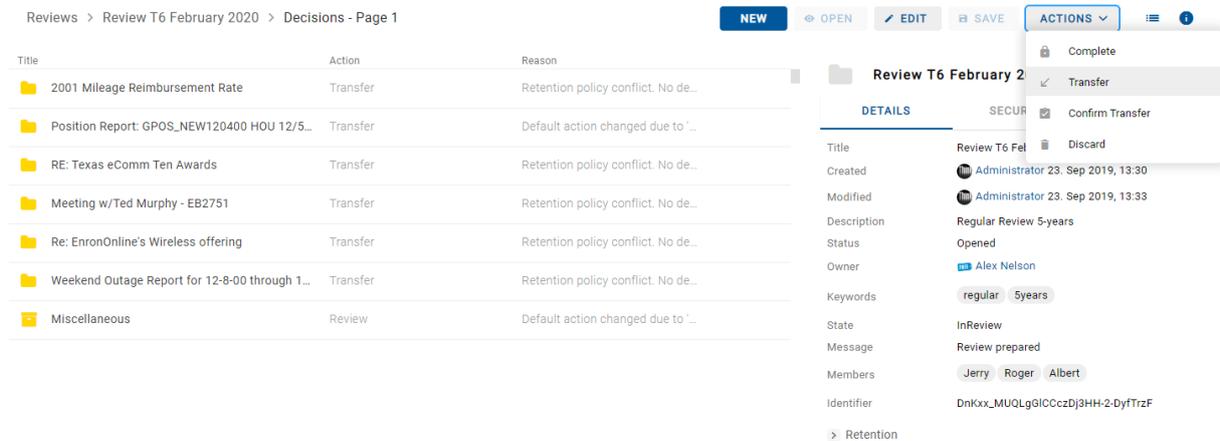


Image 370: Transfer of entities in the review process

After selecting the command, the user is shown a dialog box for setting the transfer parameters.

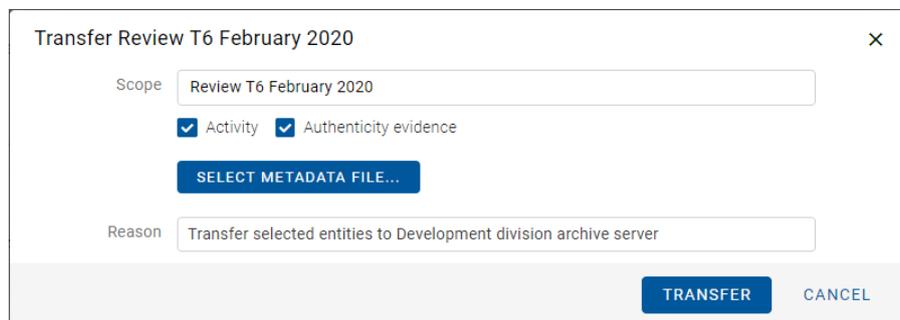


Image 371: Setting the transfer parameters

By selecting the Activity option, the audit log for an individual transferred entity can be included in the transfer.

If entity authenticity evidence has been created on the archive, the user can include it in the transfer by selecting the option Authenticity evidence.

Warning: If the user does not have the AuditLogQuery role and has nevertheless ticked the inclusion of an audit log in the transfer of entities in the transfer dialog box, the transfer is not executed.

In the Include metadata file section, the user invokes a dialog box for selecting an XML file with additional metadata to be included in the transfer.

For a description of the structure of the file with additional metadata see chapter [Format of the additional metadata export file](#).

By selecting the Transfer command, the transfer process begins. Team members can cancel the process by selecting the Cancel command.

