IMiS®/Client Manual

Version 9.9.1810

IMAGING SYSTEMS

Imaging Systems Inc.
Brnciceva 41 G
Ljubljana
Slovenia

TABLE OF CONTENTS

1 PREFACE 16
1.1 About the manual 16
1.2 Target audience 16
1.3 Conventions 16
1.4 Terms and abbreviations 17
2 INTRODUCTION 21
2.1 Features 21
2.2 Tier placement 22
2.3 Versioning and numbering 23
2.4 Functionalities 24
3 TECHNICAL DOCUMENTATION 25
3.1 Client architecture 25
3.2 Format of import / export files 26
3.2.1 File structure 28
3.2.2 List of XML tags and their meaning 28
3.2.3 Format of the additional metadata export file 45
3.3 Format of the confirmation file during transfer 46
4 USER MANUAL 47
4.1 Interface description 47
4.1.1 Classification scheme 49
4.1.2 List of entities 51
4.1.3 Entity information 52
4.1.4 The command bar 71
4.1.5 Menu functions 75
4.2 Actions 80
4.2.1 Login and logout 81
4.2.2 Document capture 85
4.2.3 Content management 103
4.2.4 Bulk document capture 106
4.2.5 Conversion 106
4.2.6 Access 109
4.2.7 Search functions 112
4.2.8 Editing entity data 120
4.2.9 Versioning 124
4.2.10 Archiving email messages 134
4.2.11 Managing physical content metadata 138
4.2.12 Print 139
4.2.13 Import 150
4.2.14 Export 155
4.2.15 Move 160

2018 © Imaging Systems, Inc., All rights reserved.

4.2.16 Delete 161
4.2.17 Changing the status of an entity 167
4.2.18 Changing the security class 168
4.2.19 Acquiring authenticity evidence 169
4.2.20 Viewing the audit log 173
4.3 System attributes 175
4.3.1 General system attributes 176
4.3.2 Security class change attributes 178
4.3.3 Moved entity attributes 178
4.3.4 Deleted entity attributes 178
4.3.5 Transferred entity attributes 179
4.3.6 Email attributes 179
4.3.7 Physical content attributes 179
4.3.8 Review process attributes 180
4.3.9 Entity attributes in the decision-making process 181
4.4 Authenticity 182
4.4.1 Digital certificate 182
4.4.2 Electronic signature 184
4.5 Review process 188
4.5.1 Preparation phase 189
4.5.2 Decision-making phase 195
4.5.3 Implementation phase 202
4.5.4 Transfer of entities from the server 203
4.5.5 Reviewing and classifying documents 210
4.5.6 Viewing selected retention policies 212
4.6 Reports 213
4.6.1 Import 214
4.6.2 Export 217
4.6.3 Deletion 220
4.6.4 Disposition 222
4.6.5 Audit log 223
4.6.6 Statistics 225
4.7 Roles 233
5 SYSTEM REQUIREMENTS 234
5.1 Hardware 234
5.1.1 Minimum requirements 234
5.1.2 Recommended hardware 234
5.1.3 Hardware supervision 234
5.2 Software 234
5.2.1 Operating systems 234
5.2.2 Minimum requirements 235

2018 © Imaging Systems, Inc., All rights reserved.

6 INSTALLATION 235
6.1 Installation procedure 235
7 UNINSTALLATION 244
7.1 Uninstallation procedure 244
8 PRODUCT MANAGEMENT 250
8.1 Startup and closing 250
8.2 Event log 251
8.3 Configuring 253
8.3.1 Adding an IMiS®/ARChive Server 253
8.3.2 Setting an IMiS®/ARChive Server 255
8.3.3 Removing an IMiS®/ARChive Server 258
8.4 Server configuration 259
8.4.1 »Access control« folder 263
8.4.2 »Archive« folder 269
8.4.3 »Attributes« folder 270
8.4.4 »Audit log« folder 274
8.4.5 »Authentication« folder 278
8.4.6 »Codelists« folder 284
8.4.7 »Content« folder 287
8.4.8 »Counters« folder 303
8.4.9 »Directory« folder 306
8.4.10 »Legacy archival« folder 313
8.4.11 »LTANS« folder 318
8.4.12 »Retention« folder 323
8.4.13 »Security« folder 328
8.4.14 »Storage« folder 337
8.4.15 »Templates« folder 344
9 TROUBLESHOOTING 349
9.1 How to avoid problems 349
9.2 Frequent errors 349
9.3 Less frequent errors 353

2018 © Imaging Systems, Inc., All rights reserved.

TABLE OF IMAGES

Table of images appearing in the manual

Image 1: Example virtual two-tier document system 23
Image 2: Client architecture 25
Image 3: XPath notation text example 27
Image 4: Example XSD scheme 45
Image 5: Example additional metadata export file 46
Image 6: Example of a confirmation file after transfer 46
Image 7: User interface of the IMiS®/Client 47
Image 8: The search results counter 49
Image 9: Display of the Archives folder 49
Image 10: Display of an archive's root classes and the Administration system folder 50
Image 11: Expanded tree view of the classification scheme 50
Image 12: List of entities contained by the selected entity 51
Image 13: Popup menu over a line of displayed attributes 52
Image 14: View of the »Attributes« tab 54
Image 15: Display of the unsaved changes alert prompt 54
Image 16: View of the »Content« tab 55
Image 17: View of the »Physical Content« tab 56
Image 18: View of the »Security« tab in preview mode 57
Image 19: User selection window of the »Security« tab in preview mode 58
Image 20: Reading mode display of the »Security« tab 59
Image 21: Editing access permissions on an entity for a user 60
Image 22: Editing access permissions on an entity for a directory entity type attribute 61
Image 23: Popup menu for selecting access permissions to a selected metadata 61
Image 24: Adding a directory entity for setting access permissions 62
Image 25: List of directory entity permissions on the selected metadata 62
Image 26: Display of retention periods in the »Retention« tab in reading mode 63
Image 27: Display of retention periods in the »Retention« tab in editing mode 63
Image 28: Display of disposition holds in the »Retention« tab in reading mode 65
Image 29: The »Reference« tab 66
Image 30: Selecting the »New reference« command 66
Image 31: The dialog box for entering the attributes of the new reference 66
Image 32: Adding a new reference under an existing reference 67
Image 33: A reference added under an existing reference 67
Image 34: Adding a new reference to an existing reference 67
Image 35: A reference added to an existing reference 68
Image 36: Removing a reference 68
Image 37: View of the »Activity Log« tab prior to retrieving an audit trail 69
Image 38: View of the »Activity Log« tab with a displayed audit trail 69
Image 39: View of the »System Properties« tab 71

2018 © Imaging Systems, Inc., All rights reserved.

Image 40: Command bar above a selected archive when logged in....71
Image 41: Command bar above a selected entity....72
Image 42: Command bar above selected entity in the “Search results” folder....73
Image 43: Command bar above selected entity in the »Queue« system folder....73
Image 44: Command bar above selected entity in the system folders »Export« and »Import«....73
Image 45: Command bar above selected entity in the system folder »Trash«....73
Image 46: An example of an entity with a defined value of the attribute »Categories«....74
Image 47: A categorized »Categories« view....74
Image 48: An example of an entity with a defined value of the attribute »Keywords«....74
Image 49: A categorized »Keywords« view....75
Image 50: Popup menu over the »Archives« folder....75
Image 51: Popup menu over the selected archive prior to login....76
Image 52: Popup menu over the selected archive when choosing the »Reports« command....76
Image 53: Popup menu over the selected archive when choosing »Print«....77
Image 54: Popup menu over the selected archive when choosing »Actions«....77
Image 55: Popup menu over the selected entity when choosing »Reports«....78
Image 56: Popup menu over the selected entity (class, folder, document) when choosing »Print«....79
Image 57: Popup menu over the selected entity when choosing »Actions«....79
Image 58: Popup menu over a line of displayed attributes....80
Image 59: Login into the selected archive via the popup menu....81
Image 60: Archive login dialog box....82
Image 61: A dialog box to confirm a remote certificate....82
Image 62: Warning about a previous installation of the remote certificate....83
Image 63: A dialog box for selecting a local certificate....84
Image 64: Logging out of the selected archive via the popup menu....84
Image 65: Creating a new entity using the command bar....86
Image 66: Entry of required metadata....87
Image 67: Entry of text metadata....88
Image 68: Entry of date and time metadata....88
Image 69: Entry of metadata with predefined values....88
Image 70: Entry of multiple value metadata....89
Image 71: Display of the type of child classification code generation....90
Image 72: Display of the entry of a child entity's classification code....90
Image 73: Display of manually entered classification code of the child folder....91
Image 74: Display of a folder with a manually entered classification code....91
Image 75: Display of setting an entity's security class without inherited value....92
Image 76: Adding content using the file system....93
Image 77: Display of added content....94
Image 78: Editing the new content's description by clicking on the description or pressing F2....94

2018 © Imaging Systems, Inc., All rights reserved.

Image 79: Editing a description of selected content via the popup menu 95
Image 80: Displaying the content's data selection 95
Image 81: Displaying content data 96
Image 82: Selecting the command »Open« to open content 96
Image 83: Opening audio content (wav, ogg, mpeg) 97
Image 84: Opening video content (mp4, webm, ogg) 97
Image 85: Enables the editing of retention periods and disposition holds 98
Image 86: Adding an explicit retention period 98
Image 87: Editing the settings of the explicit retention period 99
Image 88: A saved explicit retention period 99
Image 89: Saving a new or modified entity 99
Image 90: Example classification code 100
Image 91: Example creator of entity 100
Image 92: Example date and time an entity was opened 100
Image 93: Example date and time an entity was closed 101
Image 94: Example date and time an entity was created 101
Image 95: Example date and time of last changes to the entity 101
Image 96: Example date and time of last access to the entity 101
Image 97: Example entity identifier 101
Image 98: Example external identifiers of an entity 101
Image 99: Example save log of an entity 102
Image 100: Example date of content insertion 102
Image 101: Example date of content modification 102
Image 102: Displaying a dialog box where classification code of the target entity is entered 103
Image 103: Displaying the default content container 103
Image 104: Displaying the dialog box for entering the classification code of the target document 104
Image 105: Displaying the content copied to the target document 104
Image 106: Displaying the Detach content command 105
Image 107: Displaying detached content 105
Image 108: Displaying the tagging content for indexing command 105
Image 109: Displaying the tagging content for conversion command 106
Image 110: Opening content of document in the conversion procedure 107
Image 111: Selecting the virtual printer »IMiS Convert To PDF-A« 108
Image 112: Conversion settings via the dialog box 108
Image 113: Example of a content tree 109
Image 114: Display of root classes when logging into the selected archive 110
Image 115: Displaying the publicly accessible entity data in tabs 111
Image 116: Opening the selected entity 112
Image 117: Search of the selected entity via the popup menu 113
Image 118: Setting search parameters via the dialog box 114

2018 © Imaging Systems, Inc., All rights reserved.

Image 119: Display of search results in the right view of Windows Explorer 116
Image 120: Sample search string for searching by title of the content 117
Image 121: Results of searching by title of the content 118
Image 122: Editing an entity via the command bar 120
Image 123: Entering or editing entity metadata 121
Image 124: Adding content to an entity via the file system 121
Image 125: Opening the entity in editing mode. 122
Image 126: Opening content in the default application. 122
Image 127: Display of the modified content after modification in the default application 123
Image 128: Saving changes to the entity 123
Image 129: When saving the modified content, the »Modified« date is also changed 123
Image 130: Selecting the action »Check out« in the popup menu 124
Image 131: Displaying the document version details 125
Image 132: Checking out a document version 126
Image 133: Selecting the document version and entering a comment 127
Image 134: Details of the saved document version 127
Image 135: Selecting the command »Versions« in the bottom command bar 128
Image 136: Displaying document versions in the set »Versions« 129
Image 137: Selecting the command »Delete« on the selected document version 129
Image 138: A document version in Edit mode 130
Image 139: Saving a document draft for a later check-in of the document version 130
Image 140: A list of document drafts 131
Image 141: Document draft details in the folder »Drafts« 132
Image 142: Discarding a document draft with the command »Discard« 132
Image 143: Viewing a draft before check-in 133
Image 144: Selecting a version before checking in a document draft 133
Image 145: Displaying the document versions after checking in the draft 134
Image 146: Transferring email messages from the email client to the selected class 135
Image 147: Display of transferred email messages 136
Image 148: Automatically created email attachments 137
Image 149: Example metadata extracted from an email message 138
Image 150: Example setting custom attribute 138
Image 151: Display of entering physical content metadata 139
Image 152: Access to the content of a selected document 140
Image 153: Access to the contents of the desired document 140
Image 154: Selecting print options via the popup menu 141
Image 155: Selection of metadata print options for the chosen document 141
Image 156: Selection of metadata print options for the chosen folder 141
Image 157: Selection of metadata print options for the chosen class 142
Image 158: Print settings dialog box 142
Image 159: Example document print preview 143

2018 © Imaging Systems, Inc., All rights reserved.

Image 160: Selection of classification scheme printing options 146
Image 161: Example classification scheme print 146
Image 162: Selection of classification scheme printing options 147
Image 163: Example classification scheme with folders print from the preview 147
Image 164: Selecting the option of printing reviews 148
Image 165: Example of printing selected entities classified by retention policies 149
Image 166: Example of printing selected entities for the selected query 150
Image 167: Importing content via the popup menu 151
Image 168: Selection of the XML import list 151
Image 169: Selecting a digital certificate when importing 152
Image 170: Display of the import complete message with success rate statistics 152
Image 171: A display of a detailed report of the import 153
Image 172: Display of the import report in the »Import« system folder 154
Image 173: Exporting records via the popup menu 155
Image 174: Export settings in the dialog box 156
Image 175: Selecting a digital certificate when exporting 157
Image 176: Display of the export complete message with success rate statistics 157
Image 177: A display of a detailed report of the import 158
Image 178: Display of the export report in the »Export« system folder 159
Image 179: Popup menu where the »Move« command is found 160
Image 180: Move entity dialog box 160
Image 181: Deleting an entity via the command bar 162
Image 182: Entity deletion dialog box 163
Image 183: Display of a deleted entity's metadata 163
Image 184: Marking an entity for later deletion 164
Image 185: List of entities marked for deletion in the »Queue« folder 165
Image 186: Removing an entity from the delete queue list 166
Image 187: Popup menu for choosing the »Status« command 167
Image 188: Status change dialog box 167
Image 189: Popup menu for choosing the »Security class« command 168
Image 190: Dialog box for changing the security class 169
Image 191: Popup menu for choosing the »Authenticity evidence« command 169
Image 192: Dialog box for selecting the export folder of authenticity evidence files 170
Image 193: Example archive information package 171
Image 194: Example evidence record 172
Image 195: Popup menu for selecting the »Audit log« command 173
Image 196: Configuring the audit trail query 174
Image 197: Qualified digital certificate information 183
Image 198: Example of a pop-up window containing the result of the document's electronic signature verification. 186
Image 199: Example of a report for a valid electronic signature and valid digital certificate 187

2018 © Imaging Systems, Inc., All rights reserved.

Image 200: Example of a valid electronic signature and an expired digital certificate.....187
Image 201: Example of a valid electronic signature for which the certification authority could not be verified.....187
Image 202: Example of an invalid electronic signature due to a modification of the document after signing. 188
Image 203: Schematic of the review process 188
Image 204: Display of reviews created in the review processes.....189
Image 205: Creating a new regular review in the preparation phase.....190
Image 206: Dialog box for selecting retention periods 190
Image 207: Display of review attributes in the review process 191
Image 208: Example of creating a list of entities which were closed on a specific date 191
Image 209: Display of review attributes in the review process 192
Image 210: Saving a new or modified review in the review process.....193
Image 211: Display of a review in the preparation phase.....194
Image 212: Display of an error which occurred during the preparation phase of the review process.....195
Image 213: Display of the review page 196
Image 214: List of entities in modification mode.....198
Image 215: Display of the »Finish« and »Cancel« button 199
Image 216: Display of the page which has been modified.....200
Image 217: Display of the »Save« command in the review process.....200
Image 218: Cancellation of the review process using the »Discard« command 201
Image 219: Starting the implementation phase by selecting the »Complete« command 202
Image 220: Transfer of entities in the review process.....203
Image 221: Setting the transfer parameters 203
Image 222: Selecting a digital certificate during export 204
Image 223: Display of the export complete message with success rate statistics 205
Image 224: Manual transfer confirmation for an individual entity 208
Image 225: Transfer confirmation using a confirmation file.....209
Image 226: Selecting the confirmation file.....209
Image 227: Changing the context during the review of classified contents.....210
Image 228: Example of displaying inserted documents in »Documents« context.....211
Image 229: Changing the context in retention policies 212
Image 230: Display of the retention policy.....213
Image 231: Display of the »Import« folder in the »Administration« system folder 214
Image 232: List of content contained by an import document.....215
Image 233: Example signed »XML Report« file with a record of import actions.....216
Image 234: Example »Error report« log with a list of import errors.....216
Image 235: Example »Report« log with a list of errors and the overall import success rate 217
Image 236: Display of the »Export« folder in the »Administration« system folder 218
Image 237: List of content contained by an export document.....219

2018 © Imaging Systems, Inc., All rights reserved.

Image 238: Example »XML Report« file with a record of export actions 219
Image 239: Example »Error report« log with a list of export errors 220
Image 240: Example »Report« log with a list of export actions and the overall export success rate 220
Image 241: Display of the »Trash« folder in the »Administration« system folder 221
Image 242: Example deleted entities report 222
Image 243: Display of the list of disposed entities 223
Image 244: Selecting an audit log report via the popup menu 224
Image 245: Example audit log report 225
Image 246: Selecting a folder report via the popup menu 225
Image 247: Example folder report 226
Image 248: Selecting a document report via the popup menu 227
Image 249: Example document report 227
Image 250: Selecting a content report via the popup menu 228
Image 251: Example content report 229
Image 252: Selecting the retention report via the pop-up menu 229
Image 253: Example of a retention report 230
Image 254: Creating an access report on the selected user 230
Image 255: Selecting a user or all users 231
Image 256: Example access report on the selected user 232
Image 257: Preparing to install 235
Image 258: Beginning the IMiS®/Client installation procedure 236
Image 259: Cancelling the IMiS®/Client installation procedure 236
Image 260: Reviewing and accepting the license agreement 237
Image 261: Customer information dialog box 237
Image 262: Choice between complete and custom installation 238
Image 263: Selecting the elements and location of IMiS®/Client installation 238
Image 264: Description of the installation element icons 239
Image 265: Selecting the destination folder 239
Image 266: Available disk space 240
Image 267: Removing the printer driver during custom install 240
Image 268: Selecting the location of the Archives folder 241
Image 269: Confirming settings to begin installation 241
Image 270: Security warning notification 242
Image 271: Installation progress bar 242
Image 272: Installation complete message 243
Image 273: Virtual printer installation 243
Image 274: Uninstalling the IMiS®/Client 244
Image 275: Selecting the »Uninstall« command 244
Image 276: Uninstallation progress bar 245
Image 277: A confirmation of the closure of applications due to IMiS®/Client removal 245

2018 © Imaging Systems, Inc., All rights reserved.

Image 278: Displaying security warning 246
Image 279: IMiS®/Client has been removed from the computer 246
Image 280: Selecting the »Modify« command 247
Image 281: Opening the IMiS®/Client program maintenance..... 247
Image 282:Selecting a program maintenance action for the IMiS®/Client..... 248
Image 283: Confirming IMiS®/Client uninstallation 248
Image 284: Selecting »Uninstall« command 249
Image 285: Security warning prompt..... 249
Image 286: Uninstallation complete message..... 250
Image 287: Example log file 252
Image 288: Example error record in the log file 253
Image 289: Adding an archive via the popup menu..... 254
Image 290: Add archive dialog box 254
Image 291: Display of newly added archives 255
Image 292: Setting the archive via the pop-up menu 255
Image 293: Archive settings 256
Image 294: Removing an archive via the popup menu..... 258
Image 295: Remove archive dialog box 258
Image 296: Choosing the »Configure« command before the user has logged into the archive 259
Image 297: Choosing the »Configure« command after the user has logged into the archive... 259
Image 298: Dialog box for entering username and password 260
Image 299: List of available folders displayed after logging into the archive configuration 260
Image 300: Example of the command bar in the configuration folder with the »Filter« command 263
Image 301: List of users and user groups in the »Access control« configuration folder..... 264
Image 302: Choosing the context in the »Access control« configuration folder 264
Image 303: Entities access rights 267
Image 304: Selecting the attribute..... 267
Image 305: Access rights to attributes 268
Image 306: »Properties« list in the »Archive« configuration folder..... 270
Image 307: Attribute list in the »Attribute« configuration folder 271
Image 308: Selecting the filter in the »Attribute« configuration folder 271
Image 309: Attribute properties..... 273
Image 310: Templates, in which the attribute is used 274
Image 311: List of entity events in the »Audit log« configuration folder..... 276
Image 312: List of content events in the »Audit log« configuration folder..... 277
Image 313: List of contained folders in the »Authentication« configuration folder 278
Image 314: Displaying a list of connectors..... 279
Image 315: ActiveDirectory connector's »Properties« tab 279
Image 316: Displaying a list of external directories 280

2018 © Imaging Systems, Inc., All rights reserved.

Image 317: External directory's »Properties« tab....282
Image 318: External directory's »Authentication« tab....283
Image 319: »Properties« tab in authentication and authorization settings....284
Image 320: Attribute list in the »Codelists« folder....285
Image 321: Selecting the filter in the »Codelists« folder....285
Image 322: Codelist properties....286
Image 323: Available attribute values without quotes....286
Image 324: List of contained folders in the »Content« configuration folder....287
Image 325: List of supported MIME content types....288
Image 326: A list of content converters....289
Image 327: Converter »Properties« tab....291
Image 328: Converter »Properties« tab....292
Image 329: Conversion from DOCX to PDF/A: basic properties settings....293
Image 330: Conversion from DOCX to PDF/A: output parameters settings....293
Image 331: Example of the date of the document content change....293
Image 332: Conversion from DOC to TIFF: basic properties settings....294
Image 333: Conversion from DOC to TIFF: output parameter settings....295
Image 334: Conversion from TIFF to PDF/A: basic properties settings....295
Image 335: Conversion from DOC to TIFF: output parameters settings....296
Image 336: Example of conversion from DOC format to TIFF and PDF/A....296
Image 337: »Properties« tab in the »Digital signatures« configuration folder....297
Image 338: »Properties« tab in the »Full text indexing« configuration folder....299
Image 339: »Properties« tab in the »Parsers« configuration folder....301
Image 340: »Properties« tab in the »Settings« configuration folder....302
Image 341: Attribute list in the »Counters« folder....304
Image 342: Selecting the filter in the »Counters« folder....304
Image 343: Counter properties for the class on the first level....306
Image 344: List of users and user groups in the »Directory« folder....307
Image 345: Selecting the filter in the »Directory« folder....307
Image 346: User group properties....309
Image 347: User properties....310
Image 348: Effective roles of the user....311
Image 349: Explicit roles for the user....311
Image 350: Displaying the icon of a user or group....313
Image 351: Displaying delegates for executing operations....313
Image 352: List of contained folders in the »Legacy archival« configuration folder....314
Image 353: List of content types in the »Content type aliases« configuration folder....315
Image 354: List of templates in the »Object containers« configuration folder....315
Image 355: List of storage profiles in the »Storage profiles« configuration folder....316
Image 356: Displaying storage profile properties....317
Image 357: Displaying browsers for accessing the storage profile....317

2018 © Imaging Systems, Inc., All rights reserved.

Image 358: List of contained »LTANS« configuration folders 318
Image 359: Displaying LTANS settings 319
Image 360: Displaying the properties of timestamping chaining rules 320
Image 361: Displaying properties of the timestamp provider 321
Image 362: Displaying timestamp rules properties 322
Image 363: A list of subfolders in the »Retention« configuration folder 323
Image 364: List of disposition holds in the »Disposition holds« folder 324
Image 365: Display of disposition hold mandates 325
Image 366: List of retention policies in the »Retention policies« folder 326
Image 367: Display of retention policy properties 327
Image 368: Display of retention policy mandates 327
Image 369: List of contained folders in the »Security« configuration folder 328
Image 370: Displaying information about revoked digital certificates in the »Certificate Store« folder 329
Image 371: Displaying information about revoked digital certificates 330
Image 372: Displaying the list of trusted issuers of digital certificates 331
Image 373: Command bar in the contained »Certificates« configuration folder 332
Image 374: Selecting a filter in the »Certificates« configuration folder 332
Image 375: Displaying the properties of the digital certificate 333
Image 376: Information on digital certificate of a trusted issuer 333
Image 377: Displaying the fingerprints of a digital certificate 334
Image 378: Displaying security settings 336
Image 379: A list of subfolders in the »Server« configuration folder 337
Image 380: Attribute list in the »Profiles« folder 338
Image 381: Profile properties 339
Image 382: Volumes, which are tied to the profile 340
Image 383: Using the profile under the root class of the archive 340
Image 384: Entering the class for profile 341
Image 385: Volumes, which are tied to the profile 342
Image 386: Volume properties 344
Image 387: Attribute list in the »Templates« folder 345
Image 388: Selecting the filter in the »Templates« configuration folder 345
Image 389: Template properties 346
Image 390: List of attributes used in the template 347
Image 391: Templates and entities, where the template is used 348

+

2018 © Imaging Systems, Inc., All rights reserved.

LIST OF TABLES

Below is a list of tables appearing in the manual:

Table 1: Manual font types and their meaning 16
Table 2: Definition of abbreviations 19
Table 3: List of terms used in the manual 20
Table 4: Terminology explanation 27
Table 5: Lists of XML tags 45
Table 6: Description of possible attribute properties 175
Table 7: Description of general system attributes 177
Table 8: Description of security class change attributes 178
Table 9: Description of moved entity attributes 178
Table 10: Description of deleted entity attributes 178
Table 11: Description of moved entity attributes 179
Table 12: Description of email attributes 179
Table 13: Description of physical content attributes 180
Table 14: Description of review process attributes 181
Table 15: Description of entity attributes in the decision-making process 181

2018 © Imaging Systems, Inc., All rights reserved.

1 PREFACE

This manual describes the contents and structure of the IMiS®/Client and offers advice on the technical and operational aspects of its use.

1.1 About the manual

The manual presents the 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®/Client.

1.2 Target audience

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

1.3 Conventions

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

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

Table 1: Manual font types and their meaning

2018 © Imaging Systems, Inc., All rights reserved.

1.4 Terms and abbreviations

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

Abbreviation	Description
7ZIP	7-Zip open source file archiver and format (extension ».7z«)
ACL	Access Control List
AES	Advanced Encryption Standard
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«)
CA	Certificate Authority (trustworthy issuing authority)
CAD	Computer Aided Design
CHM	CHM Help format (extension ».chm«)
CPIO	cpio file archiver and format (Unix format – extension ».cpio«)
CRL	Certificate Revocation List (list of revoked certificates)
CSV	Comma Separated Value (text file format– extension ».csv«)
DDR	Double data rate (SDRAM memory type)
DLL	Dynamic-link library
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«)
ERS	Evidence Record Syntax
EXIF	Exchangeable image file format (image metadata format)
FB2	FixtionBook format (electronic book format – extension ».fb2«)
FIPS	Federal Information Processing Standard
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
HSM	Hierarchical Storage Management

2018 © Imaging Systems, Inc., All rights reserved.

Abbreviation	Description
HTML	HyperText Markup Language
ID	Identifier
IPTC	International Press Telecommunications Council News Feed Format
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
ISDM	Information system for document management
JPEG	Joint Photographic Experts Group format (extension ».jpg«)
KRB5TGS	Kerberos 5 Ticket Granting Service (network authentication protocol)
LDAP	Lightweight Directory Access Protocol (Internet protocol for accessing directory)
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)

2018 © Imaging Systems, Inc., All rights reserved.

Abbreviation	Description
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)
SIGEN-CA	Slovenian General Certification Authority
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)
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)
X.509	ITU-T standard for public key infrastructure use
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)
XSD	XML Schema Definition (W3C recommendations for specifying XML document structure)
ZIP	ZIP archive file format (standard archiving format – extension ».zip«)

Table 2: Definition of abbreviations

2018 © Imaging Systems, Inc., All rights reserved.

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.
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.
Windows Explorer	The Windows file manager application into which the IMiS®/Client is integrated.

Table 3: List of terms used in the manual

2018 © Imaging Systems, Inc., All rights reserved.

2 INTRODUCTION

2.1 Features

IMiS®/Client is 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.
For simple and intuitive use, the IMiS®/Client is integrated into Windows Explorer.
To scan content and classify it appropriately, the IMiS®/Client must be integrated with a separate application, the IMiS®/Scan client.

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 and/or KRB5TGS. 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 IMiS®/Client provide the verification of electronic signatures and digital certificates for all electronically signed PDF/A, TIFF, XML and EML files, in order to help you ensure the integrity and authenticity of archived content.

2018 © Imaging Systems, Inc., All rights reserved.

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®/Client 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 Tier placement

In the architectural sense, the IMiS®/Client's place in the multi-tier architecture is in the Presentation Tier, which normally accommodates archival and document system clients within multi-tiered systems. In the functional sense, it provides users with secure access and operation of electronic content archives supported by an audit trail, along with search functions based on the metadata and full text of stored documents.
The IMiS®/ARChive Servers belong to the Data and Logic tier of architecture, following the standard model of client-server architecture of the virtual Document Management System (DMS) which consists of:

- On the Data and Logic tier, one or more IMiS®/ARChive Servers in cluster or replication mode. These accommodate the system logic that controls access, security and document management processes.
- On the Presentation Tier, archive or document system clients such as the IMiS®/Client, browser, and applications for various devices (smartphone, tablet, laptop, desktop). These may optionally control devices used for the capturing and digitizing of physical content.

2018 © Imaging Systems, Inc., All rights reserved.

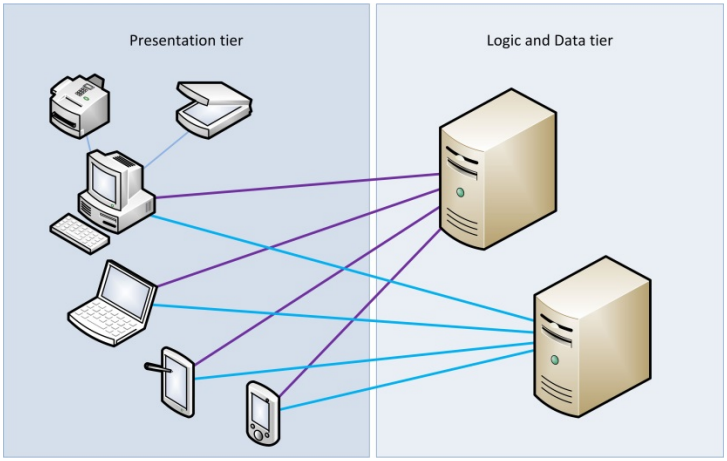


Image 1: Example virtual two-tier document system

2.3 Versioning and numbering

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

IMiS.Client.MAJOR.MINOR.RELEASE.ARCHITECURE.TYPE.msi

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.

  Example: the October 2018 IMiS® module release is represented by 1810 in the RELEASE identifier.

- ARCHITECTURE: marks the target processor architecture. Possible values are "x32" for 32-bit Windows systems, and "x64" for 64-bit systems.

2018 © Imaging Systems, Inc., All rights reserved.

- TYPE: optionally marks the type of installation package. The absence of this designation means a full version of the IMiS® module is installed. The designation "demo" represents a demo or test version of the IMiS®/Client module.

Example: full version of IMiS®/Client 9.9.1810 installation package for 64-bit Windows with .NET 4.0 framework:

IMiS.Client.9.9.1810.x64.msi

2.4 Functionalities

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

- Access to any number of IMiS®/ARChive Servers.
- Secured communication with the IMiS®/ARChive Server via SSL/TLS protocol.
- Secure user authentication (SRP-6A, LDAP, KRB5TGS).
- Simple user authentication via Single Sign-on (SSO) mode.
- Access to the records according to a predetermined organization scheme.
- Editing of access permissions for entities, attributes and metadata.
- Entry and management of the records metadata according to a predetermined attribute scheme.
- Storage of archive materials of electronic origin, or digitized using the scanner.
- Content management (capturing, viewing data, saving, opening, transferring, copying, moving, deleting, tagging for later indexing/conversion).
- Creating and checking in document versions (versioning).
- 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).
- Printing of records and classification schemes.
- Creation of access reports.

2018 © Imaging Systems, Inc., All rights reserved.

- Creation of reports on the total number of folders or documents within classes, which may be structured according to metadata properties.
- Overview of reports on the export, transfer and import of the records, accessible to authorized users.
- Overview of reports on deleted entities, accessible to authorized users.
- Marking of records as key for holding in the review process or as recommended for retention or deletion.
- Management of retention policies and disposition holds for the records.
- Support for review processes.
- Configuration and administration of IMiS®/ARChive Servers.
- Support for IPv4 and IPv6 network communication systems.

3 TECHNICAL DOCUMENTATION

3.1 Client architecture

IMiS®/Client is the user component of an electronic and physical records management system. It is integrated into the Windows Explorer and uses its framework to display and enable the management of records. The client's integration with the Explorer lets users access the electronic archive in a simple and intuitive manner and requires no additional archive management applications.

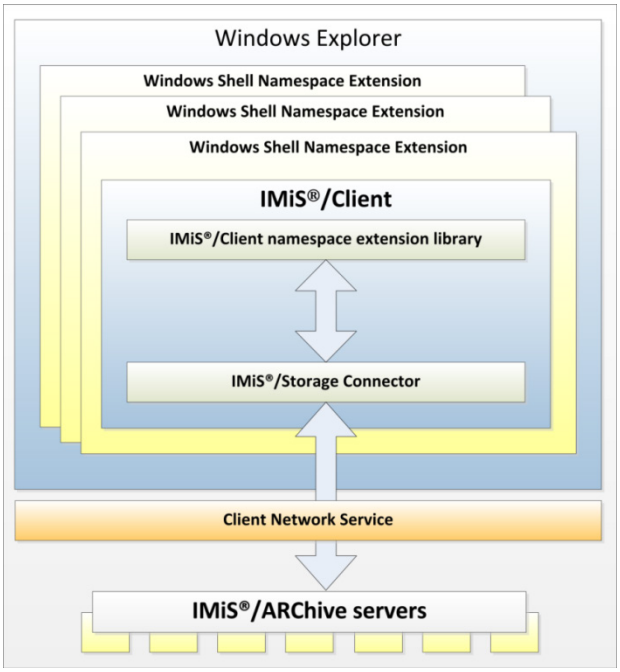


Image 2: Client architecture

The basic components of the IMiS®/Client are:

- imisclient.shellex.net.dll; performs integration with the Windows Explorer and the windows shell namespace extension.
- imisclient.net.dll; provides the business logic that governs the archive.
- imisclient.soap.net.dll; adds the business logic for archive configuration.
- storageconnector.net.dll; is used by imisclient.net.dll to connect to the IMiS®/ARChive Servers.
- converttopdf.dll; a printer driver enabling the conversion of the records into its long-term storage format (PDF/A).

To digitize (scan) physical records, the client uses the separate module IMiS®/Scan.

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.

2018 © Imaging Systems, Inc., All rights reserved.