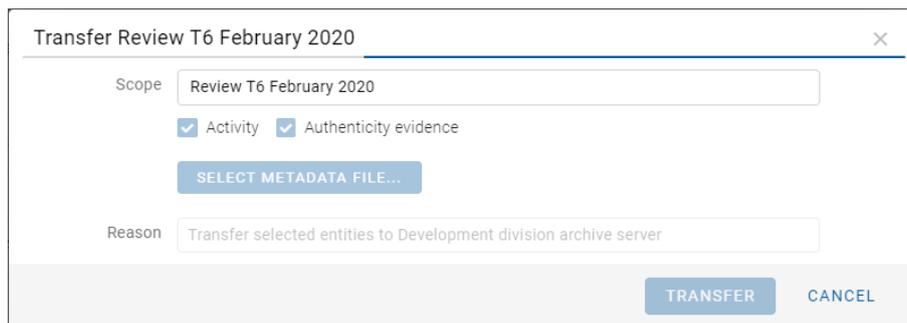


Image 372: Implementing the transfer process

The entities are exported in the XML format to the default directory Downloads. The user can access the transfer information from the notification bar by selecting the action Open in the popup menu.

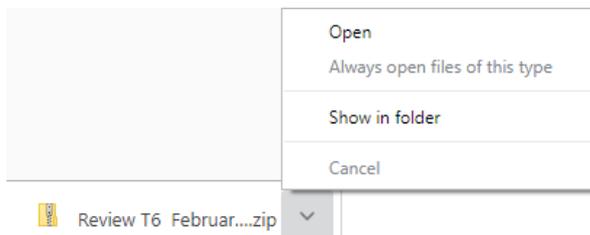


Image 373: Transfer notification

After confirming the selection Open for the compressed (zip) file, the right view of Windows Explorer shows the export reports and the additional file for the automatic transfer confirmation TransferConfirmation.csv. With it the user of a third archive system can quickly specify which entities will be confirmed as successfully transferred.

For more information see chapter [Format of confirmation file during transfer](#).

Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
ExportData	File folder					9/23/2019 1:43 PM
ExportReport	Text Document	2 KB	No	8 KB	88%	9/23/2019 1:44 PM
ExportReport	XML Document	7 KB	No	21 KB	69%	9/23/2019 1:44 PM
TransferConfirmation	Microsoft Excel Comma S...	1 KB	No	1 KB	67%	9/23/2019 1:44 PM

Image 374: Selecting the confirmation file

By selecting the confirmation file TransferConfirmation, information about the entities to be transferred is displayed.

	A	B	C
1	ClassificationCode	Transferred	ReferenceId
2	C=01^C=01^C=02^F=2019-000026	FALSE	
3	C=01^C=01^C=02^F=2019-000036	FALSE	
4	C=01^C=01^C=02^F=2019-000037	FALSE	
5	C=01^C=01^C=02^F=2019-000041	FALSE	
6	C=01^C=01^C=02^F=2019-000050	FALSE	
7	C=01^C=01^C=02^F=2019-000054	FALSE	
8			

Image 375: Displaying the confirmation file

In the next step the team members can modify the value, which specifies whether the entity has been successfully transferred to a third archive system (FALSE → TRUE), and the reference to the entity transferred to the third archive system (transfer identifier; optional).

A	B	C
ClassificationCode	Transferred	ReferenceId
C=01^C=01^C=02^F=2019-000026	TRUE	64632738
C=01^C=01^C=02^F=2019-000036	TRUE	64632738
C=01^C=01^C=02^F=2019-000037	TRUE	64632738
C=01^C=01^C=02^F=2019-000041	TRUE	64632738
C=01^C=01^C=02^F=2019-000050	TRUE	64632738
C=01^C=01^C=02^F=2019-000054	TRUE	64632738

Image 376: Confirmation of entities recorded in the confirmation file

Team members select a suitable location for saving the modified confirmation file to the file system with the command Save as.

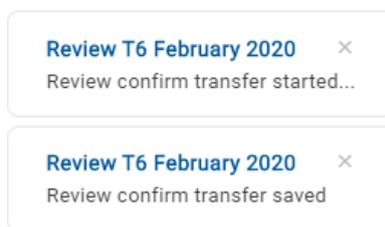


Image 377: Notification of saving the confirmation file

4.6.5.1.1 Export phase

At the start of export IMiS®/wClient creates a new review document.

For more information see chapter [Reviewing and classifying documents](#).

This document represents a report on export from the archive server. It uses the date and time of the start of export in ISO format as the document title.

During export the following two or three log files are created in the file system:

- ExportReport.xml: An XML file which contains:
 - Statistics of successfully and unsuccessfully exported entities.
 - List of unsuccessfully exported entities (including the classification code).
 - List of successfully exported entities (including the compressed value and full classification code).
- ExportReport.txt: contains a report for each successfully or unsuccessfully exported entity.
- ExportReport_ERROR.txt: contains a report for each unsuccessfully exported entity, including the returned error message.

In the event of an error when exporting an entity, the error is recorded in the ExportReport_ERROR.txt file. This file is created only in the event of an error.

After the first transfer phase – export, a new entity is attached to the review contents – a transfer report.

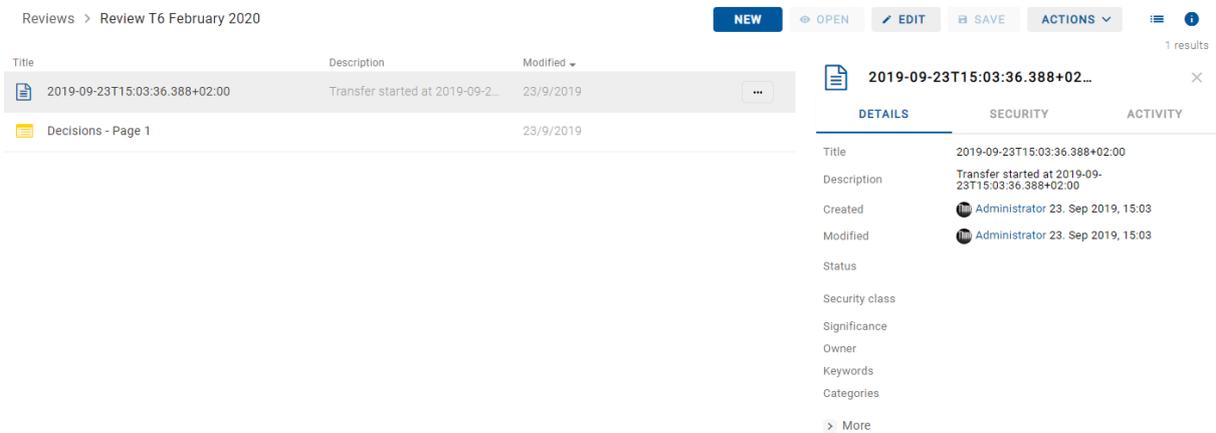


Image 378: A report on the transfer between review entities

The transfer report contains the following log files:

- XML report
- Report
- Error report, if an error occurred.

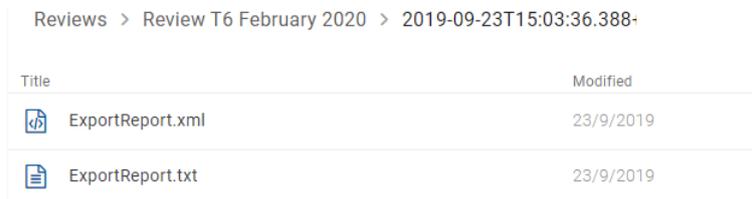


Image 379: Log files in the transfer report

By selecting the log file ExportReport.txt, the user is shown a report on successfully/unsuccessfully exported entities.

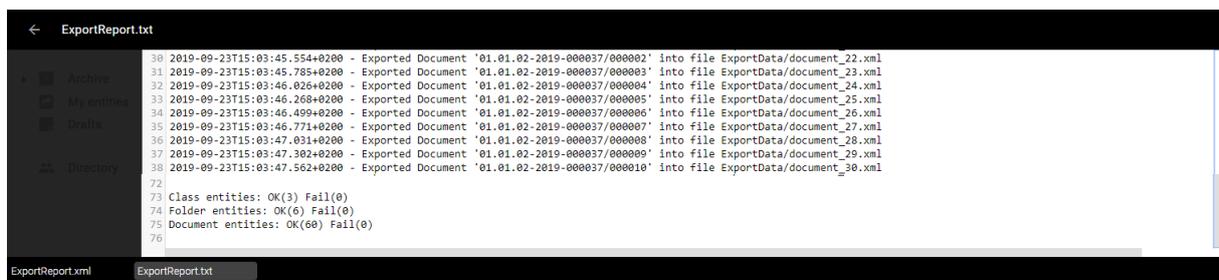


Image 380: An example of an ExportReport.txt report

4.6.5.1.2 Importing to a third archive system phase

All of the previously created files which contain exported entities must be transferred by the authorized user of the target archive to his location and an import of entities must be executed.