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 2016 </title>
...
```

Image 3: 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.

2018 © Imaging Systems, Inc., All rights reserved.

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]_nnn.xml, where nnn is the sequence number.

The exported audit log file appears in the format audit_nnn.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. For more information see 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* audit_1.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

2018 © Imaging Systems, Inc., All rights reserved.

/<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	

2018 © Imaging Systems, Inc., All rights reserved.

/<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:CurrentLocation	**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

2018 © Imaging Systems, Inc., All rights reserved.

/<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	

2018 © Imaging Systems, Inc., All rights reserved.

/<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	

2018 © Imaging Systems, Inc., All rights reserved.

/<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«. For more information see 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

2018 © Imaging Systems, Inc., All rights reserved.

/<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

2018 © Imaging Systems, Inc., All rights reserved.

/<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«. For more information see 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

2018 © Imaging Systems, Inc., All rights reserved.

/<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
Commentary:	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: • 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). 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: • 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.			

2018 © Imaging Systems, Inc., All rights reserved.

	Description of enumerator values for the type of access right: • EXPLICIT_ALLOW: explicit permission. • EXPLICIT_DENY: explicit denial. • INHERITED_ALLOW: inherited permission. • INHERITED_DENY: inherited denial.				
XMLScheme type:	none	**Reference:**	ACL	**MOREQ2 code:**	/

/<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:**	/

2018 © Imaging Systems, Inc., All rights reserved.

/<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:	The »part« label contains the name of a separate file, which contains exactly one exported document content, and the following XML attributes: • 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 hash: hash value of the content that is used for verifying the authenticity of a separate file.					
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:**	/

2018 © Imaging Systems, Inc., All rights reserved.

/<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:**	/	

2018 © Imaging Systems, Inc., All rights reserved.

/<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:	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. Two XML attributes are contained: • Hash_algorithm: »string« type containing the name of the hash algorithm. • Hash: hash value of file with the authenticity evidence. The value of the XML tag contains the name of the authenticity evidence file.					
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:**	/

2018 © Imaging Systems, Inc., All rights reserved.

/<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:	The »property« label represents the entity attribute together with values. Every »property« label can have the following XML attributes: • »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:	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. 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. For BINARY attributes the »value« label also contains the XML »mime« attribute, which contains data on the content type.					
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:	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.					
XMLSchema type:	complexType	**Reference:**	ACL		**MOREQ2 code:**	/

2018 © Imaging Systems, Inc., All rights reserved.

/<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

2018 © Imaging Systems, Inc., All rights reserved.

/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: • »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

2018 © Imaging Systems, Inc., All rights reserved.

/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 arhcived 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 4: Example XSD scheme

2018 © Imaging Systems, Inc., All rights reserved.

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 5: 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.

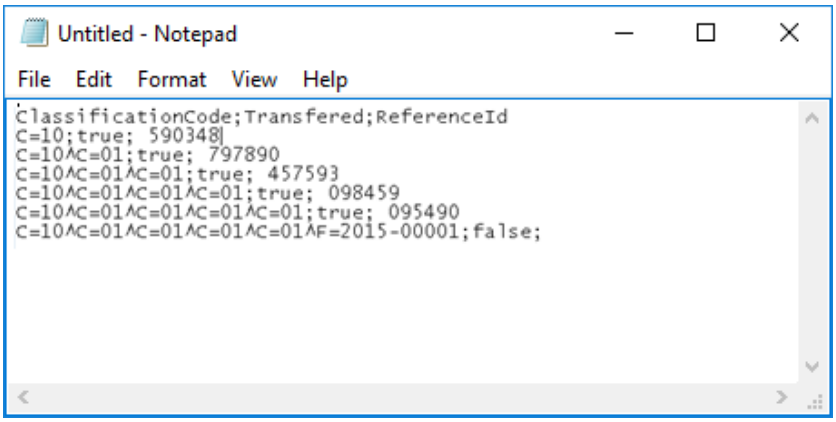


Image 6: Example of a confirmation file after transfer

2018 © Imaging Systems, Inc., All rights reserved.

4 USER MANUAL

4.1 Interface description

The user interface of the IMiS®/Client is integrated into the MS Windows Explorer. 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 three main windows described below.

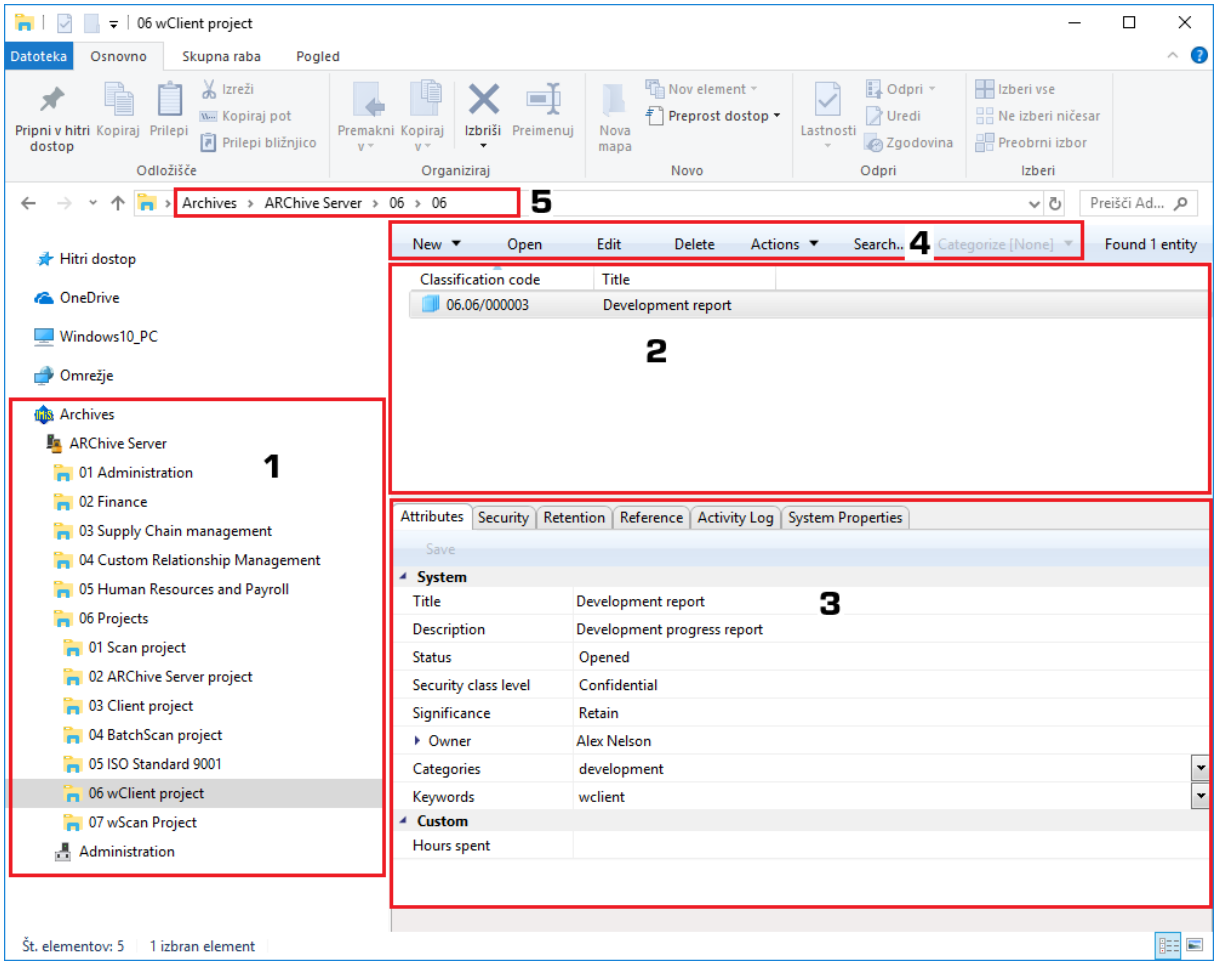


Image 7: User interface of the IMiS®/Client

The left view (number 1 in the image above) shows the »Archives« folder.
This folder contains archives which represent individual IMiS®/ARChive Servers.
Under every archive are shown the root classes according to the classification scheme, as well as a special »Administration« folder that contains predetermined system folders.

2018 © Imaging Systems, Inc., All rights reserved.

Inside each root class, there are classes or folders that are contained by the root class.
More information on the left view is found in chapter Classification scheme.

The top right view (number 2 in the image above) shows a list of entities contained by the archive, class or folder currently selected in the left view. An archive only contains classes, whereas a class or folder can contain sub-folders or documents. The contained entities are shown under a bar displaying their common attributes: »Classification code« and »Title«.
Using the common attribute bar, the user can sort the display order of entities according to the preferred attribute.
More information on the top right view is found in chapter List of entities.

The bottom right view (number 3 in the image above) shows tabs that display various kinds of data about the selected entity. When browsing publicly accessible entity information, users can generally view the publicly accessible metadata of the entity in the »Attributes« tab,
a display of the user's effective permissions for this entity in the »Security« tab, and other publicly accessible system metadata in the »System properties« tab.
Users with appropriate access rights may also access the selected retention policies and disposition holds in the »Retention« tab and audit log of the selected entity in the »Activity Log« tab. When viewing data of an open entity, users may also view other types of metadata:
in case of records this includes access logs, and for users with appropriate access rights also the possibility to edit the Access Control List (ACL) of the entity and the corresponding metadata. More information on the bottom right view is available in chapter Entity information.

The command bar of the Windows Explorer (number 4 in the image above) shows commands or actions next to the »Organize« system button. These depend on the type and status of the chosen entity in the classification scheme, or the chosen entity in the entity list, and also on the rights and roles of the user. For example, a selected »Archives« folder offers commands for adding new archives, whereas a selected archive offers commands for logging in or out of the archive, create root classes, and search the archive.
When selecting an entity, users are offered additional specialized actions for entities in addition to the »create«, »open« and »edit« commands.
More information on the command bar is available in chapter The command bar.

2018 © Imaging Systems, Inc., All rights reserved.

To the right of the command bar is the search results counter. It displays the number of entities in the right view.

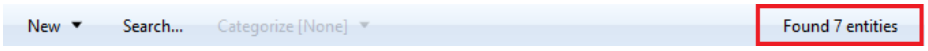


Image 8: The search results counter

To enable quicker access to entities, the user is shown a hierarchical view of the entity's position within the tree structure (under number 5 in the image) above the command bar in the user interface. It enables quick access to the parent entities.

4.1.1 Classification scheme

Upon installation, the IMiS®/Client is integrated into the Windows Explorer. According to chosen user preferences during configuration, the left view of the Window Explorer shows the »Archives« folder in the »Desktop«, the »Computer«, or the »Network« folder.
The »Archives« folder is the entry point of the IMiS®/Client operation.

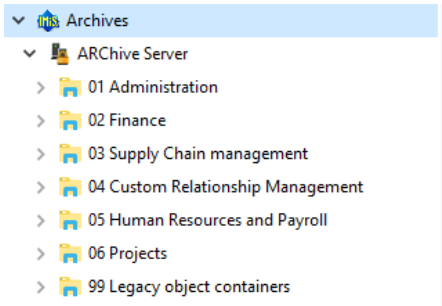


Image 9: Display of the Archives folder

Individual archives are found under the »Archives« folder. By selecting an archive and logging in via the dialog box, the user logs into the archive. A new archive is added by using the »Add archive« command in the popup menu of the »Archives« folder.
An archive is removed by using the »Remove archive« command in the popup menu of the selected archive.
Following successful login into an archive, root classes of the selected archive appear underneath the archive together with the special »Administration« folder containing system folders.

2018 © Imaging Systems, Inc., All rights reserved.

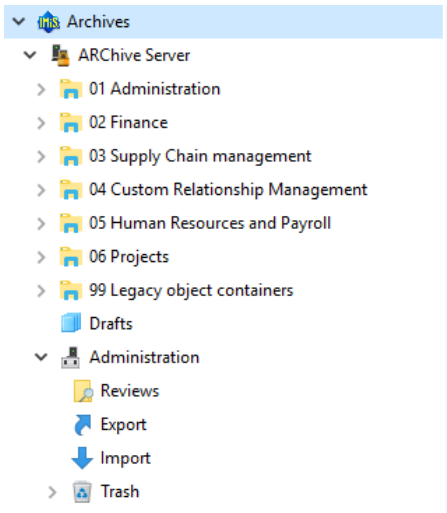


Image 10: Display of an archive's root classes and the Administration system folder

By navigating the classes and folders, the tree view of classes and folders expands according to the classification scheme.

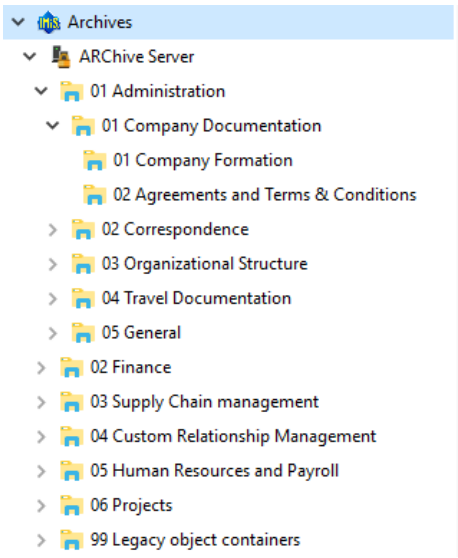


Image 11: Expanded tree view of the classification scheme

Note: By clicking the arrow in front of the selected class, the user opens a list of contained classes. A contained folder can only be selected once the user has double-clicked it in the list of contained entities, in the top right view of the Windows Explorer.

2018 © Imaging Systems, Inc., All rights reserved.

The IMiS®/ARChive Server does not limit the number of archive root classes, or the number of contained sub-classes, folders, or documents in an individual class or folder.
By configuring the server, though, limits are set for the number of hierarchy levels of classes and folders in the classification scheme.
The default server settings specify a hierarchy with a maximum of six (6) hierarchy levels for the class, and a maximum of four (4) hierarchy levels for the folder.

Tip: To preserve the clarity of the classification scheme, and due to limitations in the moving of entities, users are strongly recommended NOT to place documents directly into classes but always into appropriate folders.

4.1.2 List of entities

The list of entities (classes, folders or documents) contained by the selected class or folder is located in the top right view of Windows Explorer. The contained entities are displayed under a bar that shows the names of common entity attributes.

Tip: The user may also access an entity in the list of contained entities by pressing the Enter key.

The display order of attributes can be managed by moving the selected columns to the chosen spot. By selecting the column of the corresponding attribute, displayed entities are ordered according to the selected attribute.

Classification code	Title	Description	Status
01	Administration	Company documentation and correspondence	Opened [Inherited]
02	Finance	Account payable, Accounts receiveable, Banking	Opened [Inherited]
03	Supply Chain Management	Supply planning and scheduling records	Opened [Inherited]
04	Customer Relationship Management	Customer and Business partner records	Opened [Inherited]
05	Human Resources and Payroll	Employee records	Opened [Inherited]
06	Projects	IMiS projects	Opened [Inherited]

Image 12: List of entities contained by the selected entity

The user can add or remove attributes via the popup menu on the line of displayed attributes. The popup menu offers all the possible template attributes for the creation of sub-entities inside the selected entity. The displayed attributes are marked by a check mark.
The attribute »Classification code« is always present and cannot be removed from the list.
The settings of attributes shown only apply to the currently displayed entity and are not inherited.

2018 © Imaging Systems, Inc., All rights reserved.

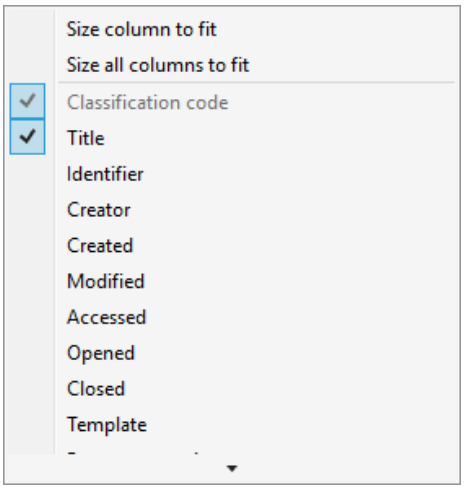


Image 13: Popup menu over a line of displayed attributes

4.1.3 Entity information

Information about the selected entity is found in tabs under the list of entities in the bottom right view of Windows Explorer. Previewing the selected entity will display those tabs and content which are publicly accessible to the user. When a selected entity is open in the reading or editing mode, the tabs are adapted according to the effective permissions of the user.

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

- »Attributes« tab: contains system metadata that may be edited, and the predefined metadata of the entity. This tab is always shown, during preview as well as in the reading or editing mode.
- »Content« tab: contains a list of the content of the entity. This tab is only shown when the entity is open in the reading or editing mode.
- »Physical Content« tab: contains the metadata of physical record that belongs to the entity. This tab is only shown when the entity is open in the reading or editing mode.
- »Security« tab: contains an overview of the effective permissions of the user on this entity. The content of the tab changes when the entity is opened in the editing mode and the user has the effective access right »Change permissions«.
  In this case, the tab shows groups or users with their access rights on this entity specified, and a table of access rights where effective permissions may be edited for each selected group or user.
- »Retention« tab: contains the settings for the selected retention periods and the selected disposition holds. The tab is shown when previewing a selected entity and when the selected entity is open in the reading or editing mode.

2018 © Imaging Systems, Inc., All rights reserved.

- »References« tab: contains a list of references to other entities in the classification scheme. The tab is always shown in the preview mode for a selected entity and when the selected entity is open in the Read-only or Edit mode.
- »Activity Log« tab: contains the audit log for the selected entity.
  This tab is always shown, during preview as well as in the reading or editing mode.
- »System Properties« tab: contains general and special system metadata which are read-only. This tab is always shown, during preview as well as in the reading or editing mode.

4.1.3.1 The »Attributes« tab

The »Attributes« tab contains a list of metadata for the selected entity.
The first column shows the names of the metadata types and the second column their values.
In the editing mode the fields for editable values change into fields into which the user enters values.

When metadata name is written in bold font, this means the metadata is required (mandatory). These values must be entered before you are able to save the entity.

Metadata in the »Attributes« tab is classified into the following groups:

- »System«: contains system metadata that may be modified and is publicly accessible.
  For more information see chapter General system attributes.
- »Email«: contains email metadata. This group is only available for documents that originate from an email template and are currently opened in the reading or editing mode. For more information see chapter Email attributes.
- »Custom«; contains custom-entered metadata of the entity. This group is only available for documents which are currently open in reading or editing mode.

2018 © Imaging Systems, Inc., All rights reserved.

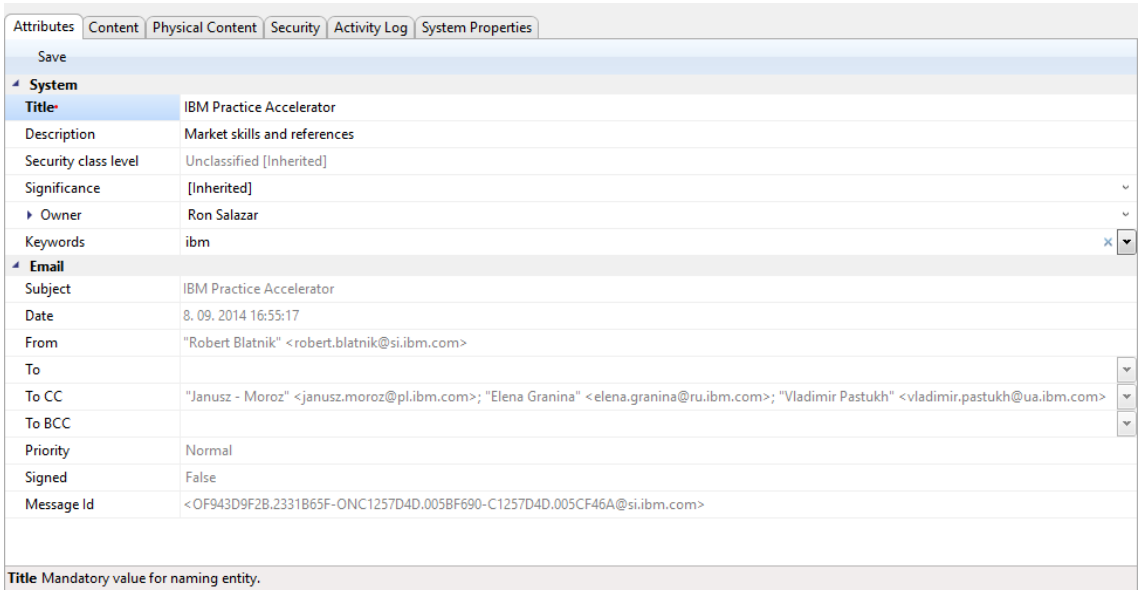


Image 14: View of the »Attributes« tab

The command bar just under the »Attributes« tab has a »Save« button that is activated when metadata is edited. By choosing the »Save« command, changes done to the entity are saved to the archive. If a user modifies the entity but does not save it, a dialog box with an alert prompt appears, where changes may be saved using the »Yes« button or discarded using the »No« button, or the user may go back to editing using the »Cancel« button.

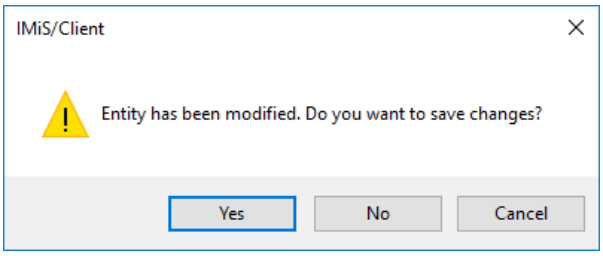


Image 15: Display of the unsaved changes alert prompt

Tip: In case the user does not wish to save any changes on the entity, user can return to the preview by using the »ESC« key and avoid the alert prompt.

4.1.3.2 The »Content« tab

The »Content« tab lets users browse the content (files) attached to the chosen entity when it is open in the reading or editing mode. Adding and removing content is possible when the entity is open in editing mode.

2018 © Imaging Systems, Inc., All rights reserved.

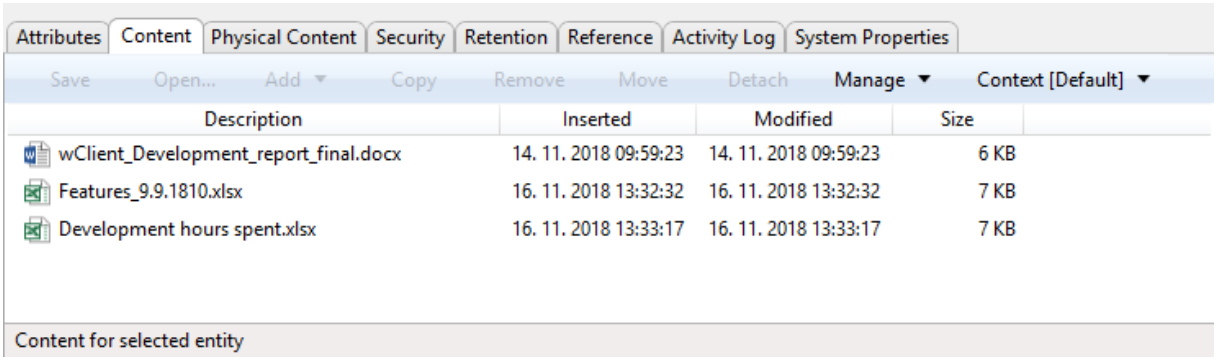


Image 16: View of the »Content« tab

The command bar just under the »Content« tab offers the following buttons:

- »Save«: becomes active when the content of the selected entity is modified, if the entity is open in editing mode (when content is added or deleted).
  The »Save« command saves changes to the archive. Unsaved changes will be discarded.
- »Open«: opens the selected content in the default application associated with the content type, as it was specified when the content was saved to the archive.
  The command is available when the selected entity is open in reading or editing mode.

  Note: a selected content may be opened even if it hasn't been saved yet.

- »Copy«: copying the content to another document.
  The command is available when the selected entity is open in Edit mode.
- »Remove«: allows you to remove content from the selected entity. The command is available when the selected entity is open in editing mode.
- »Move«: moving the entity within the classification scheme on the archive.
- »Detach«: detaching the selected converted content.
  The command is available when the selected entity is open in Edit mode.
- »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.
- »Context«: enables the display of contents in a specific context.

2018 © Imaging Systems, Inc., All rights reserved.

4.1.3.3 The »Physical Content« tab

The »Physical Content« tab shows users the metadata of physical content corresponding to the selected entity. For more information see chapter Physical content attributes.

The tab is shown for folders and documents when the selected entity is open in reading or editing mode. Physical content metadata may be entered when the selected entity is open in editing mode.

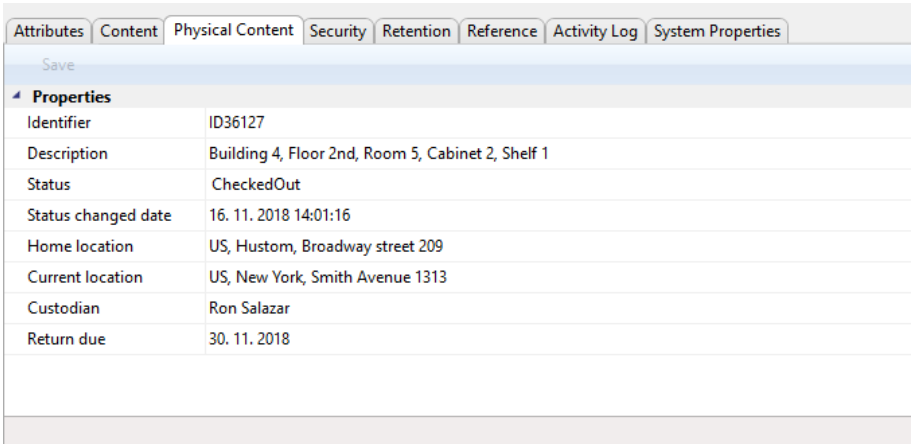


Image 17: View of the »Physical Content« tab

The command bar just under the »Physical Content« tab has a »Save« button that is activated when the value of an attribute is edited.

By using the »Save« command, changes done to the entity are saved to the archive.

Unsaved changes will be discarded.

4.1.3.4 The »Security« tab

The »Security« tab shows:

- The display of the directory entity effective access rights on the selected entity.
- The overview and editing of the Access Control List (ACL) or the explicit permissions for directory entity (group, user, attribute of directory entity type) on the entity and entity metadata.

The tab offers three types of data display for the selected entity:

- Preview mode.
- Reading mode.
- Editing mode.

2018 © Imaging Systems, Inc., All rights reserved.

The preview mode shows the title of the selected entity in the »Entity name« field.
The list below it shows the current status of effective access permissions of the registered user for the entity. By selecting the »Effective permissions« command, other users or groups can also view the effective access permissions for the entity.

The permissions status depends on the date and time of display, as certain permissions may be time-limited. The permissions that are ticked are available to the user or group at the moment.

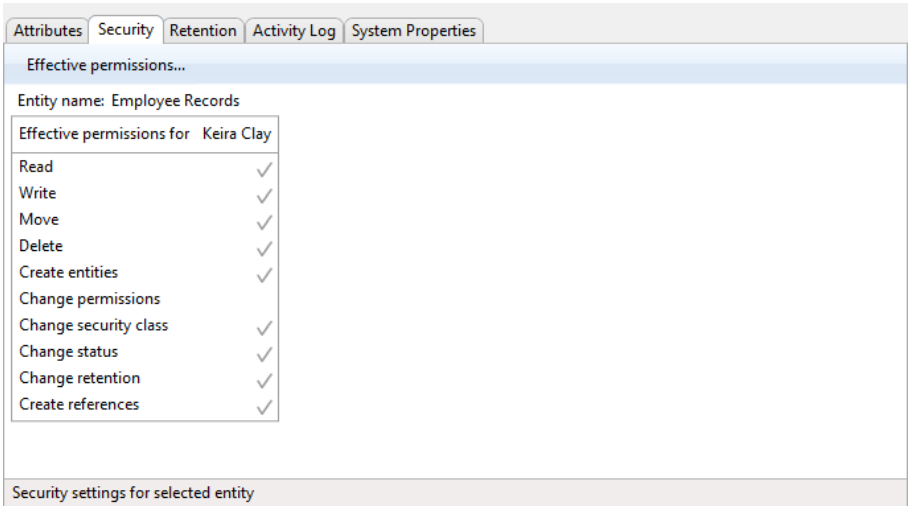


Image 18: View of the »Security« tab in preview mode

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

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

2018 © Imaging Systems, Inc., All rights reserved.

- »Change security class«: directory entity has permission to change the security class of the selected entity.
- »Change status«: directory entity has the permission to change the status of a selected entity.
- »Change retention«: directory entity has the permission to read and change the content of »Retention« tab.
- »Create reference«: directory entity has the permission to create references to the other entities.

In the preview mode, the command bar just under the »Security« tab has the »Effective permissions« button. It also enables other users to view the effective access permissions for the entity. By clicking the button, a window appears showing all the users registered on the IMiS®/ARChive Server. The window allows user to search users via the search field. By clicking the »OK« button, the tab will display the list of effective access rights granted to the selected user, on the selected entity.

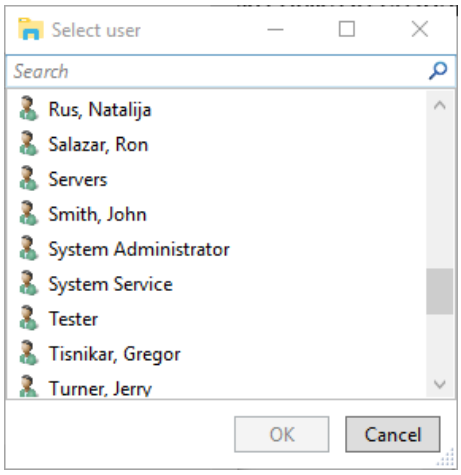


Image 19: User selection window of the »Security« tab in preview mode

In the reading mode display of the selected entity, the content of the »Security« tab changes into an overview of the Access Control List (ACL) for the entity or the selected metadata of the entity.

2018 © Imaging Systems, Inc., All rights reserved.

In the display of an open entity, the command bar just under the »Security« tab offers the following buttons:

- »Save«: becomes active in case of changes to explicit permissions of the selected directory entity, and when directory entities are added or removed. By using the »Save« command, changes to explicit permissions are saved to the server. Unsaved changes will be discarded.
- »Add«: enables the adding of directory entities registered on the IMiS®/ARChive Server into the »Group or user names« list and the setting of their explicit permissions on the chosen entity.
- »Remove«: enables the removal of selected directory entities from the »Subject« list and the revoking of their explicit permissions on the selected entity.

Just under the »Entity name« field, the selection field »Permissions on« appears, which allows the user to choose the entity or metadata governed by the Access Control List.

On the left side, the list of effective permissions for the current user is replaced by the list of directory entities. This list contains directory entities that were granted explicit access rights on the selected entity in the Access Control List.

The right side shows the list »Effective permissions for selected directory entity«, which shows the current effective permissions of the selected directory entity on the entity.

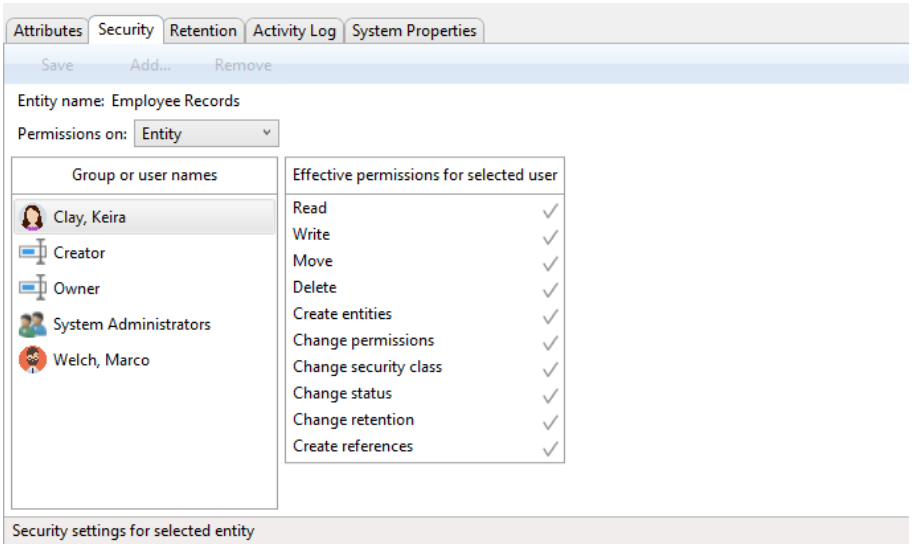


Image 20: Reading mode display of the »Security« tab

4.1.3.4.1 Editing access permissions for entities

In the editing mode display, the command bar just under the »Security« tab allows the command »Edit«. By clicking this button, the user edits the Access Control List (ACL) for the selected directory entity (user, group, attribute of the directory entity type) chosen in the field »Permissions on«.

On the right, a permissions list appears for the selected directory entity or an attribute of the directory entity type.
By ticking the »Allow« column, the user explicitly adds a permission; by ticking the »Deny« column, he revokes a permission.
The validity field containing »Valid from« and »Valid to« values allows an authorized user to set time limits for permissions granted to the selected directory entity or to the respective directory entity contained in the mentioned directory entity type attribute.

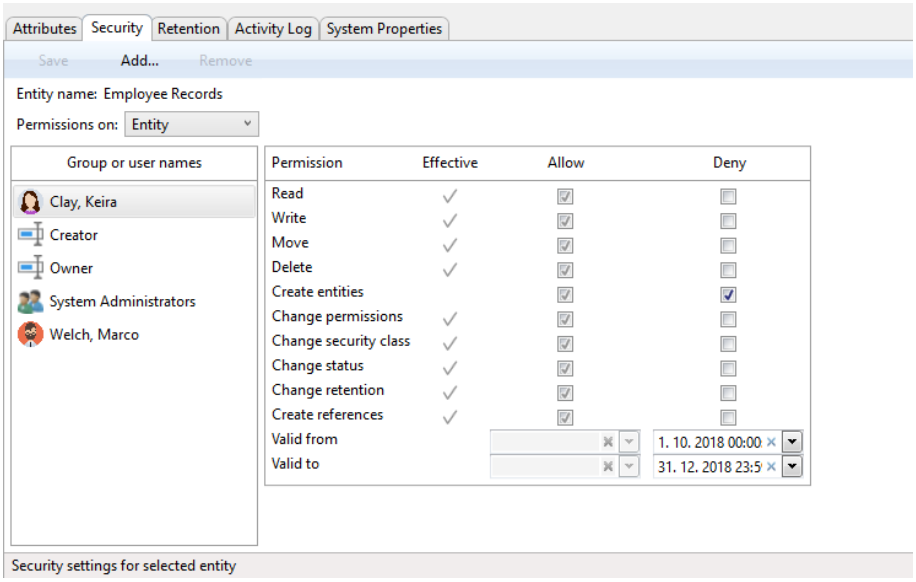


Image 21: Editing access permissions on an entity for a user

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 subordinate 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.

2018 © Imaging Systems, Inc., All rights reserved.

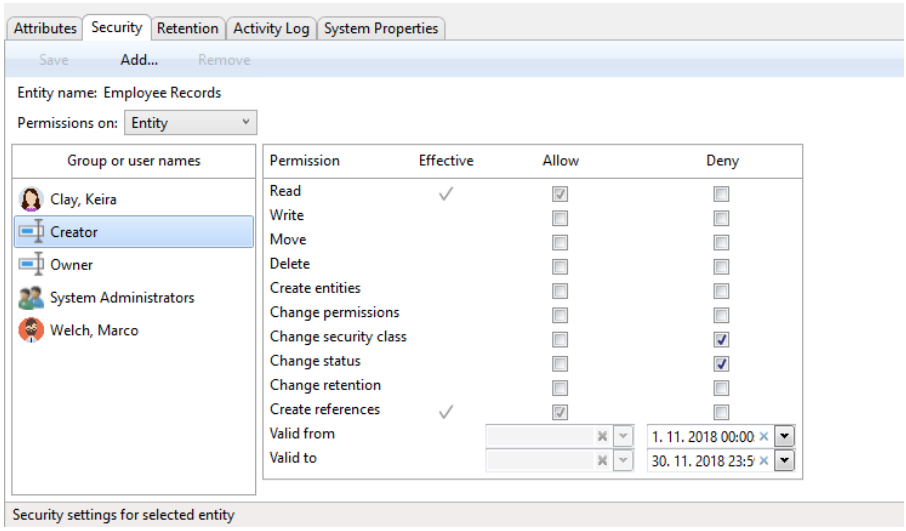


Image 22: Editing access permissions on an entity for a directory entity type attribute

4.1.3.4.2 Editing access permissions 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.

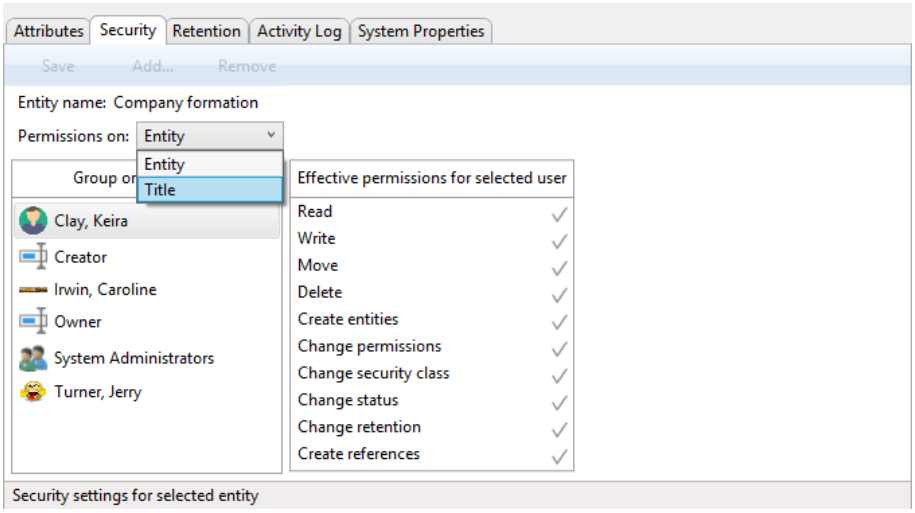


Image 23: Popup menu for selecting access permissions to a selected metadata

The left view contains a list of directory entities (user, group, directory entity type attributes) with access permissions to the selected metadata. In Edit mode, the user selects the directory entity for which he wants to set the access permissions. 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.

2018 © Imaging Systems, Inc., All rights reserved.

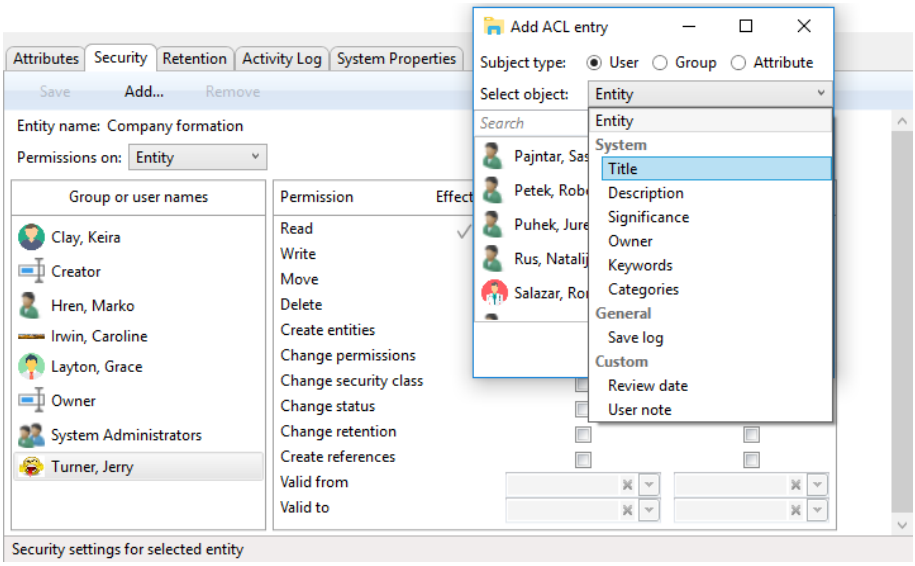


Image 24: Adding a directory entity for setting access permissions

In the right part of the view, a list of metadata editing permissions is shown for the selected directory entity. By checking the »Allow« column, a user authorized to change permissions can grant explicit permissions to the selected directory entity, and by checking the »Deny« column deny permissions.

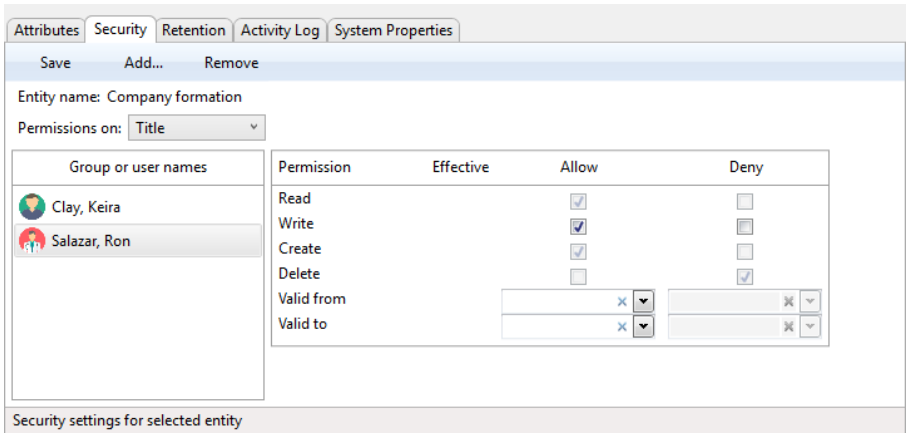


Image 25: List of directory entity permissions on the selected metadata

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

- »Read«: directory entity has permission to read the value of the selected metadata of the entity.
- »Write«: directory entity has permission to edit the value of the selected metadata of the entity.

2018 © Imaging Systems, Inc., All rights reserved.

- »Create«: directory entity has permission to create the value of the selected metadata of the entity.
- »Delete«: directory entity has permission to delete the value of the selected metadata of the entity.

The validity field containing »Valid from« and »Valid to« values allows an authorized user to set time limits for permissions granted to the selected directory entity.

4.1.3.5 The »Retention« tab

The »Retention« tab is intended for reviewing and editing retention periods and disposition holds for a selected entity, which are required in review processes.

By selecting the »Context« command in the command bar under the »Retention« tab, the user sets the view context, which is either a list of retention periods or a list of disposition holds for the selected entity.

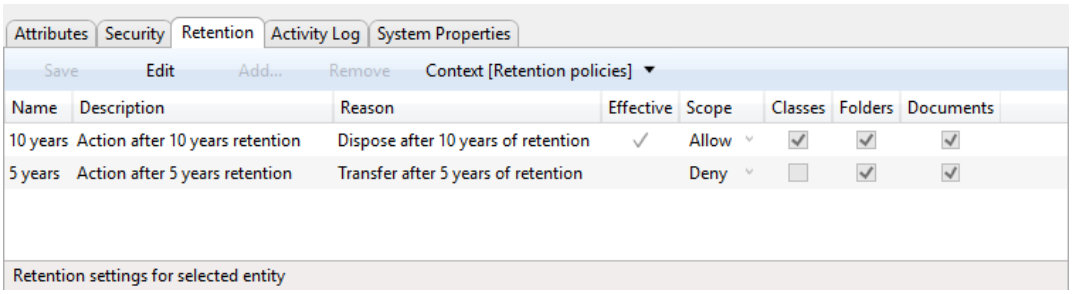


Image 26: Display of retention periods in the »Retention« tab in reading mode

In the event that the user has the »Change retention« access right, the Edit command is enabled in the command bar under the »Retention« tab.
By clicking on the command, the user enables the editing of retention periods and disposition holds for the selected entity.

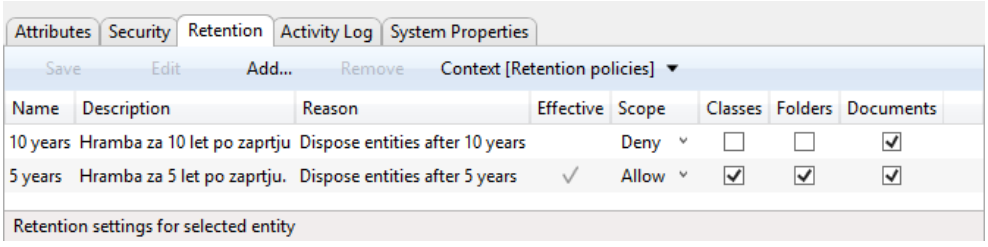


Image 27: Display of retention periods in the »Retention« tab in editing mode

2018 © Imaging Systems, Inc., All rights reserved.

In the tab under the »Retention policies« context a list of retention periods is shown for the selected entity. Among them are inherited retention periods, which are colored gray and cannot be edited, and explicit policies, which can be edited.
Each retention period contains the following data and fields:

- »Name«: represents the name of the retention period.
- »Description«: contains a description of the retention period.
- »Reason«: contains the default reason which is used in the review phase of the review process.
- »Effective«: shows the effectiveness of the retention period on the selected entity.
- »Scope«: sets the permission or prevention of operation of the retention period.
- »Classes«: the retention period applies to all classes under and including the selected entity.
- »Folders«: the retention period applies to all folders under and including the selected entity.
- »Documents«: the retention period applies to all documents under the selected entity.

In the command bar under the »Retention« tab in the »Retention policies« context the following commands are located:

- »Save«: it is activated in the event of changes to explicit retention periods, when adding or removing explicit retention periods.
  The »Save« command saves the changes to the archive, which are otherwise discarded.
- »Edit«: enables the editing of the list of explicit retention periods on the selected entity.
- »Add«: enables the adding of an explicit retention period to the selected entity from the list of available retention periods on IMiS®/ARChive Server.
- »Remove«: enables the removal of selected explicit retention periods on the selected entity.

In the tab a list of disposition holds is shown for the selected entity in the »Disposition holds« context. Each of them contains the following data and fields:

- »Name«: represents the name of the disposition hold.
- »Description«: contains a description of the disposition hold.
- »Reason«: contains the default reason which is used in the decision-making phase of the review process.

2018 © Imaging Systems, Inc., All rights reserved.

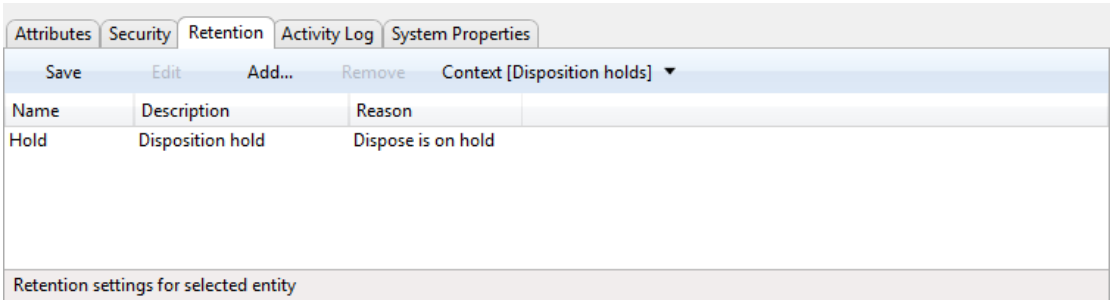


Image 28: Display of disposition holds in the »Retention« tab in reading mode

In the command bar under the »Retention« tab in the »Disposition holds« context the following commands are located:

- »Save«: it is activated in the event of changes to explicit disposition holds, or when adding or removing explicit disposition holds.
  The »Save« command saves the changes to the archive, which are otherwise discarded.
- »Edit«: enables the editing of the list of explicit disposition holds on the selected entity.
- »Add«: enables the adding of an explicit disposition hold to the selected entity from the list of available disposition holds on IMiS®/ARChive Server.
- »Remove«: enables the removal of the selected explicit disposition holds on the selected entity.

4.1.3.6 The »Reference« tab

The »References« tab contains a list of connections to other entities in the classification scheme and is available in the following three modes of displaying the data for the selected entity:

- Preview mode.
- Reading mode.
- Editing mode.

2018 © Imaging Systems, Inc., All rights reserved.

The first column contains the »Titles« of the entities, while the »Descriptions« are shown in the second column.

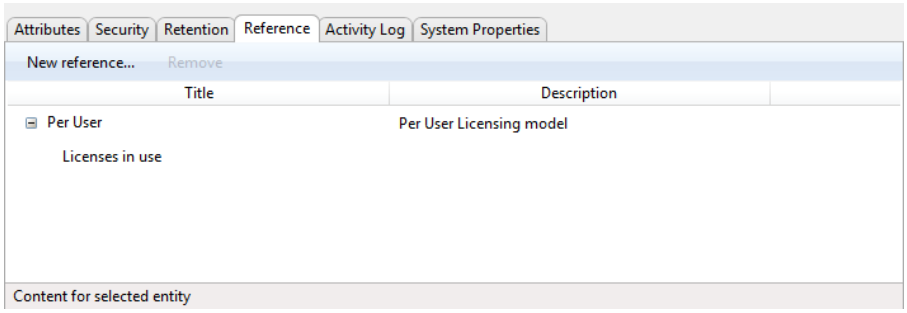


Image 29: The »Reference« tab

If the user has the »Create reference« permission, the »Actions« command in the top command bar or on the selected document on the list enables the »New reference« action.

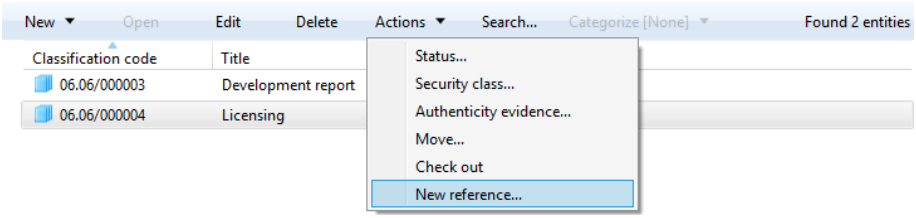


Image 30: Selecting the »New reference« command

The user is shown a dialog box for entering the values of the attributes of the new reference.

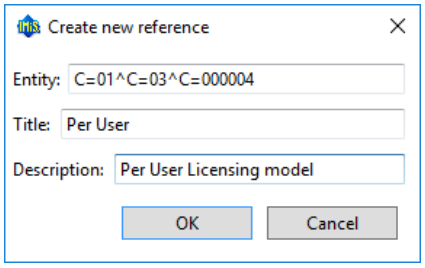


Image 31: The dialog box for entering the attributes of the new reference

In the bottom command bar, under the »References« tab, the following two commands are located:

- »New reference«: adding a connection to another entity in the classification scheme via a dialog box.
- »Remove«: enables removing the selected reference.

2018 © Imaging Systems, Inc., All rights reserved.

The user can add a new reference under an existing reference. He does that by selecting the existing reference and the »New reference« command in the bottom command bar.

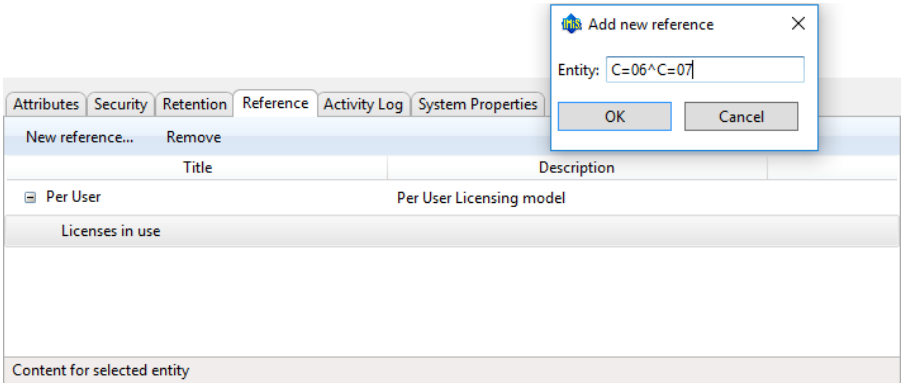


Image 32: Adding a new reference under an existing reference

The new reference is added under the existing reference.

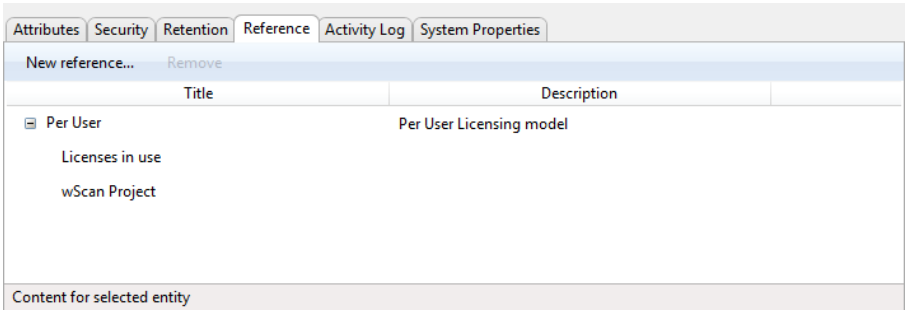


Image 33: A reference added under an existing reference

The user can also add a new reference to an existing reference. He does that by positioning the cursor on the record containing the title and description of the existing reference and selecting the »New reference« command in the bottom command bar.

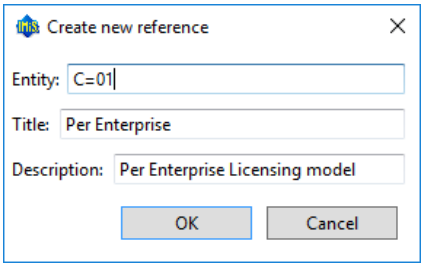


Image 34: Adding a new reference to an existing reference

2018 © Imaging Systems, Inc., All rights reserved.

After entering the Classification code, Title and Description of the new reference and confirming the entry, a new record is created containing the title and description of the reference, and a reference is added to the selected entity.

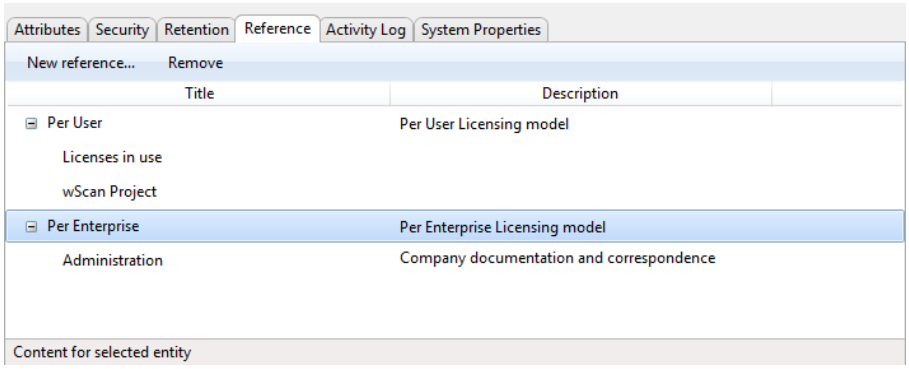


Image 35: A reference added to an existing reference

The user removes the reference by selecting the record containing the title and description of the reference, and the »Remove« command in the bottom command bar. If the user selects only the contained reference, only it can be removed.

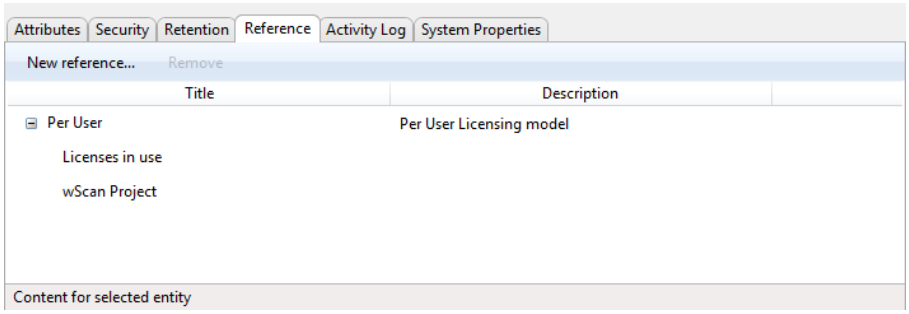


Image 36: Removing a reference

4.1.3.7 The »Activity Log« tab

The »Activity Log« tab shows the audit log for the selected entity. For users with appropriate access rights, the tab is shown when previewing the selected entity, as well as when the entity is open in reading or editing mode.

2018 © Imaging Systems, Inc., All rights reserved.

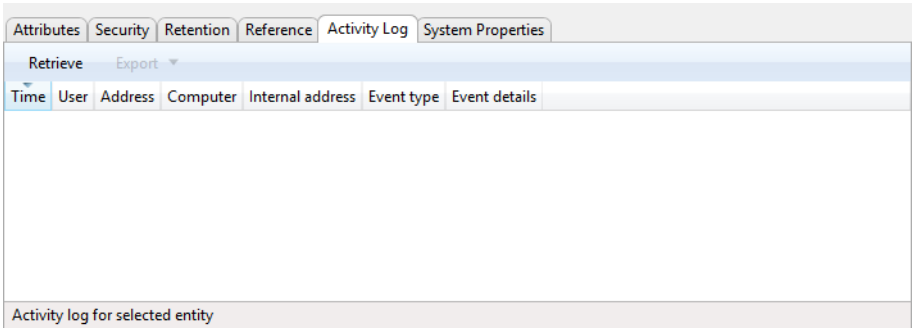


Image 37: View of the »Activity Log« tab prior to retrieving an audit trail

The audit trail is retrieved by using the »Retrieve« command in the command bar under the »Activity Log« tab. Users can refresh the audit trail by using the »Refresh« command.

The audit log records the following data:

- »Time«: time when an action was performed on the selected entity.
- »User«: name of the user who performed an action on the selected entity.
- »Address«: the network address from where the command to perform the action on the selected entity came from.
- »Computer«: the name of the computer from which the command to perform the action on the selected entity came from.
- »Event type«: type of event that was performed on the selected entity.
- »Event message«: message describing the event performed on the selected entity.

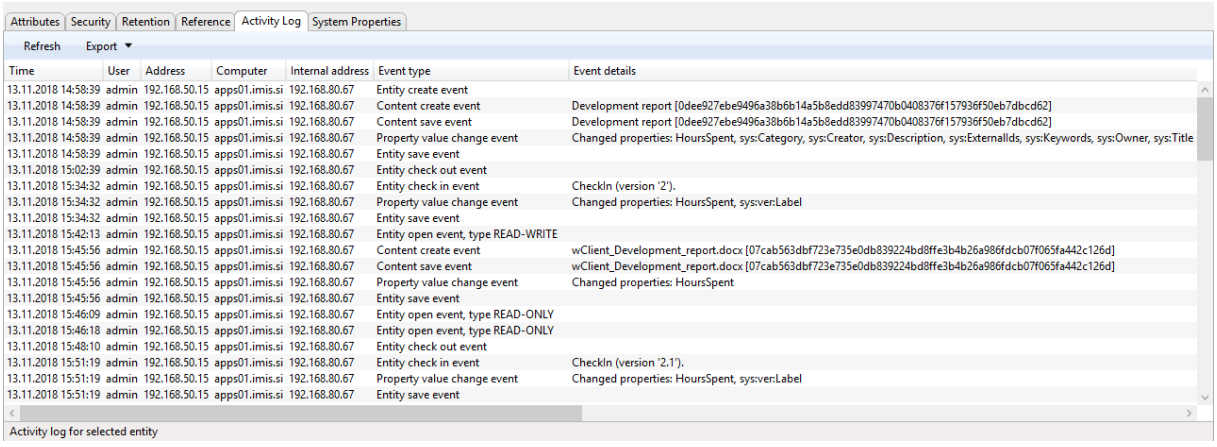


Image 38: View of the »Activity Log« tab with a displayed audit trail

2018 © Imaging Systems, Inc., All rights reserved.

When choosing the »Export« command, a popup menu appears with the possible audit log export formats for the selected entity. The supported formats are CSV and XML.
When a format is chosen, a dialog box appears enabling the user to save the audit log to the file system.

4.1.3.8 The »System Properties« tab

The »System Properties« tab contains a list of system metadata for the selected entity. Unlike the metadata shown by the »Attributes« tab which can be edited, metadata shown by the »System Properties« tab is read-only (with a few exceptions).

The first column lists the names of the attributes, and the second column shows their values. System metadata is classified into the following groups:

- »General«: contains general system metadata. For more information see chapter General system attributes.
- »Security class«: contains metadata on changes done to the entity's security class. For more information see chapter Security class change attributes. This group is only present in case of entities whose security class has been changed before, and which are currently open in the reading or editing mode.
- »Move«: contains metadata that describes the moving of the entity within the framework of the classification scheme. For more information see chapter Moved entity attributes). This group is only present in case of entities that have been moved before, and that are currently open in reading or editing mode.
- »Transfer«: contains metadata that describes the transferring of the entity around the classification scheme. For more information see chapter Transferred entity attributes. This group is only present in case of entities that have been transferred from another archive system, and that are currently open in reading or editing mode.

2018 © Imaging Systems, Inc., All rights reserved.

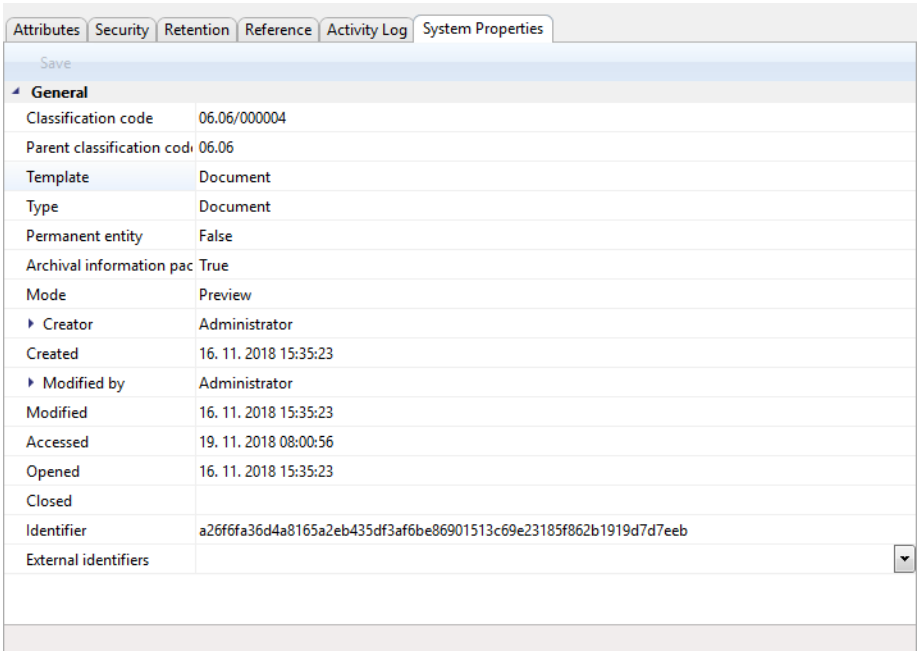


Image 39: View of the »System Properties« tab

4.1.4 The command bar

When the user successfully logs into the selected archive, in the command bar under the Windows Explorer menu, above the list of contained entities, the following commands appear on the bar:

- »New«: creates a new root class on the archive.
- »Search«: enables searching by entity metadata and searching the full text of entity content across the entire archive.
- »Categorize«: enables sorting into categories.

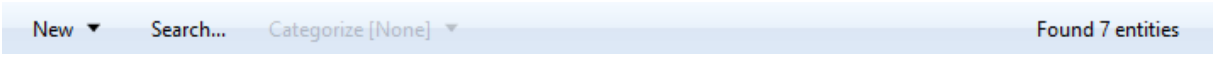


Image 40: Command bar above a selected archive when logged in

When selecting an entity in the overview of the classification scheme or the list of contained entities, the top command bar offers the following possible commands or actions on the selected entity:

- »New«: creates a new entry.
- »Open«: opens the selected entity in the reading mode.
- »Edit«: opens the selected entity in the editing mode.

2018 © Imaging Systems, Inc., All rights reserved.

- »Delete«: deletes the selected entity, including all the corresponding metadata and content.
- »Actions«: contains commands for performing various operations on the selected entity:
  - »Status«: enables the user to edit the status of the entity via a dialog box, which also offers the option to enter the reasons for the changes performed.
  - »Security class«: enables the user to change the entity's security class via a dialog box, which requires the user to enter the reasons for the change performed.
  - »Authenticity evidence«: enables the user to retrieve authenticity evidence for the selected entity.
  - »Move«: enables the user to move the selected entity around the classification scheme of the archive.
  - »Check out«: creates new version of a document.
  - »New reference«: creates a new reference.
- »Search«: allows searching by the metadata of contained entities and the full text of the selected entity content.
- »Categorize«: a view of entities classified under the same category at the same hierarchical level.
  - »None«: the entities are not sorted by keywords or categories.
  - »Keywords«: the entities are sorted by keywords.
    For more information see chapter Sorting by keywords.
  - »Category«: the entities are sorted into the same category.
    For more information see chapter Sorting into categories.

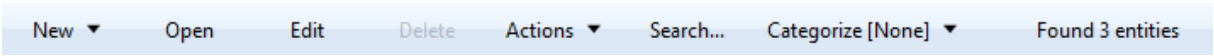


Image 41: Command bar above a selected entity

The right part of the command bar contains the search results counter. It displays the number of entities on the list of entities.

When selecting an entity in the »Search results« folder, the same commands are available as when selecting an entity in the classification scheme or the list of contained entities, with the exception of the command »New«.

2018 © Imaging Systems, Inc., All rights reserved.

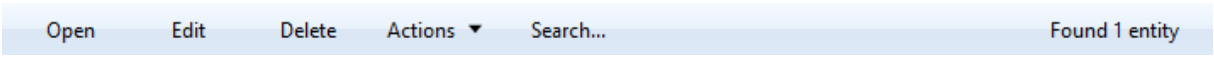


Image 42: Command bar above selected entity in the “Search results” folder

When selecting an entity in the »Queue« folder under the »Trash« and »Administration« system folders, the only available commands are »Open«, »Edit« and »Delete«. These will open the entity in reading or editing mode, or delete the entity.

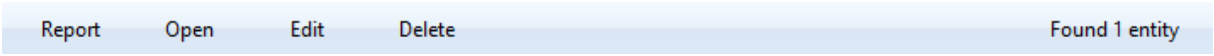


Image 43: Command bar above selected entity in the »Queue« system folder

When selecting an entity in the »Export« and »Import« folders under the system folder »Administration«, the only available command is »Open«, allowing users to open the entity in reading mode.

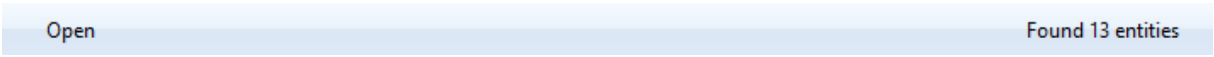


Image 44: Command bar above selected entity in the system folders »Export« and »Import«

When selecting an entity in the »Trash« folder under the »Administration« system folder, the only available command is »Report«, allowing users to create a report on deleted entities.

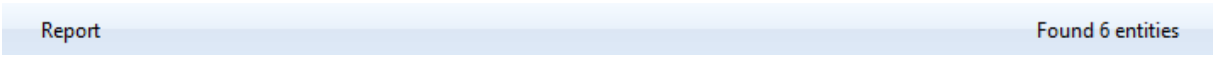


Image 45: Command bar above selected entity in the system folder »Trash«

4.1.4.1 Sorting into categories

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

2018 © Imaging Systems, Inc., All rights reserved.

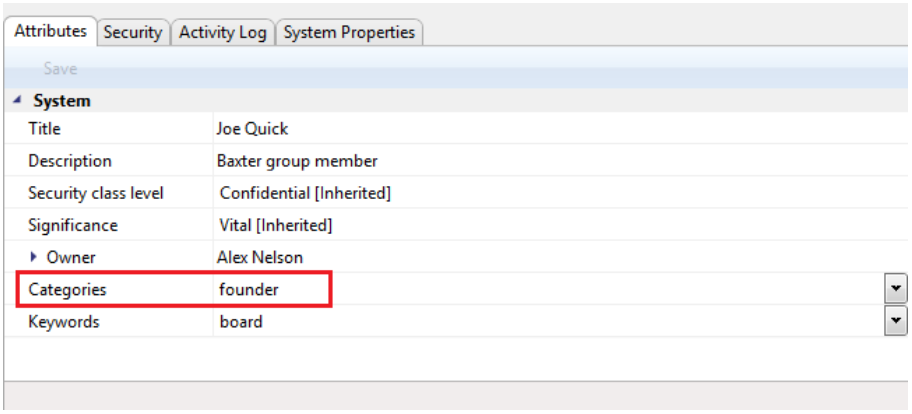


Image 46: An example of an entity with a defined value of the attribute »Categories«

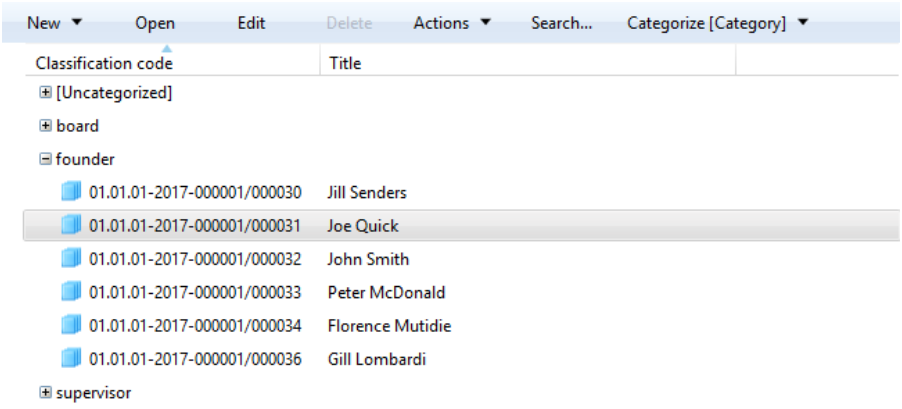


Image 47: A categorized »Categories« view

4.1.4.2 Sorting by keywords

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

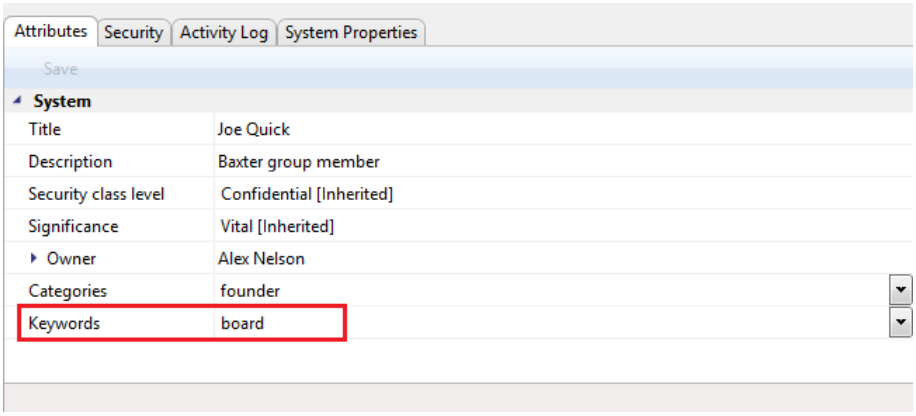


Image 48: An example of an entity with a defined value of the attribute »Keywords«

2018 © Imaging Systems, Inc., All rights reserved.

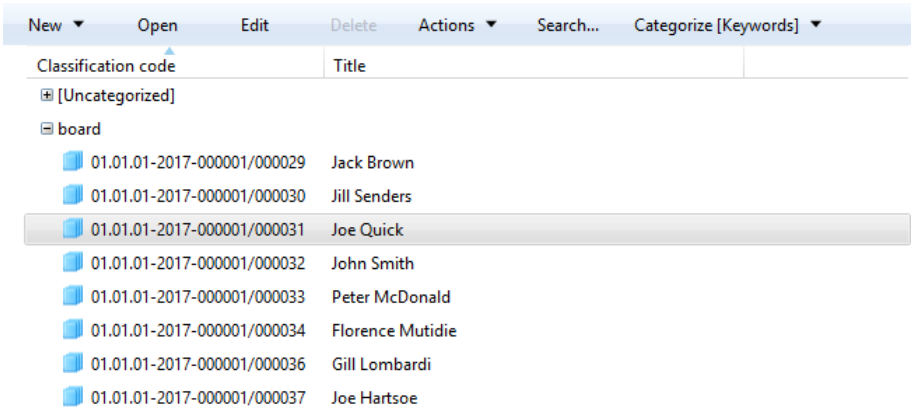


Image 49: A categorized »Keywords« view

4.1.5 Menu functions

The popup menu over the »Archives« folder offers the following commands of the IMiS®/Client, in the left view of Windows Explorer next to the OS commands:

- »Add archive«: enables users to add archives to the »Archives« folder.
- »Utilities«: contains utility commands supported by the IMiS®/Client.
- »About«: shows a dialog box with information about the client.

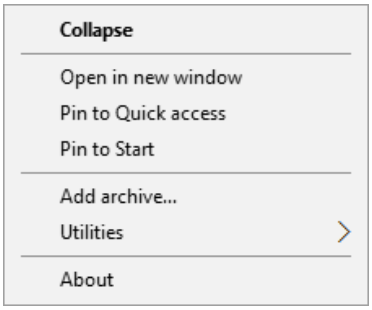


Image 50: Popup menu over the »Archives« folder

The popup menu over a selected archive in the left view (under the »Archives« folder) looks different from the one in the top right view of the Windows Explorer depending on whether the user is logged into the archive or not.
Prior to logging into a selected archive, the popup menu shows the following IMiS®/Client commands:

- »Log in«: opens a dialog box for logging into the selected archive.
- »Preferences«: a dialog box for IP address settings is displayed, where the user can view and configure the selected archive.

2018 © Imaging Systems, Inc., All rights reserved.

- »Configure«: a dialog box is displayed, where the user can log in to the configuration of the selected archive.
- »Remove archive«: removes the selected archive from the list of archives under the »Archives« folder.

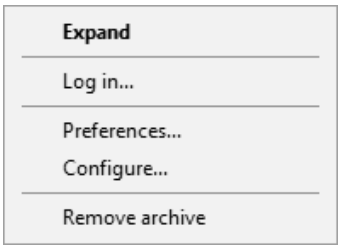


Image 51: Popup menu over the selected archive prior to login

After the user has logged in, the »Log out« command is displayed in the pop-up menu above the archive instead of the »Log in« command, where the user can log out from the selected archive. The pop-up menu is expanded with the following commands and sub-menus:

- »Reports«: contains report commands for the selected archive:
  - »Audit log«: provides access to audit logs throughout the archive.
  - »Folders«: creates a report on all the folders in the archive.
  - »Documents«: creates a report on all the documents in the archive.
  - »Contents«: creates a report on all the content of the documents of the archive.
  - »Retention«: creates a report on retention periods and disposition holds for all classes, folders and documents with specified retention periods or disposition holds.
  - »Access«: creates a report on the permissions of the selected archive user for all the classes, folders and documents of the archive.

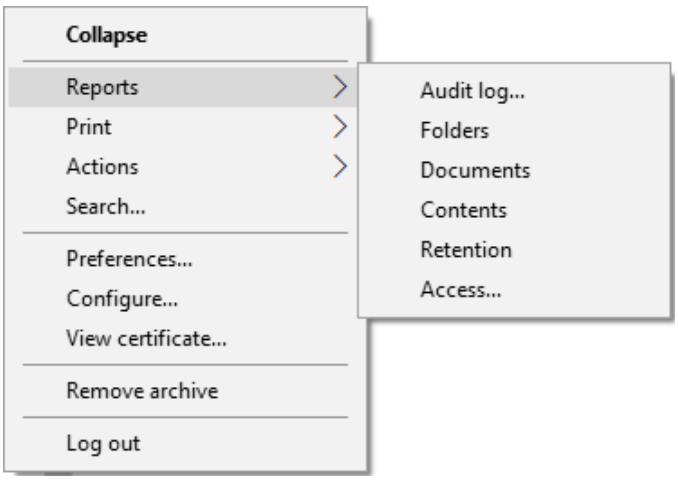


Image 52: Popup menu over the selected archive when choosing the »Reports« command

2018 © Imaging Systems, Inc., All rights reserved.

- »Print«: contains print commands for the selected archive:
  - »Classification scheme«: prints out the classes of the entire archive via the print preview mode.
  - »Classification scheme with folders«: prints out the classes of the entire archive and their folders via the print preview mode.

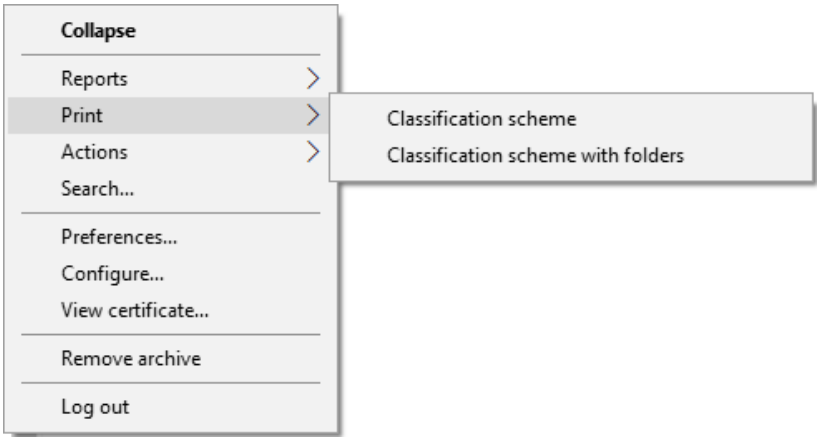


Image 53: Popup menu over the selected archive when choosing »Print«

- »Actions«: contains commands for operations on the selected archive:
  - »Import«: imports entities to the archive.
  - »Export«: exports entities from the archive.

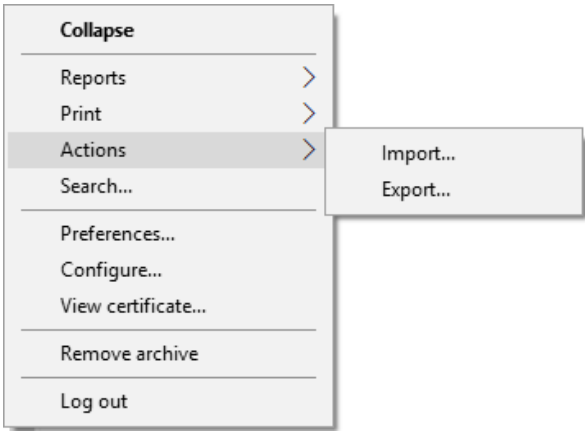


Image 54: Popup menu over the selected archive when choosing »Actions«

- »Search«: allows users to search by entity metadata and search the full text of entities on the entire archive.

2018 © Imaging Systems, Inc., All rights reserved.

The popup menu over a selected entity shows the following sub-menus and commands:

- »Reports«: contains the following report commands for the selected entity:
  - »Audit log«: depending on the user's selection, allows access to the audit log of the selected entity, or audit logs throughout the server.
  - »Folders«: creates a report on all folders contained by the selected entity.
    This command is only available for a class or folder.
  - »Documents«: creates a report on all the documents contained by the selected entity.
    This command is only available for a class or folder.
  - »Contents«: creates a report on the content of the selected entity. This command is only available for a class or folder.
  - »Retention«: creates a report on retention periods and disposition holds for all entities with specified retention periods or disposition holds under the selected entity.
  - »Access«: creates a report on the access permissions of the selected user, or all the users, for all the classes, folders and documents of the archive. This command is only available for a class or folder.

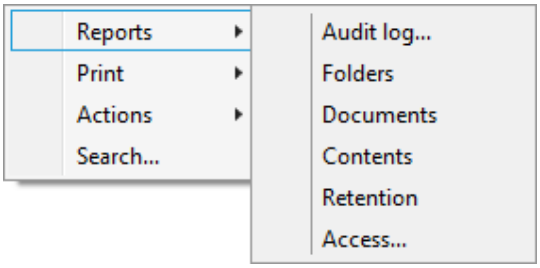


Image 55: Popup menu over the selected entity when choosing »Reports«

- »Print«: contains the following print commands for the selected entity:
  - »Class«: prints data about the selected class.
    This command is only available for classes.
  - »Folder«: prints data about the selected folder.
    This command is only available for folders.
  - »Document«: prints data about the selected document.
    This command is only available for documents.
  - »Classification scheme«: prints the classes of the archive via the print preview mode.
    This command is only available for classes.
  - »Classification scheme with folders«: prints the classes of the archive and all their folders via the print preview mode. This command is only available for classes.

2018 © Imaging Systems, Inc., All rights reserved.

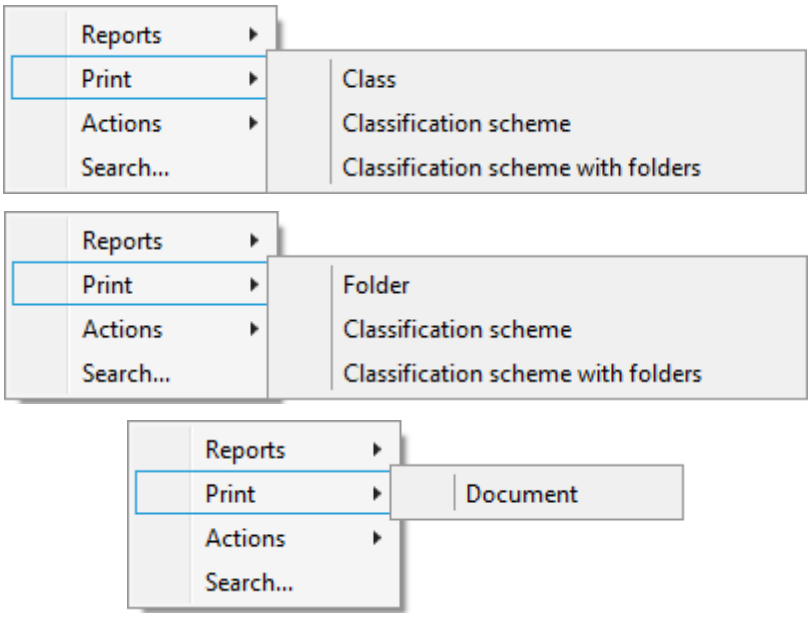


Image 56: Popup menu over the selected entity (class, folder, document) when choosing »Print«

- »Actions«: contains commands for various operations on the selected archive:
  - »Status«: enables you to change the status of the selected entity.
  - »Security class«: enables you to change the security class of the selected entity.
  - »Authenticity evidence«: enables you to retrieve authenticity evidence for the selected entity.
  - »Move«: enables you to move the selected entity within the classification scheme of the archive.
  - »Import«: enables you to import entities to the archive.
  - »Export«: enables you to export entities from the archive.

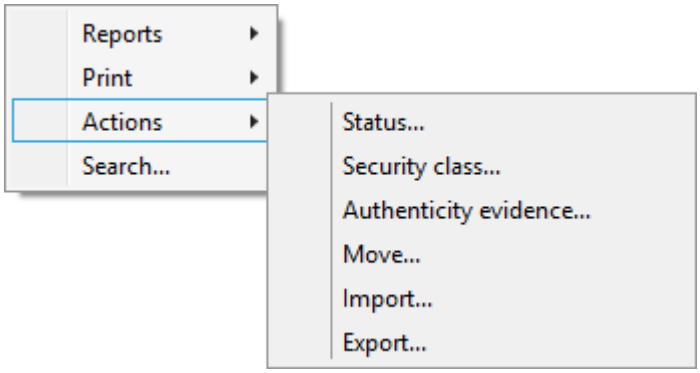


Image 57: Popup menu over the selected entity when choosing »Actions«

2018 © Imaging Systems, Inc., All rights reserved.

- »Search«: enables search by entity metadata and search the full text of content under the selected entity.

The popup menu over a line of displayed attributes in the list of contained entities (top right view of Windows Explorer) offers the following commands:

- »Size column to fit«: fits the width of the column to the data of the contained entities.
- »Size all columns to fit«: fits the width of all columns to the data of the contained entities.

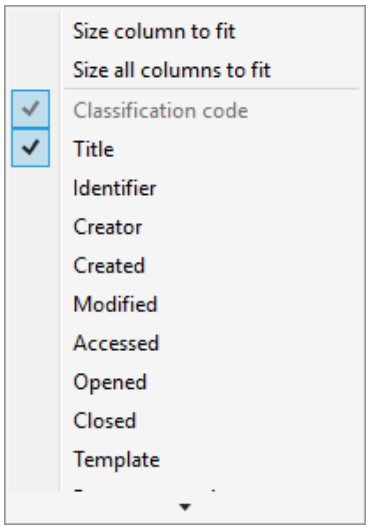


Image 58: Popup menu over a line of displayed attributes

4.2 Actions

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

- User login and logout from the archive.
- Capture and classification of records on the archive.
- Content management.
- Bulk capture of records.
- Conversion of content into long-term storage type.
- Access to records on the archive.
- Search by metadata and search full text of archived records.
- Versioning of records.
- Archiving of email messages.
- Management of physical records metadata.
- Printing of entity metadata, content and reports.

2018 © Imaging Systems, Inc., All rights reserved.

- Import, export and transfer of archived records.
- Editing, moving and deleting of records.
- Status changes.
- Security class changes.
- Authenticity evidence retrieval.
- Audit log viewing.

4.2.1 Login and logout

Users log into an IMiS®/ARChive Server by selecting the desired archive in the »Archives« virtual folder, which is found in the left view of the IMiS®/Client.

Login to an archive is done by using the »Log in« command in the:

- Popup menu over the selected archive in the left view (the classification scheme).
- Popup menu over the selected archive in the top right view (the list of archives).
- Command bar of the Windows Explorer for the selected archive.

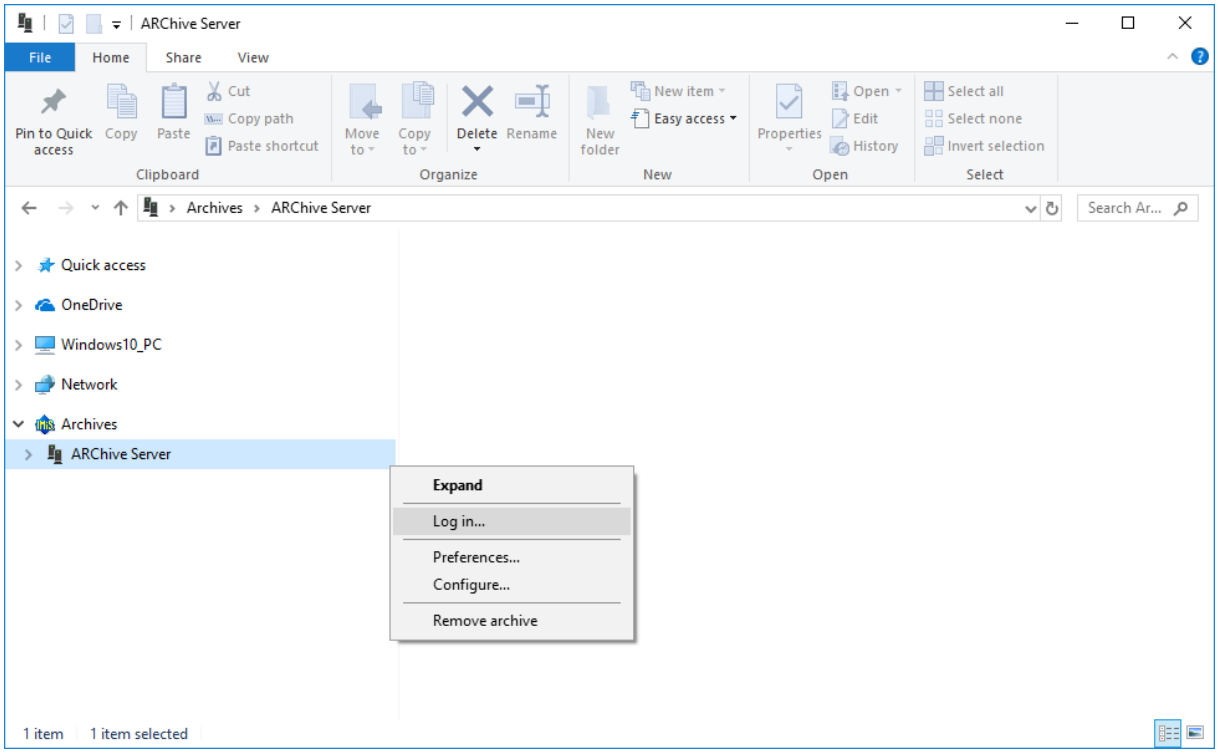


Image 59: Login into the selected archive via the popup menu

When logging in, users enter their username into the »Username« field and their password into the »Password« field. Login is confirmed by clicking »Log in« and canceled by clicking »Cancel«.

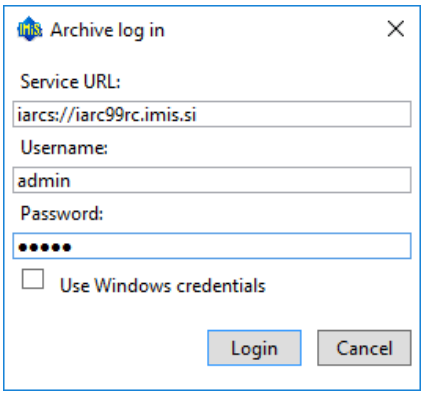


Image 60: Archive login dialog box

Logout from the archive is done by using the »Log out« command in the popup menu or command bar of the selected archive.
By selecting »Use Windows credentials« the user enables Single Sign-on (SSO) authentication mode. In the field »Username« a username is shown in SSO form that is selected in the server settings. For more information see chapter Setting an IMiS®/ARChive Server. The user does not need to enter a password in the »Password« field. As before, confirm registration by clicking »Log in« and revoke it using the »Cancel« button.

If a user is establishing a protected connection with the archive a dialog box »Security Warning« is shown. The user can view, use and set a remote certificate to protect the traffic between the server and client.

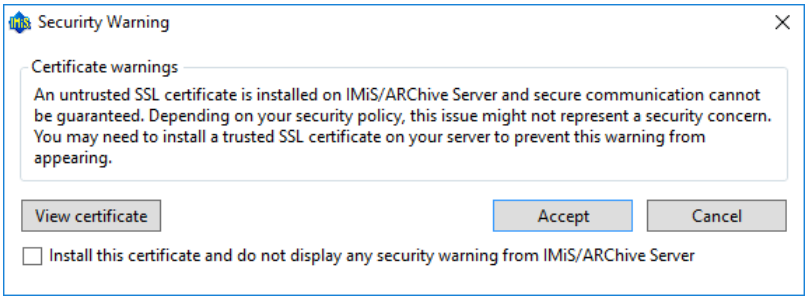


Image 61: A dialog box to confirm a remote certificate

2018 © Imaging Systems, Inc., All rights reserved.

User views the digital certificate by selecting the »View certificate« button. A digital certificate is used by selecting the »Accept« button. If the user does not confirm the digital certificate by selecting the »Cancel« button, a protected connection with the archive is not established.

By selecting »Install this certificate and do not display any security warning from IMiS®/ARChive Server«, the user saves the thumbprint of the digital certificate by selecting the »Accept« button. Every time a protected connection with the archive is established IMiS®/Client verifies the presence of the remote certificate's thumbprint.
If it does not find it, this dialog box is not shown.

If the user has previously installed the archive's digital certificate which has since then been changed or its thumbprint has been changed, a notification about the previous installation of the digital certificate is shown. By selecting the »Yes« button, a new thumbprint is used instead of the old one. By selecting the »No« button, the old thumbprint remains in use, and the protected connection is not established.

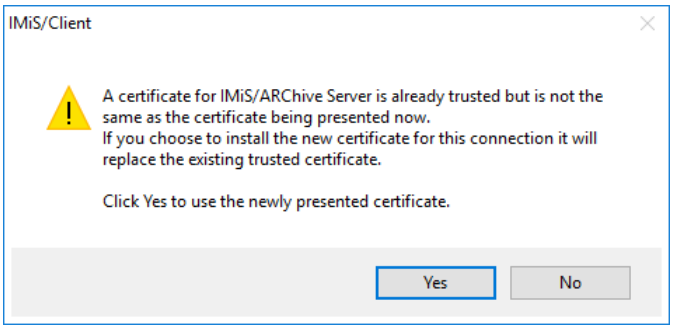


Image 62: Warning about a previous installation of the remote certificate

If the archive requests a »local certificate« to establish a protected connection, a system dialog box »Windows Security« is shown. The user can either select an appropriate local certificate by selecting the »OK« button or cancel the local certificate selection by selecting the »Cancel« button. In the latter case, a protected connection is not established.

2018 © Imaging Systems, Inc., All rights reserved.

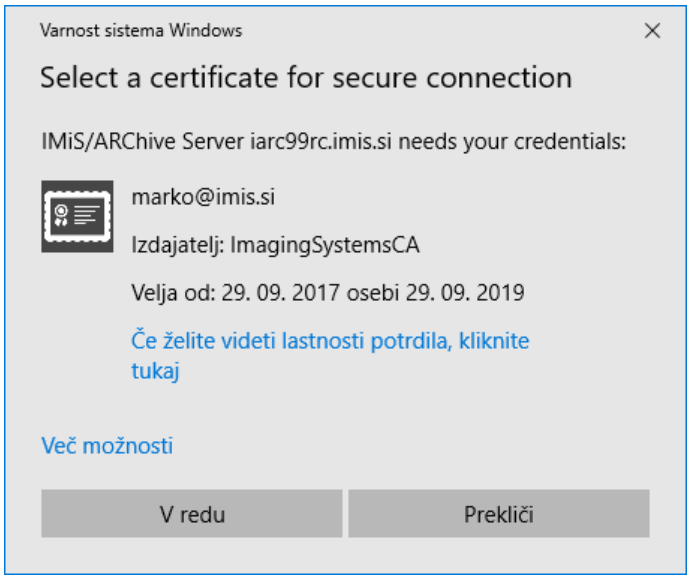


Image 63: A dialog box for selecting a local certificate

After a successful login, the user is displayed a list of classes at the root level in the classification plan of the selected archive material to which they have access rights.

This prevents access to the IMiS®/ARChive Server.

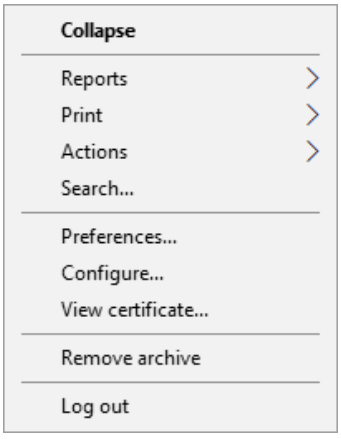


Image 64: Logging out of the selected archive via the popup menu

Note: On one computer, the IMiS®/Client does not allow simultaneous login to the selected archive for more than one user. If another user wishes to log in from the same computer, the previous user has to log out.

2018 © Imaging Systems, Inc., All rights reserved.

4.2.2 Document capture

Capture of documents in the IMiS®/Client is available to users that have the »Create entities« access right on the selected class or folder. This right allows the user to add new entities (sub-entities) to the selected entity.

For faster capture and sorting of content to its place in the classification scheme, it is advised that users separate / organize documents according to their type prior to import.
This is done by sorting the documents into appropriate »Templates« in the classification scheme.

Each template has its own predefined attributes, which are set by the administrator within the framework of the IMiS®/ARChive Server settings. User must input all the required attributes before saving the document.

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

In addition to entering metadata, the user can also attach a various content to the document. The IMiS®/Client 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).*
- *...*

2018 © Imaging Systems, Inc., All rights reserved.

Tip: If a user receives an error message when trying to save the content (Error: File <file path> cannot be attached to content), it should contact the administrator.
The administrator is advised to check if the type of file is included in the list of registered content types (MIME type) on the IMiS®/ARChive Server.

4.2.2.1 Capturing procedure

Select an archive server in the left view of Windows Explorer. In the server's classification scheme, select the class where the new document or folder should be stored. When you select a class, the right view displays the list of already contained documents or folders.

If you have the »Create entities« access right, you can add new entities by selecting the command »New« in the top command bar.
To check the effective access rights of the user on he selected entity see chapter Interface description and The »Security« tab.

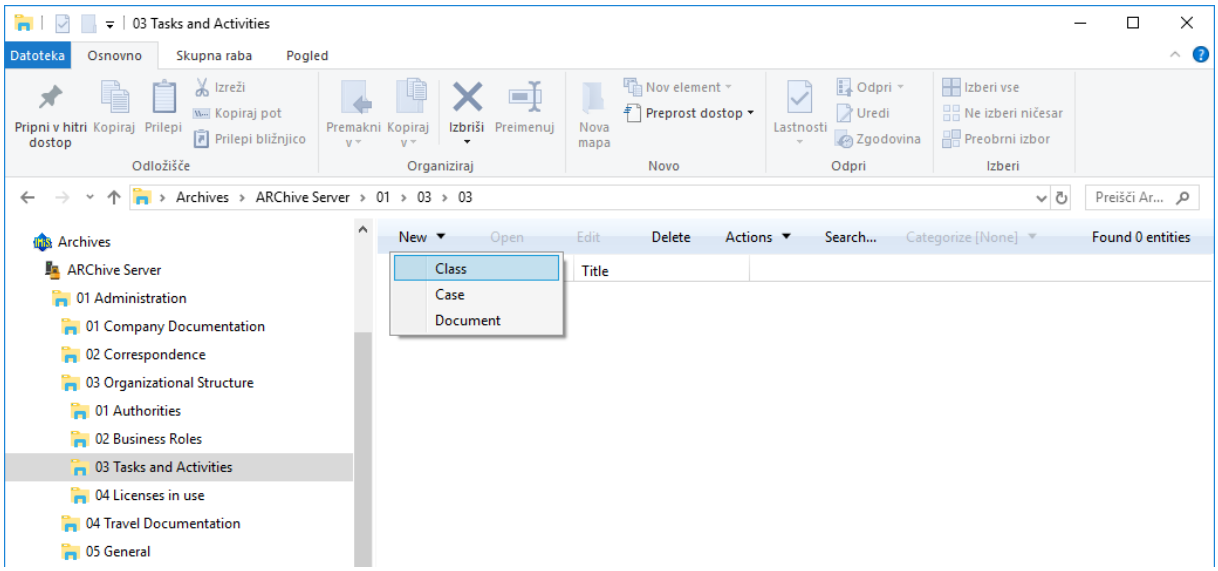


Image 65: Creating a new entity using the command bar

When a class is selected, the command »New« in the Explorer's command bar is used to open a popup menu that lists all the available templates for creating entities and sorting them into the selected class or folder. When a template is selected, the bottom right view (entity information) shows the tabs of the new document or folder.

2018 © Imaging Systems, Inc., All rights reserved.

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.*

4.2.2.2 Entry of metadata

Select the »Attributes« tab in the bottom right view (entity information). This tab lists all the attributes of the document or folder that can be entered by the user.

Each attribute selected from the list will display a longer description in the status bar of the tab. Attributes which are marked (the name of the attribute has a red dot at the end) are required (mandatory). These must be entered before the document can be saved.

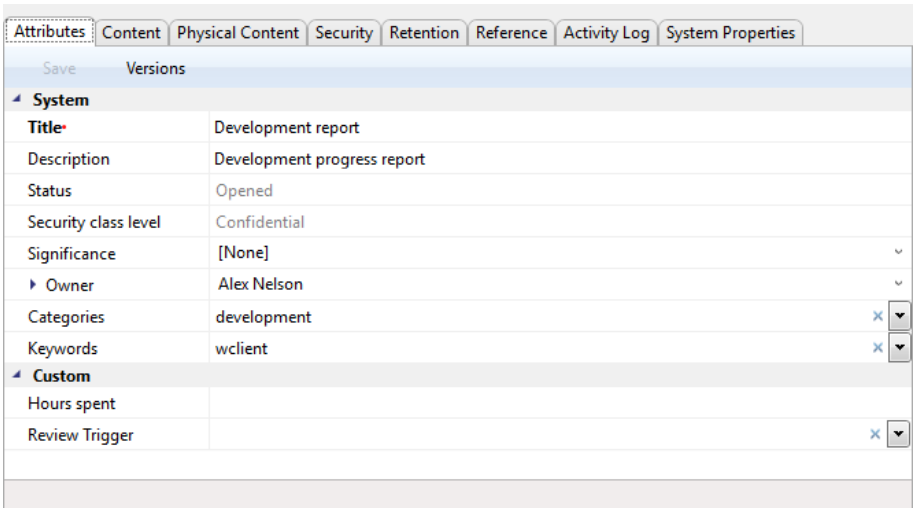


Image 66: Entry of required metadata

The list of attributes is divided into several categories:

- »System« attributes: these are present for all entities.
  For more information see chapter General system attributes.
- »Email« attributes: these are present when you select a template that contains email attributes. For more information see chapter Email attributes.
- »Custom« attributes: these are specified by the choice of the selected template and depend on the administrator's configuration of the classification scheme for the server.

2018 © Imaging Systems, Inc., All rights reserved.

Attribute entry fields are as follows:

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

Image 67: Entry of text metadata

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

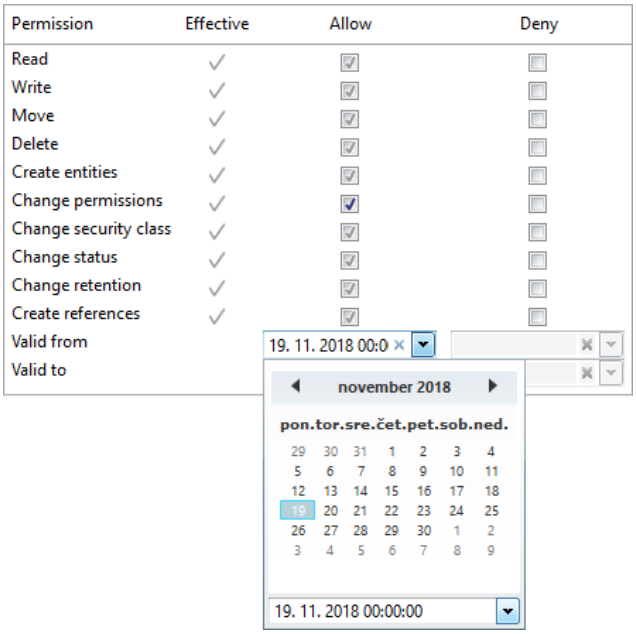


Image 68: Entry of date and time metadata

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

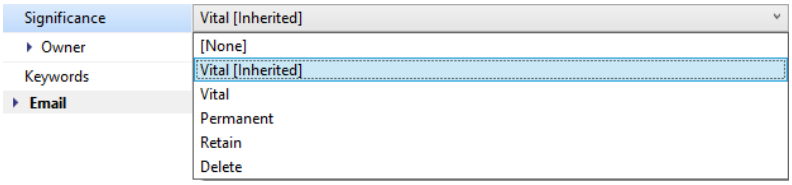


Image 69: Entry of metadata with predefined values

- A multiple value field where the user inputs any desired text values, separated by using the »Enter« key. In the multiple value display field, the individual values are separated by a semicolon mark (;).

2018 © Imaging Systems, Inc., All rights reserved.

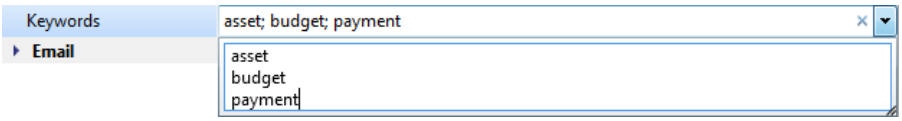


Image 70: Entry of multiple value metadata

Tip: The user can also input values in the display field, by using the semicolon mark. It is cleaner and more advisable, though, to enter them via the entry field.

When all the required and optional metadata has been entered, the user may continue to add content files via the »Content« tab.

4.2.2.3 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. This type is selected in the »System Properties« tab. 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«: where classification codes of child entities are generated automatically by the IMiS®/ARChive Server. These classification codes appear as successive numbers, with each new child entity increasing the number by one.
- »Manual«: where classification codes of child entities (class or folder) must be entered manually. This classification code may be any combination of letters and numbers, providing it is unique inside the entire parent class or folder.

Warning: In the manual entry of classification codes, the character »^« is invalid

2018 © Imaging Systems, Inc., All rights reserved.

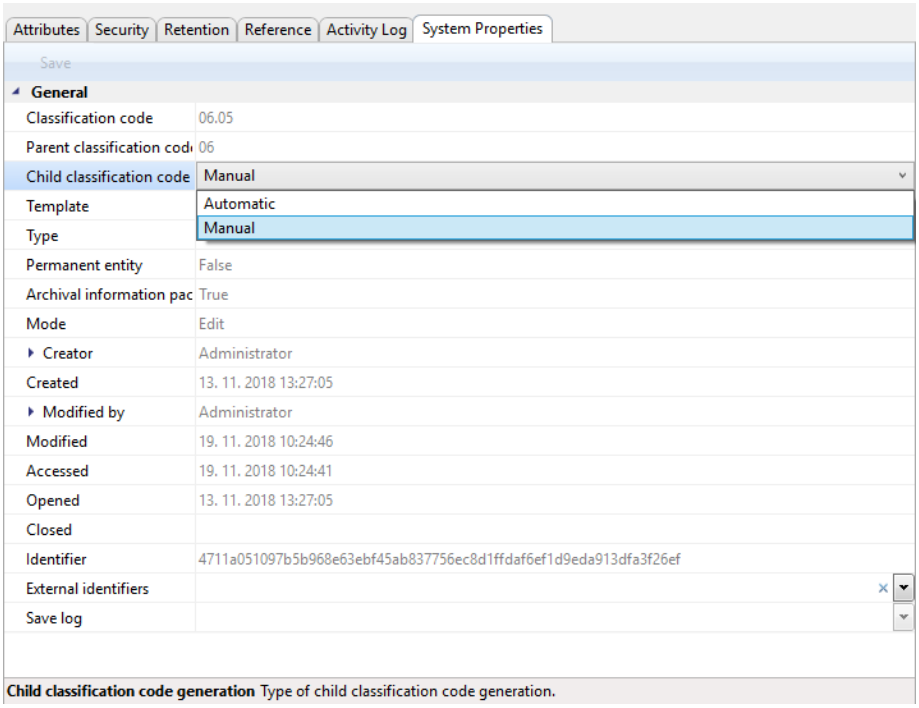


Image 71: Display of the type of child classification code generation

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

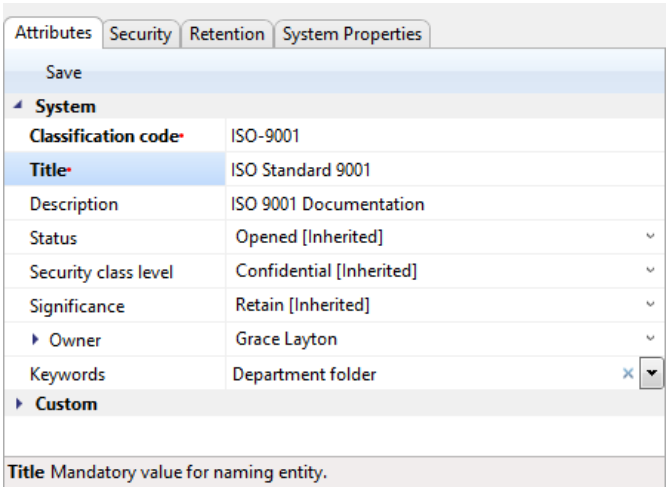


Image 72: Display of the entry of a child entity's classification code

Example: Inside a class with the classification code »06.05«, the user creates a new folder for which user manually input »ISO-9001« as the relative part of the classification code. When the folder is saved to the IMiS®/ARChive Server, its full classification code will be »06.05-ISO-9001«.

2018 © Imaging Systems, Inc., All rights reserved.

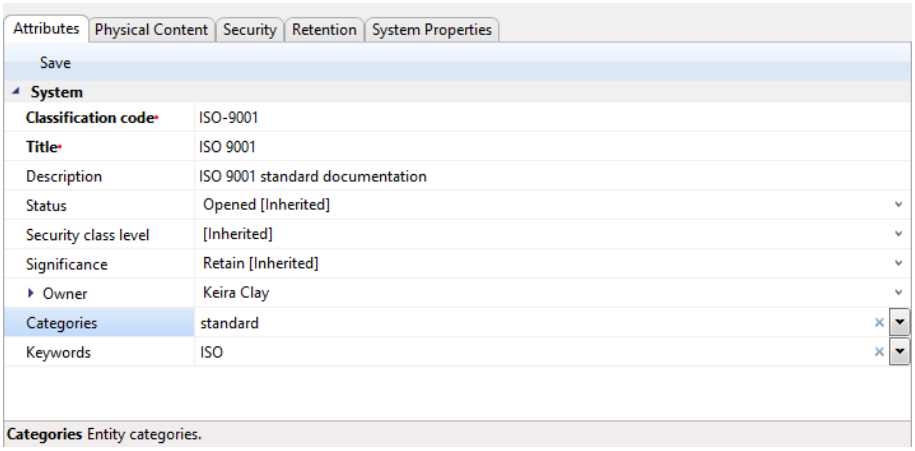


Image 73: Display of manually entered classification code of the child folder

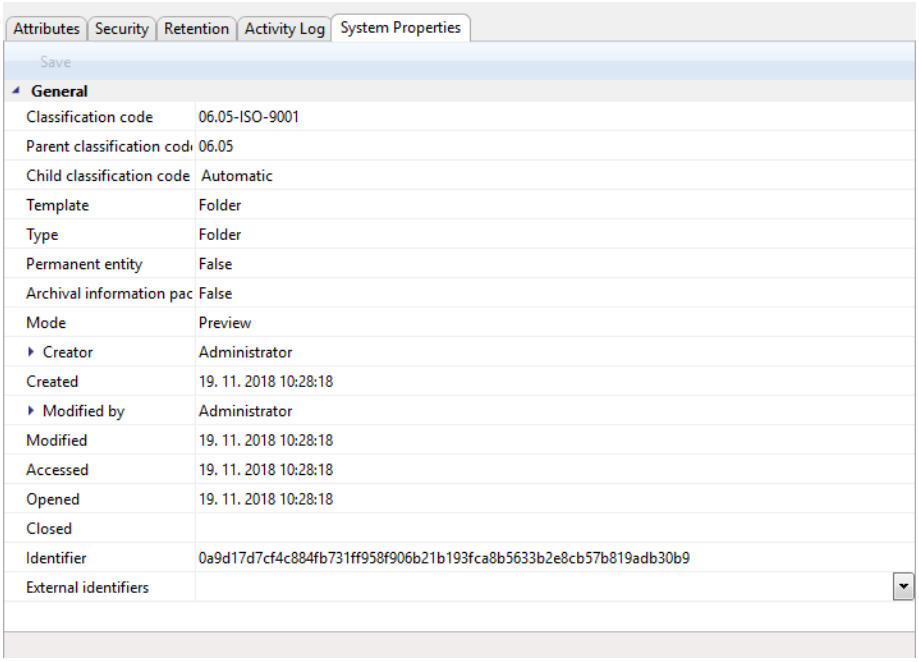


Image 74: Display of a folder with a manually entered classification code

Note: For the contained entity the user can select a random method of assigning the classification code (manually or automatically), independent of the method of assigning the classification code to the parent entity.

2018 © Imaging Systems, Inc., All rights reserved.

4.2.2.4 Setting an entity's security class

A user with the access rights can set the »Security class« of new entities.

This setting hides entities from users whose security class level is not high enough to access them. Security classes are predefined, and range from lowest to highest as follows:

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

The pick list only displays values that are lower or equal to the clearance level of the user.

In addition to values lower or equal to the clearance level of the user, when at least one parent entity has a specified security class, the pick list also displays the inherited value, marked by the suffix [Inherited].

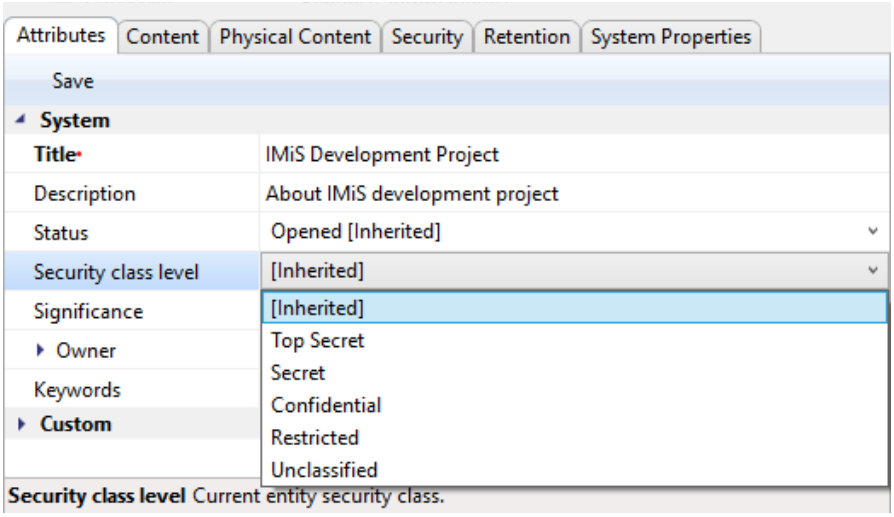


Image 75: Display of setting an entity's security class without inherited value

When a new entity has been saved, users can no longer modify the »Security class« metadata using the »Attributes« tab but only by using the »Security class« action, since a reason must be given in order to change a saved entity's security class. For more information see chapter Changing the security class.

4.2.2.5 Content capturing procedure

Select the »Content« tab in the bottom right view (entity information). This tab contains a list of content contained by the entity. If the entity is newly created, the list is empty.

Note: Content may only be attached to documents.

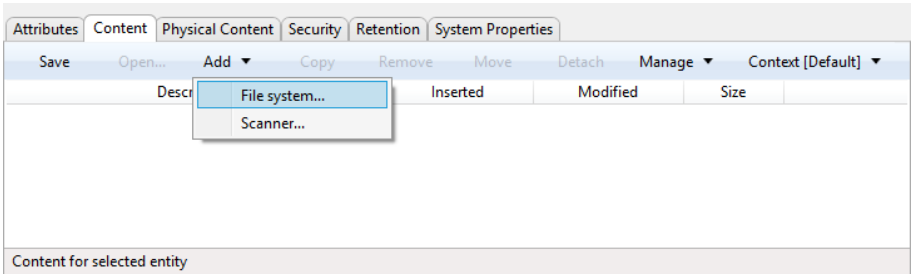


Image 76: Adding content using the file system

The user captures the content of documents in the following ways:

- Using the »File system« command, by selecting the specific content.
  Choose »Add...« in the command bar of the »Content« tab to open a popup menu with the »File system« command. This command opens the content selection dialog box.
  Find the desired file and select it. Choose »Open« to confirm your choice. This will start the transfer of the file to the IMiS®/ARChive Server. By choosing »Cancel«,
  you can cancel the capture of content. When the content has been transferred, it will appear on the list of inserted content, where its description has the same name as the captured content.
- Using the »Scanner« command, providing the IMiS®/Scan client is installed.
  Choose »Add...« in the command bar of the »Content« tab to open a popup menu with the »Scanner« command.

2018 © Imaging Systems, Inc., All rights reserved.

Selecting this command starts the IMiS®/Scan application and shows its main window. By selecting »Scan more pages« from the »Scan« menu, you begin the scanning procedure. When scanning is complete, the content is saved by choosing »Save and close« form the »File« menu. For more information on how to use the scanner client see the IMiS®/Scan Manual.

When the content is saved, the IMiS®/Scan window closes down and the procedure of transferring the content to the IMiS®/ARChive Server begins. When transfer is complete, the captured content appears on the list of inserted files. Its starting description automatically becomes »New document«, with the file extension corresponding to the type of scanned document (TIFF or PDF/A).

Troubleshooting: Most frequent issues when capturing content:

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

Note: When the content has been transferred, the new document isn't automatically saved. This means the content will not be contained in the document until you save it.

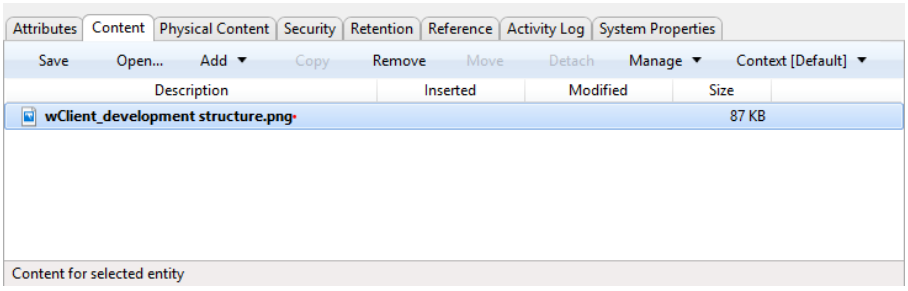


Image 77: Display of added content

All the new, currently unsaved content are marked in bold and have a red dot at the end. The attributes »Inserted« and »Modified« are empty because the content of document hasn't been saved to the IMiS®/ARChive Server yet.

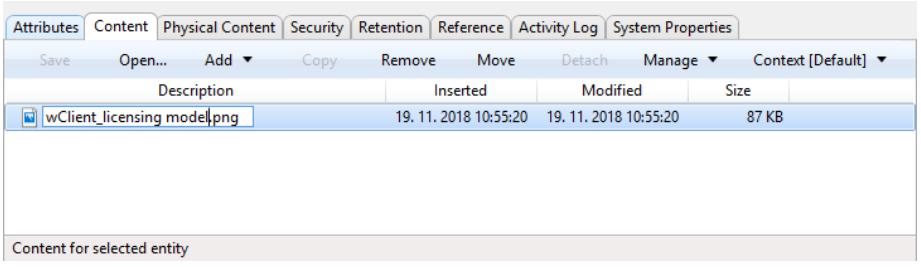


Image 78: Editing the new content's description by clicking on the description or pressing F2

2018 © Imaging Systems, Inc., All rights reserved.

The description of the content is changed by clicking its name on the list or pressing the »F2« key or via the popup menu by pressing the right mouse button. Write your description and press the »Enter« key to confirm it.

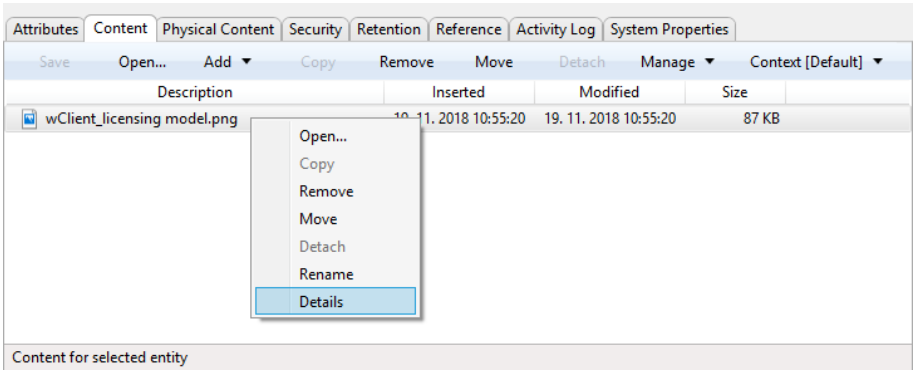


Image 79: Editing a description of selected content via the popup menu

When you are done capturing all the content, you can decide to save the entity (chapter Saving an entity) or proceed to enter data about the physical content.

4.2.2.6 Overviewing the content details

Details of the entity's content provide user with some information that is otherwise not displayed in the content list. The user accesses the information by right-clicking on the content in the popup menu, and then selecting the »Details« command.

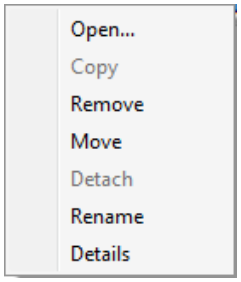


Image 80: Displaying the content's data selection

The following data on the entity's content is displayed in the right part of the content list:

- Content identifier.
- Content type.
- Content Description.
- Date and time when content was inserted.
- Date and time when content was modified.

2018 © Imaging Systems, Inc., All rights reserved.

- Date and time when content was accessed.
- Content size in kB.
- States whether the content was indexed.
- States whether the content was electronically signed.

Note: From the displayed data, the user can only modify the content description.

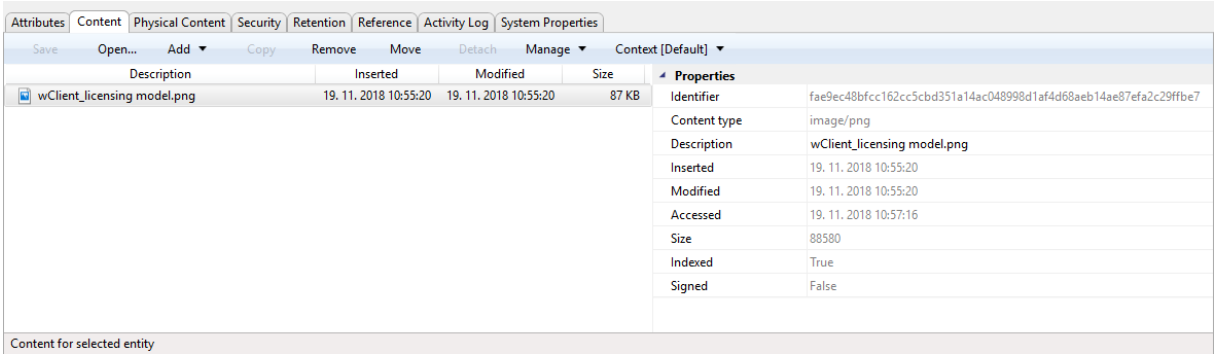


Image 81: Displaying content data

The user can open the content in the source program registered for this type of content (MIME type). In Open or Edit mode, the user begins by tagging the content.
In the bottom command bar, the user selects the command »Open« or opens it by double clicking on the content record.

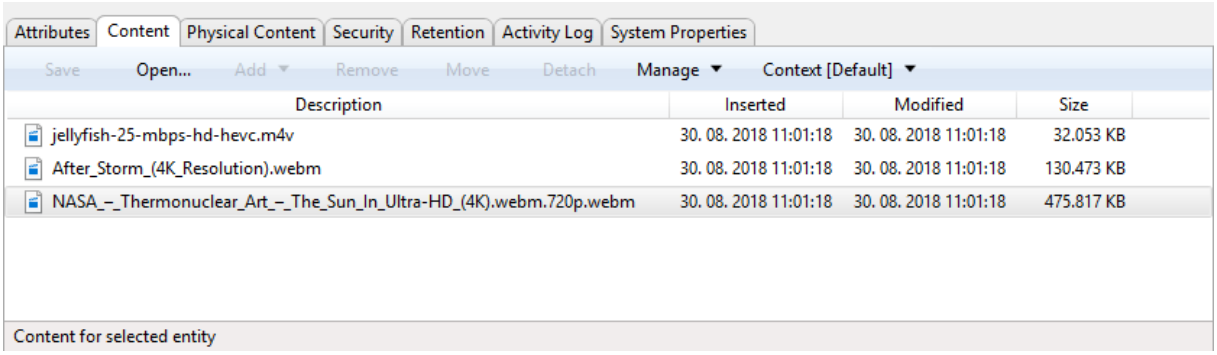


Image 82: Selecting the command »Open« to open content

2018 © Imaging Systems, Inc., All rights reserved.

Example: The user is enabled playing audio and video contents in streaming mode.

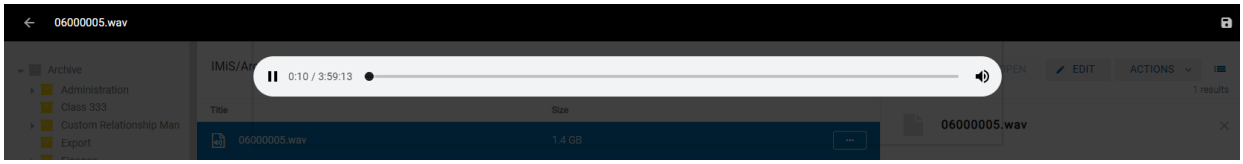


Image 83: Opening audio content (wav, ogg, mpeg)

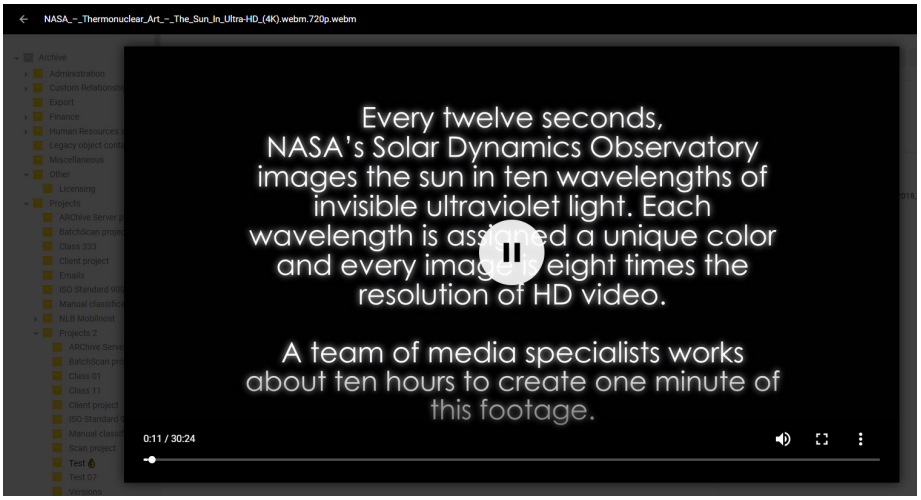


Image 84: Opening video content (mp4, webm, ogg)

4.2.2.7 Entry of physical content attribute values

Select the »Physical Content« tab in the bottom right view (entity information). This tab contains a list of all attributes that deal with the description of the physical content the entity corresponds to, or is based on. For more information see chapter Managing physical content metadata.

4.2.2.8 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. An effective retention period is required for implementation of the review process.

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

2018 © Imaging Systems, Inc., All rights reserved.

The adding of a retention period is started with the »Edit« command in the »Retention« tab.

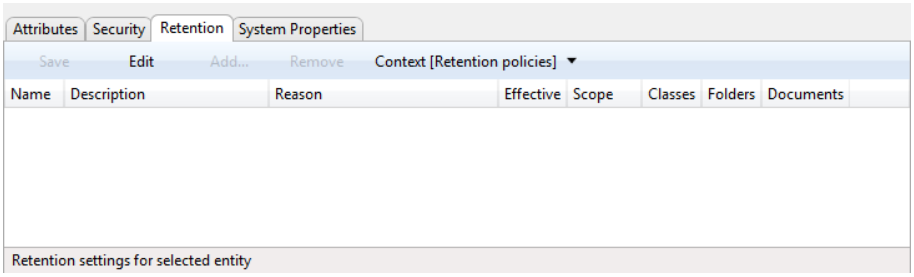


Image 85: Enables the editing of retention periods and disposition holds

By clicking on the »Add« command, the »Select retention policy« options window appears, containing a list of available retention periods. These are specified in the archive's configuration. For more information see chapter The »Retention« tab.

The user selects the retention period. The selection is confirmed by clicking on the »Add« button on the list of retention periods on the tab.

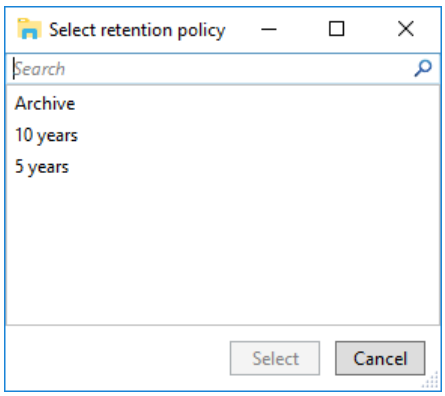


Image 86: Adding an explicit retention period

The following values can be set for the retention period:

- »Scope«: by selecting the »Allow« value, the retention period is allowed, and by selecting the »Deny« value, it is denied.
- »Classes«: a tick means that the retention period applies to the selected entity and to all of the contained classes.
- »Folders«: a tick means that the retention period applies to the selected folder and to all of the contained folders.
- »Documents«: a tick means that the retention period applies to all documents under the selected entity.

2018 © Imaging Systems, Inc., All rights reserved.

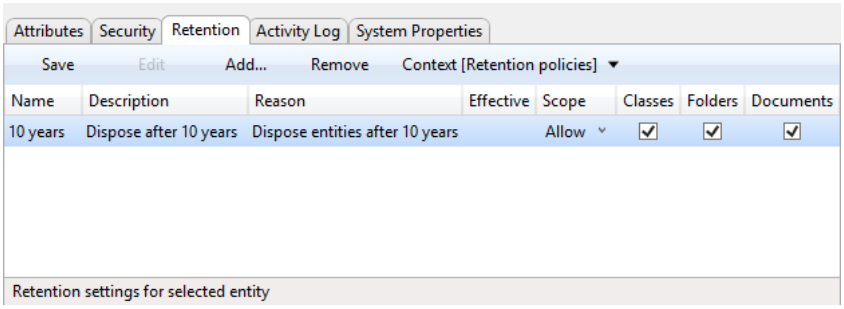


Image 87: Editing the settings of the explicit retention period

By clicking on the »Save« button, the user saves the retention period to the list in the tab.
If the saved retention period is effective, the entity can be saved. If not, the user must return to editing mode via the »Edit« command and reset the retention period.

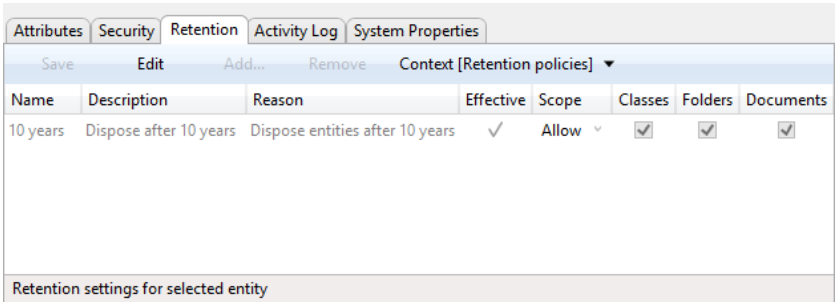


Image 88: A saved explicit retention period

4.2.2.9 Saving an entity

When the content has been captured and the required metadata entered, user must save the entity to the IMiS®/ARChive Server to archive it.

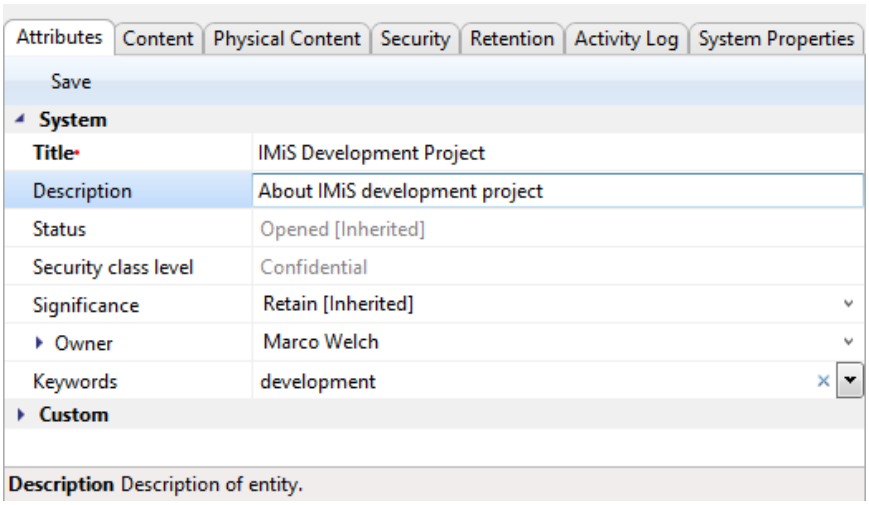


Image 89: Saving a new or modified entity

This is performed by using the »Save« command in command bar under the tabs.

This begins the transfer of all entered metadata to the server.

The content that have been captured will be inserted into the saved document.

Troubleshooting: Most frequent errors when saving:

- *The value of a mandatory attribute was not specified.*
- *The entered attribute value is not allowed.*

4.2.2.10 Saving entities with electronically signed content

If, when capturing content, the user adds an electronically signed content (PDF/A, TIFF, XML or EML file), the procedure of checking the electronic signatures of captured content will automatically start while saving the entity and its contents to the IMiS®/ARChive Server.

For more information see chapter Verifying the validity of electronic signatures.