A description of the process of importing to a third archive is not covered by this manual.

It is recommended that a confirmation file is created when importing to a third archive, which will enable successful confirmation of the transfer on IMiS®/ARChive Server

For more information see chapter [Format of confirmation file during transfer](#).

4.6.5.2 Transfer confirmation

Prior to completing the transfer, the user must execute transfer confirmation for each entity undergoing the review process which has been marked for transfer.

Confirmation can be executed in one of the following ways:

- Manually for each transferred entity.
- Automatically with a confirmation file.

When the review process is completed, only those entities for which transfer has been confirmed are disposed of.

4.6.5.2.1 Manual transfer confirmation

Manual transfer confirmation is executed similarly to the modification of action on an individual entity in the review process.

For more information see chapter [Modification of the attribute values in the review](#).

The screenshot displays the IMiS interface for manual transfer confirmation. At the top, there is a navigation bar with 'Reviews > Review T6 February 2020 > Decisions - Page 1' and a toolbar with buttons for 'NEW', 'OPEN', 'EDIT', 'SAVE', and 'ACTIONS'. A '1235 results' indicator is visible on the right.

Title	Action	Reason
2001 Mileage Reimbursement Rate	Transfer	Retention policy conflict. No d...
Position Report: GPOS_NEW120400 HOU 12...	Transfer	Default action changed due to...
RE: Texas eComm Ten Awards	Transfer	Retention policy conflict. No d...
Meeting w/Ted Murphy - EB2751	Transfer	Retention policy conflict. No d...
Re: EnronOnline's Wireless offering	Transfer	Retention policy conflict. No d...
Weekend Outage Report for 12-8-00 through ...	Transfer	Retention policy conflict. No d...
Miscellaneous	Transfer	Transfer entities to another ar...

The 'Miscellaneous' entity is selected, and its details are shown in a form on the right. The form has tabs for 'DETAILS', 'SECURITY', and 'ACTIVITY'. The 'DETAILS' tab is active, showing the following fields:

- Title: Miscellaneous
- Action: Transfer (dropdown menu)
- Reason: Transfer entities to another archive
- Comment: Manual transfer
- Transferred:
- Transfer Identifier: 718283
- Classification Code: C=07
- Navigate to: [button]

Image 381: Manual transfer confirmation for an individual entity

Team members must specify for each entity on the list whether it has been transferred.

They do so by ticking the box of the Transferred attribute.

If they wish, they can also enter a reference to the transferred entity by entering the value of the “Transfer identifier” attribute.

After completion the team members save all confirmations on the IMiS®/ARChive Server by selecting the Save command.

4.6.5.2.2 Automatic transfer confirmation

If there is a confirmation file from a third archive, team members use it for automatic confirmation of entity transfer. In the Reviews folder they select the review for which they wish the transfer confirmation to be executed. In the command bar they select the Actions command and the action Confirm transfer in the popup menu.