4.2.2.11 Metadata records

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

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

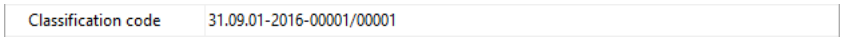


Image 90: Example classification code

- »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.

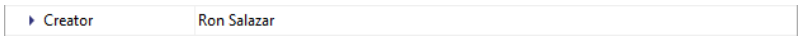


Image 91: Example creator of entity

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

Image 92: Example date and time an entity was opened

2018 © Imaging Systems, Inc., All rights reserved.

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

Image 93: Example date and time an entity was closed

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

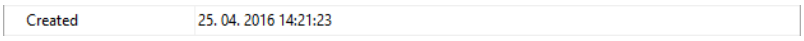


Image 94: Example date and time an entity was created

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

Image 95: Example date and time of last changes to the entity

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

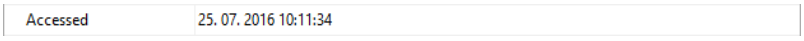


Image 96: Example date and time of last access to the entity

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

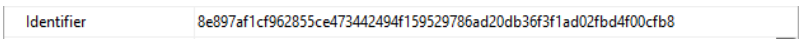


Image 97: Example entity identifier

- »External identifiers«: a list of the entity's unique external identifiers on the server.

Image 98: Example external identifiers of an entity

- »Save log«: contains a report on the verification of electronic signatures and digital certificates in the captured files.

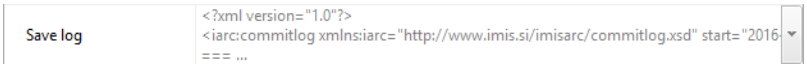


Image 99: Example save log of an entity

When entity content is being saved to the IMiS®/ARChive Server, the following metadata is automatically recorded into the entity:

- »Inserted«: date and time when the user saved a document to which a new content was attached (inserted). As long as the content exists on the document, this metadata does not change.

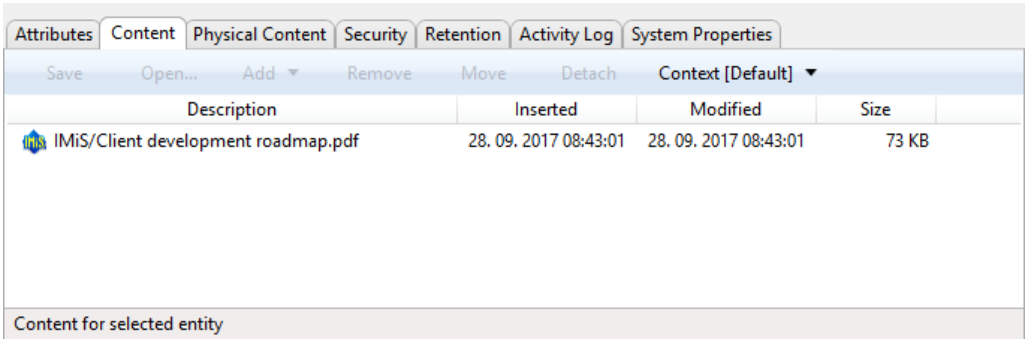


Image 100: Example date of content insertion

- »Modified«: date and time when the user changed the content of the document. This metadata changes every time a user changes an inserted content by using »Save« button.

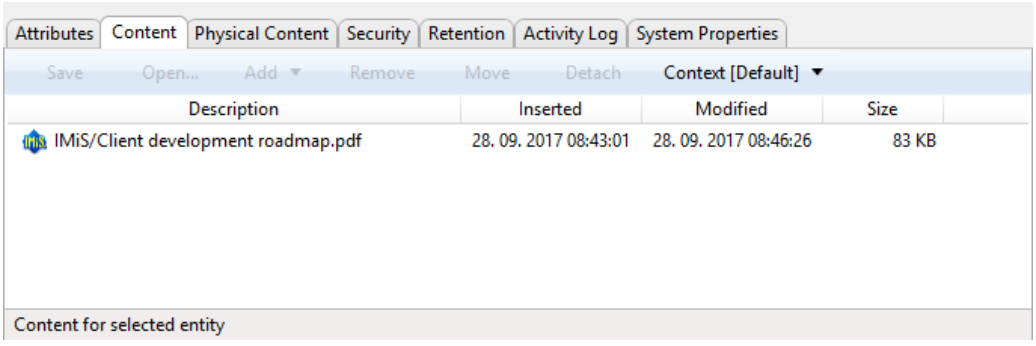


Image 101: Example date of content modification

2018 © Imaging Systems, Inc., All rights reserved.

4.2.3 Content management

Content management related to moving, copying and detaching entity content in the IMiS®/Client can be performed by any user with appropriate rights, independent of the »ContentManagement« role.

Content management related to tagging entity content for indexing and conversion in the IMiS®/Client can only be performed by a user with a »ContentManagement« role.

4.2.3.1 Moving content

Moving content from one entity to another can be performed by any user with the »Write« right. The user selects the content in the Edit mode. The »Move« button becomes enabled in the bottom command bar. By selecting the button, a dialog box for entering the classification code of the target entity is opened.

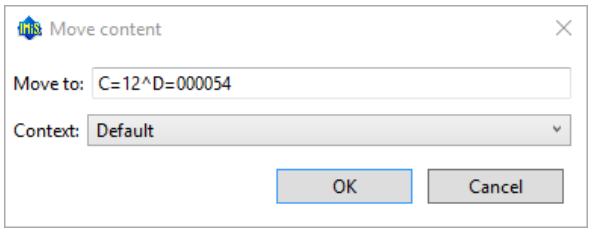


Image 102: Displaying a dialog box where classification code of the target entity is entered

By confirming the selection with the OK button, the content is temporarily removed from the content list. Content migration is not performed until after saving changes.

By selecting the »Context« button, the user can replace the system content container in the bottom command bar with any alternative container.

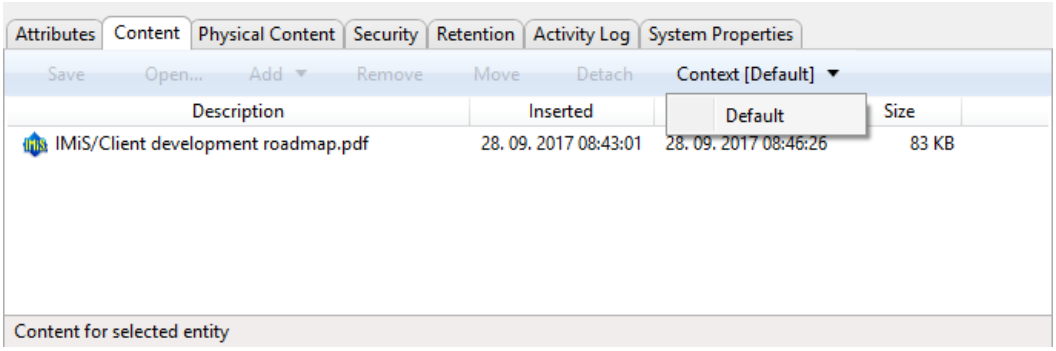


Image 103: Displaying the default content container

4.2.3.2 Copying content

The copying of content from one entity to another can be performed by any user with the »Write« permission. The user makes a copy of the content and copies it to another document-type entity.

In Open mode, the user selects the content. In the bottom command bar he selects the button »Copy«. A dialog box opens for entering the classification code of the target document.

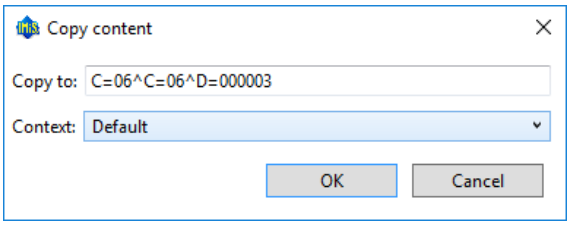


Image 104: Displaying the dialog box for entering the classification code of the target document

After confirming the selection by clicking »OK«, a copy of the content is saved to the selected document. The user is informed of saving a copy of the content.

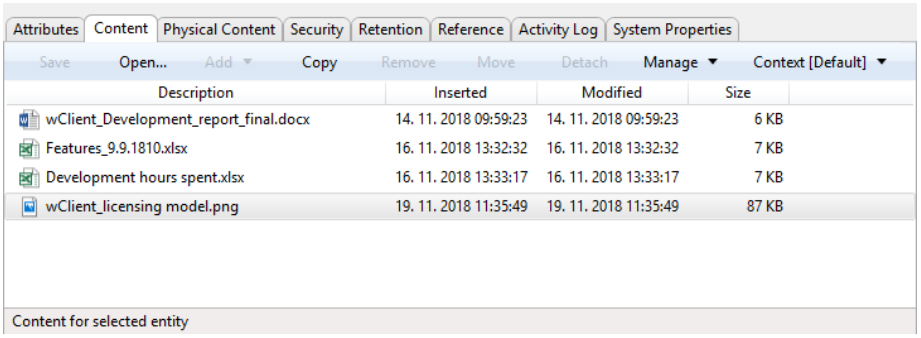


Image 105: Displaying the content copied to the target document

4.2.3.3 Detaching content

Detaching content included in a specific content can be performed by a user with the »Write« right. The user selects the content in the Edit mode.

In the bottom command bar, the user selects the »Detach« button.

2018 © Imaging Systems, Inc., All rights reserved.

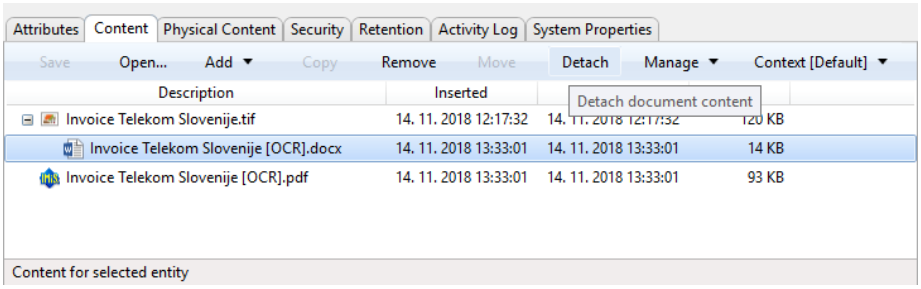


Image 106: Displaying the Detach content command

After the detachment, the original content is placed below the last content in the list.

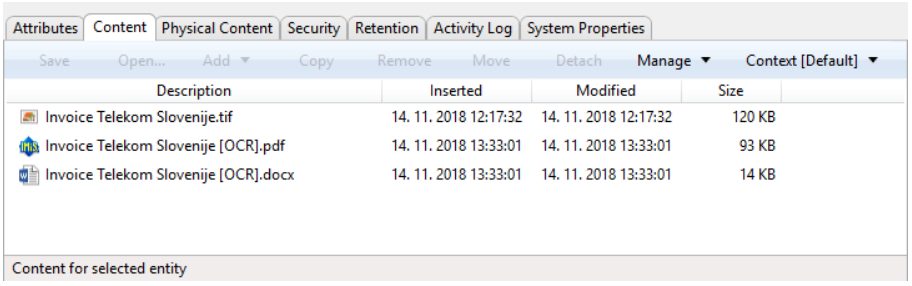


Image 107: Displaying detached content

4.2.3.4 Indexing content

Indexing content can be performed automatically with the appropriate settings on the IMiS®/ARChive Server or manually for individual content within the interval specified in the server settings. When manually tagging content for indexing, the user with the »ContentManagement« role selects the content in the Open mode.

In the bottom command bar, the user selects the »Manage« button and the »Queue for Index« command in the drop-down menu. The selected content is tagged for later indexing.

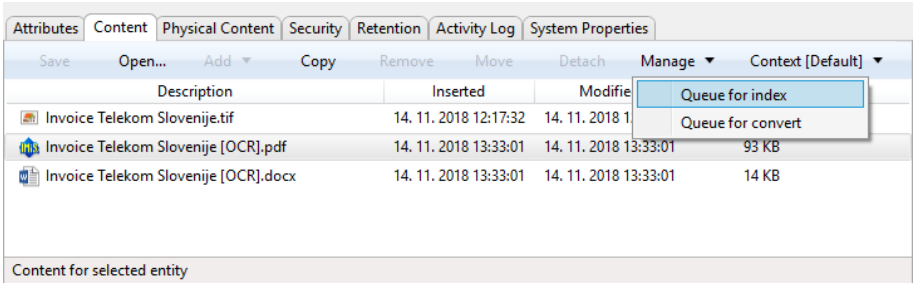


Image 108: Displaying the tagging content for indexing command

2018 © Imaging Systems, Inc., All rights reserved.

4.2.3.5 Content conversion

Content conversion can be performed automatically with the appropriate settings on the IMiS®/ARChive Server or manually for individual content within the interval specified in the server settings. When manually tagging content for conversion, the user with the »ContentManagement« role selects the content in the Open mode. In the bottom command bar, the user selects the »Manage« button and the »Queue for Convert« command in the drop-down menu. The selected content is tagged for later conversion.

For more information on content conversion see chapter Conversion.

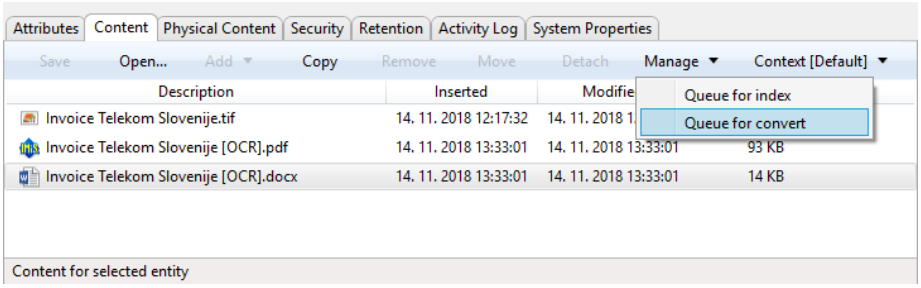


Image 109: Displaying the tagging content for conversion command

4.2.4 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®/Client 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.

4.2.5 Conversion

For the needs of long-term content storage, the user can convert all files on the document into a long-term storage type (PDF/A, TIFF, for example).

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.

The user can choose between two conversion modes:

- Capture and convert to a PDF/A file via a virtual printer.
- Automatically convert content to a long-term storage format (server setting).

2018 © Imaging Systems, Inc., All rights reserved.

4.2.5.1 Converting via a virtual printer

Using the IMiS®/Convert To PDF-A virtual printer application, all the original components of the content (pages of a document, for example) are captured via the virtual printer and converted into a PDF/A file format. The components of the content remain identical.

In addition to the original components, the new file also records the following metadata:

- Convert Date
- Convert Reason
- Convert Details
- Original Software name
- Convert Software name.

In the IMiS®/Client, the user must then manually import the converted file back into the document where it originated. The converted content and all the added metadata may be viewed using any external viewer used to open PDF/A files (Adobe Reader, for example).

4.2.5.1.1 Conversion procedure

In Windows Explorer, locate the document whose content you wish to convert.
Open the document in reading mode by selecting »Open« in the top command bar.
The tab »Content« will then appear.
Choose the content from the list. By double clicking the content or selecting »Open« in the bottom command bar, the content will be opened in the software currently registered for opening the content's type (MIME type).

Note: To open the file, the user must have appropriate software installed on the computer that can open the attachment's file type.

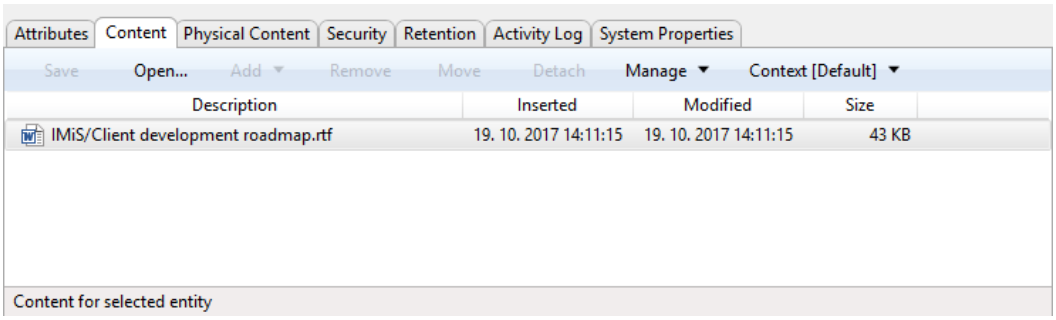


Image 110: Opening content of document in the conversion procedure

In the source software (Microsoft Word, for example), you can then convert the content using the virtual printer IMiS®/Convert To PDF-A. It is important to convert the complete content (all the pages of a document, for example).

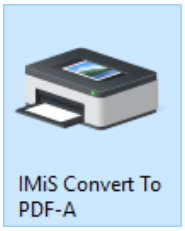


Image 111: Selecting the virtual printer »IMiS Convert To PDF-A«

Prior to beginning the conversion procedure, the user receives the »Convert Settings« dialog box.

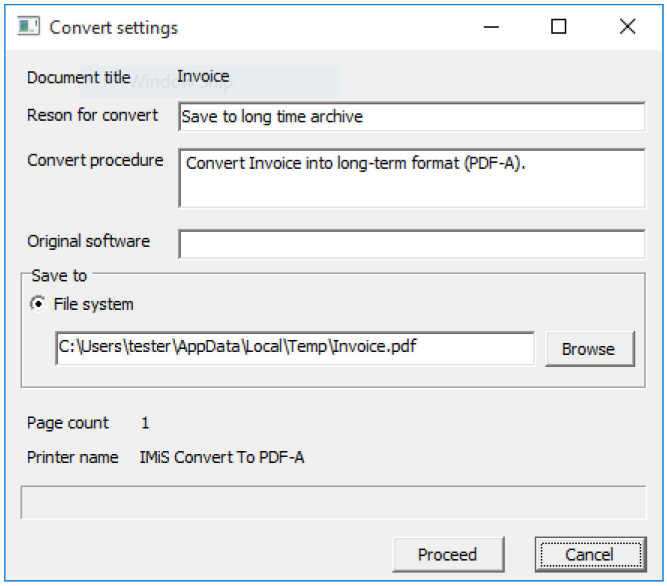


Image 112: Conversion settings via the dialog box

The dialog box requires the user to enter the following fields:

- »Original software« states the name of the original software (source software or current program using the virtual printer for conversion).
- »Reason to convert« states the reason for conversion.
- »Convert procedure« describes the conversion procedure.

2018 © Imaging Systems, Inc., All rights reserved.

The »Save to« section contains the default option of saving to the file system.
By choosing »Browse« you can freely select the desired location where you wish to save the converted file. To continue the conversion procedure, select »Proceed«. The conversion procedure may be cancelled at any time using the »Cancel« command. When conversion is complete, you have to manually import the resulting PDF/A file into the document where the original file is located. For more information see chapter Content capturing procedure.

4.2.5.1.2 Automatically converting content

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.

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. According to the IMiS®/ARChive Server settings, the name of the converted content can be complemented with information about the conversion, the number of converted content pages, the conversion date ...

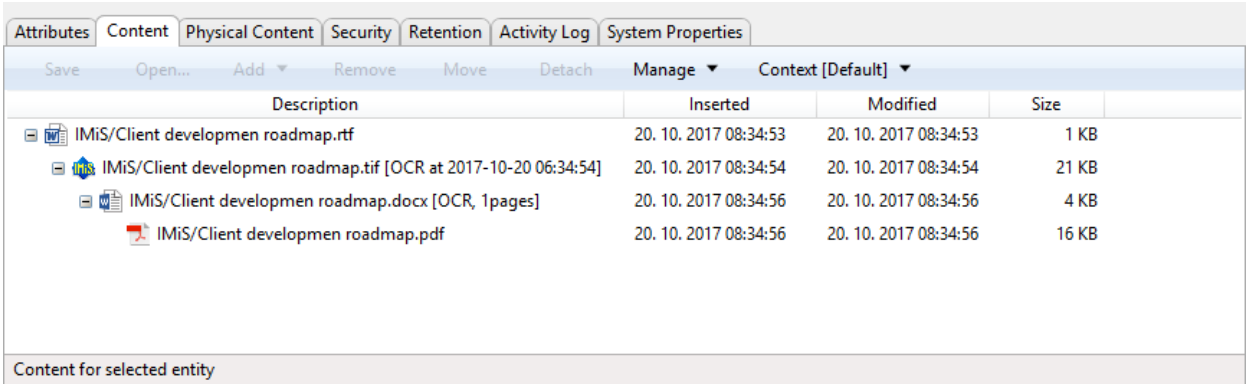


Image 113: Example of a content tree

Warning: Removal of the original content is only possible with prior removal of all the content interpretations. When removing content on individual levels, the entity must be saved.

4.2.6 Access

Access to entities in the classification scheme depends on the security class of the content, the user's clearance level, and the user's explicit permissions.

2018 © Imaging Systems, Inc., All rights reserved.

For more information on the security classes see chapter Access in the IMiS®/ARChive Server Manual. To learn how to change the security class of an entity see chapter Changing the security class.

When logging into the selected archive (chapter Login and logout), the user is authenticated by his username and password. The IMiS®/ARChive Server will display those root classes of the archive for which the logged user has the »Read« permission. The classes are shown in the »Archives« folder under the selected archive in the left view, and in the list of contained entities in the top right view of Windows Explorer.

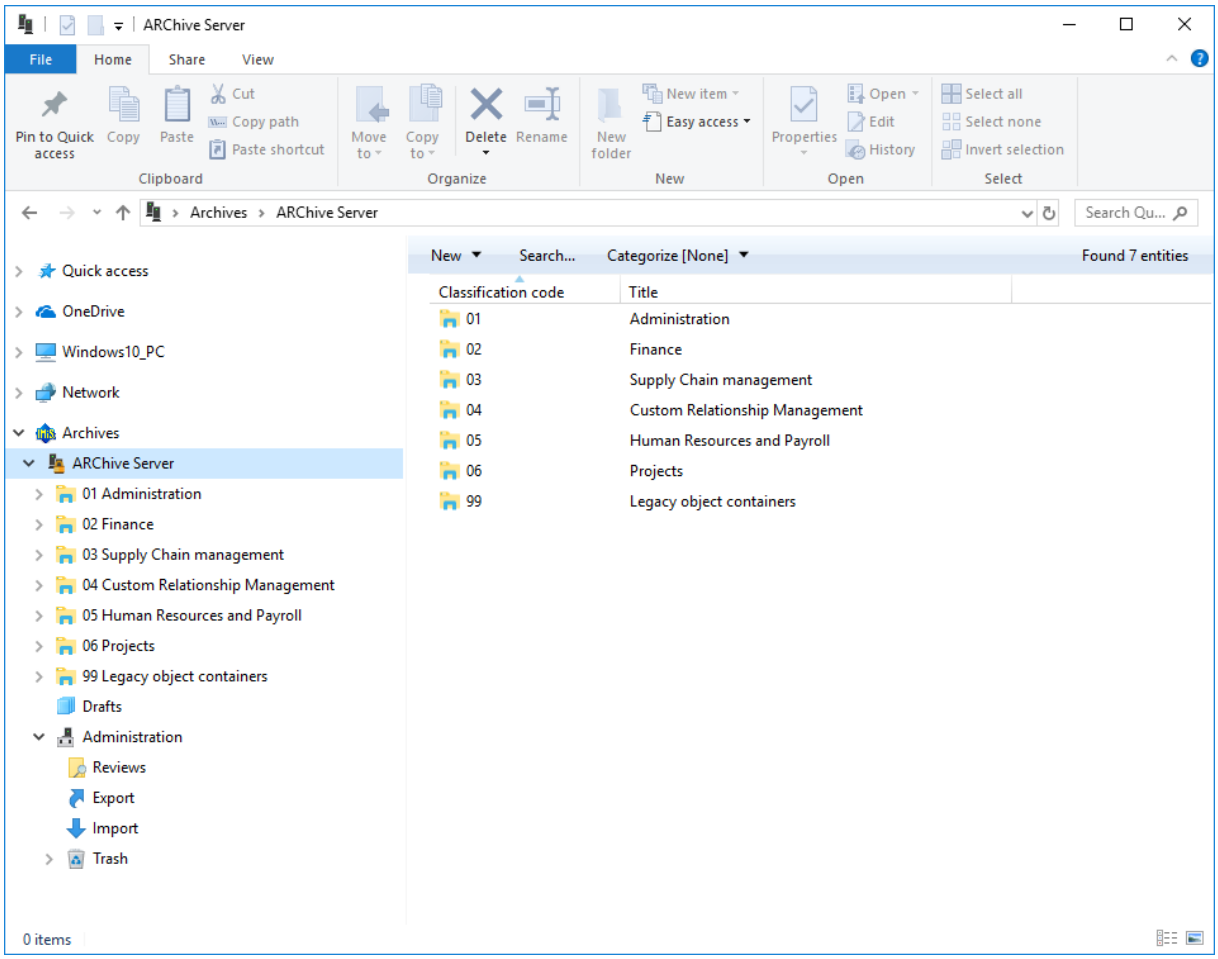


Image 114: Display of root classes when logging into the selected archive

When accessing data in the selected root class of the archive, in the bottom right view of Windows Explorer in the following tabs are displayed, showing only the publicly accessible data for the class:

- »Attributes«: contains a list of entity metadata.
- »Security«: displays the effective access rights of the user on the entity.

2018 © Imaging Systems, Inc., All rights reserved.

- »Activity log«: shows the audit trail of the entity. The tab is only visible to appropriately authorized users.
- »Reference«: contains connections to other entities in the classification scheme.
  This tab is shown only if at least one reference to another entity has been established in the classification scheme.
- »System properties«: contains a list of the entity's system properties.

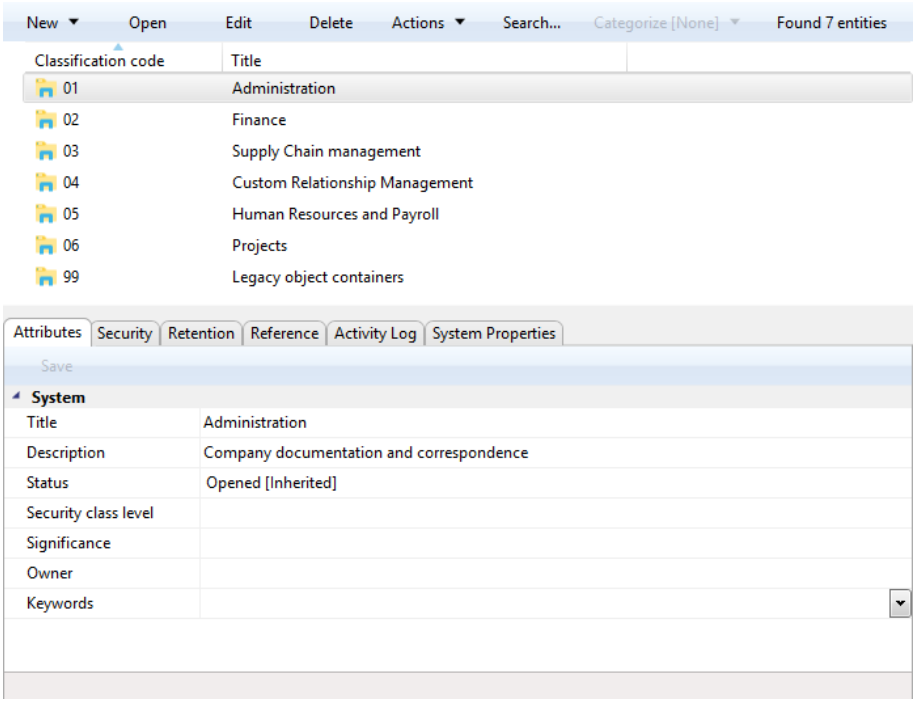


Image 115: Displaying the publicly accessible entity data in tabs

After choosing the »Open« command in the command bar above the list of entities, the server delivers all the data the current user is authorized to access. This also happens when user accesses entities contained in the root classes of the archive.

The tabs initially display only the publicly accessible entity information. Once the »Open« command has been chosen, the tabs then display all the information the current user is authorized to access. New data is either added to the existing tabs or appears under new tabs such as:

- »Content«: shows a list of the entity's content (files).
  This tab is only displayed for documents.
- »Physical Content«: shows a list of the entity's physical content metadata.
  This tab is only displayed for folders and documents.

2018 © Imaging Systems, Inc., All rights reserved.

When the user has the »Write« permission, user can also choose the »Edit« command in the command bar above the list of entities. In that case, the tabs display the same sets of data as when choosing the »Open« command. Data that is not specified as read-only on the server may then be edited and modified. For more information see chapter Editing entity data.
When editing is complete, changes to the entity are saved to the server using the »Save« command in the toolbar under the name of the tab.

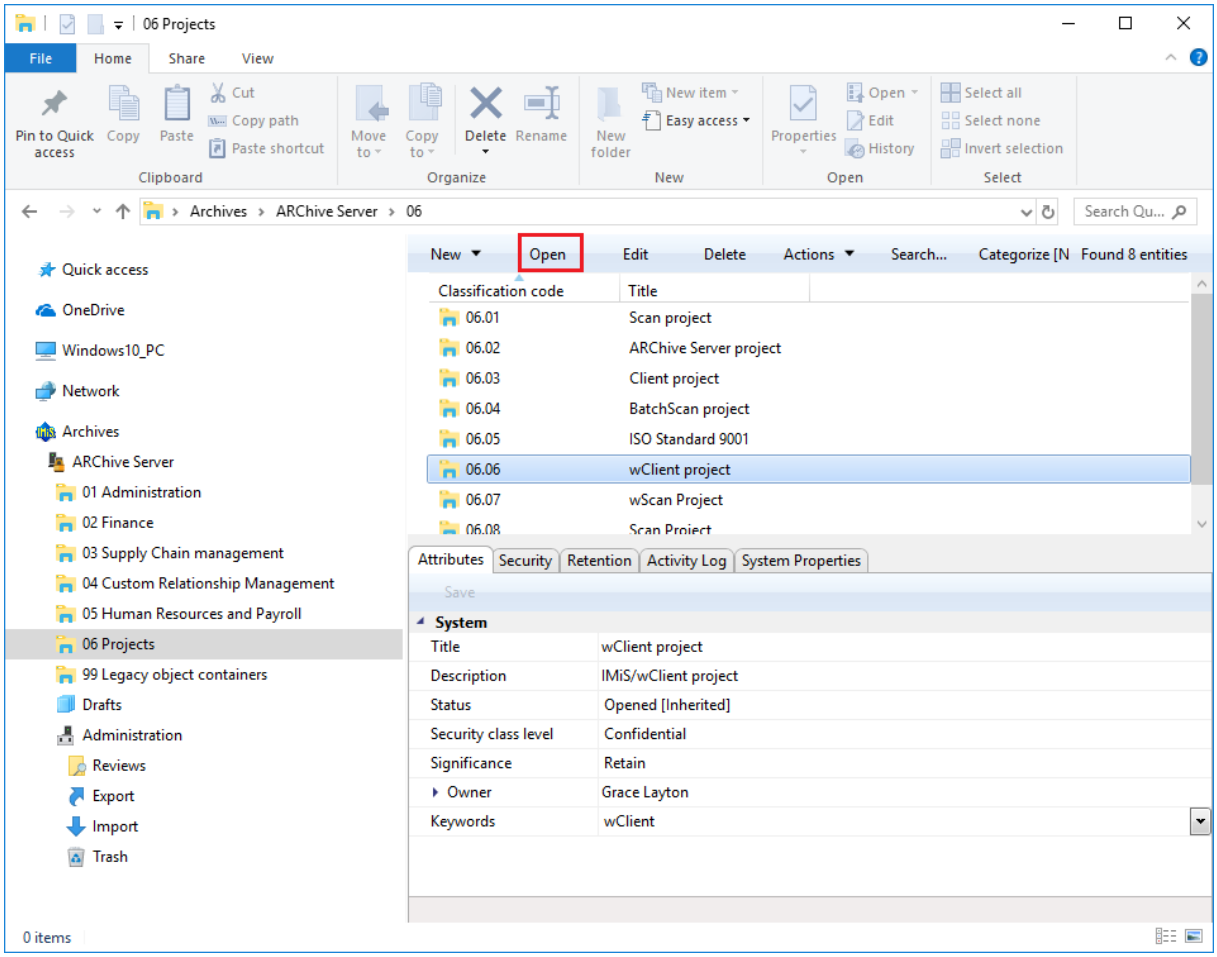


Image 116: Opening the selected entity

4.2.7 Search functions

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

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

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

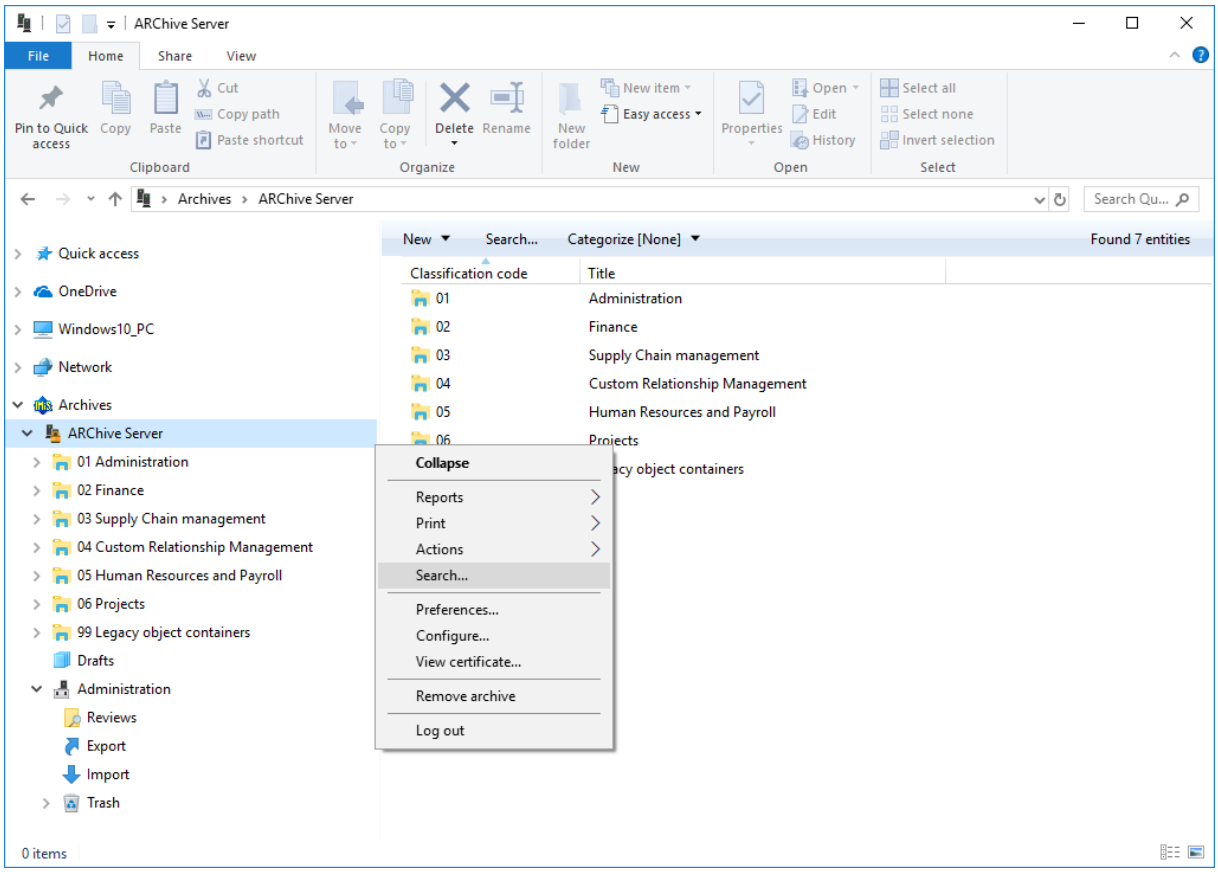


Image 117: Search of the selected entity via the popup menu

Search operations are executed using the »Search builder« and started by using the »Search« command available in:

- The popup menu over the selected archive, class or folder under the »Archives« folder in the tree view of Windows Explorer.
- The popup menu over the selected entity in the list of contained entities.
- The command bar above the selected archive or entity.

The search builder consists of several sections that relate to the scope of the search, the search conditions for search by metadata and search full text, and the option to sort search results.

2018 © Imaging Systems, Inc., All rights reserved.

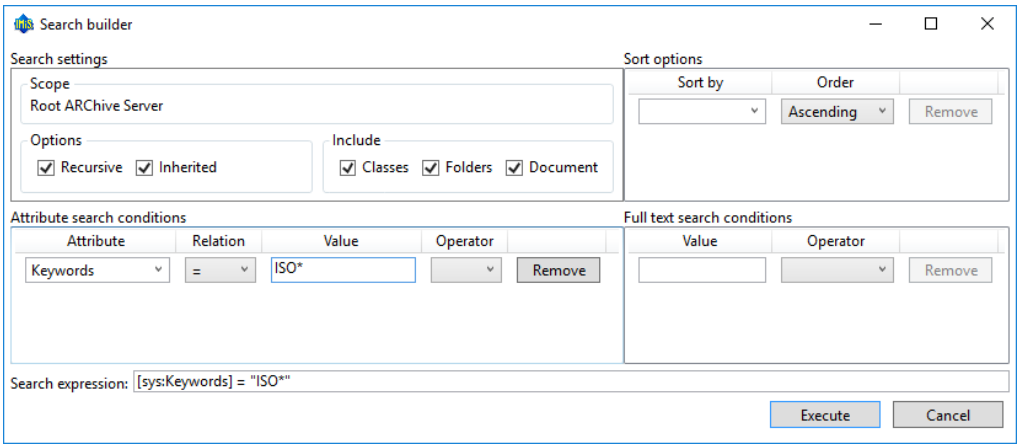


Image 118: Setting search parameters via the dialog box

The section »Scope« shows the name of the archive or selected entity inside which the user is searching.

The section »Options« offers the following choices:

- »Recursive«: turning this option on means search will be conducted on the selected entity and all the entities it contains. When the option is off, search is conducted only on the selected entity and the first sub-level of contained entities.
- »Inherited«: turning this option on means search will be conducted by inherited values as well as explicit values. When the option is off, search is conducted only by explicit metadata values.

The section »Include« lets users select the type of entities they wish to include in the search. The following may be selected:

- Classes
- Folders
- Documents.

In the »Sort options« table, users select the preferred order of search results:

- »Sort by«: sorts by selected attribute.
- »Order«: sets the order of displayed search results. The possible options are »Ascending« and »Descending«.

The conditions of search results are added by selecting the desired attribute, and removed by clicking »Remove«.

2018 © Imaging Systems, Inc., All rights reserved.

In the »Attribute search conditions« table, the user configures simple metadata search conditions. The search conditions table has the following columns:

- »Attribute«: is the name of the attribute the search condition applies to.
- »Relation«: specifies the comparative relation.
  Possible comparative operators are; equal to (=), other than (<>),
  higher than (>), lower than (<), greater or equal (>=), and lower or equal (<=).
- »Value«: specifies the base value to which attribute value is being compared.
- »Logical operator«: represents the logical operator for chaining simple search conditions into complex search conditions. The available operators are the logical inclusive (AND), the logical interchangeable (OR), and the logical mutually exclusive (XOR). The negative operator (NOT) can be entered manually in the »Search expression« field.

Simple metadata search conditions are added together by selecting the corresponding logical operator, and removed by clicking »Remove«.

In the »Full text search conditions« table, the user configures simple full text search conditions.

- »Value«: represents the string you are searching for in the full text.
- »Operator«: represents the logical operator for chaining simple search conditions into complex search conditions. The available operators are the logical inclusive (AND), the logical interchangeable (OR), and the logical mutually exclusive (XOR). The negative operator (NOT) can be entered manually in the »Search expression« field.

Similar to the »Attribute search conditions« table, the user adds simple full text search conditions using the »Add« button and removes them using the »Remove« button.

The »Search expression« field will display the selected conditions and the logical operators between them. The search expression can also be manually edited, by taking into account the appropriate search string syntax. For more information see chapter Search string rules in the IMiS®/ARChive Server Manual.

The search results are displayed in the list of entities, in the right view of Windows Explorer. Results only show those entities the current user is authorized to access.
The total number of entities found by the search is stated in the status bar of Windows Explorer, in the bottom left.

2018 © Imaging Systems, Inc., All rights reserved.

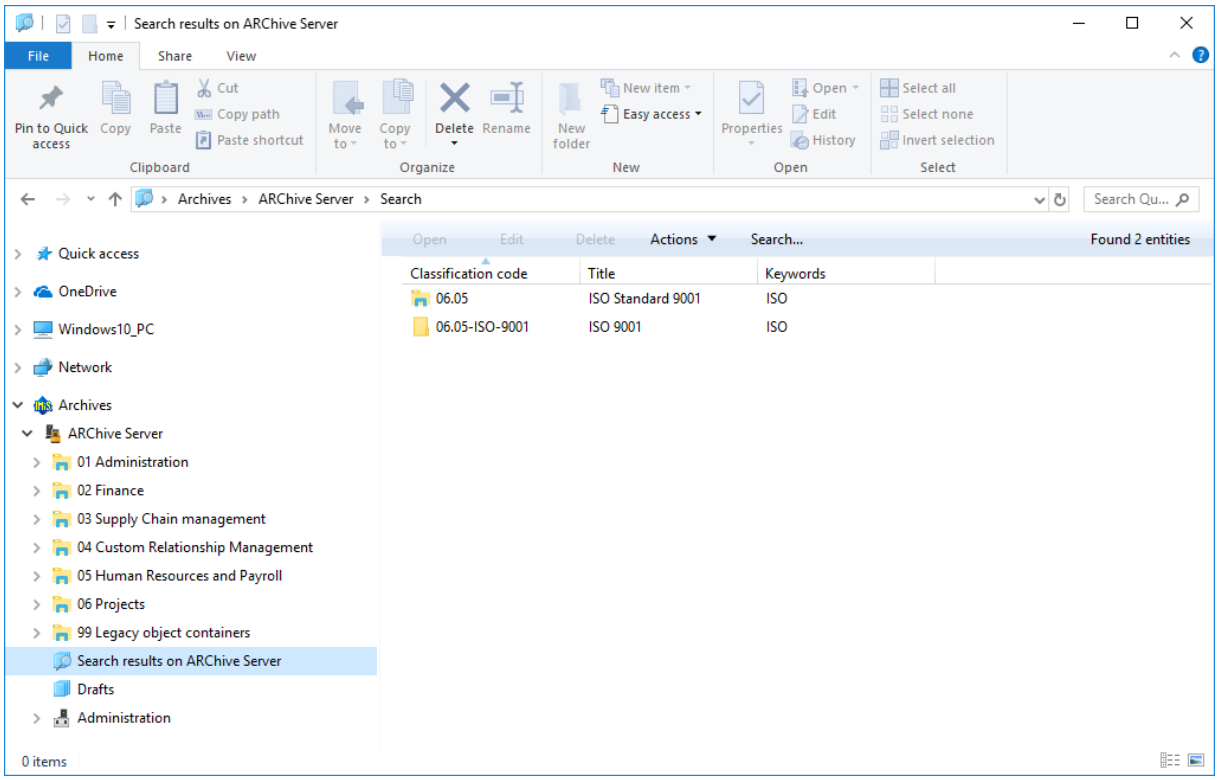


Image 119: Display of search results in the right view of Windows Explorer

4.2.7.1 Search by metadata

To search by metadata, the user has to configure a search string from one or more simple search conditions in the »Attribute search conditions« table of the »Search builder« window. The type of value you are searching for depends on the type of metadata.

When choosing text metadata, the search value must be text. When searching text metadata, the value does not have to be exactly identical. The IMiS®/Client 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.

The search is not case sensitive.

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 «.

2018 © Imaging Systems, Inc., All rights reserved.

- *»*en« searches for entities whose title ends with a string of characters »en«. For instance: »then«, »when«, »hen«, »maiden«.*
- *»d?b« searches for entities whose title has a specified first and third letter (in this case »d« and »b«), while the second letter and all other letters can be random.*
  For example, producing: »debate«, »Debit«, »dab« or »dubious claims«.

This does not work when searching metadata whose value is represented by the name of a IMiS®/ARChive Server user (for example the metadata »Owner«).
For these values, the search string must be identical to the value of the metadata.

The input of search values when searching by »date and time« metadata is simplified by the date and time popup window. In case of using the relation operators »equal to« (=) or »other than« (<>) only the date is inserted, while the time is automatically turned into the range of one day by the IMiS®/Client. With other relation operators, the date and time must both be input.

Tip: In case you are only familiar with the initial part of an attribute's value, you can use the relation »>« or »>=«. In the latter case, the search results display all values that are equal to the search criteria, and all those values whose initial value parts contain characters and numbers higher, in a successive sequence, than the search criteria.

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

4.2.7.1.1 Search by Content descriptions

Users may also search by title of contained content. The »Attribute search conditions« option lets you create a search string using one or more simple conditions.

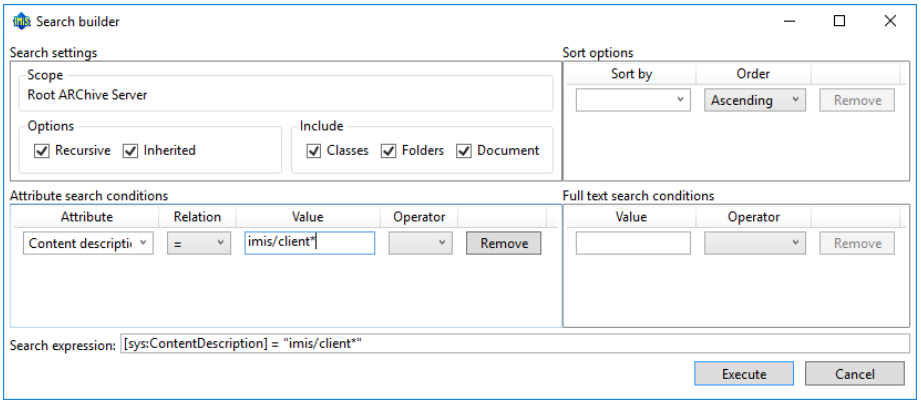


Image 120: Sample search string for searching by title of the content

List of entities that shows the matching search results.

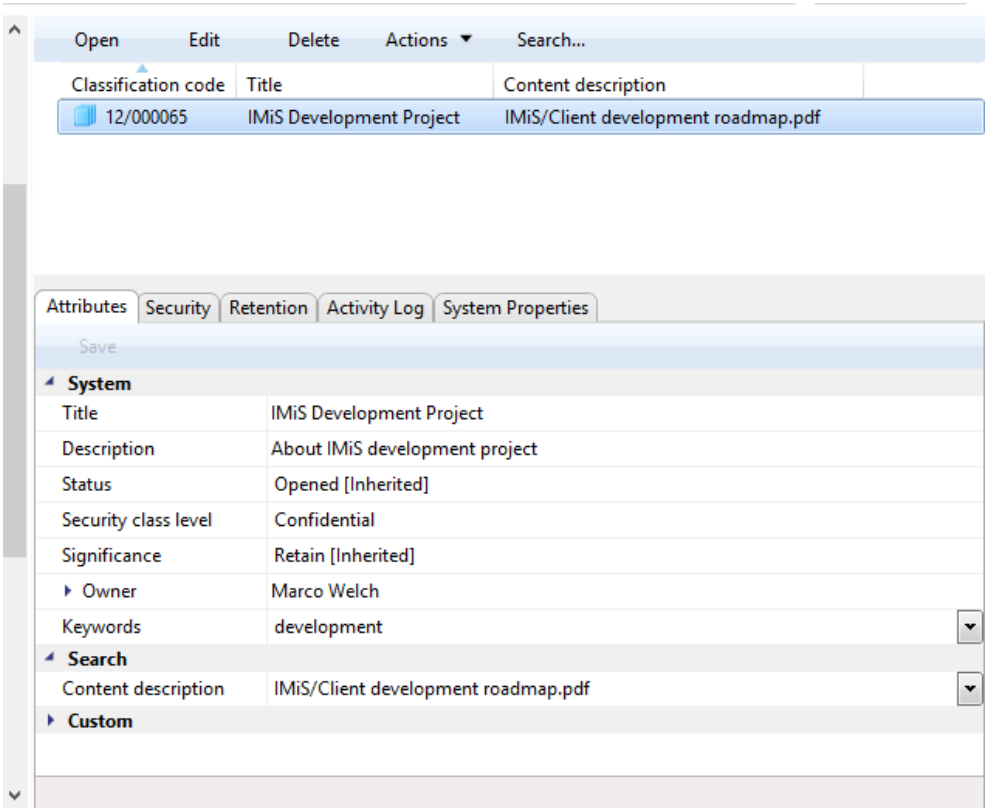


Image 121: Results of searching by title of the content

4.2.7.2 Full text search

To search the full text of the content, the user must configure a search string of one or more simple search conditions in the »Full text search conditions« table in the »Search builder« window.

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.*

2018 © Imaging Systems, Inc., All rights reserved.

- ***»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, …)*

Searching the full text is not case sensitive. You may also perform a »wildcard search« by using the special characters »*« and »?« in the search string.

For more information on how to use these characters to search partial values see chapter Search by metadata.

The full text search of content can only be conducted for those content formats that allow the IMiS®/ARChive Server to recognize text.

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).

2018 © Imaging Systems, Inc., All rights reserved.

4.2.7.3 Combined search by metadata and full text search

Searching by entity metadata and the full text of content can also be combined, which is automatically enabled by the »Search builder«.

4.2.8 Editing entity data

Editing data about an entity in the IMiS®/Client 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 top command bar.

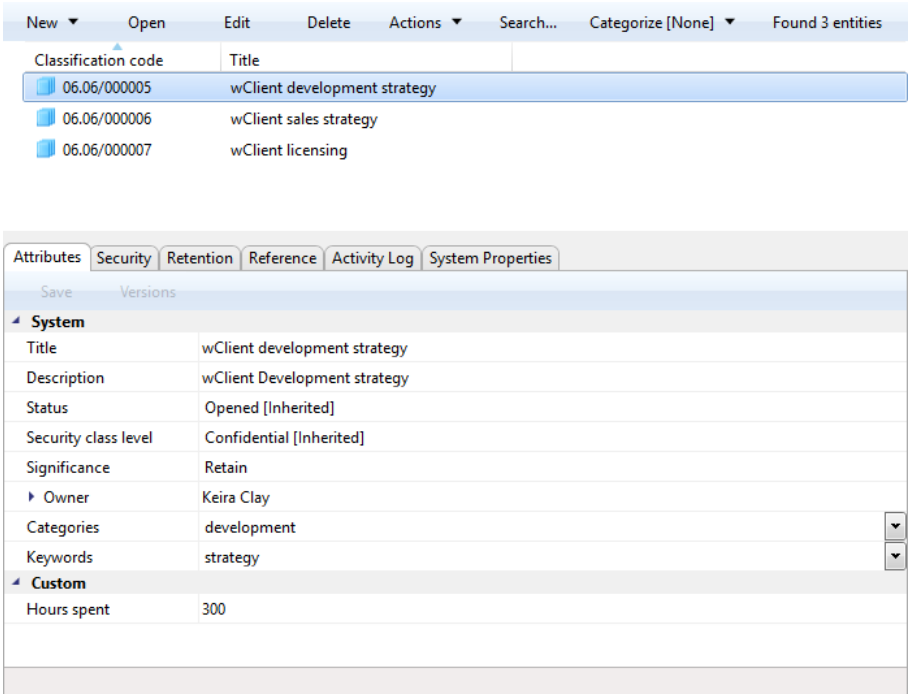


Image 122: Editing an entity via the command bar

Metadata that is not »Read-only« and may be edited is found in the tabs »Attributes« and »Physical content«. To the right of the metadata's title is a field where users can change the value of the metadata. The value can be text, date and time, logical, or predefined.

You can predefine any number of values.

2018 © Imaging Systems, Inc., All rights reserved.

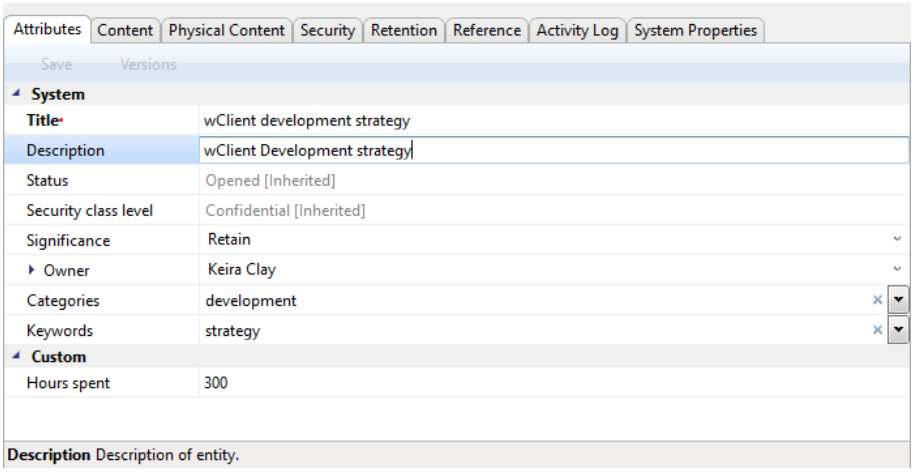


Image 123: Entering or editing entity metadata

Changes to an entity also involve the adding (chapter Document capture), deleting and modifying of the entity's content. The user performs these actions through the »Content« tab.

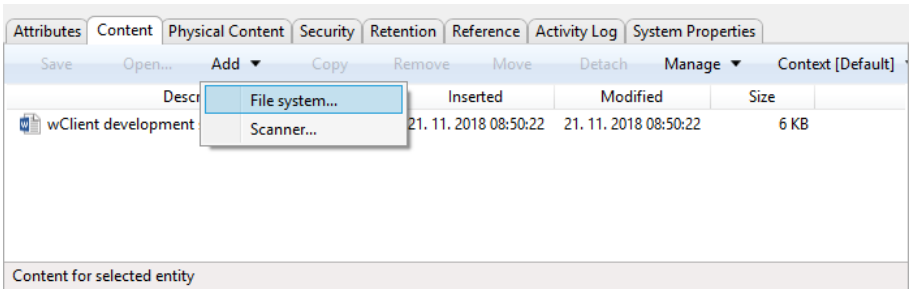


Image 124: Adding content to an entity via the file system

Content is added by choosing the »Add« command in the command bar of the tab.
This opens a popup menu that lets you select the source of new content. The source can be either the »File system« or the »Scanner«. When you select »File system«, you will receive a dialog box enabling you to select the file you wish to import as the content of an entity, which must be located somewhere on the local computer.
When selecting »Scanner«, this starts the IMiS®/Scan application that allows you to scan content and import it into the content of an entity.

Content is removed using the »Remove« command in the bottom command bar found under the tabs. The user selects any number of the content, user wish to remove from the list. Users may also edit the content of an entity, though archiving rarely requires this particular functionality. Any modifications to the content of an entity will be recorded in the audit log.

2018 © Imaging Systems, Inc., All rights reserved.

Warning: Content can be successfully modified only if the entity is in editing mode.

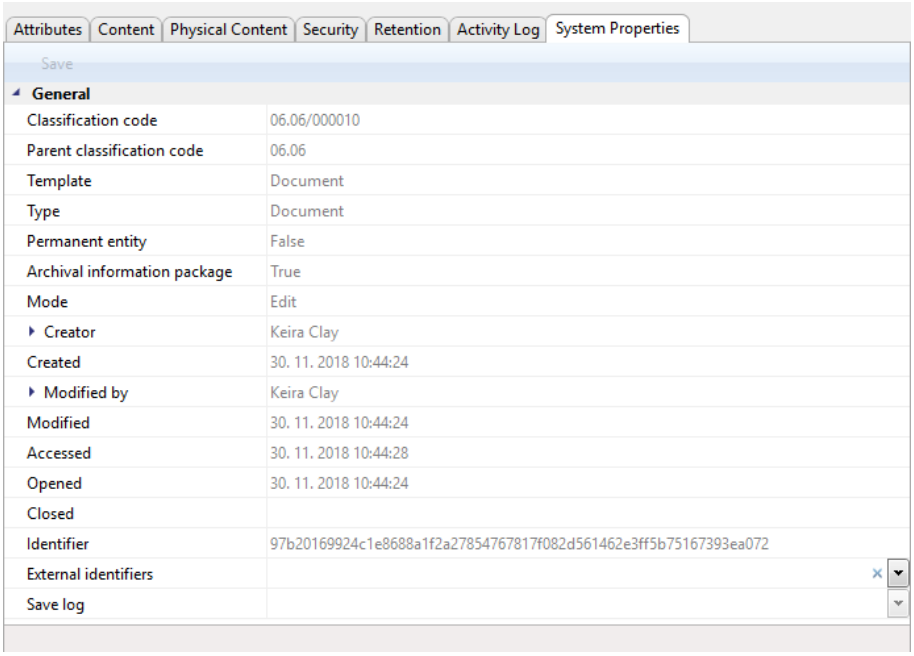


Image 125: Opening the entity in editing mode.

Content is opened in the default application for its file type by using the »Open« command.

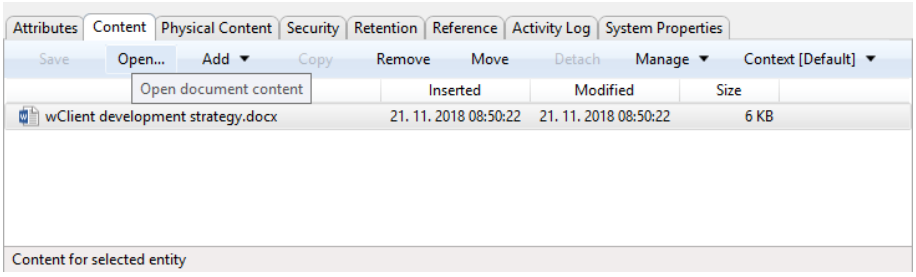


Image 126: Opening content in the default application.

Note: If a user wishes to open multiple contents at once, he must first select these contents and then select the »Open« command in the bottom command bar. The contents are opened successively.

After performing the modification in the default application, the user saves the content and closes it. IMiS®/Client marks the modified content in bold and prepares it for transfer to the archive system.

2018 © Imaging Systems, Inc., All rights reserved.

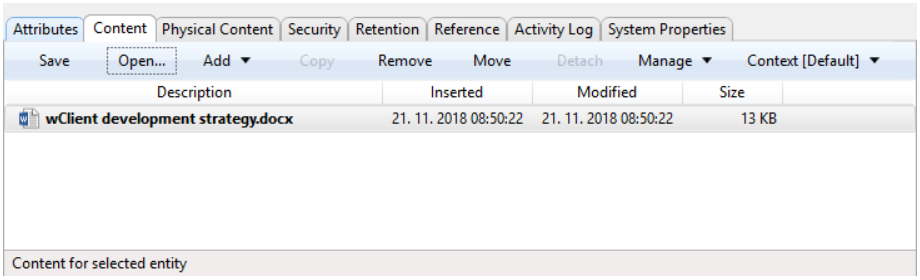


Image 127: Display of the modified content after modification in the default application

Changes to the entity are confirmed using the »Save« command in the bottom command bar. If you wish to discard changes, simply select another entity and click »Don't save« in the save prompt.

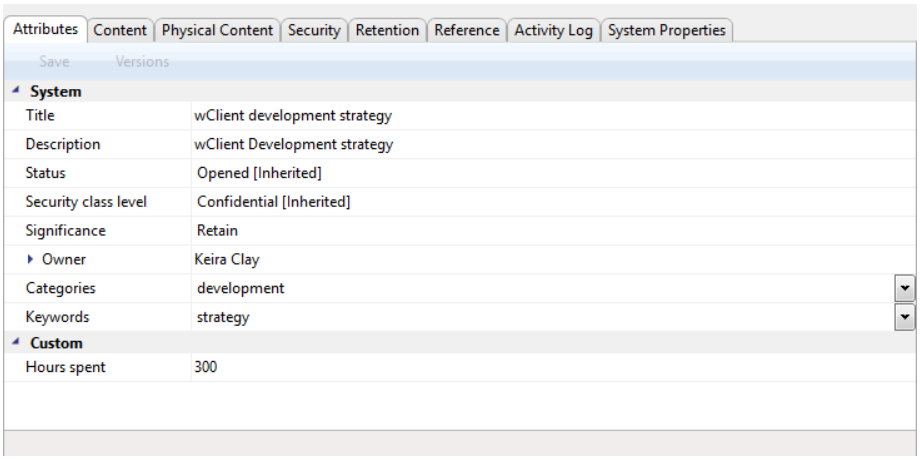


Image 128: Saving changes to the entity

When saving the document, the »Modified« date is also changed on the modified document content.

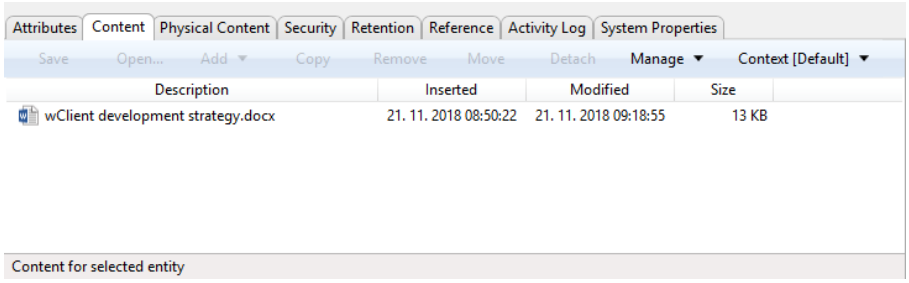


Image 129: When saving the modified content, the »Modified« date is also changed

2018 © Imaging Systems, Inc., All rights reserved.

4.2.9 Versioning

The user is enabled the versioning of all document-type entities. The properties that have been modified in individual document versions can only be viewed on templates that enable versioning.

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

The user with the »Draft Management« role can perform the following actions:

- Checking out a document version (Check out)
- Checking in a document version (Check in)
- Discarding a document version (Discard).

Access to a document version is enabled to the user with the »Read« access permission.
The »Draft Management« role is not required for opening a document version.

4.2.9.1 Checking out a document version

By selecting the action »Check out« on the »Actions« button in the top command bar or in the popup menu on the document selected from a list, the user is shown a dialog box with the relevant tabs and set of attributes.

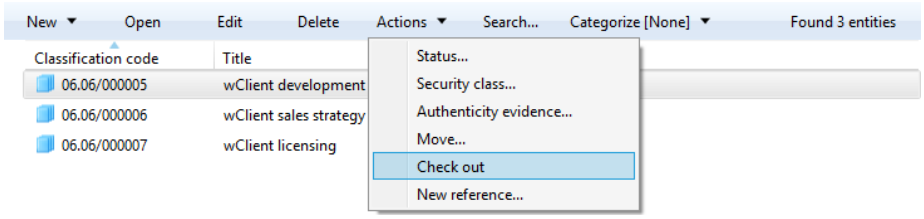


Image 130: Selecting the action »Check out« in the popup menu

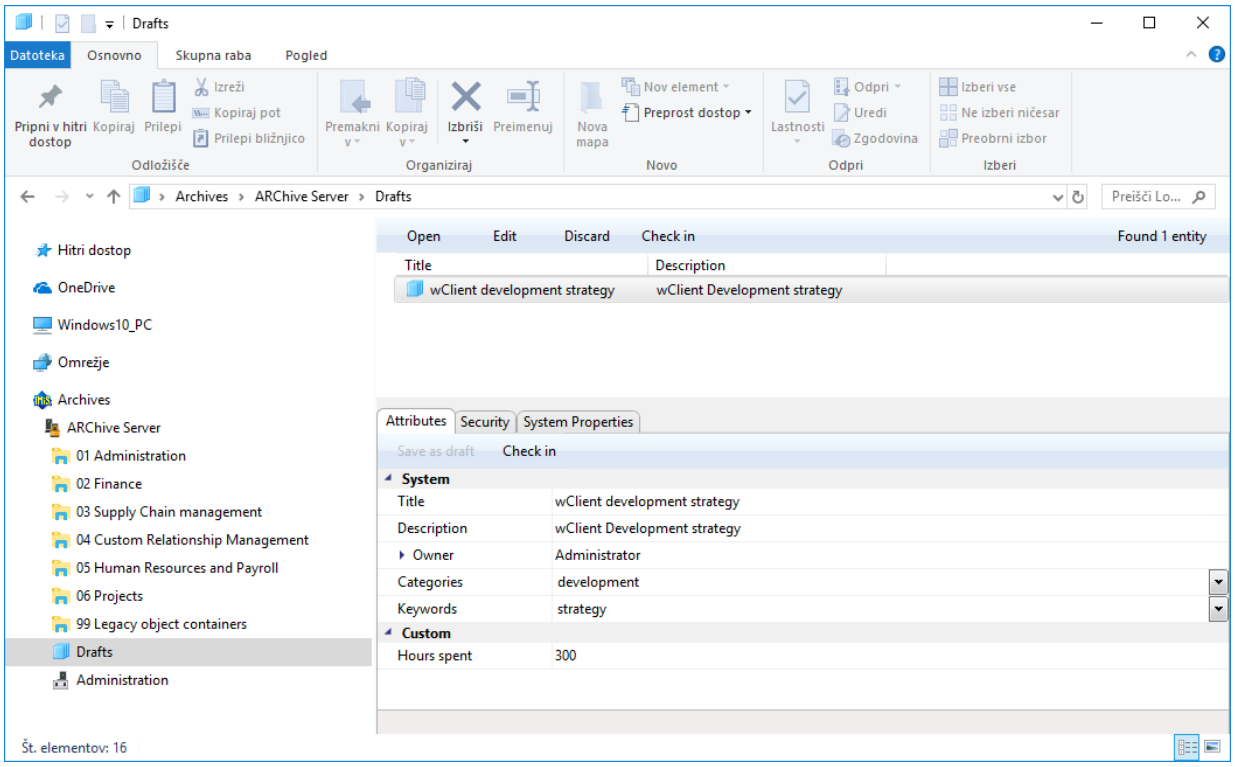


Image 131: Displaying the document version details

The created document version is a copy of the source entity and is based on the same template as the source one. It is located in the folder »Drafts« in the left view. When making a copy of a document, the IMiS®/Client makes a copy of the attributes and content, while the IMiS®/ARChive Server also adds access permissions.

In the »Attributes« tab the following attributes are available to the user in the bottom right view of Windows Explorer:

- »Name«: the name of the document. This attribute is mandatory.
- »Description«: a short description of the document.
- »Owner«: the directory entity (user or group) that is responsible for the selected document version (owner).
- »Categories«: a collection of document categories.
- »Keywords«: document-related keywords.
  This attribute can have multiple values.
- »Custom«: the attributes are defined by the selected template. The display depends on the set of attributes in the template, which are defined by the administrator of the classification scheme on the server.

2018 © Imaging Systems, Inc., All rights reserved.

Note: The values of the »Security class level« and »Significance« attributes are preserved based on the source document and cannot be edited by the user.

The user can create new attribute values on a document only, if the attribute is marked as »versionable« on the template. The values of versionable attributes change with each version. The values of attributes which are not versionable stay the same in all document versions.

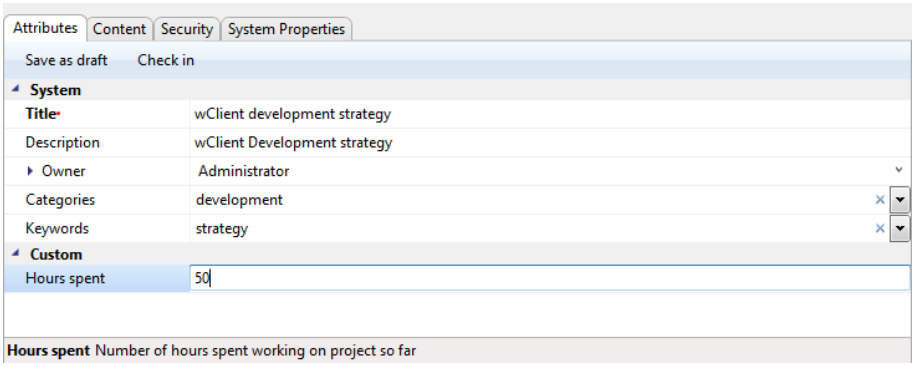


Image 132: Checking out a document version

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« in the bottom command bar.

By selecting the command »Check in«, a dialog box opens in which the user can define the values of the following attributes:

- »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.

2018 © Imaging Systems, Inc., All rights reserved.

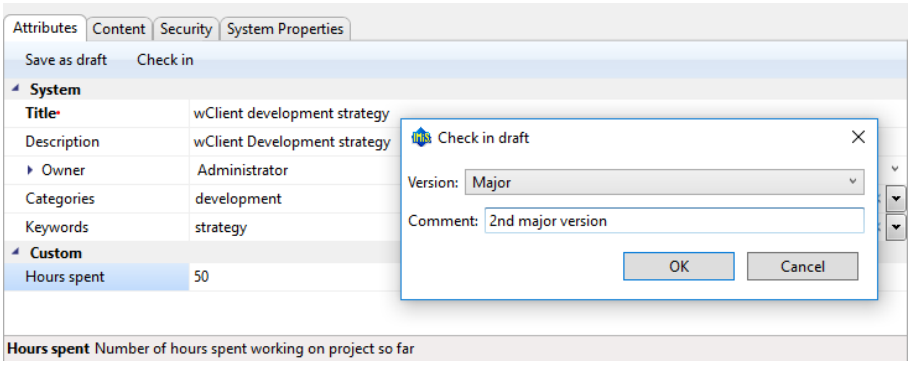


Image 133: Selecting the document version and entering a comment

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

When checking out a new document version, the values of versionable attributes are assigned a new sequence number which represents the document version.

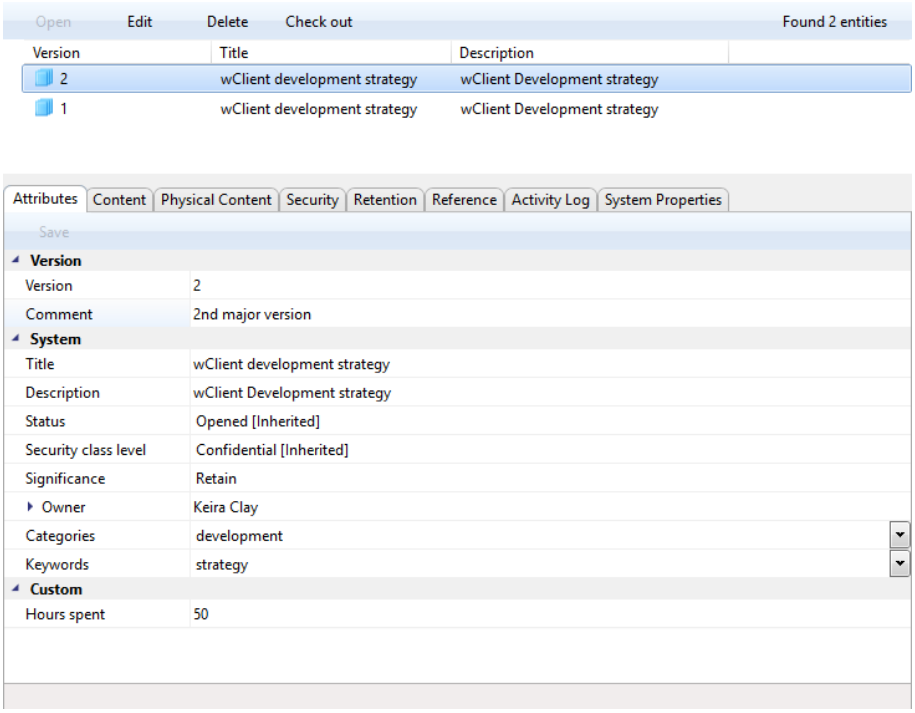


Image 134: Details of the saved document version

By selecting the document version, the user can choose from the following options in the top command bar:

- Viewing a document version (Open).
  For more information see chapter Viewing a document version.
- Editing a document version (Edit).
  For more information see chapter Editing a document version.
- Deleting a document version (Delete).
  For more information see chapter Deleting a document version.
- Checking out a new document version (Check out).
  For more information see chapter Checking out a document version.

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

4.2.9.2 Viewing a document version

In all viewing modes the user can view document versions by selecting the command »Versions« in the bottom command bar in the »Attributes« tab.

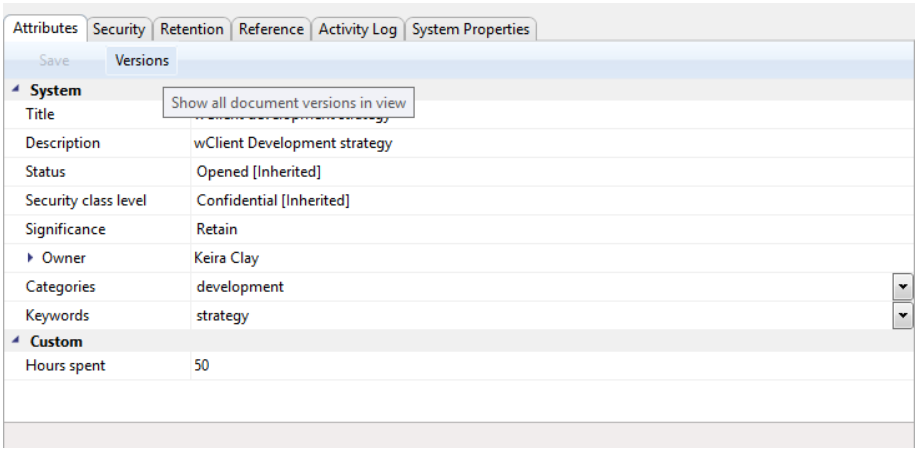


Image 135: Selecting the command »Versions« in the bottom command bar

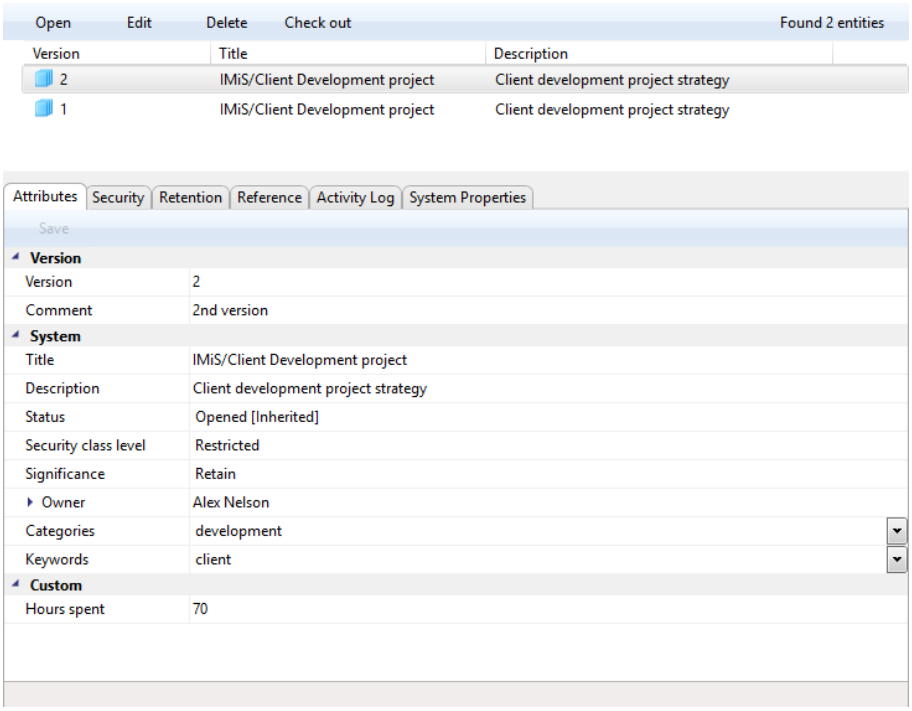


Image 136: Displaying document versions in the set »Versions«

4.2.9.3 Deleting a document version

By selecting a document version and the command »Delete« in the top command bar, the user deletes the document version. Deletion is not possible, if the document is in Edit mode.

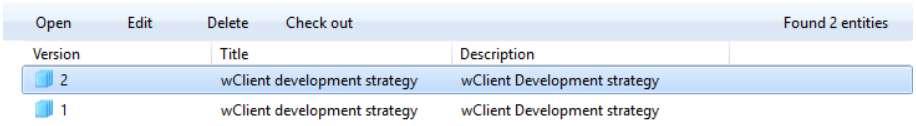


Image 137: Selecting the command »Delete« on the selected document version

Note: The user deletes the source document by removing all document versions beforehand.

4.2.9.4 Editing a document version

The actions of checking out a document version (CheckOut) and editing a document (Edit) are mutually exclusive. Editing is not possible if a document version has been created, and vice versa; a document version cannot be created on documents which are being edited.

By selecting the »Edit« command in the top command bar, the user can edit the values of the versionable attributes to which he has the relevant access permissions.

2018 © Imaging Systems, Inc., All rights reserved.

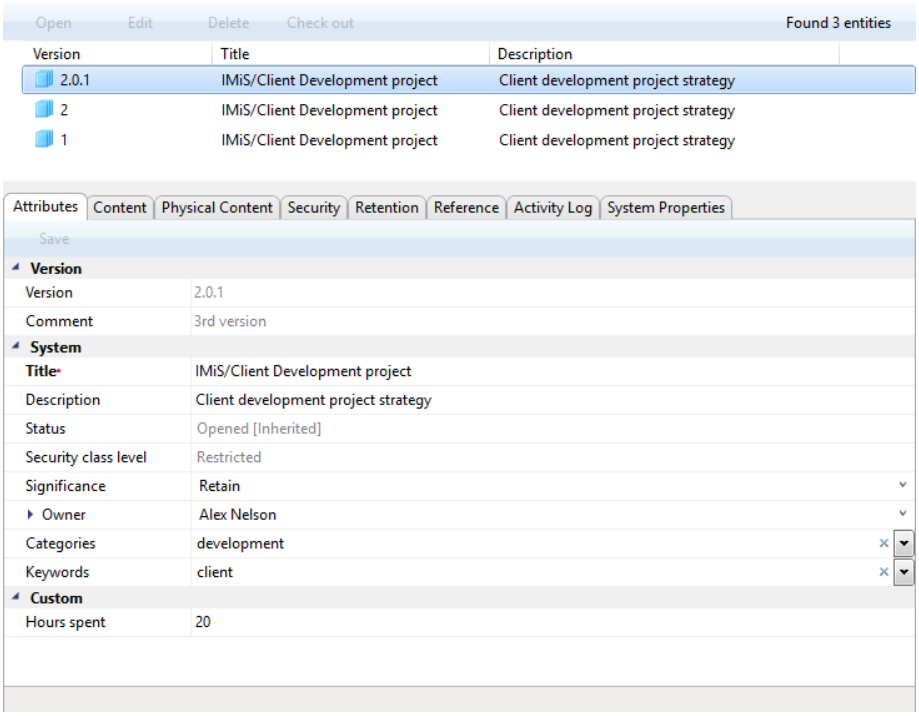


Image 138: A document version in Edit mode

<u>Note:</u> 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.

4.2.9.5 Checking out a document draft

If the user has checked out a new document version and wants to check it in at a later time, he can save it temporarily with the command »Save Draft«.

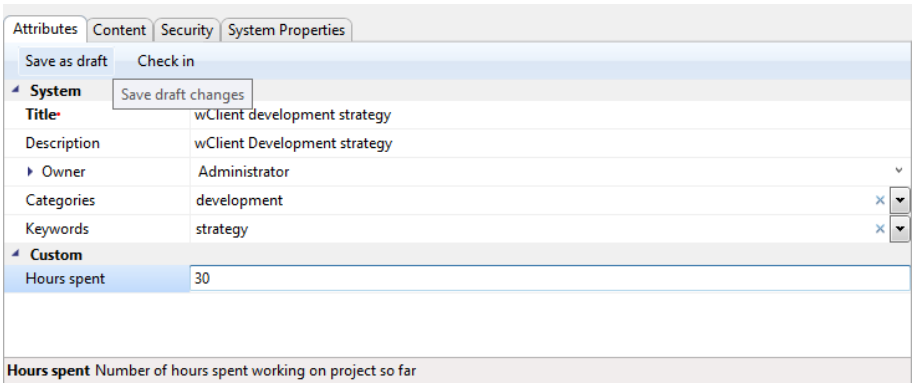


Image 139: Saving a document draft for a later check-in of the document version

After saving the document draft, the right view shows the user a list of document drafts saved in the folder »Drafts«.

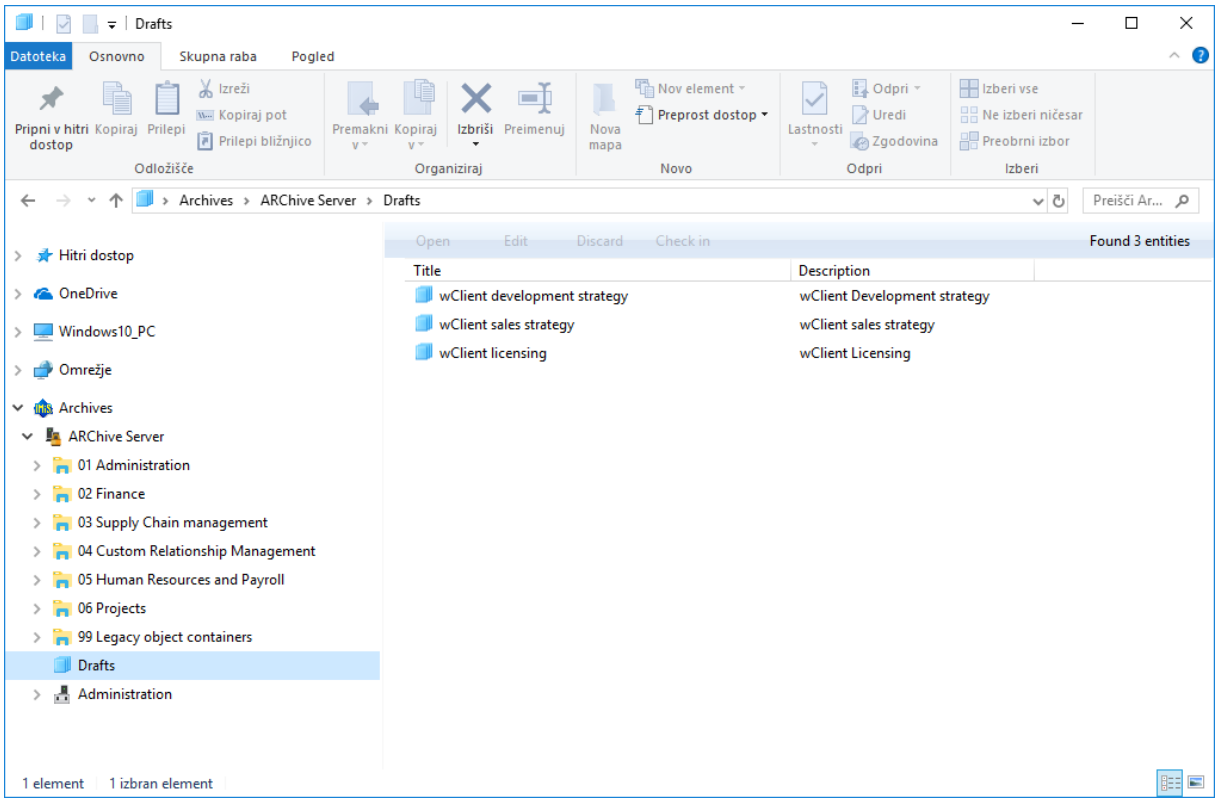


Image 140: A list of document drafts

By selecting the document draft, the user can choose from the following commands in the command bar:

- Viewing a document draft (Open).
- Editing a document draft (Edit).
- Discarding a document draft (Discard).

  For more information see chapter Discarding a document draft.
- Checking in a document draft (Check In).

  For more information see chapter Checking in a document draft.

2018 © Imaging Systems, Inc., All rights reserved.

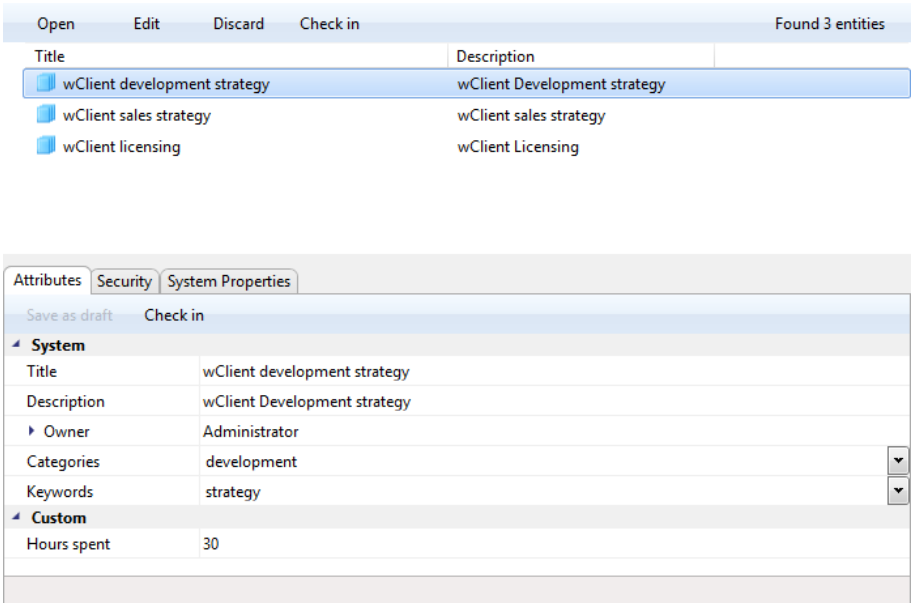


Image 141: Document draft details in the folder »Drafts«

4.2.9.6 Discarding a document draft

The user can discard a document draft with the command »Discard« and by entering a comment (optional). After confirmation (OK), the document draft is removed from the list.

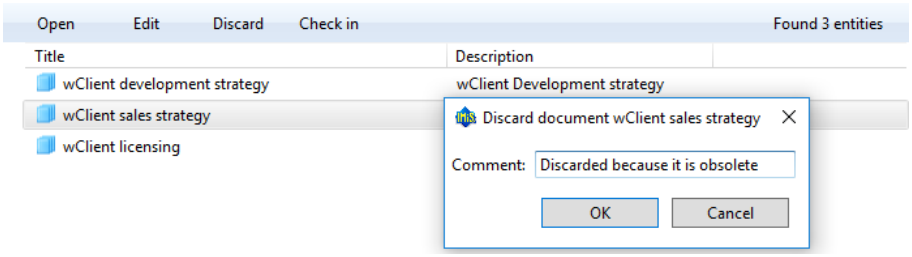


Image 142: Discarding a document draft with the command »Discard«

4.2.9.7 Checking in a document draft

The user checks in a version of a document saved in the »Drafts« folder by selecting the command »Check In« in the command bar.

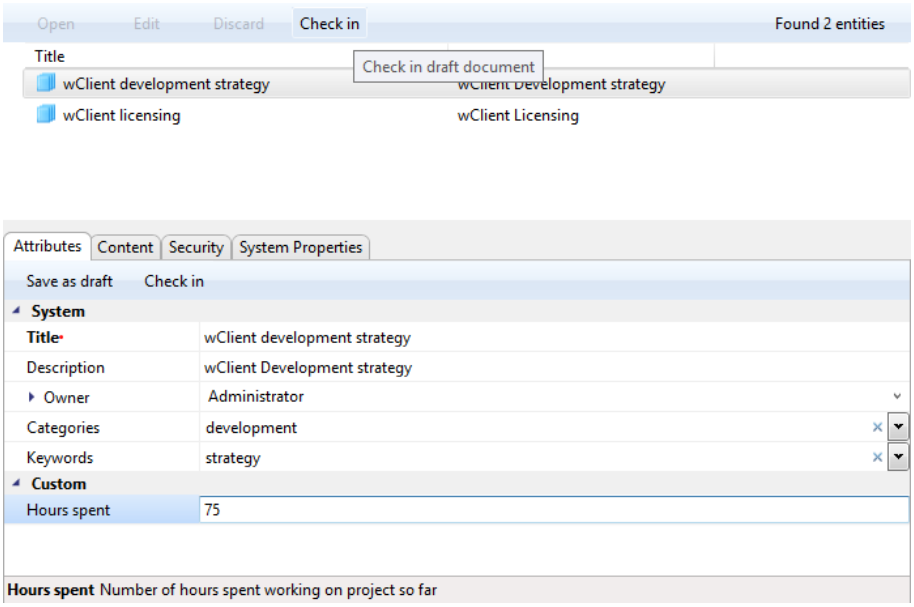


Image 143: Viewing a draft before check-in

Before check-in the user selects the document version and enters a comment (optional).

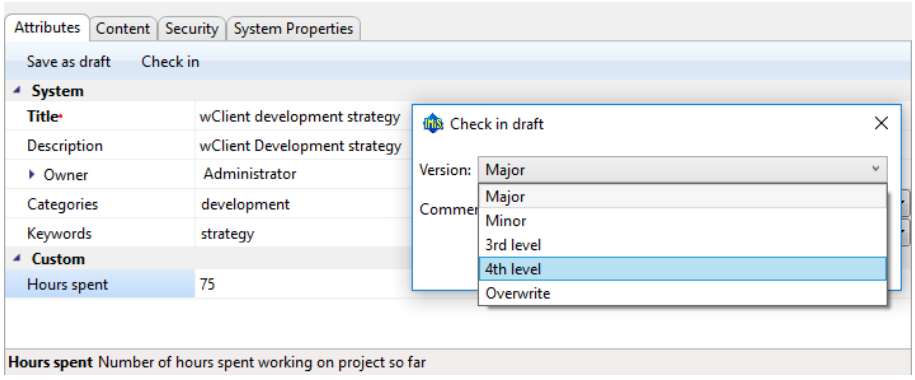


Image 144: Selecting a version before checking in a document draft

After checking in a document draft, the user has the option to view versions of the document. He does that by selecting the command »Versions« in the bottom command bar.

2018 © Imaging Systems, Inc., All rights reserved.

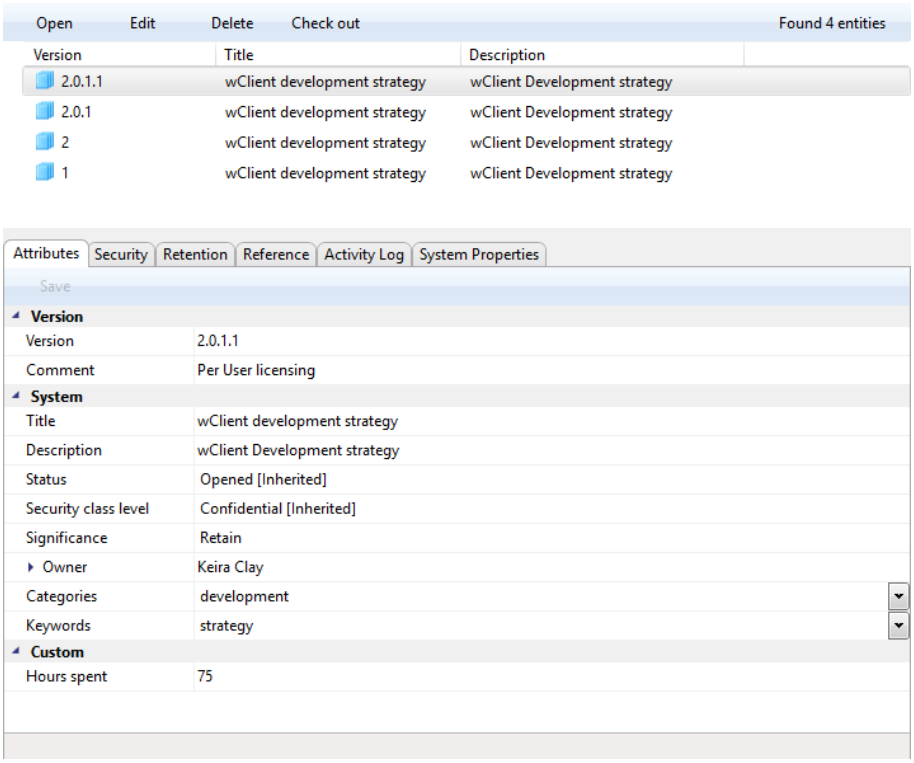


Image 145: Displaying the document versions after checking in the draft

4.2.10 Archiving email messages

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

4.2.10.1 Email archiving procedure

The user captures email messages by using the Windows »Drag and drop« functionality.
The user marks one or several email messages, including their attachments, in the email client (MS Outlook, IBM Notes etc.) and »drags« them to the selected class or folder in the classification scheme in Windows Explorer.

If the user wishes to mark several different messages, he holds down the »Ctrl« key and selects individual messages with the left mouse button.

The user arranges the Windows Explorer 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 right view of Windows Explorer.

2018 © Imaging Systems, Inc., All rights reserved.

If the mouse cursor changes to a copy cursor , the user can archive the email message to this folder or class.

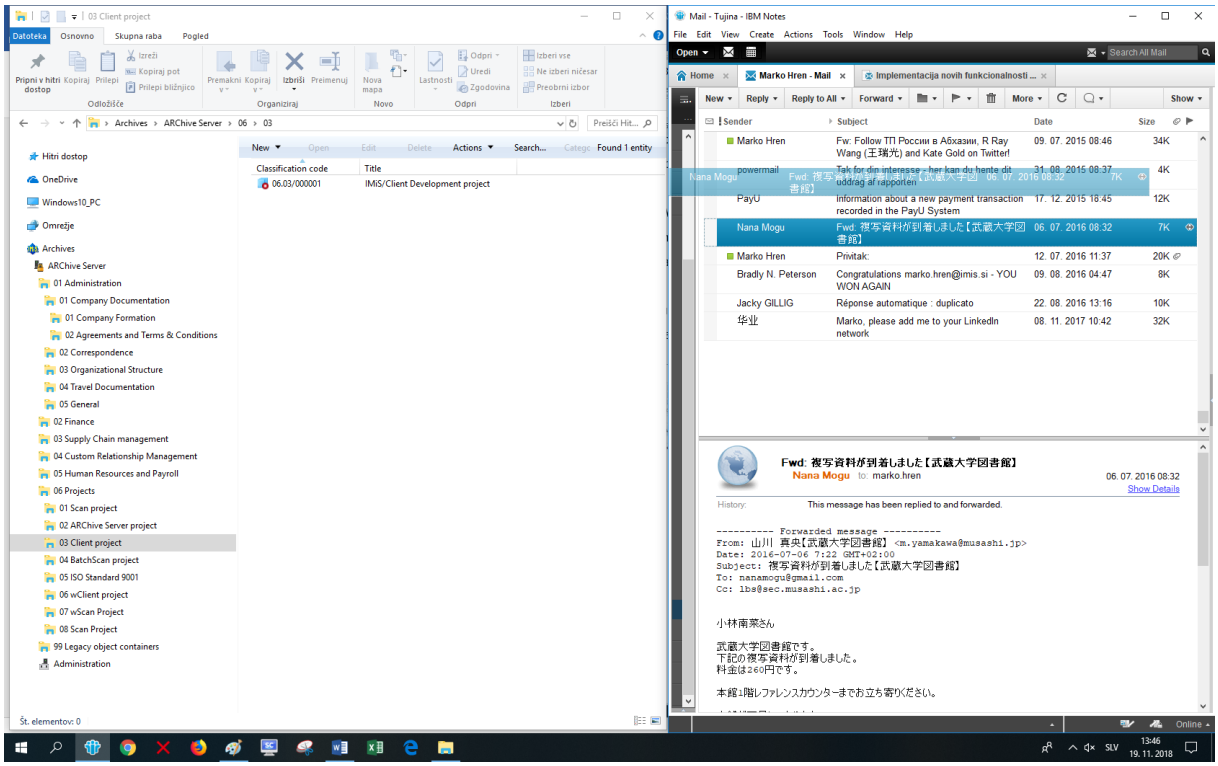


Image 146: Transferring email messages from the email client to the selected class

When you let go of the left mouse button, the selected messages are automatically transferred to the desired location in the classification scheme together with their metadata and content, and are saved to the IMiS®/ARChive Server.

2018 © Imaging Systems, Inc., All rights reserved.

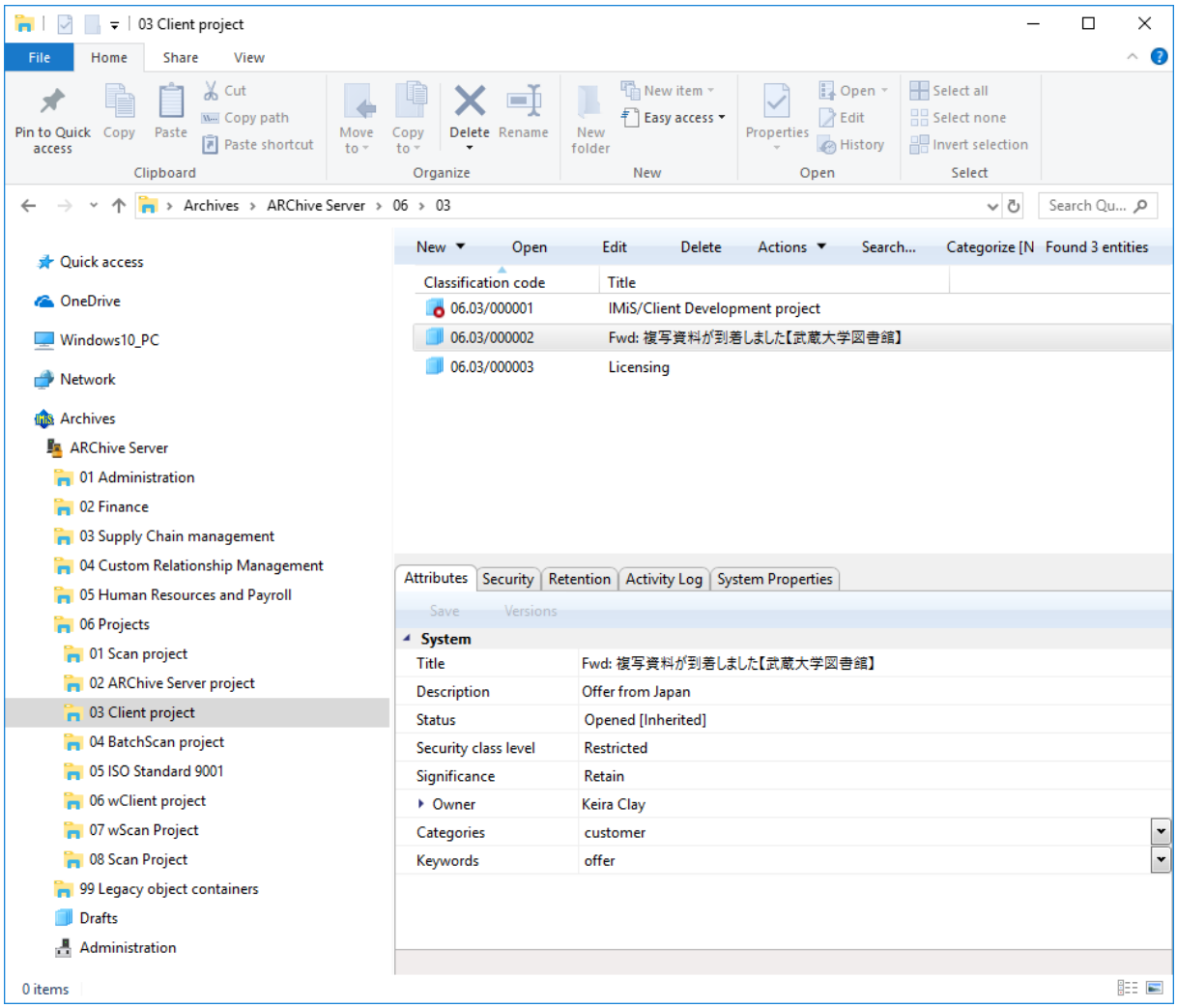


Image 147: Display of transferred email messages

Warning: The capture of email messages works according to the selection of files in MS Windows. The order of files, and consequently the order of classification codes of transferred email messages in the classification scheme, depends on the order in which the messages are selected in the email client.

In the »Content« tab, the user can see all the content that was saved together with the email message. In addition to the message itself, two attachments are always made automatically:

- »Email – raw«: the original email message in EML format.
- »Email – body«: the body of the original email in either text or HTML format.
  This format depends on the type of the email message's body.

2018 © Imaging Systems, Inc., All rights reserved.

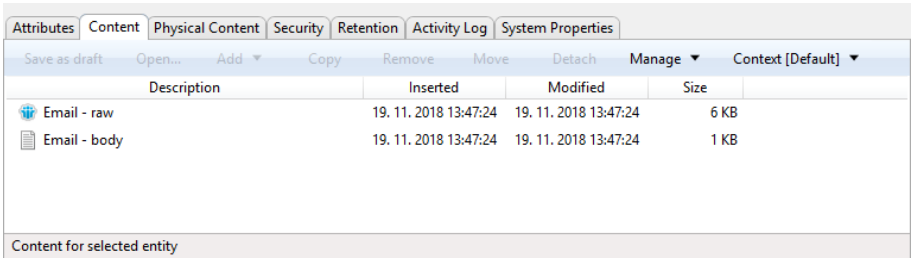


Image 148: Automatically created email attachments

Note: By clicking the »Email – raw« file, the user opens the original email message in the default client used to open EML files.

4.2.10.2 Functionality description

The selected email messages are copied to the specified location in the classification scheme, in the form of an EML file. For each email message, the IMiS®/Client creates a new document containing the original message, the metadata and any captured content.

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

- »Subject«: the subject of the message.
- »Date«: the date and time the message was sent or received.
- »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.
- »Priority«: priority status of the email.
- »Signed«: a value that registers if the email message was electronically signed.
- »Message Id«: automatically generated message identifier.

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

2018 © Imaging Systems, Inc., All rights reserved.

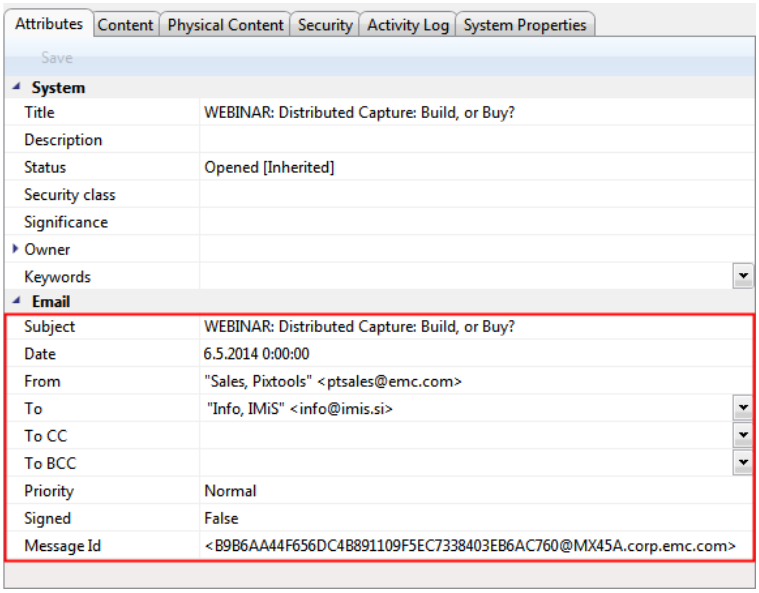


Image 149: Example metadata extracted from an email message

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

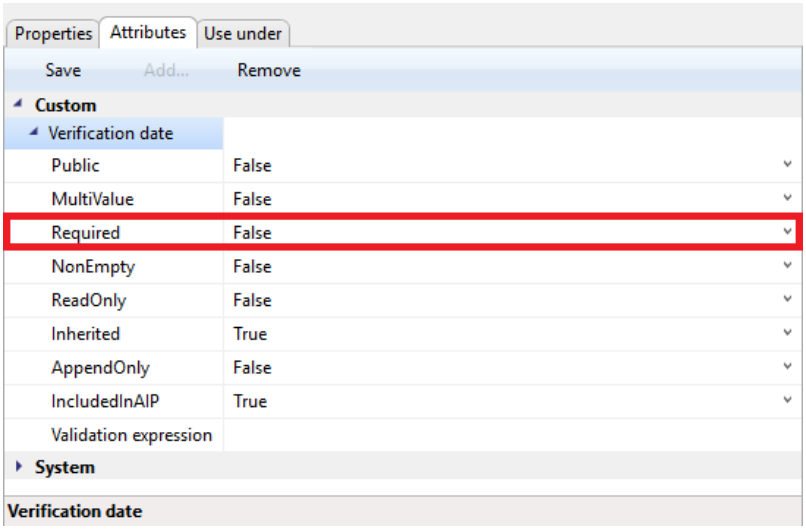


Image 150: Example setting custom attribute

4.2.11 Managing physical content metadata

When capturing physical content into its electronic form, users may add metadata that describes the physical location of the stored content, in addition to other types of metadata. The location metadata is optional. If the user enters at least one attribute from the list of physical content, user also have to enter the identifier of the physical content. Entry of physical content metadata for a folder or document is possible upon capture / import, or later when the content is already stored in electronic form.

2018 © Imaging Systems, Inc., All rights reserved.

If you want to perform the entry of physical content metadata during capture (chapter Document capture) or later on, select the »Physical Content« tab.
Find the appropriate class or folder in the classification scheme (chapter Classification scheme) in the left view of Windows Explorer. Then select a document or folder in the list of entities (top right view). By choosing »Edit« in the command bar of Windows Explorer, the selected document or folder is opened in editing mode. In the overview of entity information, there is a new tab »Physical Content« that shows physical content metadata.
For more information see chapter Interface description.

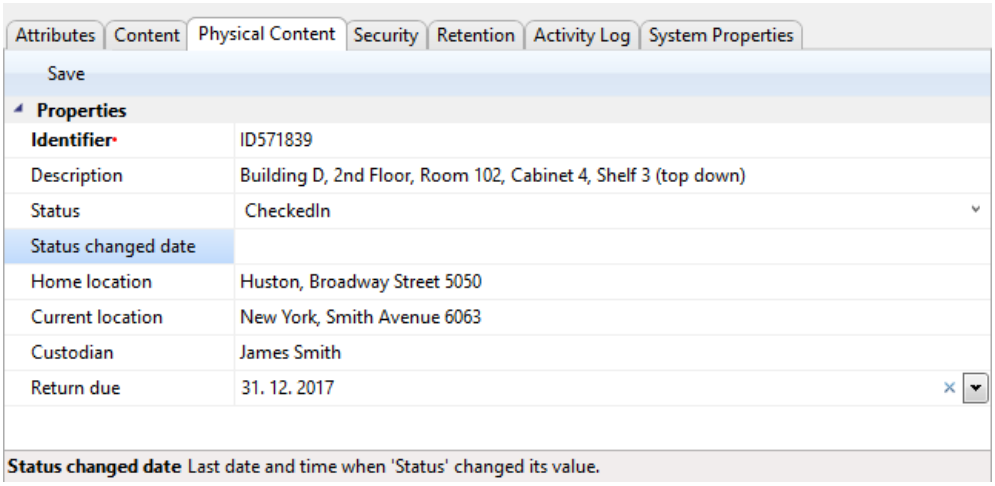


Image 151: Display of entering physical content metadata

The user can complete all the fields except »Status change date«, which is automatically completed with the date of the last change to the »Status« field. When capturing content, set the »Status« field to the value »CheckedIn«. For more information on a description of physical content metadata see chapter Physical content attributes.

4.2.12 Print

Printing functionalities are divided into:

- Printing the content of a document.
- Performing print functions via the popup menu.

4.2.12.1 Printing the content of a document

A document can contain content of different types, created by different applications. Since every application will correctly print its corresponding file format, the printing of document content is performed through applications for its particular content type.

2018 © Imaging Systems, Inc., All rights reserved.

Select the archive server in the left view of Windows Explorer and locate the document containing the content you wish to print.

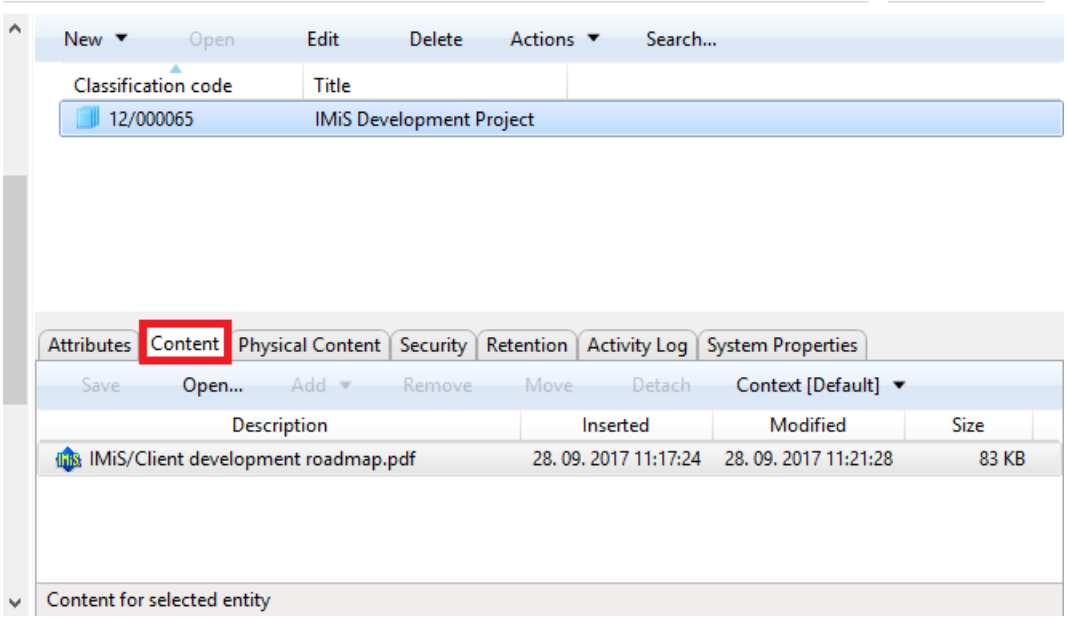


Image 152: Access to the content of a selected document

In the top right view, select the document. Access to the content is only available when the document is open in reading mode, which is done by choosing the »Open« command in the top command bar or double clicking the document.

A new tab »Content« then appears in the bottom right view. Selecting this tab will display a list of all the content in the document.

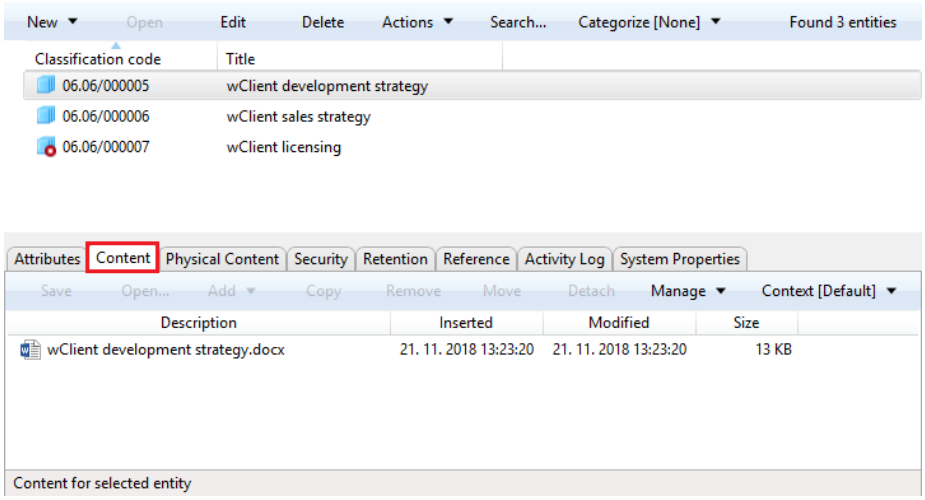


Image 153: Access to the contents of the desired document

2018 © Imaging Systems, Inc., All rights reserved.

The selected content is opened in the default application for the corresponding content type by choosing the »Open« command in the top command bar or by double clicking.

Once the application is open, you can print the content.

Repeat this procedure for all content in the document.

4.2.12.2 Performing print functions via the popup menu

Printing can also be performed by choosing one of the options in the popup menu opened by right-clicking a selected entity or IMiS®/ARChive Server. Depending on the type of the currently selected entity or server, the popup menu changes in appearance.

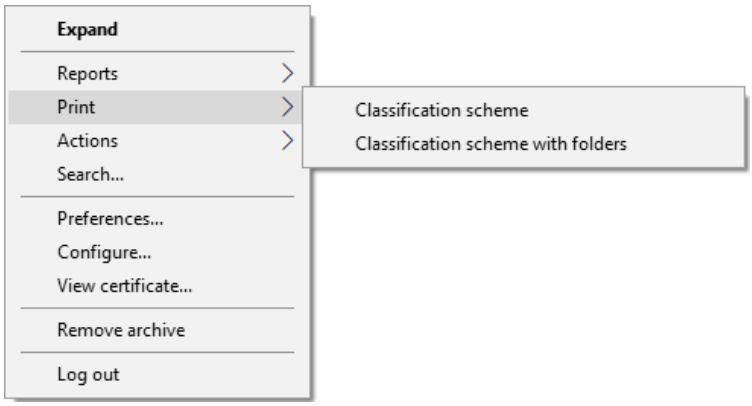


Image 154: Selecting print options via the popup menu

4.2.12.3 Printing metadata, document security settings and properties

Printing the metadata of the selected document is done by choosing the »Print« and then »Document« commands.

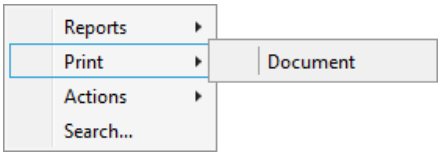


Image 155: Selection of metadata print options for the chosen document

Printing the metadata of the selected folder is done by choosing the »Print« and then »Folder« commands.

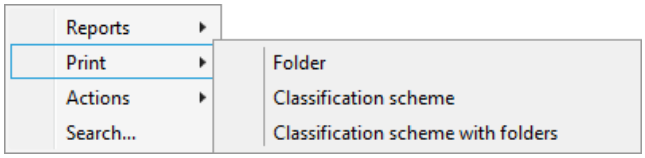


Image 156: Selection of metadata print options for the chosen folder

2018 © Imaging Systems, Inc., All rights reserved.

Printing the metadata of the selected class is done by choosing the »Print« and then »Class« commands.

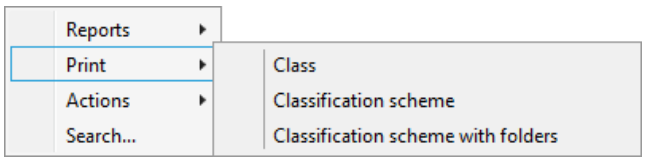


Image 157: Selection of metadata print options for the chosen class

After choosing the metadata print command, you will receive the »Print settings« dialog box, where you may specify the structure of the printout.

Note: The user must have reading rights on the entity. Prior to showing the print settings dialog box, the entity is automatically opened in reading mode.

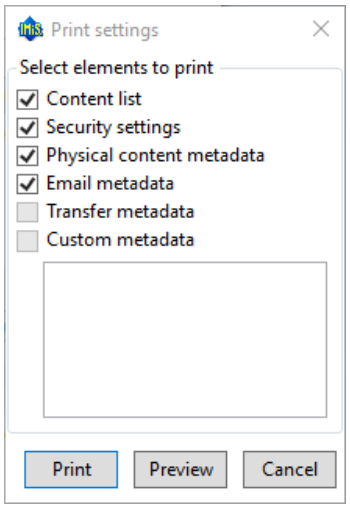


Image 158: Print settings dialog box

The printout always includes system metadata, and may optionally also include the following data:

- Content list for the entity.
- Security settings.
- Physical content metadata.
- Email metadata.
- Transfer metadata.
- Custom metadata.

2018 © Imaging Systems, Inc., All rights reserved.

By unchecking the boxes in the »Print settings« window, you remove particular data types from the printout.

By choosing »Print«, the selected metadata will print on the current default printer.

If you wish to preview the print or select another printer, use the »Preview« command.

You can also cancel printing using the »Cancel« command.

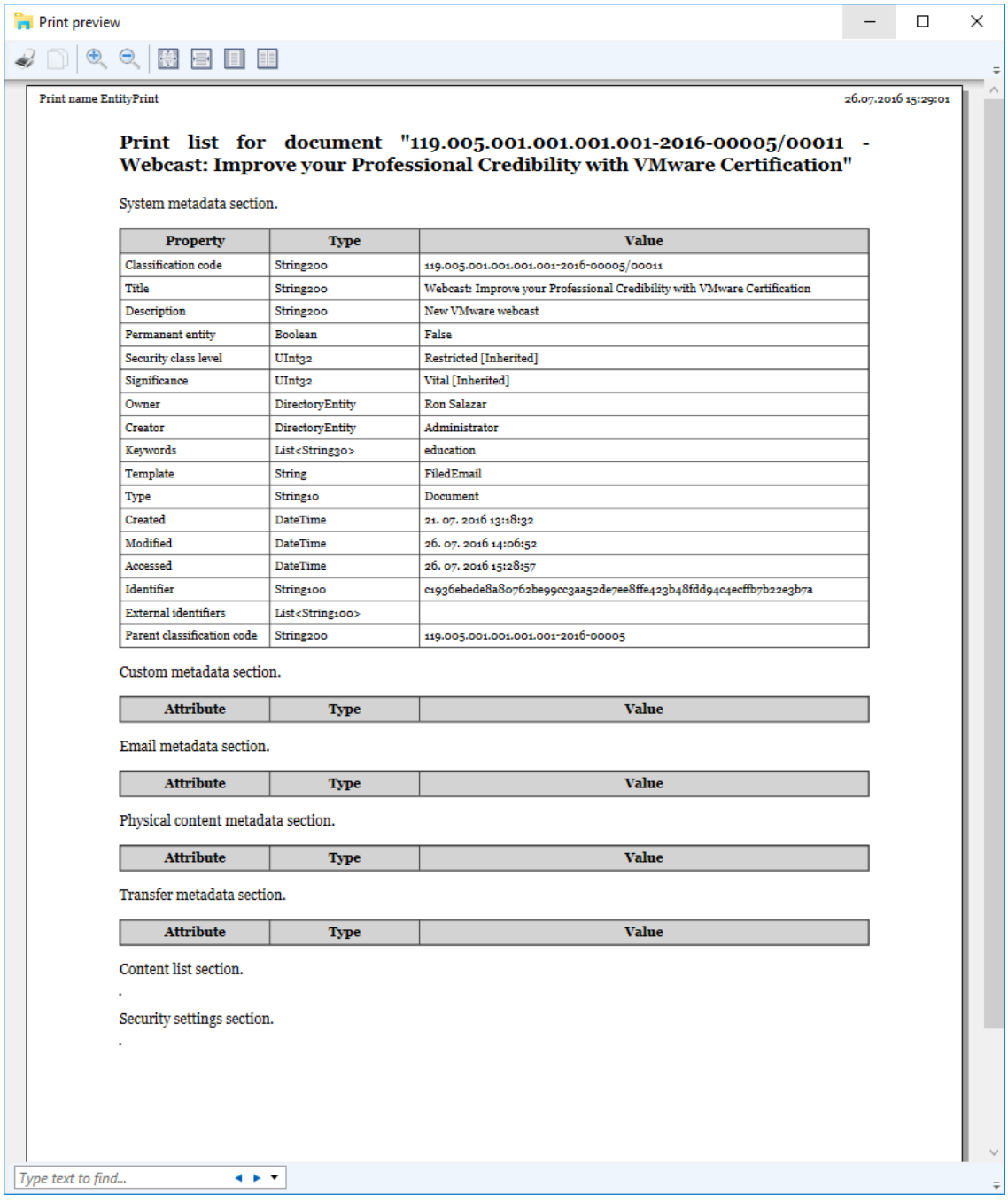


Image 159: Example document print preview

The »System property section« is the section of the printout related to the system metadata of the document. It is predefined and contains the following data:

- Classification code.
- Id of the entity.
- Type of entity.
- Created date and time.
- Modified last date and time.
- Accessed last date and time.
- Parent classification code.
- Title of the entity.
- Description.
- Keywords.

For each individual entity, the user specifies which user added metadata will be printed out in the »Metadata section«. The »Content list section« is the section of the printout related to document information. It contains the following data:

- Description.
- Extension.
- Content type.
- Size in bytes.
- Inserted date and time.
- Modified last date and time.
- Accessed last date and time.

The security settings that are printed out are the following:

- Subject.
- Group.
- Description.
- Permission type.
- Read permission.
- Write permission.
- Move permission.
- Delete permission.

2018 © Imaging Systems, Inc., All rights reserved.

- Modify security permission.
- Create entities permission.
- Valid from date.
- Valid to date.

The physical content metadata section contains the following information:

- Identifier.
- Description.
- Content status.
- Status changed date.
- Home location.
- Current location.
- Custodian.
- Date of expected return of checked out content.

The email metadata section of the printout contains the following information:

- Subject of email, which is also the title of the document.
- Date.
- From.
- To.
- To CC.
- To BCC.
- Priority.
- Message id.

4.2.12.4 Printing the classes of the classification scheme

Before printing, select a class whose classification scheme (all the child classes contained inside) you wish to print. If an archive server is selected, the printed list will include classes contained by the entire classification scheme.

Select a class in the top right view, or an archive server in the left view of Windows Explorer. By choosing a class or an archive server and right-clicking it, you will open a popup menu where you can choose »Print« and then »Classification scheme«.

2018 © Imaging Systems, Inc., All rights reserved.

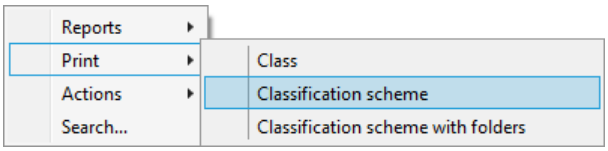
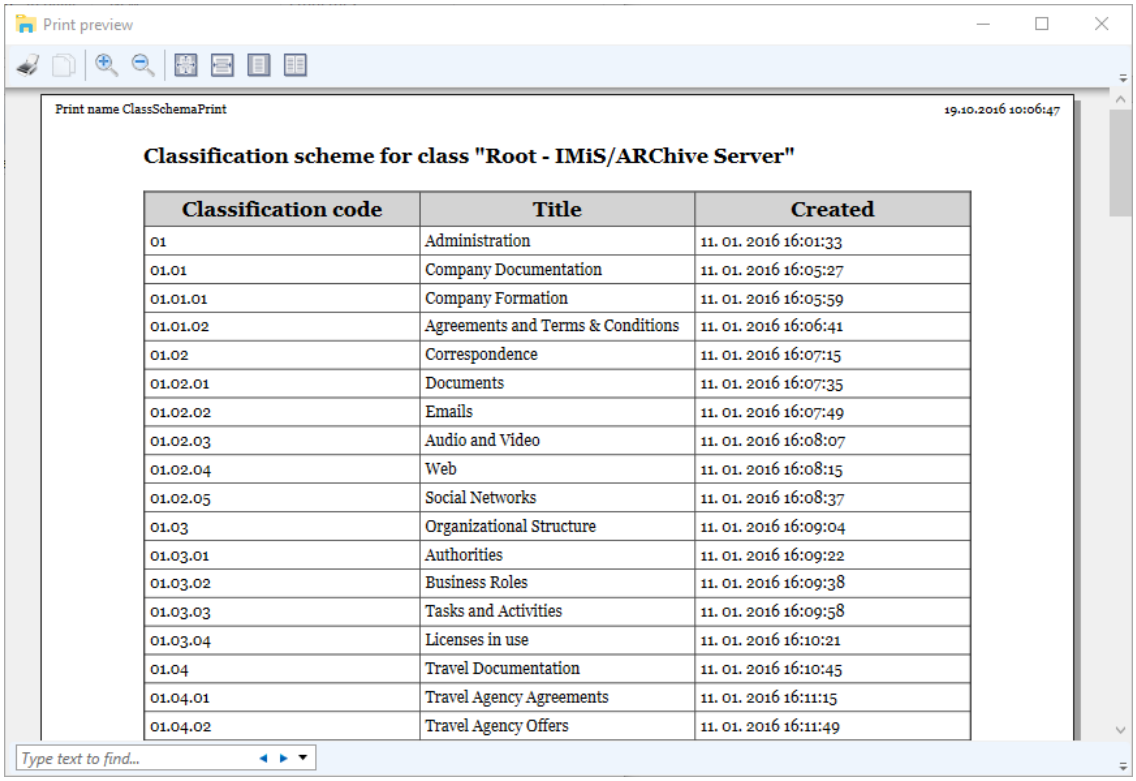


Image 160: Selection of classification scheme printing options

A »Print preview« window then appears, where the »Print« command is used to select a printer and print the preview. You can cancel the printing procedure by closing the preview window.



Classification code	Title	Created
01	Administration	11. 01. 2016 16:01:33
01.01	Company Documentation	11. 01. 2016 16:05:27
01.01.01	Company Formation	11. 01. 2016 16:05:59
01.01.02	Agreements and Terms & Conditions	11. 01. 2016 16:06:41
01.02	Correspondence	11. 01. 2016 16:07:15
01.02.01	Documents	11. 01. 2016 16:07:35
01.02.02	Emails	11. 01. 2016 16:07:49
01.02.03	Audio and Video	11. 01. 2016 16:08:07
01.02.04	Web	11. 01. 2016 16:08:15
01.02.05	Social Networks	11. 01. 2016 16:08:37
01.03	Organizational Structure	11. 01. 2016 16:09:04
01.03.01	Authorities	11. 01. 2016 16:09:22
01.03.02	Business Roles	11. 01. 2016 16:09:38
01.03.03	Tasks and Activities	11. 01. 2016 16:09:58
01.03.04	Licenses in use	11. 01. 2016 16:10:21
01.04	Travel Documentation	11. 01. 2016 16:10:45
01.04.01	Travel Agency Agreements	11. 01. 2016 16:11:15
01.04.02	Travel Agency Offers	11. 01. 2016 16:11:49

Image 161: Example classification scheme print

The printout of the classification scheme includes the following information in separate columns:

- Classification code.
- Title.
- Created time and date.

2018 © Imaging Systems, Inc., All rights reserved.

4.2.12.5 Printing the classes and folders of the classification scheme

Before printing, user select a class whose classification scheme including folders (all the child classes and sub-folders) user wish to print. If an archive server is selected, the printed list will include the classes and folders of the entire classification scheme.

Select a class in the top right view, or an archive server in the left view of Windows Explorer. By choosing a class or archive server and right-clicking it, you will open a popup menu where you can choose »Print« and then »Classification scheme with folders«.

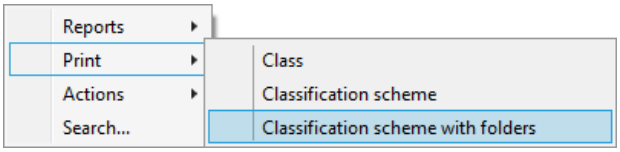
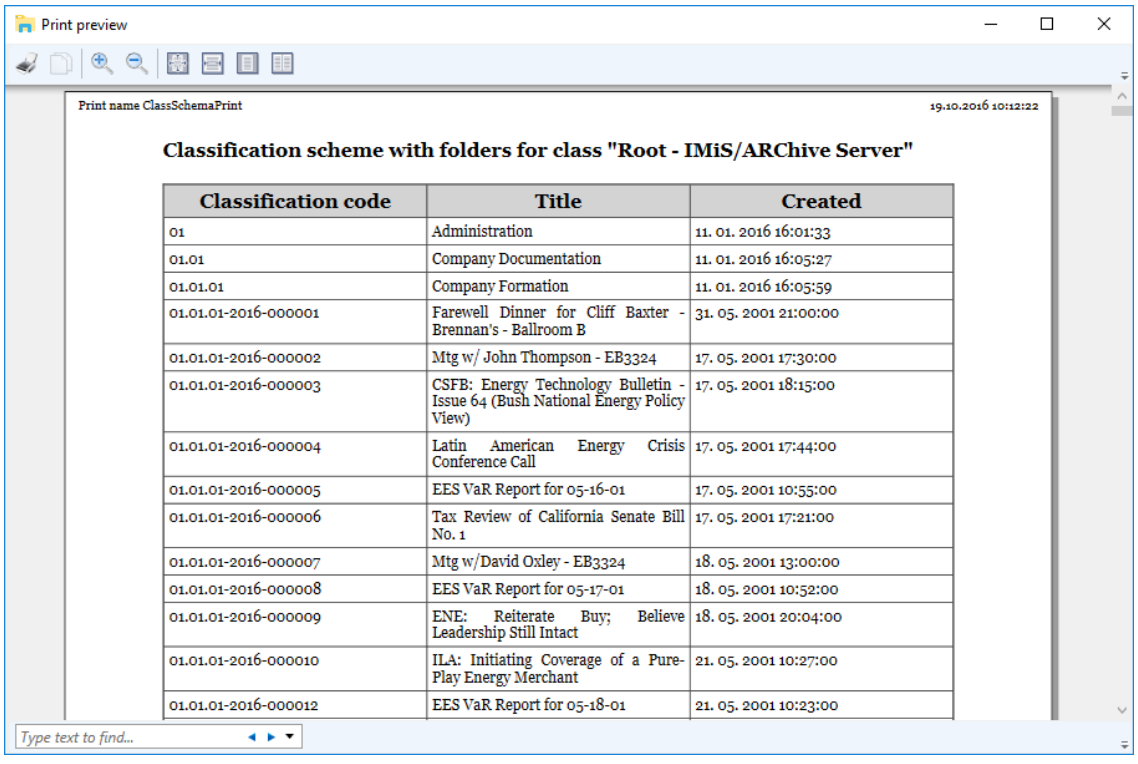


Image 162: Selection of classification scheme printing options

A »Print preview« window then appears, where the »Print« command is used to select a printer and print the preview. You can cancel the printing procedure by closing the preview window.



Classification code	Title	Created
01	Administration	11. 01. 2016 16:01:33
01.01	Company Documentation	11. 01. 2016 16:05:27
01.01.01	Company Formation	11. 01. 2016 16:05:59
01.01.01-2016-000001	Farewell Dinner for Cliff Baxter - Brennan's - Ballroom B	31. 05. 2001 21:00:00
01.01.01-2016-000002	Mtg w/ John Thompson - EB3324	17. 05. 2001 17:30:00
01.01.01-2016-000003	CSFB: Energy Technology Bulletin - Issue 64 (Bush National Energy Policy View)	17. 05. 2001 18:15:00
01.01.01-2016-000004	Latin American Energy Crisis Conference Call	17. 05. 2001 17:44:00
01.01.01-2016-000005	EES VaR Report for 05-16-01	17. 05. 2001 10:55:00
01.01.01-2016-000006	Tax Review of California Senate Bill No. 1	17. 05. 2001 17:21:00
01.01.01-2016-000007	Mtg w/David Oxley - EB3324	18. 05. 2001 13:00:00
01.01.01-2016-000008	EES VaR Report for 05-17-01	18. 05. 2001 10:52:00
01.01.01-2016-000009	ENE: Reiterate Buy; Believe Leadership Still Intact	18. 05. 2001 20:04:00
01.01.01-2016-000010	ILA: Initiating Coverage of a Pure-Play Energy Merchant	21. 05. 2001 10:27:00
01.01.01-2016-000012	EES VaR Report for 05-18-01	21. 05. 2001 10:23:00

Image 163: Example classification scheme with folders print from the preview

2018 © Imaging Systems, Inc., All rights reserved.

The printout of the classification scheme contains the following information in separate columns:

- Classification code.
- Title.
- Created date and time.

4.2.12.6 Printing reviews of the review process

Prior to printing, the user selects the review under which he will be printing the reviews. Each review created is located in the »Reviews« folder contained in the »Administration« system folder. Users with the »Read« right have access to the »Reviews« folder. This right is set by the administrator in the scope of specifying access rights via the configuration interface in the »Context[Reviews]«. For more information on setting access rights for administrative folders see chapter »Access control« Folder. Printing reports is limited to users with assigned »Reports« role. By right-clicking on the selected review, the user is shown a pop-up menu. The user selects the »Print - Review« command.

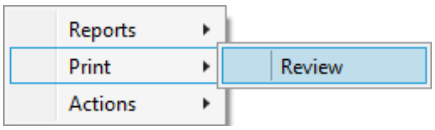


Image 164: Selecting the option of printing reviews

The Print preview window appears in which the user selects the printer by selecting the »Print« command and prints the preview. If the user wishes to cancel the printing procedure, he closes the preview window.

2018 © Imaging Systems, Inc., All rights reserved.

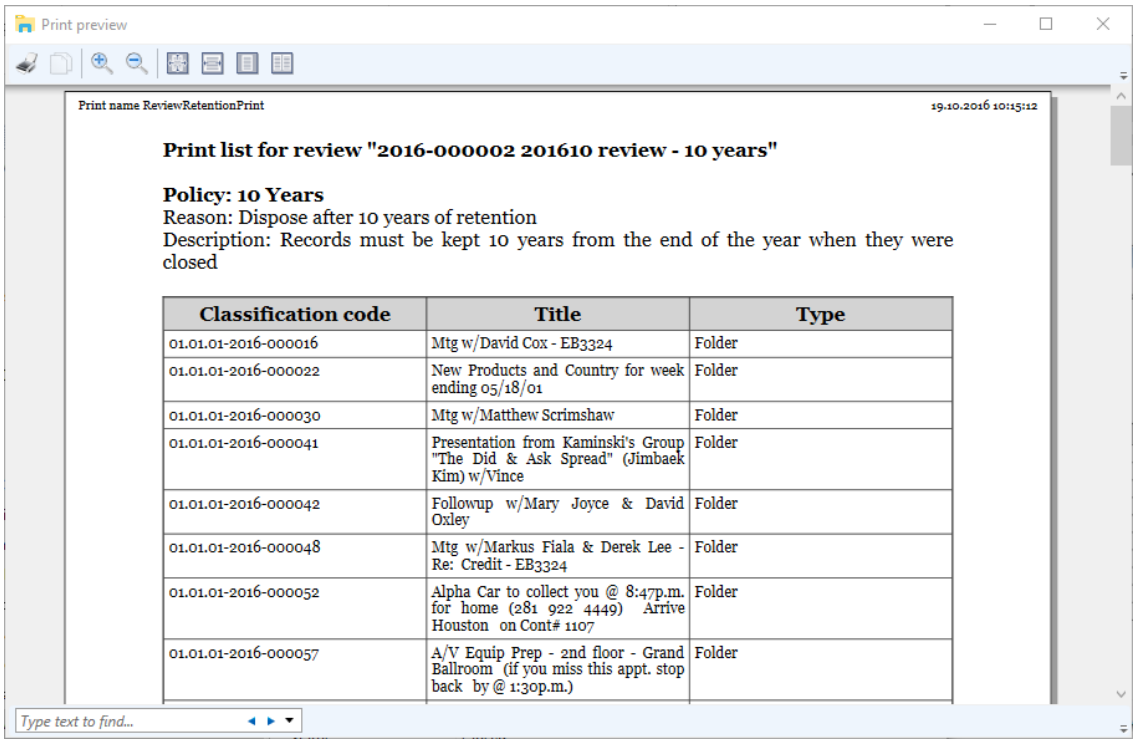


Image 165: Example of printing selected entities classified by retention policies

Printouts differ depending on the type of review. With »Regular« reviews list of entities included in the review are sorted by retention periods.

The printout of retention periods contains the following data for each retention period:

- »Policy«: title of the retention period.
- »Reason«: the reason for creating a retention period.
- »Description«: a short description of the retention period.

With »Ad hoc« reviews list of entities for the selected query is displayed.

It includes the following data:

- »Query«: an expression for searching entities included in the review.
- »Description«: a brief description of the review.
- »Comments«: an entry of various comments, explanations and other information connected to the review process.

2018 © Imaging Systems, Inc., All rights reserved.

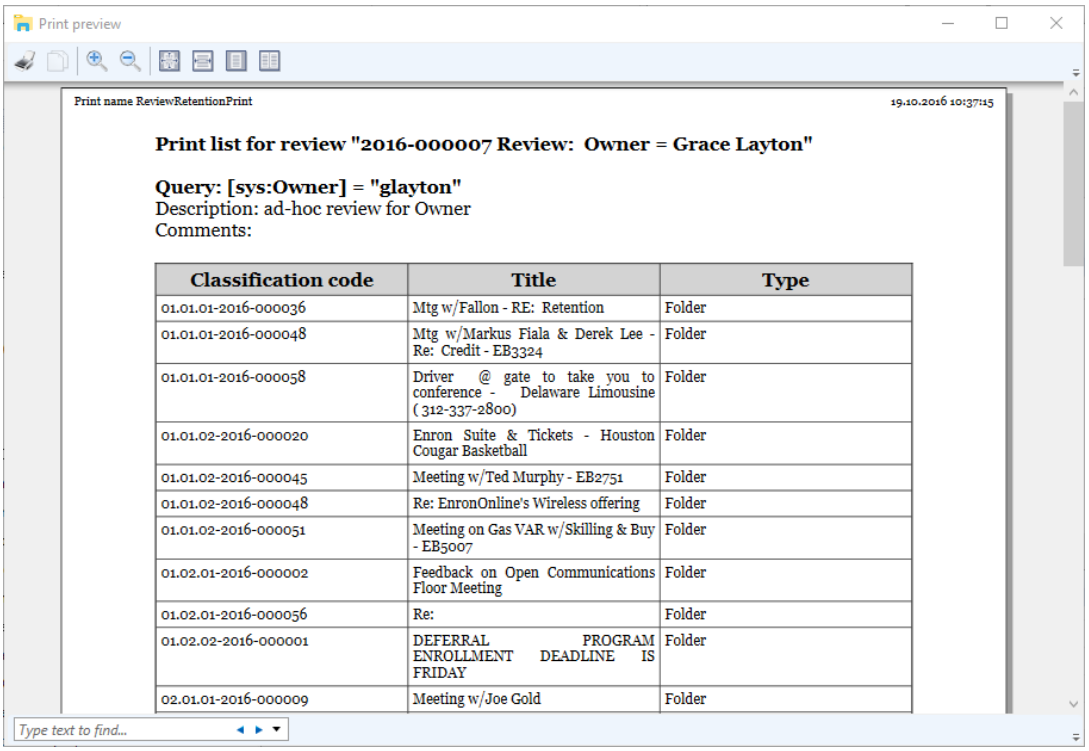


Image 166: Example of printing selected entities for the selected query

A list of selected entities is printed for each review, which contains the following data:

- »Classification code« of the selected entity.
- »Title« of the selected entity.
- »Type« of the selected entity (class, folder, document).

4.2.13 Import

The IMiS®/Client enables the import of entities to the IMiS®/ARChive Server together with their metadata. Entities, which can only be imported by a user who has the »ImportExport« permission (role), must be prepared in the prescribed XML form.

Import may be performed into the root class of the classification scheme or into any chosen class or folder. For more information on the import file format and file structure see chapter Format of the import/export file. For more information on server roles / permissions see chapter Access in the IMiS®/ARChive Server manual.

Select an archive server in the left view of Window Explorer.

If you wish to perform import into a class or folder, select it in the classification scheme or in the list of entities. By selecting an archive, a class or a folder and right clicking, you will open a popup menu where you can choose »Actions« and then the »Import« command (user must have »Transfer« permission (role) on the archive server).

2018 © Imaging Systems, Inc., All rights reserved.

Image 167: Importing content via the popup menu

After choosing »Import«, you will receive the »Select file for import« dialog box, where you select the XML file with the list of entities you wish to import.

In case the list was obtained by using the »Export« or »Transfer« commands, the XML's name will be »ExportReport«.

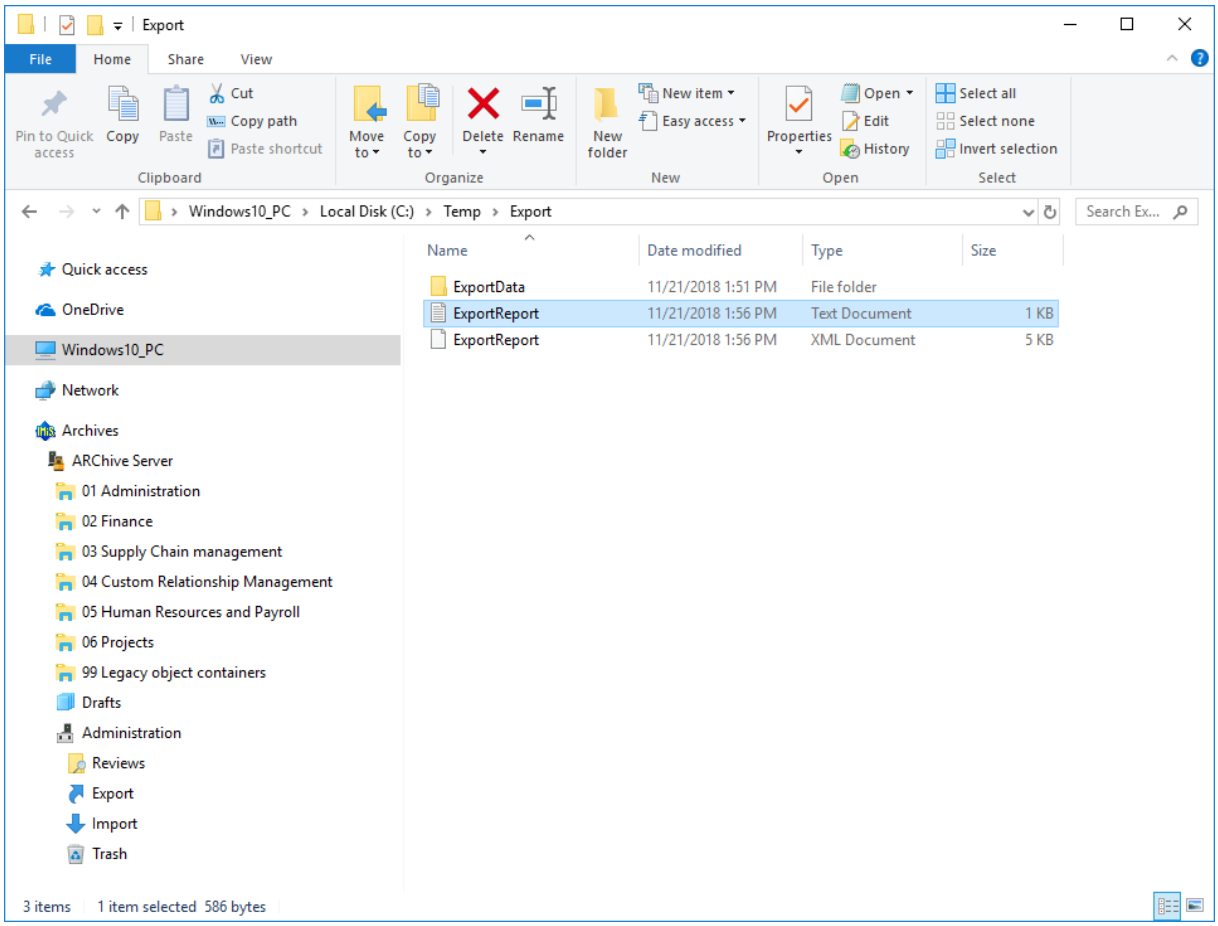


Image 168: Selection of the XML import list

The import procedure is started by choosing the »Open« command. It can be canceled by using the »Cancel« command.

Users finish the import procedure by selecting a digital certificate used to sign the XML report file according to the XML Signature standard. This ensures that the authenticity of the report, and the imported files themselves, can be verified.

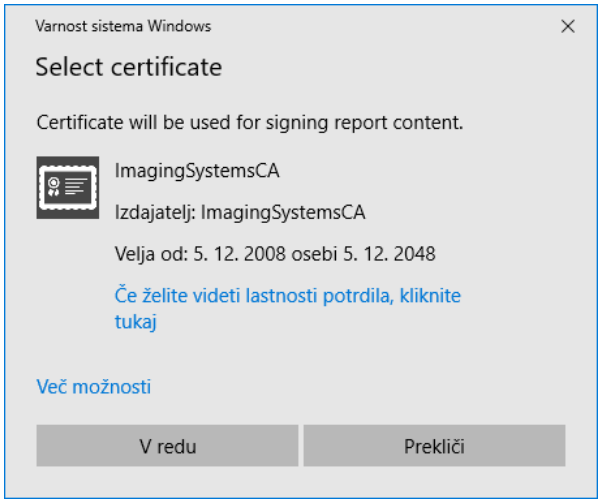


Image 169: Selecting a digital certificate when importing

Warning: Import will be successful even when the user does not select a digital certificate. If a digital certificate is not selected, the import record file will not be signed.

When the import procedure is completed, a popup window appears in the bottom right view of Windows Explorer showing the import success rate. For each entity type, the number of successfully imported entities is listed compared to the total number of entities in the import list. The import success rate popup stays open until you click anywhere outside it.

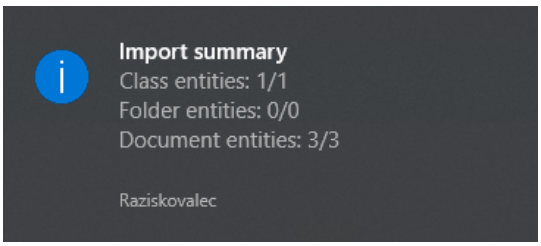


Image 170: Display of the import complete message with success rate statistics

2018 © Imaging Systems, Inc., All rights reserved.

By clicking on a pop-up window, the user can display detailed information about the import (separate case).

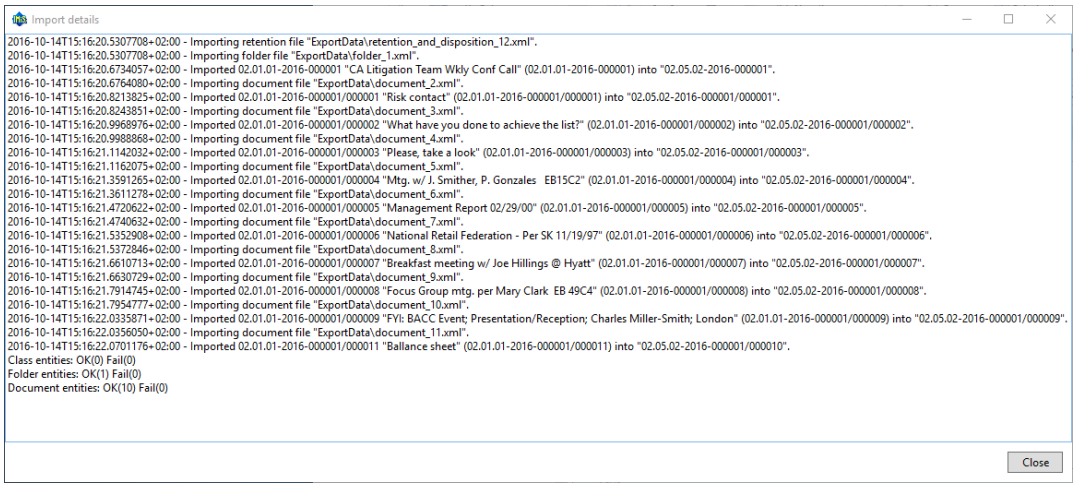


Image 171: A display of a detailed report of the import

Warning: When importing entities an error occurs »Empty security class not allowed« if the entity under which the user imports the entities doesn't have a set security class. The import of the entity is not carried out.

4.2.13.1 Import procedure

At the start of the import procedure, the IMiS®/Client 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.

2018 © Imaging Systems, Inc., All rights reserved.

- »ImportReport_ERROR.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.

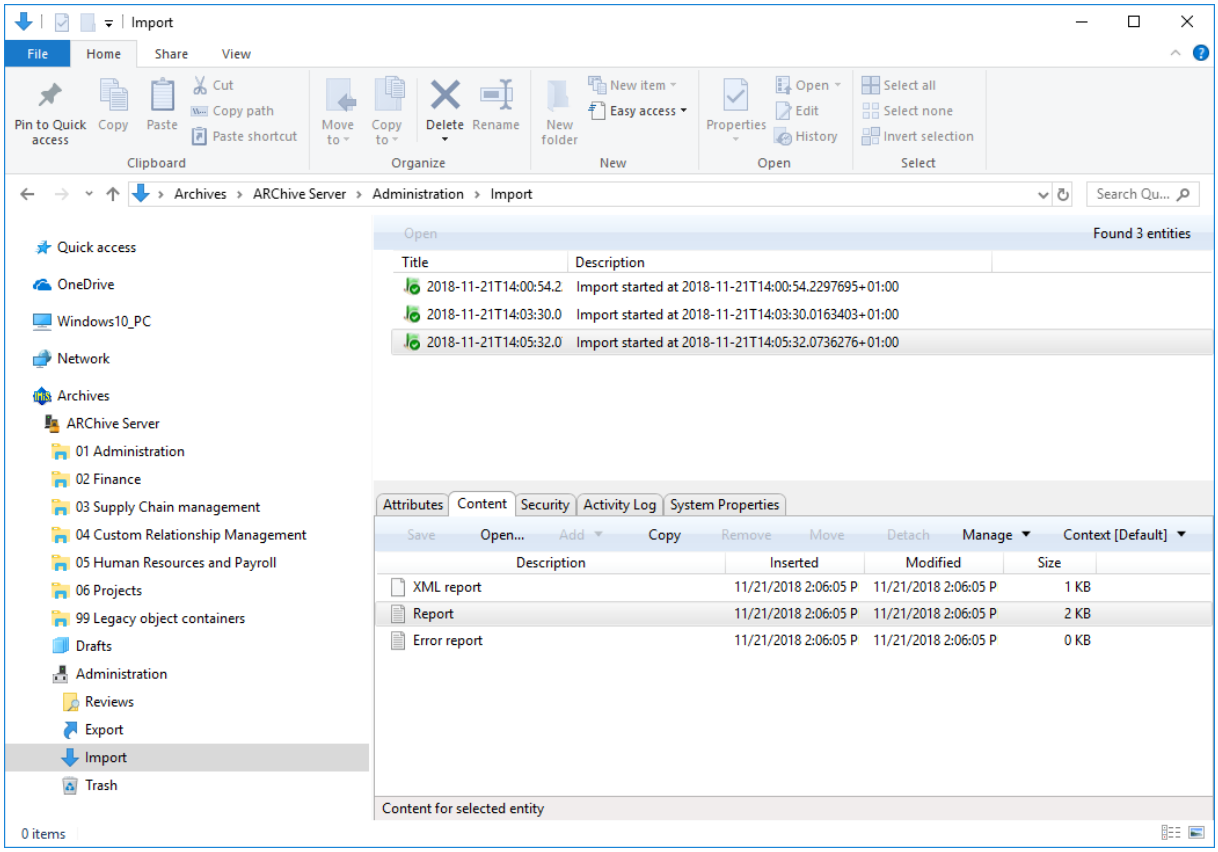


Image 172: Display of the import report in the »Import« system folder

4.2.14 Export

The IMiS®/Client enables the export of entities from the IMiS®/ARChive Server.

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 export/import file.

For more information on server roles see chapter Access in the IMiS®/ARChive Server Manual.

To begin exporting, select an archive server in the left view of Windows Explorer.

If you wish to export a specific entity, first select it in the classification scheme or in the list of entities. When an archive or entity is selected, you can right click it to open a popup menu where you can choose »Actions« and then the »Export« command (user must have »ImportExport« role on the archive server).

Image 173: Exporting records via the popup menu

After choosing the »Export« command, the user receives a dialog box for setting the export parameters.

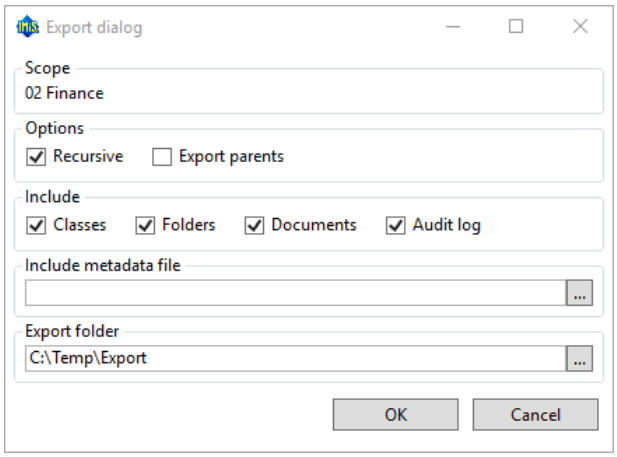


Image 174: Export settings in the dialog box

In the »Scope« section, the user checks whether he wishes to export to the root class of the archive, or an entity currently selected in the classification scheme. The default classification code and title of the selected archive, class or folder means that, in addition to the selected entity, all other contained entities are exported too.

In the »Options« section, you can choose to additionally export:

- All the recursively contained entities – »Recursive«.
- All the parent entities – »Export parents«.

In the »Include« section, you can choose the types of entities to be included in the export:

- Classes
- Folders
- Documents.

By choosing »Audit log«, you can also export the audit log for individual exported entities.

By clicking the button »...« in the section »Include metadata file« the user opens a dialog box for the selection of an XML file with the additional metadata that should 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.

By clicking the button »...« in the »Export folder« section, the user opens a popup window for the selection of the folder where entities in XML format will be exported.

2018 © Imaging Systems, Inc., All rights reserved.

The command »OK« begins the export procedure. The export can be cancelled using the »Cancel« command.

The export procedure is completed with the selection of a digital certificate used to sign the export report XML file using the XML Signature standard. This ensures that the authenticity of the report, and the exported files, can be verified.

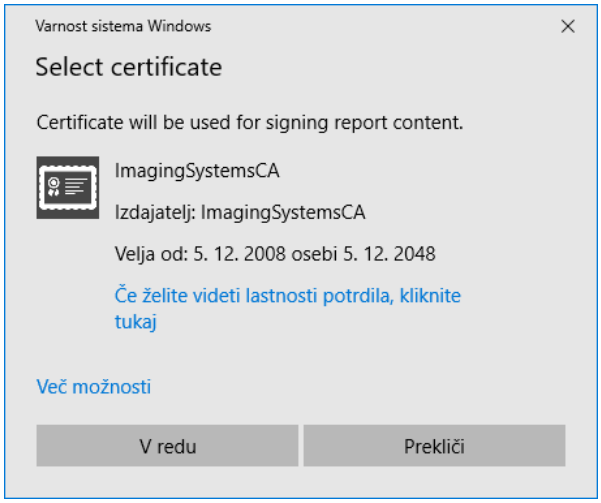


Image 175: Selecting a digital certificate when exporting

Warning: Export will be successful even when the user does not select a digital certificate. If a digital certificate is not selected, the export record file will not be signed.

When the export procedure is completed, a popup window appears in the bottom right view of Windows Explorer showing the export success rate. For each entity type, the number of successfully exported entities is listed compared to the total number of entities that were queued for export. The export success rate popup stays open until you click anywhere outside it.

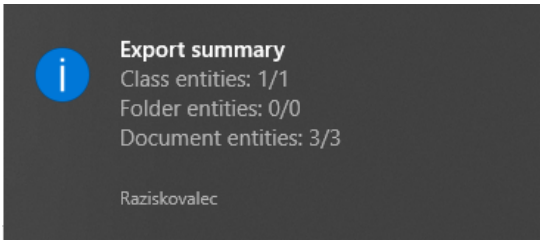


Image 176: Display of the export complete message with success rate statistics

By clicking on a pop-up window, the user can display detailed information about the export (separate case).

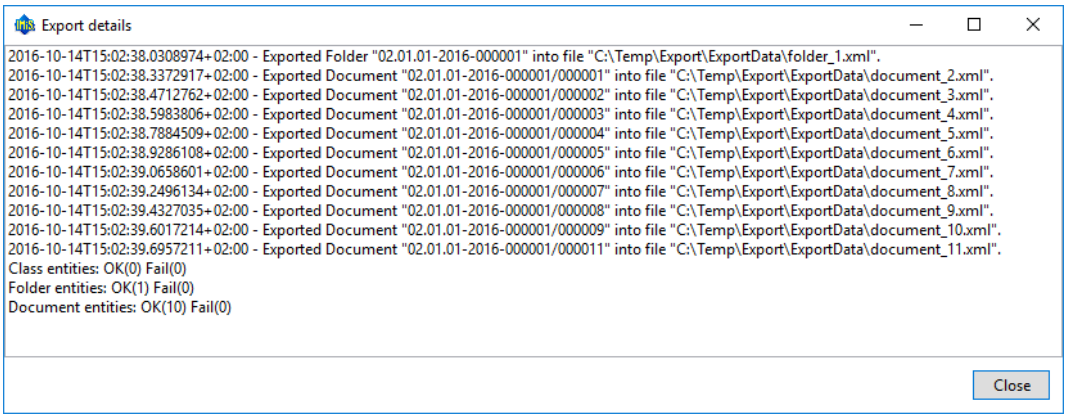


Image 177: A display of a detailed report of the import

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.

4.2.14.1 Export procedure

At the start of the export procedure, the IMiS®/Client 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 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.

2018 © Imaging Systems, Inc., All rights reserved.

When all entities are exported, the »ExportReport.xml« file is electronically signed with the selected digital certificate using the XMLDSIG standard. This ensures the authenticity of the export report and the exported files.

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, the other sub-entities will still be exported, providing the export of the parent entity was successful.

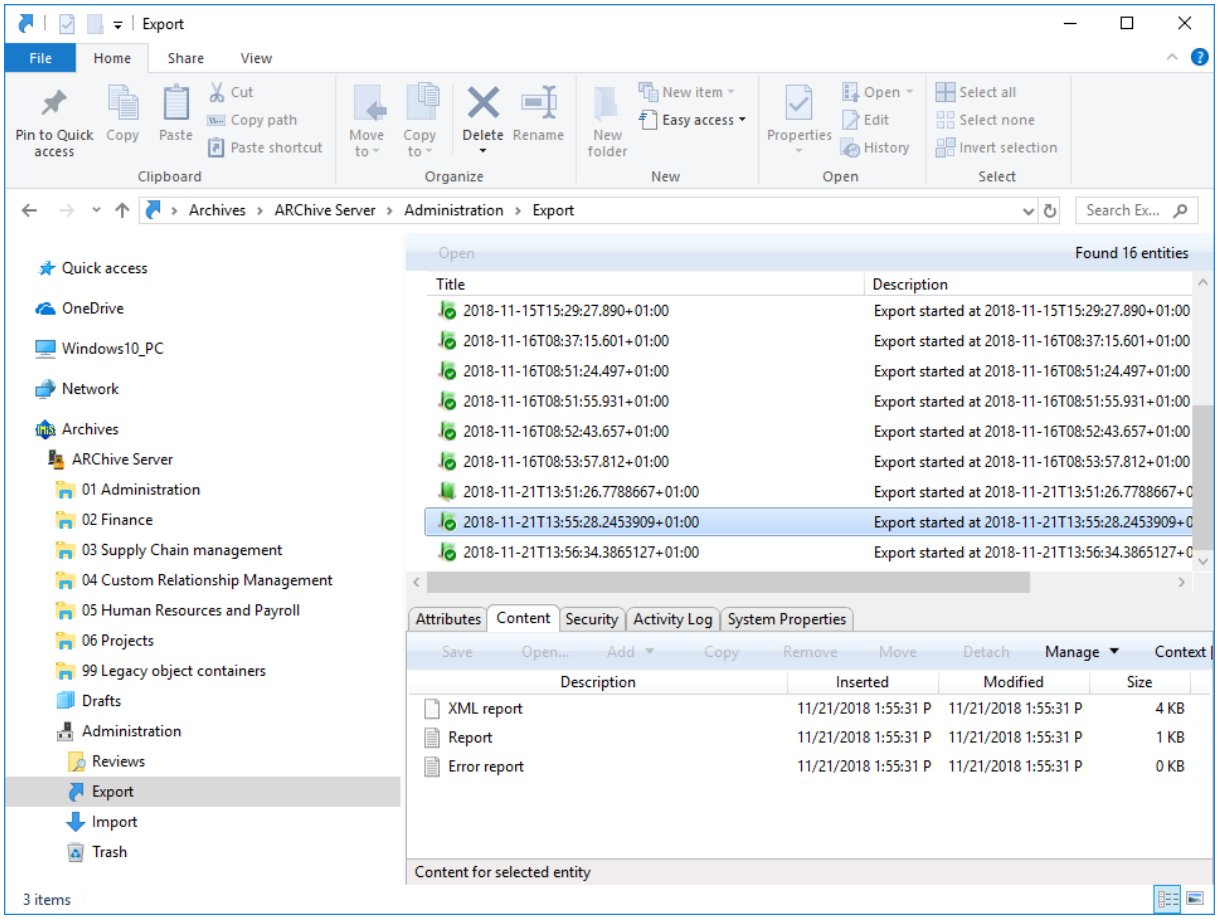


Image 178: Display of the export report in the »Export« system folder

2018 © Imaging Systems, Inc., All rights reserved.

4.2.15 Move

The IMiS®/Client 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 entities within the classification scheme, select the entity you wish to move, choose »Actions« and then the »Move« command. You can find the »Actions« section via:

- Command bar of Windows Explorer.
- Right-click popup menu in the classification scheme overview.
- Right-click popup menu in the list of entities.

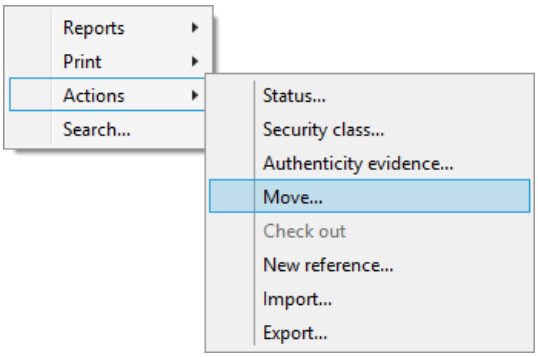


Image 179: Popup menu where the »Move« command is found

When selecting the »Move« command, you will receive the »Move entity« dialog box, where the »Move to« field is used to enter the classification code of the new parent entity, and the »Reason to move« field is used to enter the reason for the move.

The move of the entity is confirmed using the »OK« button.

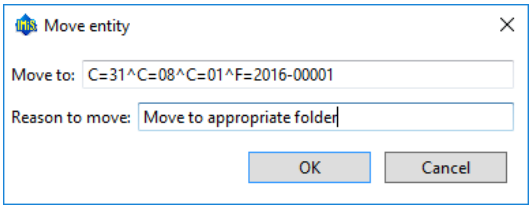


Image 180: Move entity dialog box

The classification code serves as a unique locator of the entity within the classification scheme and appears in canonical form. It consists of the relative classification codes of the entities, which are made of prefixes that specify the type of entity and its value, and are separated by the character »^«. The prefixes are as follows:

- »C=« for classes.
- »F=« for folders.
- »D=« for documents.

Example: The canonical form of the classification code of document 0001 located inside folder 2018-01, which is located inside class 002, which is located inside class 01 looks like this: C=01^C=002^F=2018-01^D=0001

For more information on classification codes in canonical form see chapter Access in the IMiS®/ARChive Server Manual.

When a moved entity is opened in the reading or editing mode, it has a new section called »Move« under the »System properties« tab in the bottom right view of Windows Explorer. The section »Move« shows the metadata of the moved entity. For more information see chapter Moved entity attributes.

Warning: The following rules apply when a user is moving entities:

- *All entities can be moved, no matter if they are closed or open.*
- *Several entities can be moved simultaneously when they are selected together in the list of entities.*
- *Classes can be moved directly into the root of the archive by leaving the »Move to« field empty, and only completing the »Reason to move« field. When moving an entity, be careful that its security class is not »Inherited« but always explicitly set.*
- *Documents that are situated directly inside a class cannot be moved inside folders, and documents situated in a folder cannot be moved directly inside a class.*

4.2.16 Delete

The IMiS®/Client enables two ways of removing an entity from the classification scheme:

- Immediate deletion.
- Marking an entity for later deletion (delete queue).

2018 © Imaging Systems, Inc., All rights reserved.

A user must have the appropriate access rights to execute any of these two actions.

4.2.16.1 Immediate 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.

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

Note: Classes or folders that contain entities cannot be deleted. The same is true for all closed entities (the value of the »Status« attribute is »Closed«).

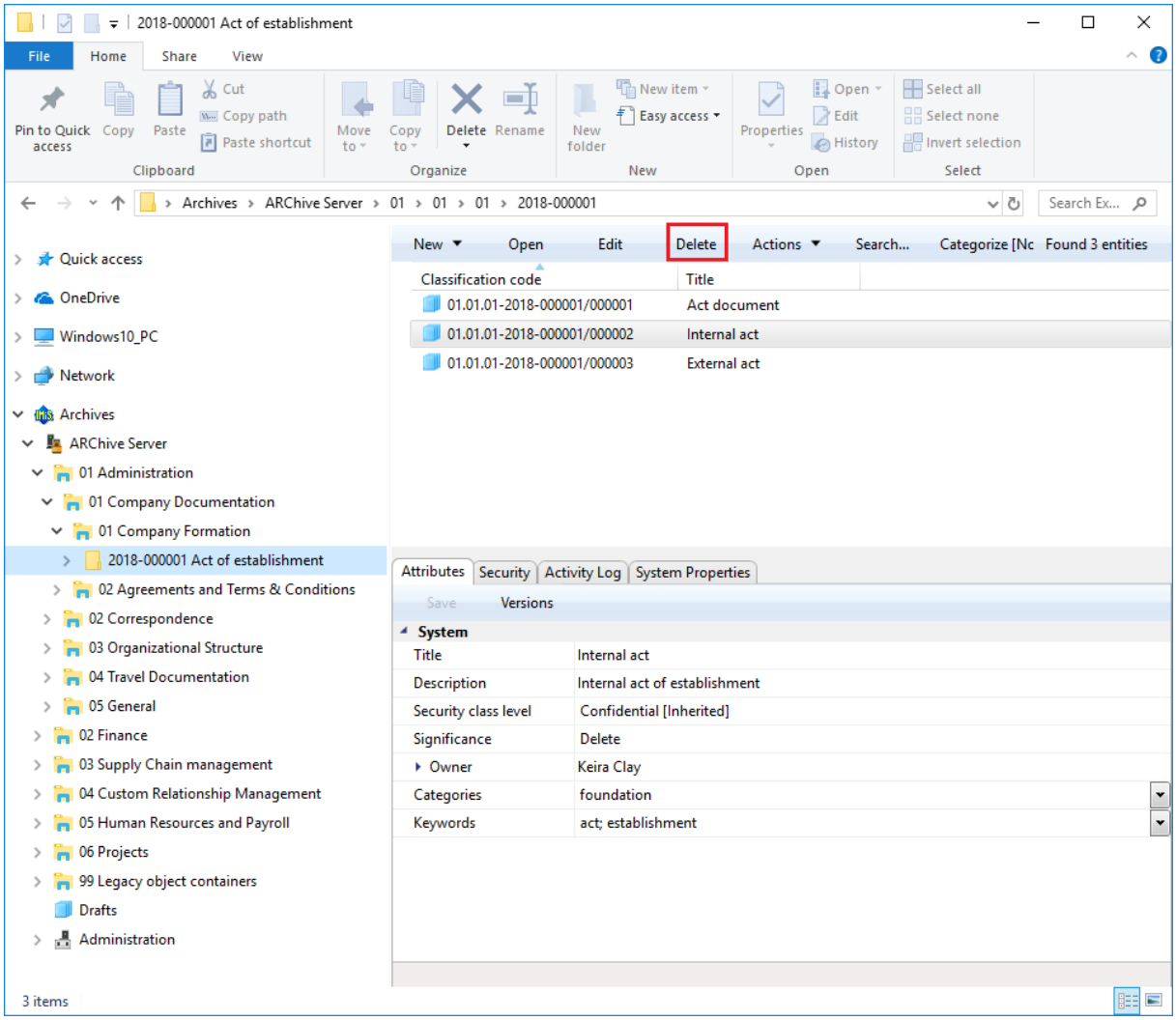


Image 181: Deleting an entity via the command bar

To delete an entity, first select an archive server in the left view of Windows Explorer. Find and select the entity you wish to delete. By choosing the »Delete« command in the top command bar, or by pressing the »Delete« key, you will open the entity deletion dialog box.

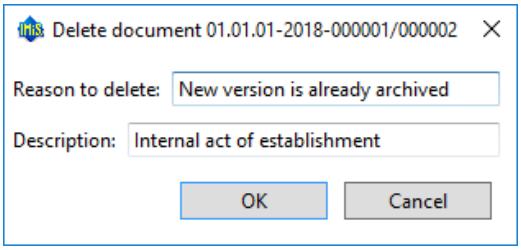


Image 182: Entity deletion dialog box

Enter the »Reason to delete« into the appropriate field, which is mandatory. Since the entity's description is an optional metadata that becomes mandatory when the entity is being deleted, you are now able to change it. If the entity contains no description and you attempt to delete it, the server will deny the request. Once the mandatory fields are completed, deletion is executed by choosing »OK«, or it can be cancelled by choosing »Cancel«.

Following deletion, the entity is removed from its previous class or folder and goes into the »Trash« system folder. The following attributes remain unchanged on the entity: classification code, title and description. All other metadata is removed.
A deleted entity receives the following new attributes:

- »Date deleted«: date and time of deletion.
- »Agent«: the user who executed the delete action.
- »Reason«: reason for deletion as it was input by the agent.

Classification code	Title	Description	Reason	Date deleted	Agent	Reference
02.01.01-2016-000001/000010	FW: Seminars, Forums, Conferences Sub Group	Seminar & Forum	Invitation is not actual any	14. 10. 2016 15:02:24	Administrator	

Image 183: Display of a deleted entity's metadata

The entity is no longer accessible in the classification scheme, and remains visible only in the »Trash« report.

4.2.16.2 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 Entity information.

2018 © Imaging Systems, Inc., All rights reserved.

All types of entities can be marked for later deletion. The procedure is as follows:

1. Find and select the entity you wish to mark for later deletion.
2. By choosing the »Edit« command or pressing the »F2« key, the selected entity is opened in editing mode.
3. In the first tab »Attributes« in the section »System«, 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.

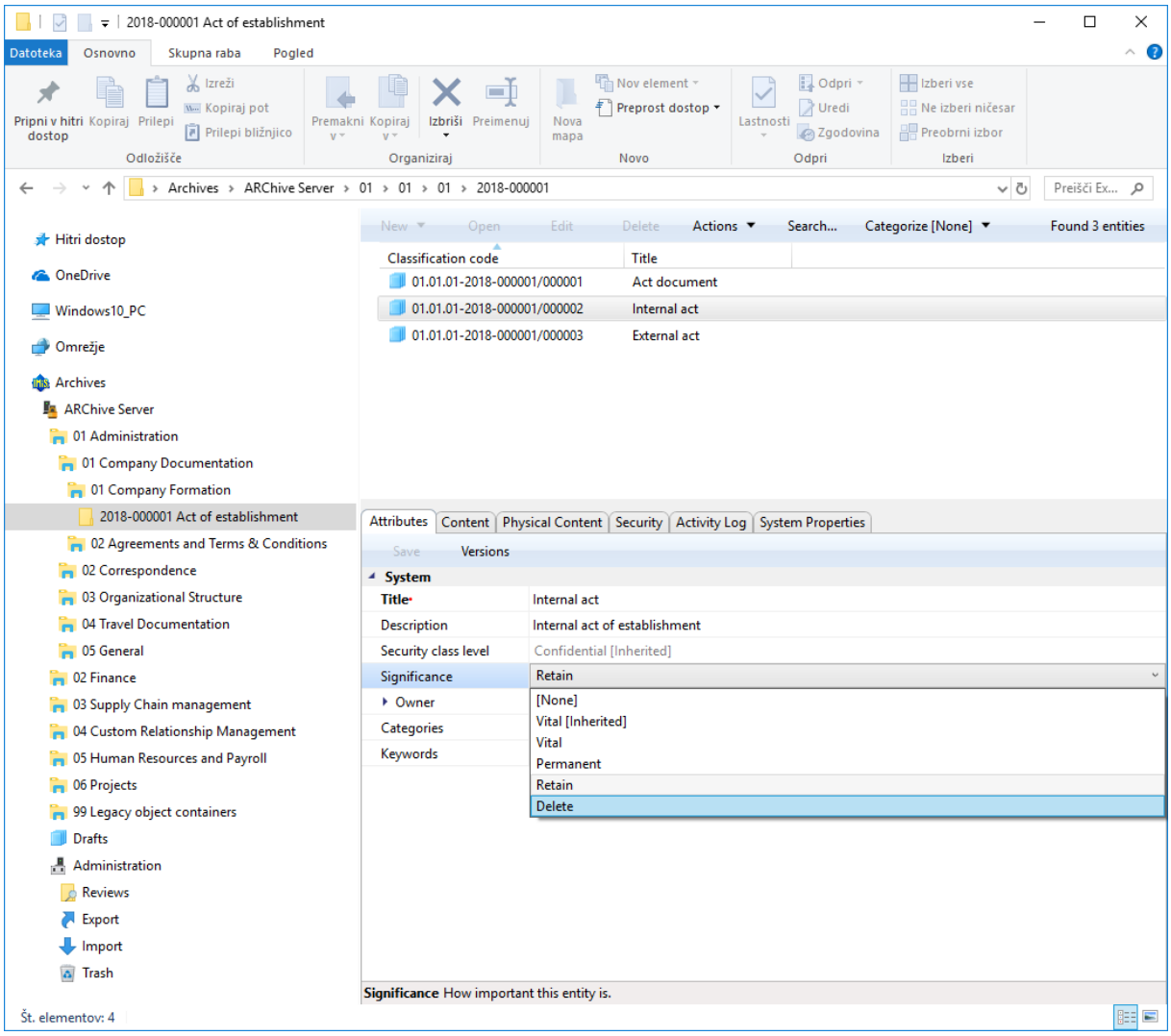


Image 184: Marking an entity for later deletion

4.2.16.3 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.

Note: User with appropriate rights can limit user access to the »Queue« folder by assigning explicit Deny Read right to users in the configuration folder »Access Control« in the context »Deleted«.

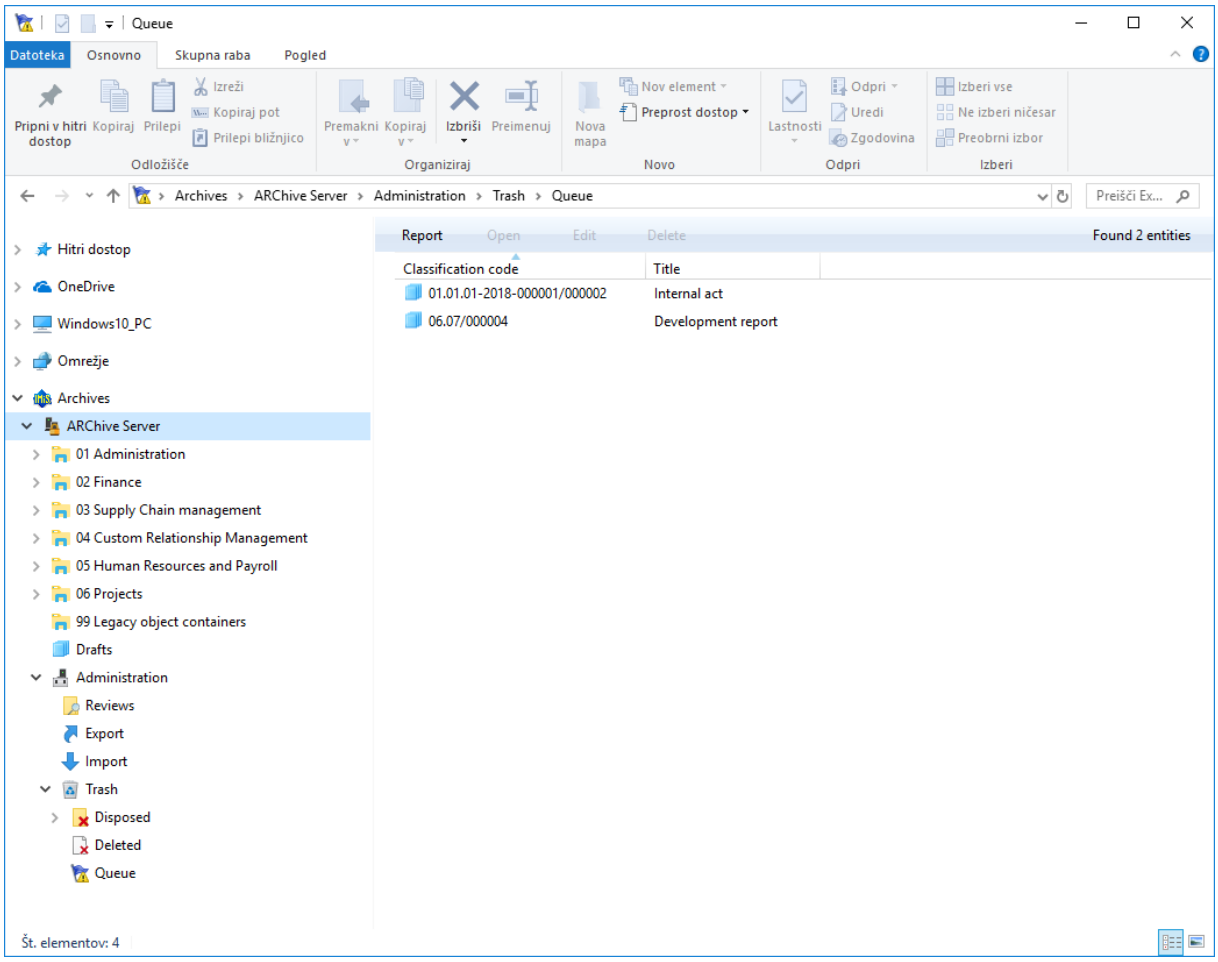


Image 185: List of entities marked for deletion in the »Queue« folder

By selecting the »Queue« folder, the bottom right view shows all the entities that were marked for deletion by various users. In this overview, the classification code is expressed as an absolute value. 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 top command bar or pressing the »Delete« key. The deletion procedure is outlined in chapter Immediate deletion of an entity.

2018 © Imaging Systems, Inc., All rights reserved.

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 or pressing the »F2« key, the selected entity is opened in editing mode.
3. In the first tab »Attributes«, under the section »System«, 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, and the entity will be removed from the list.

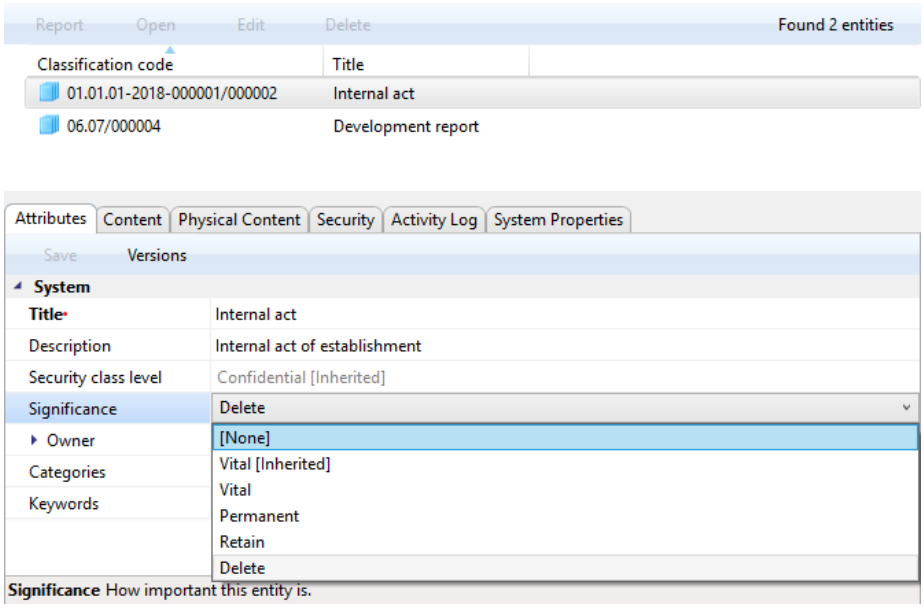


Image 186: Removing an entity from the delete queue list

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.

2018 © Imaging Systems, Inc., All rights reserved.

4.2.17 Changing the status of an entity

To change the status of an entity, the user must have the »Change status« access right on the entity. Changing the status of existing entities in the IMiS®/Client is done using the »Status« command, which is available for the selected entity in the »Actions« section accessible in the:

- Command bar of Windows Explorer.
- Right-click popup menu in the classification scheme.
- Right-click popup menu in the list of contained entities.

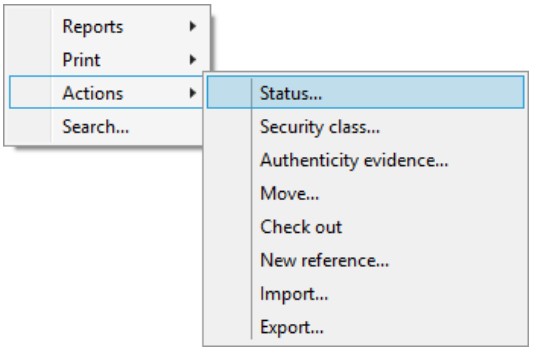


Image 187: Popup menu for choosing the »Status« command

In the »Set entity status« dialog box, the user selects the desired status from a pick list offered in the »Status« field. The list only shows values other than the current status of the entity.

The following predefined status values are possible:

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

The user writes a reason for the status change in the »Reason to change« field.
The change of status for the selected entity is confirmed using the »OK« button.

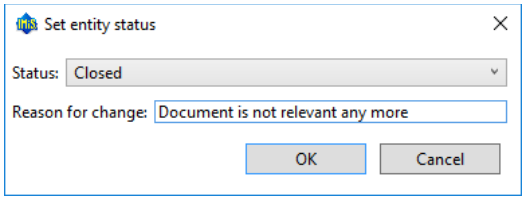


Image 188: Status change dialog box

2018 © Imaging Systems, Inc., All rights reserved.

4.2.18 Changing the security class

To change an entity's security class, the user must have the »Change security class« access right on the entity. Changing the security class of an entity in the IMiS®/Client is done using the »Security class« command, which is available for the selected entity in the »Actions« section accessible in the:

- Command bar of Windows Explorer.
- Right-click popup menu in the classification scheme.
- Right-click popup menu in the list of contained entities.

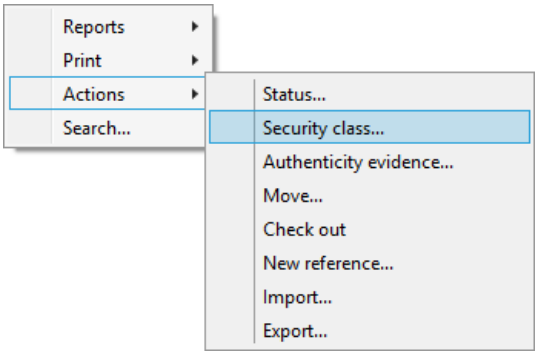


Image 189: Popup menu for choosing the »Security class« command

In the »Set entity security class« dialog box, the user selects the desired security class from a pick list offered in the »Security class« field. The list only shows values lower or equal to the user's own security class level.

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

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

2018 © Imaging Systems, Inc., All rights reserved.

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

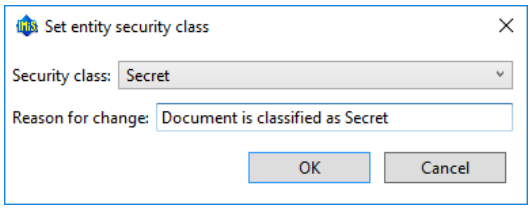


Image 190: Dialog box for changing the security class

4.2.19 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 in the chpter Rules in the IMiS®/ARChive Server Manual.

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

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

This command is found in the »Actions« section accessible via the:

- Command bar of Windows Explorer.
- Right-click popup menu in the classification scheme.
- Right-click popup menu in the list of contained entities.

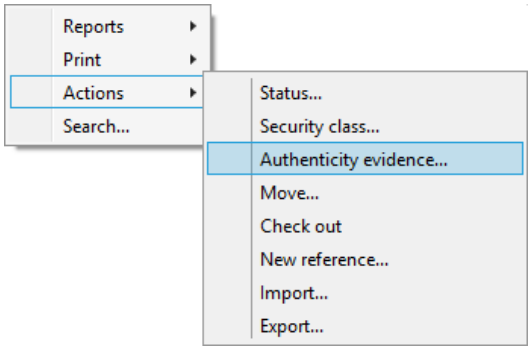


Image 191: Popup menu for choosing the »Authenticity evidence« command

2018 © Imaging Systems, Inc., All rights reserved.

When choosing »Authenticity evidence«, the user receives a dialog box for the selection of the folder where the evidence files should be exported. The export of evidence is confirmed using the »OK« button.

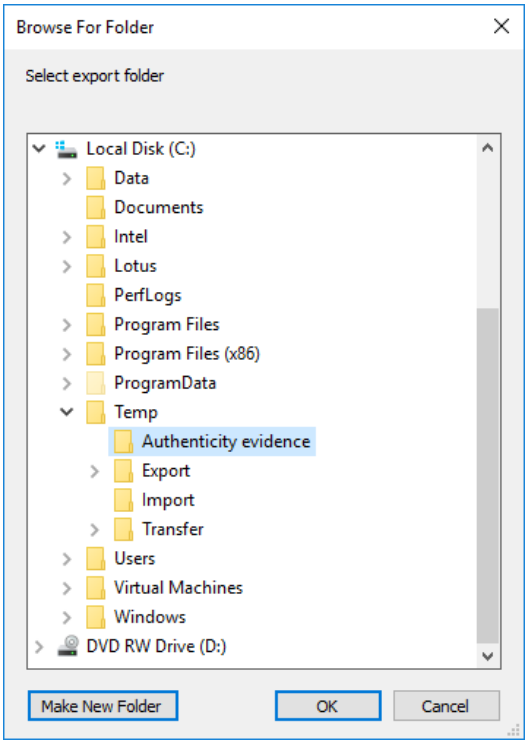


Image 192: Dialog box for selecting the export folder of authenticity evidence files

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.

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.

2018 © Imaging Systems, Inc., All rights reserved.