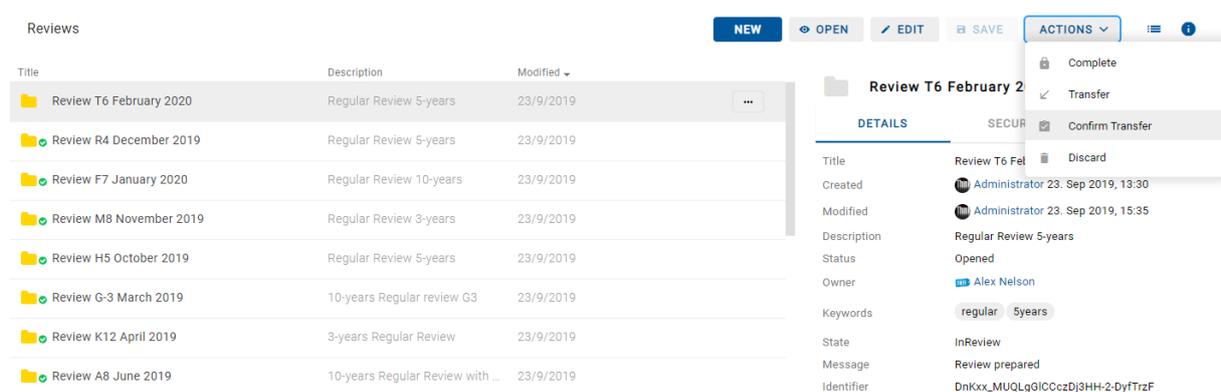


Image 382: Transfer confirmation using a confirmation file

After selecting the command, a dialog box appears for selecting the confirmation file.

They search for the desired file in the file system and confirm their selection with the Open command.



Image 383: Selecting the confirmation file

The confirmation of all entities recorded in the confirmation file begins to be executed.

For more information see chapter [Format of the confirmation file during transfer](#).

Team members confirm the selection of the confirmation file with Open or cancel it with the Cancel command.

After confirmation the changes are transferred to the relevant review. After refreshing the view of IMiS/wClient the changes are visible to the team members.

4.6.6 Reviewing and classifying documents

An integral part of the review process is the reviewing and classifying of documents, created by team members.

4.6.6.1 Classifying documents

During the review process the team members have the option of adding documents to the review. They select the relevant review from a list and then using the New command in the popup menu they select Document.

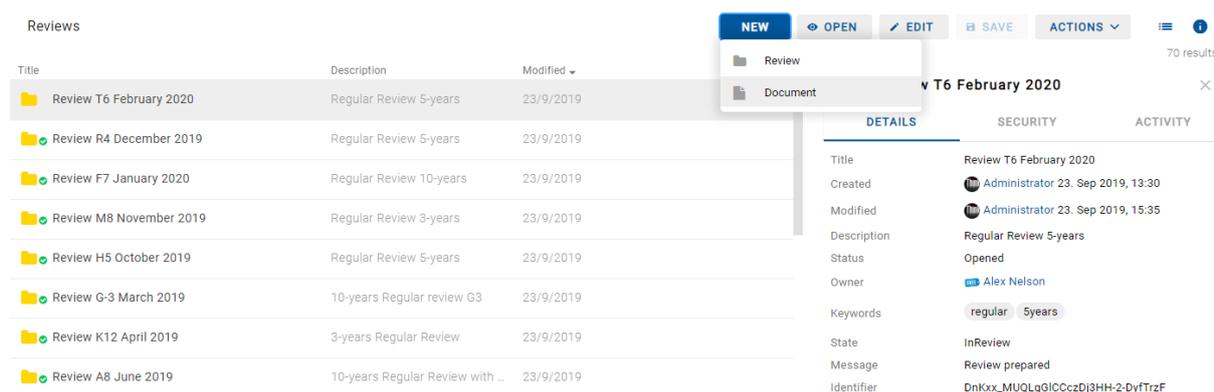


Image 384: Adding documents to the review

The dialog box shows the attributes of the new document.

In the Details tab they define the values of attributes and add contents.

After entering the metadata, they include the document in the review by selecting the action Create.

The screenshot shows a 'Create Document' dialog box with three tabs: DETAILS, PHYSICAL PROPERTIES, and SECURITY. The DETAILS tab is active. The fields are as follows:

- Parent: Review T6 February 2020
- Title*: Review T6 Document (Mandatory value for naming entity)
- Description: Document related to the T6 review
- Security class: INHERITED
- Significance: None
- Owner: Alex Nelson
- Keywords: regular, document
- Categories: review
- Content: A dashed box with a cloud icon and the text 'Drag and drop files or click'. Below it, a file 'Document_1.docx' (13.3 kB) is listed.
- External Identifiers: (Empty field)
- Reason: (Empty field)

Buttons for 'CREATE' and 'CANCEL' are at the bottom right.