```
<?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>0NPJp3qfSkFm...T5irp0T+SrJMp+VE=</ds:DigestValue>
                </aip:ContentValue>
        </aip:Content>
</aip:AIP>
```

Image 193: 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>RiHMqrhrGATA/fDYJVO2lVg4fTw=</DigestValue>
<DigestValue>dawWHxN2IuddA7O+NGHYNd3ApG8=</DigestValue>
</Sequence>
<Sequence Order="2">
<DigestValue>vqBElqW7kGPUaFB/g6tfUFWwylE=</DigestValue>
</Sequence>
</HashTree>
<TimeStamp>
<TimeStampToken Type="XMLENTRUST">
<dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Id="TimeStampToken">
<dsig:SignedInfo>
<dsig:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
```

2018 © Imaging Systems, Inc., All rights reserved.

<dsig:Reference URI="#TimeStampInfo-13ED106F54C2C33ED420000000000007BD7">
<dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<dsig:DigestValue>fWwSCkW04udY+/kvwMgL59scG3k=</dsig:DigestValue>
</dsig:Reference>
<dsig:Reference URI="#TimeStampAuthority">
<dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<dsig:DigestValue>j8bwhFukHoD6jcjmzgEZtXDF/ko=</dsig:DigestValue>
</dsig:Reference>
</dsig:SignedInfo>
<dsig:SignatureValue>J5Vmm9HR9gYzPouh... ELWNov32qUw==
</dsig:SignatureValue>
<dsig:KeyInfo Id="TimeStampAuthority">
<dsig:X509Data>
<dsig:X509Certificate>MIIFYDCCBEi...InphHBlzxEkFU3</dsig:X509Certificate>
</dsig:X509Data>
</dsig:KeyInfo>
<dsig:Object Id="TimeStampInfo-13ED106F54C2C33ED420000000000007BD7">
<ts:TimeStampInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:ts="http://www.entrust.com/schemas/timestamp-protocol-20020207">
<ts:Policy id="http://www.si-tsa.si/dokumenti/SI-TSA-politika-za-casovni-zig-1.pdf"/>
<ts:Digest>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>kKsYK3bWkp5Zc/wbgssA/XIbNsA=</ds:DigestValue>
</ts:Digest>
<ts:SerialNumber>108487637460...6624147310345175</ts:SerialNumber>
<ts:CreationTime>2014-04-02T09:45:00.093Z</ts:CreationTime>
<ts:Nonce>794941113917975O976</ts:Nonce>
</ts:TimeStampInfo>
</dsig:Object>
</dsig:Signature>
</TimeStampToken>
<CryptographicInformationList>
<CryptographicInformation Order="1"
Type="CERT">MIIEHDCCAwSgBAgIE...z90z6gk/2vorAfGEhuB9nBxVeoQp</CryptographicInformation>
<CryptographicInformation Order="2"
Type="CRL">MIISKTCCERECAQEwDQYJ....pYO2SYQMkw819LR9I/YOFg</CryptographicInformation>
</CryptographicInformationList>
</TimeStamp>
</ArchiveTimeStamp>
</ArchiveTimeStampChain>
</ArchiveTimeStampSequence>
</EvidenceRecord>

Image 194: Example evidence record

2018 © Imaging Systems, Inc., All rights reserved.

4.2.20 Viewing the audit log

You can view the audit log by using the »Audit log« command accessible via the:

- Popup menu in the »Reports« section for the selected archive, class or folder in the classification scheme.
- Popup menu over an entity selected in the list of contained entities.

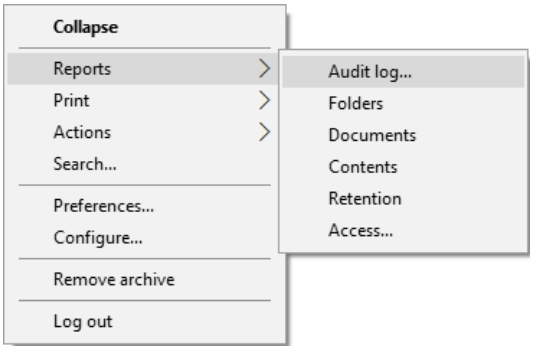


Image 195: Popup menu for selecting the »Audit log« command

The »Audit log query builder« dialog box is displayed, where the user can set the following audit trail search parameters:

- »Date Range«: the audit log query can be limited by setting the initial and final date. The final date is sufficient to start a query. If the initial date is not specified, the search takes complete history into account.
- »Parameters type«: search the audit log by:
  - IP addresses by choosing »IP address«.
  - User names by choosing »User name«.
  - Computer names by choosing »Computer name«.
- »Parameters scope«: specify the scope of parameters:
  - Range between an initial and a final value when choosing »Range«.
  - List of individual values when choosing »List«.
- »Addresses«: the user gives a list of IP addresses of the searched users.
- »Entity Ids«: the user gives a list of identifiers of the searched entities.
- »Sort order«: specify the sort order of audit log search results according to:
  - Date and time, represented by the value »Timestamp«.
  - Object identifier, represented by the value »Object Id«.
  - Session number, represented by the value »Session number«.

2018 © Imaging Systems, Inc., All rights reserved.

- »Report formats«: selection of audit log query formats. The possible formats are:
  - XML.
  - Text (individual fields separated by a comma, CSV).
- »Report file path«: set the path of the report file. The option »Automatically launch default application« allows you to open the report in the default application for the selected report format.

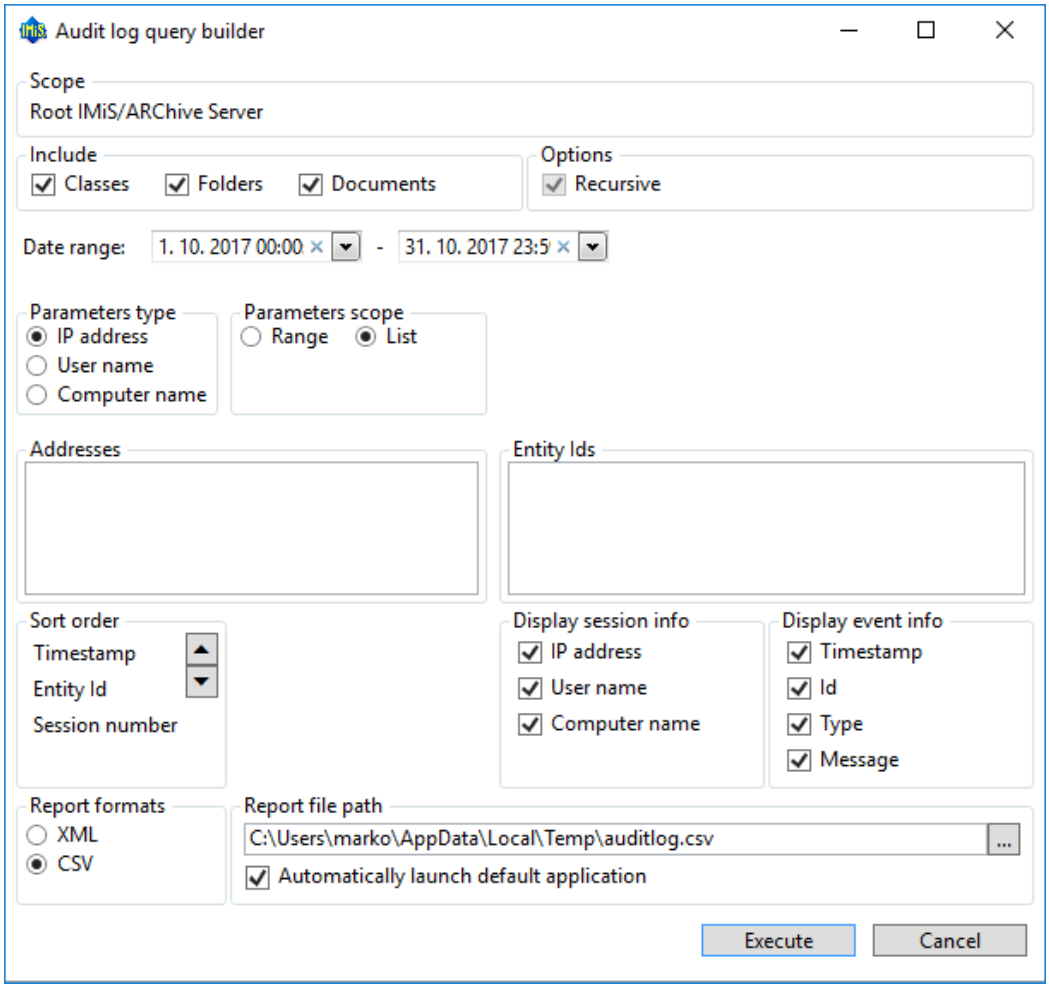


Image 196: Configuring the audit trail query

When the parameters are set, the query is started by choosing »Execute« or cancelled by using »Cancel«.

2018 © Imaging Systems, Inc., All rights reserved.

4.3 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 (accessible to all users no matter what access rights and roles they have).
- Required, which means that the attribute value has to be input before the entity can be saved.
- Read-only.

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

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

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, such as transfer or import.

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

2018 © Imaging Systems, Inc., All rights reserved.

4.3.1 General system attributes

The general system attributes of an entity consist of various attributes such as »Title«, »Description« and »Classification code«.

General attributes contain mandatory as well as optional attributes. Most attributes are available for all entities. The exceptions are »Status«, »Opened date« and »Closed date«, which are present for classes, folders, and those documents that are located directly under a class. Attribute »Significance« is available for folders and documents only.
The table below lists and describes all the general system attributes.

Name	Description
Classification code	Contains the entity's classification code within the classification scheme. The classification code is generated automatically on the archive server. *Example: The classification code 01-2018-00004/00001 represents document 00001, located inside folder 2018-00004, located inside class 01. The classification code is a publicly accessible type of metadata.*
Title	Saves/contains the title of the entity. The title is a required, public metadata that enables search.
Description	Saves/contains a short description of the entity. The description is a public metadata.
Status	Saves/contains the status of the entity. The status is a required metadata for all entities that are either classes, folders, or documents directly under classes. It is a public metadata that enables search. The possible values are: • »Opened«: the entity can be edited by a user with the appropriate effective access rights (the right to write) • »Closed«: the entity cannot be edited.
Opened date	Contains the date and time the status of the entity was changed to »Opened«. The opened date is public metadata, is read-only and enables search.
Closed date	Contains the date and time the status of the entity was changed to »Closed«. The closed date is public metadata, is read-only and enables search.
Significance	Saves/contains the significance rating of the entity. Significance is a required metadata for folders and documents. It is public metadata that enables search. The possible values are: • »Vital«: entity is vital. • »Permanent«: entity is permanent. • »Retain«: entity should be retained. • »Delete«: entity is queued for deletion.

2018 © Imaging Systems, Inc., All rights reserved.

Name	Description
Security class	Saves/contains the security class of the entity. The security class is optional metadata for all new entities. Once it is set, it cannot be modified without stating a reason for change. The security class is a public metadata that enables inheriting and enables search. The possible predefined values are: • »Unclassified«: entity is freely accessible. • »Restricted«: entity is of an internal nature. Can only be accessed by users with clearance level »Restricted« or higher. • »Confidential«: entity is confidential. Can only be accessed by users with clearance level »Confidential« or higher. • »Secret«: entity is secret. Can only be accessed by users with clearance level »Secret« or higher. • »Top Secret«: entity is top secret. Can only be accessed by users with clearance level »Top Secret«.
Creator	Contains the creator of the entity (name of user who created it). The value is set when an entity is created on the IMiS®/ARChive Server and cannot be changed. The creator is a public metadata, is read-only and enables search.
Owner	Saves/contains the owner of the entity. The value of the attribute is selected from among the currently registered users of the archive server. The owner is a public metadata that enables search.
Keywords	Saves/contains keywords related to the entity. This attribute can have multiple values and is a public metadata that enables search.
External Ids	Saves/contains external identifiers of the entity. This attribute can have multiple unique values and is a public metadata that enables search. *<u>Warning</u>: When entering values, keywords should be separated using the »Enter« key or the semicolon character (;).*
Save log	Contains a report on the verification of the electronic signature for digitally signed content. This attribute can have multiple, added values. It is a public metadata that enables search

Table 7: Description of general system attributes

2018 © Imaging Systems, Inc., All rights reserved.

4.3.2 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

4.3.3 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

4.3.4 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

2018 © Imaging Systems, Inc., All rights reserved.

4.3.5 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

4.3.6 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

4.3.7 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.

2018 © Imaging Systems, Inc., All rights reserved.

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

Table 13: Description of physical content attributes

4.3.8 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: • »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.

2018 © Imaging Systems, Inc., All rights reserved.

Name	Description
State	This value is set by IMiS®/ARChive Server during the review process. Valid values: • »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	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.
Query	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.

Table 14: Description of review process attributes

4.3.9 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	This attribute value states whether the entity transfer was successful or not. Valid values: »true« or »false«.
Transfer id	Contains a value that represents a reference to the transferred entity.

Table 15: Description of entity attributes in the decision-making process

2018 © Imaging Systems, Inc., All rights reserved.

4.4 Authenticity

The IMiS®/Client ensures the authenticity of stored electronic records for the lifelong duration of storage.

4.4.1 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.

Example: The image below shows the qualified digital certificate issued by SIGEN-CA (Slovenian General Certification Authority).

2018 © Imaging Systems, Inc., All rights reserved.

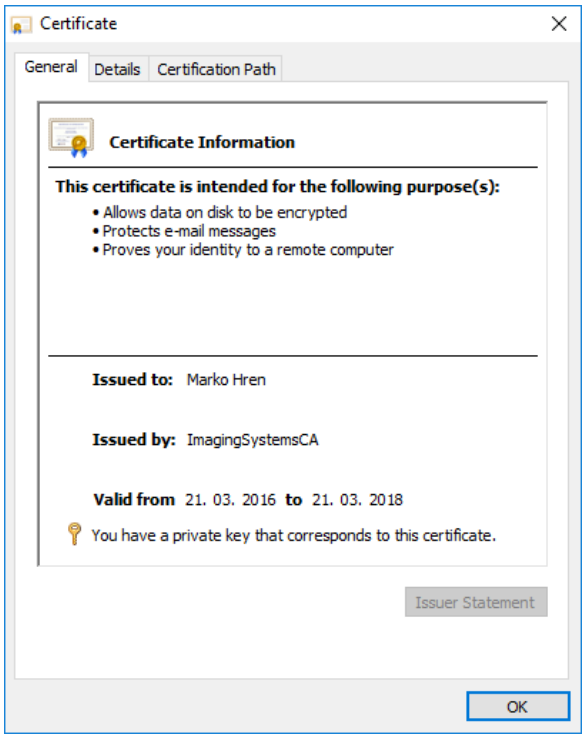


Image 197: Qualified digital certificate information

Users can have several different digital certificates installed on their computer.

The choice of trusted certification authority is up to the user.

4.4.1.1 Digital certificate validity

The digital certificate has an expiration date. The validity of the electronic signature depends on the validity of the digital certificate, which is limited to a maximum time period of 5 years according to provisions of Article 32 of the Regulation on Electronic Business and Electronic Signatures.

When a digital certificate expires, it becomes invalid and can no longer be used.

4.4.1.2 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.

2018 © Imaging Systems, Inc., All rights reserved.

4.4.1.3 Installation of the digital certificate

A digital certificate is obtained from a trusted Certificate Authority (CA). The issuing authority's website describes the procedure of installing the certificate on the computer.
If you wish to view all the currently installed digital certificates, use the following Windows commands: »Tools« -> »Internet options« -> »Content« -> »Certificates«.

4.4.1.4 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.

4.4.2 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.

4.4.2.1 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.

2018 © Imaging Systems, Inc., All rights reserved.

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.
By using the public key, anyone can then verify the user's electronic signature.

The IMiS®/Client enables the electronic signing of TIFF and PDF/A file types.
This requires the use of either the IMiS®/Scan or IMiS®/View software modules.
For more information see chapter Electronic signatures in the IMiS®/Scan and IMiS®/View Manual.

4.4.2.2 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®/Client 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 under the »Content« tab, in the bottom right view of Windows Explorer.

2018 © Imaging Systems, Inc., All rights reserved.

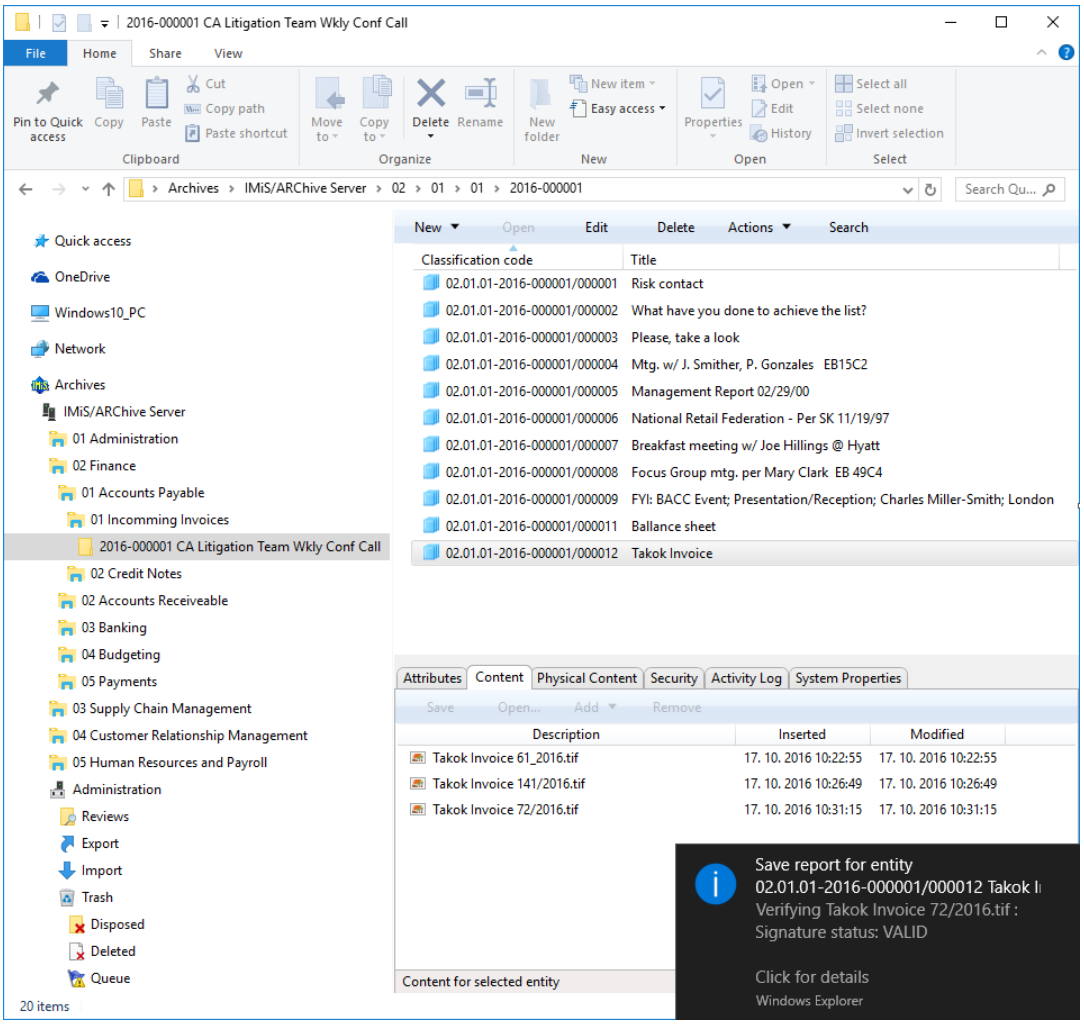


Image 198: Example of a pop-up window containing the result of the document's electronic signature verification.

The pop-up window automatically closes after a few seconds. By clicking on it in time, the user is shown a pop-up window containing a report on the verification of the signed document.

The signature is automatically verified when a document is being archived to the server.

The archive server also saves documents with invalid electronic signatures.

2018 © Imaging Systems, Inc., All rights reserved.

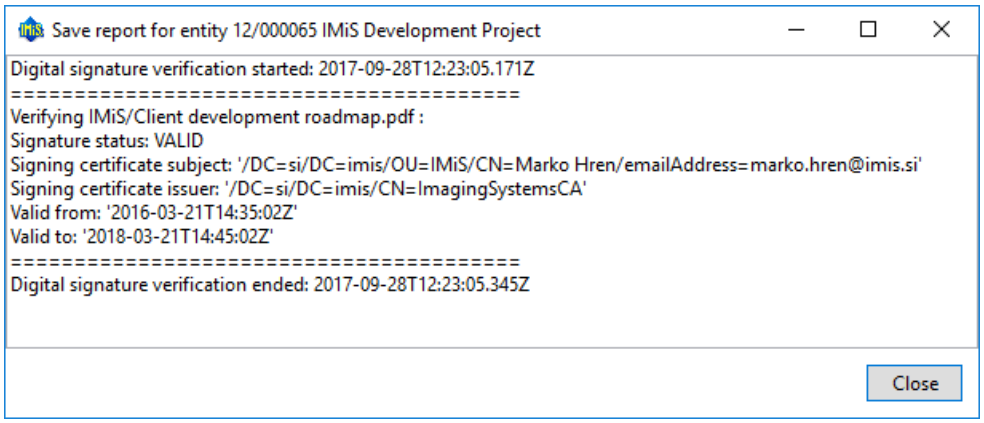


Image 199: Example of a report for a valid electronic signature and valid digital certificate

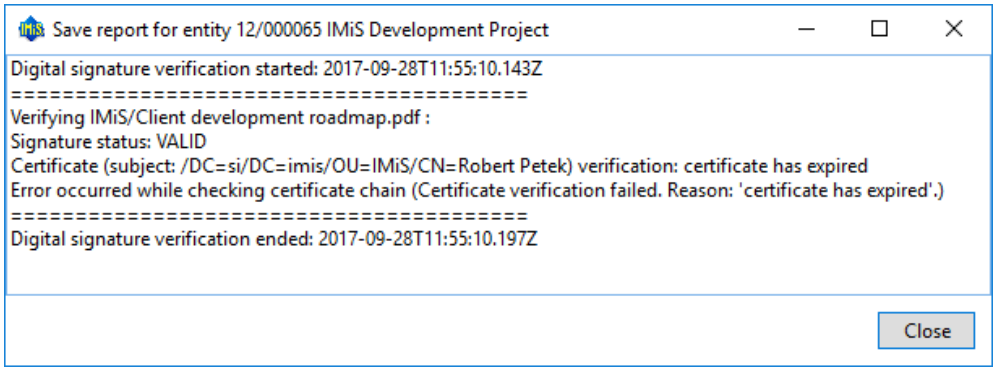


Image 200: Example of a valid electronic signature and an expired digital certificate

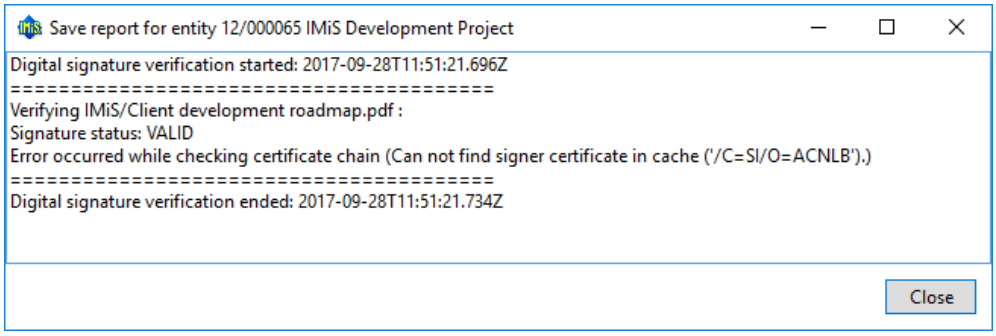


Image 201: Example of a valid electronic signature
for which the certification authority could not be verified.

2018 © Imaging Systems, Inc., All rights reserved.

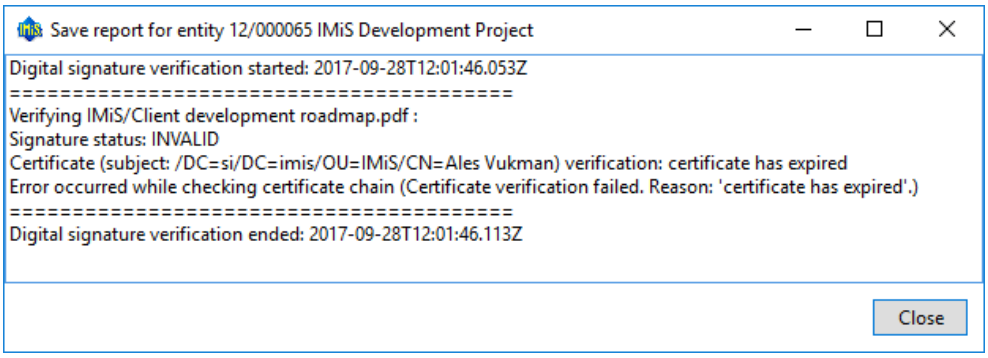


Image 202: Example of an invalid electronic signature due to a modification of the document after signing.

4.5 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.

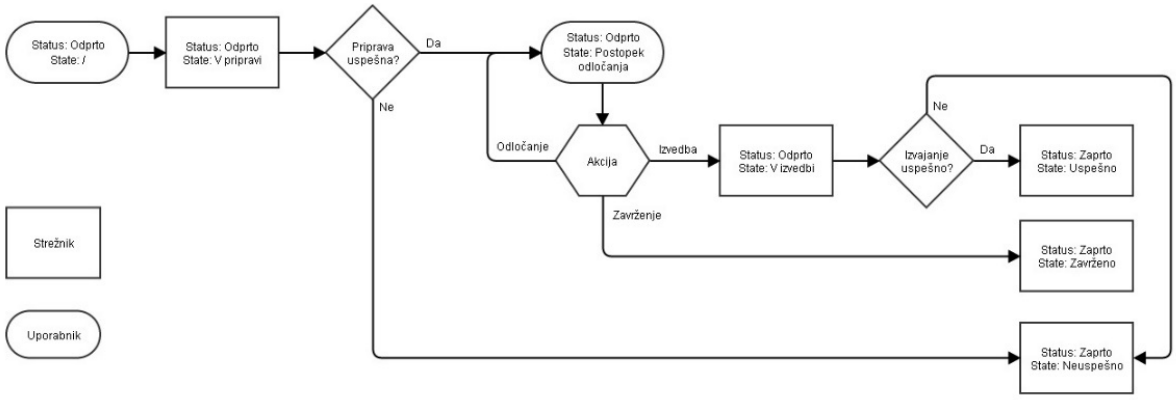


Image 203: Schematic of the review process

IMiS®/Client 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.

All activities in the review process are implemented in the »Reviews« folder, classified under the »Administration« system folder.

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.

These access rights are set by the administrator when setting the access rights in the »Configure« interface and the »Reviews« context. For more information on access rights settings see chapter »Access control« Folder.

4.5.1 Preparation phase

In the left view of Windows Explorer, the user selects the archive. Under the expanded list of root classes the user expands the »Administration« system folder in which the »Reviews« folder is located. By selecting the folder, the top right view shows the already prepared »Reviews«.

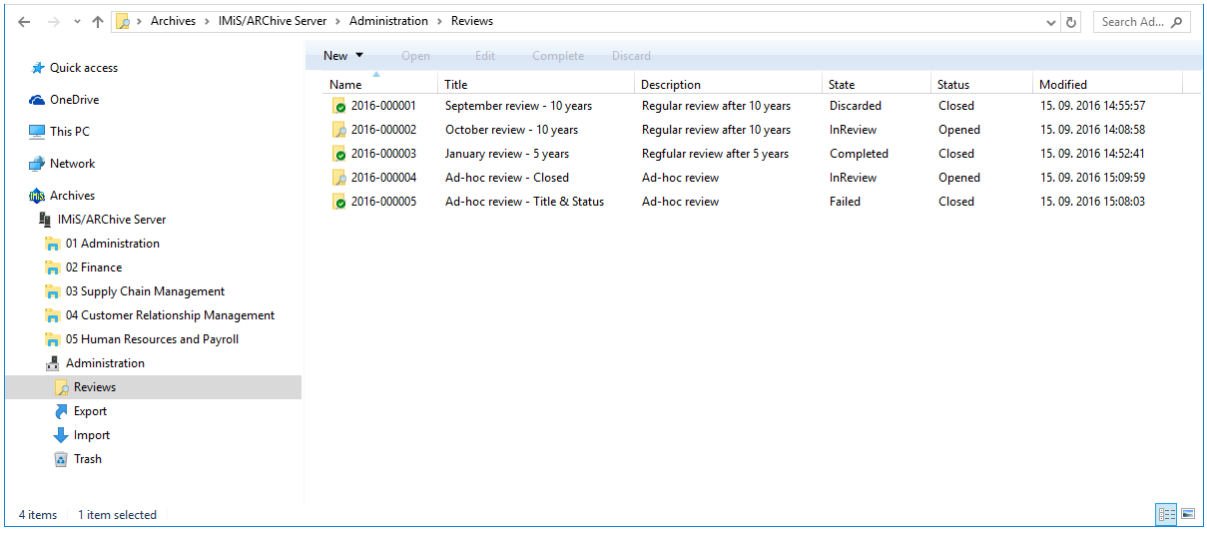


Image 204: Display of reviews created in the review processes

By selecting the »New« command in the top command bar, a pop-up menu appears, which offers 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.

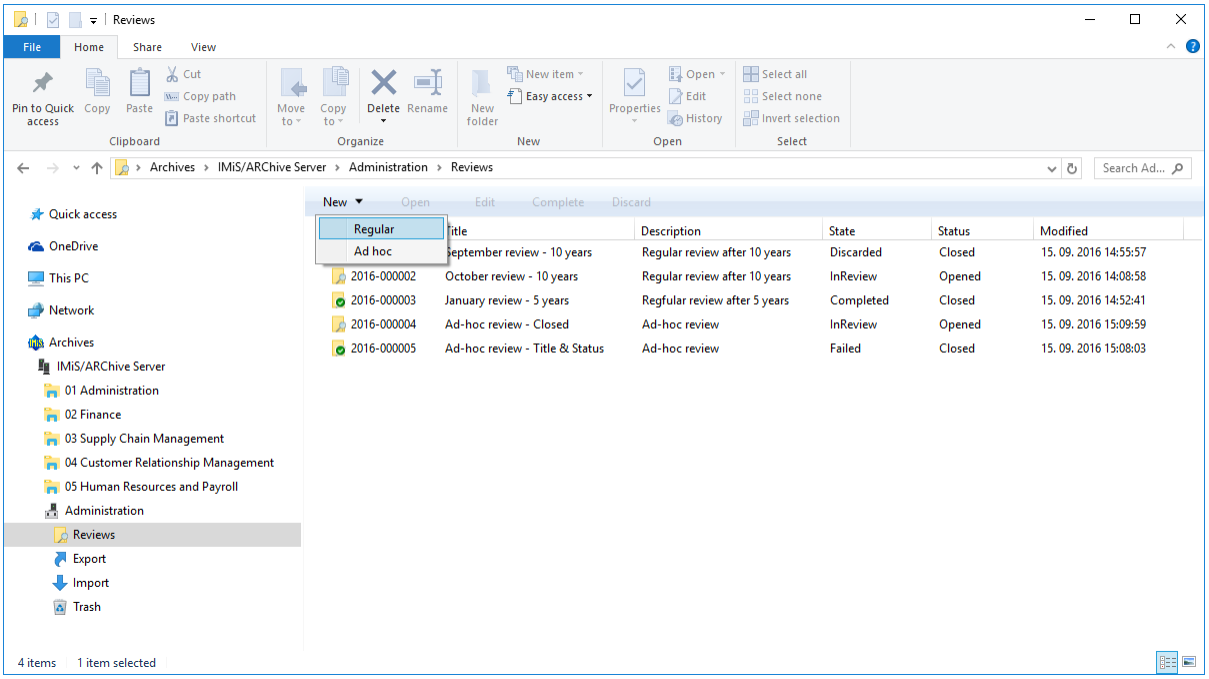


Image 205: Creating a new regular review in the preparation phase

After selecting the »Regular« command, the user is shown a dialog box for selecting retention periods.

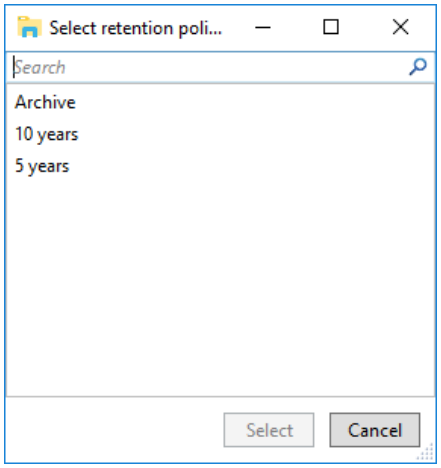


Image 206: Dialog box for selecting retention periods

The user can select one or several retention periods for which he wishes to obtain a list of entities. After confirmation with the »Select« command, the bottom right view shows the tabs of a new review in the review process under entity information.

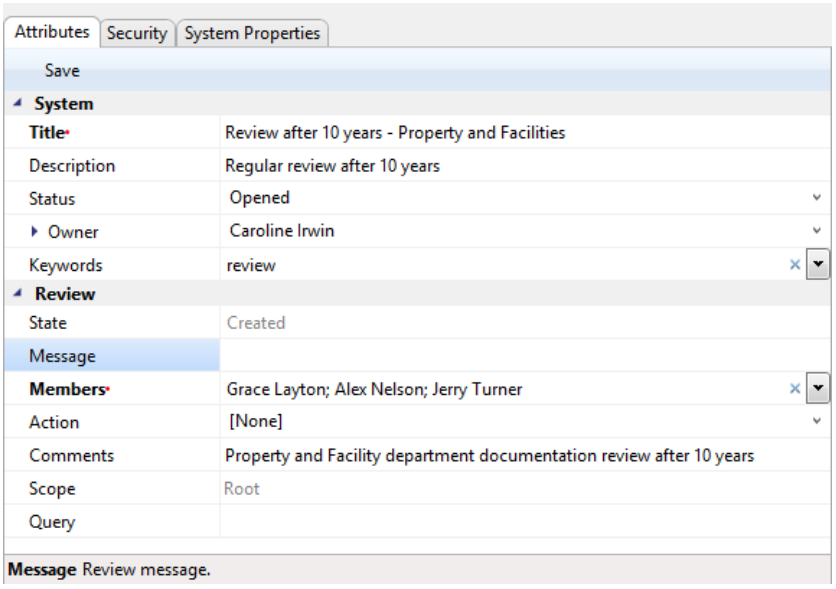


Image 207: Display of review attributes in the review process

After selecting the »Ad hoc« command, the »Search builder« appears to the user.
The user enters a query into the »Search builder«, based on which a list of selected entities will be created. The »Search builder« is described in chapter Search functions.

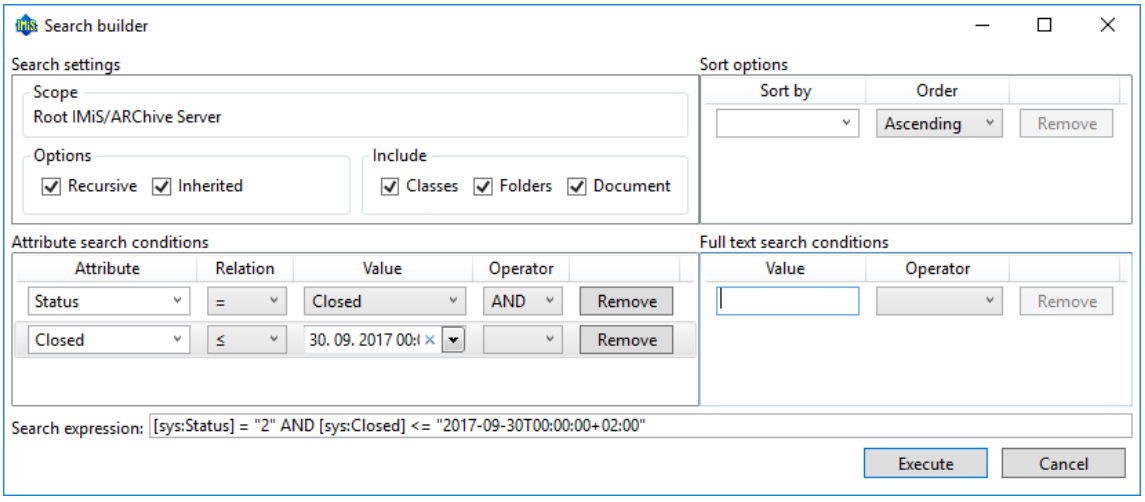


Image 208: Example of creating a list of entities which were closed on a specific date

2018 © Imaging Systems, Inc., All rights reserved.

After confirmation by clicking on the »Execute« button, the bottom right view shows the tabs of a new review in the review process under entity information.

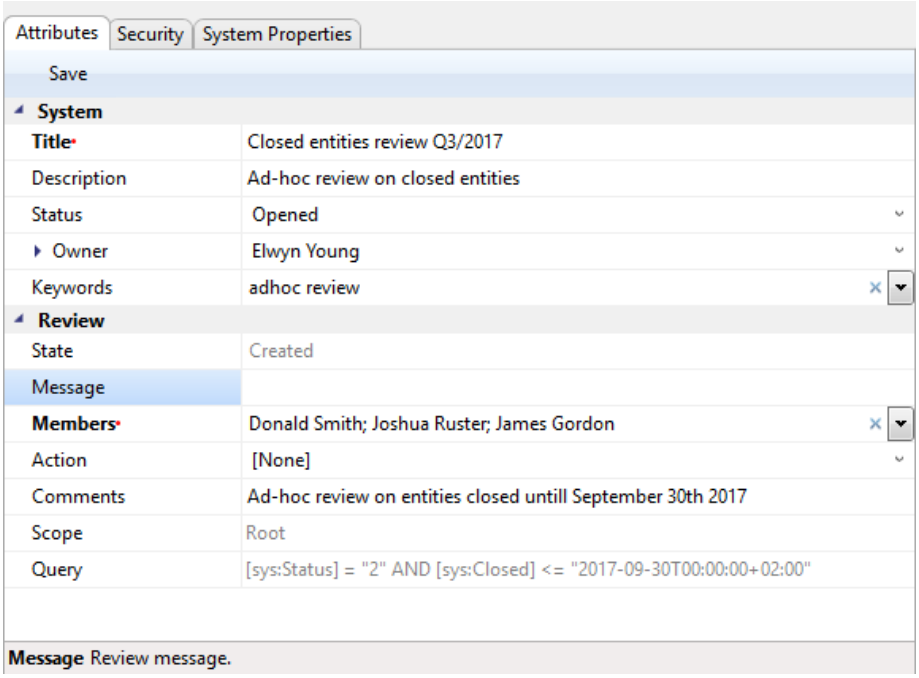


Image 209: Display of review attributes in the review process

The value of the »Query« attribute represents a previously created query which cannot be modified subsequently.

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.

4.5.1.1 Entry of metadata

If the »Attributes« tab in the bottom right view of entity information has not been selected, the user starts by selecting it. This tab contains the list of all process attributes which can be entered by the user. For more information on entering metadata see chapter Entry of metadata.

The list of attributes is divided into several categories:

- »System«: attributes are present on all entities. For more information see chapter General system attributes.
- »Review«: attributes are present only when the entity is undergoing the review process. For more information see chapter Review process attributes.

2018 © Imaging Systems, Inc., All rights reserved.

By creation of the review, two attributes are mandatory: »Title« and »Members«.
The user enters the title of the review into the »Title« attribute and the names of team members performing the review into the »Members« attribute.

After entering the metadata, the user saves the review to IMiS®/ARChive Server.
The user executes this by selecting the »Save« command in the bottom command bar.

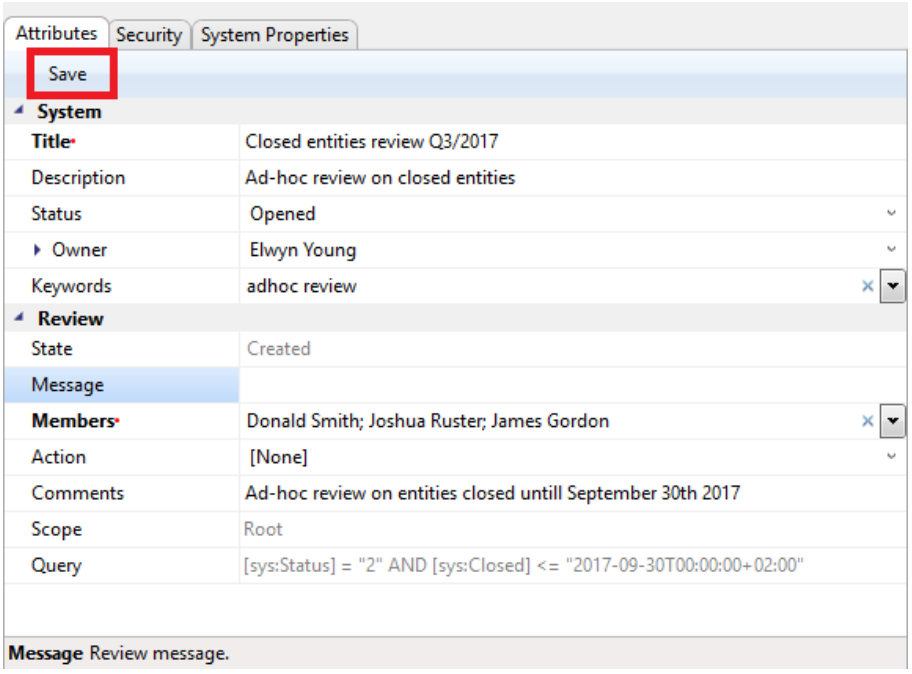


Image 210: Saving a new or modified review in the review process

This starts the transfer of all entered metadata to IMiS®/ARChive Server. After the review has been saved, it is queued for preparation.

Problem: The most common problem during saving is that the value of the mandatory attribute has not been entered.

4.5.1.2 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.
More information is available in chapter Filtering process in the IMiS®/ARChive Server Manual.

2018 © Imaging Systems, Inc., All rights reserved.

While the review process is in the preparation phase, it cannot be modified.
During that time, its »State« attribute shows the »Preparing« value.

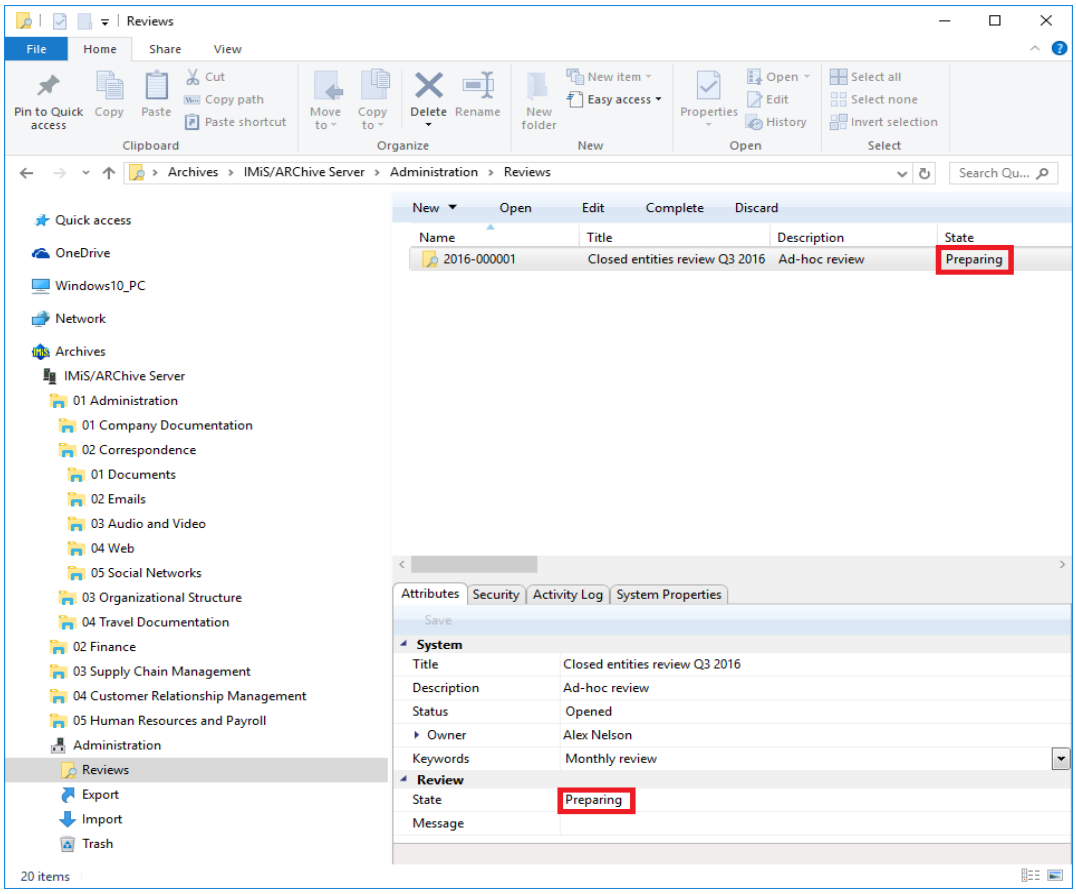


Image 211: Display of a review in the preparation phase

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.

2018 © Imaging Systems, Inc., All rights reserved.

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.

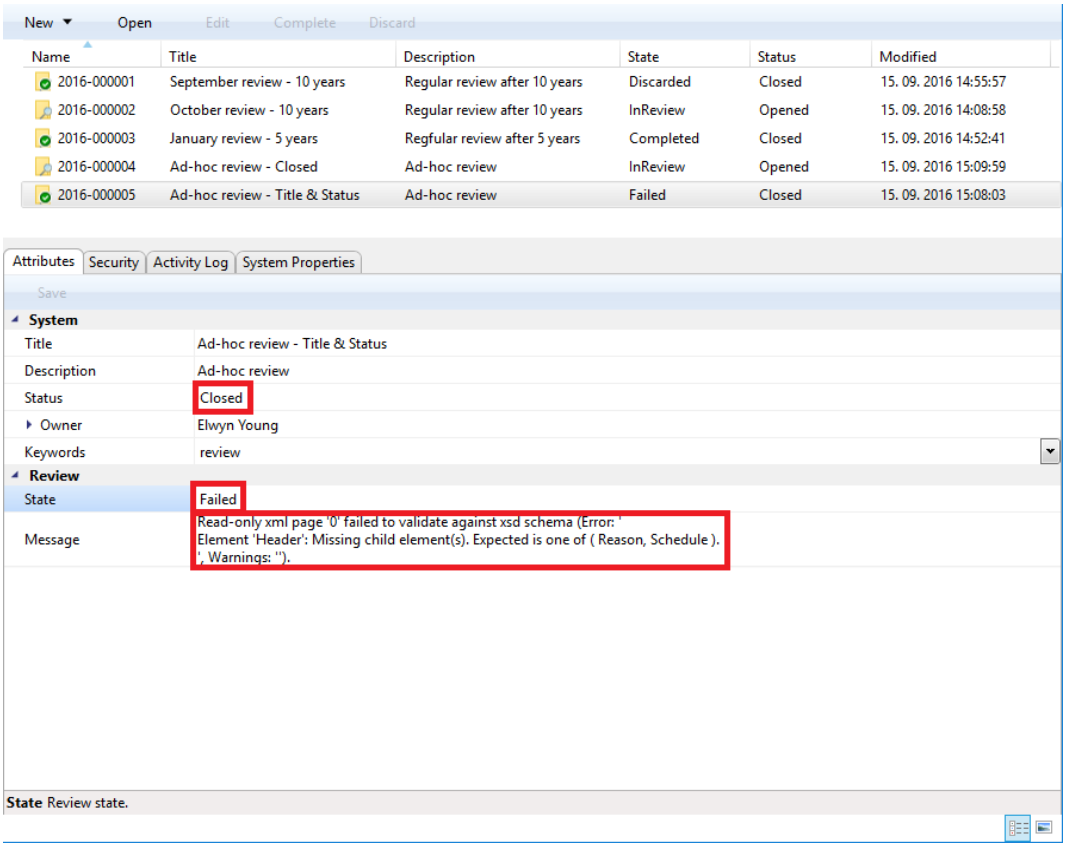


Image 212: Display of an error which occurred during the preparation phase of the review process

4.5.2 Decision-making phase

Each review created is visible in the »Reviews« folder, which is contained in the »Administration« system folder. This folder can only be accessed by users with the »Read« right. Creating reviews is enabled for users with the »Create entities« right.
More information on roles is available in chapter Roles in the IMiS®/ARChive Server Manual.

By selecting the folder, the top right view shows all of the reviews created. By selecting the appropriate review, review pages are shown, containing the entities which are the object of the review process.

2018 © Imaging Systems, Inc., All rights reserved.

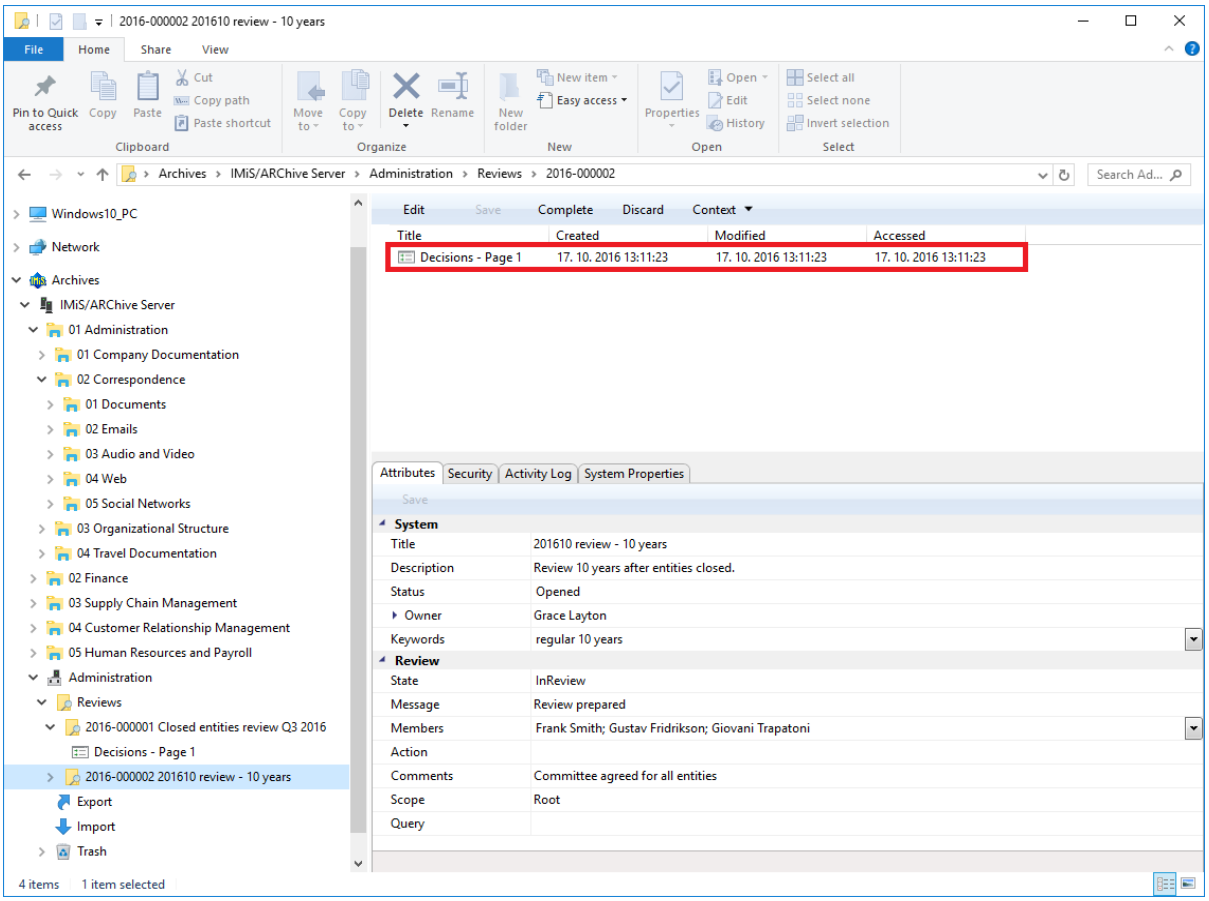


Image 213: Display of the review page

In the review the following data is visible for each page:

- Sequential title of page in the »Title« line.
- Date of page creation in the »Created« line.
- Date of last page modification in the »Modified« line.
- Date of last viewing of the page in the »Accessed« line.

Each page contains the final number of entities. The default value is 2,000 entities.

By clicking on the selected page, the top right 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.

2018 © Imaging Systems, Inc., All rights reserved.

An entity which is undergoing the review process can be marked by team members with 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.

- »Transfer«: after confirming the transfer and successfully completing the transfer process, the entity will be disposed of.
- »InReview«: an action which does not modify the entity's life span. The entity can be selected in the next transfer process.

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. The same applies to the »Reason« attribute.

By clicking on an entity on the list, the bottom right view shows entity information which cannot be modified.

An entity which is included on the list of an individual review page has the following tabs:

- Attributes. For more information see chapter General system attributes.
- System Properties. For more information see chapter General system attributes.
- Review. For more information see chapter Entity attributes in the decision-making process.

By clicking on the »Navigate to« button in the top command bar, the selected entity is shown in the classification scheme.

After reviewing all of the entities in the review process, team members can choose among the following actions:

- Modification of the action on an individual entity in the review process.
- Process completion.
- Process cancellation.
- Transfer of entities from IMiS®/ARChive Server.

2018 © Imaging Systems, Inc., All rights reserved.

4.5.2.1 Modification of action on an individual entity

If team members decide that the actions of certain entities must be modified, they can do so with the »Edit« command.

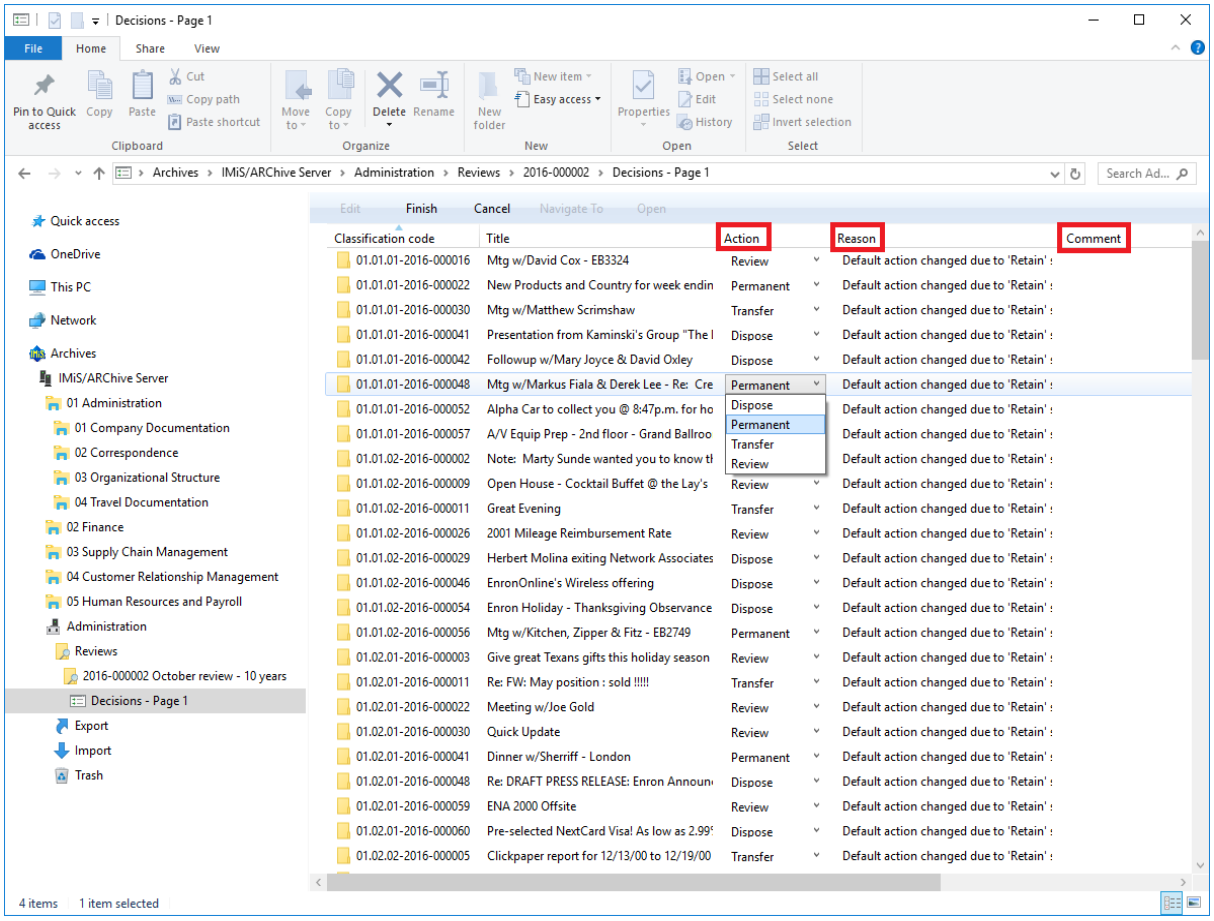


Image 214: List of entities in modification mode

The list is refreshed and the following attributes can be modified:

- Action
- Reason
- Comment.

The value of attributes can be modified by team members directly in the top right view or in the »Review« tab. For more information see chapter Entity attributes in the decision-making process).

2018 © Imaging Systems, Inc., All rights reserved.

They can specify one of the following actions for each entity:

- »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.
- »Transfer«: after confirming the transfer and successfully completing the transfer process, the entity will be disposed of.
- »InReview«: an action which does not modify the entity's life span. The entity can be selected in the next transfer process.

Every time the »Action« attribute is modified it is recommended that team members also record the reason for the modification in the »Reason« attribute.
After finishing reviewing the list, they can implement all modifications with the »Finish« command or undo them with the »Cancel« command.
Both buttons are located in the top command bar.

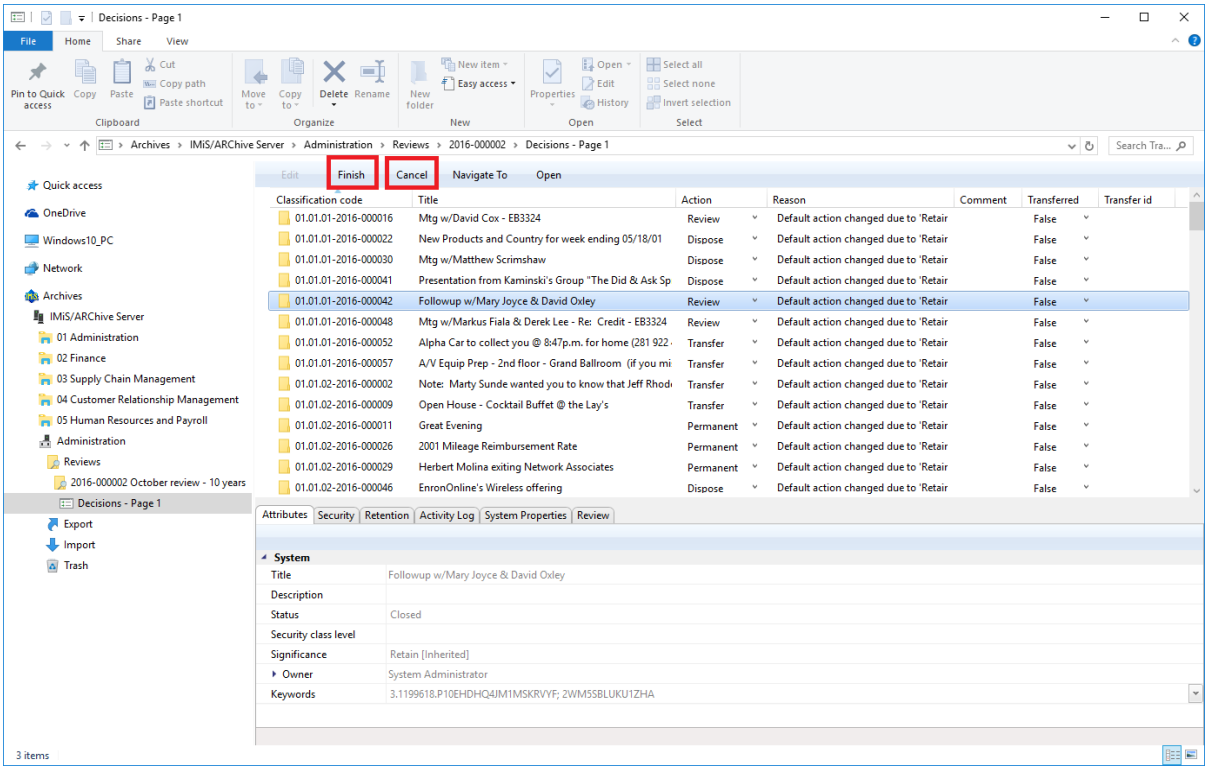


Image 215: Display of the »Finish« and »Cancel« button

If the page has been modified, its title is written in bold in the view.

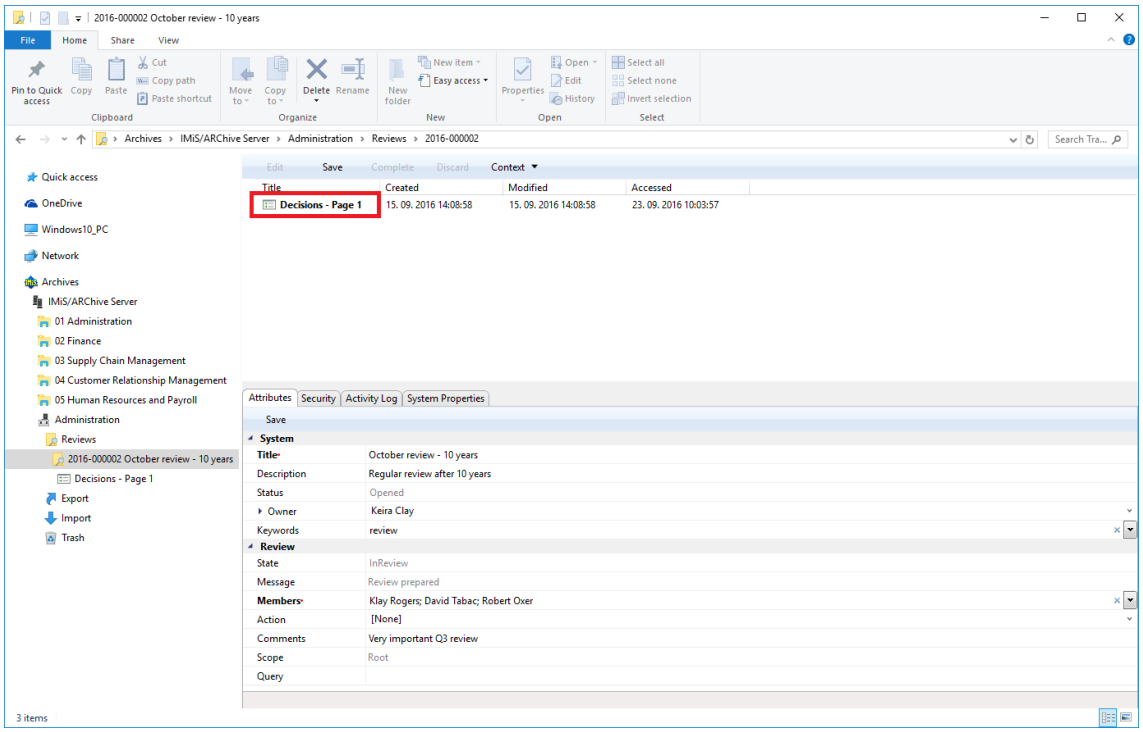


Image 216: Display of the page which has been modified

Modifications of entities in the review process are not saved to IMiS®/ARChive Server until the user selects the »Save« command in the top command bar.

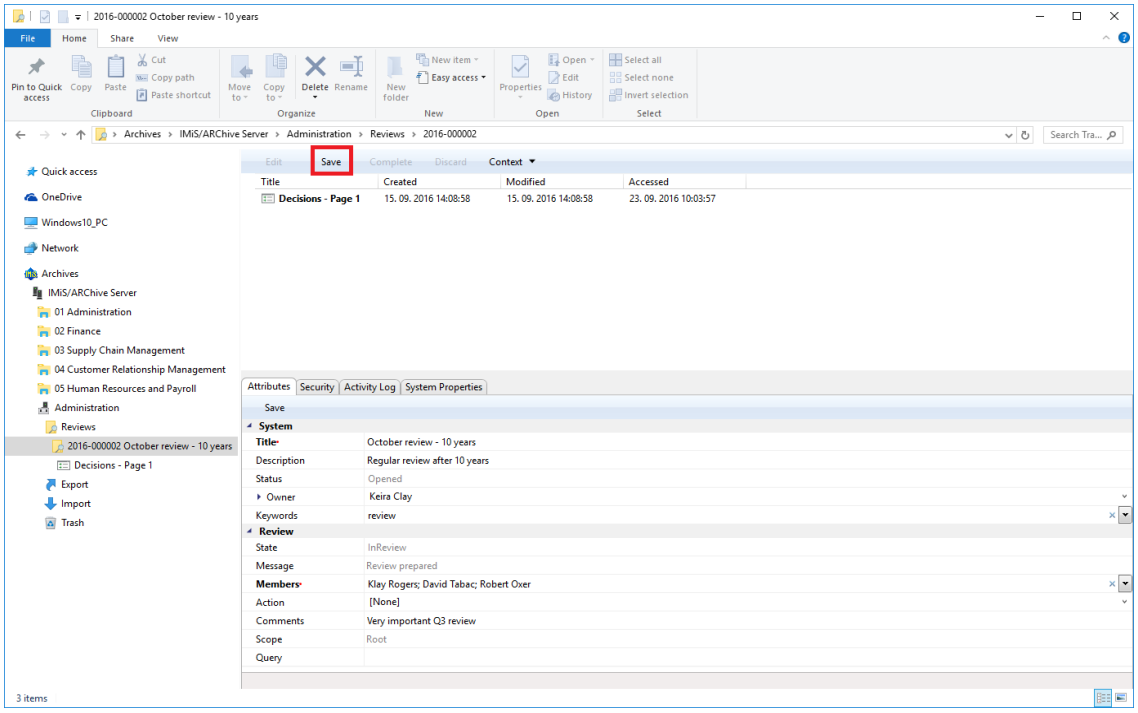


Image 217: Display of the »Save« command in the review process

4.5.2.2 Cancelling the decision-making phase

The decision-making phase can be cancelled by team members with the »Discard« command in the top command bar.

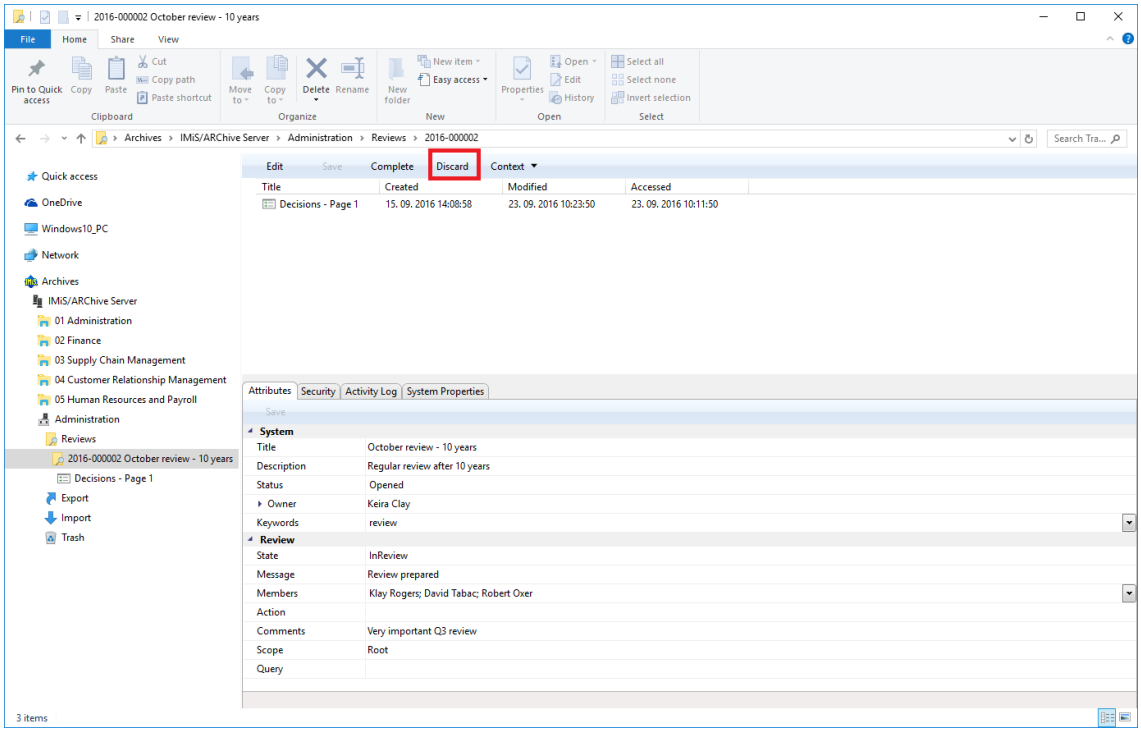


Image 218: Cancellation of the review process using the »Discard« command

When cancelling the decision-making phase, 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 cancelled by the user. In this case the entire review process must be recreated.

2018 © Imaging Systems, Inc., All rights reserved.

4.5.3 Implementation phase

The decision-making phase is followed by the implementation phase. Team members complete the review with the »Complete« command in the top command bar.

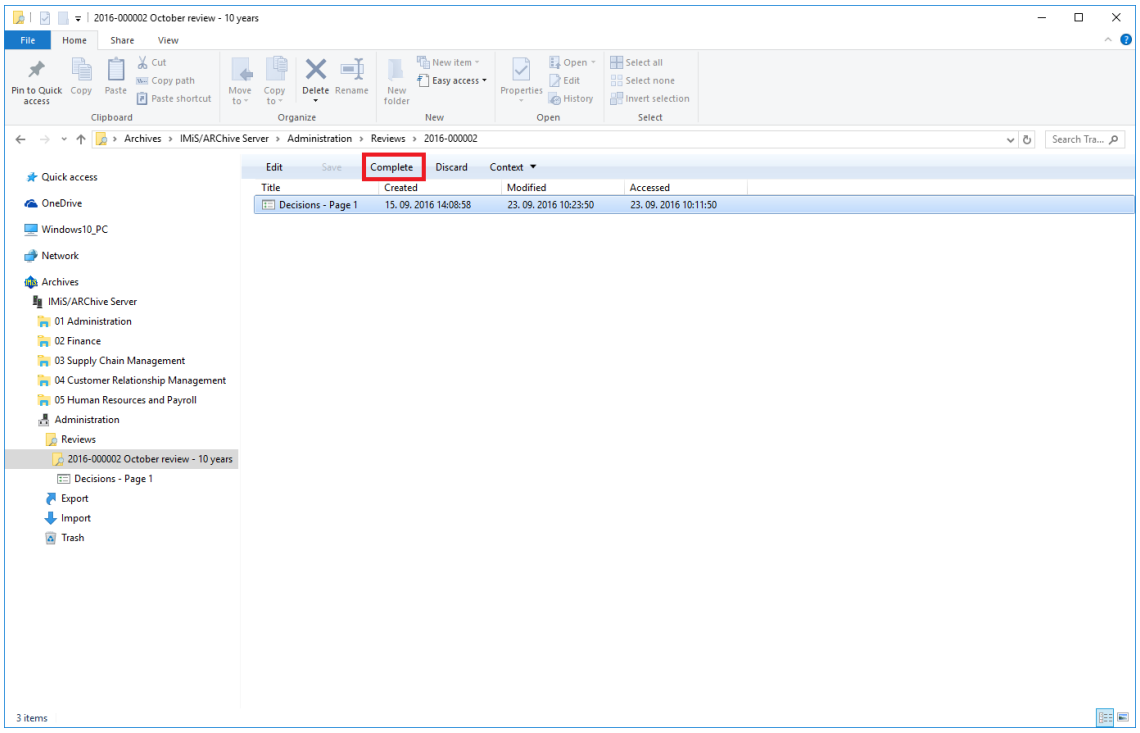


Image 219: Starting the implementation phase by selecting the »Complete« command

IMiS®/ARChive Server implements the review process of the disposition, transfer and permanent retention of entities. It automatically creates a full report on the implementation phase and files it among the review contents.

For more information see chapter Reviewing and classifying documents.

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 »State« attribute to »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 to »Closed«.

  In this case the entire review process must be recreated.

2018 © Imaging Systems, Inc., All rights reserved.

4.5.4 Transfer of entities from the server

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.

4.5.4.1 Exporting to a file system

The user executes the transfer of entities by right-clicking on the selected review, where he selects the »Transfer« command in the pop-up menu under the »Actions« section.

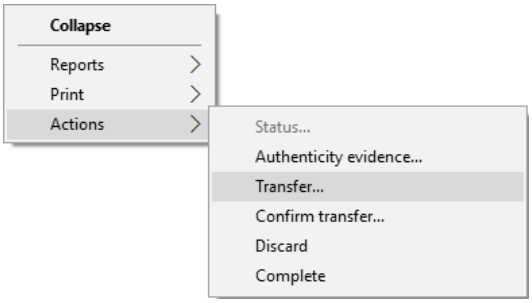


Image 220: Transfer of entities in the review process

After selecting the command, the user is shown a dialog box for setting the transfer parameters.

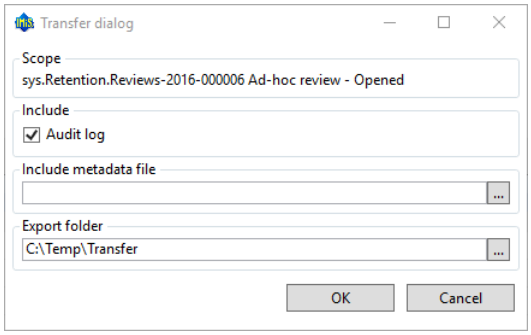


Image 221: Setting the transfer parameters

By selecting the »Audit log« option, the audit log for an individual transferred entity can be included in the transfer.

2018 © Imaging Systems, Inc., All rights reserved.

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 »Documents« context the user will receive the following notification of the reason for the error in the transfer report: »Error acquiring audit log from server«.

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 by clicking on the »...« button.
For a description of the structure of the file with additional metadata see chapter Format of the additional metadata export file.

In the »Export folder« section the user invokes a dialog box for selecting the folder to which entities in XML format will be transferred by clicking on the »...« button.

The user completes the export process by selecting the digital certificate to be used for signing the XML file containing a transfer report according to the »XML Signature« standard. This ensures the verification of the authenticity of the report and of the exported files.

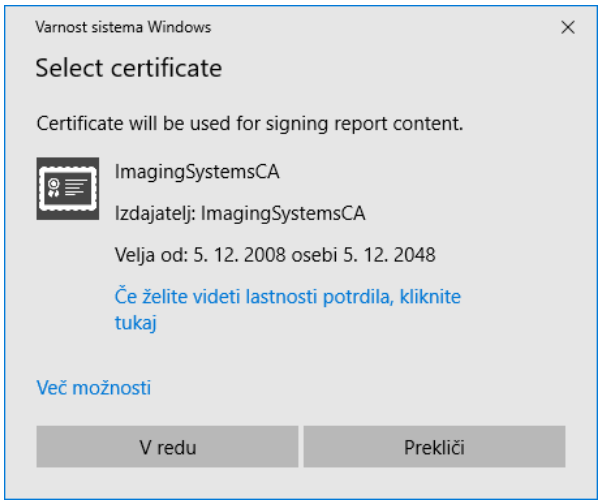


Image 222: Selecting a digital certificate during export

Warning: Export is executed regardless of whether the user has selected a digital certificate. If the user does not select a digital certificate, the XML file containing the export report is not signed.

2018 © Imaging Systems, Inc., All rights reserved.

When the export process is completed, the bottom right view of Windows Explorer shows a notification in the form of a pop-up window with the success rate statistics by entity type. The number of successfully exported entities with regard to the number of all entities chosen for export is shown for each entity type. The pop-up window stays open until you click outside of it for the first time.

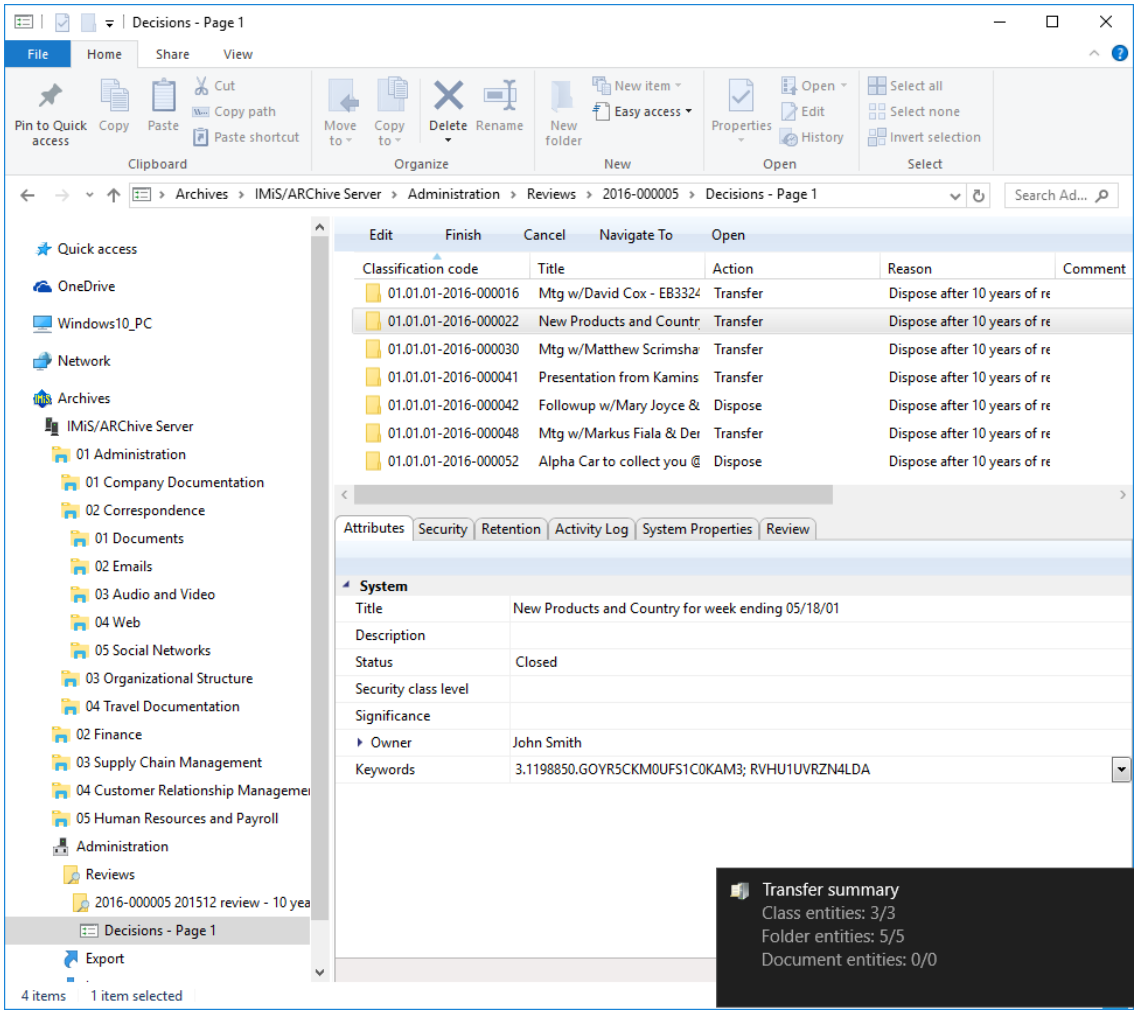


Image 223: Display of the export complete message with success rate statistics

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.

2018 © Imaging Systems, Inc., All rights reserved.

4.5.4.1.1 Export phase

At the start of export IMiS®/Client 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 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.

Additionally, a utility file for automatic transfer confirmation »TransferConfirmation.csv« is created. With it the user of a third archive can quickly specify which entities will be confirmed as successfully transferred.

In the event of an error when exporting an entity, the error is recorded in the Error report file. After all entities have been exported, the »ExportReport.xml« file is digitally signed with the selected digital certificate according to the XMLDSIG standard. This provides the option of verifying the authenticity of the report and the authenticity of the exported files.

After the first transfer phase - export - is completed, the following log files are attached to the document:

- XML report
- Report
- Error report.

2018 © Imaging Systems, Inc., All rights reserved.

4.5.4.1.2 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.

4.5.4.2 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.

4.5.4.2.1 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 action on an individual entity.

2018 © Imaging Systems, Inc., All rights reserved.

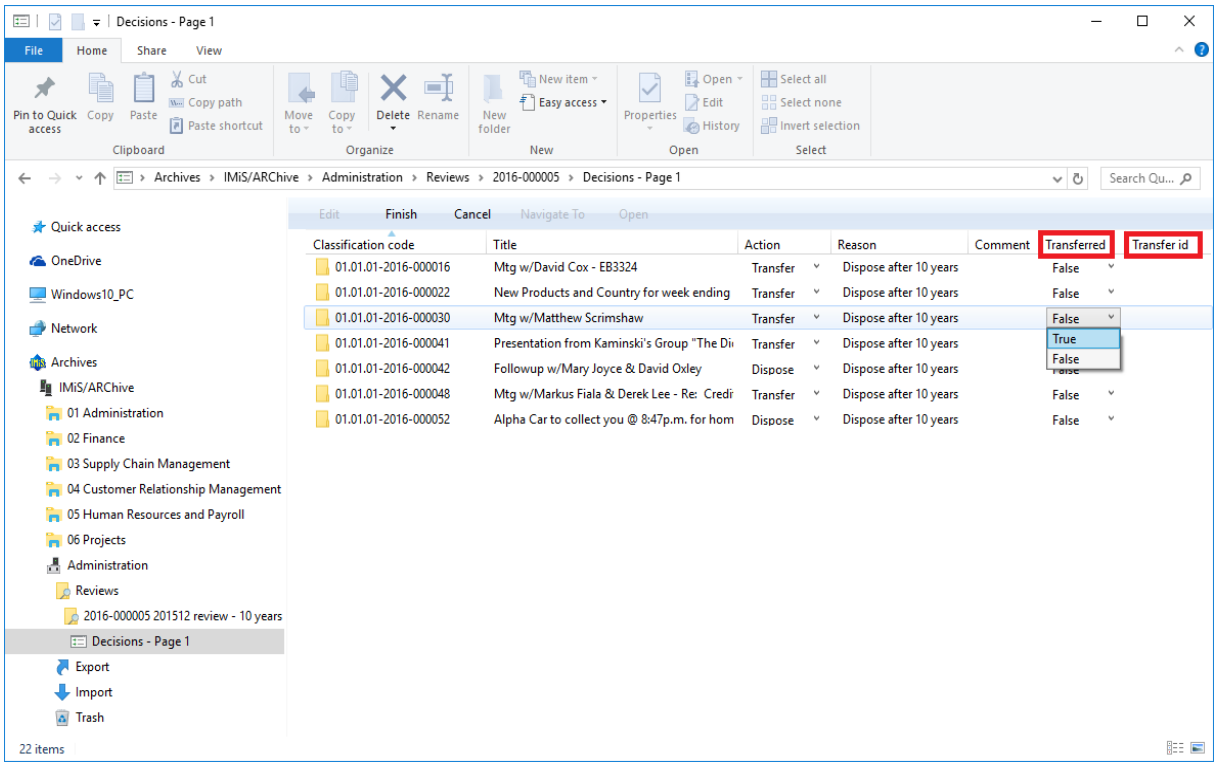


Image 224: Manual transfer confirmation for an individual entity

Team members must specify for each entity on the list whether it has been transferred. They do so by changing the value of the »Transferred« attribute to »Yes« in the drop-down menu. If they wish, they can also enter a reference to the transferred entity by entering the value of the »Transfer id« attribute.

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.

4.5.4.2.2 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. By right-clicking, a pop-up menu appears in which they select the »Confirm transfer« command in the »Actions« section.

2018 © Imaging Systems, Inc., All rights reserved.

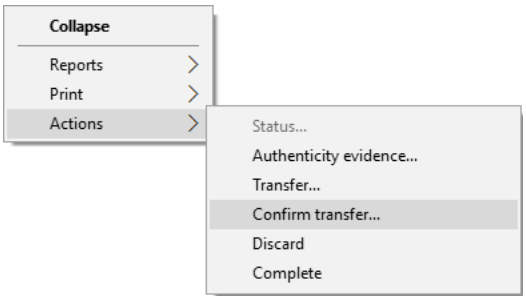


Image 225: Transfer confirmation using a confirmation file.

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.

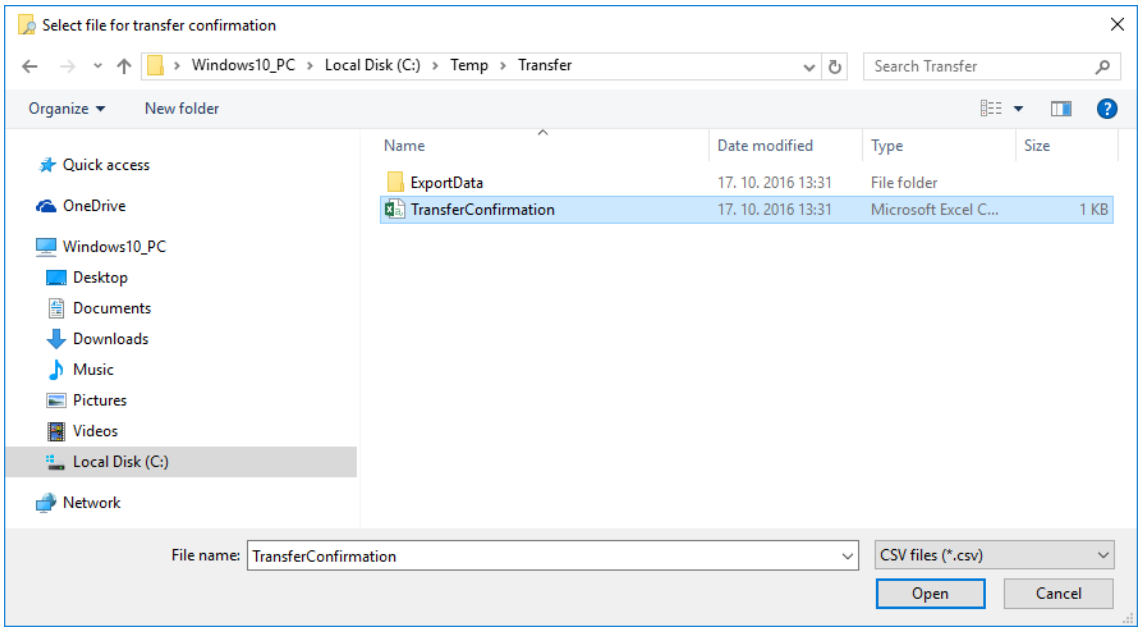


Image 226: Selecting the confirmation file

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.

With the »Cancel« command team members cancel the selection of the confirmation file.

2018 © Imaging Systems, Inc., All rights reserved.

4.5.5 Reviewing and classifying documents

An integral part of the review process is the reviewing and classifying of documents.

The user accesses documents by selecting the archive server in the left view of Windows Explorer. Under the expanded list of root classes the user expands the »Administration« system folder in which the »Reviews« folder is located.

By selecting this folder, the top right view shows the already created reviews.

By double-clicking on the desired review, individual pages with entity lists are shown.

4.5.5.1 Reviewing documents

The user selects the appropriate review page with a list of entities. By clicking on the »Context« command in the top command bar, a pop-up menu appears which lists all of the available review contexts. The user selects the »Documents« context.

A list of classified documents appears in the top right view.

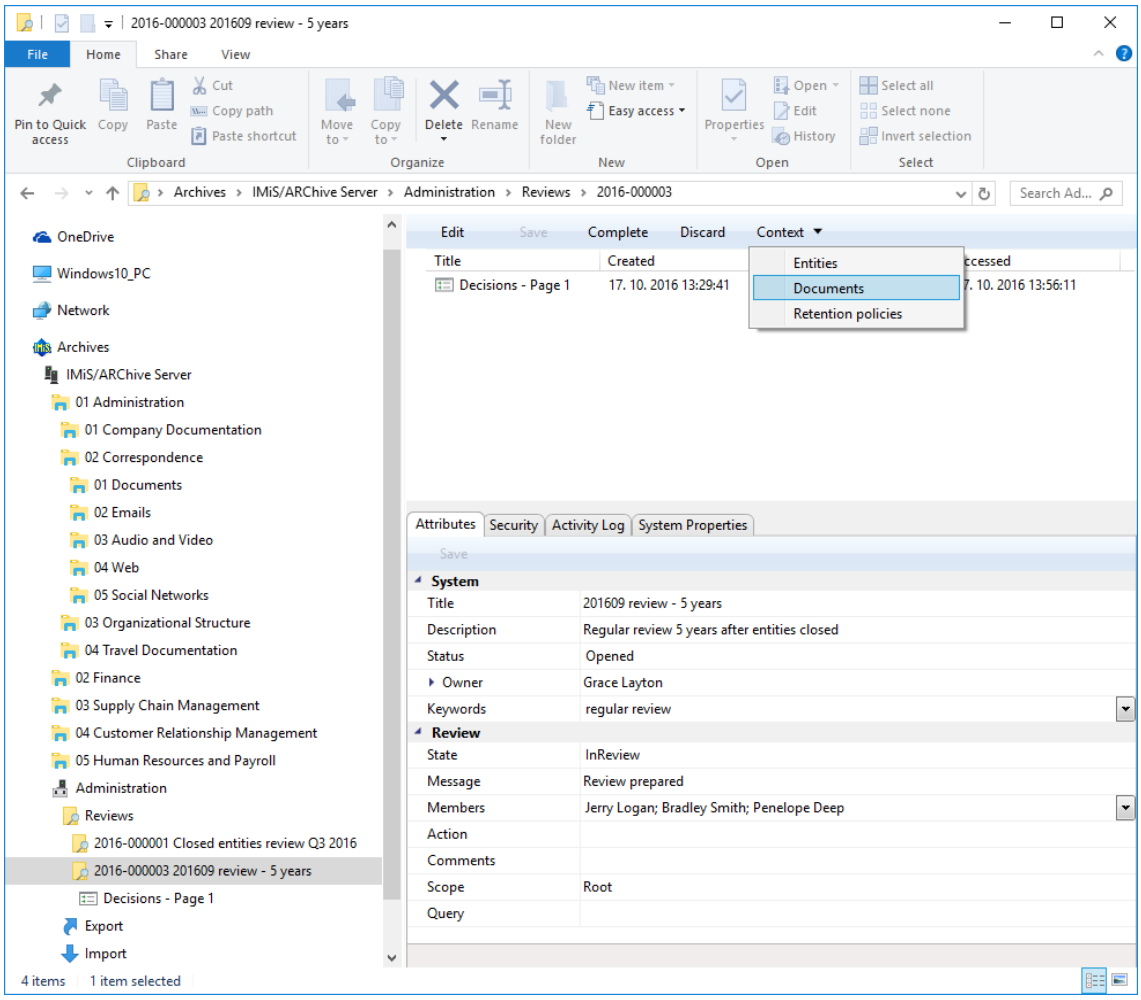


Image 227: Changing the context during the review of classified contents

Examples of classified contents:

- *Report on the implementation phase of the review process.*
- *Transfer report.*
- *Custom document.*

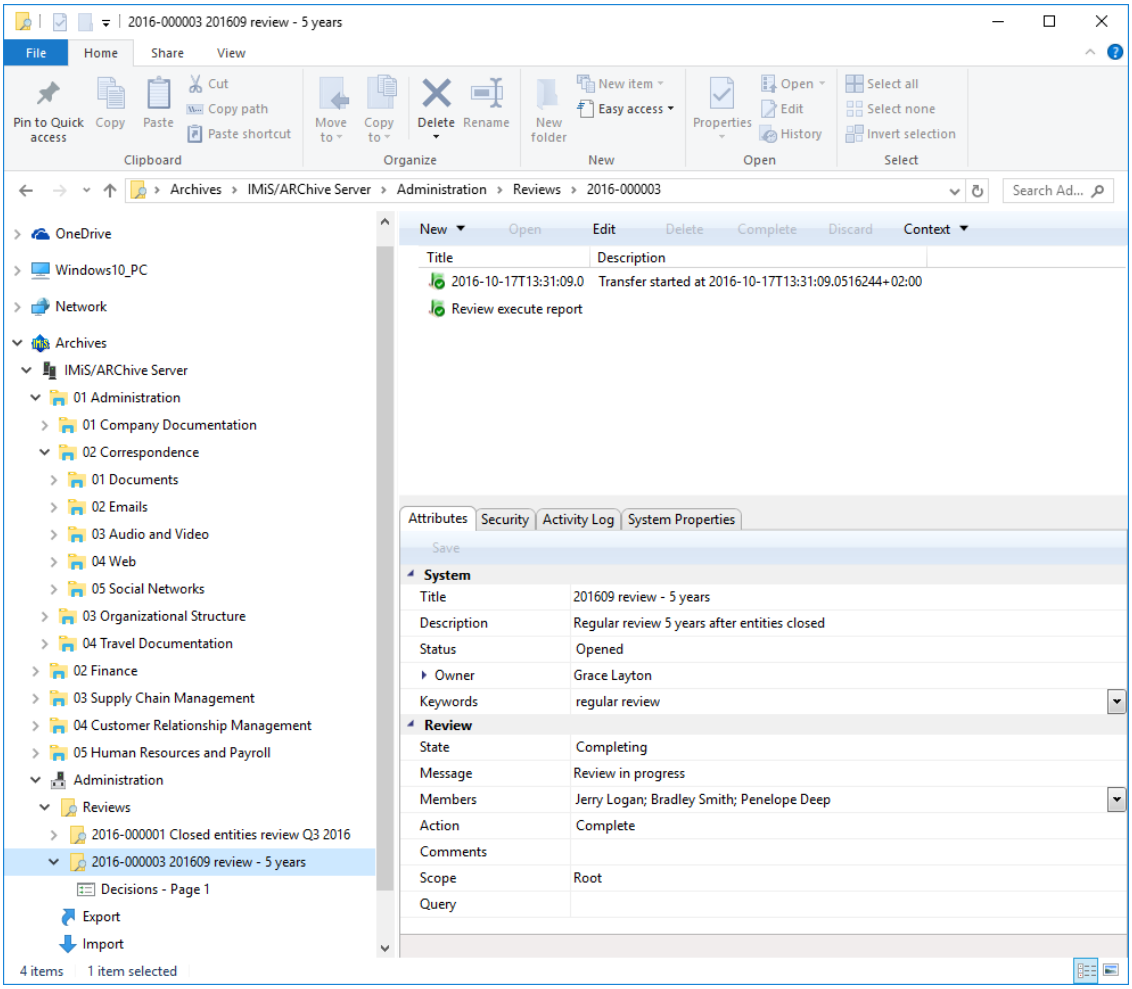


Image 228: Example of displaying inserted documents in »Documents« context

For updating and viewing contents see chapter Entity information.

4.5.5.2 Classifying new documents

In the event that team members create a team record or other document connected with the review process, they can classify it among review documents.

They can classify new documents into an incomplete review by clicking on the »New« button in the top command bar. The bottom right view shows the attributes of the new document.

For updating new content see chapter Entry of metadata.

2018 © Imaging Systems, Inc., All rights reserved.

4.5.6 Viewing selected retention policies

Team members can check which retention policies were used for creating the review.

By clicking on the »Context« command in the top command bar, a pop-up menu appears, in which they select »Retention policies« among the available review contexts.

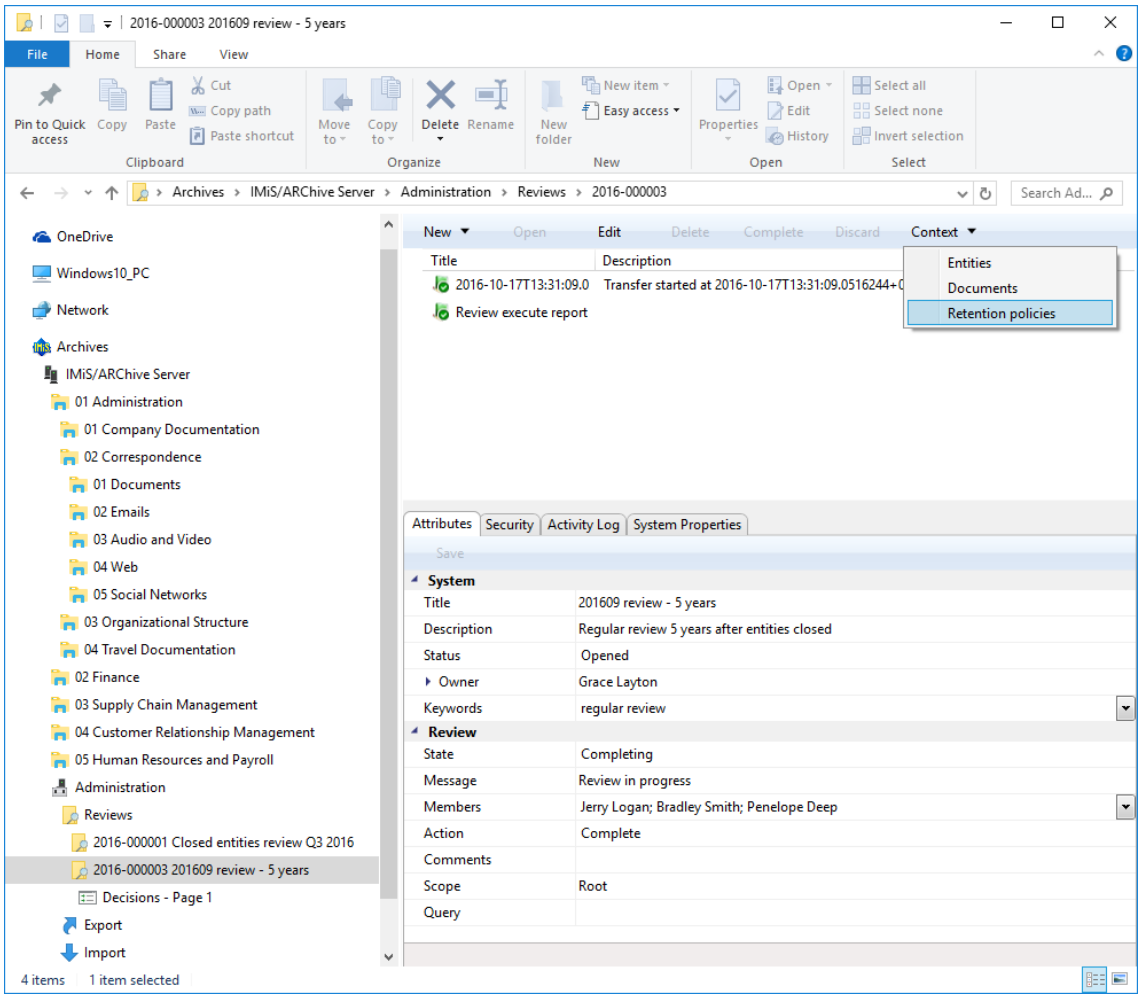


Image 229: Changing the context in retention policies

By clicking on an individual retention policy, the bottom right view shows the attributes of the selected retention policy. For a description of attributes see chapter Review process attributes.

2018 © Imaging Systems, Inc., All rights reserved.

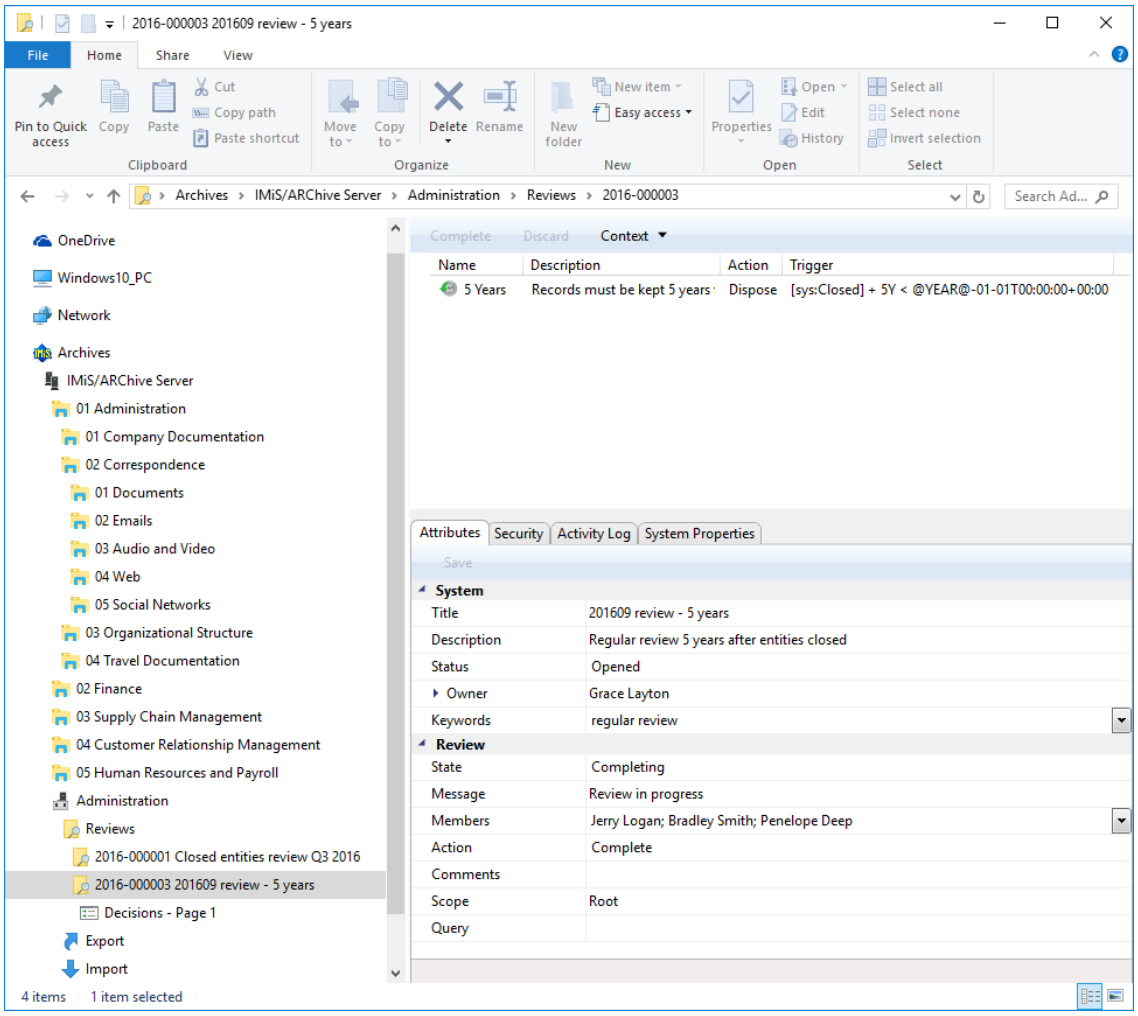


Image 230: Display of the retention policy

4.6 Reports

The IMiS®/Client enables users with a »Reports« role on the server to:

- Create reports on folders, documents and their content, as well as user access reports.
- Printing the metadata of a class, folder or document, and the classes (and folders) of the classification scheme.

Access to reports about export and import actions, which include reports on any errors encountered, is available to users that have a »Reports« role on the server and the appropriate access rights for accessing importing and exporting logs. These access rights are granted by the administrator via the »Configure« interface for access rights settings.

2018 © Imaging Systems, Inc., All rights reserved.

4.6.1 Import

Every import action to the IMiS®/ARChive Server is recorded in the »Import« folder located in the »Administration« system folder. The folder is accessed through the classification scheme of a selected archive. For more information see chapter Import.

The »Import« folder can only be accessed by users with a »Reports« role on the server. More information on roles and permissions is available in chapter Access in the IMiS®/ARChive Server manual.

By selecting the »Import« folder, the top right view will display import documents that were created during individual import events. The title of the document is identical to the date and time the import was started. If no critical error occurred during the import procedure, the document's status will be »Closed«. Documents with a »Closed« status cannot be edited.

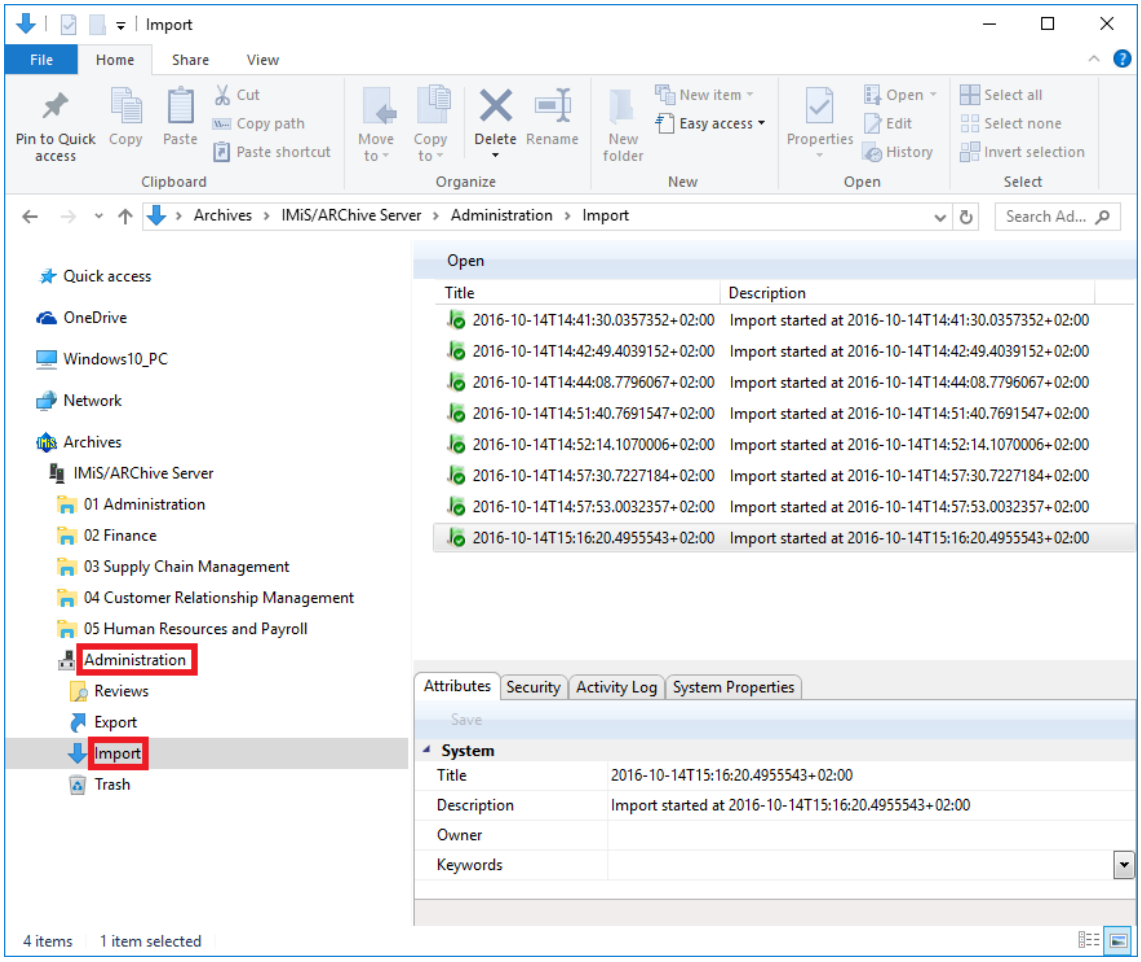


Image 231: Display of the »Import« folder in the »Administration« system folder

Each import document contains the following files:

- »XML Report«: electronically signed XML file that contains:
  - Statistics of successfully and unsuccessfully imported entities.
  - List of failed import attempts (including classification codes).
  - List of successfully imported files (including hash values and full classification codes).
- »Report«: contains a full import log for each imported entity. The log shows the success rate of import and is used to check if the import was satisfactory.
- »Error report«: contains an error log for each unsuccessfully imported entity, including the returned error. Any reasons for an import failure should be checked and fixed, if possible. Users can also attempt to enter the unsuccessfully imported entity into the archive manually.

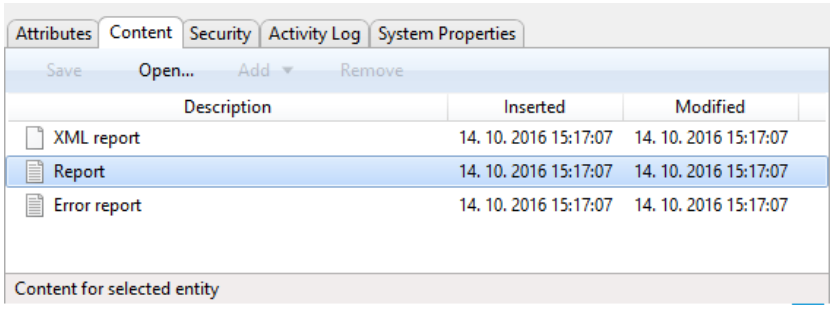


Image 232: List of content contained by an import document

The import document is opened using the »Open« command in the top command bar, or by double clicking. Import files are then listed under the »Content« tab. By double clicking the selected import file, you will open it in the default application.

2018 © Imaging Systems, Inc., All rights reserved.

```
<Report date="2016-07-27T09:30:20.6538377+02:00"><Statistics
classSuccess="1" classFailure="0" fileSuccess="1" fileFailure="0"
recordSuccess="3" recordFailure="0" /><Failure /><Success><Class
classificationCode="119.005.001.001.001.004"
oldClassificationCode="117.002.002.001"
hash="AE6CC67711D3629FBA6A8FE5D2BBC75A34C6113BB2D3FF19105DE3E4E0D
3AB6C" hash_algorithm="SHA256">ExportData\class_1.xml</Class>
<File classificationCode="119.005.001.001.001.004-2016-00001"
oldClassificationCode="117.002.002.001-2016-00001"
hash="FE030DBBBA79FECC5C84DB64E852692EFB5B375F8EDFDCAB4070060D84D
F8130" hash_algorithm="SHA256">ExportData\folder_2.xml</File>
<Record
classificationCode="119.005.001.001.001.004-2016-00001/00001"
oldClassificationCode="117.002.002.001-2016-00001/00002"
hash="F9ADC0245F1FF11B7640703E78DB3E644452763D1E64368CB6376CC4A59
5138E" hash_algorithm="SHA256">ExportData\document_3.xml</Record>
<Record
classificationCode="119.005.001.001.001.004-2016-00001/00002"
oldClassificationCode="117.002.002.001-2016-00001/00004"
hash="3283C2E06730D6308C2EBEF2B164128B69E0D23140272500E3266068F13
74E37" hash_algorithm="SHA256">ExportData\document_4.xml</Record>
<Record
classificationCode="119.005.001.001.001.004-2016-00001/00003"
oldClassificationCode="117.002.002.001-2016-00001/00007"
hash="12EBBC8A883383240C10A6EEC4FF248C3CB8B7C485F060BD792C8B9B468
D380F" hash_algorithm="SHA256">ExportData\document_5.xml</Record>
</Success><Retention_And_Disposition_Schedules /><Signature
xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-
xml-c14n-20010315" /><SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<Reference URI=""><Transforms><Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
/></Transforms><DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>kL+S35Ctb1tOdB4CUA/mrbjhkLU=</DigestValue>
</Reference></SignedInfo><SignatureValue>
EEs+eOL+M8riOVmHnKYHjaOA+hmQwguEoSndVyvPZqXjGNQonIEptZq0A5Hc1Xb66
eCNCapQK19EqxWM4kJtrsMqW3dHiqrUc4rIbGUZXgzuGyo3OD3lGTTLHBZFuD0yis
zBC0akVVQpw9UmGvZOaF/BZIjwK2J3BRBDq1DwgG4=</SignatureValue>
<KeyInfo><X509Data><X509Certificate>
MIIFKDCCAxCgAwIBAgIKckAa6gAAAAABFTANBgkqhkiG9w0BAQUFADBFMRIwEAYKC
ZImiZPyLGQBGRYCc2kxFDASBgoJkiaJk/IsZAEZFgRpbWlzMRkwFwYDVQQDExBJbW
FnaW5nU3lzdGVtc0NBMB4XDTE2MDMyOTE0MDYzOFoXDTE3MDMyOTE0MDYzOFowTzE
SMBAGCgmSJomT8ixkARkWAnNpMRQwEgYKCZImiZPyLGQBGRYEaW1pczENMAsGA1UE
CxMESU1pUzEUMBIGA1UEAxMLQWxlcyBWdWttYW4wgZ8wDQYJKoZIhvcNAQEBBQADg
Y0AMIGJAoGBAKkQrpv+NzqTTEsa699XqWnNQGWkGFHpAjvub2LJ/ozjruZgHyUvAq
/YdEMhzkAa39s5RBKVqE6NWD0rxp8jzGJV5RvDsAlwVHAfesZCzI2cmnWJdaKpd9J
zoSz2bFjp3muOSjs+FRDBMsxR6J9Z5zOkzVfAaoHXKHkovDJxFzRRAgMBAAGjggGS
MIIBjjAVBgkrBgEEAYI3FAIECB4GAEUARgBTMBUGA1UdJQQOMAwGCisGAQQBgjcKA
```


Image 233: Example signed »XML Report« file with a record of import actions

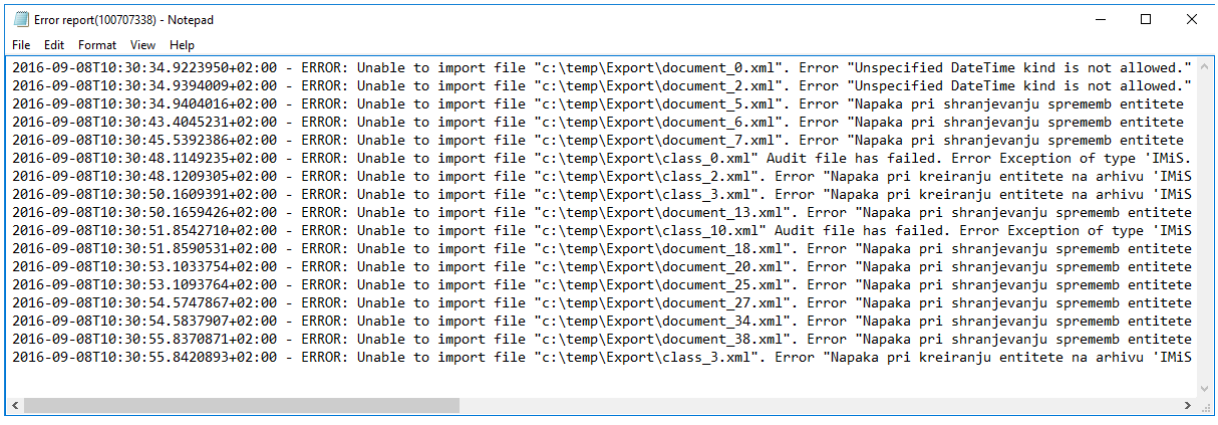


Image 234: Example »Error report« log with a list of import errors

2018 © Imaging Systems, Inc., All rights reserved.

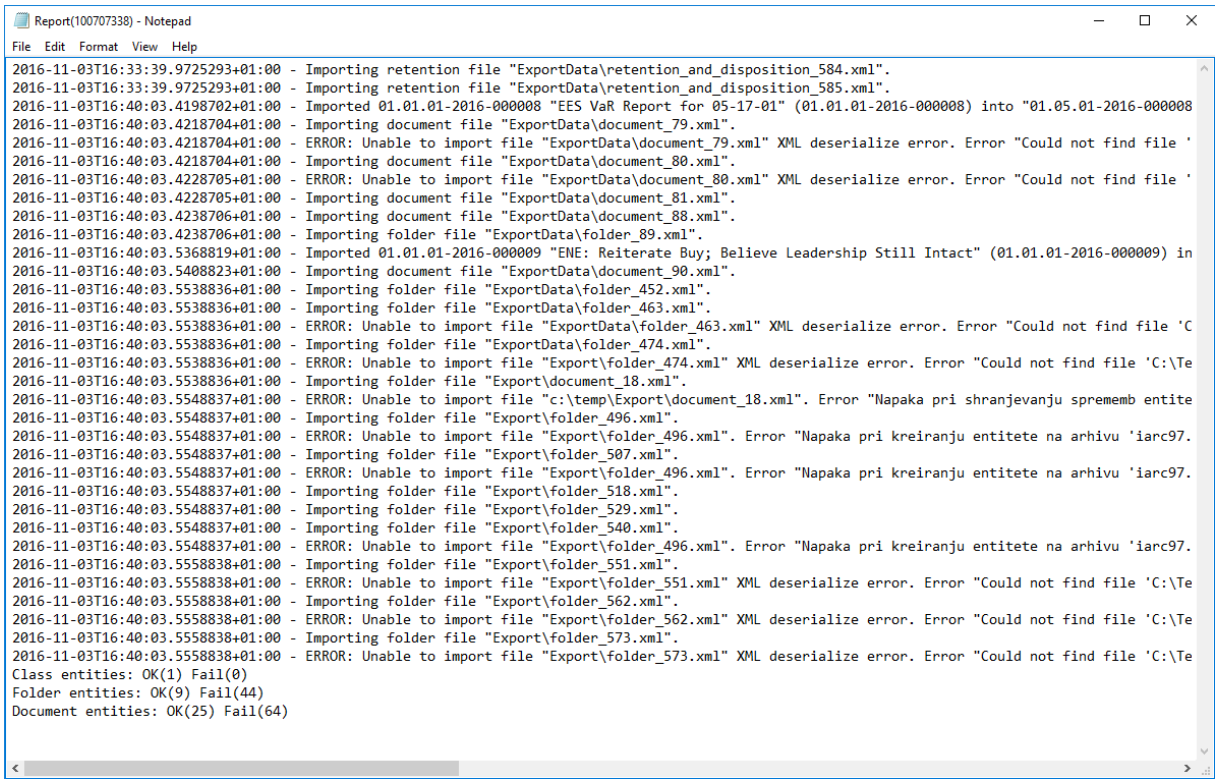


Image 235: Example »Report« log with a list of errors and the overall import success rate

4.6.2 Export

Every export action from the IMiS®/ARChive Server is recorded in the »Export« folder located in the »Administration« system folder. The folder is accessed through the classification scheme of a selected archive. For more information see chapter Export.

The »Export« folder can only be accessed by users with a »Reports« role on the server.

More information on roles and permissions is available in chapter Access in the IMiS®/ARChive Server manual.

By selecting the »Export« folder, the top right view will display export documents that were created during individual export events. The title of the document is identical to the date and time the export was started. If no critical error occurred during the export procedure, the document's status will be »Closed«. Documents with a »Closed« status cannot be edited.

2018 © Imaging Systems, Inc., All rights reserved.

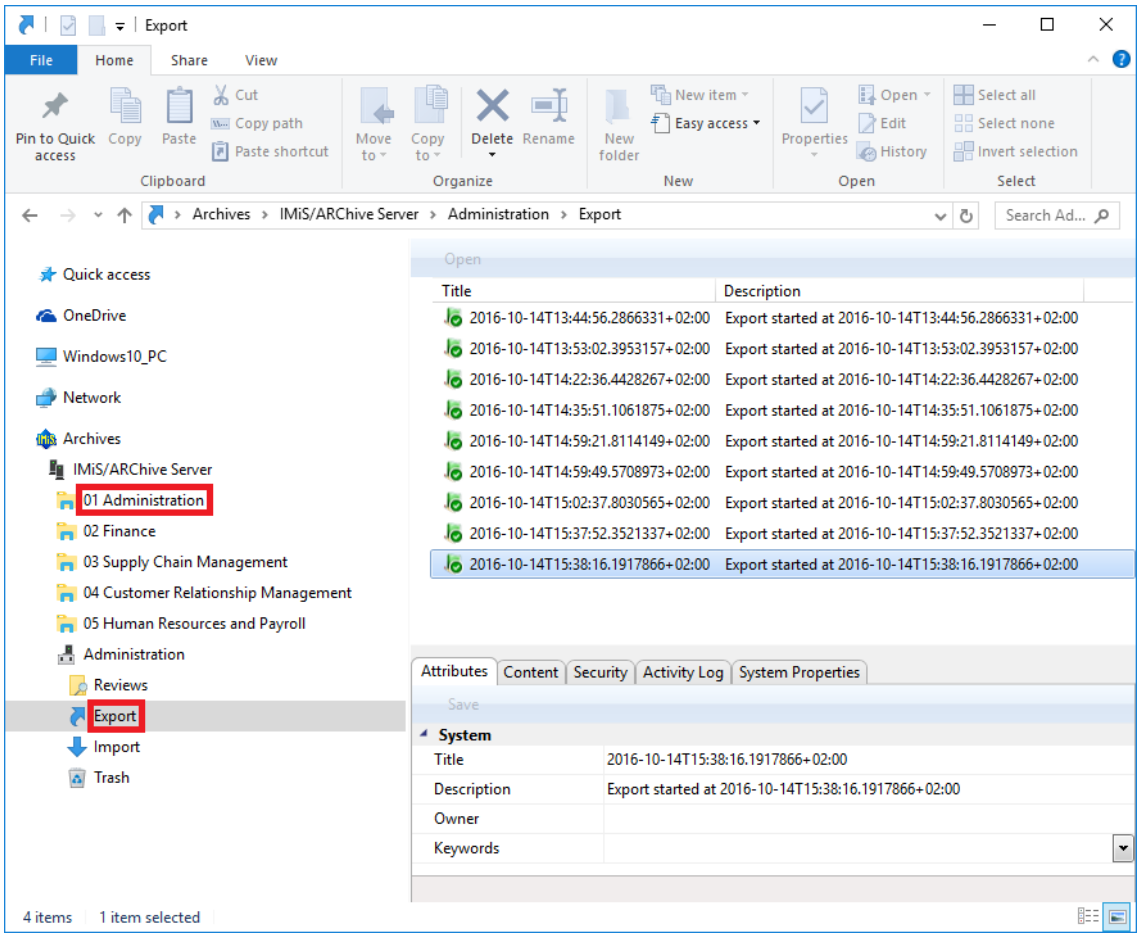


Image 236: Display of the »Export« folder in the »Administration« system folder

Each export document contains the following files:

- »XML Report«: electronically signed XML file that contains:
  - Statistics of successfully and unsuccessfully exported entities.
  - List of failed export attempts (including classification codes).
  - List of successfully exported files (including hash values and full classification codes).
- »Report«: contains a full export log for each exported entity. The log shows the success rate of export and is used to check if the export was satisfactory.
- »Error report«: contains an error log for each unsuccessfully exported entity, including the returned error.

2018 © Imaging Systems, Inc., All rights reserved.

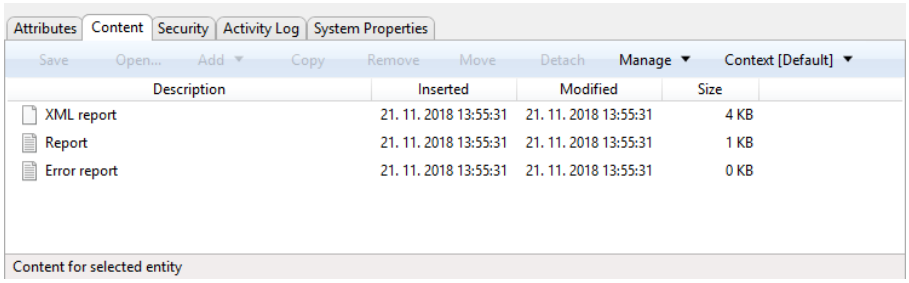


Image 237: List of content contained by an export document

The export document is opened using the »Open« command in the top command bar, or by double clicking. Content is listed under the »Content« tab. By double clicking the selected content, you will open it in the default application.

<Report date="2016-08-22T09:10:47.7845642+02:00"><Statistics classSuccess="0" classFailure="0" fileSuccess="0" fileFailure="0" recordSuccess="1" recordFailure="0" /><Failure /><Success><Record classificationCode="110-2016-00002-00001-00001-00001-00001-00001/00053" hash="6FE860A04D0B7A752C7C1AD4A19848943A9FA5032874EFB8C74C8385F9990E28" hash_algorithm="SHA256">ExportData\document_1.xml</Record></Success><Retention_And_Disposition_Schedules><Retention_And_Disposition>ExportData\retention_and_disposition_2.xml</Retention_And_Disposition><Retention_And_Disposition>ExportData\retention_and_disposition_3.xml</Retention_And_Disposition></Retention_And_Disposition_Schedules><Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" /><SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" /><Reference URI=""><Transforms><Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" /></Transforms><DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" /><DigestValue>4pJDwLgpuOtKqaz/jmV+5OeagQA=</DigestValue></Reference></SignedInfo><SignatureValue>LAwlAZRylPlHWhtVh6DPhkfcSuBOqr0iUwO8EFDZuFuF6Eb/3FkJarRwZBQSOgsS/XEVGeCKMqCQYCugPIinwWw1a0YwjGUToK8X2hy7zrA2T2LT+BU1WbcKRnSWI+OKQdxtZ0NN1CKetA0WCQdEZwJKawlALrAlz0MMFj3fmsc=</SignatureValue><KeyInfo><X509Data><X509Certificate>MIIFKDCCAxCgAwIBAgIKckAa6gAAAAABFTANBgkqhkiG9w0BAQUFADBFMRIwEAYKCZImiZPyLGQBGRYCc2kxFDASBgoJkiaJk/IsZAEZFgRpbWlzMRkwFwYDVQQDExBJbWFnaW5nU3lzdGVtc0NBMB4XDTE2MDMyOTE0MDYzOFoXDTE3MDMyOTE0MDYzOFowTzESMBAGCgmSJomT8ixkARkWAnNpMRQwEgYKCZImiZPyLGQBGRYEaW1pczENMAsGA1UECxMESU1pUzEUMBIGA1UEAxMLQWxlcyBWdWttYW4wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKkQrpv+NzqTTEsa699XqWnNQGWkGFHpAjvub2LJ/ozjruZgHyUvAq/YdEMhzkAa39s5RBKVqE6NWD0rxp8jzGJV5RvDsAlwVHAfesZCzI2cmnWJdaKpd9JzoSz2bFjp3muOSjs+FRDBMsxR6J9Z5zOkzVfAaoHXKHkovDJxFzRRAgMBAAGjggGSMIIBjjAVBgkrBgEEAYI3FAIECB4GAEUARgBTMBUGA1UdJQQOMAwGCisGAQQBgjcKAwQwCwYDVR0PBAQDAgUgMEQGCSqGSIb3DQEJDwQ3MDUwDgYIKoZIhvcNAwICAgCAMA4GCCqGSIb3DQMEAgIAgDAHBgUrDgMCBzAKBggqhkiG9w0DBzAnBgNVHREEIDAeoBwGCisGAQQBgjcUAgOgDgwMYWxlc0BpbWlzLnNpMB0GA1UdDgQWBBQyXznpb+vt4S2jB320t3tCWbDaTjAfBgNVHSMEGDAWgBSzVibb4GqcWHYAaPa+XNrklj1AFzBEBgNVHR8EPTA7MDmgN6A1hjNodHRwOi8vcGVjYS5pbWlzLnNpL0NlcnRFbnJvbGwvSW1hZ2luZ1N5c3RlbXNDQS5jcmwwXAYIKwYBBQUHAQEEUDBOMEwGCCsGAQUFBzABhkBodHRwOi8vcGVjYS5pbWlzLnNpL0NlcnRFbnJvbGwvcGVjYS5pbWlzLnNpX0ltYWdpbmdTeXN0ZW1zQ0EuY3J0MA0GCSqGSIb3DQEBBQUAA4ICAQCU1E6JuveHGuWK1t8JILM6bUyxn76htY9kWf9lhuyB0w0mKtdmJ8YgeCKbcVgGyGxzAKofc5CpIIN+KubnMSKmRgDaYp4ODc6X7IfOO76lNw4Yf9NrpbQf22agfUlYdaxS765JHZENxlGZqGPSVj4R4+7EaFlmwFVKtyHa7SNyLVSLLW3OE+YR3wCBED1RKVggLwCJTLTKKk+b5YvqI1qR

Image 238: Example »XML Report« file with a record of export actions

2018 © Imaging Systems, Inc., All rights reserved.

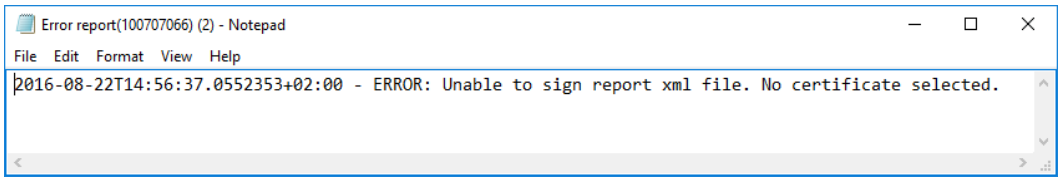


Image 239: Example »Error report« log with a list of export errors

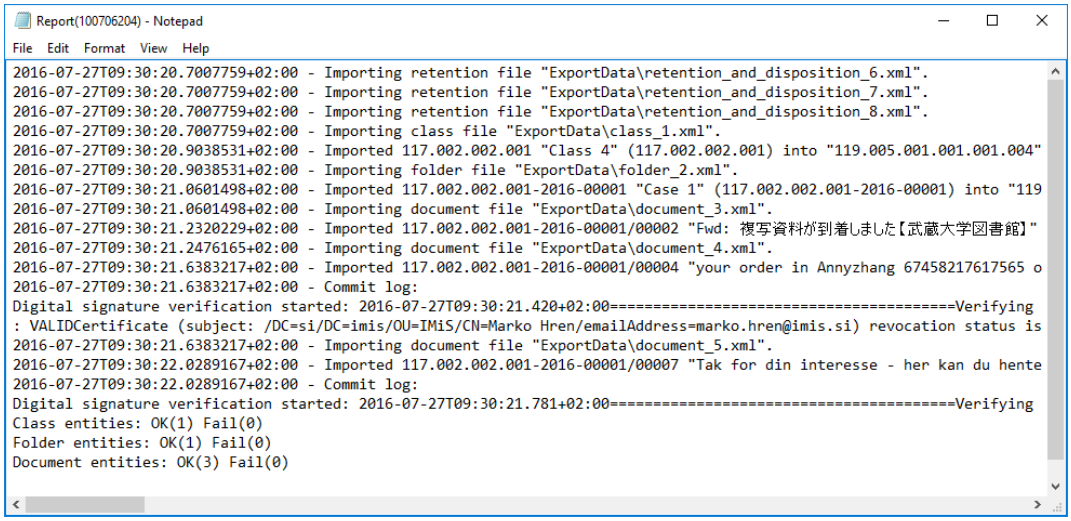


Image 240: Example »Report« log with a list of export actions and the overall export success rate

4.6.3 Deletion

Entities deleted by users appear in the »Trash« folder inside the »Administration« system folder, in their raw form.

Note: User with appropriate rights can limit user access to the »Deleted« folder by assigning explicit Deny Read right to users in the configuration folder in the context »Deleted«.

By selecting the »Trash« folder, the right view will display all the deleted entities.

The list of deleted entities shows the following entity information:

- »Classification code«: the classification code of the deleted entity.
- »Title«: the title of the deleted entity.
- »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.

2018 © Imaging Systems, Inc., All rights reserved.

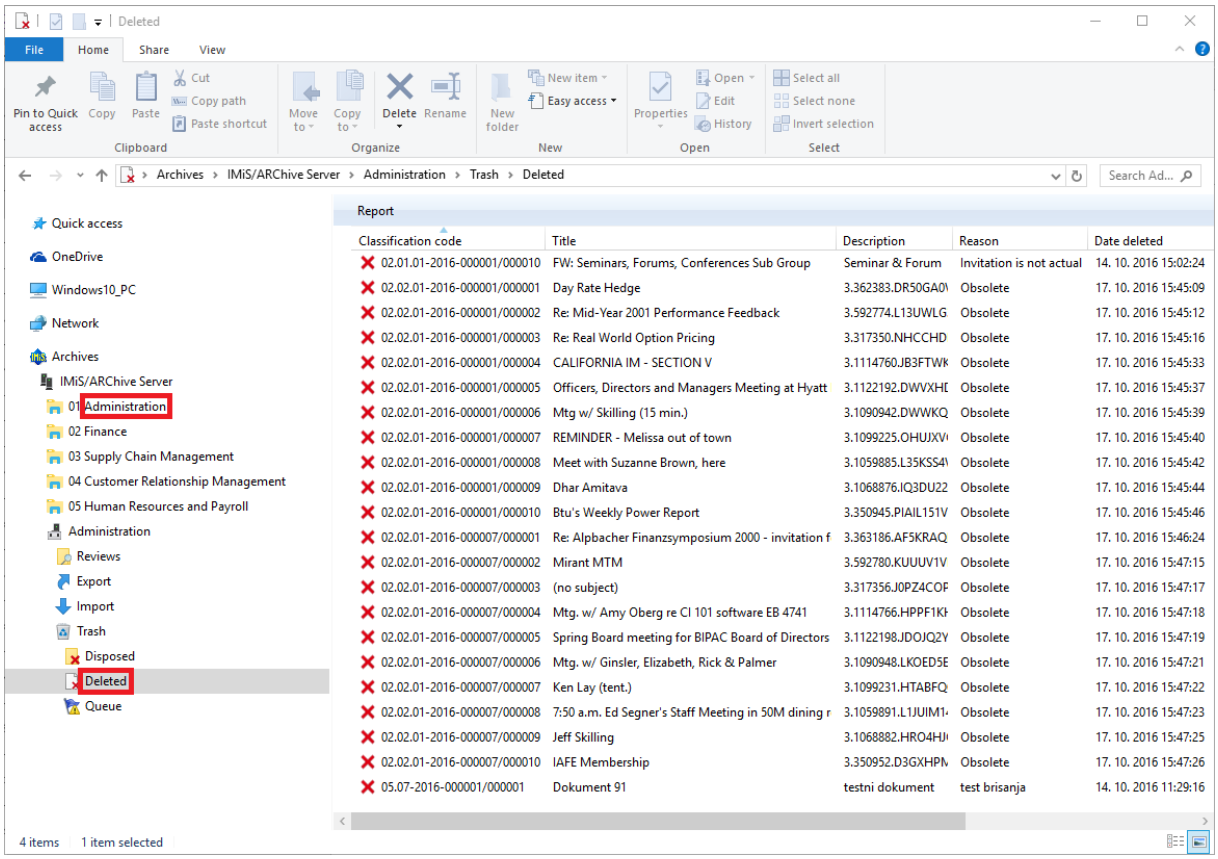


Image 241: Display of the »Trash« folder in the »Administration« system folder

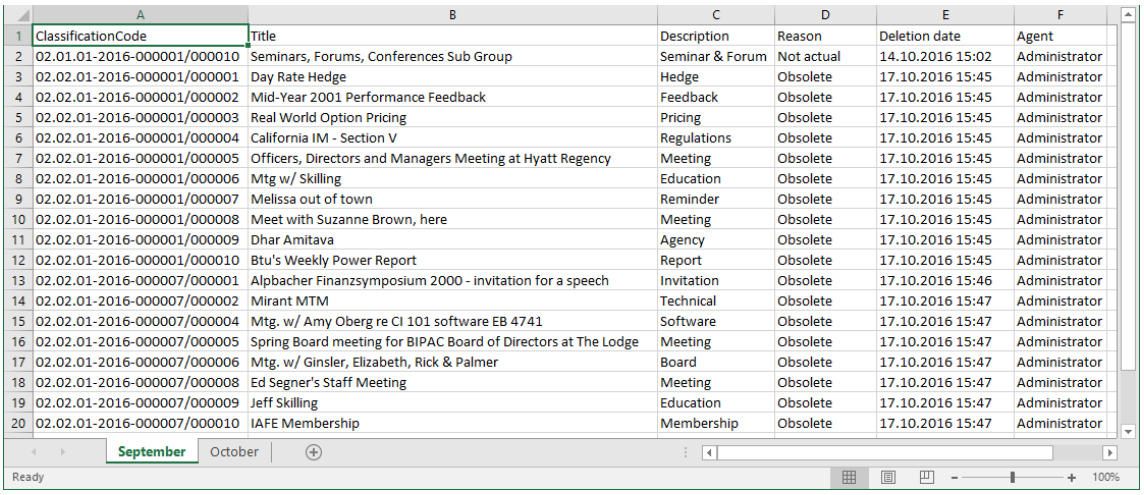
The classification code, title and description are the only attributes still preserved when an entity has been deleted. All other metadata of the entity is erased, replaced with the following attributes:

- »Reason«: the reason for deletion as it was input by the user when removing the entity.
- »Date deleted«: date and time of the entity's deletion.
- »Agent«: name of the user who executed the delete command.

Users with a »Reports« role on the server can create a report on the complete list of deleted entities (trash), which appears as a text file. In the report, individual entity attributes are separated by a comma (CSV form). The content of the report is identical to the content of the »Trash« folder.

The deleted entities report is created using the »Report« command in the top command bar of Windows Explorer and will be automatically opened in the default CVS file application.

2018 © Imaging Systems, Inc., All rights reserved.



	A	B	C	D	E	F
1	ClassificationCode	Title	Description	Reason	Deletion date	Agent
2	02.01.01-2016-000001/000010	Seminars, Forums, Conferences Sub Group	Seminar & Forum	Not actual	14.10.2016 15:02	Administrator
3	02.02.01-2016-000001/000001	Day Rate Hedge	Hedge	Obsolete	17.10.2016 15:45	Administrator
4	02.02.01-2016-000001/000002	Mid-Year 2001 Performance Feedback	Feedback	Obsolete	17.10.2016 15:45	Administrator
5	02.02.01-2016-000001/000003	Real World Option Pricing	Pricing	Obsolete	17.10.2016 15:45	Administrator
6	02.02.01-2016-000001/000004	California IM - Section V	Regulations	Obsolete	17.10.2016 15:45	Administrator
7	02.02.01-2016-000001/000005	Officers, Directors and Managers Meeting at Hyatt Regency	Meeting	Obsolete	17.10.2016 15:45	Administrator
8	02.02.01-2016-000001/000006	Mtg w/ Skilling	Education	Obsolete	17.10.2016 15:45	Administrator
9	02.02.01-2016-000001/000007	Melissa out of town	Reminder	Obsolete	17.10.2016 15:45	Administrator
10	02.02.01-2016-000001/000008	Meet with Suzanne Brown, here	Meeting	Obsolete	17.10.2016 15:45	Administrator
11	02.02.01-2016-000001/000009	Dhar Amitava	Agency	Obsolete	17.10.2016 15:45	Administrator
12	02.02.01-2016-000001/000010	Btu's Weekly Power Report	Report	Obsolete	17.10.2016 15:45	Administrator
13	02.02.01-2016-000007/000001	Alpbacher Finanzsymposium 2000 - invitation for a speech	Invitation	Obsolete	17.10.2016 15:46	Administrator
14	02.02.01-2016-000007/000002	Mirant MTM	Technical	Obsolete	17.10.2016 15:47	Administrator
15	02.02.01-2016-000007/000004	Mtg. w/ Amy Oberg re CI 101 software EB 4741	Software	Obsolete	17.10.2016 15:47	Administrator
16	02.02.01-2016-000007/000005	Spring Board meeting for BIPAC Board of Directors at The Lodge	Meeting	Obsolete	17.10.2016 15:47	Administrator
17	02.02.01-2016-000007/000006	Mtg. w/ Ginsler, Elizabeth, Rick & Palmer	Board	Obsolete	17.10.2016 15:47	Administrator
18	02.02.01-2016-000007/000008	Ed Segner's Staff Meeting	Meeting	Obsolete	17.10.2016 15:47	Administrator
19	02.02.01-2016-000007/000009	Jeff Skilling	Education	Obsolete	17.10.2016 15:47	Administrator
20	02.02.01-2016-000007/000010	IAFE Membership	Membership	Obsolete	17.10.2016 15:47	Administrator

Image 242: Example deleted entities report

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.

Note: User with appropriate rights can limit user access to the »Disposed« folder by assigning explicit Deny Read commands to users in the configuration folder »Access Control« in the context »Disposed«.

By selecting the »Disposed« folder, the right 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.

The list of disposed entities shows only the following entity information:

- »Classification code«: the classification code of the disposed entity.
- »Title«: the title of the disposed entity.
- »Description«: a description of the disposed entity.

2018 © Imaging Systems, Inc., All rights reserved.

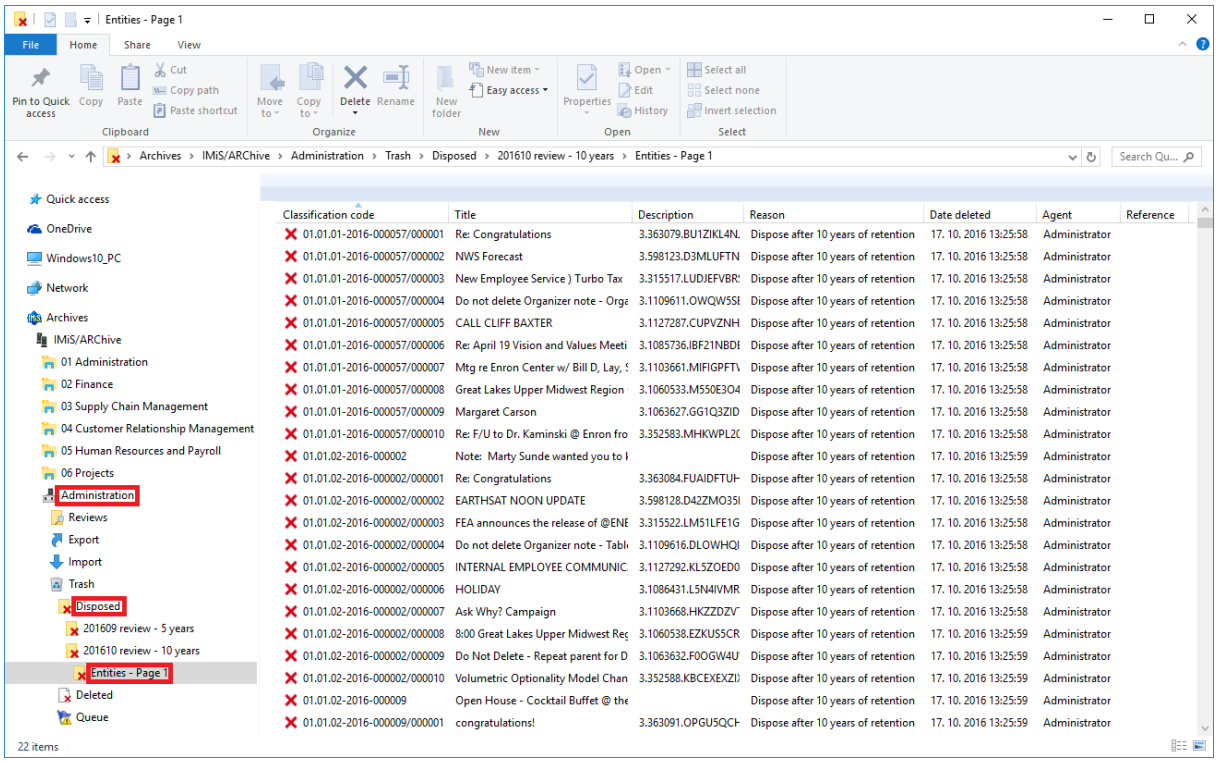


Image 243: Display of the list of disposed entities

The classification code, title and longer 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.
- »Date deleted«: the date and time of the disposition of the entity.
- »Agent«: the team member who completed the review process, thus disposing of the entity.

4.6.5 Audit log

The audit log records the audit trail and contains information about the actions of all users on a specific archived entity. Audit log reports are created by users with an »AuditLogQuery« role on the server. They may be accessed by choosing the »Audit log« command in the »Reports« section, in the right-click popup menu over the selected archive, class or folder.

2018 © Imaging Systems, Inc., All rights reserved.

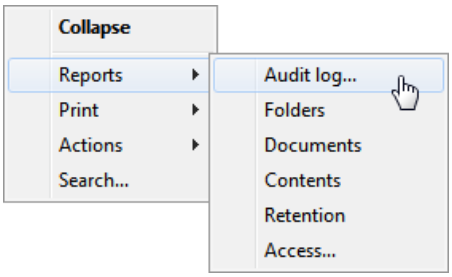


Image 244: Selecting an audit log report via the popup menu

Within the framework of audit log search settings (chapter Viewing the audit log), the user specifies the following information in the »AuditLogQuery« dialog box:

- Scope of the audit log report which may include the entire archive or just content under a specific entity.
- Types of included entities (class, folder, document); these will be included in the report along with any of their combinations.
- Time period that limits the audit log query.

In addition, a user with the »AuditLogQuery« role can limit the audit log report to:

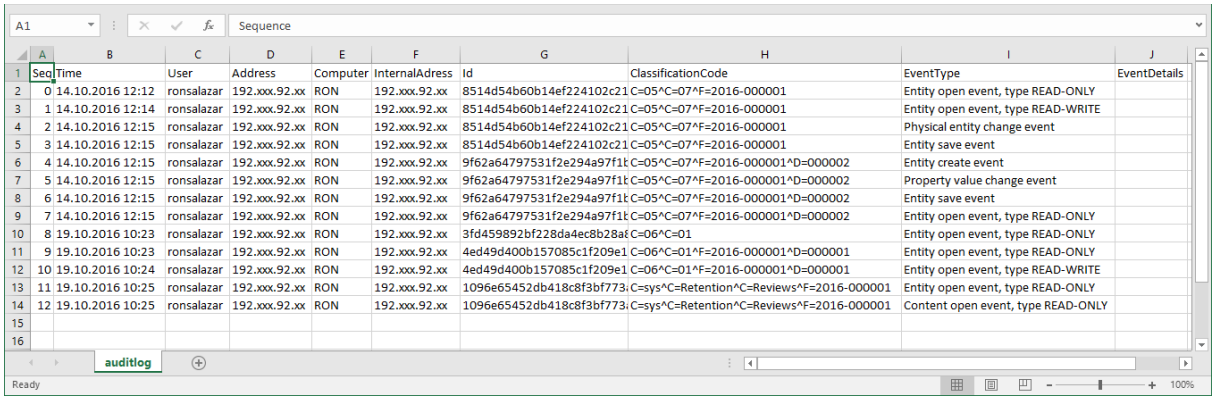
- Specific users, computer names or IP addresses.
- Specific entities or types of events.

The query results are returned in one of the available formats, as selected in the »AuditLogQuery« dialog box:

- XML file created by the IMiS®/ARChive Server.
  For more information see chapter Report format in the IMiS®/ARChive Server manual.
- CSV file listing the audit log query data in the following columns:
  - »Sequence«: sequence number of the record.
  - »Time«: time of action performed on the entity.
  - »User«: name of user who performed the action.
  - »Address«: the IP address of the computer on which the command was executed.
  - »Computer«: the name of the computer on which the command was executed.
  - »ID«: identifier of the entity on which the action was performed.
  - »ClassificationCode«: classification code of the entity in canonical form.
  - »EventType«: type of event on the entity.
  - »EventDetails«: message describing the event.

2018 © Imaging Systems, Inc., All rights reserved.

The image below shows an example audit log report in CSV form, opened in the MS Excel application where users may browse and sort the audit trail data.



Seq	Time	User	Address	Computer	InternalAdress	Id	ClassificationCode	EventType	EventDetails
0	14.10.2016 12:12	ronsalazar	192.xxx.92.xx	RON	192.xxx.92.xx	8514d54b60b14ef224102c21	C=05^C=07^F=2016-000001	Entity open event, type READ-ONLY	
1	14.10.2016 12:14	ronsalazar	192.xxx.92.xx	RON	192.xxx.92.xx	8514d54b60b14ef224102c21	C=05^C=07^F=2016-000001	Entity open event, type READ-WRITE	
2	14.10.2016 12:15	ronsalazar	192.xxx.92.xx	RON	192.xxx.92.xx	8514d54b60b14ef224102c21	C=05^C=07^F=2016-000001	Physical entity change event	
3	14.10.2016 12:15	ronsalazar	192.xxx.92.xx	RON	192.xxx.92.xx	8514d54b60b14ef224102c21	C=05^C=07^F=2016-000001	Entity save event	
4	14.10.2016 12:15	ronsalazar	192.xxx.92.xx	RON	192.xxx.92.xx	9f62a64797531f2e294a97f1	C=05^C=07^F=2016-000001^D=000002	Entity create event	
5	14.10.2016 12:15	ronsalazar	192.xxx.92.xx	RON	192.xxx.92.xx	9f62a64797531f2e294a97f1	C=05^C=07^F=2016-000001^D=000002	Property value change event	
6	14.10.2016 12:15	ronsalazar	192.xxx.92.xx	RON	192.xxx.92.xx	9f62a64797531f2e294a97f1	C=05^C=07^F=2016-000001^D=000002	Entity save event	
7	14.10.2016 12:15	ronsalazar	192.xxx.92.xx	RON	192.xxx.92.xx	9f62a64797531f2e294a97f1	C=05^C=07^F=2016-000001^D=000002	Entity open event, type READ-ONLY	
8	19.10.2016 10:23	ronsalazar	192.xxx.92.xx	RON	192.xxx.92.xx	3fd459892bf228da4ec8b28a	C=06^C=01	Entity open event, type READ-ONLY	
9	19.10.2016 10:23	ronsalazar	192.xxx.92.xx	RON	192.xxx.92.xx	4ed49d400b157085c1f209e1	C=06^C=01^F=2016-000001^D=000001	Entity open event, type READ-ONLY	
10	19.10.2016 10:24	ronsalazar	192.xxx.92.xx	RON	192.xxx.92.xx	4ed49d400b157085c1f209e1	C=06^C=01^F=2016-000001^D=000001	Entity open event, type READ-WRITE	
11	19.10.2016 10:25	ronsalazar	192.xxx.92.xx	RON	192.xxx.92.xx	1096e65452db418c8f3bf773	C=sys^C=Retention^C=Reviews^F=2016-000001	Entity open event, type READ-ONLY	
12	19.10.2016 10:25	ronsalazar	192.xxx.92.xx	RON	192.xxx.92.xx	1096e65452db418c8f3bf773	C=sys^C=Retention^C=Reviews^F=2016-000001	Content open event, type READ-ONLY	

Image 245: Example audit log report

4.6.6 Statistics

The IMiS®/Client enables users with a »Reports« role on the server to create reports dealing with the statistics of the folders, documents, content and user access on the IMiS®/ARChive Server.

Reports are opened in applications set as default for their format, or in any Windows application that can read CSV files.

4.6.6.1 Folder report

A folder report contains information about all the folders inside the selected archive, class or folder. It is created using the »Folders« command in the »Reports« section after right-clicking the selected archive, class or folder.

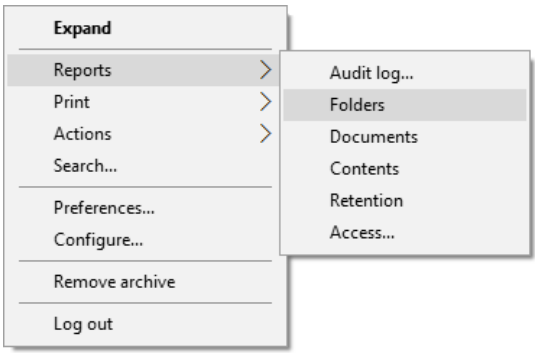


Image 246: Selecting a folder report via the popup menu

2018 © Imaging Systems, Inc., All rights reserved.

Information about folders is listed in the following columns:

- »ClassificationCode«: 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.
- »SecurityClass«: 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.
- »CurrentLocation«: the current location of the folder's physical content.
- »HomeLocation«: the home location of the folder's physical content.
- »DocumentCount«: the number of folders or documents contained inside the folder.

The image below displays an example audit log report open in Microsoft Excel, where users may sort and calculate folder data by columns.

	A	B	C	D	E
1	ClassificationCode	Title	Template	Status	DocumentCount
2	01.01.02-2016-000001	Appt w/Gilbert	Case	Opened	10
3	01.01.02-2016-000003	Meeting w/Tom Korman w/Sound Image (per Mary Whalley)	Case	Closed	10
4	01.01.02-2016-000004	Mtg.w/ Andrew Miles Enron Compression Services Re: Project Excelerator EB 2802a	Case	Closed	10
5	01.01.02-2016-000005	Brief Staff Mtg w/Liz	Case	Closed	10
6	01.01.02-2016-000007	Meeting w/Jodi Coulter - EB2801	Case	Opened	10
7	01.01.02-2016-000008	Meeting w/John Lavorato - EB2801	Case	Closed	10
8	01.01.02-2016-000010	Meeting w/Skilling, McDonald & Buy - EB4903	Case	Closed	10
9	01.01.02-2016-000013	Power companies	Case	Opened	10
10	01.01.02-2016-000014	Venture News	Case	Closed	10
11	01.01.02-2016-000016	Clickpaper report 12/2000	Case	Closed	10
12	01.01.02-2016-000019	Raptor Position Reports for 12/2000	Case	Opened	10
13	01.01.02-2016-000020	Enron Suite & Tickets - Houston Cougar Basketball	Case	Closed	10
14	01.01.02-2016-000021	Quick Phone Call w/Ann Chai (see material on your desk)	Case	Closed	10
15	01.01.02-2016-000023	Meeting w/Rebecca McDonald - EB2751	Case	Closed	10
16	01.01.02-2016-000024	CSFB: The Fuel Cell Monitor - December 2000	Case	Closed	10

October

Ready 100%

Image 247: Example folder report

4.6.6.2 Document report

A document report contains information about all the documents contained inside a selected archive, class or folder. It is created using the »Documents« command in the »Reports« section after right-clicking the selected archive, class or folder.

2018 © Imaging Systems, Inc., All rights reserved.

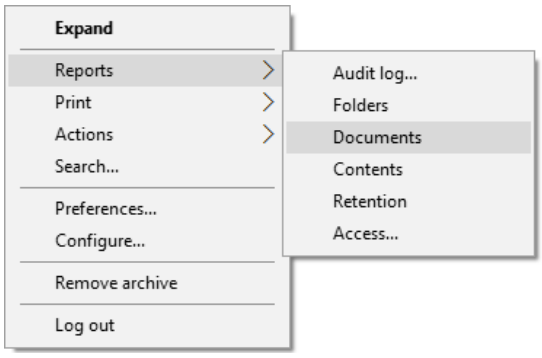


Image 248: Selecting a document report via the popup menu

Information about documents is listed in the following columns:

- »ClassificationCode«: 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.
- »Significance«: the significance of the document in the context of the archive.
- »Status«: the current status of the document in the context of the archive. Status dictates whether certain actions on the document are allowed or not.
- »CurrentLocation«: the current location of the document's physical content.
- »HomeLocation«: the home location of the document's physical content.
- »ContentCount«: the number of content(s) in the document.

The image below displays an example audit log report open in Microsoft Excel where users may sort and calculate document data by columns.

	A	B	C	D
1	ClassificationCode	Title	Template	ContentCount
2	01.01.01-2016-000001/000003	Speech by Chairman Pat Wood of PUCT - CTAEE Meeting	FiledDocument	1
3	01.01.01-2016-000001/000004	Transmission Providers and Power Marketers meeting	FiledDocument	1
4	01.01.01-2016-000001/000005	Lou Pai staff meeting EB 791	FiledDocument	1
5	01.01.01-2016-000001/000007	200 Commission Meeting	FiledDocument	1
6	01.01.01-2016-000001/000008	Govt Affairs Update Conf Call EB 1049 713-853-3233	FiledDocument	1
7	01.01.01-2016-000001/000009	Mtg. w/ Jim Steffes & Rita Hartfield	FiledDocument	1
8	01.01.01-2016-000001/000010	Headcount File	FiledDocument	1
9				

October

Ready 100%

Image 249: Example document report

2018 © Imaging Systems, Inc., All rights reserved.

4.6.6.3 Content report

The content report contains information about all the files attached to the documents inside the selected archive, class or folder. It is created using the »Contents« command in the »Reports« section after right-clicking the selected archive, class or folder.

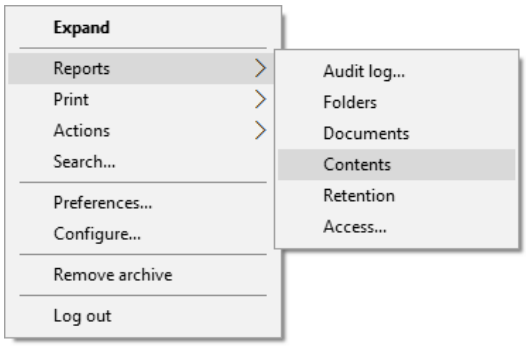


Image 250: Selecting a content report via the popup menu

Information about content is listed in the following columns:

- »ClassificationCode«: the classification code of the document whose content is being described.
- »Title«: the title of the document whose content is being described.
- »Template«: the name of the template, on which the document was created.
- »ContentDescription«: description of content (files) attached to a document.
- »ContentType«: types of content (files) attached to a document.
- »ContentSize«: sizes of content (files) attached to a document.

The image below displays an example audit log report open in Microsoft Excel where users may sort and calculate content data by columns.

2018 © Imaging Systems, Inc., All rights reserved.

	B	C	D	E	F
1	Title	Template	ContentDescription	ContentType	ContentSize
2	Speech by Chairman Pat Wood of PUCT - CTAEE Meeting	FiledDocument	00950.pdf	application/pdf	188947
3	Transmission Providers and Power Marketers meeting	FiledDocument	02650.pdf	application/pdf	172482
4	Lou Pai staff meeting EB 791	FiledDocument	01076.pdf	application/pdf	294118
5	200 Commission Meeting	FiledDocument	00565.pdf	application/pdf	361410
6	Govt Affairs Update Conf Call EB 1049 713-853-3233	FiledDocument	02058.pdf	application/pdf	340977
7	Mtg. w/ Jim Steffes & Rita Hartfield	FiledDocument	02901.pdf	application/pdf	481692
8	Headcount File	FiledDocument	02529.pdf	application/pdf	404214
9	Greg - Insurance in Australia	FiledDocument	02801.pdf	application/pdf	262147
10	Year End 2016 Feedback	FiledDocument	00950.pdf	application/pdf	188947
11	Corp. staff meeting in Energizer	FiledDocument	02650.pdf	application/pdf	172482
12	Lou Pai staff meeting EB 791	FiledDocument	01076.pdf	application/pdf	294118
13	Rick's Regional Director Conference call	FiledDocument	01491.pdf	application/pdf	251550
14	News From the Jones Graduate School of Management	FiledDocument	00565.pdf	application/pdf	361410
15	Govt Affairs Update Conf Call EB 1049	FiledDocument	02058.pdf	application/pdf	340977
16	Spring Board meeting for BIPAC Board of Directors	FiledDocument	02901.pdf	application/pdf	481692
17					

October

Ready 100%

Image 251: Example content report

4.6.6.4 Retention report

The retention report contains information on retention policies and disposition holds on all entities under the selected archive, class or folder. The user with appropriate access rights can create it with the »Retention« command in the »Reports« submenu in the pop-up menu of the selected archive, class or folder.

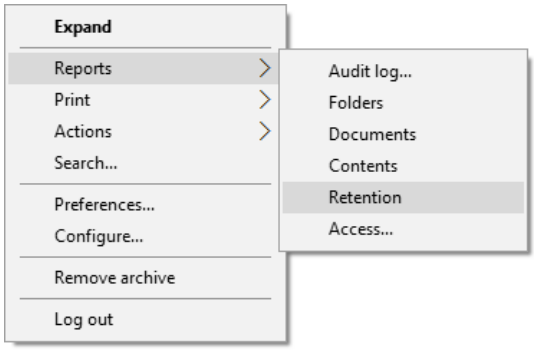


Image 252: Selecting the retention report via the pop-up menu

Information on retention is listed in the following columns:

- »ClassificationCode«: contains the classification code of the entity in the classification scheme.
- »Title«: contains the title of the entity being described.
- »Type«: contains the type of the entity being described.
- »Policy/Hold«: represents the type of entry (retention policy or disposition hold).

2018 © Imaging Systems, Inc., All rights reserved.

- »Name«: represents the name of the retention policy or disposition hold.
- »Reason«: represents the reason for the retention policy or disposition hold.
- »Description«: represents a description of the retention policy or disposition hold.

In the image below the report is open in the Microsoft Excel application, in which users can view and edit retention information by selected columns.

	A	B	C	D	E	F	G	H
1	ClassificationCode	Title	Type	Template	Policy/Hold	Name	Reason	Description
2	01.01.01-2016-000001	Farewell Dinner for Cliff Baxter	Folder	Case	Retention policy	5 Years	Records must be kept 5 years from the end of the year	Dispose after 5 years of retention
3	01.01.01-2016-000002	Mtg w/ John Thompson - EB3324	Folder	Case	Retention policy	2 Years	Records must be kept 2 years from the end of the year	Dispose after 2 years of retention
4	01.01.01-2016-000003	CSFB: Energy Technology Bulletin	Folder	Case	Retention policy	2 Years	Records must be kept 2 years from the end of the year	Dispose after 2 years of retention
5	01.01.01-2016-000004	Energy Crisis Conference Call	Folder	Case	Retention policy	Permanent	Records which need to be kept permanently	Materials of at most importance to the Company
6	01.01.01-2016-000005	EES VaR Report	Folder	Case	Retention policy	3 Years	Records must be kept 3 years from the end of the year	Dispose after 3 years of retention
7	01.01.01-2016-000006	Tax Review of California Senate	Folder	Case	Retention policy	2 Years	Records must be kept 2 years from the end of the year	Dispose after 2 years of retention
8	01.01.01-2016-000007	Mtg w/David Oxley - EB3324	Folder	Case	Retention policy	Permanent	Records which need to be kept permanently	Materials of at most importance to the Company
9	01.01.01-2016-000008	EES VaR Report for 05-17-01	Folder	Case	Retention policy	Archives	Documents of National importance	Material of National significance transferred to National Archives
10	01.01.01-2016-000009	ENE: Reiterate Buy	Folder	Case	Retention policy	3 Years	Records must be kept 3 years from the end of the year	Dispose after 3 years of retention
11	01.01.01-2016-000010	Pure-Play Energy Merchant	Folder	Case	Retention policy	2 Years	Records must be kept 2 years from the end of the year	Dispose after 2 years of retention
12	01.01.01-2016-000012	EES VaR Report	Folder	Case	Retention policy	3 Years	Records must be kept 3 years from the end of the year	Dispose after 3 years of retention
13	01.01.01-2016-000013	Mtg w/Rick Causey - EB3324	Folder	Case	Retention policy	Permanent	Records which need to be kept permanently	Materials of at most importance to the Company
14	01.01.01-2016-000014	Global Investment Strategy	Folder	Case	Retention policy	Permanent	Records which need to be kept permanently	Materials of at most importance to the Company
15								

October

Ready

Image 253: Example of a retention report

4.6.6.5 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. A report about a specific user, or about all users of the archive, is created by using the »Access« command in the »Reports« section after right-clicking the selected archive, class or folder.

Select a specific user you wish to create a report about, or select »All« in the dialog box to create a report about all the users of the archive.

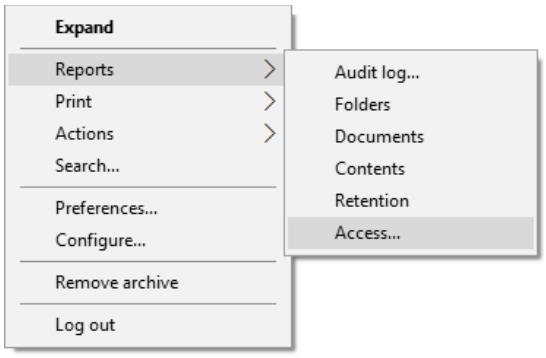


Image 254: Creating an access report on the selected user

The »Select user« options window appears, in which the user with appropriate access rights selects or wishes to create an access report about a specific user or about all the users of the archive.

If you wish to create an entity access report on all the users of the archive, select the command »All users« in the window. Otherwise select only a specific user.

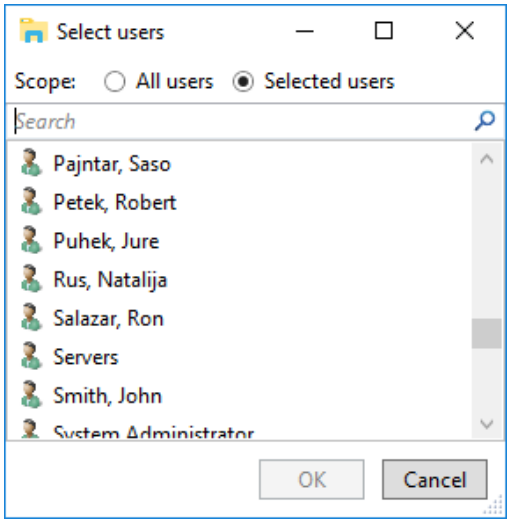


Image 255: Selecting a user or all users

By selecting the »OK« command, the user confirms the creation of a report; by selecting the »Cancel« command, he cancels it.

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

- »ClassificationCode«: 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.
- »SecurityClass«: 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.
- »CurrentLocation«: the current location of the entity's physical content.

2018 © Imaging Systems, Inc., All rights reserved.

- »HomeLocation«: 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 a »Read« access right on the folder or document.
- »Write«: this value tells if the user has a »Write« access right on the folder or document.
- »Delete«: this value tells if the user has a »Delete« access right on the folder or document.
- »Move«: this value tells if the user has a »Move« access right on the folder or document.
- »CreateSubEntities«: this value tells if the user has a »Create entities« access right on the folder or document.
- »ChangeRights«: this value tells if the user has a »Change permissions« access right on the folder or document.
- »ChangeSecurityClass«: this value tells if the user has a »Change security class« access right on the folder or document.
- »ChangeStatus«: this value tells if the user has a »Change status« access right on the folder or document.
- »ChangeRetention«: this value tells if the user has a »Change retention« access right on the folder or document.

The image below displays an example audit log report open in Microsoft Excel where users may sort and calculate content data by columns.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	ClassificationCode	Title	Type	Template	Status	Significance	SecurityClass	Current	Home	User	Read	Write	Delete	Move	CreateSub	ChangeRights	ChangeSecurity	ChangeStatus	ChangeRetention
2	01.01.01-2016-000001/000004	Transmission Providers	Document	FiledDocument	Opened	Retain	Unclassified			Grace Layton	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
3	01.01.01-2016-000001/000007	Commission Meeting	Document	FiledDocument	Opened	Retain	Restricted			Grace Layton	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
4	01.01.01-2016-000001/000010	Headcount File	Document	FiledDocument	Opened	Permanent	Top Secret			Grace Layton	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
5	01.01.01-2016-000002/000008	Govt Affairs Update	Document	FiledDocument	Opened	Permanent	Restricted			Grace Layton	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
6	01.01.01-2016-000002/000009	BIPAC Board meeting	Document	FiledDocument	Opened	Vital	Confidential			Grace Layton	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
7	01.01.01-2016-000003	Energy Technology Bulletin	Folder	Case	Closed	Retain	Unclassified			Grace Layton	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
8	01.01.01-2016-000004	Latin American Energy Crisis	Folder	Case	Closed	Vital	Restricted			Grace Layton	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
9	01.01.01-2016-000005/000003	Anonymous Reporting Facilities	Document	FiledDocument	Opened	Retain	Unclassified			Grace Layton	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
10	01.01.01-2016-000006	Tax Review of California Senate	Folder	Case	Closed	Vital	Confidential			Grace Layton	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
11	01.01.01-2016-000006/000007	Wholesale Marketing Issues	Document	FiledDocument	Opened	Retain	Unclassified			Grace Layton	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
12	01.01.01-2016-000010/000002	PAC Contributions	Document	FiledDocument	Opened	Retain	Restricted			Grace Layton	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
13	01.01.01-2016-000012/000005	Operating Committee	Document	FiledDocument	Opened	Permanent	Top Secret			Grace Layton	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
14	01.01.01-2016-000014	Global Investment Strategy	Folder	Case	Closed	Vital	Confidential			Grace Layton	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
15	01.01.01-2016-000015	NEPCO Project	Folder	Case	Closed	Permanent	Top Secret			Grace Layton	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
16	01.01.01-2016-000017/000006	Vision Focus Groups	Document	FiledDocument	Opened	Vital	Secret			Grace Layton	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
17	01.01.01-2016-000022	New Products and Countries	Folder	Case	Closed	Vital	Secret			Grace Layton	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
18	01.01.01-2016-000025/000004	National Retail Federation	Document	FiledDocument	Opened	Permanent	Confidential			Grace Layton	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
19																			
20																			

tmpB352

Image 256: Example access report on the selected user

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 open the »Directory« configuration folder and grant the following roles to other users or groups:

- »AuditLogQuery«: allows access to the audit log.
  Users with an »AuditLogQuery« role see the Activity Log tab in the entity information overview and can access the audit trail through this tab.
  User can also create audit log reports for the complete archive or for individual entities by opening the appropriate Reports / AuditLog popup menu.
- »Content management«: the role enables content management.
  The user with the »Content management« role can tag content for indexing or conversion.
- »ImportExport«: this role enables the import and export of entities.
  Users with the »ImportExport« role can execute »Import« and »Export« actions on the archive or individual entities by opening the appropriate popup menu.
- »Reports«: this role enables the display of system reports on imports, exports, access, folders, documents, contents and retention periods.
  User can also print the metadata of a class, folder or document, and the classes (and folders) of the classification scheme.
- »Draft Management«: this role enables viewing and filing/discarding a document draft of other users (combined with the entity access permissions).

2018 © Imaging Systems, Inc., All rights reserved.

5 SYSTEM REQUIREMENTS

The following are system requirements for IMiS®/Client installation.

5.1 Hardware

Most current workstations and computers should be able to run the IMiS®/Client without problems, as it requires few resources and operates smoothly in virtual environments.

5.1.1 Minimum requirements

- Must satisfy the minimum requirements of the installed operating system.
- Size of available work memory should be at least 256 MB larger than the operating system's memory requirements.
- Minimum free disk capacity for installing the IMiS®/Client is 200 MB.
- TCP/IP network access (IPv4 or IPv6).

5.1.2 Recommended hardware

- Size of available work memory should be about 1 GB larger than the operating system's memory requirements.
- Minimum free disk capacity for installing the IMiS®/Client is 1 GB.
- TCP/IP network access (IPv4 or IPv6).

5.1.3 Hardware supervision

IMiS®/Client requires no particular hardware supervision in addition to the platform's requirements.

5.2 Software

5.2.1 Operating systems

IMiS®/Client works on Windows 32-bit or 64-bit operating systems.

Below is a list of supported Windows versions:

- Windows 7 (32-bit or 64-bit)
- Windows 8 (32-bit or 64-bit)
- Windows 8.1 (32-bit or 64-bit)
- Windows 10 (32-bit or 64-bit).

2018 © Imaging Systems, Inc., All rights reserved.

5.2.2 Minimum requirements

IMiS®/Client requires Microsoft .NET Framework 4.0.

6 INSTALLATION

This chapter describes the installation procedure. The IMiS®/Client can be installed by an administrator or any other user with the appropriate software installation rights.
The installation is conducted step-by-step and is the same for everyone.

6.1 Installation procedure

The product must be installed in an environment that satisfies minimum requirements.
To install the IMiS®/Client, you must have local administration rights on the computer.
Installation is conducted using the install wizard, which provides a step-by-step installation procedure. Recommended system specifications are advised for optimal performance.
Installation is executed by launching the installer package.

Example: When launching the installer package:
IMiS.Client.9.9.1810.x64.msi

The following window appears:

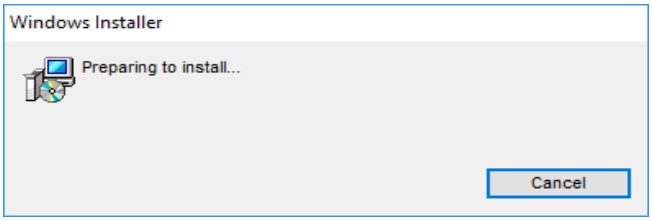


Image 257: Preparing to install

Next, a dialog box with the install wizard is shown, prompting the administrator to continue with the installation or cancel it.

2018 © Imaging Systems, Inc., All rights reserved.

Image 258: Beginning the IMiS®/Client installation procedure

During each step, the administrator may:

- Continue to the following step by choosing »Next«.
- Return to the previous step by choosing »Back«.
- Cancel the installation procedure by choosing »Cancel«.

If installation is interrupted using the »Cancel« command, a dialog box will appear asking the user to confirm the cancellation.

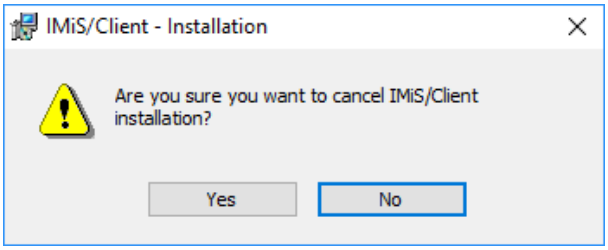


Image 259: Cancelling the IMiS®/Client installation procedure

If the installation procedure is cancelled, any already installed files and Windows registry settings are deleted.

2018 © Imaging Systems, Inc., All rights reserved.

The next step will prompt you to carefully read the license agreement.

If you agree to the terms and conditions, choose »I accept the terms in the license agreement« which signifies your explicit acceptance of the licensing terms and conditions. If you disagree with the terms and conditions, choose »I do not accept the terms in the license agreement« and abort the installation procedure by choosing »Cancel«.