Image 385: Adding document metadata

The screenshot shows the 'Create Document' dialog box during the upload phase. A blue progress bar is at the bottom, with the text 'Uploading Document_1.docx (100%)' centered below it. A circular loading icon is positioned above the progress bar.

Image 386: Adding a document to the review

Review T6 February 2020

DETAILS SECURITY ACTIVITY

Title Review T6 February 2020

Created Administrator 23. Sep 2019, 13:30

Modified Administrator 23. Sep 2019, 16:00

Description Regular Review 5-years

Status Opened

Owner Alex Nelson

Keywords regular 5years

State InReview

Message Review prepared

Members Jerry Roger Albert

Identifier DnKxx_MUQLgGICczDj3HH-2-DyfTrzF

> Retention

Review T6 Document

Entity created

Image 387: Notification about a document added to the review

4.6.6.2 Reviewing documents

The team members can review documents in the review by first selecting the relevant review from the list and opening it. In the center the review pages are shown with the corresponding documents and reports.

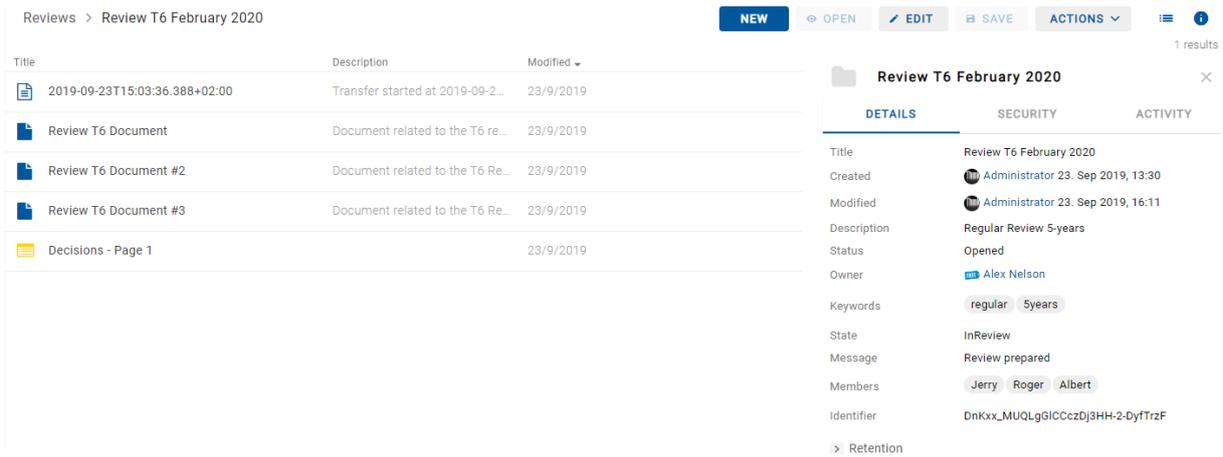


Image 388: Reviewing documents

Examples of classified contents:

- *Review execute report*
- *Transfer report*
- *Team minutes*
- *Attachment*
- *Custom document.*

By selecting the popup menu on the entity selected from the list, the team members have the option of performing various actions on the entity.