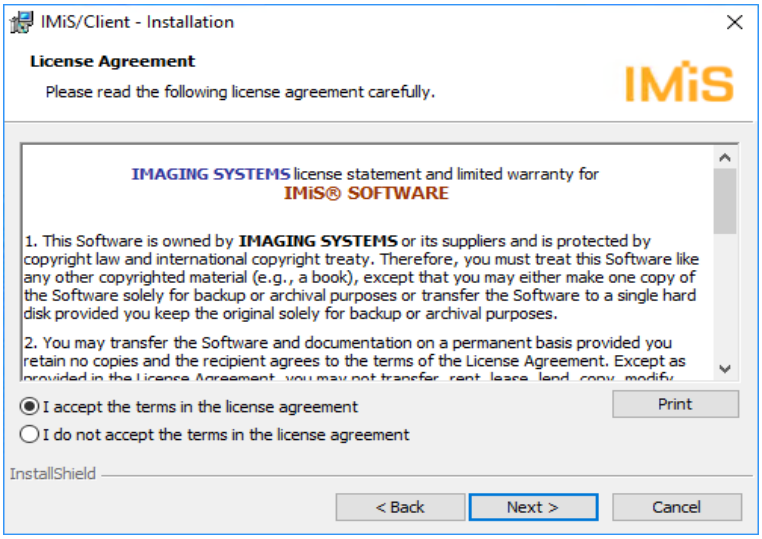


Image 260: Reviewing and accepting the license agreement

The administrator continues by entering the customer information, the user name in the »User Name« field and the organization's name in the »Organization« filed. The next choice is to install the application only for the current user by choosing »Only for me«, or for all users on this computer by choosing »Anyone who uses this computer«.

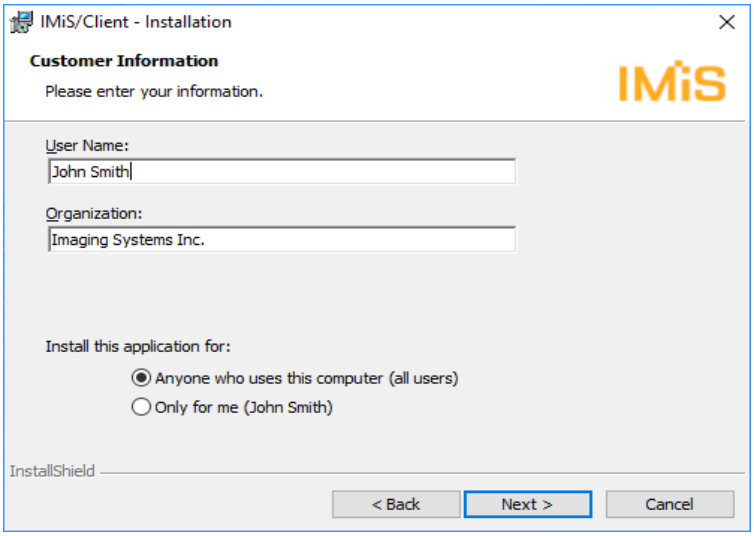


Image 261: Customer information dialog box

The next step is a choice between »Complete« or »Custom« setup type. Choosing »Complete« will perform a full install of all the files in the install package.

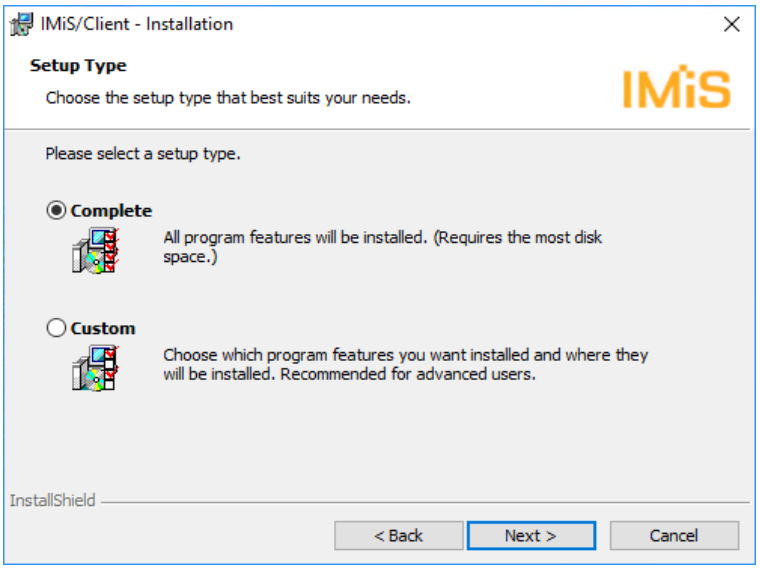


Image 262: Choice between complete and custom installation

When choosing the »Custom« setup type, you will receive the following dialog box:

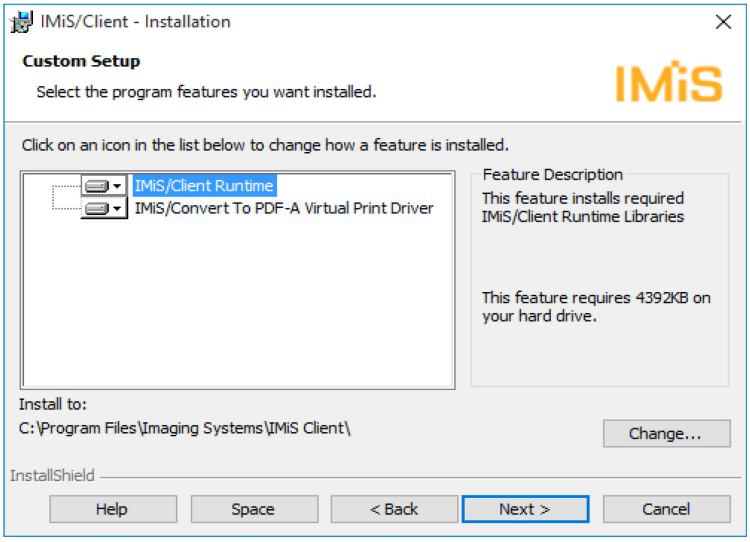


Image 263: Selecting the elements and location of IMiS®/Client installation

Choosing the »Help« command will open the following setup tips:

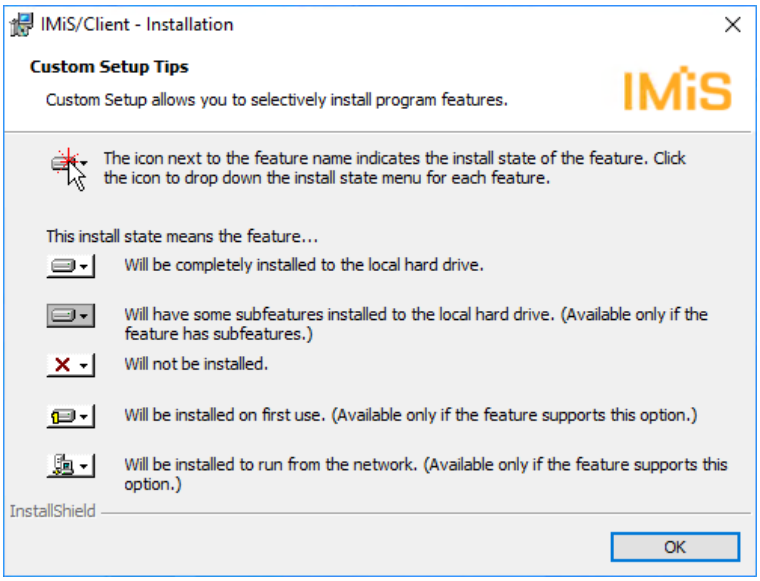


Image 264: Description of the installation element icons

By choosing »Change«, the administrator can change the IMiS®/Client's installation path.

A dialog box appears, prompting the selection of a preferred destination folder, which is then confirmed using the »OK« button.

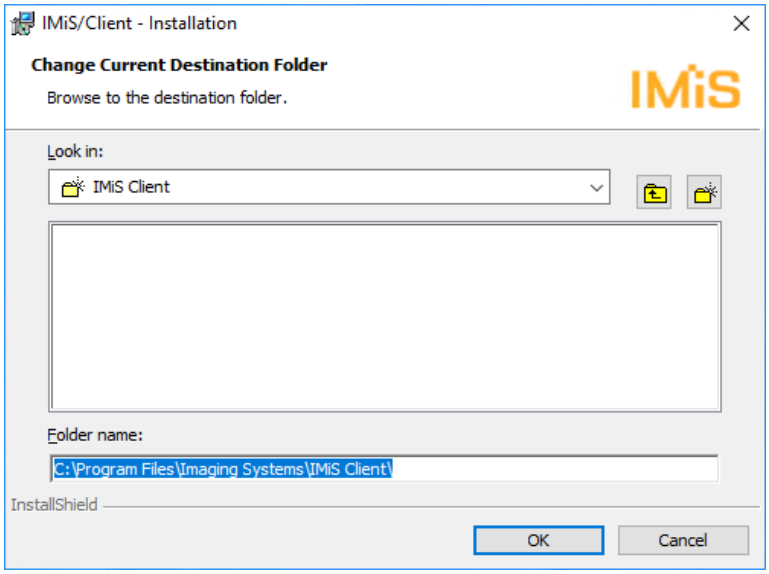


Image 265: Selecting the destination folder

2018 © Imaging Systems, Inc., All rights reserved.

By choosing »Space«, the administrator can check if there is enough space in the selected location. A dialog box appears listing all the accessible disks, their size and available space. Disks with insufficient space are highlighted.

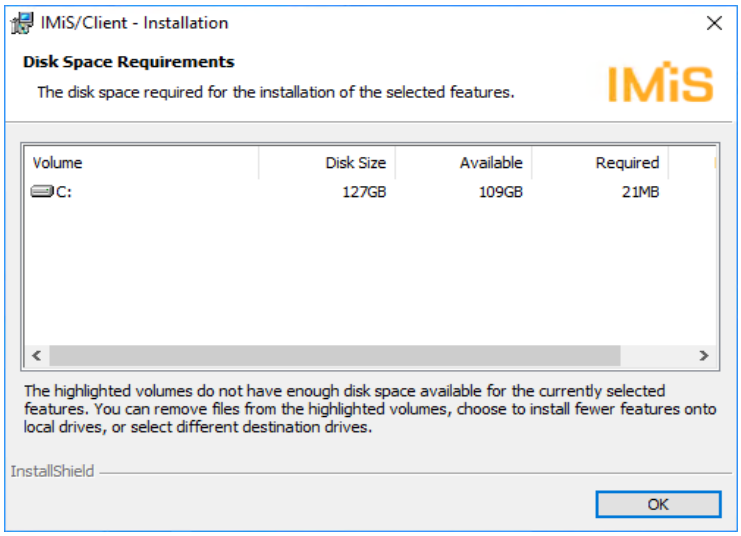


Image 266: Available disk space

The selection of custom IMiS®/Client installation elements is the following:

- »IMiS/Client Runtime«: installs the runtime libraries of the IMiS®/Client.
  This element is required for installation and cannot be removed.
- »IMiS/Convert To PDF-A Virtual Printer Driver«: installs the virtual printer driver, which can be used to convert documents to PDF/A format.
  This element can be removed through a popup menu.

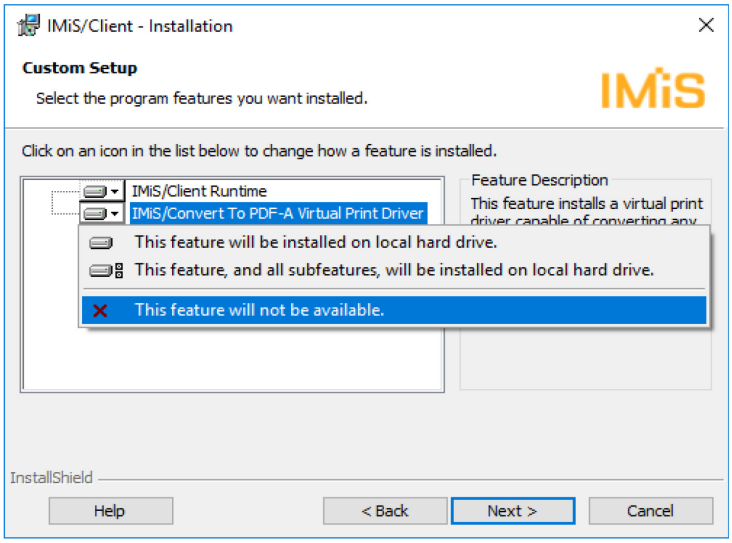


Image 267: Removing the printer driver during custom install

The next step of the installation wizard prompts you to select one or more locations for the »Archives« virtual folder of the IMiS®/Client, within the framework of Windows Explorer's left view:

- »Computer«: the Archives folder is installed under the »Computer« folder.
- »Desktop«: the Archives folder is installed under the »Desktop« folder.
  This choice also offers the »Desktop Icon« option. Selecting it will create an Archives folder icon on the computer's desktop.
- »Network«: the Archives folder is installed under the »Network« folder.

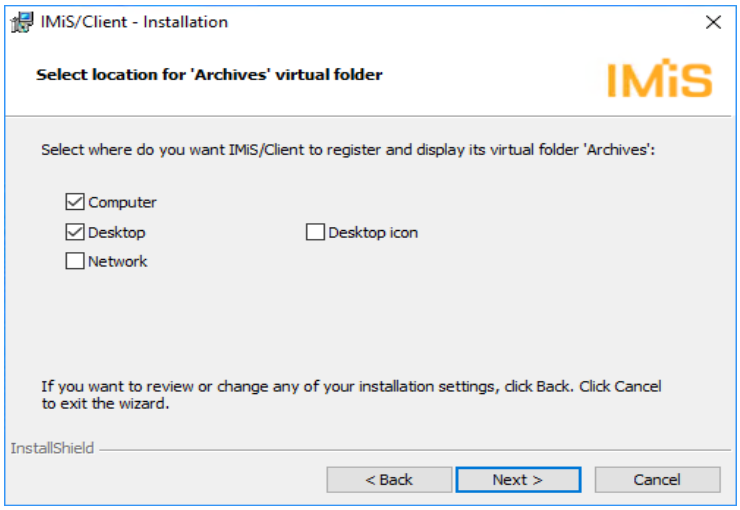


Image 268: Selecting the location of the Archives folder

The next step prompts you to confirm the selected settings and begin installation by clicking »Install«.

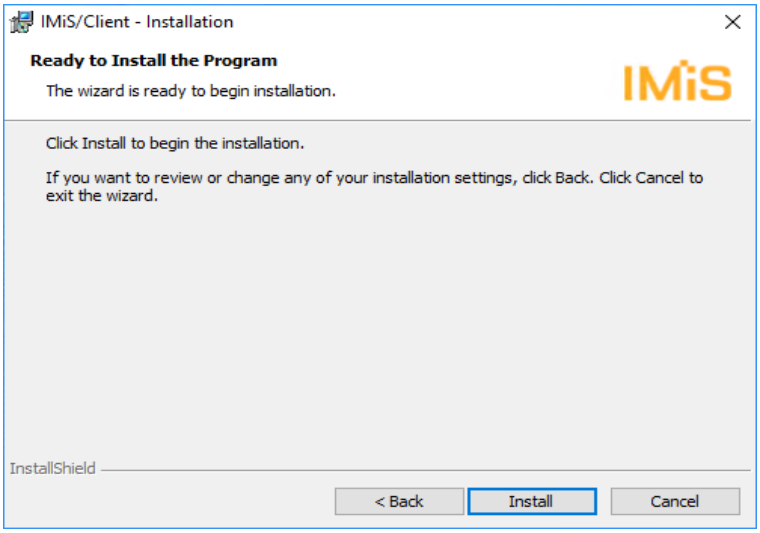


Image 269: Confirming settings to begin installation

2018 © Imaging Systems, Inc., All rights reserved.

The installation of the IMiS®/Client requires administrator privileges. If the »User Access Control« window appears during installation, you must select »Yes« to agree to the installation or it will be aborted.

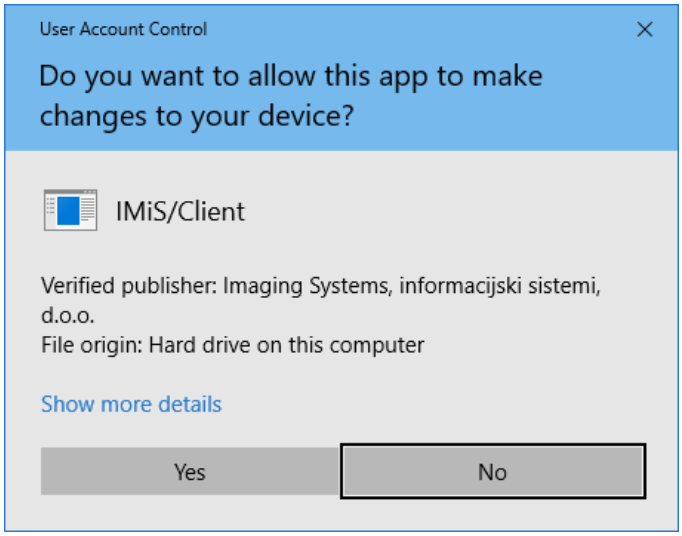


Image 270: Security warning notification

When all the above steps are complete, the installation procedure of the IMiS®/Client begins. The progress bar shows the progress of copying files to the selected location.

The installation takes anywhere between a couple of seconds and a few minutes, depending on the chosen installation package and the speed of the computer.

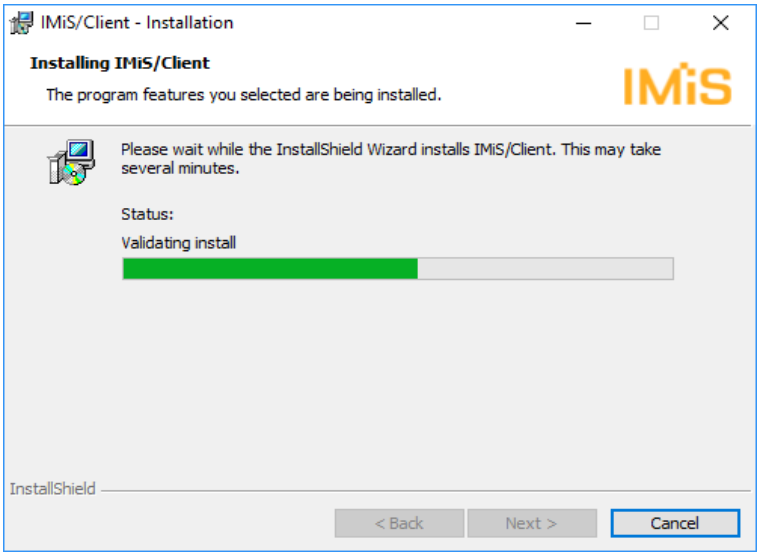


Image 271: Installation progress bar

Installation is completed by clicking »Finish« in the final dialog box.

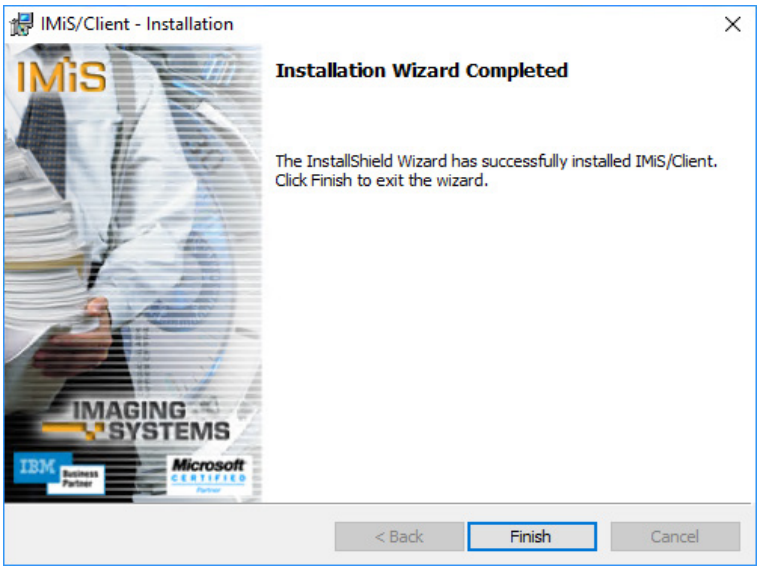


Image 272: Installation complete message

Unless the administrator removed the installation of the »IMiS/Convert To PDF-A Virtual Printer Driver« during custom setup, a new virtual printer named »IMiS Convert To PDF-A« will appear on the computer. It can be used to create PDF/A files using the application of your choice.

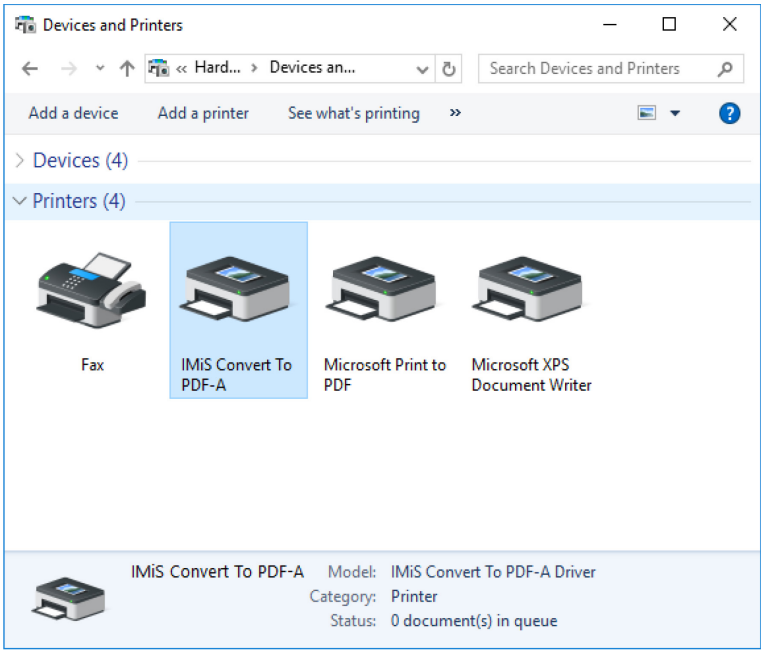


Image 273: Virtual printer installation

7 UNINSTALLATION

IMiS®/Client can be uninstalled by the local administrator or by any user with the equivalent privileges.

7.1 Uninstallation procedure

To uninstall the IMiS®/Client, administrator privileges are required. The client is uninstalled using the standard Windows application »Add or Remove Programs«.

To open it, select the »Start« command and enter »Add or remove programs« in the search field to retrieve the link, then click it.

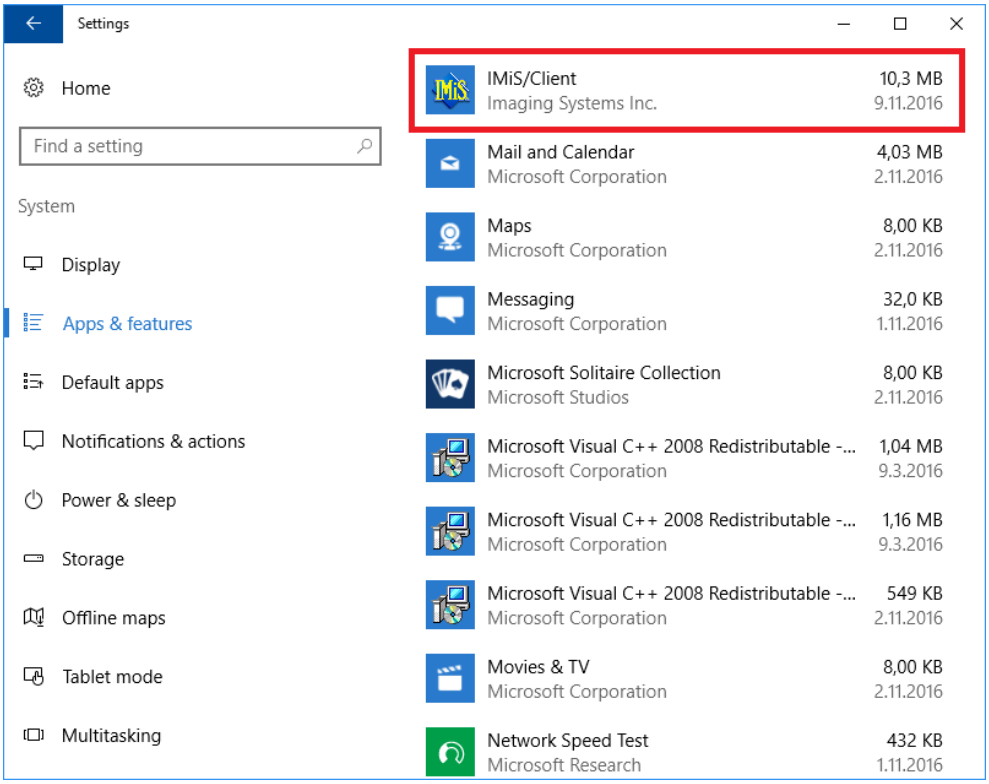


Image 274: Uninstalling the IMiS®/Client

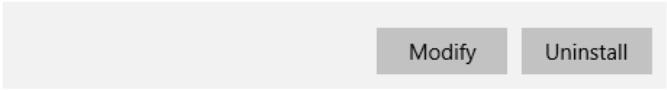


Image 275: Selecting the »Uninstall« command

2018 © Imaging Systems, Inc., All rights reserved.

If »Uninstall« command is confirmed, the uninstallation procedure will begin. The progress is displayed in the progress bar window. Uninstallation can still be cancelled at this time, by selecting the »Cancel« command.

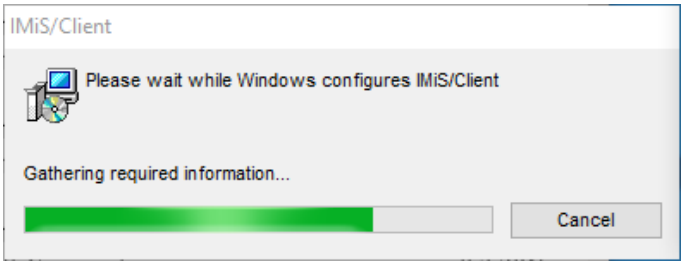


Image 276: Uninstallation progress bar

In the next step the user with appropriate rights must ensure that all applications that affect the process of removing the IMiS®/Client are closed.

By choosing the default command »Automatically close applications and attempt to restart them after setup is complete« and confirming the selection with »OK«, the applications from the list are closed.
An alternative option is to select the command »Do not close applications. (A reboot may be required), which performs the removal even though the applications from the list remain open. The process of removal continues.

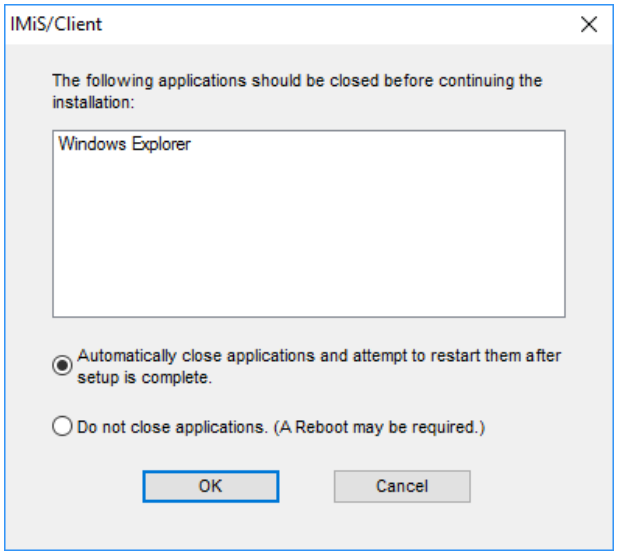


Image 277: A confirmation of the closure of applications due to IMiS®/Client removal

2018 © Imaging Systems, Inc., All rights reserved.

Installing the IMiS®/Client requires administrator rights. If during the installation a dialog box »User Access Control« is shown, the user confirms that he agrees with the removal by selecting »Yes«. Otherwise the removal will fail.

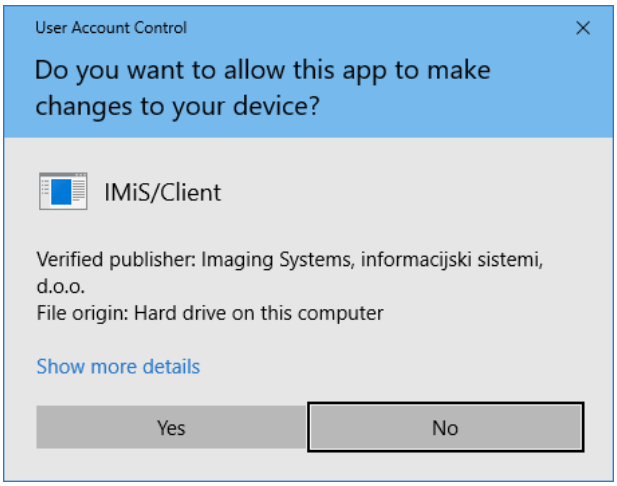


Image 278: Displaying security warning

The process of IMiS®/Client removal begins. A progress bar shows the progress of file transfer to the appropriate locations. The removal process removes all files and settings created by the installation package. Removal takes a few seconds.

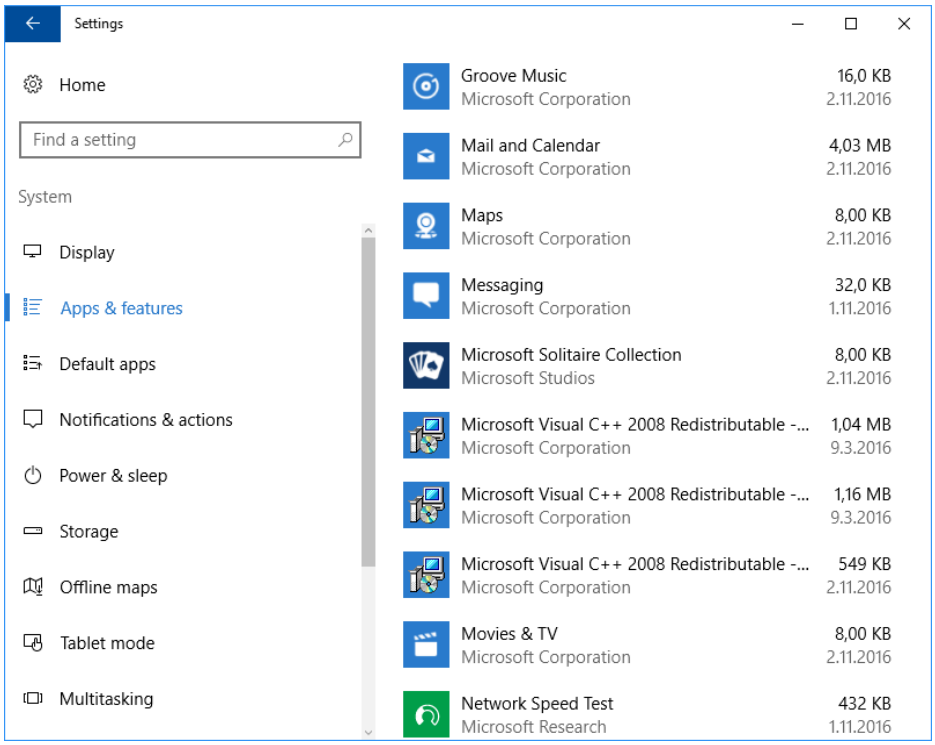


Image 279: IMiS®/Client has been removed from the computer

IMiS®/Client can also be removed using the »Modify« command.

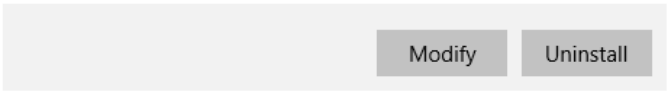


Image 280: Selecting the »Modify« command

It opens the initial window of the install wizard where modification, repair or removal of the client can be started by selecting »Next«.

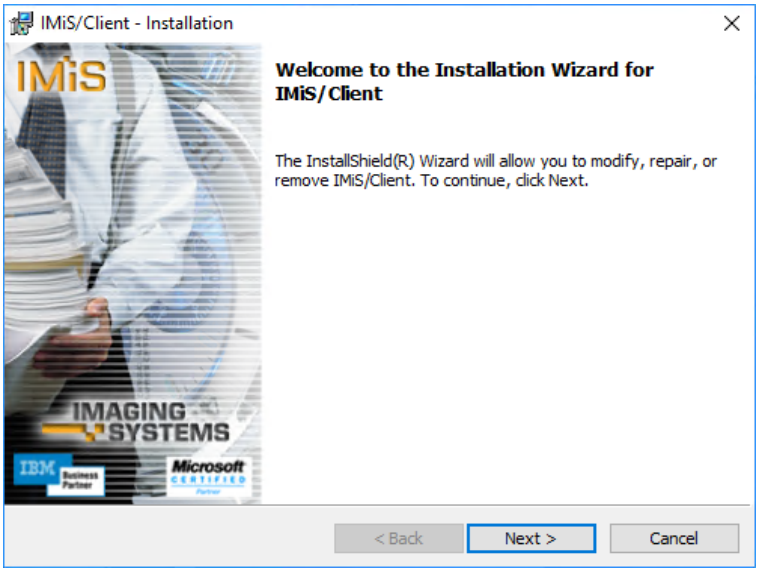


Image 281: Opening the IMiS®/Client program maintenance

If the administrator continues the procedure, the next dialog box offers the option to modify, repair or remove the client, which can be uninstalled using the »Remove« and then »Next« command.

2018 © Imaging Systems, Inc., All rights reserved.

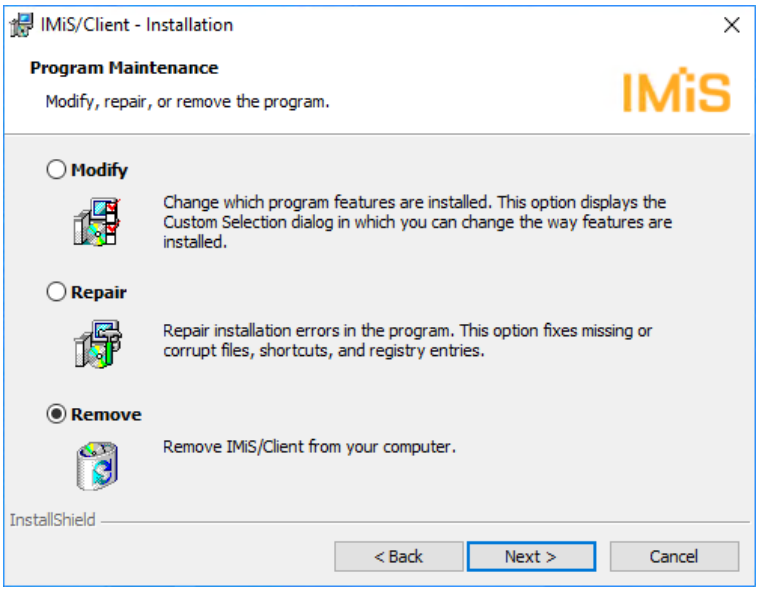


Image 282:Selecting a program maintenance action for the IMiS®/Client

At the next step, uninstallation is confirmed by clicking »Remove«.

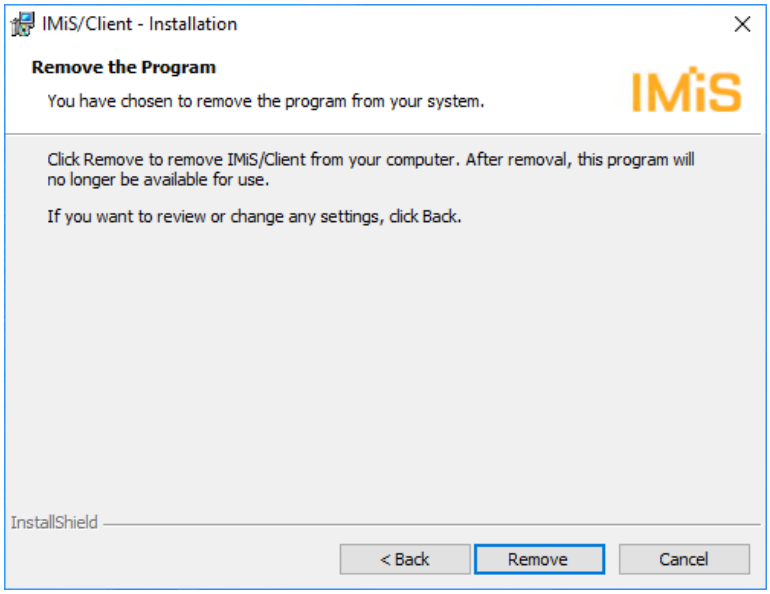


Image 283: Confirming IMiS®/Client uninstallation

IMiS®/Client removal process has begun. A progress bar shows the progress of file removal from the appropriate locations. Removal takes a few seconds.

2018 © Imaging Systems, Inc., All rights reserved.

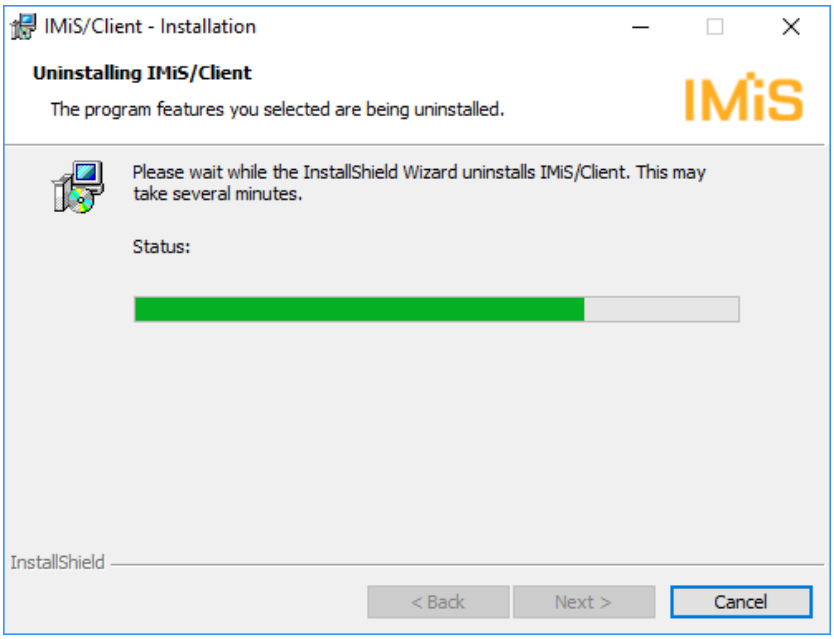


Image 284: Selecting »Uninstall« command

If the »User Access Control« window appears during uninstallation, you must select »Yes« to agree to the uninstallation or it will be aborted.

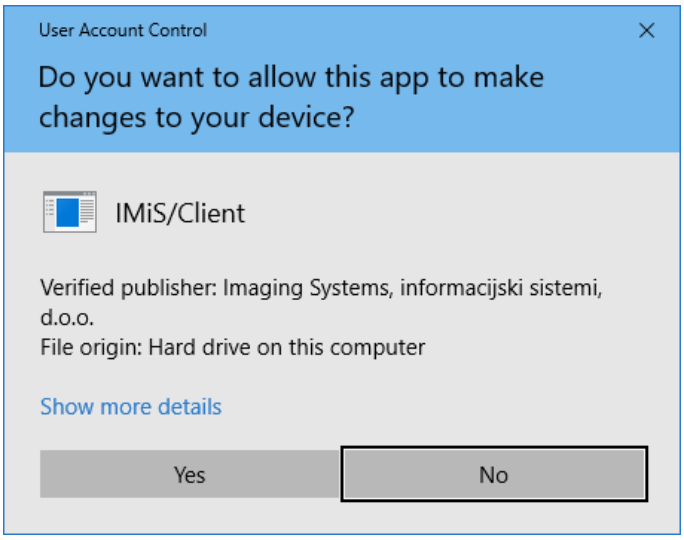


Image 285: Security warning prompt

Uninstallation takes anywhere between a couple of seconds and a few minutes, depending on the installed package and the speed of the computer. When the process is complete, a »Finish« dialog box lets you know the client was successfully uninstalled.

2018 © Imaging Systems, Inc., All rights reserved.

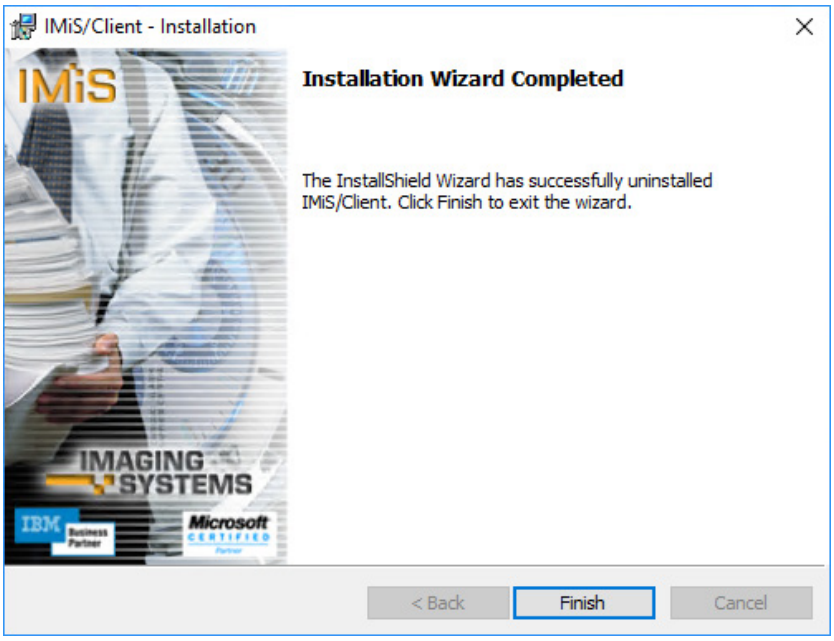


Image 286: Uninstallation complete message

8 PRODUCT MANAGEMENT

IMiS®/Client can be managed by an administrator, as well as regular users.

8.1 Startup and closing

IMiS®/Client starts up when you start the Windows Explorer. The user interface of the client is integrated into the user interface of Explorer.

When you first start Windows Explorer once the client has been installed, the only new folder appearing in the left view of explorer is the »Archives« folder.
To access an IMiS®/ARChive Server, you have to manually add it into the »Archives« folder.
For more information on this procedure see chapter Adding an IMiS®/ARChive Server.
Users must log in before they can access the archive.
For more information see chapter Login and logout.

IMiS®/Client is closed by logging out of the archive using the »Log out« command.

Warning: closing the Windows Explorer window does not log you out of the client.

2018 © Imaging Systems, Inc., All rights reserved.

8.2 Event log

The IMiS®/Client event log is used to monitor activities, which is performed by the administrator according to need. It is especially useful when something goes wrong and you wish to pinpoint the cause of the error.

The client records operations in a rotating event log stored in the temporary system folder »%TEMP%« accessible via the Windows Explorer. The name of the log file is IMiS.Client.NET.X.log , where X is the generation number that specifies the generation of the rotating log file.
The number of rotating log files is capped at 10, and each file is limited to a maximum size of around 1MB. The newest event log is the one with the generation number 0, into which events are being currently recorded, and the oldest one is the one with the highest generation number.

The log file records the following data:

- Date and time of the log entry.
- Process and Thread ID, separated by a colon.
- Name of the module or DLL library that recorded the entry.

During normal operation, the entry continues with the:

- Name of the method that was conducted during log entry, which appears inside the characters < and >.
- Operation message, which briefly describes the current operation or state of the client.

2018 © Imaging Systems, Inc., All rights reserved.

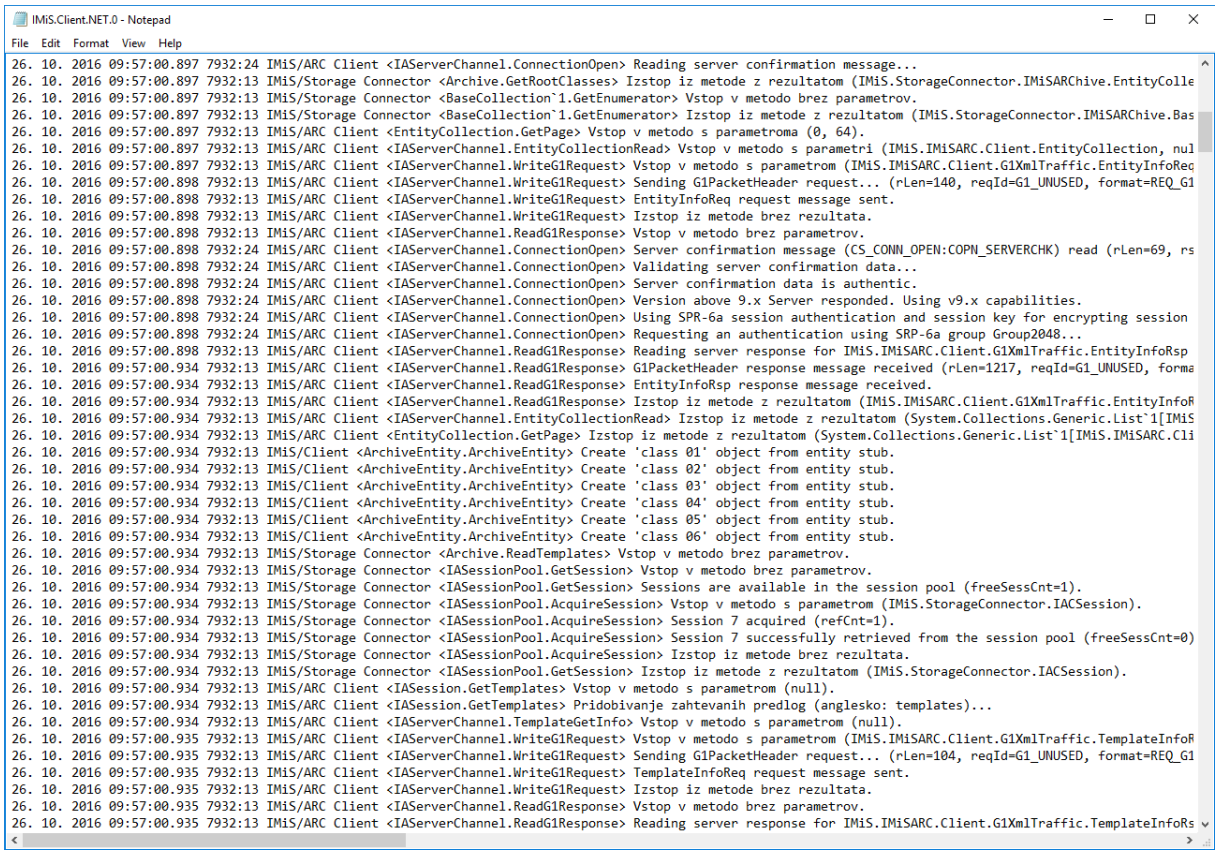


Image 287: Example log file

If there is an error in the client's operation, the entry continues with the:

- Error message, which briefly describes the error or issue.
- Error stack trace, which contains a detailed description of the reason for error.

2018 © Imaging Systems, Inc., All rights reserved.

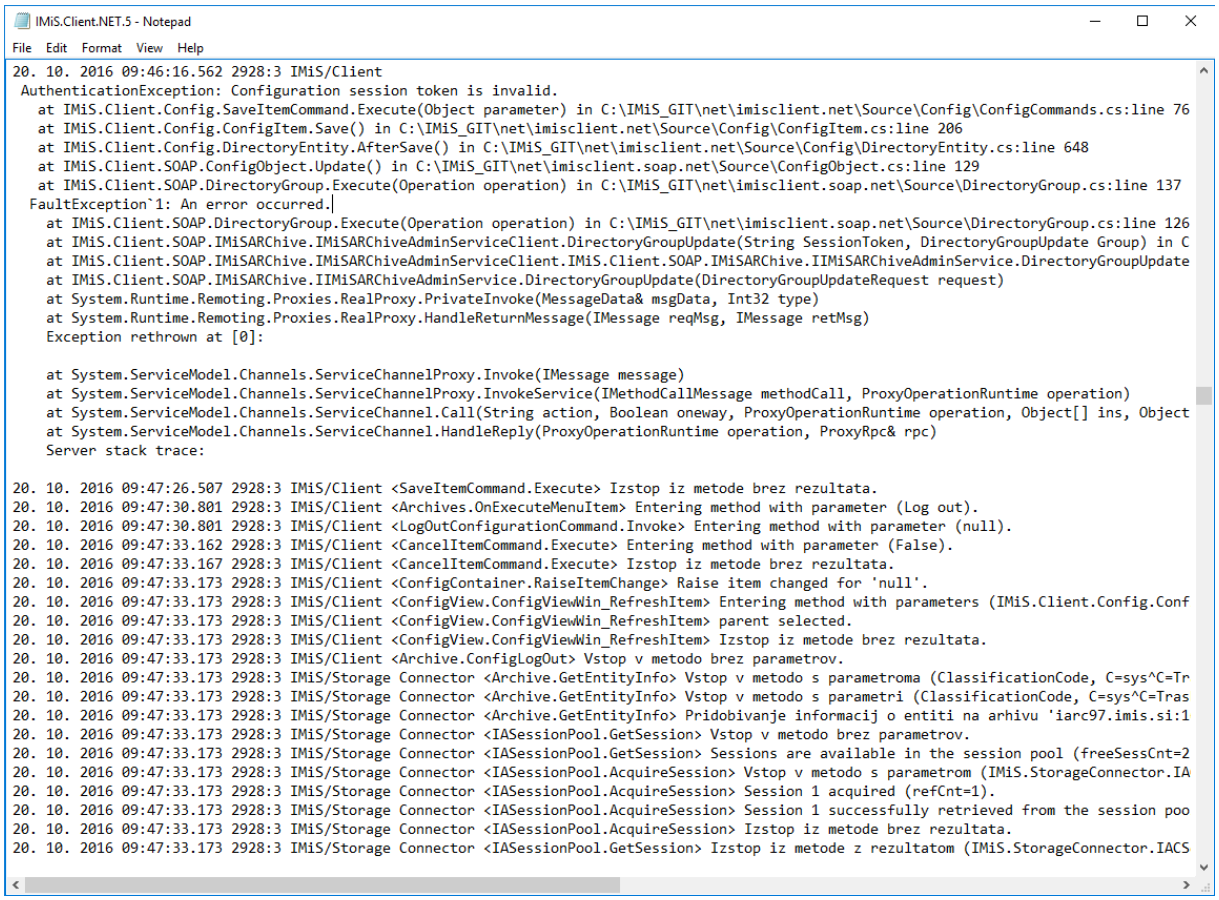


Image 288: Example error record in the log file

If the administrator is unable to solve the issue using the log, administrator is advised to forward it to the software developer for analysis, by sending an email with the issue's description to support@imis.eu.

8.3 Configuring

Configuration is performed by the user versed in the operation of the IMiS®/Client in connection with the IMiS®/ARChive Server and has appropriate access rights.

8.3.1 Adding an IMiS®/ARChive Server

After the first launch, Windows Explorer will only show the »Archives« folder in the left view. To access an IMiS®/ARChive Server, it is necessary to add it into the »Archives« folder.

2018 © Imaging Systems, Inc., All rights reserved.

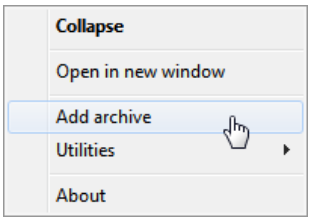


Image 289: Adding an archive via the popup menu

Archives are added by right-clicking the »Archives« folder, then choosing the »Add archive« command in the upper command bar. The »Add archive« dialog box appears in which the user enters the path to the IMiS®/ARChive Server in appropriate form.
For more information see chapter Server configuration.

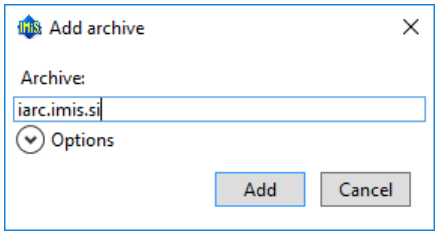


Image 290: Add archive dialog box

The process is confirmed by clicking »Add« or pressing the »Enter« key, or cancelled by clicking »Cancel«. The added server is recorded in an XML file located in a hidden system folder, which is separate for each user (»Local application data«).

Note: When adding a server, you will not be asked to log into it. Access to server is checked when the user logs in for the first time.

2018 © Imaging Systems, Inc., All rights reserved.

When the server is added, it will appear in the »Archives« folder.

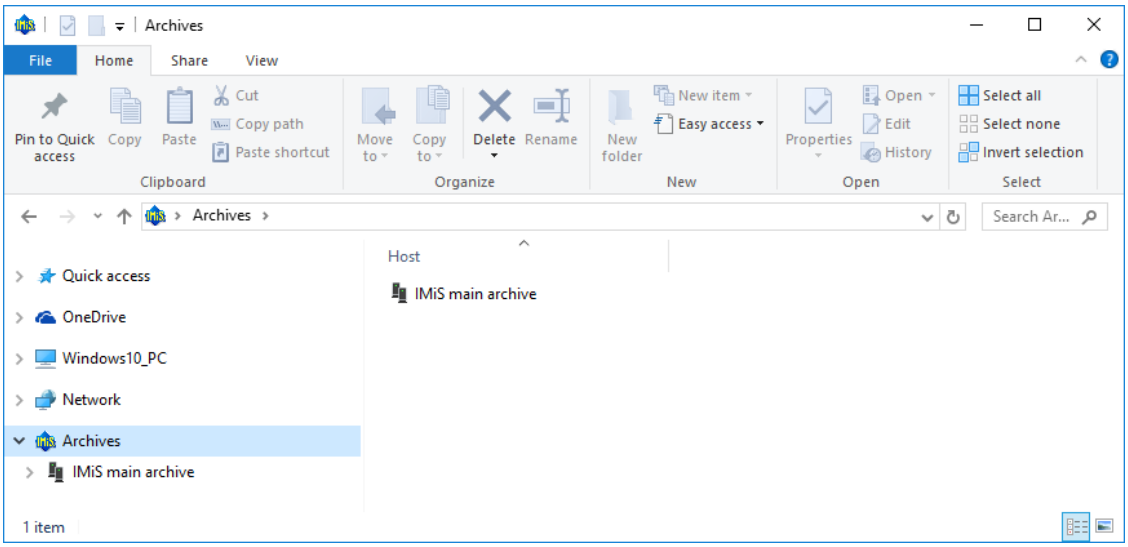


Image 291: Display of newly added archives

Users that wish to access the archive must first log into it.

For more information see chapter Login and logout.

8.3.2 Setting an IMiS®/ARChive Server

User can access the server settings by clicking the right mouse button over the folder »Archives«. In the above command bar select the command »Preferences«.

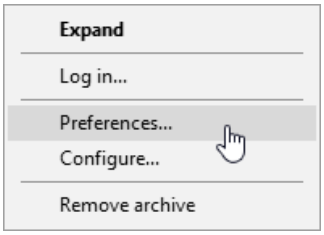


Image 292: Setting the archive via the pop-up menu

2018 © Imaging Systems, Inc., All rights reserved.

A dialog box »Preferences« with IMiS®/ARChive Server settings is shown.

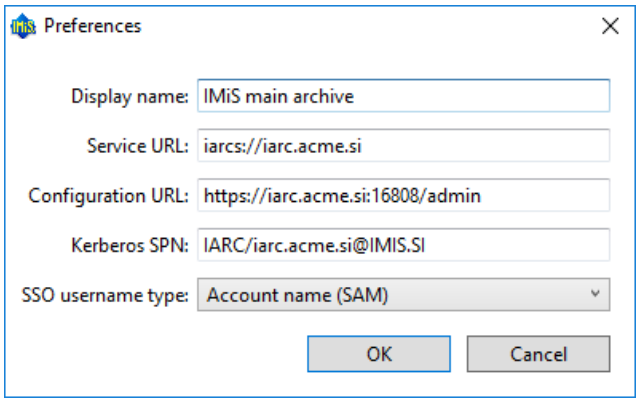


Image 293: Archive settings

The user has the following settings options for the selected server:

- »Display name«: The user can name the server freely.
- The default name when adding a new archive is »IMiS/ARChive«;
- »Service URL«: The user can edit the server path in a prescribed form as described below.
- »Configuration URL«: The user specifies the path to server configuration in a prescribed form as described below.
- »Kerberos SPN«: The user specifies the Kerberos SPN (Service Principal Name).
- »SSO username type«: The user chooses the form of the name to be used for simple authentication.

Service URL must be given in the following form:

<scheme>://<host>:<port>

where:

- »scheme«: Optional scheme for the connection type with the archive server.
  Valid values are »iarcs« for a protected connection and »iarc« for an unprotected connection.
  If the scheme is not specified, the default scheme is used (unprotected connection).
- »host«: The network name or IP address of the archive server.
- »port«: Optional network port of the archive server. If the network port is not specified, it is determined according to the selected scheme. The default network port for a protected connection is16806, and 16807 for an unprotected connection.

2018 © Imaging Systems, Inc., All rights reserved.

Configuration URL must be given in the following form:
<scheme>://<host>:<port>/admin

where:

- »scheme«: A scheme for the connection type with the archive server.
  Valid values are »https« for a protected connection and »http« for an unprotected connection.
- »host«: The network name or IP address of the archive server.
- »port«: The network port of the archive server. The default network port for connecting with a configuration URL is 16808.

In the field »Kerberos SPN« the user specifies the Kerberos Service Principal Name in the following form:
<prefix>/<host>/<realm>

where:

- »prefix«: Identifier of the Kerberos service with the default value »IARC«.
- »host«: The network name or IP address of the archive server.
- »realm«: The realm of the Kerberos service whose default value is the network realm in capital letters.

SSO username type refers to selecting a username for Single Sign-on authentication.
SSO name options are:

- »Account name (SAM)«: The form of the name is the same as the account name which corresponds to the value of the »sAMAccountName« attribute in the LDAP scheme Active Directory Domain Services (example: »johnsmith«).
- »Common name«: The form of the name is the same as the user's first and last name. The name usually corresponds to the »cn« attribute in the LDAP scheme Active Directory Domain Services (example: »John Smith«).
- »User principal name«: The form of the name consists of the account name and DNS domain name separated with »@«. The main name corresponds to the value of the »userPrincipalName« attribute in the LDAP scheme Active Directory Domain Services (example: »johnsmith@acme.si«).

2018 © Imaging Systems, Inc., All rights reserved.

- »Distinguished name«: The form of the name corresponds to the value of the »distinguishedName« attribute in the LDAP scheme Active Directory Domain Services (example: "CN=John Smith,OU=ACME,DC=acme,DC=si").
- »Email address«: The form of the name is the same as the user's email address and corresponds to the value of the »mail« attribute in the LDAP scheme Active Directory Domain Services (example: »john.smith@acme.si«).

User completes the server setup by selecting the command »OK« or by pressing the »Enter« button. By selecting the »Cancel« command the server setup is cancelled.

8.3.3 Removing an IMiS®/ARChive Server

Existing servers can be removed by selecting them in the left view of Windows Explorer, then right-clicking to open the popup menu where the »Remove archive« command can be selected.

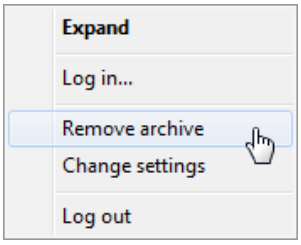


Image 294: Removing an archive via the popup menu

This will open a dialog box asking for confirmation to remove the selected IMiS®/ARChive Server.

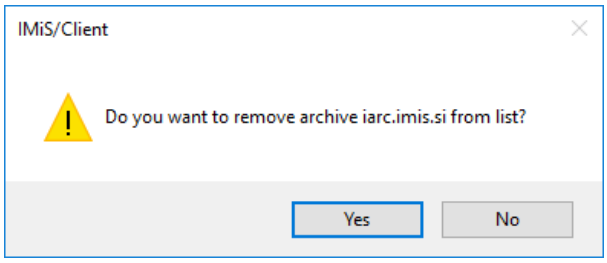


Image 295: Remove archive dialog box

Removal is confirmed by clicking »Yes« or cancelled by clicking »No«. When the IMiS®/ARChive Server is removed from the list, it will no longer appear in the »Archives« folder.
A new IMiS®/ARChive Server is added according to the procedure described in chapter Configuring in the IMiS®/ARChive Server manual.

2018 © Imaging Systems, Inc., All rights reserved.

8.4 Server configuration

Access to the configuration of the IMiS®/ARChive Server is only possible when the user has activated the HTTP authentication and has generated a password. By right-clicking the selected archive, the user selects the »Configure« command in the popup menu.

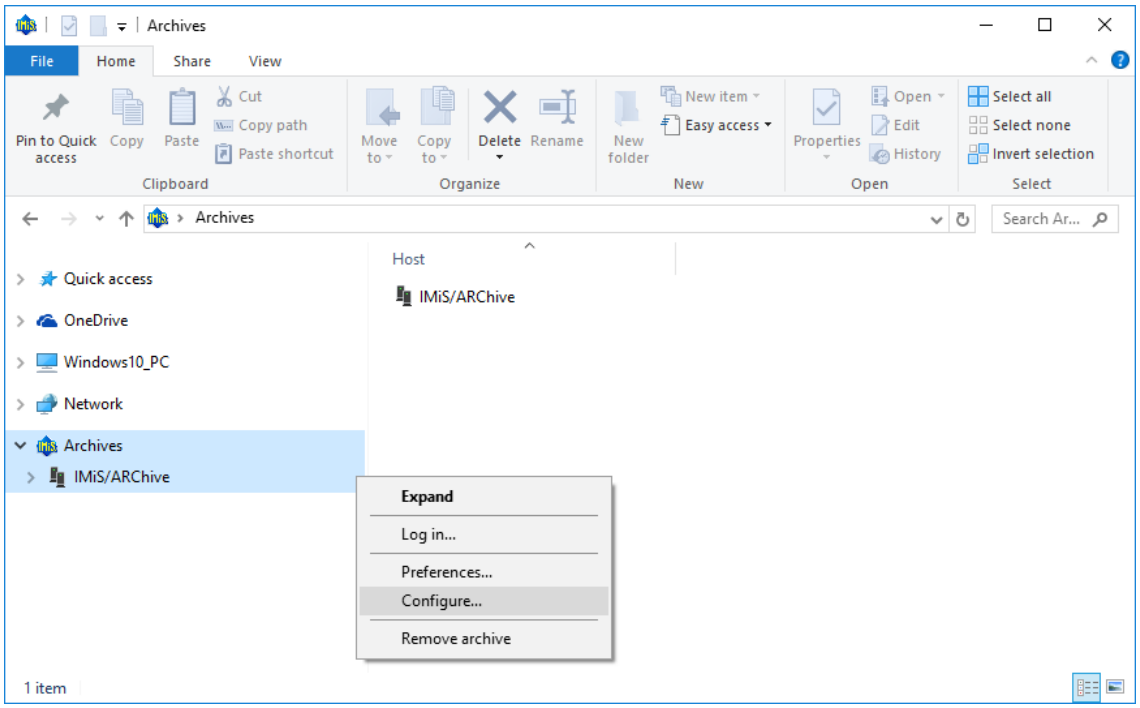


Image 296: Choosing the »Configure« command before the user has logged into the archive

The user can also configure the IMiS®/ARChive Server after he has already logged into the archive.

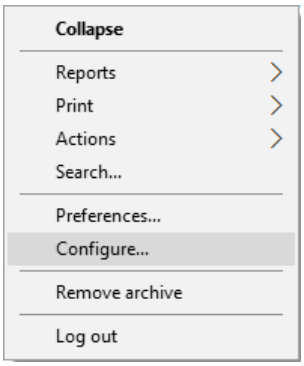


Image 297: Choosing the »Configure« command after the user has logged into the archive

2018 © Imaging Systems, Inc., All rights reserved.

After choosing the »Configure« command, the »Configuration log in« dialog box appears, where the user can enter his username into the »Username« field and his password into the »Password« field. Login is confirmed by clicking »Log in« and cancelled by clicking »Cancel«.

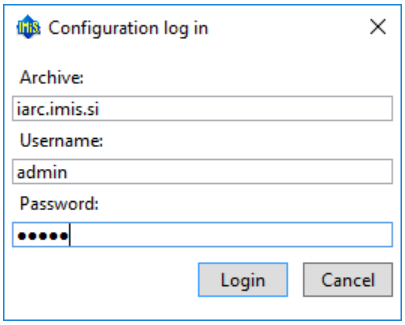


Image 298: Dialog box for entering username and password

Following a successful authentication, a list of configuration folders is displayed in the right view:

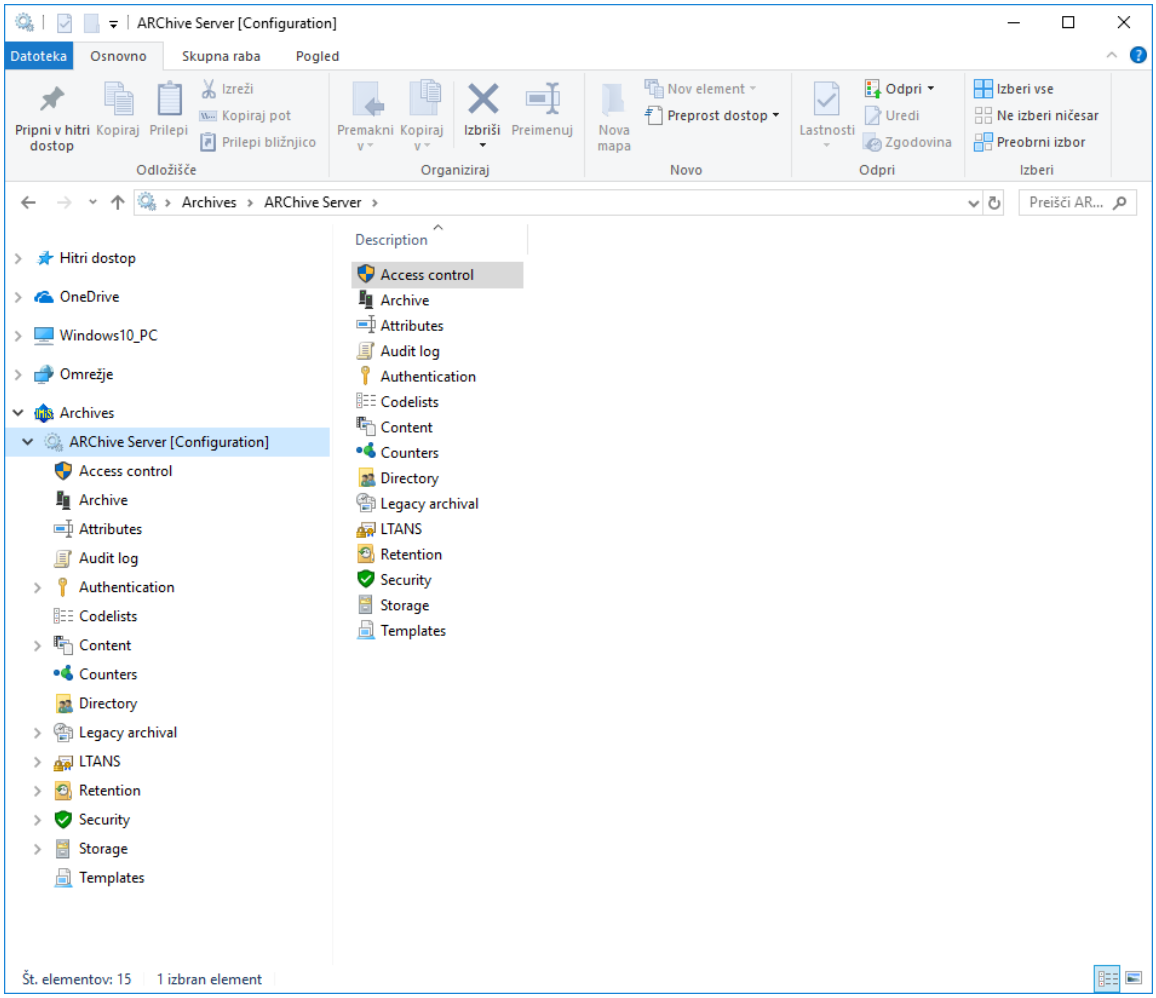


Image 299: List of available folders displayed after logging into the archive configuration

The availability of the configuration folders depends on the user's roles.

The following configuration folders can be displayed:

- »Access Control«: contains a list of users and user groups, for which the user with appropriate access rights has set rights to entities and user entered attributes.
- »Archive«: contains the delimiter settings in classification codes between classes, folders and documents for an individual archive storage profile.
- »Attributes«: contains a list of system attributes and user entered attributes, which are used for setting properties.
- »Audit log«: contains the audit log settings, including the parameters which must be entered when establishing a connection to the archive, and the actions to be recorded in the audit log.
- »Authentication«: contains a list of system settings for links and external directories.
  - »Connectors«: contains a list of plugins.
  - »External directories«: contains a list of external directories.
  - »Settings«: contains authentication and authorization settings.
- »Codelists«: contains a list of attributes, which user set the value range.
- »Content«: contains folders with content access settings.
  - »Converters«: contains content converter settings.
  - »Digital signatures«: contains the settings for the scope of the implementation of digital signatures.
  - »Full text indexing«: contains the settings for full text indexing.
  - »Parsers«: contains the list of parsers bound to the digital signature and content verification.
  - »Settings«: contains access properties to contents in the archive.
- »Counters«: the user sets tree depth of the entities in the classification scheme and entry format of the classification code for an individual entity type on a specific level.
- »Directory«: contains a list of users and user groups of the server, including the corresponding information about the user, authentication, roles and memberships in the groups.

2018 © Imaging Systems, Inc., All rights reserved.

- »Legacy archival«: contains folders for legacy archival settings.
  - »Content type aliases«: contains a translation table of content types that is used for legacy archival.
  - »Object containers«: specifies the attribute of each template when the template is used for legacy archival.
  - »Storage profiles«: specifies settings (template, container identifier, names, descriptions, etc.) for each archive profile when the profile is used for legacy archival.
- »LTANS«: contains folders with content timestamping settings.
  - »Settings«: contains the settings of timestamping properties.
  - »Timestamp chaining rules«: contains a list of rules for timestamp chaining.
  - »Timestamp providers«: contains a list of timestamp providers.
  - »Timestamp rules«: contains a list of timestamp rules.
- »Retention«: contains two folders with settings for retention policies and disposition holds:
  - »Retention policies«: contains a list of retention policies for the archived content.
  - »Disposition holds«: contains a list of disposition holds for the archived content.
- »Security: contains folders with security mechanism settings.
  - »Certificates: contains a list of certificates.
  - »Settings«: contains security settings for public attributes.
- »Storage«: contains two folders for the profiles and volumes specified on the server.
  - »Profiles«: contains a list of the profiles specified on the server.
  - »Volumes«: contains a list of all volumes on the server.
- »Templates«: contains a list of templates for setting attributes.

Depending on the selected configuration folder, the following commands are displayed in the command bar:

- »Edit«: the selected entity/objects open in the editing mode.
  This command is only available for the entities/objects, which can be set by the user.
- »Add«: allows the user to add the selected entities/objects from the list.
  This command is only available for the entities/objects, which can be set by the user.
- »Remove«: allows the user to remove the selected entities/objects from the list.
  This command is only available for the user defined entities/objects, when the selected entity is opened in the edit mode.

2018 © Imaging Systems, Inc., All rights reserved.

- »Context«: enables the display of directory entities and their access rights on the level of the entire archive or only according to certain archive functionalities. The command »Context« in the command bar is added for the configuration folder »Access Control«.
- »Disable«: disables or enables a directory entity in the list for the »Directory« configuration folder or a digital certificate of trusted issuers for the »Digital certificates« configuration folder.

For the selected configuration folders »Attributes«, »Codelists«, »Counters«, »Directory« or »Templates«, the »Filter« command is also displayed in the command bar.

The latter enables viewing of a specific set of objects only.

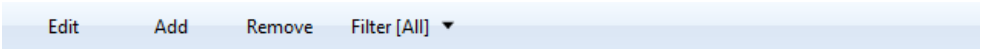


Image 300: Example of the command bar in the configuration folder with the »Filter« command

Advice: The user with appropriate access rights can save the default settings of the filter for the individual configuration folders. Clicking the selected filter while pressing Left+Shift saves the default setting.

When the »Access control« configuration folder is selected, the »Context« command is added in the command bar. The latter enables viewing the entire archive or only individual system entities.

8.4.1 »Access control« folder

The »Access Control« folder contains a list of users and user groups, for which rights for accessing the entities and attributes are set by the user with appropriate access rights.
The basic information about users and user groups is listed in the columns.
To ensure clarity, users and user groups have their own icons.

2018 © Imaging Systems, Inc., All rights reserved.

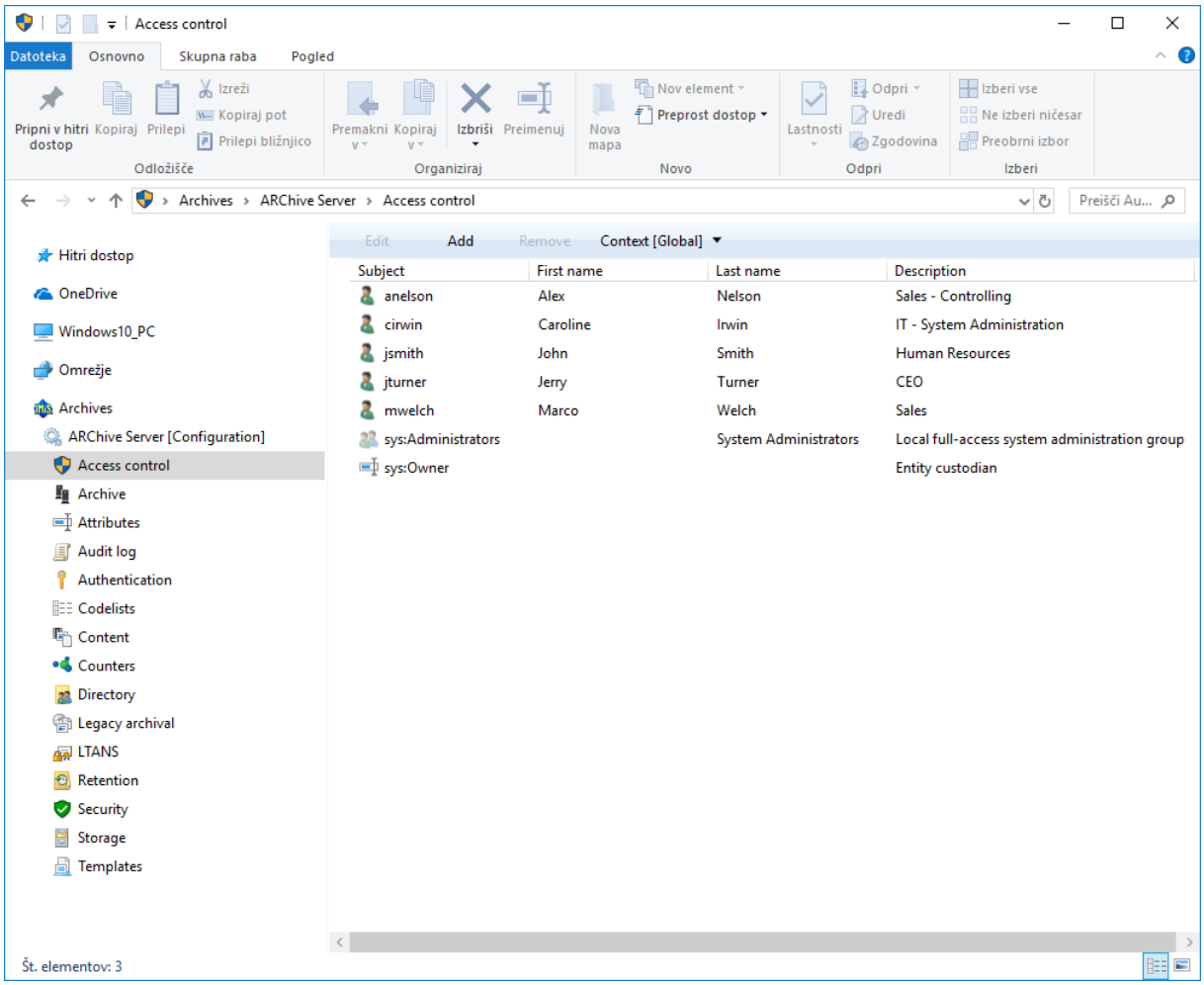


Image 301: List of users and user groups in the »Access control« configuration folder

By choosing the »Context« command in the upper command bar, the user with appropriate access rights can set the view context.

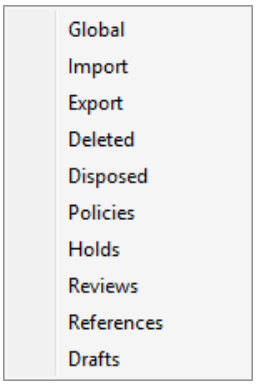


Image 302: Choosing the context in the »Access control« configuration folder

2018 © Imaging Systems, Inc., All rights reserved.

The user can choose between the following contexts:

- »Global«: contains rights for accessing the entities and attributes on the level of the entire archive. For more information see chapter Selecting »Global«.
- »Import«: contains rights for accessing the entities and attributes in the »Import« system folder.
  - »Export«: contains rights for accessing the entities and attributes in the »Export« system folder.
  - »Deleted«: contains rights for accessing the entities and attributes in the »Deleted« folder in the »Trash« system folder.
- »Disposed«: contains rights for accessing the entities and attributes in the »Disposed« folder in the »Trash« system folder.
- »Policies«: include access rights to entities and attributes in the system folder »Policies«.
- »Holds«: include access rights to entities and attributes in the system folder »Holds«.
- »Reviews«: contains rights for accessing the reviews in the »Reviews« system folder.
- »References«: contains the permissions to create references to entities in the classification scheme.
- »Drafts«: contains the permissions to access document drafts.

8.4.1.1 Selecting »Global«

The user with appropriate access rights can set rights for accessing the entities and attributes for an individual user or user group on the level of the entire archive.

By selecting the »Add« command in the command bar and by choosing the appropriate user from the available users and user groups, the user with appropriate access rights can add a new user or user group. User can also set rights for accessing the entities and attributes for a user or user group. The selected settings are saved by choosing the »Save« command.

By choosing the appropriate user from the available users and by selecting the »Remove« command, the user with appropriate access rights can remove the new user.

2018 © Imaging Systems, Inc., All rights reserved.

»Properties« tab

By clicking on a user on the list, the »Properties« tab appears in the bottom right view of Windows Explorer. The user can view the following values of attributes:

- »Subject type«: defines the type of user (user, group).
- »Subject«: a unique tag of a user or group in the archive.
  For greater clarity the users and groups have their own icon.
- »First name«: the first name of a user or group.
- »Last name«: the last name of a user or group.
- »Description«: a short description of a user or group.

»Entity rights« tab

By clicking the user on the list, the »Entity rights« tab is displayed in the lower right view of the Windows Explorer. By clicking the »Add« command, the user with appropriate access rights can allow the following actions over the entities, which are valid for the entire archive:

- »Read«: the user has permission to read data on the selected entity.
- »Write«: the user has permission to edit entity data.
- »Move«: the user has permission to move the entity within the classification scheme.
- »Delete«: the user has permission to delete entity data.
- »Create entities«: the user has permission to create sub-entities under the selected entity.
- »Change permissions«: the user has permission to change the effective permissions of other users on the selected entity.
- »Change security class«: the user has permission to change the security class of the selected entity.
- »Change status«: the user has permission to change the entity status.
- »Change retention«: the user has permission to change the validity of an entity's retention periods.

2018 © Imaging Systems, Inc., All rights reserved.

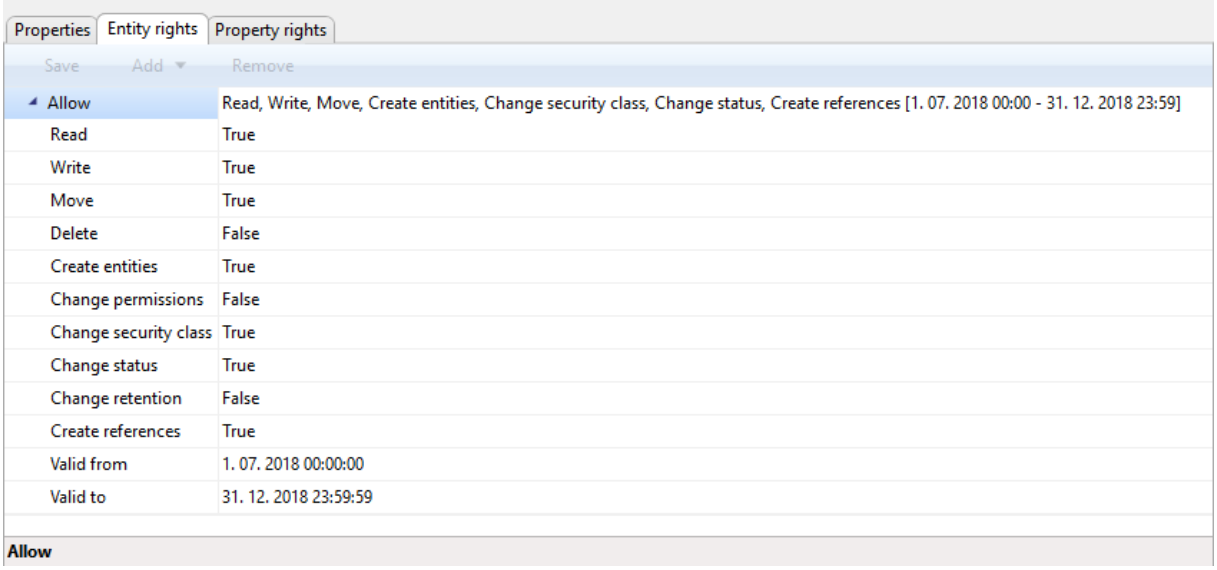


Image 303: Entities access rights

The rights are changed by choosing one of both options »True« and »False«. Time restriction is set by choosing the date and time, by setting the permission expiration date in the calendar for the »Valid from« and »Valid to« fields.

Warning: After changing the global rights, the current user rights are valid for the entire duration of his session or until the user logs into the archive again.

»Property rights« tab

By clicking the »Property rights« tab in the lower right view of the Windows Explorer and the »Add« tab, the user with appropriate access rights begins by selecting the attribute.

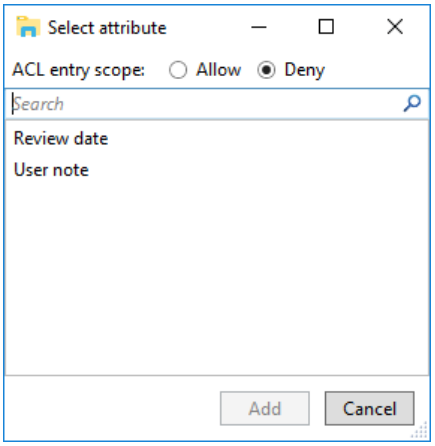


Image 304: Selecting the attribute

The user can define the following permissions (Allow) or prohibitions (Deny) for each attribute selected, which are valid for the entire archive:

- »Read«: the user has permission to read the attribute value.
- »Write«: the user has permission to write the attribute value.
- »Create«: the user has permission to create the attribute value.
- »Delete«: the user has permission to delete the attribute value.

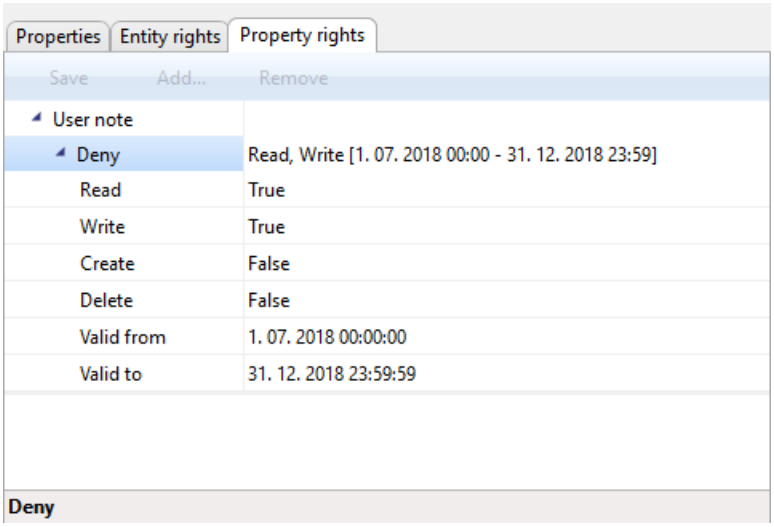


Image 305: Access rights to attributes

The rights are changed by choosing one of both options »True« and »False«. Time restriction is set by choosing the date and time, by setting the permission expiration date in the calendar for the »Valid from« and »Valid to« fields.

Warning: After changing the global rights, the current user rights are valid for the entire duration of his session or until the user logs into the archive again.

Note: On the archive level, restrictions (»Deny«) of the access rights settings have no meaning, because access right by default sittings are not allowed.

8.4.1.2 Selecting the rest contexts

Access rights to entities and attributes for an individual user or user group are set by the user with appropriate access rights in the system folders: »Import«, »Export«, »Deleted«, »Disposed«, »Policies«, »Holds«, »Reviews«, »Reference« and »Drafts«.

2018 © Imaging Systems, Inc., All rights reserved.

Rights are described in the chapter Selecting »Global«.

The user with appropriate access rights can »Allow« or »Deny« explicit permissions for each right from the list.
In addition to explicit rights, inherited rights (»Allow [Inherited]«), which are set on the level of the entire archive, are also available in the »Entity rights« and »Property rights« tab.
The inherited rights cannot be changed; however, they can be replaced with the explicit rights.

8.4.2 »Archive« folder

The »Archive« folder contains archive settings – the name of the archive server, delimiters in the entity's classification codes and the name of the default profile.

»Properties« tab

By clicking the »Archive« folder, the following settings are displayed in the right pane of the Windows Explorer in the »Properties« tab:

- »Name«: specifies the default name of the archive server.
- »Class delimiter«: specifies a delimiter between classes in the entity's classification code.
- »Folder delimiter«: specifies a delimiter between a class/folder and a folder in the entity's classification code.
- »Document delimiter«: specifies a delimiter between a class/folder and a document in the entity's classification code.
- »Storage profile«: specifies a default profile for storing entities and contents.

2018 © Imaging Systems, Inc., All rights reserved.

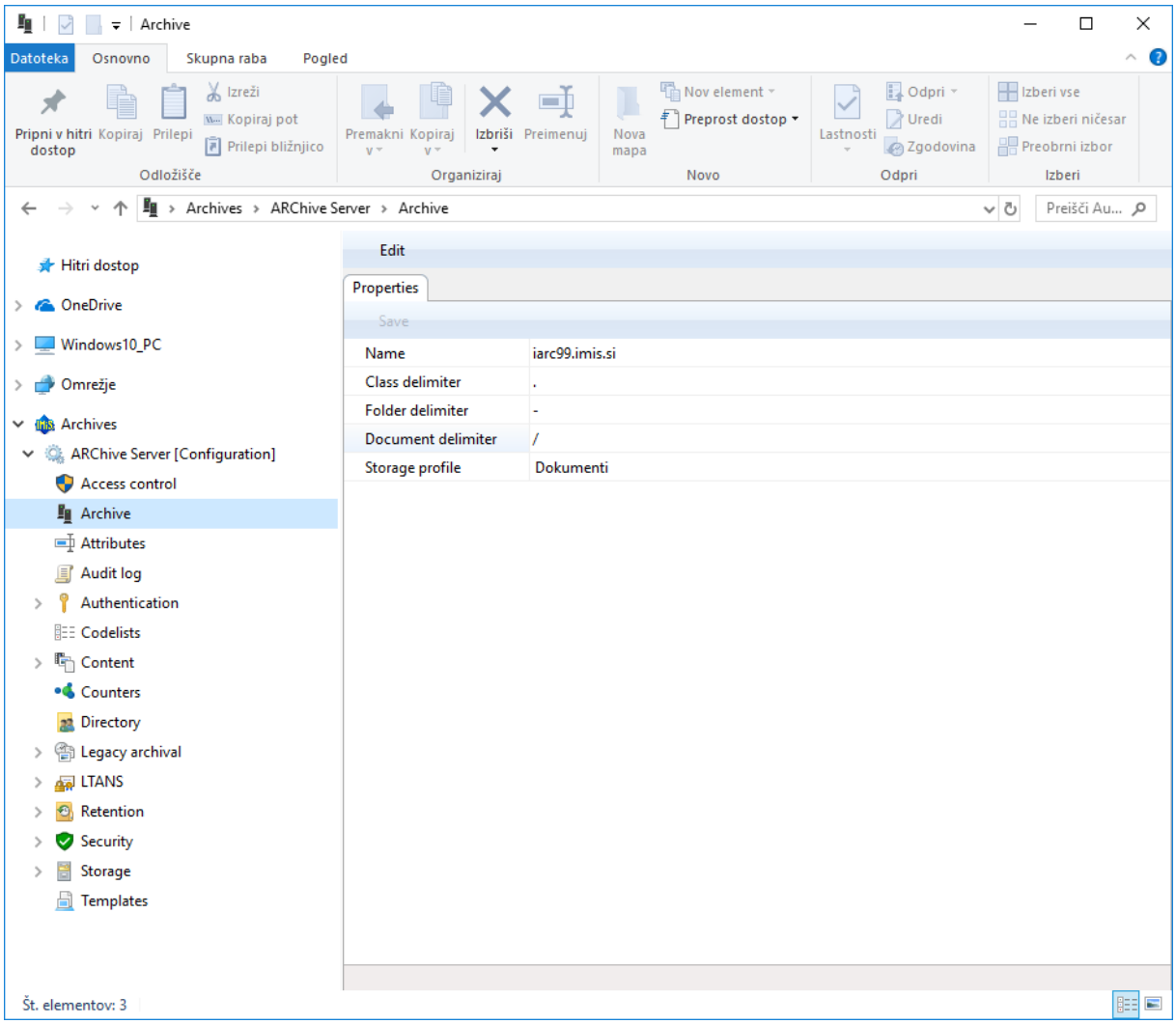


Image 306: »Properties« list in the »Archive« configuration folder

8.4.3 »Attributes« folder

The »Attributes« folder contains a list of attributes described with their values.

The following attribute information is listed in the columns:

- »Name«: contains the name of the attribute.
- »Type«: contains the type of the attribute.
- »Description«: contains the description of the attribute.
- »Used by«: contains titles of the templates, in which the attribute is used.

2018 © Imaging Systems, Inc., All rights reserved.

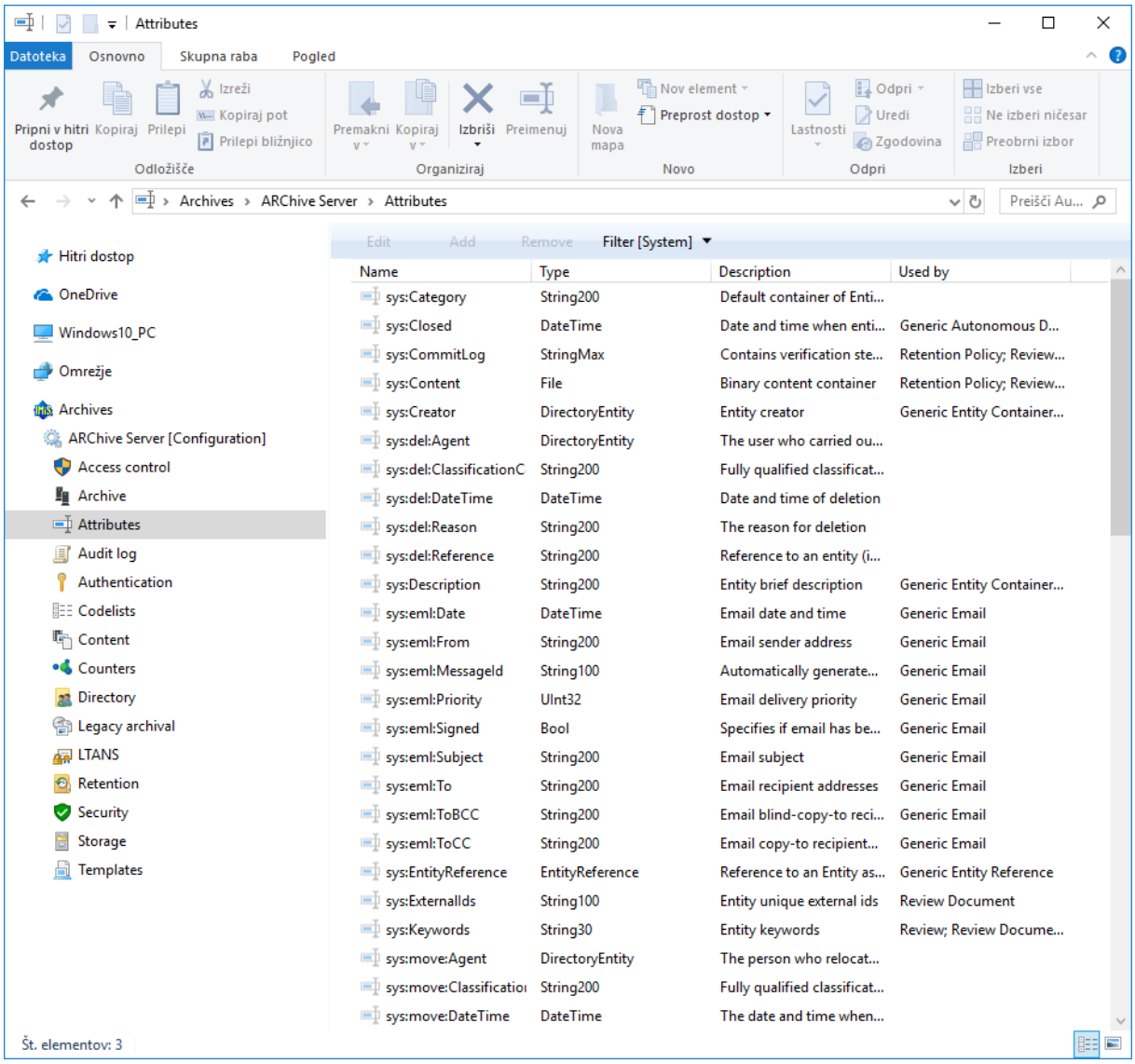


Image 307: Attribute list in the »Attribute« configuration folder

By choosing the »Filter« command in the upper command bar, the user with appropriate access rights can set the view content.

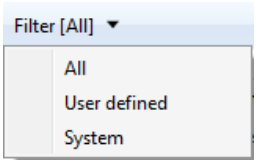


Image 308: Selecting the filter in the »Attribute« configuration folder

2018 © Imaging Systems, Inc., All rights reserved.

The user can choose between the following options:

- »All«: all attributes are shown on the list.
- »User defined«: only user defined attributes are shown on the list.
- »System«: only system attributes are shown on the list.

The system attributes cannot be changed.

»Attribute Properties« bar

By clicking the attribute on the list, the following value settings are shown in the "Properties" tab in the lower right view of the Windows Explorer.

- »Name«: contains the name of the attribute. In case of a system attribute, the attribute type is shown at the beginning (sys:, eml:, prm:, trf:) and a short description follows. For each new entry, the value for the attribute name has to be selected before saving. Once the entry is saved, the value cannot be changed any more.
- »Type«: specifies the attribute type (for example DirectoryEntity, Boolean, Int32, Double, DateTime, String, Decimal, Binary or File). For each new entry, the value for the attribute type has to be selected before saving. Once the entry is saved, the value cannot be changed any more.
- »Description«: contains a short description of the attribute.
- »Label«: the attribute value represents the label of the version in the series. This value is created automatically on checking in the working copy and represents the next version in the series.
- »Validation Expression«: specifies the value that represents the regular expression used to check the new or changed attribute values. Further information about the syntax and rules: http://en.wikipedia.org/wiki/Regular_expression.
- »Searchable«: specifies if search by its value is possible. »True« setting; marks that search by the attribute value is possible using the search functions.
- »Unique«: if the selected value is »True«, the attribute value is unique throughout the whole archive. The user with appropriate access rights can select this value if he wants to avoid entering the attribute value, which is already specified by a different entity.
- »PickList«: if the selected value is »True«, the values have been pre-set. It is not possible to enter the values manually outside of the list of allowed values.

2018 © Imaging Systems, Inc., All rights reserved.

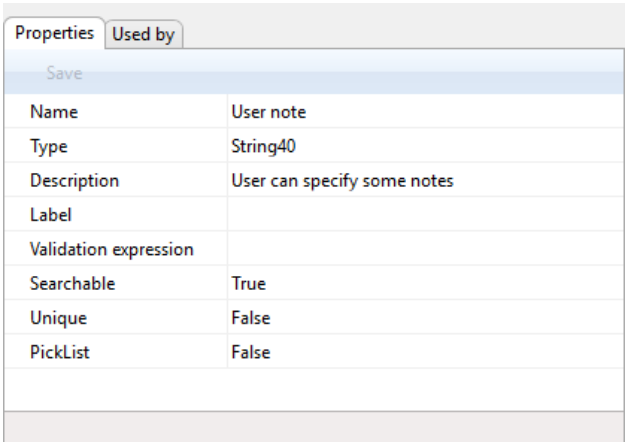


Image 309: Attribute properties

Examples of validation formula:

On the IMiS®/ARChive Server a Perl syntax of regular expressions is implemented.

The whole value of the attribute must match the syntax of the validation formula. A user can check the adequacy of the syntax on this web address http://www.perlfect.com/articles/regextutor.shtml.

Below are a few examples. Values are written in single quotes and are not a part of values.

Regular expression: 'A-Za-z'

Accepted value: value 'A-Za-z'

The value of the attribute must be equal to the value of the regular expression.

Regular expression: '[A-Za-z]'

Accepted values: one letter that has values between 'A' and 'Z' or 'a' and 'z'

All other combinations (i.e.: 'ab', 'Ab', 'aB', '123a' and so on.) are invalid.

*Regular expression: 'a*b'*

Accepted values: combination of values 'ab', 'aaaaab', 'aaaaaaaaaaab', also only 'b'. A star means that the previous character 'a' isn't present or can be repeated multiple times. All other combinations that are a partial match (i.e.: '123aaaab', 'aaab123') or not a match (i.e.: 'gbrtz', '12345') are invalid.

Regular expression: 'a+b'

Accepted values: combination of values 'ab', 'aaaaab' and so on. Character '+' demands a presence of a previous character 'a', that can also be repeated. In this case value 'b' is invalid. For all other combinations see the previous example.

Regular expression: '.at'

Accepted values: all three character values ending with 'at' (npr. 'cat', 'tat', 'pat', '5at', and so on).

All other values are invalid.

2018 © Imaging Systems, Inc., All rights reserved.

»Use under« tab

By clicking the »Use under« tab in the lower right view of the Windows Explorer, all templates, in which the attribute is used are listed. For more information see chapter »Templates« folder.

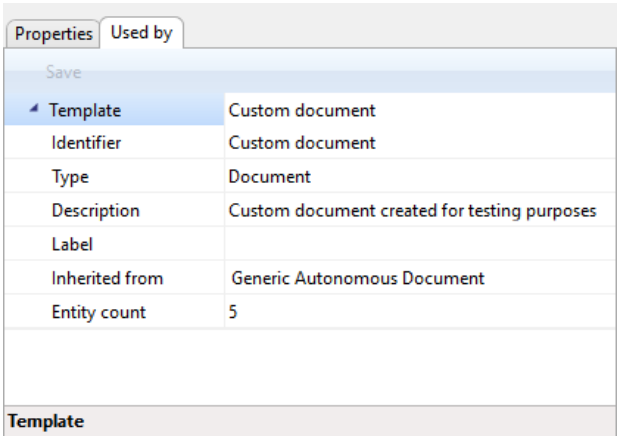


Image 310: Templates, in which the attribute is used

8.4.4 »Audit log« folder

The »Audit log« folder contains the audit log parameters.

»Entity events« tab

By clicking the »Entity events« tab in the »Audit log« folder, the right view of Windows Explorer shows the following value settings:

- »Audit log«: searching the audit log is recorded in the audit log.
- »Create«: the action of creating an entity is recorded in the audit log.
- »Open«: the action of opening an entity in reading mode is recorded in the audit log.
- »Edit«: the action of opening an entity in writing mode is recorded in the audit log.
- »Save«: the action of saving an entity is recorded in the audit log.
- »Move«: the action of moving an entity is recorded in the audit log.
- »Delete«: the action of deleting an entity is recorded in the audit log.
- »Access control change«: the action of changing access control is recorded in the audit log.
- »Attributes change«: the action of changing the values of entity attributes is recorded in the audit log.
- »Physical content change«: the action of changing the values of physical content attributes is recorded in the audit log.

2018 © Imaging Systems, Inc., All rights reserved.

- »Security class change«: the action of changing the entity's security class is recorded in the audit log.
- »Status change«: the action of changing the entity's status is recorded in the audit log.
- »Dispose«: the action of disposing an entity in the review process is recorded in the audit log.
- »Permanent«: the action of marking an entity as permanent in the review process is recorded in the audit log.
- »Transfer«: the action of transferring an entity in the review process is recorded in the audit log.
- »Review«: the action of reviewing an entity in the review process is recorded in the audit log.
- »Check out«: the action of checking out a document version is recorded in the audit log.
- »Check in«: the action of checking in a document version is recorded in the audit log.
- »Discard draft«: the action of discarding a document draft is recorded in the audit log.

2018 © Imaging Systems, Inc., All rights reserved.

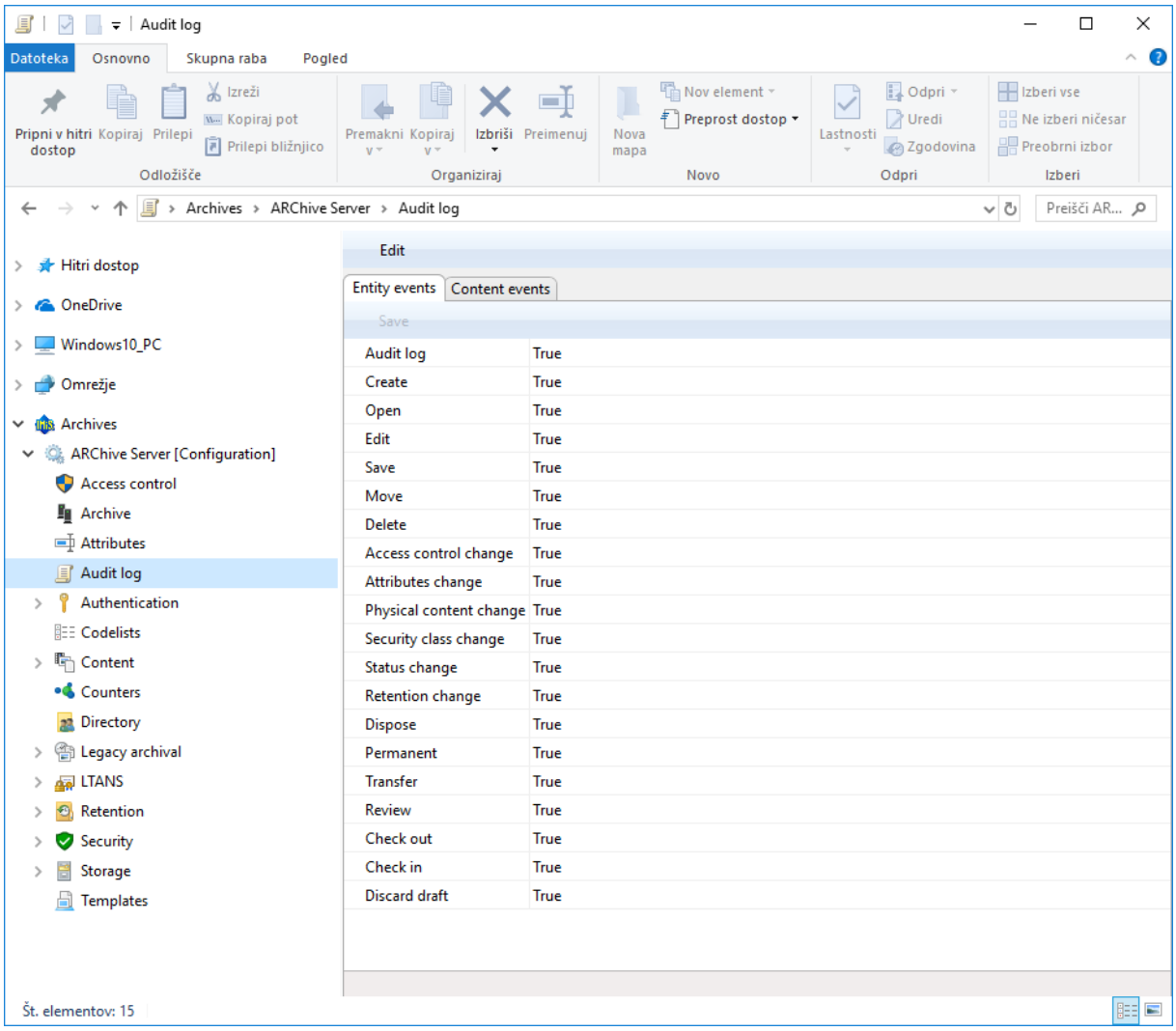


Image 311: List of entity events in the »Audit log« configuration folder

A value set to »True« denotes that event recording in the audit trail is enabled.

On the contrary, by changing the value to »False« users with appropriate rights disable any event recording in the audit trail.

»Content events« tab

By clicking the »Content events« tab in the »Audit log« folder, the right view of Windows Explorer shows the following value settings:

- »Create«: the action of creating content is recorded in the audit log.
- »Open«: the action of opening an entity in reading mode is recorded in the audit log.
- »Edit«: the action of opening an entity in writing mode is recorded in the audit log.
- »Save«: the action of saving content changes is recorded in the audit log.

2018 © Imaging Systems, Inc., All rights reserved.

- »Move«: moving content is recorded in the audit trail.
- »Delete«: the action of deleting content is recorded in the audit log.
- »Attributes change«: the action of changing the values of content attributes is recorded in the audit log.

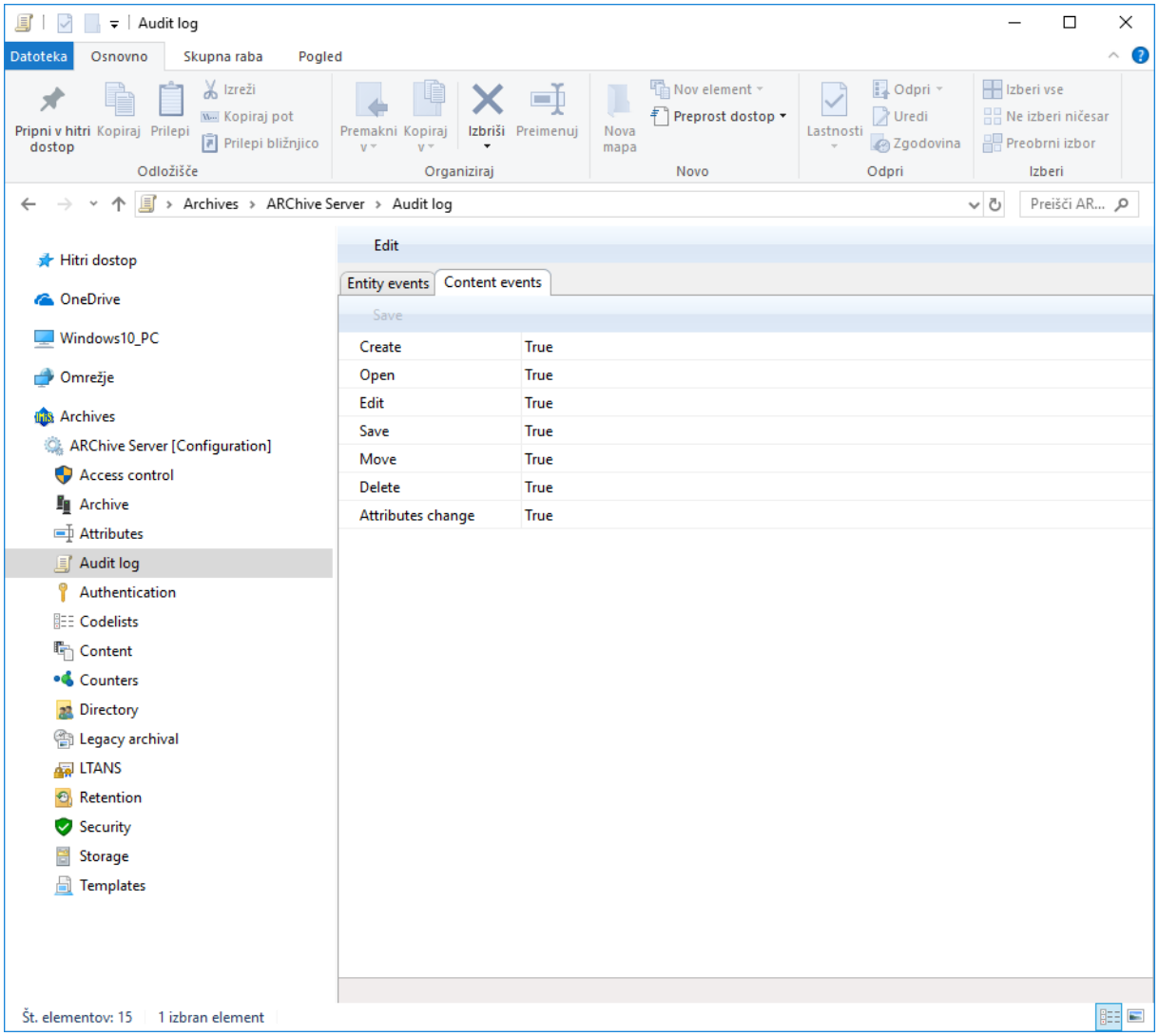


Image 312: List of content events in the »Audit log« configuration folder

A value set to »True« enables content actions to be recorded in the audit trail.

On the contrary, by changing the value to »False« users with appropriate rights disable any content action from being recorded in the audit trail.

8.4.5 »Authentication« folder

The »Authentication« folder contains the following folders: »Connectors«, »External directories« and »Settings«.

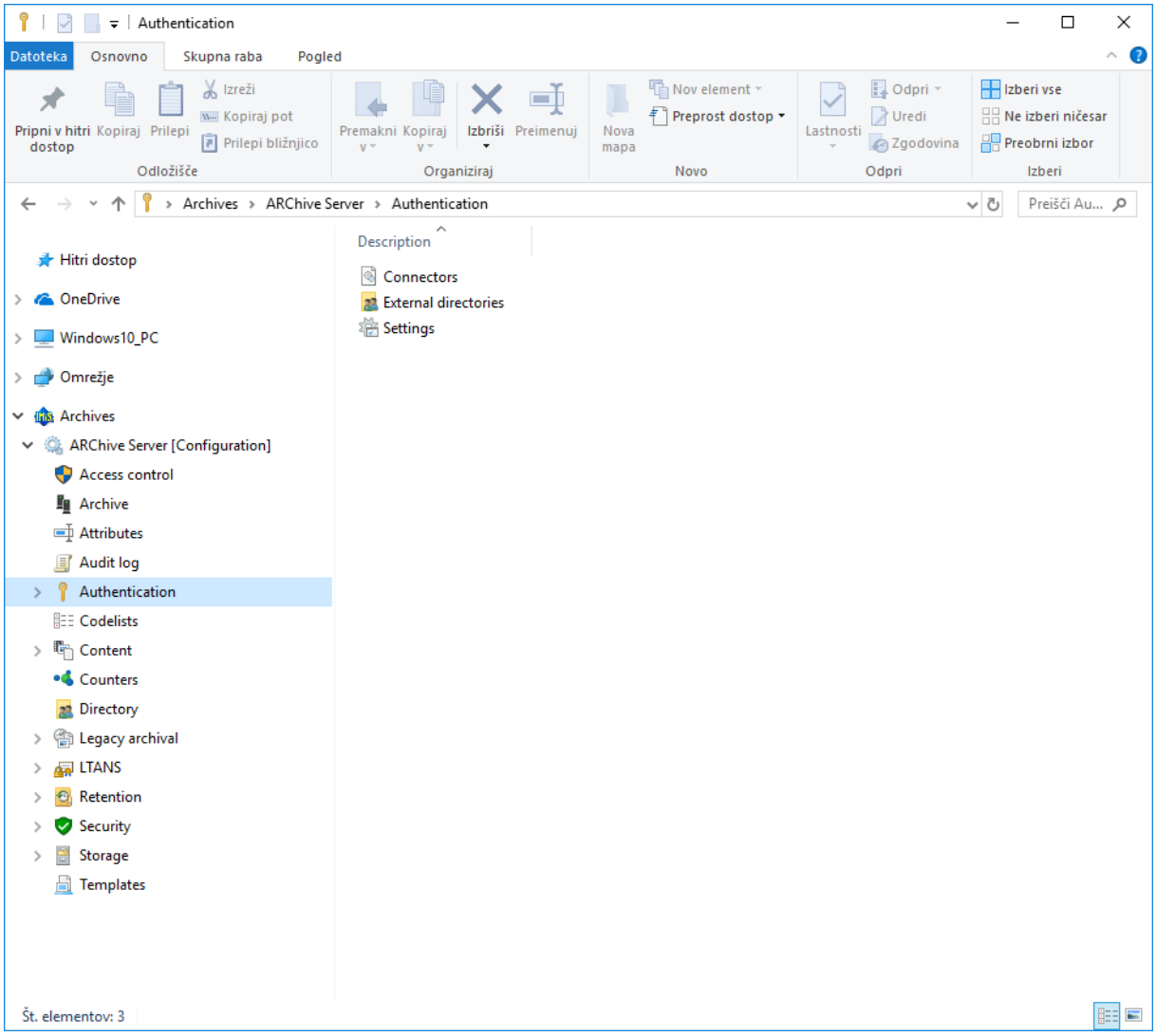


Image 313: List of contained folders in the »Authentication« configuration folder

8.4.5.1 »Connectors« folder

The »Connectors« folder contains a list of connectors that enables users with appropriate rights to set parameters for accessing external directory providers (i.e. Active Directory, LDAP ...).

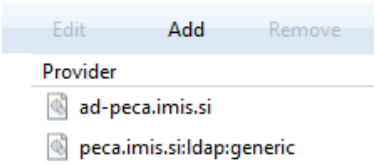


Image 314: Displaying a list of connectors

»Properties« tab

By clicking the individual connector from the list, the following settings are displayed in the bottom right pane of Windows Explorer:

- »Identifier«: specifies a unique connector identifier.
- »Provider«: specifies data on the name and type of connector.

  Users with appropriate rights can view and/or change the following settings:
  - »Name«: unique name of the connector
  - »Type«: connector type (i.e. Plugin)
  - »Driver«: connector driver
  - »Arguments«: connector arguments, specific for each connector type. We enter an XML set of configuration data into the parameter, which the plugin then uses for initializing the connector (the name and credentials for accessing the external directory service, connection parameters, translation tables of attributes, etc.).

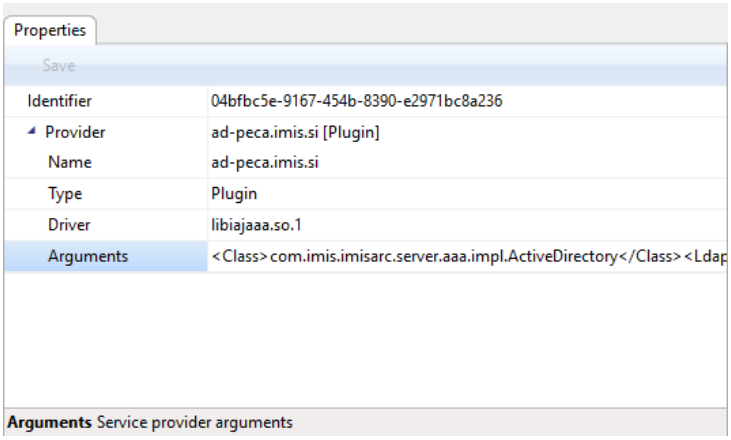


Image 315: ActiveDirectory connector's »Properties« tab

2018 © Imaging Systems, Inc., All rights reserved.

8.4.5.2 »External directories« folder

The »External directories« folder contains a list of external directories.

Users with appropriate rights specify external directory settings that are used for synchronization with the IMiS®/ARChive Server.

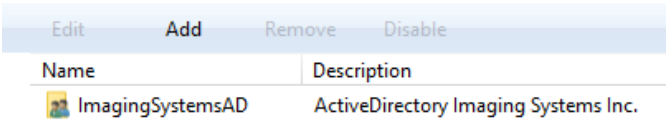


Image 316: Displaying a list of external directories

»Properties« tab

By clicking the external directory in the list, the following settings are displayed in the bottom right pane of Windows Explorer:

- »Identifier«: specifies the unique external directory identifier.
- »Name«: specifies the name of the external directory.
- »Description«: specifies the description of the external directory.
- »Synchronization«: specifies synchronization settings of the external directory with the internal directory of the IMiS®/ARChive Server.

  Users with appropriate rights can view and/or change the following settings:

  - »Connector: unique connector name.
  - »Schedule«: synchronization schedule. The default value is an empty string, which means synchronization of the external directory with the server's internal directory is not performed.

    *Example: Setting 0 5 * * * * means that synchronization is performed every 5 minutes.*

    The syntax is as follows:

    0 – seconds (0 - 59)

    5 – minutes (0 - 59)

    * - hours (0 - 23)

    * - day of the month (1 - 31)

    * - month (1 – 12)

    * - day of the week (0 – 6 [Monday - Saturday], in some systems there can be 7 [Sunday])

2018 © Imaging Systems, Inc., All rights reserved.

- »Enabled: value set to »True« denotes that synchronization is enabled.
  On the contrary, by changing values to »False« users with appropriate rights disable the synchronization of the external directory with the server's internal directory.
- »Synchronize users«: value set to »True« denotes that synchronization of users is enabled. On the contrary, by changing values to »False«, users with appropriate rights disable the synchronization of users of the external directory with the server's internal directory.
- »Synchronize groups«: value set to »True« denotes that synchronization of groups is enabled. On the contrary, by changing values to »False« users with appropriate rights disable the synchronization of the external directory groups with the server's internal directory.
- »Delete unknown entities«: value set to »False« denotes that the entities in the directory, which are not found during the synchronization with the external source of the directory service, will not be deleted from the server's internal directory. On the contrary, by changing values to »True« users with appropriate rights enable the deletion of these entities during the synchronization of the external directory with the server's internal directory.
- »User fields«: value set to »True« denotes that the synchronization of the external directory with the server's internal directory at the level of a specific user field is enabled. By changing values to »False«, users with appropriate rights disable the synchronization of the user field.
- »Group fields«: value set to »True« denotes that the synchronization of the external directory with the server's internal directory at the level of a specific group field is enabled. By changing values to »False«, users with appropriate rights disable the synchronization of the group field.

2018 © Imaging Systems, Inc., All rights reserved.

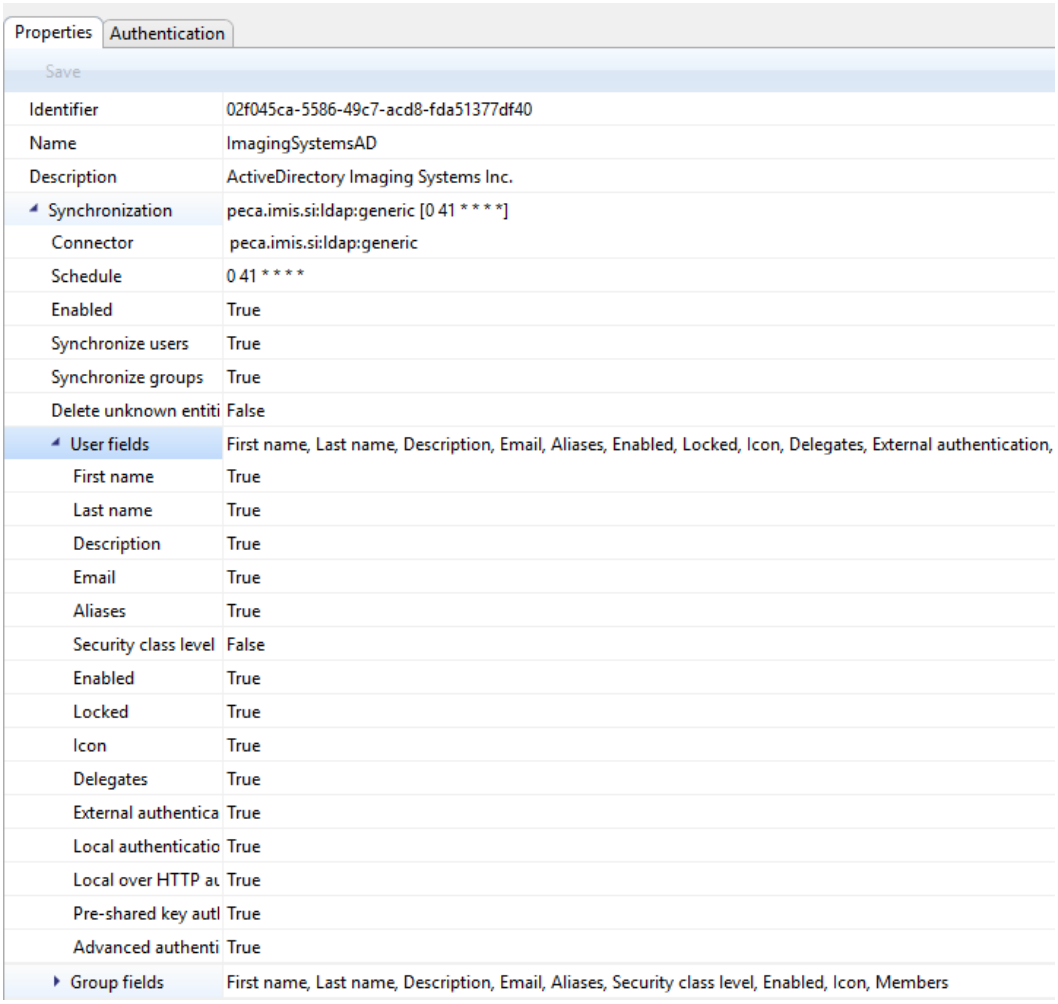


Image 317: External directory's »Properties« tab

»Authentication« tab

By clicking the external directory in the list, the following settings are displayed in the bottom right pane of Windows Explorer:

- »Method«: specifies authentication method (i.e.. LDAP, Kerberos5ServiceTicket).
- »Connector«: specifies unique connector name.

2018 © Imaging Systems, Inc., All rights reserved.

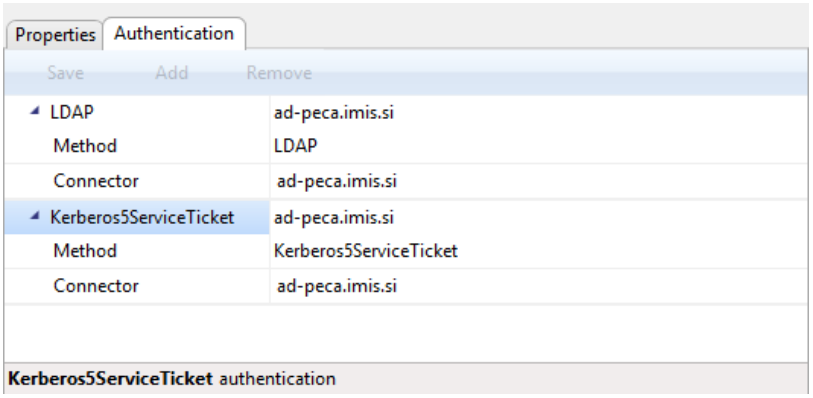


Image 318: External directory's »Authentication« tab

8.4.5.3 »Settings« folder

»Settings« folder contains general settings that influence user authentication and authorization.

»Properties« tab

By clicking the entry in the list, the following settings are displayed in the bottom right pane of Windows Explorer:

- »Realm«: The Kerberos service realm; its default value is the same as the network realm in capital letters.
- »Lockout count«: specifies the number of unsuccessful successive user authentications to the IMiS®/ARChive Server before disabling access. It applies for local and external users if they are using the IMiS®/ARChive Server's local authentication method.
  In case of using external authentication (LDAP, Kerberos ...), the number of unsuccessful successive user authentications before account lockout is determined by the external directory service.
  The account lockout status is determined by the »Locked« attribute of the directory entity. If the directory entity is synchronized, the attribute is a part of the synchronized attributes.
- »Max icon size«: defines the maximum size of the icon file which represents a user or group of users.
- »Editable user fields«: defines the fields of user directory entities which can be edited.

2018 © Imaging Systems, Inc., All rights reserved.

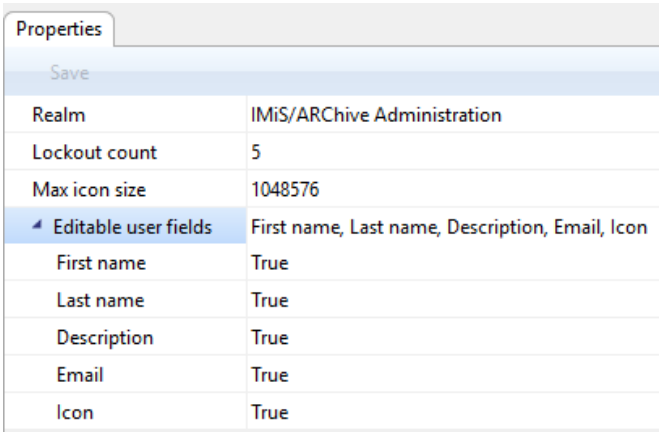


Image 319: »Properties« tab in authentication and authorization settings

8.4.6 »Codelists« folder

The »Codelists« folder contains a list of codelists, for which the user with appropriate access rights sets the value range. The following codelist information is listed in the columns:

- »Attribute«: attribute, to which the codelist is tied.
- »Template«: template, to which the codelist is tied.

2018 © Imaging Systems, Inc., All rights reserved.

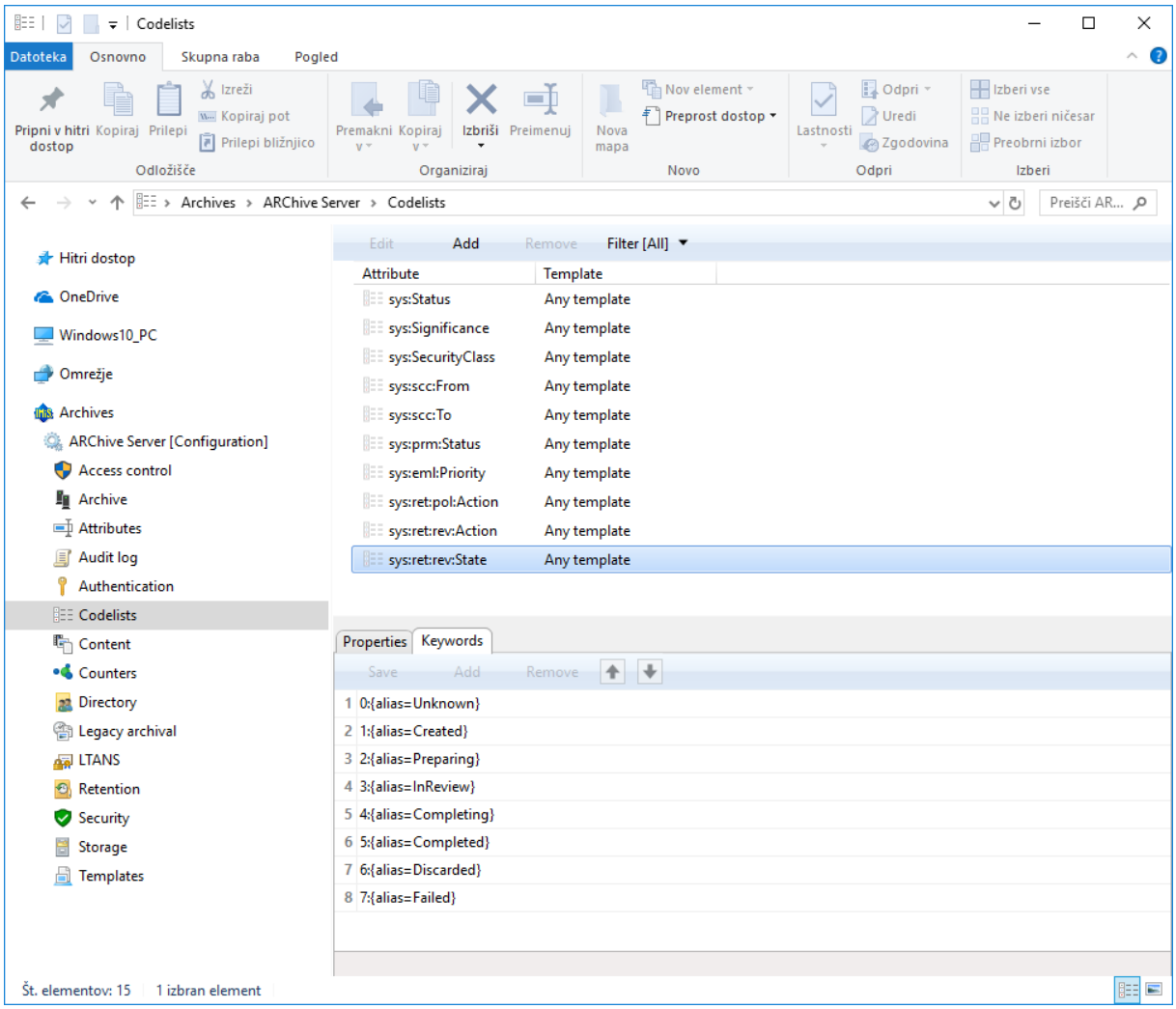


Image 320: Attribute list in the »Codelists« folder

By choosing the »Filter« command in the upper command bar, the user with appropriate access rights sets the view content.

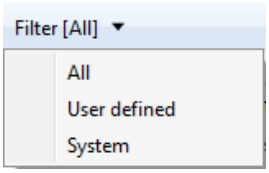


Image 321: Selecting the filter in the »Codelists« folder

The user can choose between the following options:

- »All«: all codelists are shown on the list.
- »User defined«: only user defined codelists are shown on the list.
- »System«: only system codelists are shown on the list.

2018 © Imaging Systems, Inc., All rights reserved.

»Properties« bar

By clicking the codelist on the list, the following value settings are shown in the »Properties« tab in the lower right view of the Windows Explorer.

- »Attribute«: contains the name of the attribute. Specifying the field value is mandatory for new entries. Once saved, the value can no longer be changed.
- »Template«: contains the value from the list of available templates, from which the user will select one of the attribute values from the codelist. The user can select the name of the individual template (for example Class, Case, Document...) or all templates.

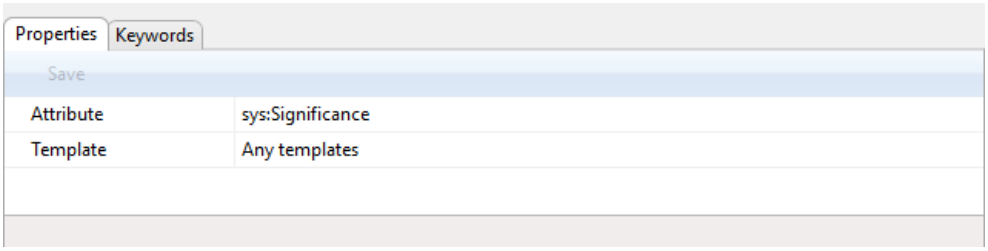


Image 322: Codelist properties

»Keywords« tab

By clicking the »Keywords« tab in the lower right view of the Windows Explorer, the user with appropriate access rights specifies the range of available attribute values.

Warning: It is important to ensure the correct syntax when adding values.
Attribute value can be written with or without quotes.

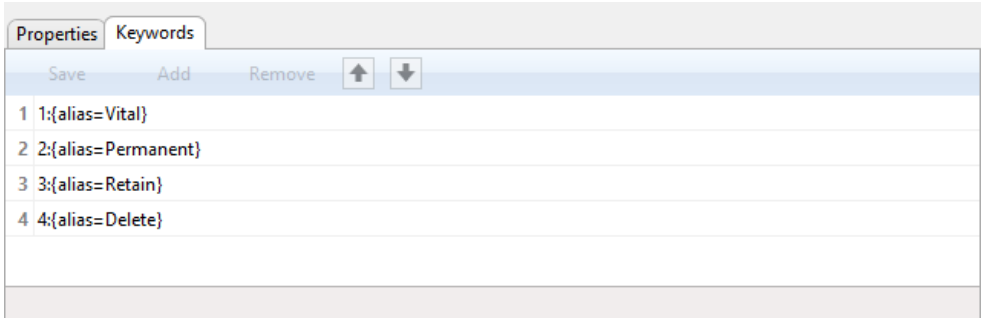


Image 323: Available attribute values without quotes

Warning: It is required to restart the IMiS®/ARChive Server in order to effect changes of the value settings in the »Codelists« folder.

2018 © Imaging Systems, Inc., All rights reserved.

8.4.7 »Content« folder

»Content« folder contains the following folders:

- Content types
- Converters
- Digital signatures
- Full text indexing
- Parsers
- Settings.

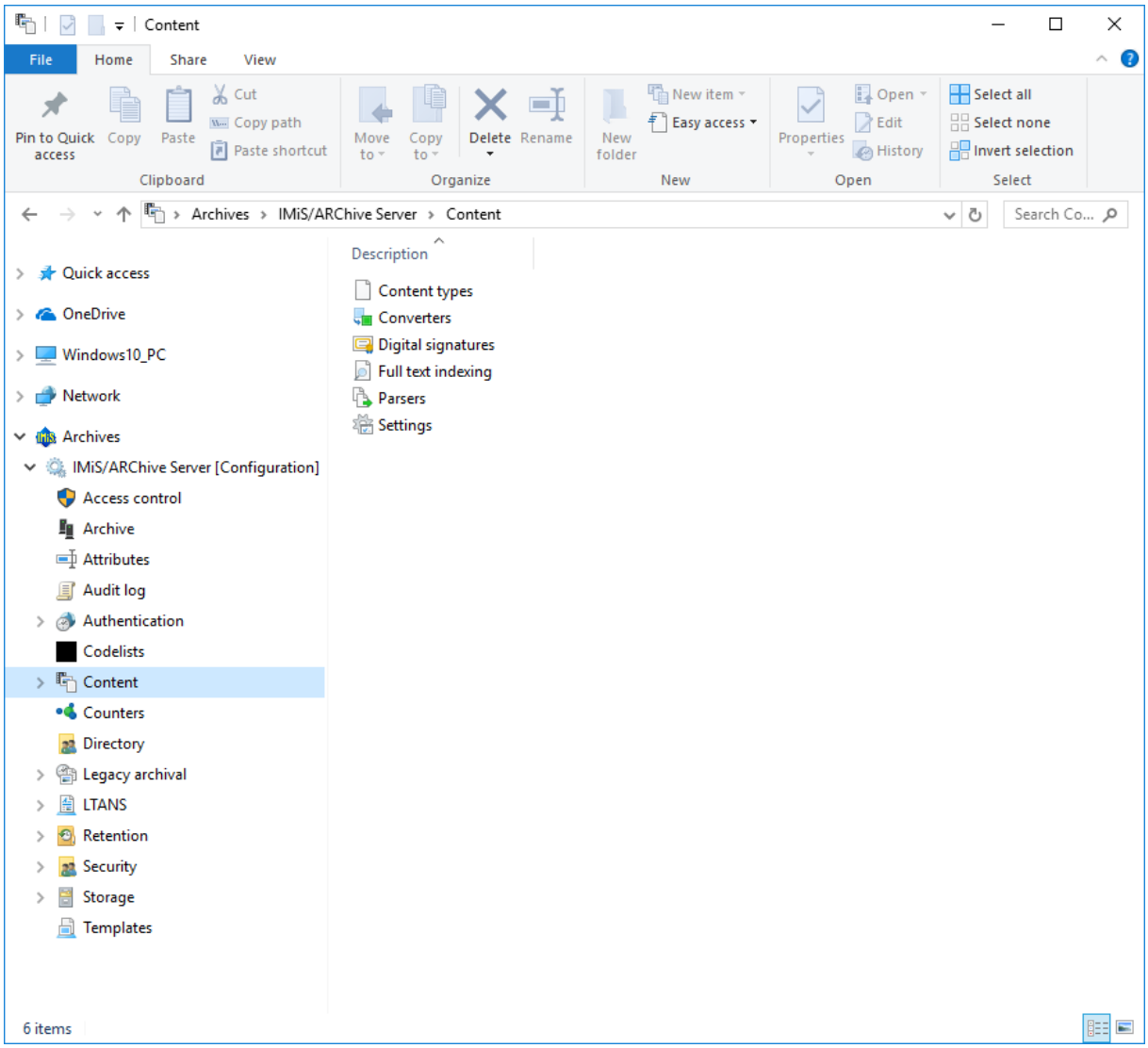


Image 324: List of contained folders in the »Content« configuration folder

8.4.7.1 »Content types« folder

The »Content types« folder contains a list of supported content types on the archive server.

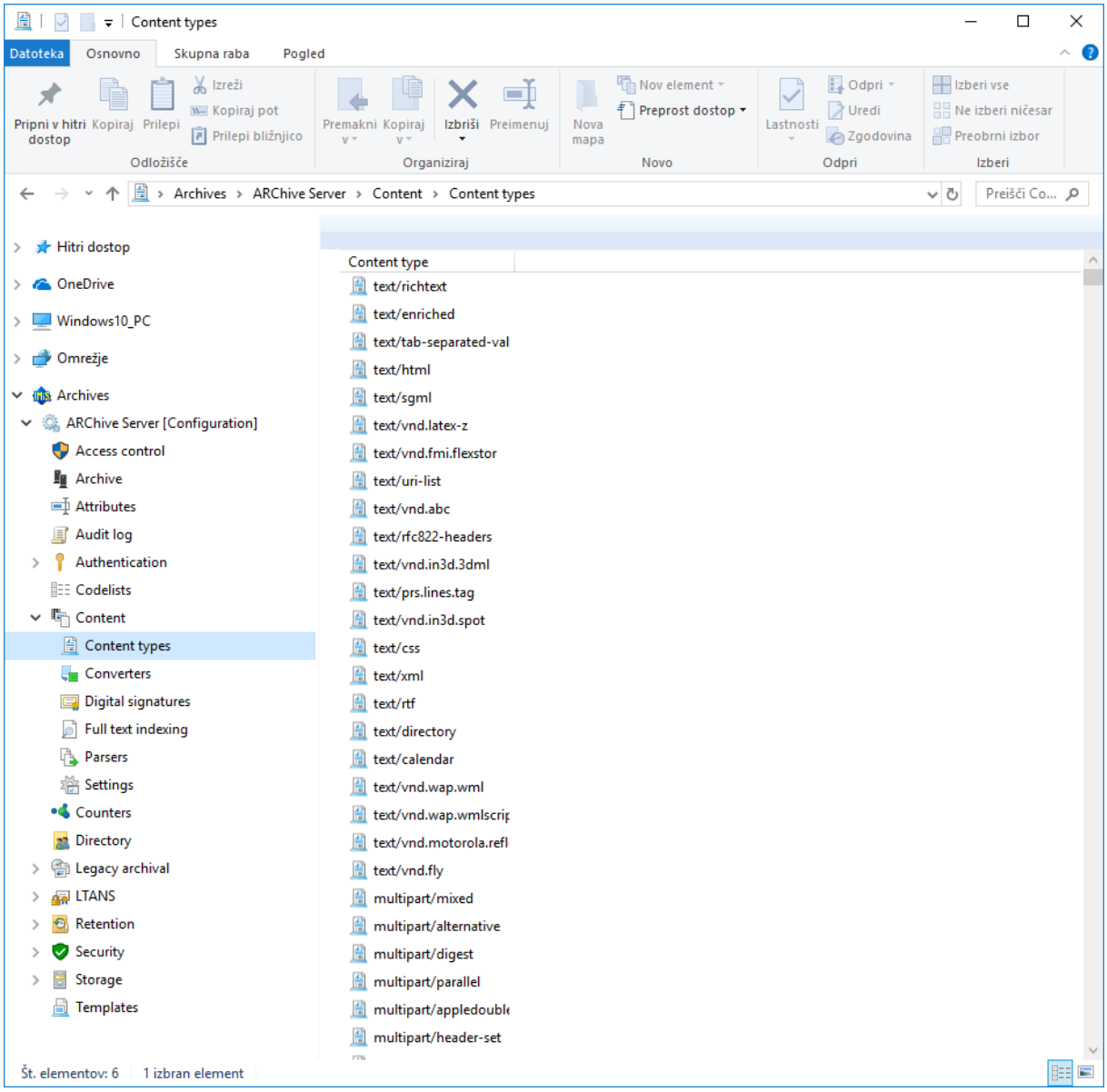


Image 325: List of supported MIME content types

8.4.7.2 »Converters« folder

The »Converters« folder contains a list of content converters.

Users with appropriate rights specify converters that are used to convert content from one format to another.

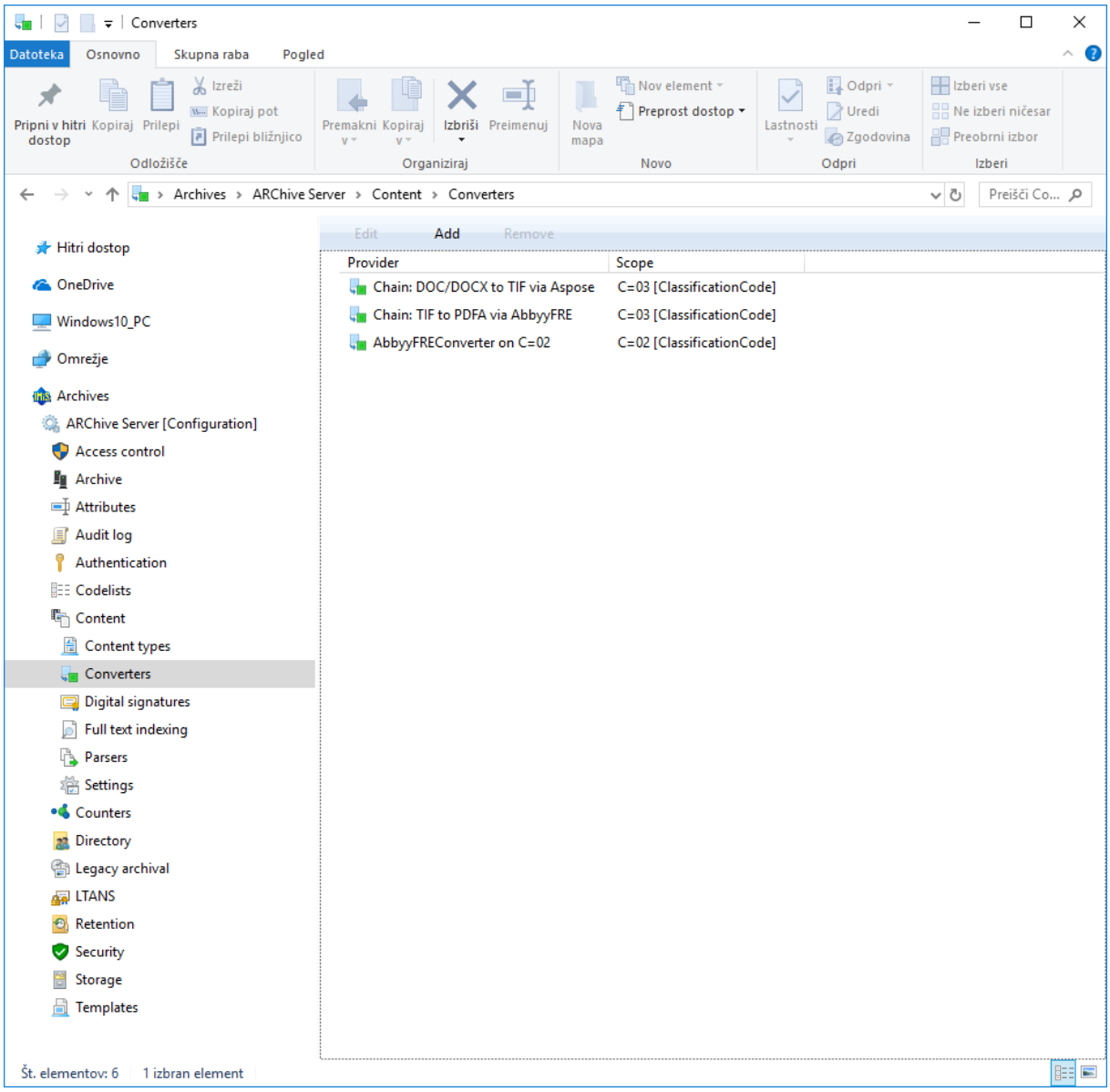


Image 326: A list of content converters

»Properties« tab

By clicking a converter in the list, the following settings are displayed in the »Properties« tab in the bottom right pane of Windows Explorer:

- »Identifier«: specifies the unique converter identifier.

- »Source operation«: specifies an operation that is performed with the original content during conversion.

  Users with appropriate rights can choose between the following options:

  - »None«: during conversion no operation is performed with the original content
  - »Delete after conversion«: after conversion, the original content is deleted
  - »Replace with conversion output«: the original content is deleted and replaced with the converted content after conversion.
- »Provider«: specifies data on the provider that is used for content conversion.

  Users with appropriate rights can view and/or change the following settings:

  - »Name«: name of the converter that is determined when the converter is created. After saving the converter, the name can no longer be changed.
  - »Type«: provider type (the default setting is »Plugin«)
  - »Driver«: content conversion driver
  - »Arguments«: specifies configuration parameters of the content conversion driver.
- »Content type filter«: specifies filter settings for content types on which conversion will be performed. Users with appropriate rights can view and/or change the following settings:

  - »Disposition«: specifies whether content types are included in the conversion. Value set to »Include« denotes that content types are included. On the contrary, by changing the value to »Exclude« users with appropriate rights exclude content types.
  - »Content types«: type of content on which conversion is performed.
- »Scope«: specifies which part of the classification tree will be converted.

  Users with appropriate rights can view and/or change the following settings:

  - »Type«: specifies the type of entity identifier (internal, external or classification code).
  - »Value«: specifies the value of entity identifier.

    The set value indicates conversion will be performed on entities that are listed under the selected entity and its contained entities. If the value is not set, there are no limitations and the conversion will be performed on the entire archive.

2018 © Imaging Systems, Inc., All rights reserved.

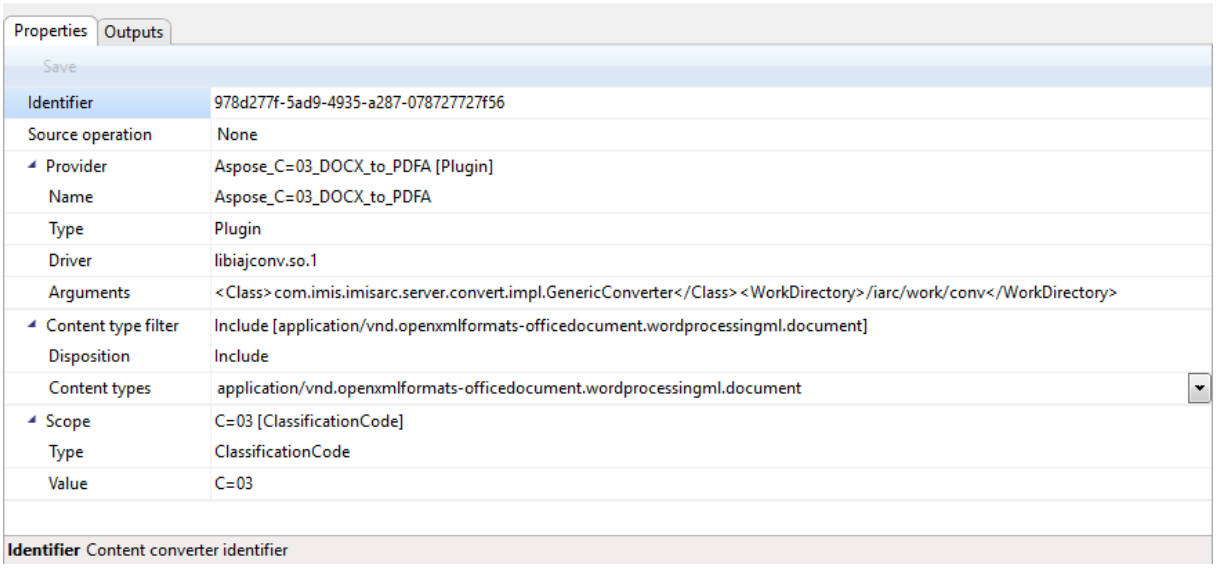


Image 327: Converter »Properties« tab

»Outputs« tab

By clicking a converter in the list, the user can set the output settings for content conversion in »Outputs« tab in the bottom right pane of Windows Explorer. By choosing the »Add« command in the bottom command bar, the user can add and set a new output for content conversion. By choosing the »Remove« command, the user can remove it.

Users with appropriate rights can choose between the following options:

- »Content type«: specifies the output content type.
- »Queue for FTI«: specifies whether the output content is assigned to queue for full text indexing creation. Value set to »True« denotes converted content will be assigned to queue for full text indexing creation. On the contrary, the value »False« denotes converted content will not be assigned to queue for full text indexing.
- »Next Converter«: name of the next content converter.
  In case of choosing the converter, the first content conversion is followed by conversion to other formats. Otherwise, only the original conversion is performed.
- »Replace source«: specifies whether source content is replaced with converted content. Value set to »True« denotes converted content will replace the source content after conversion. On the contrary, the value »False« denotes converted content will not replace the source content.

2018 © Imaging Systems, Inc., All rights reserved.

- »Standalone«: specifies whether converted content is displayed as standalone content (is excluded from the source content representations) in the content.
  Value set to »True« denotes converted content will be displayed as standalone content. On the contrary, the value »False« denotes converted content will be displayed as the source content representation.
- »Description expression«: specifies how the name of the converted content will be recorded. If the expression for the name of the converted content is specified, it is applied when naming the converted content. Otherwise, it stays the same as the name of the source content. For better understanding see chapter Conversion examples.

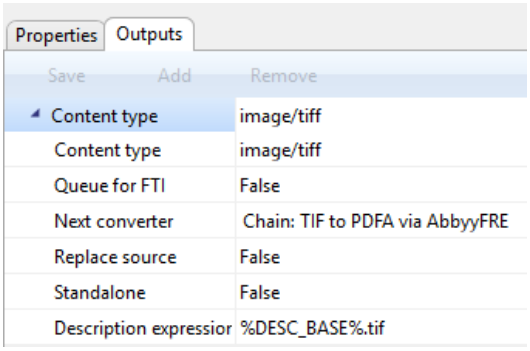


Image 328: Converter »Properties« tab

8.4.7.3 Conversion examples

Below are some examples for better understanding of the conversion process.

Example 1:

We will take the conversion of an MS Word document DOCX format to a format for long-term content storage PDF/A as an example.

Server settings specify that:

- *all DOCX content format are converted to PDF/A when saved.*
- *no source content is deleted or replaced with the converted content (Source operation=None).*
- *conversion is performed only on content listed below a specified root class (C=01).*
- *name of the converted content is not changed (Description expression=%DESC_BASE%.pdf).*

2018 © Imaging Systems, Inc., All rights reserved.

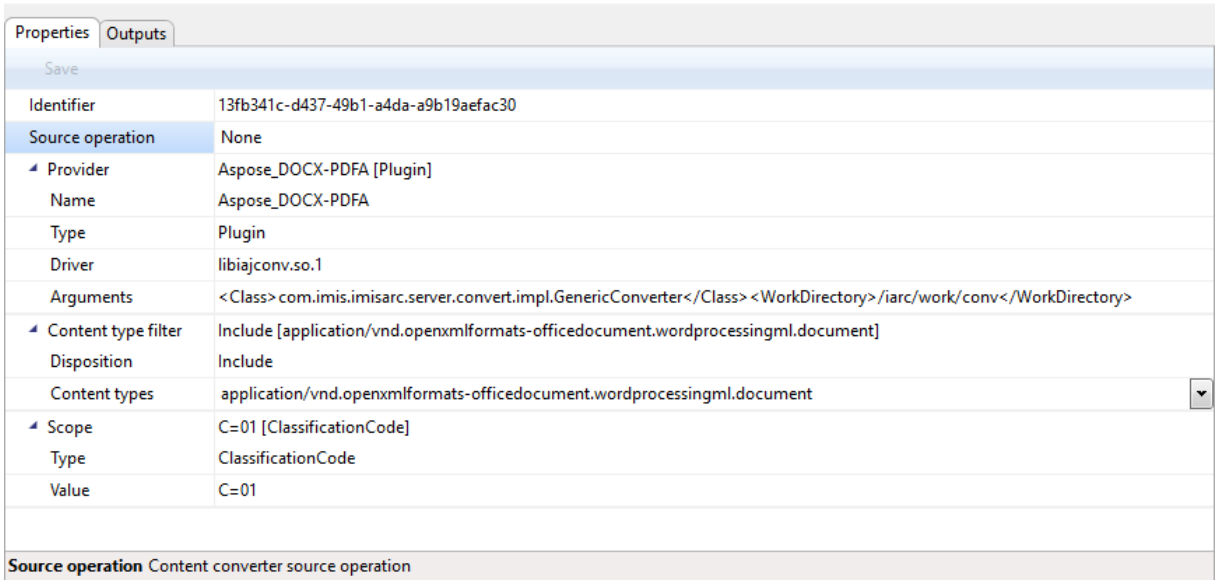


Image 329: Conversion from DOCX to PDF/A: basic properties settings

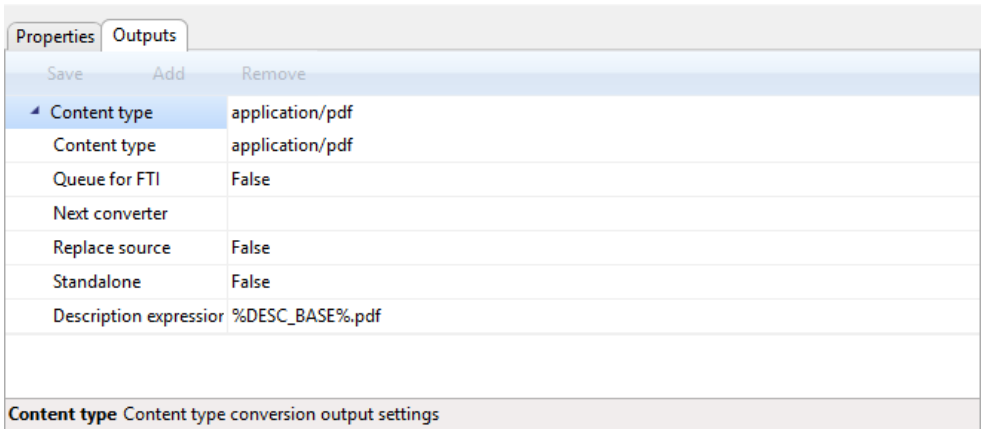


Image 330: Conversion from DOCX to PDF/A: output parameters settings

The display of the conversion result is as follows:

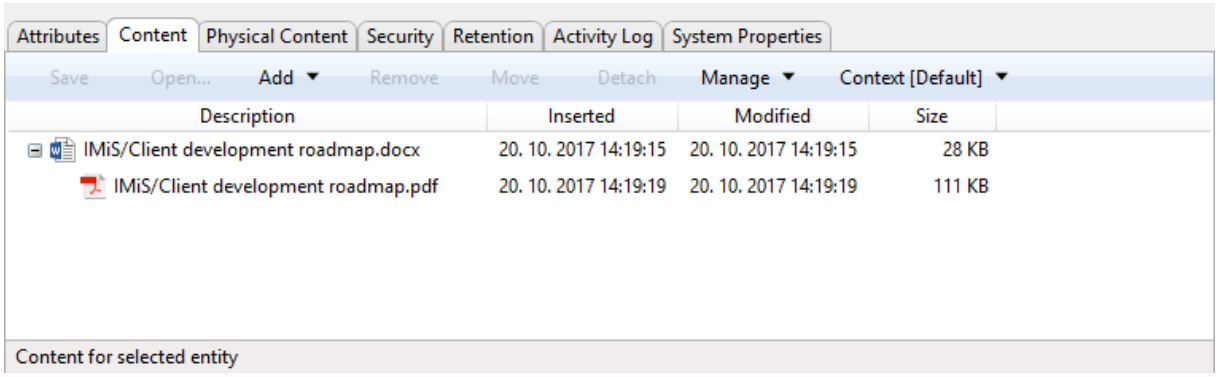


Image 331: Example of the date of the document content change

2018 © Imaging Systems, Inc., All rights reserved.

Example 2:

We will take the conversion of a DOC format to a format for long-term content storage -TIFF and PDF/A as an example.

Server settings specify that:

- *on the level of the entire archive the DOC formats are first converted to TIFF upon being saved (Scope=Root [Classification code]).*
- *no source content is deleted or replaced with the converted content (Source operation=None).*
- *conversion to TIFF is performed on all DOC format content in the archive (value of the Value attribute stays empty).*
- *TIFF to PDF/A conversion is performed only on content listed below a specified root class (C=01).*
- *name of the converted content is not changed:*
  - *conversion from DOC to TIFF: Description expression=%DESC_BASE%.tif [OCR at %NOW_YEAR%-%NOW_MONTH%-%NOW_DAY% %NOW_HOUR%:%NOW_MINUTE%:%NOW_SECOND%.*

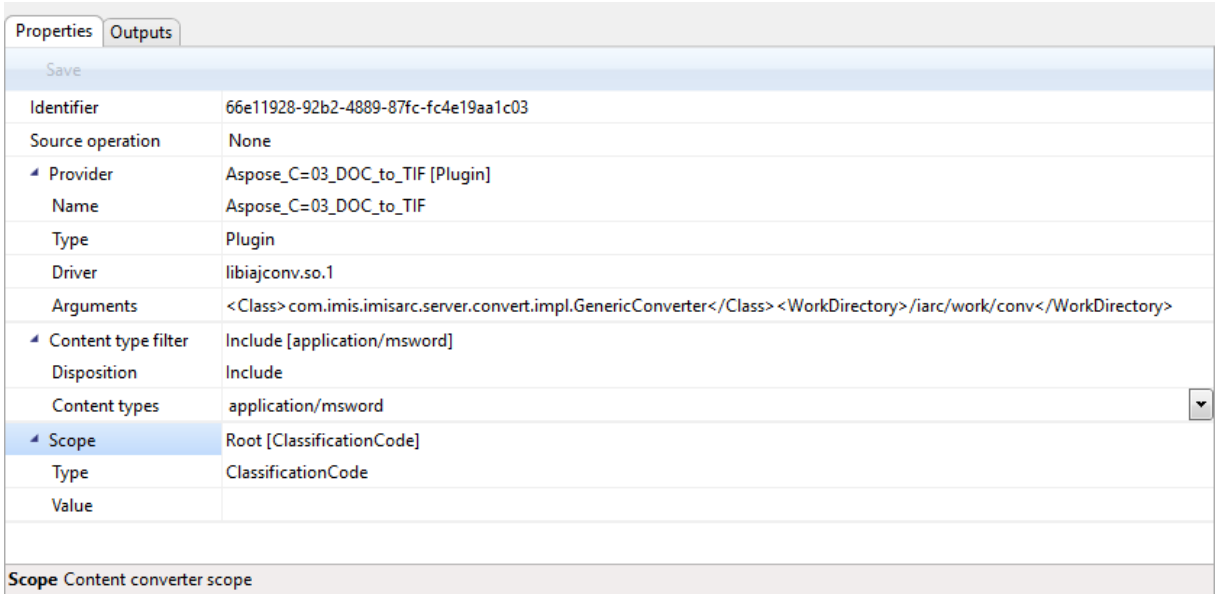


Image 332: Conversion from DOC to TIFF: basic properties settings

2018 © Imaging Systems, Inc., All rights reserved.

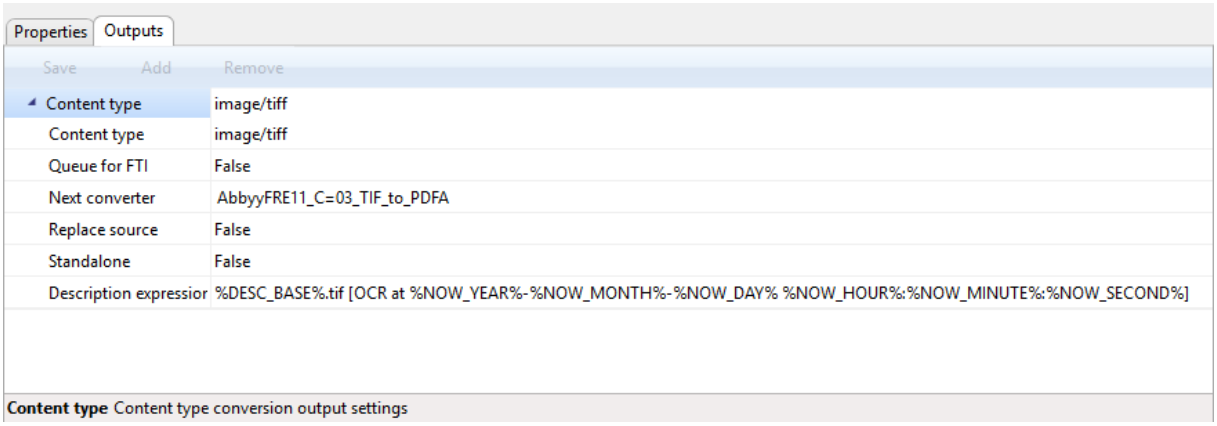


Image 333: Conversion from DOC to TIFF: output parameter settings

– *conversion from TIFF to PDF/A: Description expression=%DESC_BASE%.pdf [OCR, %PAGE_COUNT%pages.*

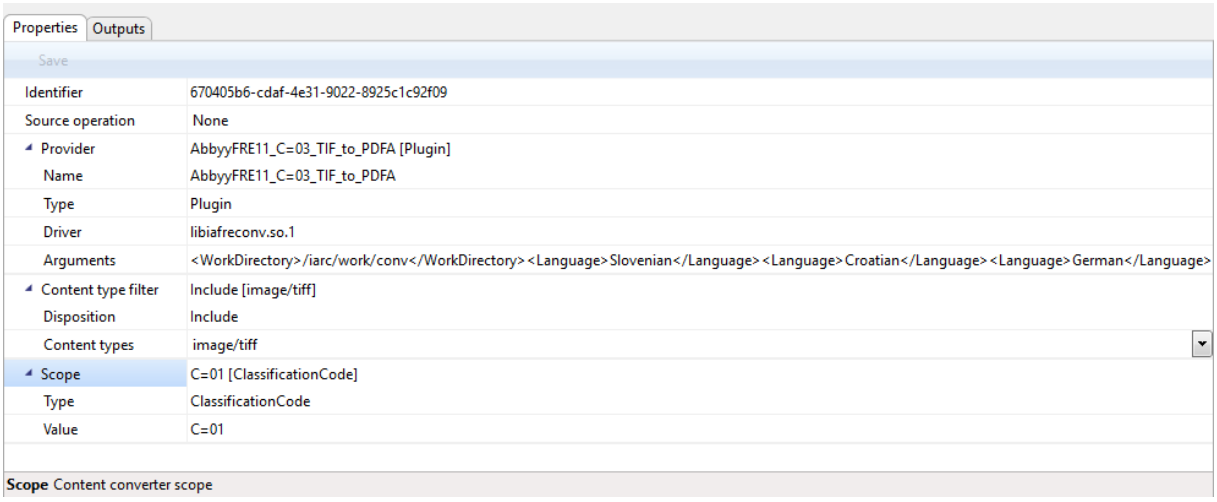


Image 334: Conversion from TIFF to PDF/A: basic properties settings

2018 © Imaging Systems, Inc., All rights reserved.

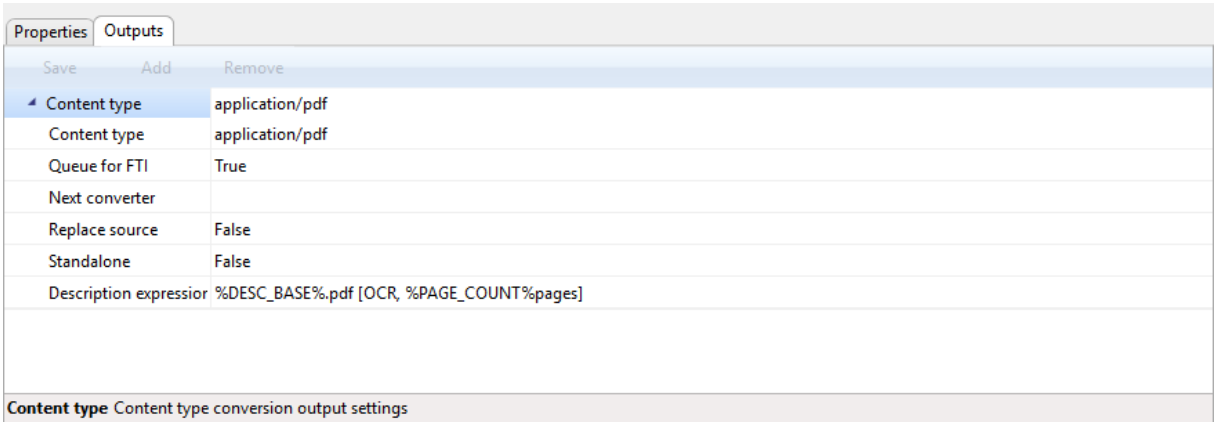


Image 335: Conversion from DOC to TIFF: output parameters settings

The display of the conversion result is as follows:

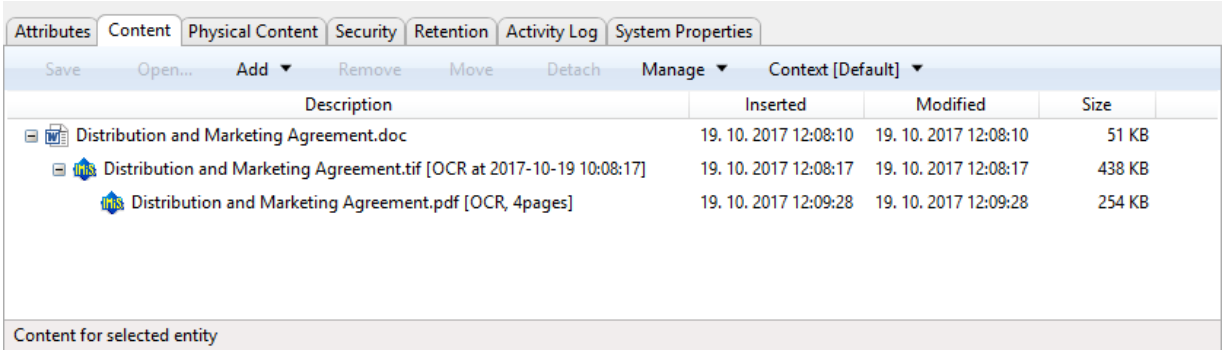


Image 336: Example of conversion from DOC format to TIFF and PDF/A

2018 © Imaging Systems, Inc., All rights reserved.

8.4.7.4 »Digital signatures« folder

The »Digital signatures« folder contains digital signed content settings.

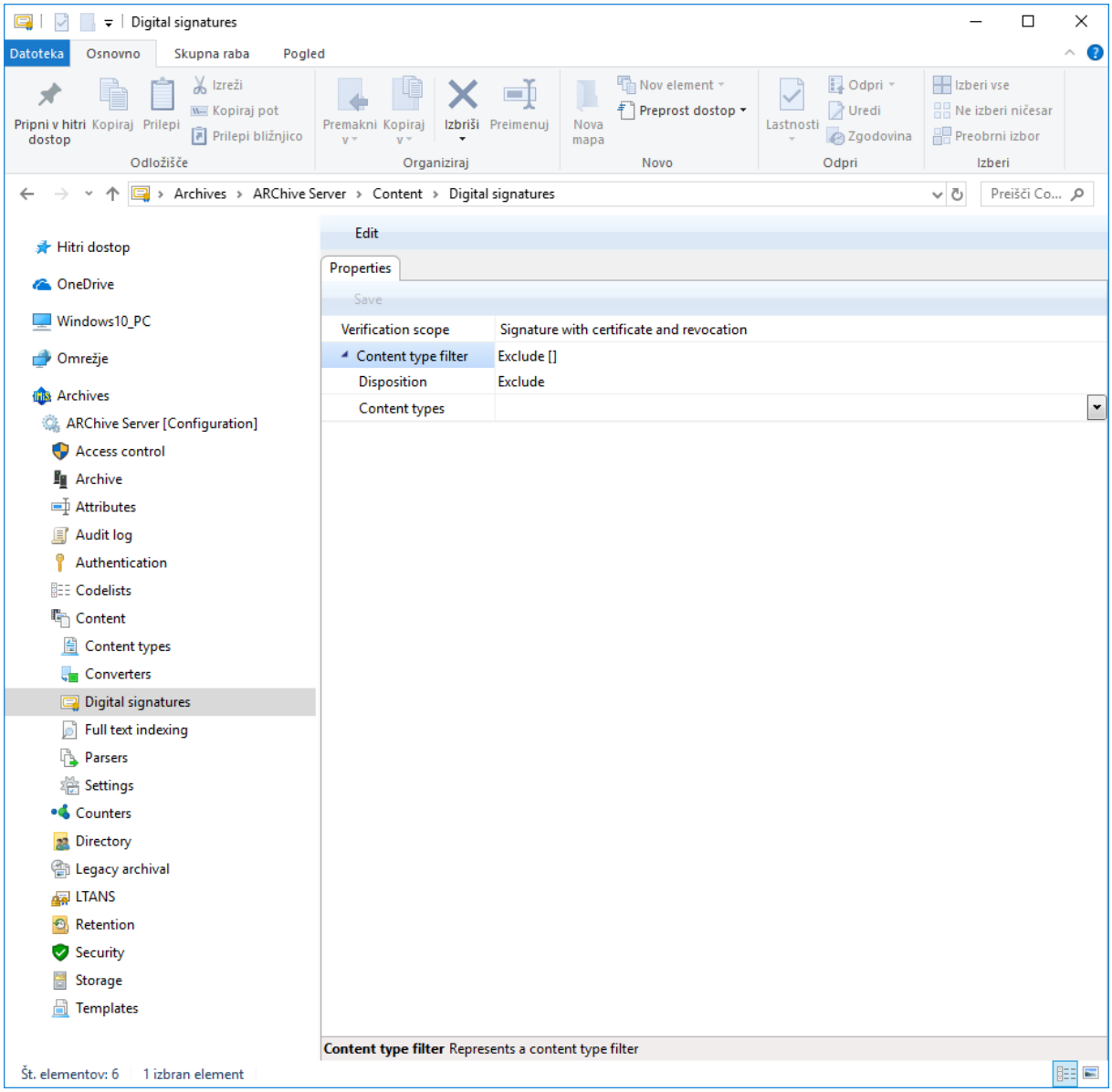


Image 337: »Properties« tab in the »Digital signatures« configuration folder

»Properties« tab

By clicking the »Digital signatures« folder, the following settings are displayed in the »Properties« tab in the right pane of Windows Explorer:

- »Verification scope«: specifies how digital signatures are verified. Users with appropriate rights can choose between the following options:
  - »None«: denotes that verification of digital signatures is not performed.

2018 © Imaging Systems, Inc., All rights reserved.

  - »Signature«: denotes that only verification of digital signatures of contents is performed.
  - »Signature with certificate«: denotes that verification of digital signatures of contents and digital certificates is performed.
  - »Signature with certificate and revocation«: denotes that verification of digital signatures of contents, digital certificates and digital certificate revocations is performed.
  - »Signature with certificate chain and revocation«: denotes that verification of digital signatures of contents, digital certificates chain and digital certificate revocations is performed.
- »Content type filter«: specifies content type filter settings on which verification of digital signatures will be performed.

  Users with appropriate rights can view and/or change the following settings:
  - »Disposition«: specifies whether content types are included in the verification of digital signatures.

    Value set to »Include« denotes that content types are included. On the contrary, by changing the value to »Exclude« users with appropriate rights exclude content types.
  - »Content types«: type of content on which verification of digital signatures is performed.

2018 © Imaging Systems, Inc., All rights reserved.

8.4.7.5 »Full text indexing« folder

The »Full text indexing« folder contains the settings for indexing the full text of documents.

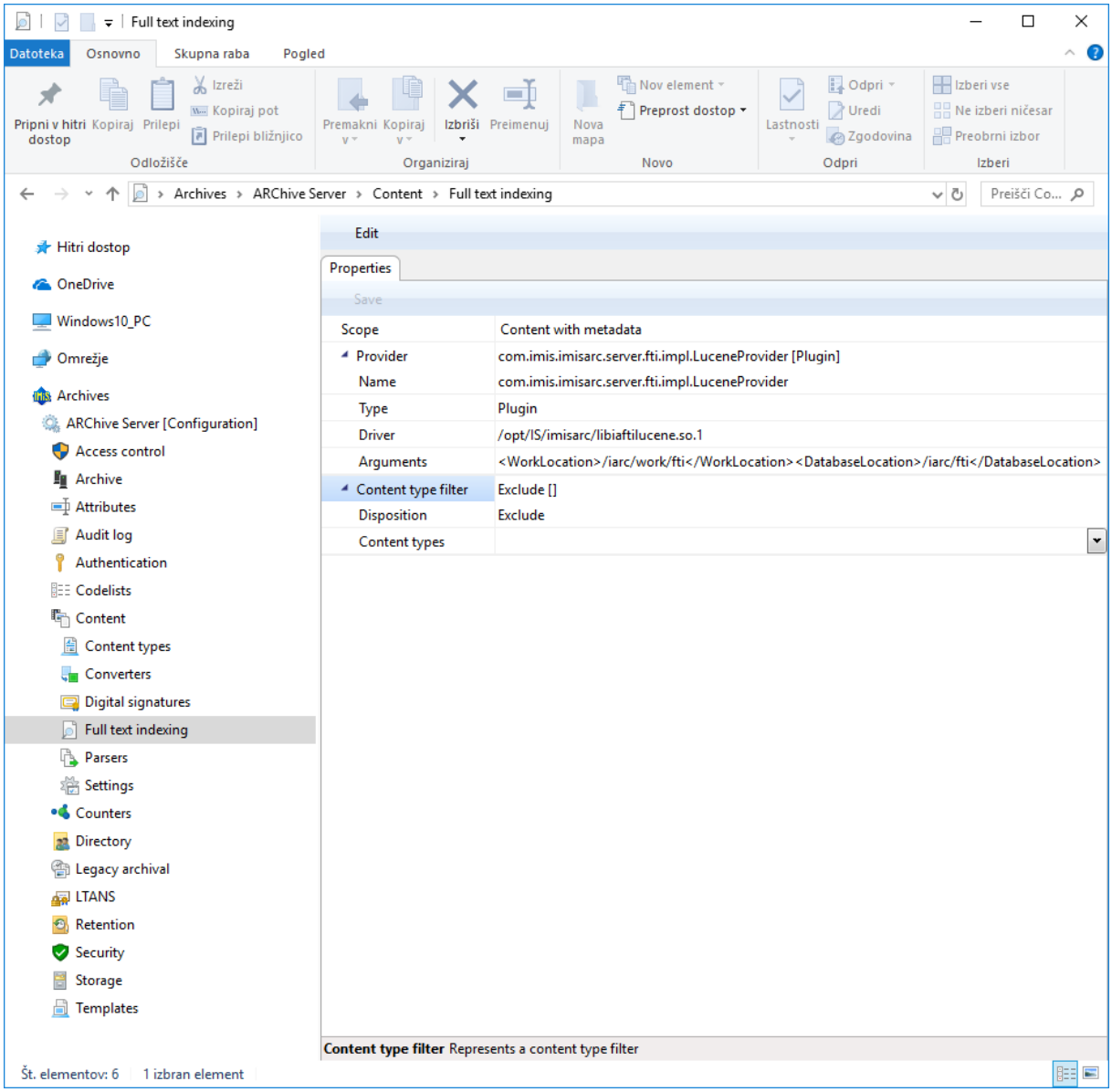


Image 338: »Properties« tab in the »Full text indexing« configuration folder

»Properties« tab

By clicking the »Full text indexing« folder, the following settings are displayed in the »Properties« tab in the right pane of Windows Explorer:

- »Scope«: specifies the extent of text indexing creation. Users with appropriate rights can choose between the following options:
  - »None«: denotes that full text indexing is not performed

  - »Content«: denotes that indexing is performed on the entire text of the content without its metadata
  - »Content with metadata«: denotes that indexing is performed on the entire text of the content and its metadata.
- »Provider«: specifies provider data that is used for text indexing. Users with appropriate rights can view and/or change the following settings:
  - »Name«: name of the provider
  - »Type«: provider type (default setting is »Plugin«)
  - »Driver«: driver for indexing content text
  - »Arguments«: specifies configuration parameters of the driver for indexing content text.
- »Content type filter«: specifies content type filters on which full text indexing will be performed.
- Users with appropriate rights can view and/or change the following settings:
  - »Disposition«: specifies whether content types are included in full text indexing. Value set to »Include« denotes that content types are included. On the contrary, by changing the value to »Exclude« users with appropriate rights exclude content types.
  - »Content types«: type of content on which full text indexing is performed.

8.4.7.6 »Parsers« folder

The »Parsers« folder contains parser properties settings.

IMiS®/ARChive Server uses parsers to extract text from the various stored content types, and then returns them to the full text indexing subsystem. The second parser functionality is capturing and verifying the validity of different types of digital certificates, if they exist. Parsers return the digital signatures and corresponding digital certificates to the IMiS®/ARChive Server for storage that is separated from contents, and can be used by the server in the authentication assurance strategy algorithms.

2018 © Imaging Systems, Inc., All rights reserved.

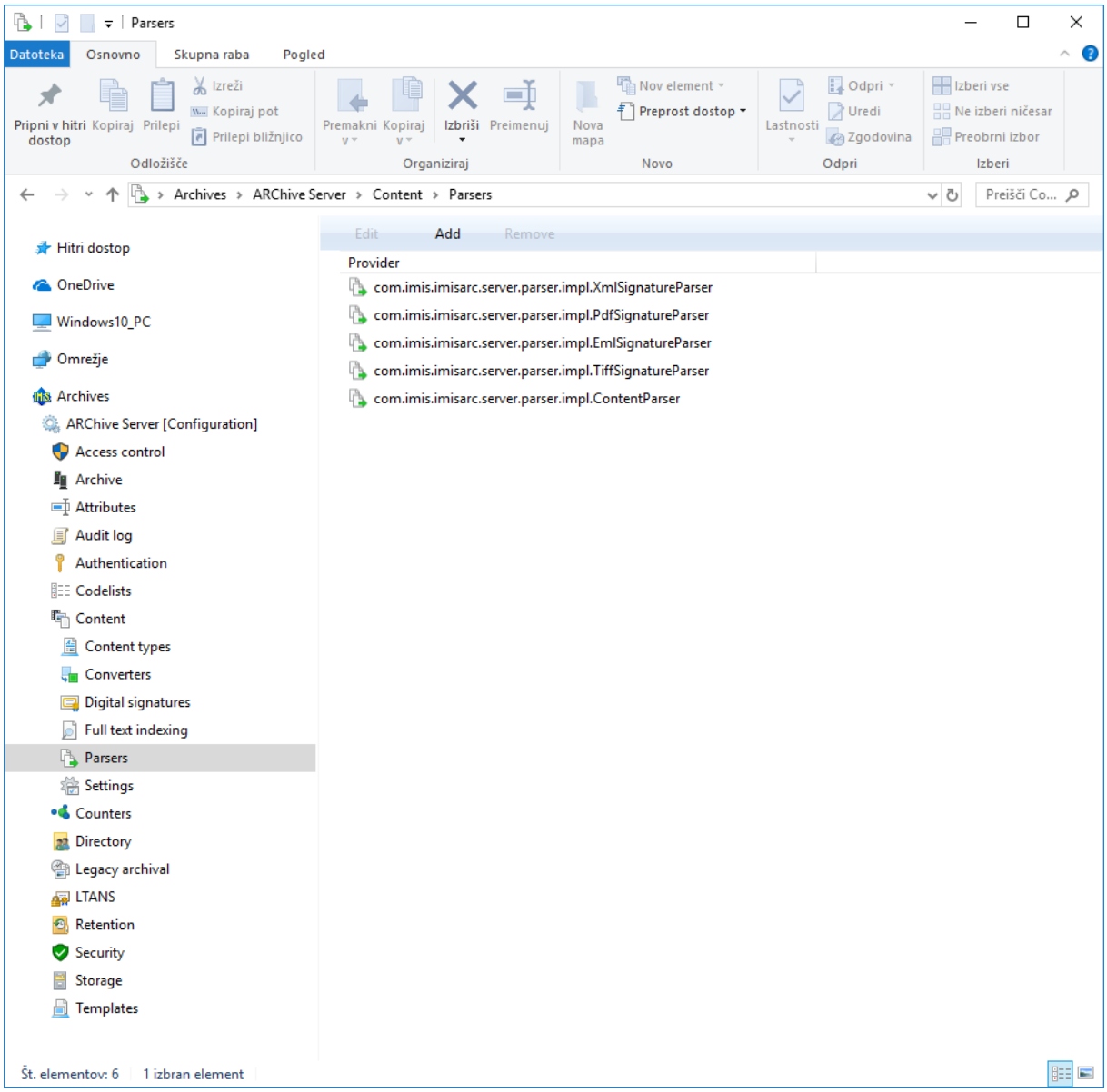


Image 339: »Properties« tab in the »Parsers« configuration folder

»Properties« tab

- »Identifier«: specifies a unique parser identifier.
- »Provider«: specifies data on the provider that is used for content parsing.

  Users with appropriate rights can view and/or change the following settings:

  - »Name«: name of the provider that is determined when the content parser is created. After saving the parser, the name can no longer be changed
  - »Type«: provider type (the default setting is »Plugin«)
  - »Driver«: content parser driver
  - »Arguments«: specifies configuration parameters of the content parser driver.

2018 © Imaging Systems, Inc., All rights reserved.

- »Content type filter«: specifies filter settings for content types on which parsing will be performed.

  Users with appropriate rights can view and/or change the following settings:

  - »Disposition«: specifies whether content types are included in the parsing.

    Value set to »Include« denotes that content types are included. On the contrary, by changing the value to »Exclude« users with appropriate rights exclude content types.
  - »Content types«: type of content on which parsing is performed.

8.4.7.7 »Settings« folder

The »Settings« folder contains settings for content management.

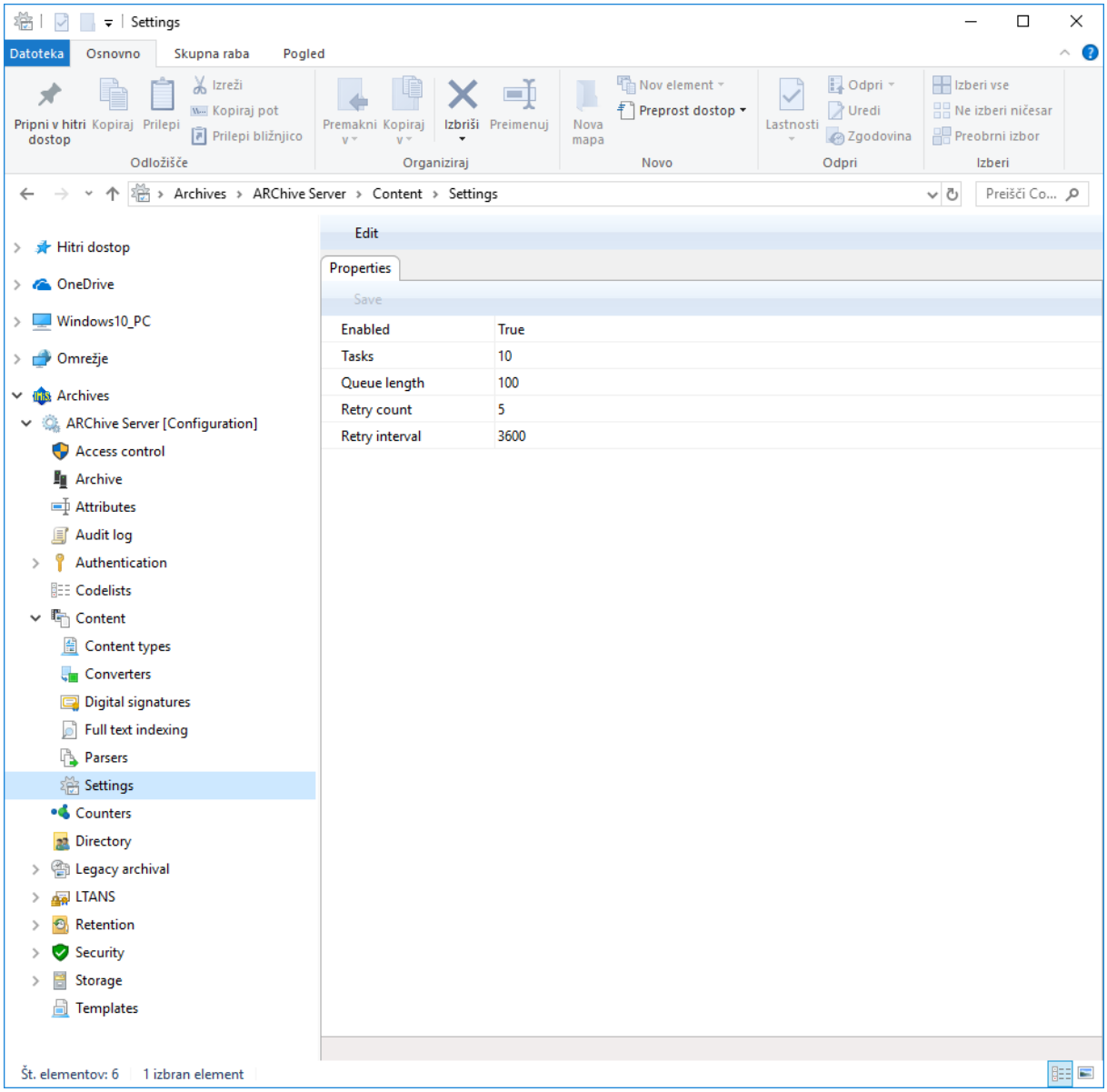


Image 340: »Properties« tab in the »Settings« configuration folder

»Properties« tab

By clicking the »Settings« folder, the following settings are displayed in the »Properties« tab in the right pane of Windows Explorer:

- »Enabled«: denotes whether content conversion is enabled.
  Default value set to »True« denotes that content conversion is enabled. On the contrary, by changing the value to »False« users with appropriate rights disable content conversion.
- »Tasks«: specifies the number of parallel content conversion tasks.
- »Queue length«: specifies the maximum number of jobs the IMiS®/ARChive Server assigns to a single content conversion task at a time.
- »Retry count«: specifies the number of times content conversion attempts are repeated in the event of conversion errors.
- »Retry interval«: specifies the minimum time in seconds between content conversion attempts when conversion ends with an error.

8.4.8 »Counters« folder

In the »Counters« folder the user with appropriate access rights can define counters, which are used for generating values of the selected attributes. The following information about the values of the selected attributes is listed in the columns:

- »Scope«: defines the entity type, for which the counter is used. To ensure clarity, individual counter types have their own icons.
- »Level«: defines the entity level in the classification scheme.
- »Level aspect«: defines the entity position in the classification scheme according to its parent entity.
- »Storage«: attribute, for which the value is generated using the counter.
- »Unique within«: defines the uniqueness of the counter within the selected context.

2018 © Imaging Systems, Inc., All rights reserved.

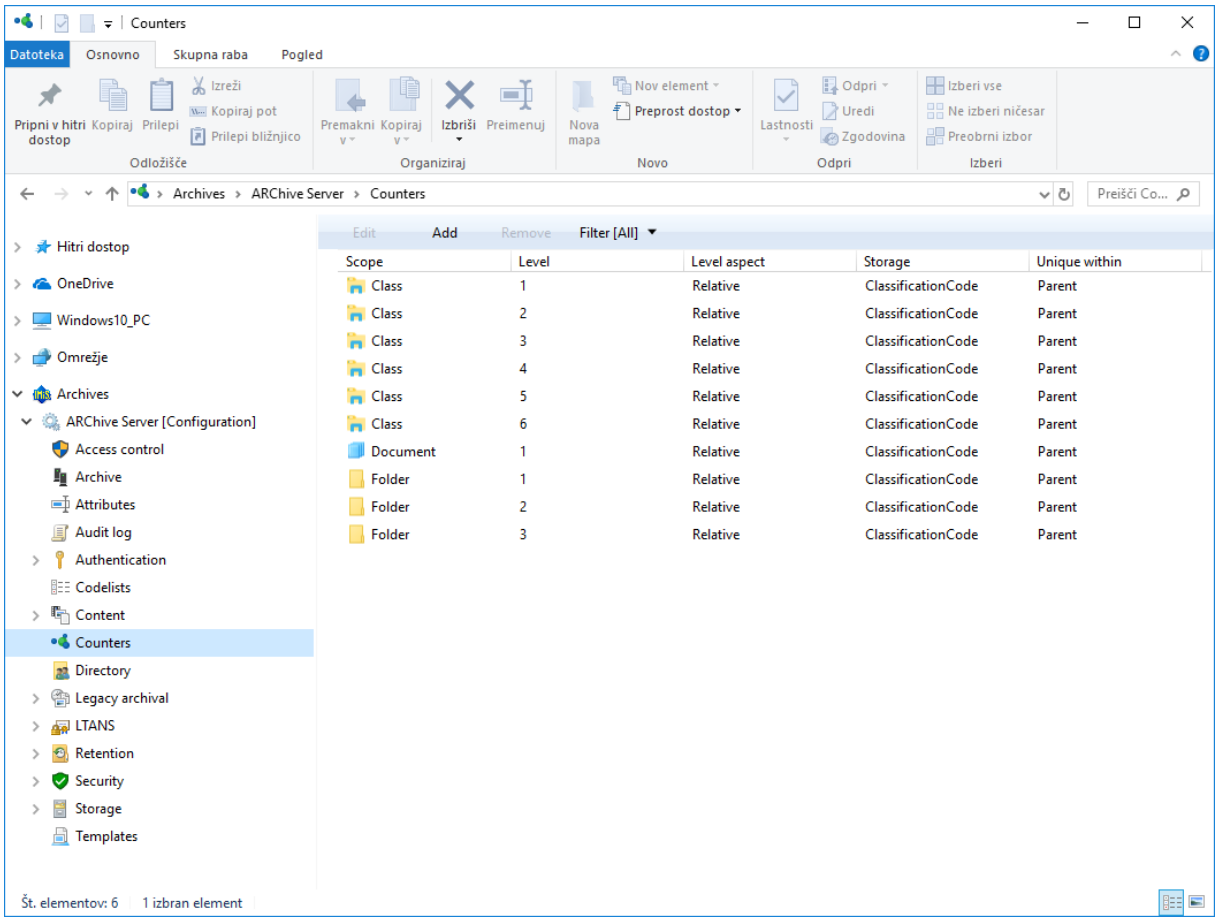


Image 341: Attribute list in the »Counters« folder

By choosing the »Filter« command in the upper command bar, the user with appropriate access rights can set the view content.

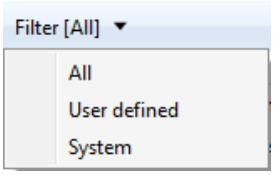


Image 342: Selecting the filter in the »Counters« folder

The user can choose between the following options:

- »All«: all counters are shown on the list.
- »Class«: only counters for classes are shown on the list.
- »Folder«: only counters for folders are shown on the list.
- »Document«: only counters for documents are shown on the list.

2018 © Imaging Systems, Inc., All rights reserved.

It is defined for the class, folder and documents, until which level in the classification scheme the user with rights for creating entities can create sub-entities.

»Properties« bar

By clicking the counter on the list, the following value settings are shown in the lower right view of the Windows Explorer:

- »Scope«: defines the entity type. The user with appropriate access rights can choose between the class, folder or document. Specifying the field value is mandatory for new entries. It cannot be changed for the existing entries.
- »Level«: defines the entity level in the classification scheme.
  When defining a new level of the class, folder or document, the user with access rights for creating entities can create a new sub-entity of this type. Specifying the field value is mandatory for new entries. It cannot be changed for the existing entries.
- »Level aspect«: defines the entity position in the classification scheme according to its parent entity. The user with appropriate access rights can choose between the »Relative« or »Absolute« value. When the selected value is »Relative«, the uniqueness of counting is set in the »Unique within« field. When the selected value is »Absolute«, the counting is unique on the level of the entire archive.
- »Attribute«: attribute, for which the value is generated using the counter.
  The user with appropriate access rights can choose between the »Classification code« and user-defined attributes. Specifying the field value is mandatory for new entries.
  It cannot be changed for the existing entries.
- »Unique within«: defines the uniqueness of the counter within the selected context.
  The user with appropriate access rights can choose between the following contexts:
  - »Archive«: uniqueness applies to the entire archive.
  - »Parent«: uniqueness applies to the parent class.
  - »Root class«: uniqueness applies to the first class in the chain of parent classes.
  - »Leaf class«: uniqueness applies to the last class in the chain of parent classes.
- »Initial value«: defines the initial value of the attribute value counter, which is selected in the »Storage« field.
- »Increment«: defines, in which steps the counter will increase for the attribute level selected in the »Storage« field.
- »Format«: defines the attribute value entry selected in the »Storage« field.

2018 © Imaging Systems, Inc., All rights reserved.

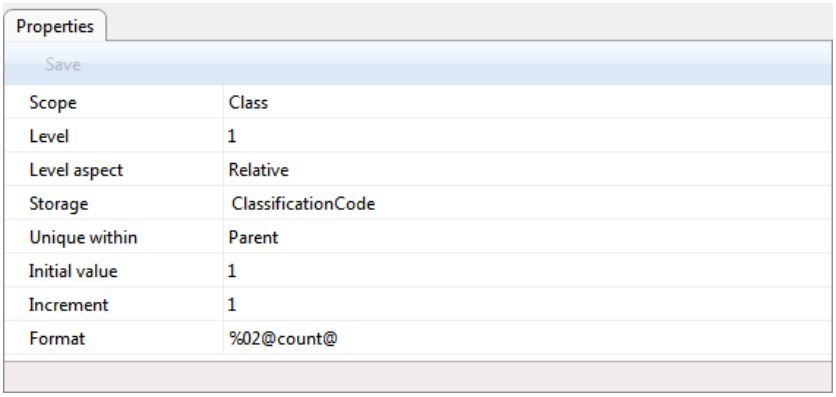


Image 343: Counter properties for the class on the first level

Warning: Archive administrator must carefully plan the entity tree structure. For correct sorting of entities in the classification scheme it is advisable to anticipate the number of root classes. Based on their number the format is determined accordingly.

Example: The value »%02@count@« of the attribute Format in the image above determines that the class classification codes are recorded from 1 to 99. With this setting the classes with a classification code between 100 and 199 would be sorted between 10 and 20, which would lead to the lack of clarity in classification scheme. If the anticipated number of classes is around 100, the necessary value of the attribute »Format« must be set to »%03@count@«.

8.4.9 »Directory« folder

The »Directory« folder contains a list of users and user groups of the archive.

The following information about users or user groups is listed in the columns:

- »Subject«: a unique code for the user or user group in the archive.
  To ensure clarity, the users and user groups have their own icons.
- »First Name«: name of the user or user group.
- »Last name«: last name of the user or user group.
- »Description«: a short description of the user or user group.
- »Directory«: directory name.

2018 © Imaging Systems, Inc., All rights reserved.

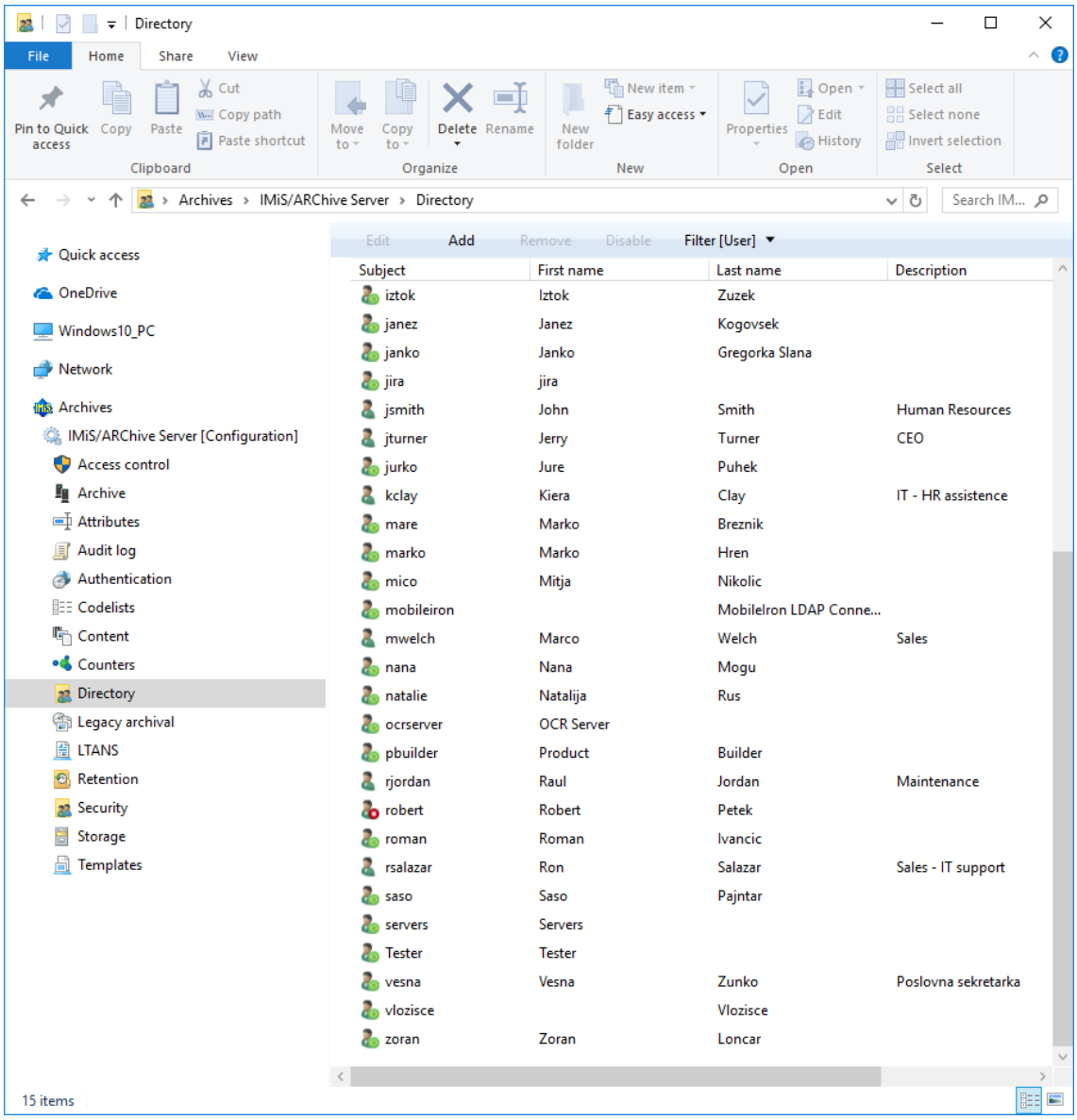


Image 344: List of users and user groups in the »Directory« folder

By choosing the »Filter« command in the upper command bar, the user with appropriate access rights can set the view content.

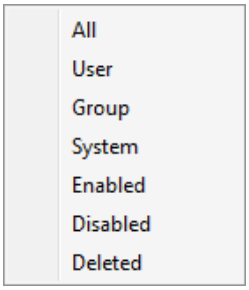


Image 345: Selecting the filter in the »Directory« folder

2018 © Imaging Systems, Inc., All rights reserved.

The following groups are available in the filter:

- »All«: all users and user groups are shown on the user list.
- »User«: all active users are shown on the list.
- »Group«: all active user groups are shown on the list.
- »System«: all active system users and groups are shown on the list.
- »Disabled«: all inactive system users and groups are shown on the list.
  To activate the users and user groups again, the »Enabled« value in the »Properties« tab must be changed to »True«.
- »Deleted«: all deleted users and groups are shown on the list.
  Once the users and user groups are deleted, they cannot be activated again.

»Properties« bar

By clicking the individual entry on the list, the following value settings are displayed in the lower right view of the Windows Explorer.

- »Subject«: contains a unique user code - his username. The user can access the archive using this username (and set password). It is required to define the field value for all new entries. It cannot be changed for the existing entries.
- »Type«: contains the user type. The user with appropriate access rights can choose between the »User« and »Group«. It is required to define the field value for all new entries. It cannot be changed for the existing entries.
- »Name«: contains the name of the user or first name of the user group.
- »Last name«: contains the last name of the user or the second name of the user group. It is required to define the field value for all new entries. It is possible to change the value of the existing entries; however, empty value is not permitted.
- »Description«: can contain a description of the user's position in the company.
- »Email«: contains the user's email address.
- »Directory«: specifies the name of the directory through which users access the archive server.
- »Aliases«: contains alternative usernames for the users to access the archive.
- »Security class level«: defines until which security class level the user can view the entities. The user can only view the entities if the security class of the entities is lower or the same as his clearance level.
- »Password hash«: contains a 40-character hash of the user's password if one has been set by the user with appropriate rights.

2018 © Imaging Systems, Inc., All rights reserved.

- »Locked«: value set to »False« denotes the user is not locked and can access the archive according to his rights.
  On the contrary, by changing the value to »True« the user cannot access the IMiS®/ARChive Server. Users with appropriate rights can change the value for local or non-synchronized users (Synchronization enabled = False).

  Note: After the lock, users can access the entities and perform actions as long as their session is still valid. It is not possible to login to the archive again and establish a session until the settings are changed.

- »Synchronization enabled«: if the selected value is »True«, data on the user is synchronized with the external directory. When changing the value to »False«, the user with appropriate access rights disables user synchronization with the external directory.
- »Member in groups«: contains a list of groups, in which the user is a member.

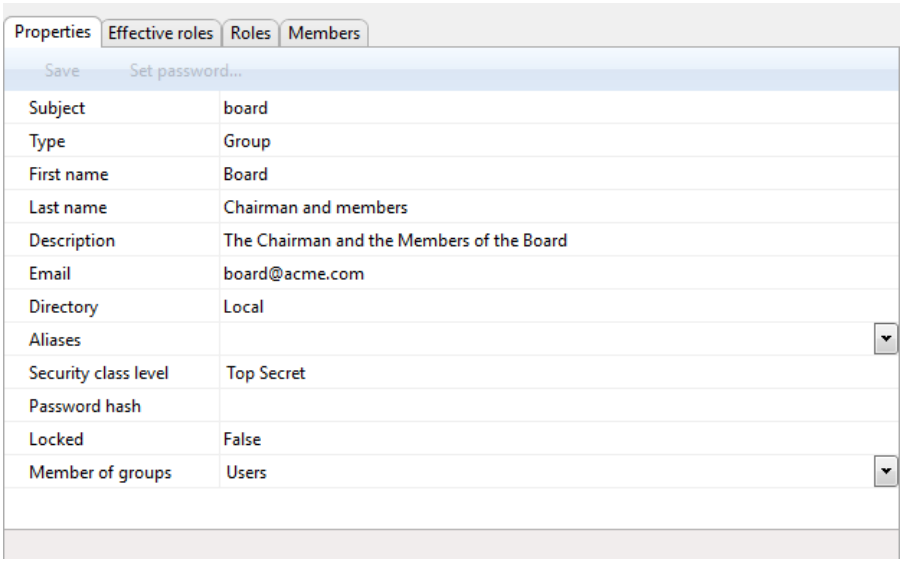


Image 346: User group properties

The fields listed above are available for users as well as for user groups. The additional value settings are displayed for the users:

- »Authentication«: enables the verification of user authentication when logging on to the archive server. Users with appropriate rights can choose between the following options:
  - »External«: enables external users to login via an external directory.
  - »Local«: enables local users to login to the archive server using a username and password.

2018 © Imaging Systems, Inc., All rights reserved.

- »Local over HTTP«: enables users to login to the archive configuration via the HTTP protocol.
- »Pre-shared key«: enables users to login to the archive server with a pre-shared key. During the authentication process the user's identity is established based on a confidential key shared between the client and the server.
- »Advanced«: enables the use of more complicated (HMAC) methods for setting up server sessions, which includes mandatory and non-mandatory client metadata.

Value set to »False« denotes that this type of user authentication is not available.
On the contrary, by changing the value to »True« this type of user authentication is enabled.

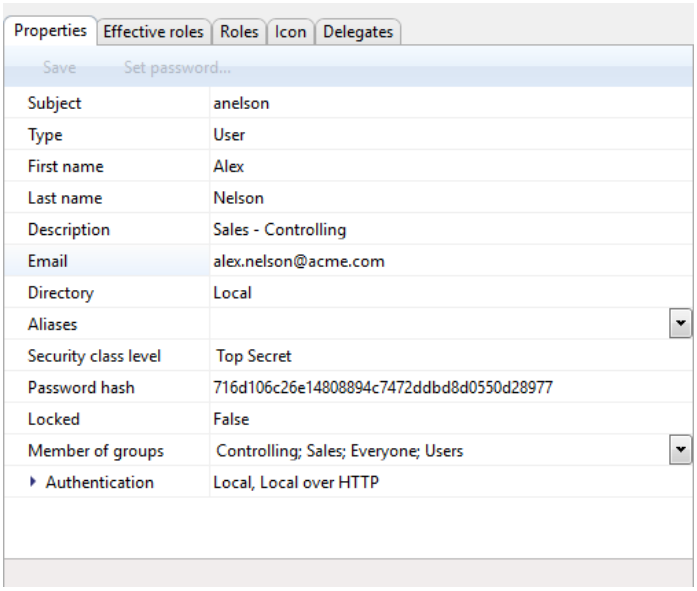


Image 347: User properties

»Effective roles« tab

By clicking the »Effective roles« tab, the effective roles for the individual users or user groups appear in the lower right view of the Windows Explorer. The displayed roles are informative; therefore, they cannot be changed. They include the current roles, which can be replaced with explicit roles in the »Roles« tab by the user with appropriate access rights.

2018 © Imaging Systems, Inc., All rights reserved.

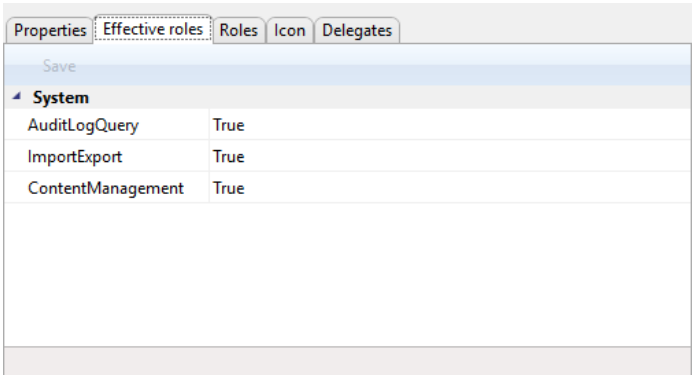


Image 348: Effective roles of the user

»Roles« tab

By clicking the »Roles« tab in the lower right view of the Windows Explorer, the user with appropriate access rights can define the following system roles for the users or user groups:

- AuditLogQuery
- ImportExport
- ContentManagement
- Reports
- DraftManagement.

The user can set effective roles for server configuration in the »Configuration« section.
They define rights for accessing and changing entries in the individual configuration folders.

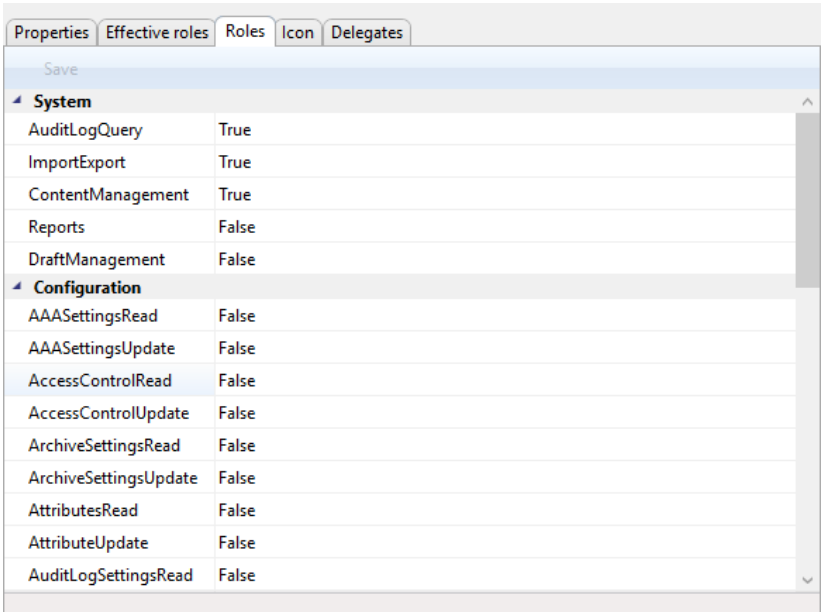


Image 349: Explicit roles for the user

2018 © Imaging Systems, Inc., All rights reserved.

Users can access and change the following configuration folders in the »Configuration« folder:

- Authentication
- Access Control
- Archive
- Attributes
- Codelists
- Content
- Counters
- Directory
- Legacy archival
- Long Term Archive and Notary Services - LTANS
- Profiles
- Retention
- Security
- Templates
- Volumes.

The user with appropriate access rights can set the role or right of reading and changing values in the configuration folder. The rights are set by selecting »True« or »False« for each right.

Warning: After changing the roles, the current user roles are valid for the entire duration of his session or until the user logs into the archive again.

»Icon« tab

By clicking the »Icon« tab in the bottom right view of Windows Explorer, the user with appropriate rights can add an icon which represents a user or group of users.
In Edit mode, the user selects the appropriate file in the file system in a graphic format (.bmp, .jpg, .gif, .png, etc.) and saves it on the server.

The user changes the icon with the command »Change« or removes it with the command »Remove«.

2018 © Imaging Systems, Inc., All rights reserved.