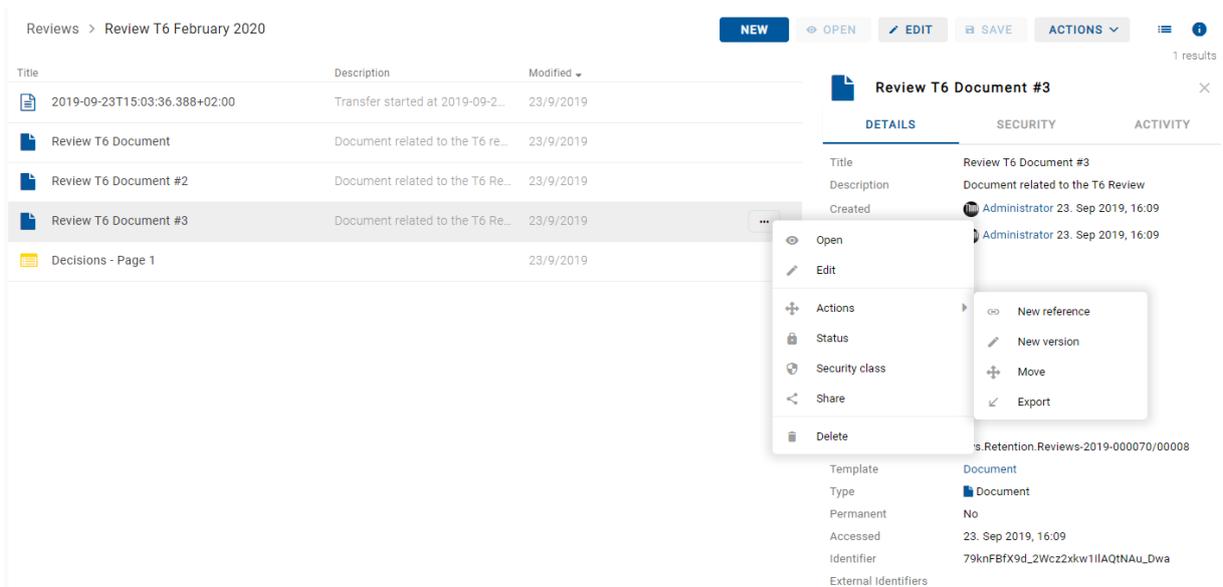


Image 389: Options of performing actions on entities

Warning: A user can export different entities to the same export folder several times without having to delete the export files prior to each export. When saving exported entities to the selected export folder, the previous export files are replaced.

4.7 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.
- **ImportExport:** this role enables the import and export of content. Users with the ImportExport role can perform entity »Import« and Export actions via the popup menu for the entire archive or for an individual entity.
- **Reports:** this role enables the display of system reports on export and import.
The Administration folder contains the subfolders Import and Export.
- **DraftManagement:** this role enables viewing and filing/discarding a document draft of other users (combined with the entity access permissions).

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.

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

- Brskalniki:
 - Chrome ≥ 77.0.3865.90
 - Firefox ≥ 69.0.1
 - Edge ≥ 44.18362.1.0
 - Safari ≥ 12.1.2
 - Internet Explorer 11 ≥ 11.0.10240.16384.
- 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®/Storage Connector Services REST 9.4.1910.104.
- Minimum free disk capacity for installing the IMiS®/wClient is 6GB.
- TCP/IP network access (IPv4 or IPv6).

5.2.2 Recommended requirements

- IMiS®/StorageConnector Services REST 9.5.1910.105.
- Disk capacity for installing the IMiS®/wClient is ≥ 6GB.
- 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®/Storage Connector Services REST must be entered into the assets/settings.json as the URL property.

Example of the settings.json:

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

url	String	Address of the IMiS®/Storage Connector Services REST.
requestTimeout	Integer	The timeout of an individual request to the service in <i>ms</i> (optional). The default value is 120000.
logLevel	String	Log records level (optional). Set of values: - DEBUG - INFO - WARNING - ERROR (default) - NONE.
entitiesPageSize	Integer	The number of entities loaded when displaying a single page (optional, default value: 50).

search.maxElements	Integer	Maximum number of search results displayed. The user can change this value in the profile settings, where they also have the option to reset it to this value (optional).
search.hideFields	String []	Collection of fields which are hidden in the search dialog by default.
scan.apiKey	String	The key to accessing IMiS®/wScan (optional).
scan.url	String	The address of IMiS®/wScan (optional).
collections.maxSize	Integer	The maximum number for loading the collection. The user can change this value in the profile settings, where they also have the option to reset it to this value.
collections.displaySearchButton	Boolean	Specifies whether the button for showing the search dialog is displayed when the collection does not load.
collections.displayLoadButton	Boolean	Specifies whether the button for loading the collection is displayed when the collection does not load.
preview.word	String	Defines the URL to the Office Online service for previewing Word contents (optional).
preview.excel	String	Defines the URL to the Office Online service for previewing Excel contents (optional).
preview.powerpoint	String	Defines the URL to the Office Online service for previewing PowerPoint contents (optional).
preview.onenote	String	Defines the URL to the Office Online service for previewing OneNote contents (optional).

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.

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.

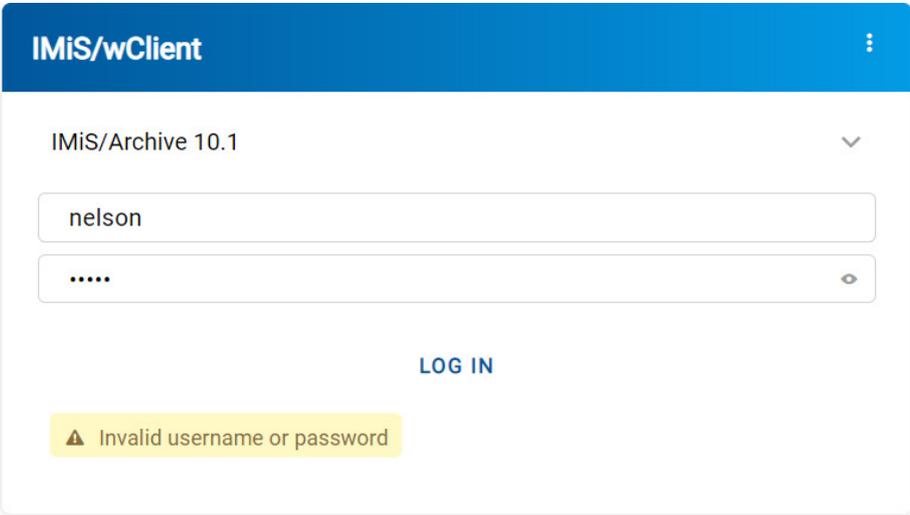
Solution: First, check the validity of the IP address and the network port. If that's not the cause, check if communication between the client and the server is open and reconfigure any firewalls as necessary.

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.



The screenshot shows the IMiS/wClient login window. At the top, there is a blue header with the text "IMiS/wClient" and a three-dot menu icon. Below the header, the text "IMiS/Archive 10.1" is displayed with a dropdown arrow. There are two input fields: the first contains the username "nelson", and the second contains a masked password "....." with an eye icon to toggle visibility. A blue "LOG IN" button is centered below the fields. At the bottom, a yellow warning box contains a triangle icon and the text "Invalid username or password".

IMiS/wClient (v1.5.2010.5)



Image 390: 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.

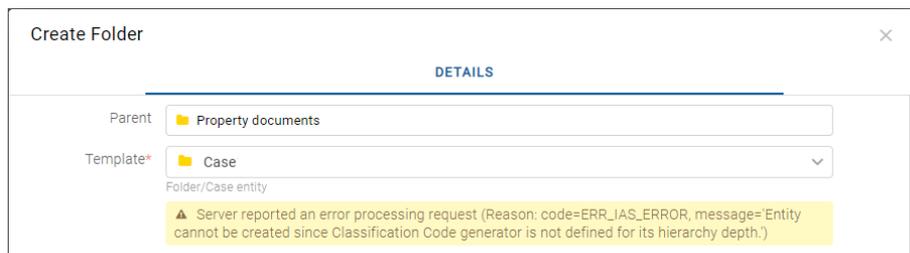


Image 391: An example of an error when saving a new folder

[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 392: An example of an error when opening an entity in editing mode

Content scanning icon does not appear

Likely cause: Wrong key for accessing the IMiS®/Capture Service.

Solution: In the IMiS®/Capture Service settings check the suitability of the key in the “Security” tab. The service key value in the IMiS®/Capture Service settings must match the API key value in the user profile settings (“Profile / Settings”) of the IMiS®/wClient.

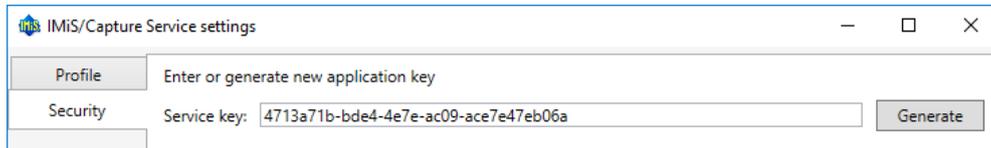


Image 393: Example of defining the service key