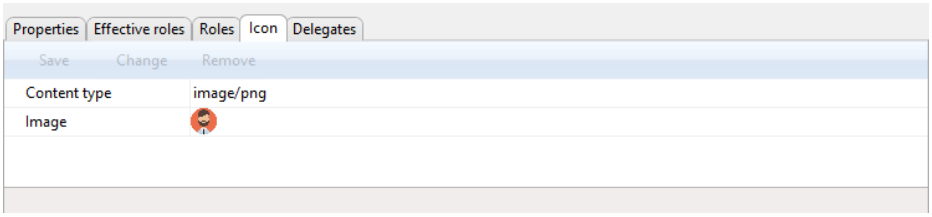


Image 350: Displaying the icon of a user or group

»Delegates« tab

By clicking the »Delegates« tab in the bottom right view of Windows Explorer, the user with appropriate rights can add and view registered users. In the authentication process, they can present themselves as persons authorized for other users and execute operations on their behalf.

A user can add delegates with the »Add« command or remove them with the »Remove« command.

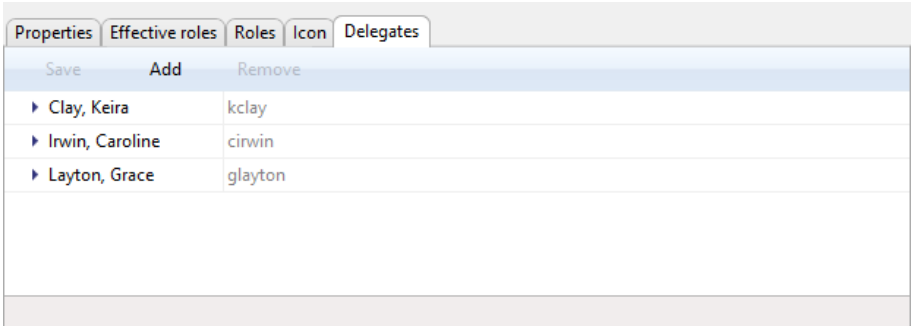


Image 351: Displaying delegates for executing operations

8.4.10 »Legacy archival« folder

The »Legacy archival« folder contains the following folders: »Content type aliases«, »Object containers« and »Storage profiles«.

2018 © Imaging Systems, Inc., All rights reserved.

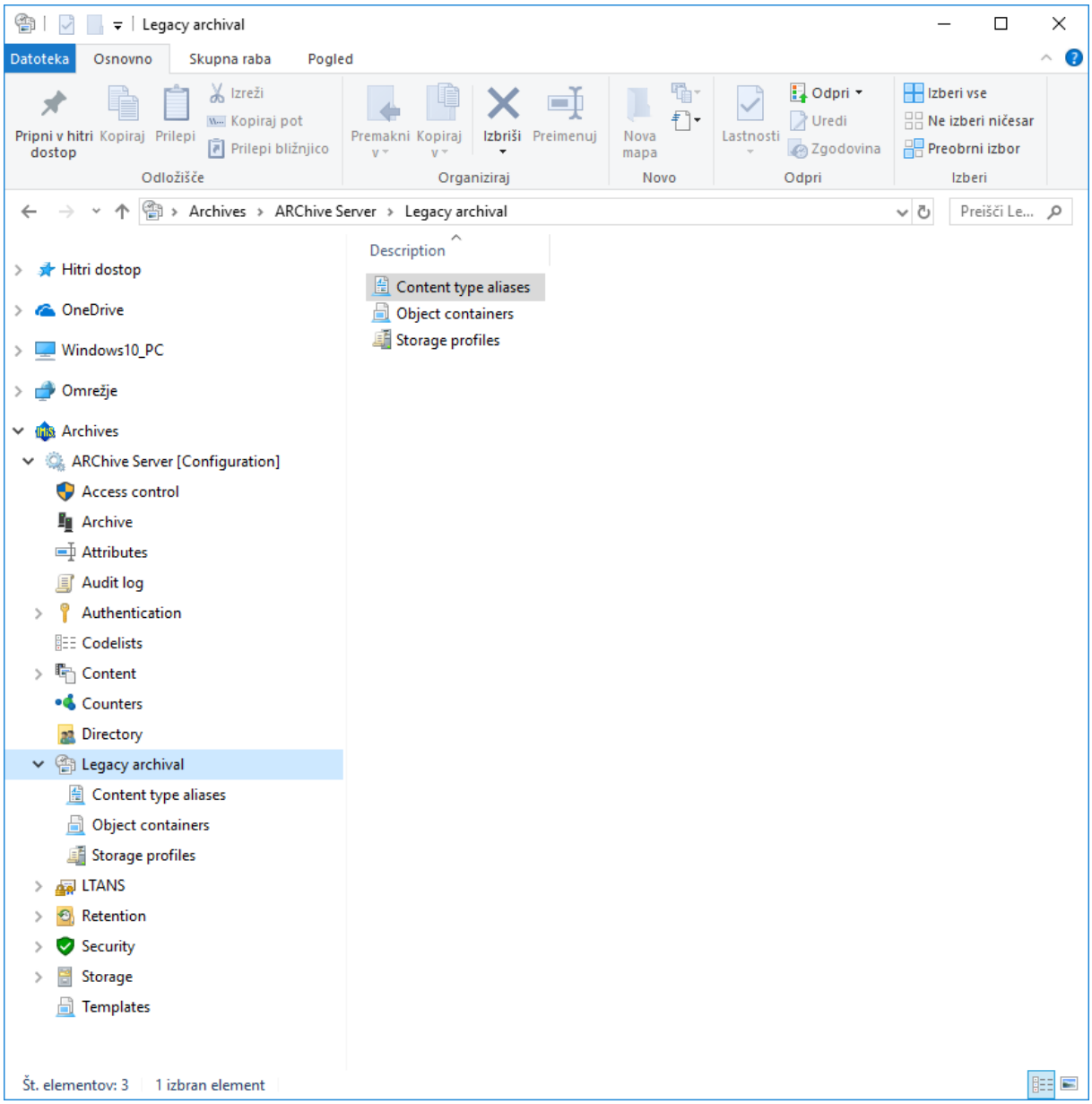


Image 352: List of contained folders in the »Legacy archival« configuration folder

8.4.10.1 »Content type aliases« folder

The »Content type aliases« folder: contains aliases settings for standard content types, which are used for accessing the same content via the legacy archival interface on the IMiS®/ARChive Server. Legacy archival protocol (Legacy API) has a limited size of the content type name (63 characters); it is not possible to exchange content over this character limit (i.e. MS OfficeOpen formats). For more information see chapter »Content types« folder.

2018 © Imaging Systems, Inc., All rights reserved.

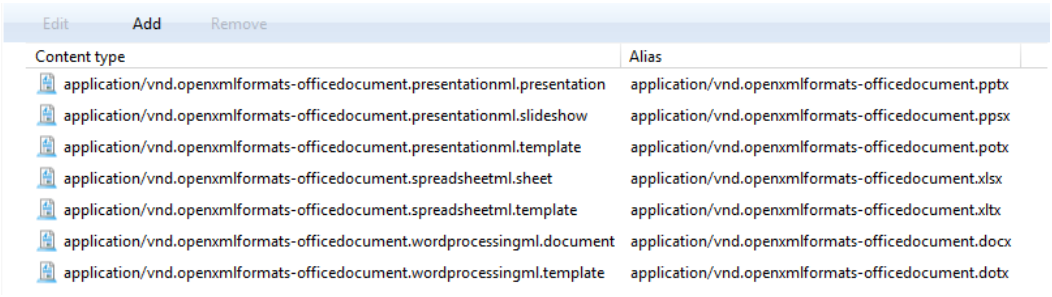


Image 353: List of content types in the »Content type aliases« configuration folder

»Properties« tab

By clicking the content type, the following settings are displayed in the »Properties« tab in the right pane of Windows Explorer:

- »Content type«: specifies the standard content type prescribed by IANA (Internet Assigned Numbers Authority).
- »Alias«: specifies an alias for a standard content type when accessing the same content via a Legacy API.

8.4.10.2 »Object containers« folder

The »Object containers« folder contains settings for storing files from clients for legacy archival on the IMiS®/ARChive Server.

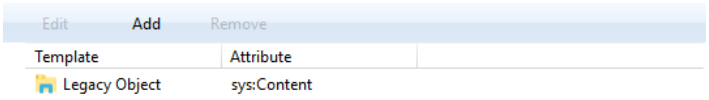


Image 354: List of templates in the »Object containers« configuration folder

»Properties« tab

By clicking the template in the list, the following settings are displayed in the »Properties« tab in the right pane of Windows Explorer:

- »Template«: specifies the template for entity (document) creation that contains »File« type attributes.
- »Attribute«: specifies a »File« type attribute« where the file is stored via the legacy archival client.

2018 © Imaging Systems, Inc., All rights reserved.

8.4.10.3 »Storage profiles« folder

The »Storage profiles« folder contains profile settings for storing content on the IMiS®/ARChive Server via legacy archival clients.

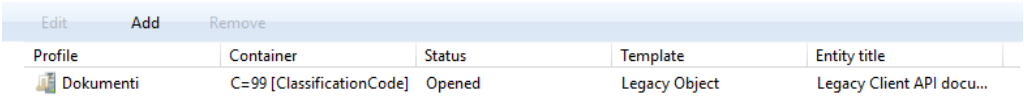


Image 355: List of storage profiles in the »Storage profiles« configuration folder

»Properties« tab

By clicking the storing profile in the list, the following settings are displayed in the »Properties« tab in the right pane of Windows Explorer:

- »Profile«: specifies a profile for storing content via legacy archival clients.
- »Container«: specifies an entity (class, folder) under which content is stored via a legacy archival client. Users with appropriate rights can view and/or change the following settings:
  - »Type«: specifies the type of the entity identifier (internal, external or classification code).
  - »Value«: specifies the value of the entity identifier.
    Set value denotes that the content of the legacy archival clients will be stored under this entity.
- »Template«: specifies the type of entity template to be used when storing content of the legacy archival clients.
- »Status«: specifies the default entity status after storing the content of the legacy archival clients. Status »Opened« means that the entity remains open after storing, while status »Closed« means the entity closes after storing.
- »Title«: specifies the default entity title when storing individual content of the legacy archival clients.
- »Description«: specifies the default entity description when storing individual content of the legacy archival clients.
- »Object description«: specifies the default object description when storing individual content (file) of the legacy archival clients.

2018 © Imaging Systems, Inc., All rights reserved.

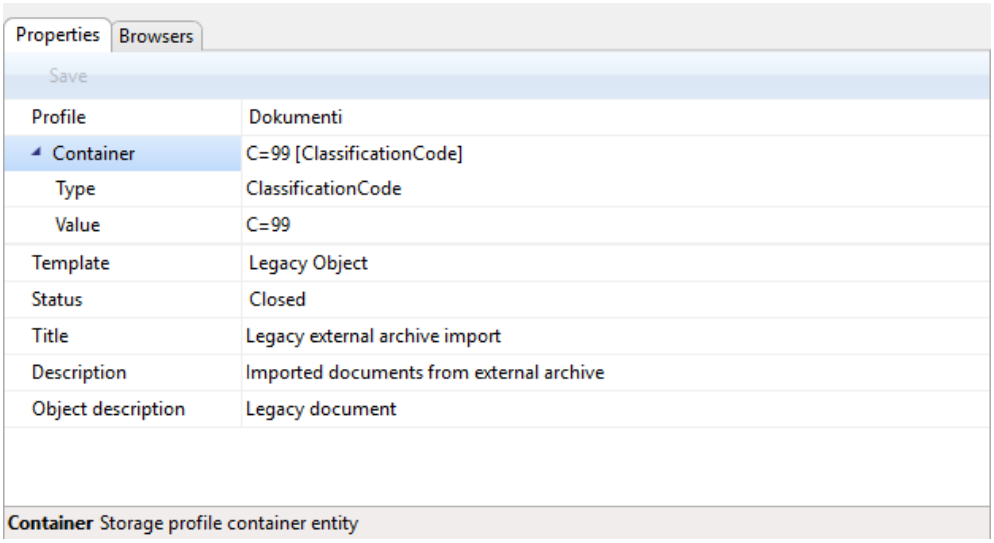


Image 356: Displaying storage profile properties

»Browsers« tabs

By clicking the individual records in the list, the following settings, described in chapter »Directory« folder, are displayed in the »Browsers« tab in the bottom right pane of Windows Explorer. Users with appropriate rights can add or remove browsers or view settings (read-only).

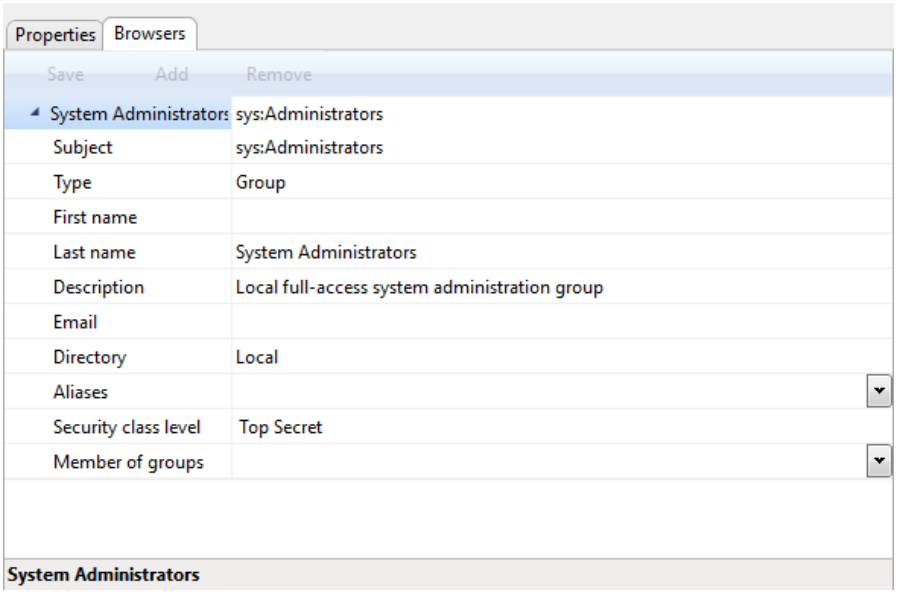


Image 357: Displaying browsers for accessing the storage profile

8.4.11 »LTANS« folder

LTANS is used for assuring the authenticity of the stored material via the creation and long-term maintenance of exhibits that assure the stored material remained unchanged.

The »LTANS« (Long Term Archive and Notary Services) folder contains the following folders: »Settings«, »Timestamp chaining rules«, »Timestamp providers« and »Timestamping rules«.

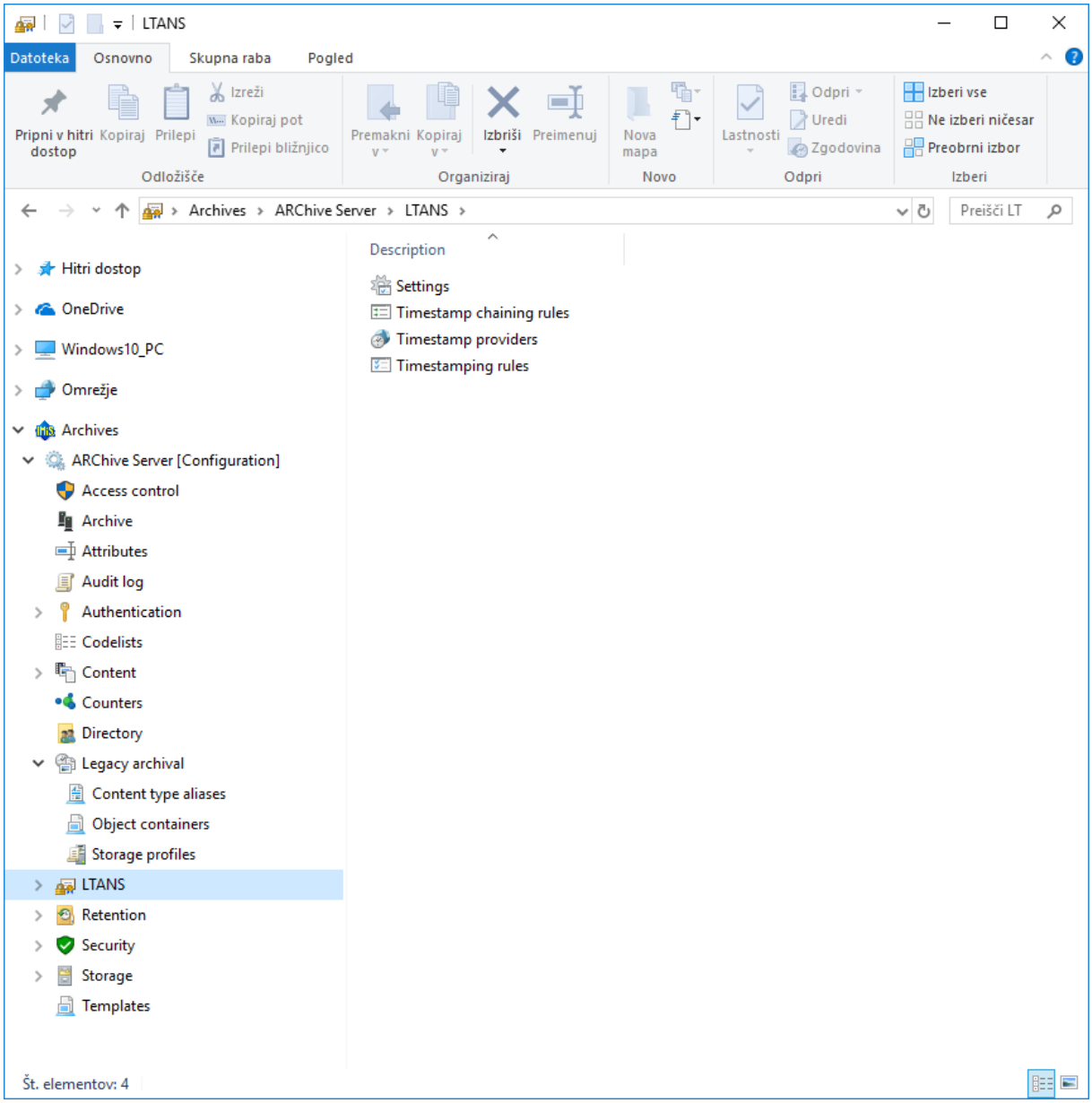


Image 358: List of contained »LTANS« configuration folders

8.4.11.1 »Settings« folder

The »Settings« folder contains LTANS settings.

»Properties« tab

By clicking the »Settings« folder, the following settings are displayed in the »Properties« tab in the right pane of Windows Explorer:

- »Enabled«: value set to »True« denotes that assuring the authenticity of the stored material is enabled. On the contrary, by changing the value to »False« users with appropriate rights disable the assuring of the authenticity of the stored material.
- »Max batch size«: specifies the maximum number of archival information packages (AIP) that are timestamped with a single timestamp.
  Value can't be higher than 1.000.000 or lower than the minimum batch size.
- »Min batch size«: specifies the minimum number of archival information packages (AIP) that are timestamped with a single timestamp.
  Value can't be lower than 1 or higher than the maximum batch size.
- »Timestamping schedule«: specifies the schedule for the execution of timestamping.
  The default value is 0 0 * * * *. For a description of the settings see https://linux.die.net/man/5/crontab.
- »Timestamp chaining schedule«: specifies the schedule for the execution of timestamping of the digital certificate chains. The set value on the server is 0 0 3 * * *.
  For a description of the settings see also https://www.freebsd.org/cgi/man.cgi?crontab(5).

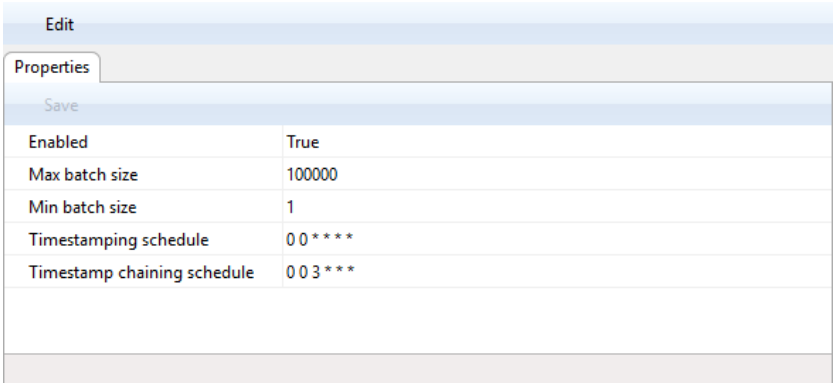


Image 359: Displaying LTANS settings

8.4.11.2 »Timestamping chaining rules« folder

The »Timestamping chaining rules« folder contains the settings for the timestamping chaining rules.

»Properties« tab

- »Identifier«: specifies the unique timestamping chaining rules identifier that is created after the rules are saved.
- »Provider«: specifies the data on the timestamping provider.
- »Digest«: value specifies the digest algorithm used in the chain. Users with appropriate rights can choose between the following options:
  MD5, SHA1, SHA224, SHA256, SHA384 and SHA512.
- »Expiration«: specifies a timeframe in which the digital certificate that performed the timestamping must still be valid in order to extend the timestamp.

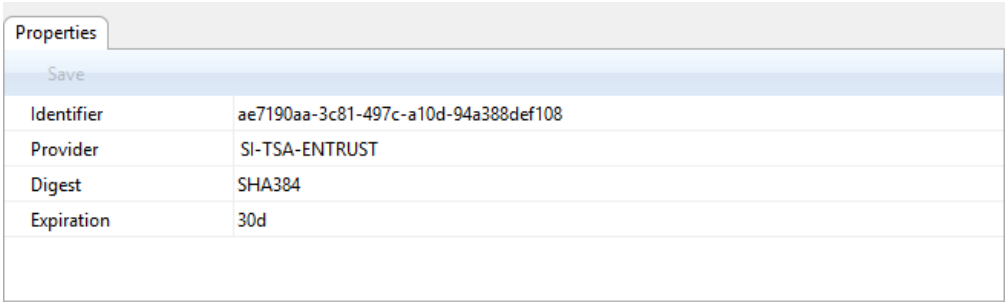


Image 360: Displaying the properties of timestamping chaining rules

8.4.11.3 »Timestamp providers« folder

The »Timestamp providers« folder contains the settings for timestamp providers.

»Properties« tab

By clicking the timestamp provider in the list, the following settings are displayed in the »Properties« tab in the bottom right pane of Windows Explorer:

- »Identifier«: specifies a unique timestamp provider identifier that is created after saving the provider.

2018 © Imaging Systems, Inc., All rights reserved.

- »Provider«: specifies data on the name and type of the timestamp provider. Users with appropriate rights can view and/or change the following settings:
  - »Name«: name of the timestamp provider.
  - »Type«: type of the timestamp provider (i.e. Plugin).
  - »Driver«: timestamp provider driver.
  - »Arguments«: specifies configuration parameters of the timestamp provider driver.
- »Default«: value set to »True« denotes that the timestamp provider is set as the default provider. On the contrary, by changing the value to »False« users with appropriate rights denote that the provider is not set as the default provider.
- »Digest«: value specifies the digest algorithm.
  Users with appropriate rights can choose between the following values:
  MD5, SHA1, SHA224, SHA256, SHA384 and SHA512.

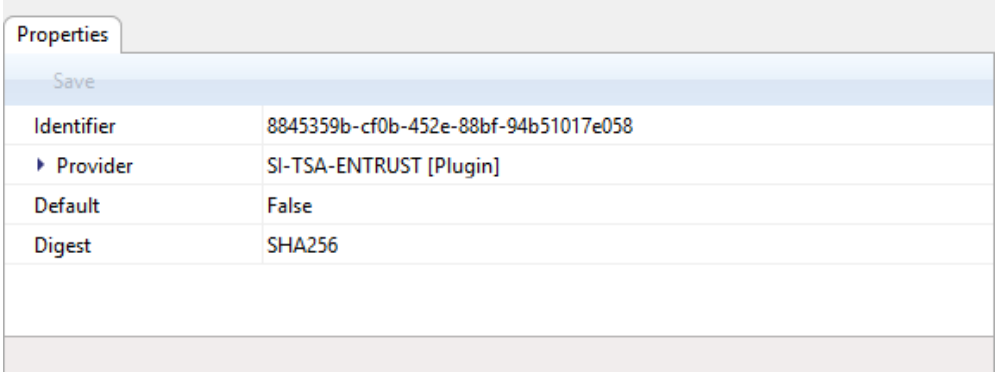


Image 361: Displaying properties of the timestamp provider

8.4.11.4 »Timestamp rules« folder

The »Timestamp rules« folder contains settings for the timestamp rules.

»Properties« tab

- »Identifier«: specifies a unique timestamp rules identifier.
- »Provider«: specifies data on the timestamp provider.
- »Type«: specifies the type of timestamp rules. Explicit rules are applied when deciding whether timestamping will be performed on the entity. During the timestamping procedure, implicit and explicit rules are additionally applied when expanding the selection of subordinated entities.

2018 © Imaging Systems, Inc., All rights reserved.

- »Scope«: specifies on which part of the classification tree the timestamp rule is applied. Users with appropriate rights can choose between the following options:
  - »Type«: specifies the type of the entity identifier (internal, external or classification code).
  - »Value«: specifies the value of the entity identifier.
    Set value denotes that the timestamp rule will apply to entities listed below the selected entity and its contained entities. If the value is not set, then there are no limitations and the rule apply for the entire archive.
- »Include children«: value denotes whether the timestamp rules also apply for contained entities. Value set to »True« denotes that they apply. By changing the value to »False« users with appropriate rights denote that timestamp rules do not apply for contained entities.
- »Template filter«: enables restricting entity selection according to the template for which timestamp rules apply.
- »Search expression«: enables restricting entity selection according to the expression for which timestamp rules apply.

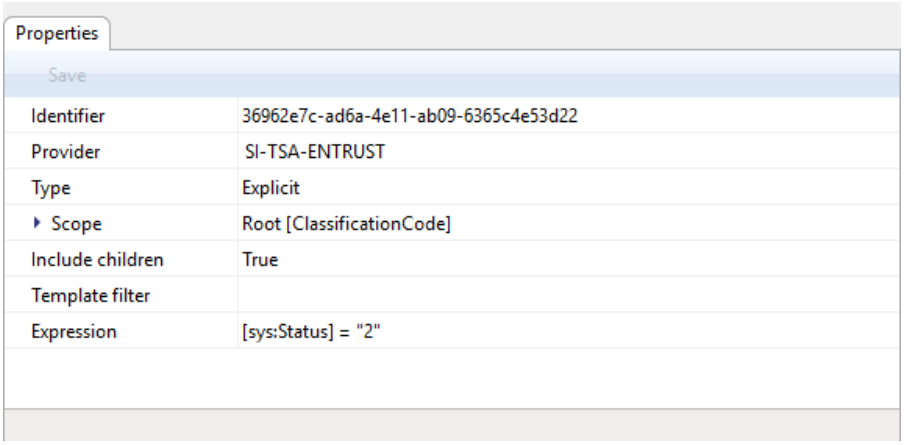


Image 362: Displaying timestamp rules properties

2018 © Imaging Systems, Inc., All rights reserved.

8.4.12 »Retention« folder

The »Retention« folder contains the »Retention policies« and the »Disposition holds« subfolders.

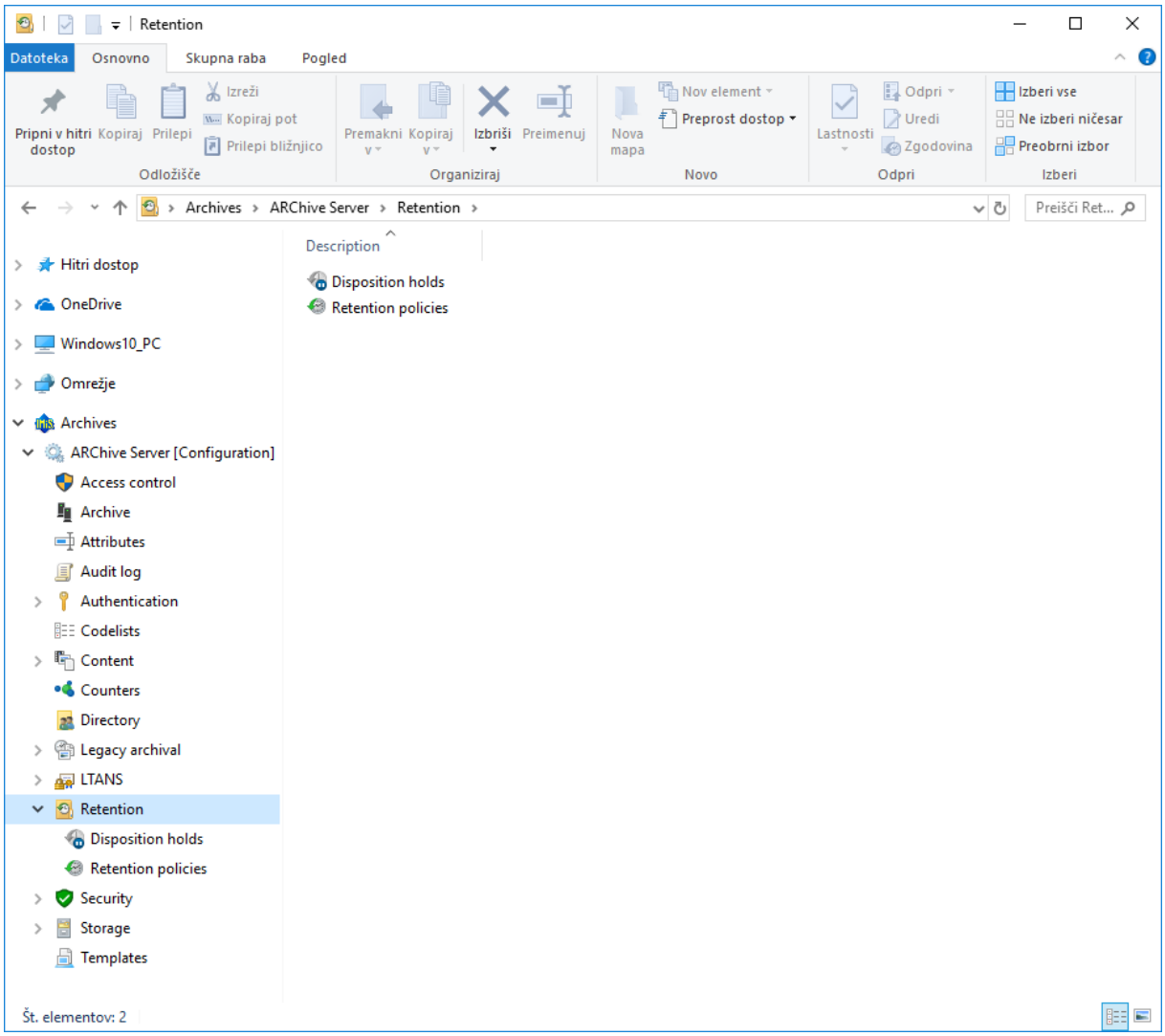


Image 363: A list of subfolders in the »Retention« configuration folder

8.4.12.1 »Disposition holds«

The »Disposition holds« folder contains a list of disposition holds.

By default, the disposition holds list shows the following information on retention policies in columns:

- »Name«: the unique name of disposition holds.
- »Description«: short description of disposition holds.
- »Reason«: the default reason for the existence of disposition holds to be implemented in the implementation phase of the review process.

2018 © Imaging Systems, Inc., All rights reserved.

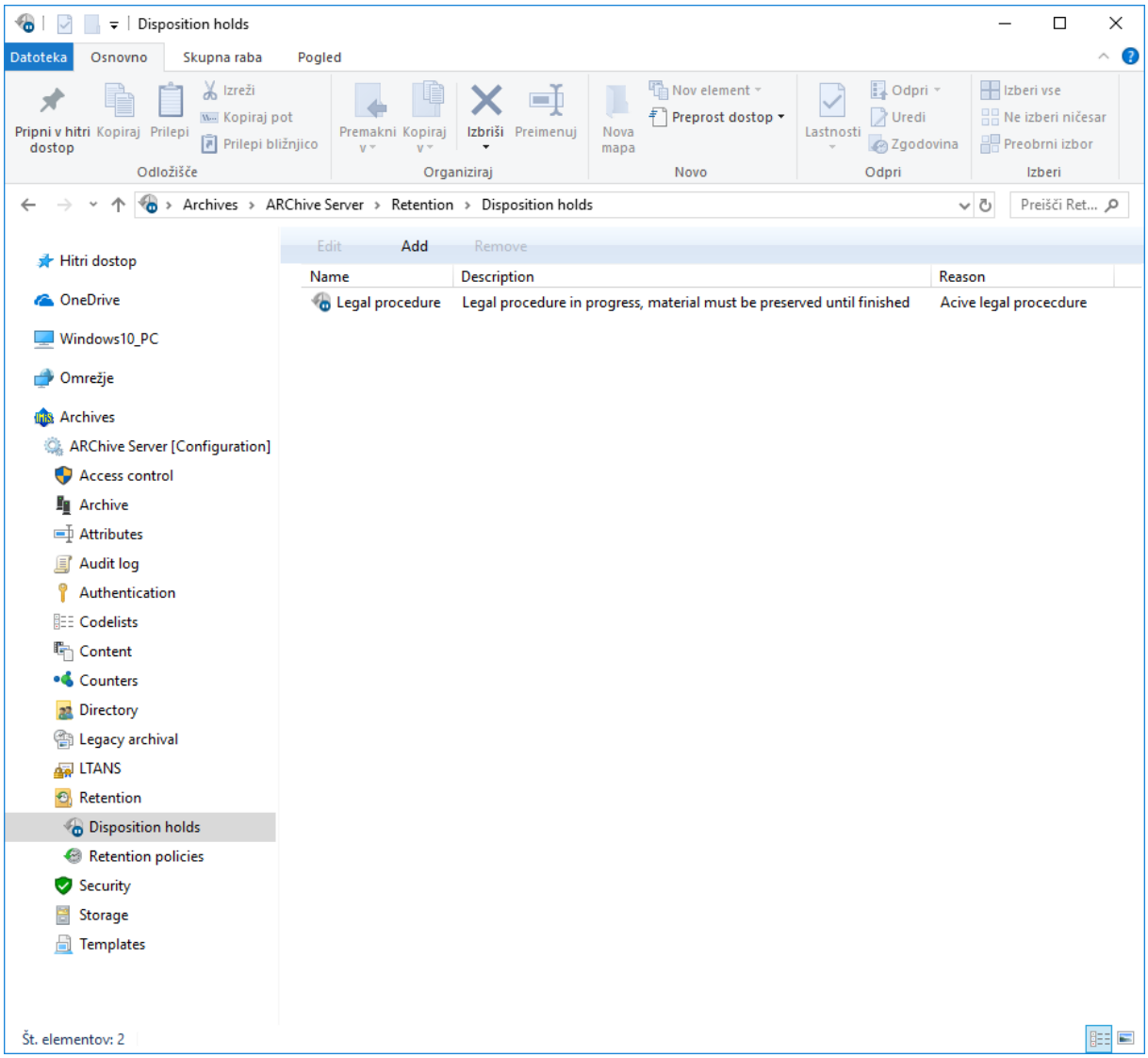


Image 364: List of disposition holds in the »Disposition holds« folder

»Properties« tab

By clicking on an individual disposition hold on the list, the following value settings appear in the bottom right view of Windows Explorer, under the »Properties« tab:

- »Identifier«: unique identifier of the disposition hold.
- »Name«: the unique name of the disposition hold. The field value must be entered for new entries before saving. The value can be modified after saving, but it must not be empty.
- »Description«: short description of the disposition hold.
- »Reason«: the default reason for the disposition hold in the implementation phase of the review process.

2018 © Imaging Systems, Inc., All rights reserved.

- »Author«: user (author) of the disposition hold.
- »Created«: the date and time when the disposition hold was created.

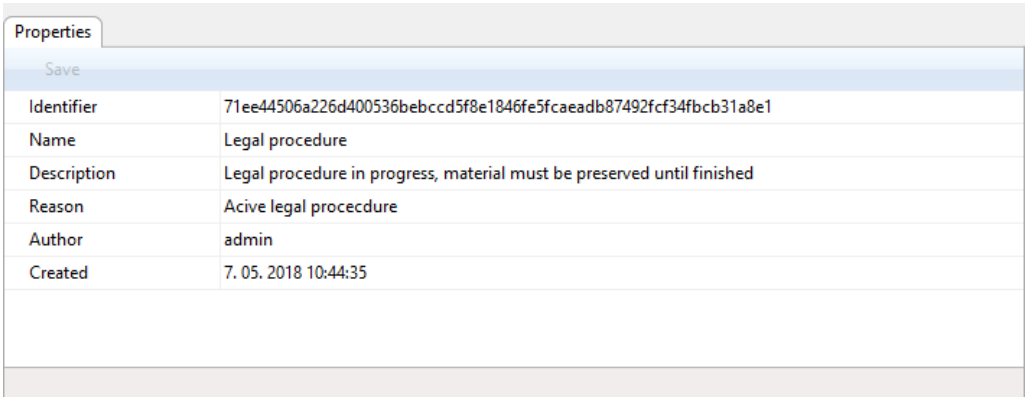


Image 365: Display of disposition hold mandates

8.4.12.2 »Retention policies«

The »Retention policies« subfolder contains a list of retention policies. By default, the retention policies list shows the following information on retention policies in columns:

- »Name«: the unique name of the retention policy.
- »Description«: short description of the retention policy.
- »Action«: the default action in the implementation phase of the review process.
- »Reason«: the reason for the existence of the retention policy which is used in the decision-making phase of the review process.

2018 © Imaging Systems, Inc., All rights reserved.

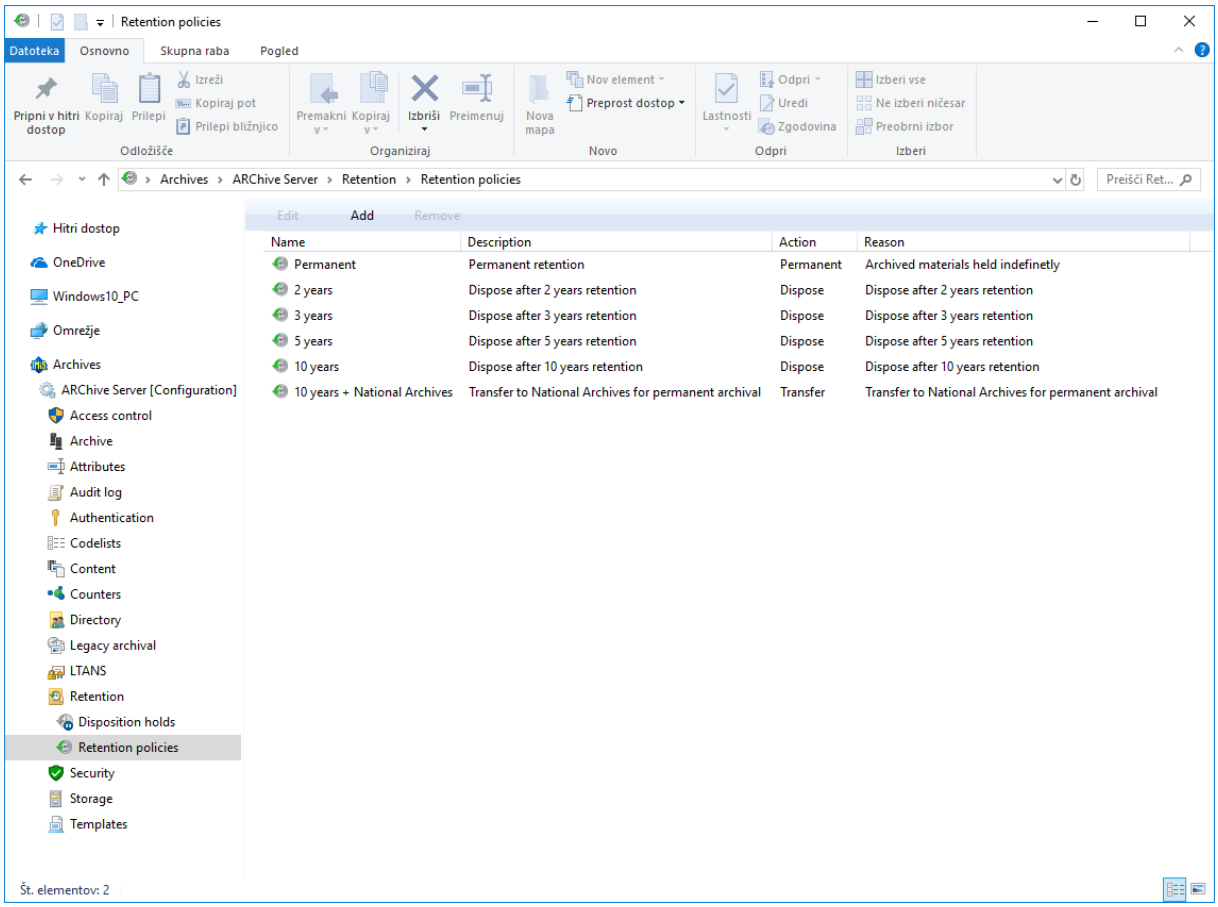


Image 366: List of retention policies in the »Retention policies« folder

»Properties« tab

By clicking on an individual retention policy on the list, the following value settings appear in the bottom right view of Windows Explorer, under the »Properties« tab:

- »Identifier«: unique identifier of the retention policy.
- »Name«: the unique name of the retention policy. The field value must be entered for new entries before saving. The value can be modified after saving, but it must not be empty.
- »Description«: short description of the retention policy.
- »Detailed description«: a detailed description of the retention policy.
- »Action«: the default action from the list of actions for entities which are available in the implementation phase of the review process.
- »Trigger«: a query which executes the search for entities in the implementation phase of the review process.
- »Reason«: the default reason for actions to be implemented in the implementation phase of the review process.

2018 © Imaging Systems, Inc., All rights reserved.

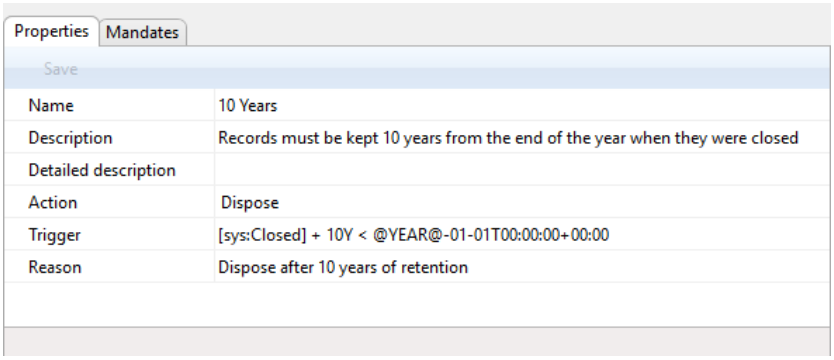


Image 367: Display of retention policy properties

»Mandates« tab

By clicking on an individual retention policy on the list, the contents (files) of mandates for an individual retention policy appear in the bottom right view of Windows Explorer, under the »Mandates« tab.

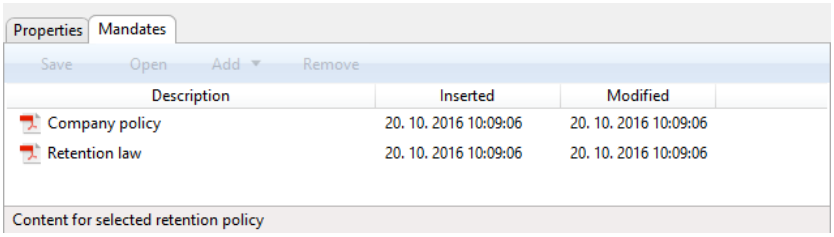


Image 368: Display of retention policy mandates

If the user wishes to open more mandates at once, he first selects the mandates and then selects the »Open« command in the bottom command bar. The mandates are opened successively.

The user can similarly delete the selected mandates by first selecting them and then selecting the »Remove« command in the bottom command bar.

In the bottom command bar, under the »Mandates« tab, the following commands are located:

- »Add«: allows you to add mandate content to the selected retention policy.
  The source can either be existing files in the file system or files scanned using the separate IMiS®/Scan application. The command is available when the selected retention policy is open in editing mode.
- »Save«: becomes active when the mandates for the selected retention policy are modified, if the policy is open in editing mode (when content is added or deleted).
  The »Save« command saves changes to the archive. Unsaved changes will be discarded.

2018 © Imaging Systems, Inc., All rights reserved.

- »Open«: opens the selected file in the application associated with the content type, as it was specified when the content was saved to the archive.
  The command is available when the selected retention policy is open in editing mode.

  Note: The selected content can be opened by a user even if it has not been saved yet.

- »Remove«: allows you to remove content from the selected retention policy.
  The command is available when the selected retention policy is open in editing mode.

8.4.13 »Security« folder

The »Security« folder contains the folders: Certificate Store, Certificates and Settings.

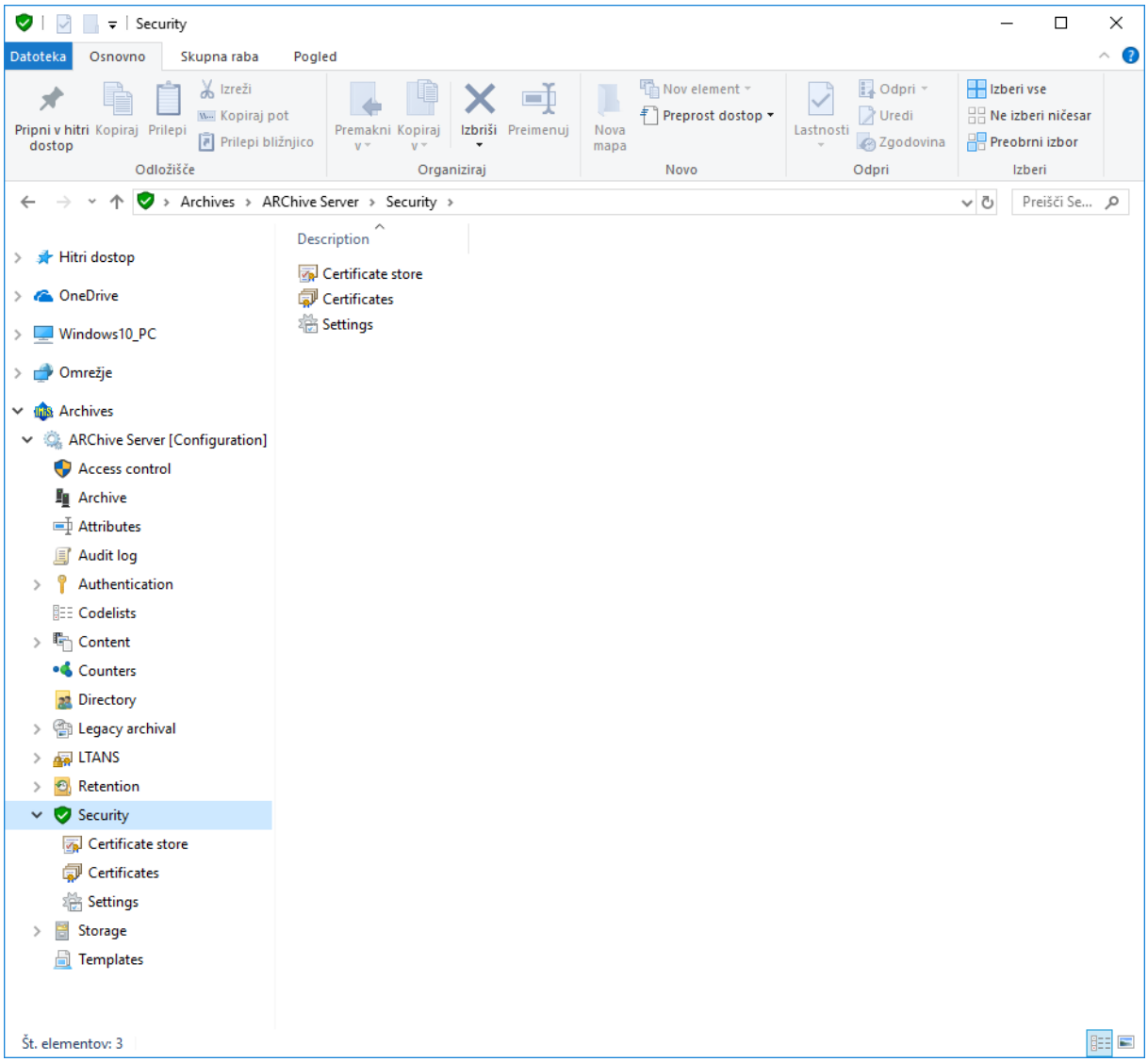


Image 369: List of contained folders in the »Security« configuration folder

8.4.13.1 »Certificate Store« folder

The »Certificate Store« folder contains the settings related to digital certificates and to the functionalities of obtaining revocation data.

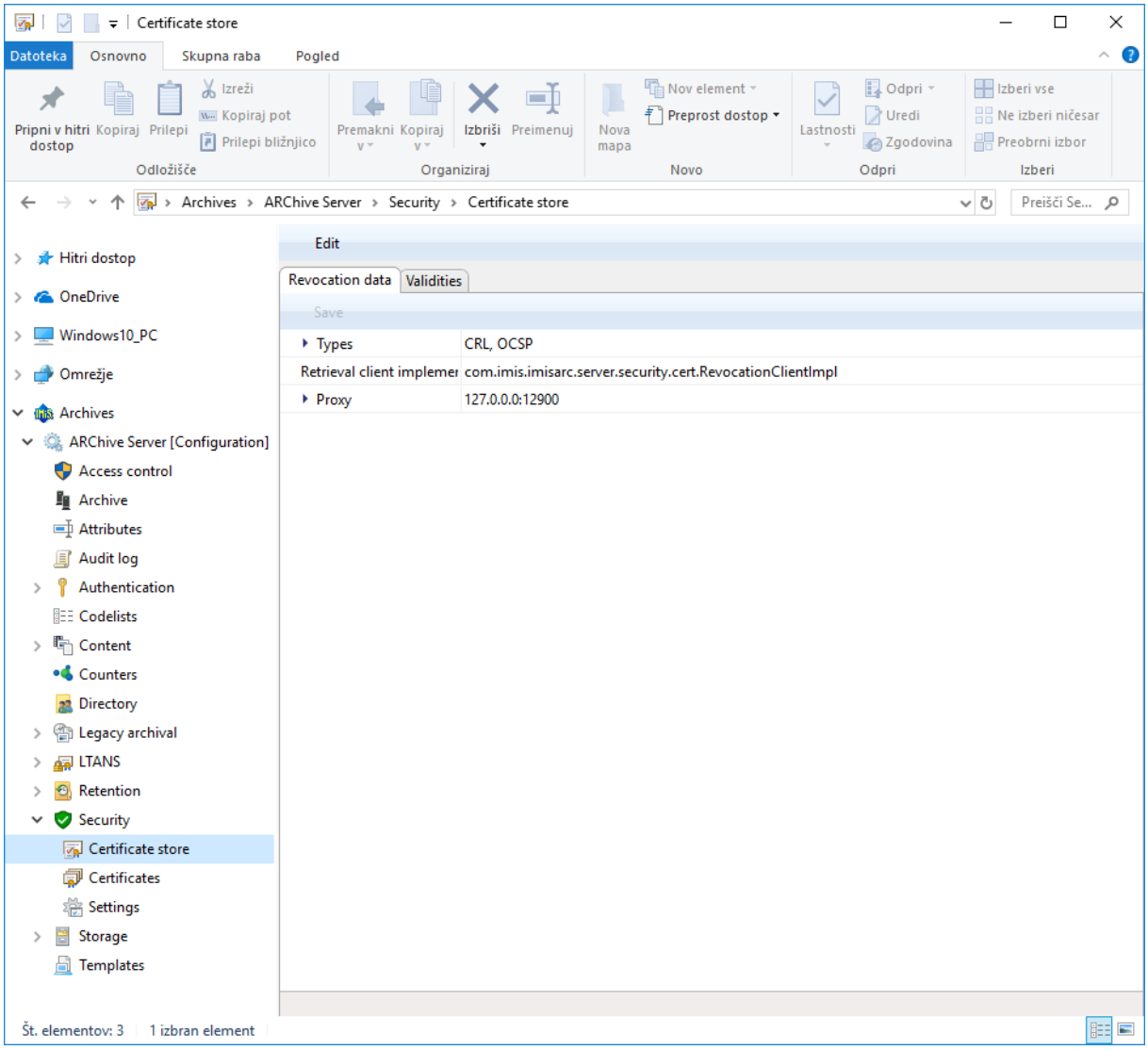


Image 370: Displaying information about revoked digital certificates in the »Certificate Store« folder

»Revocation data« tab

By clicking the »Revocation data« tab in the subfolder »Certificate Store« of the »Security« folder, the right view of Windows Explorer shows the following value settings:

- »Types«: defines the types of information about revoked digital certificates.
  A user with the appropriate rights can define or view the following settings:
  - »CRL«: defines whether a list of revoked digital certificates is enabled (True) or disabled (False);
  - »OCSP«: defines whether the internet protocol for checking the status of digital certificates is enabled (True) or disabled (False).
- »Retrieval client implementation«: defines the implementation of the client for information about revoked digital certificates.
- »Proxy«: contains proxy server data with information about revoked digital certificates.
  A user with the appropriate rights can define or view the following settings:
  - »Host«: defines the IP address of the proxy server with information about revoked digital certificates;
  - »Port«: defines the port for access to the proxy server with information about revoked digital certificates;
  - »Username«: defines the username for access to the proxy server with information about revoked digital certificates;
  - »Password«: defines the password for access to the proxy server with information about revoked digital certificates.

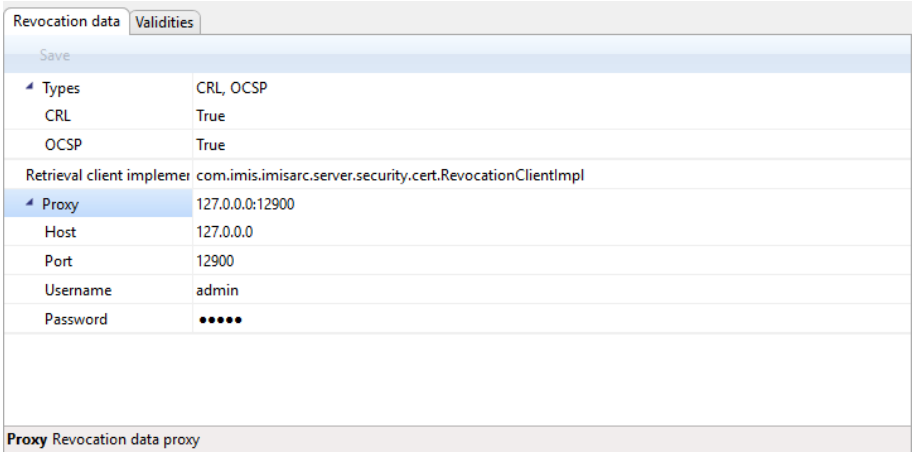


Image 371: Displaying information about revoked digital certificates

»Validities« tab

By clicking the »Validities« tab in the subfolder »Certificate Store« of the »Security« folder, the right view of Windows Explorer shows a list of validities of information about revoked digital certificates:

- »Validity name«: A user with the appropriate rights can define or view the following settings:
  - »URL«: defines the URL of the path to the server;
  - »Period«: defines the validity period for the information about revoked digital certificates.

8.4.13.2 »Certificates« folder

The »Certificates« folder contains a list of thrusted issuers of digital certificates.

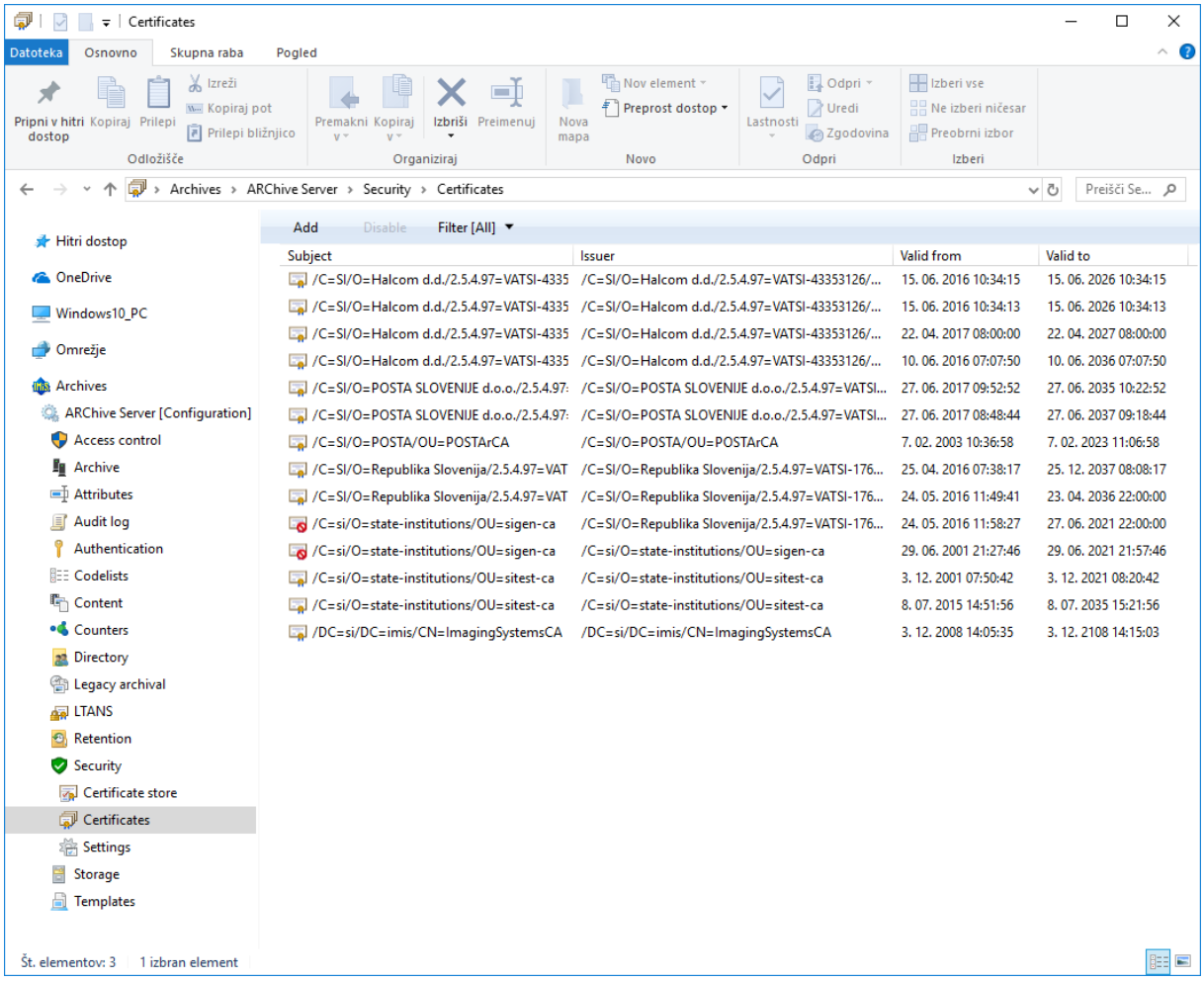


Image 372: Displaying the list of trusted issuers of digital certificates

To select the contained »Certificates« folder the following commands are available in the command bar:

- »Add«: enables adding digital certificates of trusted issuers.
- »Disabled«: disables the selected digital certificate of a trusted issuer of digital certificates.
- »Filter«: enables specification of content display.

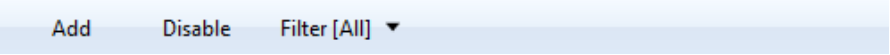


Image 373: Command bar in the contained »Certificates« configuration folder

You can choose between the following options:

- »All«: all digital certificates of trusted issuers are shown on the list.
- »Enabled«: only enabled digital certificates of trusted issuers are shown on the list.
- »Disabled«: only disabled digital certificates of trusted issuers are shown on the list.

Image 374: Selecting a filter in the »Certificates« configuration folder

»Properties« tab

By clicking on the individual digital certificate of a trusted issuer in the list, the following settings are displayed in the »Properties« tab in the bottom right pane of Windows Explorer:

- »Identifier«: unique identifier of a digital certificate.
- »Type«: type of digital certificate.
- »Serial«: serial number of the digital certificate.
- »Subject«: full (distinguished) name of the digital certificate.
- »Issuer«: full (distinguished) name of the issuer of the digital certificate according to the X.509 standard.
- »Valid From«: date and time of validity of the digital certificate.
- »Valid to«: date and time of the end of validity of the digital certificate.

2018 © Imaging Systems, Inc., All rights reserved.

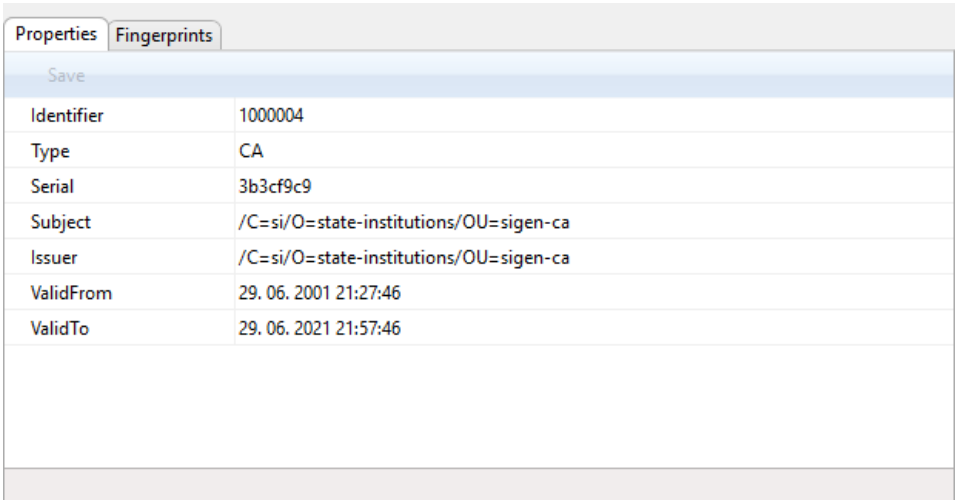


Image 375: Displaying the properties of the digital certificate

By clicking the »View«, a digital certificate of a trusted issuer is displayed to the user in a separate window.

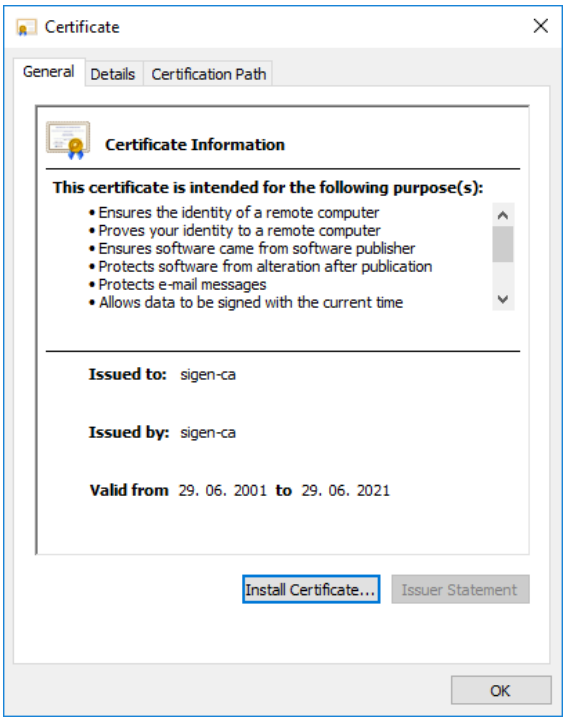


Image 376: Information on digital certificate of a trusted issuer

2018 © Imaging Systems, Inc., All rights reserved.

»Fingerprints« tab

By clicking the »Fingerprints« tab, fingerprints of a digital certificate, calculated on the basis of different algorithms (such as SHA1, SHA256) are displayed.

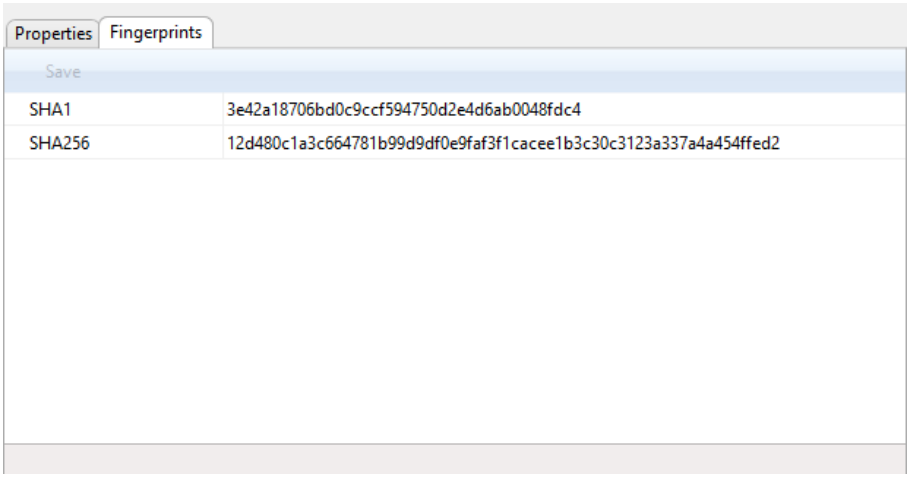


Image 377: Displaying the fingerprints of a digital certificate

8.4.13.3 »Settings« folder

The »Settings« folder contains security settings.

»Properties« tab

By clicking »Settings«, the right view of Windows Explorer shows the following value settings under the »Properties« tab:

- »Auto delete entity references«: defines whether entity references are not deleted automatically (False), or are deleted (True).
- »Version series locking«: defines whether the process of checking in a working copy (Check in) locks the version of a specific entity (True), or not (False).

»Unrestricted public attributes« tab

By clicking the »Unrestricted public attributes« folder in the right view of Windows Explorer in Edit mode, the user with the appropriate rights begins by selecting an attribute from the list with the »Add« command.

2018 © Imaging Systems, Inc., All rights reserved.

By clicking an attribute on the list, the following value settings appear:

- »Name«: contains the name of the attribute. If it is a system attribute, the type of attribute (sys:, eml:, prm:, trf:) is mentioned first, which is followed by a short description. For new entries the value for the attribute name must be specified before saving; it cannot be changed after saving.
- »Type«: defines the type of attribute (for example DirectoryEntity, Boolean, Int32, Double, DateTime, String, Decimal, Binary, or File). For new entries the value for the type of attribute must be selected before saving, as it cannot be changed after saving.
- »Description«: contains a short description of the attribute.
- »Label«: the attribute value represents the label of the version in the series. This value is created automatically on checking in the document draft and represents the next version in the series.
- »ValidationExpression«: defines the value which represents a Regular expression, which is used to check new or modified attribute values. More on syntax and rules: http://en.wikipedia.org/wiki/Regular_expression.
- »Searchable«: defines whether it can be searched by value. The setting »True« denotes that searching by the attribute value is possible using search functions.
- »Unique«: value set to »True« denotes that the attribute value is unique throughout the archive. The user with appropriate rights sets it if he does not want an attribute value, which is already specified by another entity, to be entered.
- »PickList«: value set to »True« denotes that the values are pre-set and it is therefore not possible to enter the values manually outside of the list of allowed values.

2018 © Imaging Systems, Inc., All rights reserved.

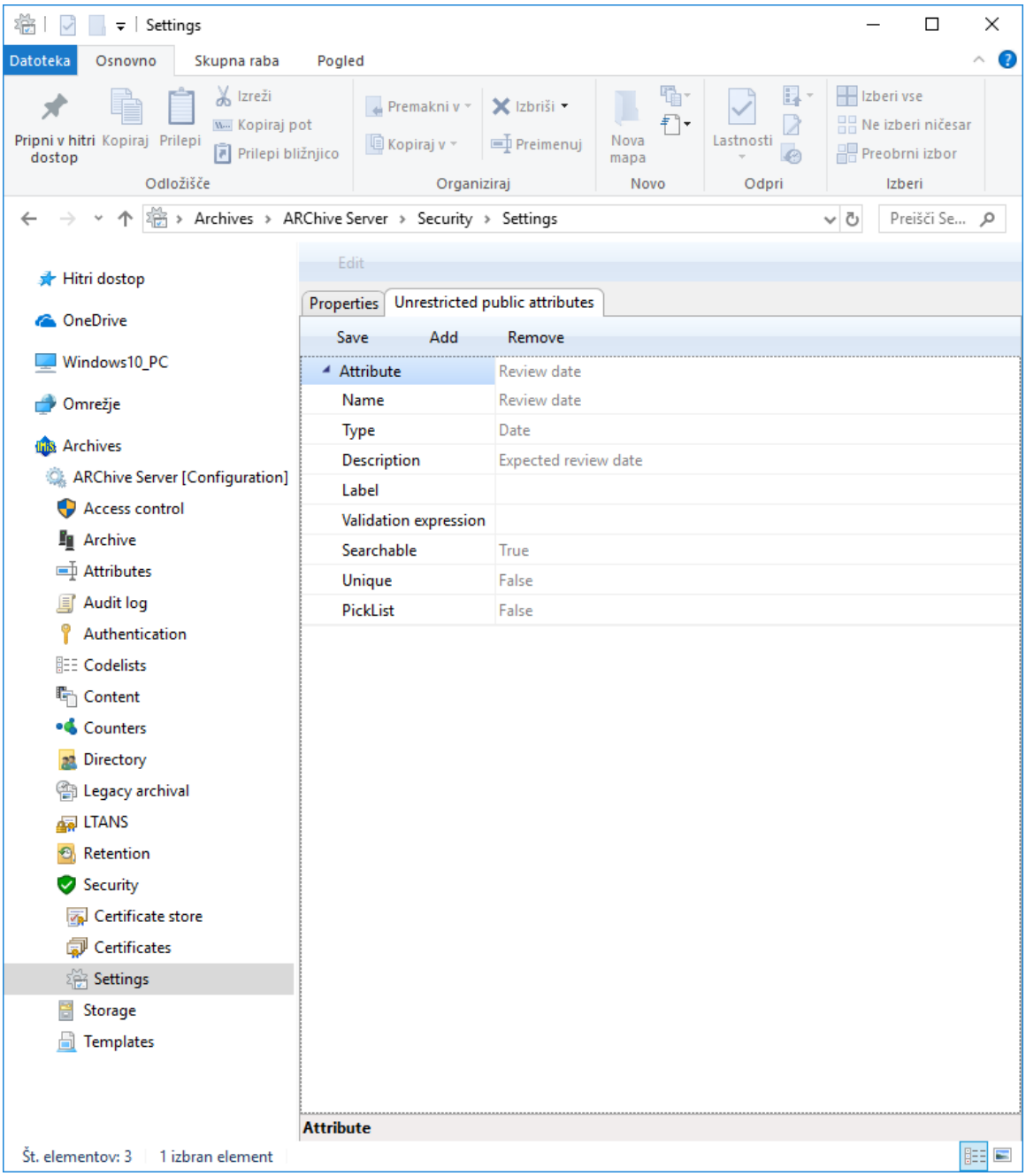


Image 378: Displaying security settings

In the bottom command bar under »Unrestricted public attributes« tab are the following commands:

- »Add«: enables adding attributes to the attribute list with unrestricted access.
- »Remove«: enables removing attributes from the attribute list with unrestricted access.
- »Save«: saves changes of the attribute list with unrestricted access.

2018 © Imaging Systems, Inc., All rights reserved.

Warning: By adding attributes to the »Unrestricted public attributes« tab, users with appropriate rights influence the display of entities in the material classification plan. If the list is empty, meaning it does not contain attributes, the user does not see the entities if he does not have the right to read entities.
On the contrary, if the list contains at least one attribute, the user, regardless if he has the right to read entities, sees the entity (without its name and its key properties), access rights, retention periods and its system properties.

8.4.14 »Storage« folder

The »Storage« folder contains the »Profiles« and »Volumes« subfolders.

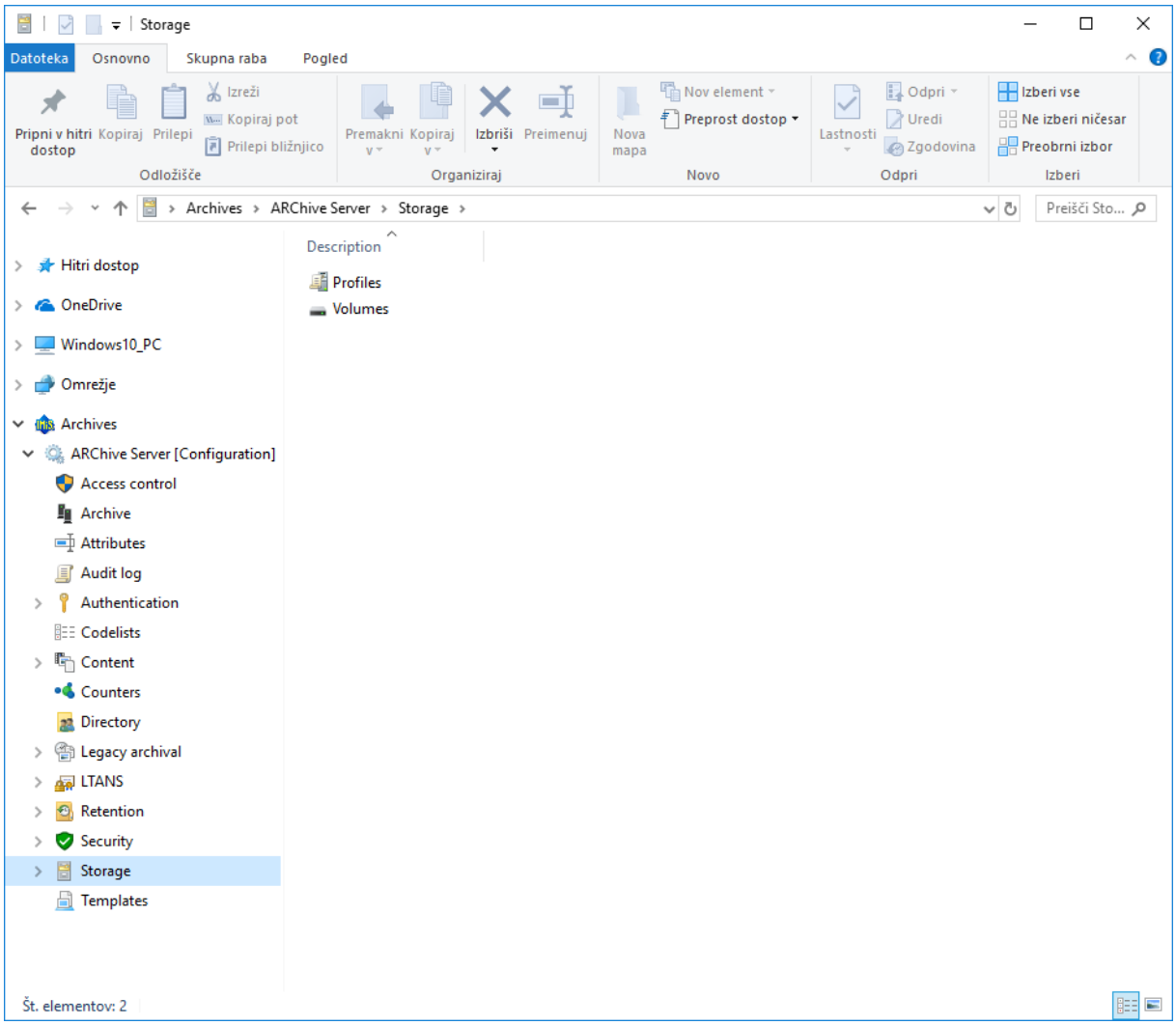


Image 379: A list of subfolders in the »Server« configuration folder

8.4.14.1 »Profiles« subfolder

The »Profiles« subfolder contains a list of profiles. The following profile information is listed in the columns:

- »Name«: contains the unique profile name.
- »Description«: contains a short description of the profile.
- »Object count«: shows the number of archived objects in the individual profiles.
- »Used [bytes]«: shows the size of used space and the percentage of used space for the individual profiles in kilobytes (KB).
- »Size [bytes]«: shows the size of free space for the individual profiles in kilobytes (KB).

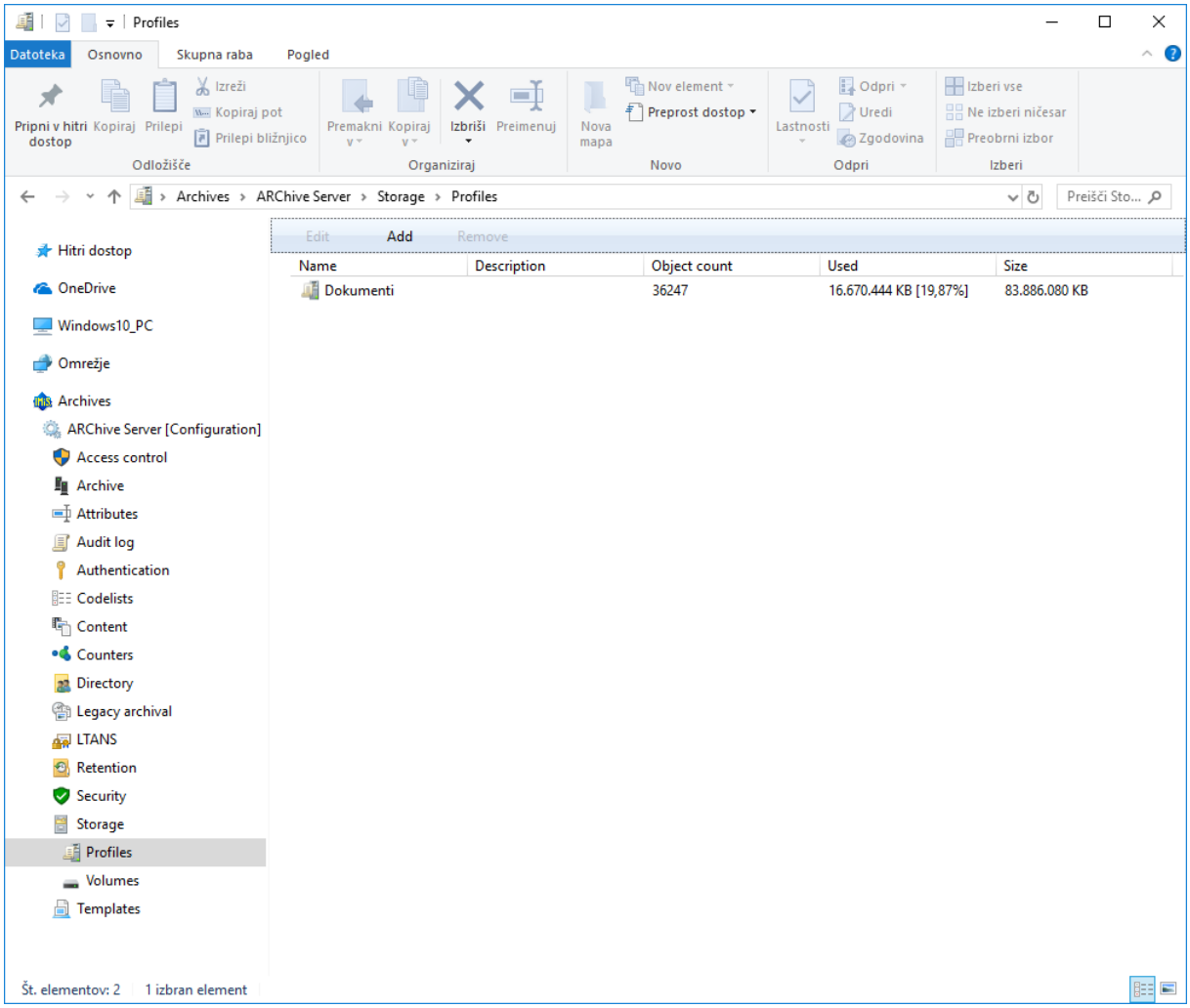


Image 380: Attribute list in the »Profiles« folder

By selecting the contained »Profiles« folder, the following commands are available:

- »Edit«: enables editing the profile's attribute values.
- »Add«: enables adding profiles.
- »Remove«: enables removing profiles.

»Properties« tab

By clicking the individual profile on the list, the user with appropriate access rights can see the following profile properties in the »Properties« tab in the lower right view of the Windows Explorer:

- »Name«: represents the unique profile name. Specifying the field value is mandatory for new entries. It cannot be changed for the existing entries.
- »Description«: represents a short description of the profile.
- »Object count«: shows the number of archived objects in the profiles.
- »Used [bytes]«: shows the size of used space for the profile in bytes.
- »Size [bytes]«: shows the size of free space for the profile in bytes.
- »Read only«: if the selected value is »True«, new objects cannot be created into the profile and the existing objects can only be read. The user with appropriate access rights can select this value to prevent changes of the profile content.
- »Write once, read many«: value set to »False« denotes content can be written and read many times. On the contrary, value set to »True« denotes content can be read many times, but can only be written once.
- »Stop adding objects«: value set to »True« denotes it is not possible to add content to the profile. On the contrary, value set to »False« denotes it is possible to add content.

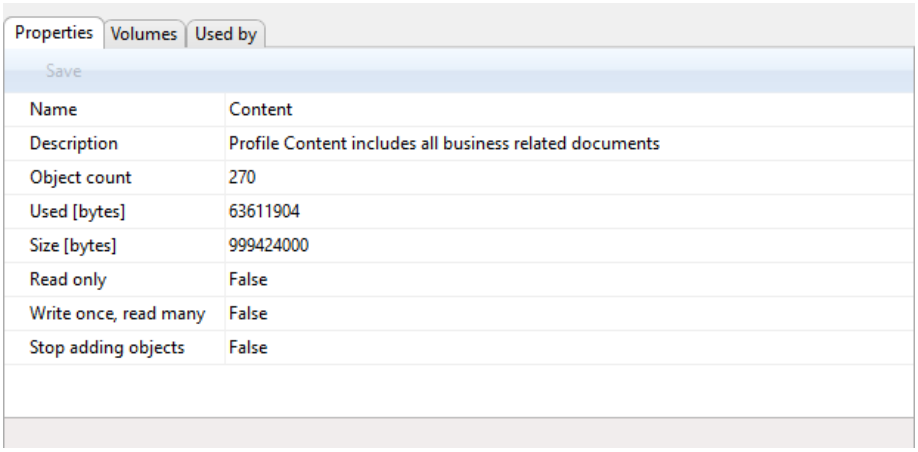


Image 381: Profile properties

2018 © Imaging Systems, Inc., All rights reserved.

»Volumes« tab

In the »Volumes« tab the user with appropriate access rights can view the attribute values, which are tied to the profile in the lower right view of the Windows Explorer; however, he cannot change the values. The »Volumes« tab content is the same as the content of the »Properties« tab in the »Volumes« configuration subfolder.

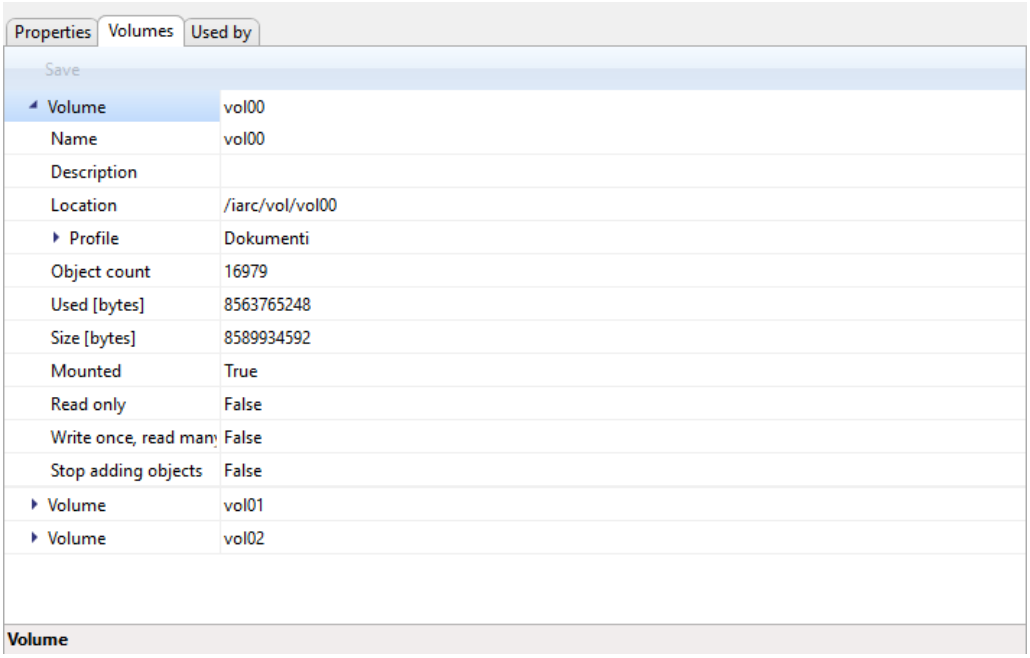


Image 382: Volumes, which are tied to the profile

»Use under« tab

In the »Used by« tab the user with appropriate access rights can set in the lower right view of the Windows Explorer under which class the selected profile is used. If the value is not set, the profile is used under the root class.

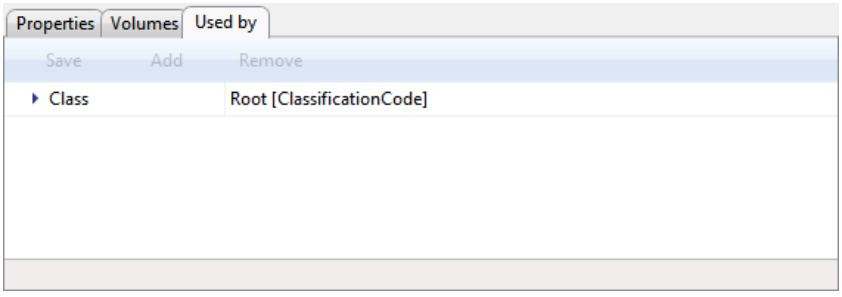


Image 383: Using the profile under the root class of the archive

2018 © Imaging Systems, Inc., All rights reserved.

The user with appropriate access rights can add a new class by selecting the »Add« command in the command bar and by setting the class identifier accordingly. When the identifier value is not set, the profile is used on the level of the archive. Otherwise the profile is used only under the selected class. The user can enter either the classification code, the internal or external class identifier. The new class is saved by choosing the »Save« command.

The class is removed by choosing the »Remove command«.

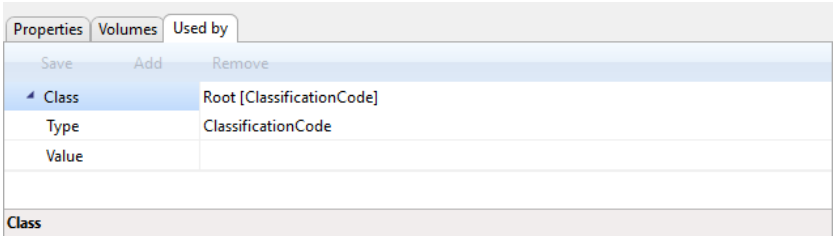


Image 384: Entering the class for profile

Warning: It is required to restart the IMiS®/ARChive Server in order to effect changes of the value settings in the »Storage« folder.

2018 © Imaging Systems, Inc., All rights reserved.

8.4.14.2 »Volumes« subfolder

In the »Volumes« subfolder the user with appropriate access rights can view the attribute values, which are tied to the profile in the lower right view of the Windows Explorer.

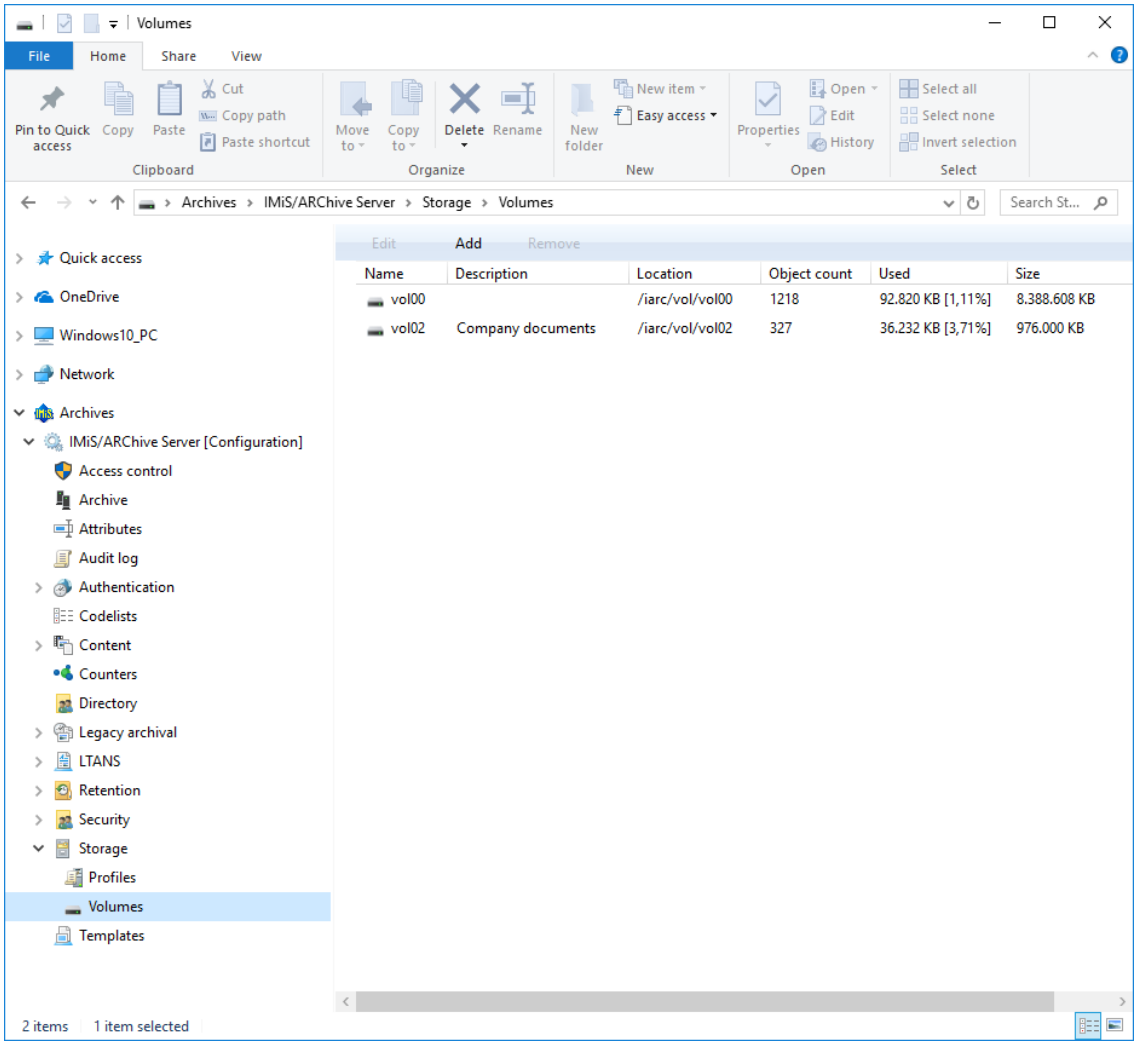


Image 385: Volumes, which are tied to the profile

The »Properties« tab content is the same as the content of the »Volumes« tab in the »Properties« configuration subfolder.

<u>»Properties« tab</u>

By clicking the individual volume on the list, the following value settings are shown in the »Properties« tab in lower right view of the Windows Explorer.

- »Name«: contains the unique volume name.
- »Description«: contains a short description of the volume.

2018 © Imaging Systems, Inc., All rights reserved.

- »Location«: contains logical path to the volume in the file system. After the value has been saved for the first time, it becomes immutable.
  »Profiles«: contains a link to the profile, in which the volumes are situated.
  For a new entry the user has to choose the profile name that he wants to link to the volume in the »Name« field. In the »Used after« field the user has to set the position in the queue of profile volumes. By selecting »First«, the profile is placed at the beginning of the queue. Alternatively, the user can select the existing volume name, after which the volume should be placed. When there are no objects on the volume, the profile name and position can be changed. Otherwise, the values become immutable after they are saved for the first time.
- »Object count«: shows the number of archived objects on the volume.
- »Used [bytes]«: shows the size of used space on the volumes in bytes.
- »Size [bytes]«: shows the size of free space on the volumes in bytes. The user with appropriate access rights can grant the volume more space by entering a new value or by increasing the value with 1024-byte increments. When the user wants to prevent further archiving of objects into the volume, he must set the size of available space to be the same as the value of the »Used« attribute.
- »Read only«: changing the default values from »False« to »True« can also prevent saving of objects into the volume.
- »Mounted«: by changing the default value from »True« to »False«, the volume is marked as unavailable for use.
- »Write once, read many«: value set to »False« denotes content can be written and read many times. On the contrary, value set to »True« denotes content can be read many times, but can only be written once.
- »Stop adding objects«: value set to »True« denotes it is not possible to add content to the profile. On the contrary, value set to »False« denotes it is possible to add content.

2018 © Imaging Systems, Inc., All rights reserved.

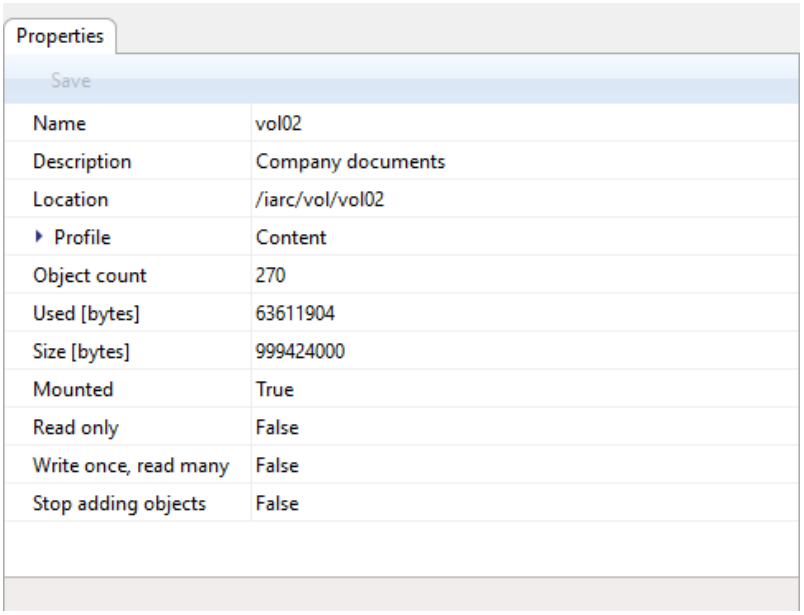


Image 386: Volume properties

Warning: The user with appropriate access rights can increase or decrease available space of the volume in bytes. When the »Size« attribute level is the same or smaller than the »Used« attribute level, the volume cannot be accessed.

Warning: It is required to restart the IMiS®/ARChive Server in order to effect changes of the value settings in the »Volumes« subfolder.

8.4.15 »Templates« folder

The »Templates« folder contains a list of templates. The following profile information is listed in the templates list:

- »Name«: unique template name. To ensure clarity, individual template types have their own icons.
- »Description«: a short description of the template.
- »Inherited from«: a list of templates, from which the template is inherited.

2018 © Imaging Systems, Inc., All rights reserved.

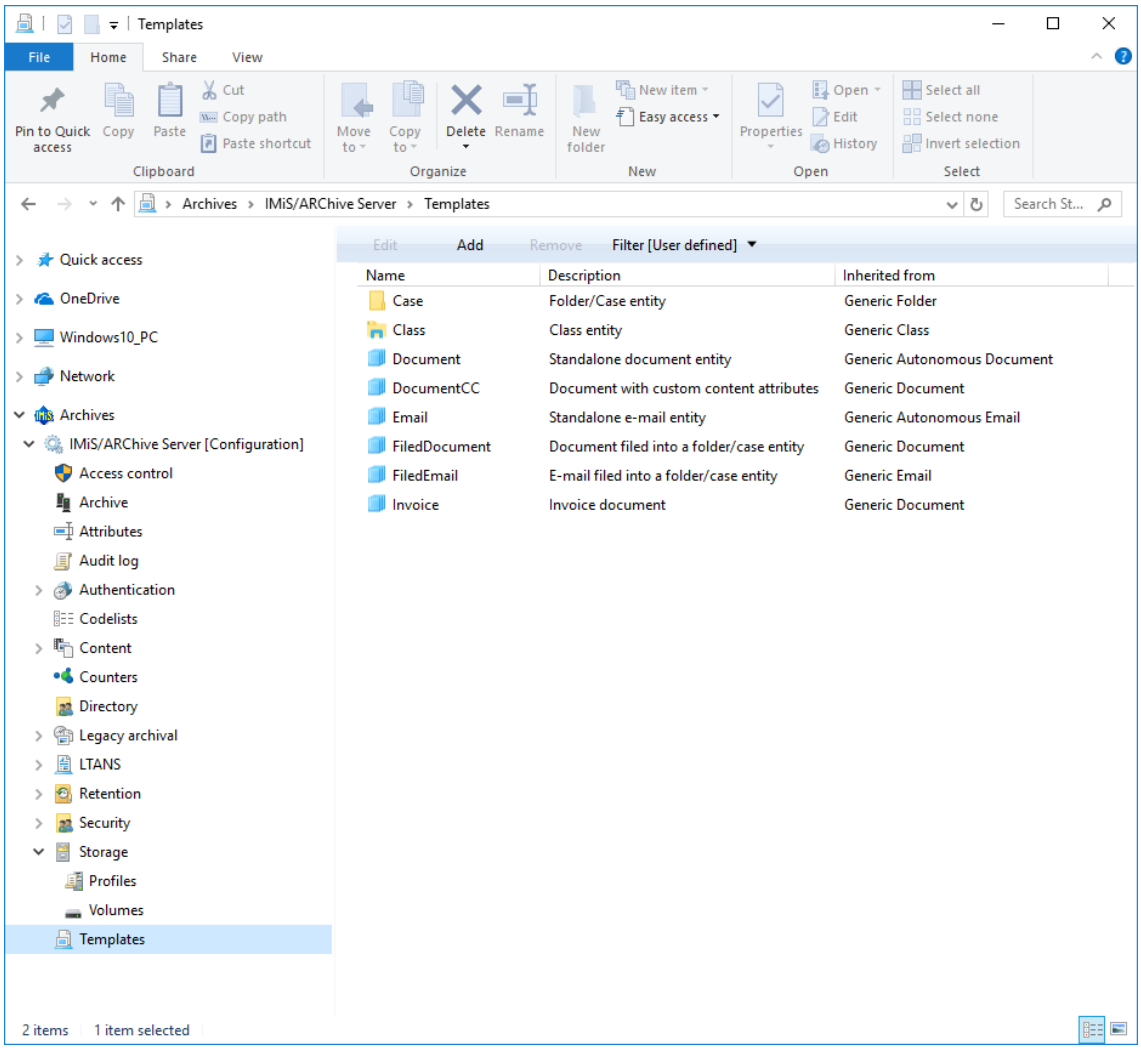


Image 387: Attribute list in the »Templates« folder

By choosing the »Filter« command in the upper command bar, the user with appropriate access rights can set the view content.

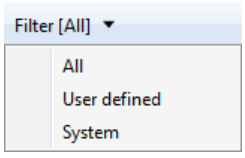


Image 388: Selecting the filter in the »Templates« configuration folder

The user can choose between the following options:

- »All«: all templates are shown on the list.
- »User defined«: only user-defined templates are shown on the list.
- »System«: only system templates are shown on the list.

2018 © Imaging Systems, Inc., All rights reserved.

The user-defined templates can only be set by the user with appropriate access rights. Based on these templates, the users create new entities according to the settings.

»Properties« tab

By clicking the individual template on the list, the following value settings are shown in the »Properties« tab in the lower right view of the Windows Explorer:

- »Name«: unique template name. After the value has been saved for the first time, it becomes immutable.
- »Type«: the user with appropriate access rights can choose between the following values: Class, Folder, Document. After the value has been saved for the first time, it becomes immutable.
- »Description«: a short description of the template.
- »Label«: the attribute value represents the label of the version in the series. This value is created automatically on checking in the document draft and represents the next version in the series.
- »Inherited from«: the user with appropriate access rights can define from which template the created template is inherited. The latter takes over all attributes from the inherited template. After the value has been saved for the first time, it becomes immutable.
- »Entity count«: number of entities, in which the template is used.

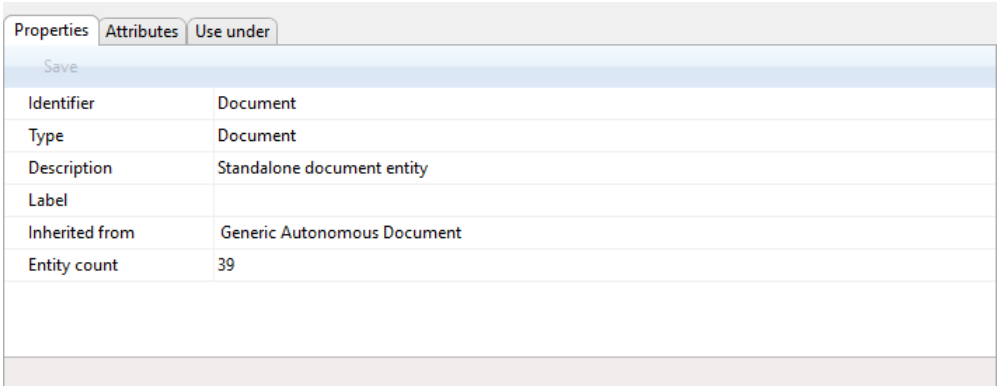


Image 389: Template properties

»Attributes« tab

All attributes tied to the template, including their properties are listed in the »Attributes« tab in the lower right view of the Windows Explorer.

2018 © Imaging Systems, Inc., All rights reserved.

The attributes are shown in two groups, in the system group and in the custom group. There are different types of attributes, depending on whether they are inherited and therefore especially marked or not. Only attributes that have not been inherited can be edited.

The following properties of the attribute that have not been inherited can be edited:

- »Public«: if the selected value is »True«, the attribute is accessible for all users regardless of their rights.
- »MultiValue«: if the selected value is »True«, the attribute can have multiple values.
- »Non Empty«: value set to »True« denotes that the attribute value cannot be empty.
- »Required«: if the selected value is »True«, the attribute value is mandatory.
- »Read only«: if the selected value is »True«, the attribute value cannot be changed.
- »Inherited«: if the selected value is »True«, the attribute values are inherited from the parent hierarchy.
- »AppendOnly«: if the selected value is »True«, the attribute value can only be added to the existing values.
- »IncludedInAIP«: if the selected value is »True«, the attribute values are part of the archival information package.
- »Validation Expression«: specifies the value that represents the regular expression used to check the new or changed attribute values. Further information about the syntax and rules: http://en.wikipedia.org/wiki/Regular_expression.

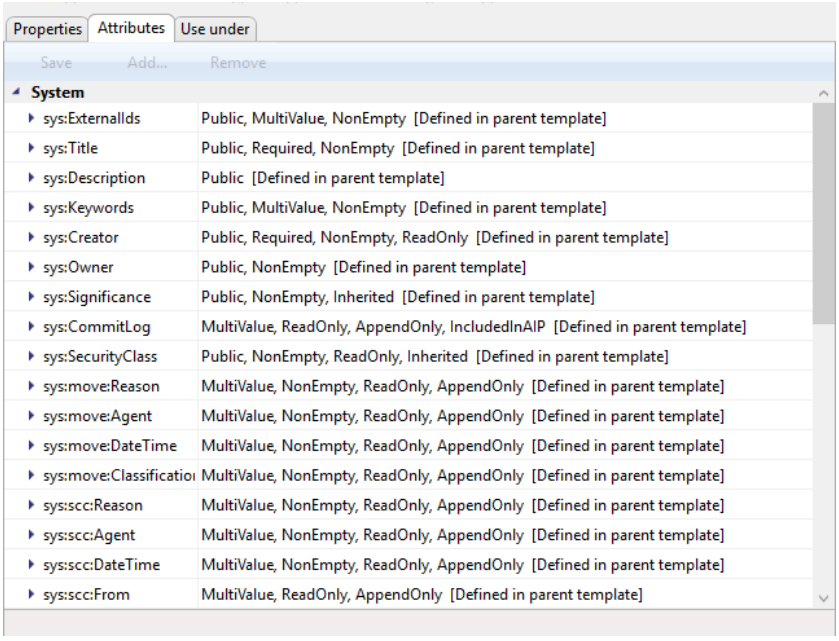


Image 390: List of attributes used in the template

2018 © Imaging Systems, Inc., All rights reserved.

Warning: The user with appropriate access rights can only add user-defined attributes.
System attributes are inherited from the template, which can be set in the »Properties« tab.

»Use under« tab

In the »Use under« tab in the lower right view of the Windows Explorer, templates and entities, in which a certain template is used are listed.

Image 391: Templates and entities, where the template is used

The user with appropriate access rights can add a new template or entity by selecting the »Add« command in the command bar and by choosing the »Template« or »Entity« command. When adding a template, the user has to select the desired template from the generic system and user defined templates. The new template or entity is saved by choosing the »Save« command.

When adding the entity, the user has to set the entity identifier accordingly.
When the identifier value is not set, the template is used on the level of the archive.
Otherwise the template is used only under the selected entity. The user can enter either the classification code, the internal or external entity identifier.

The template or entity is removed by choosing and using the »Remove« command.

2018 © Imaging Systems, Inc., All rights reserved.

9 TROUBLESHOOTING

Users of the IMiS®/Client 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.

9.1 How to avoid problems

Regular updating of the IMiS®/Client 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.

9.2 Frequent errors

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

2018 © Imaging Systems, Inc., All rights reserved.

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.

Error during user login (»Authentication was unsuccessful«)

Likely cause: Unregistered or invalid username, or wrong password.

Solution: Double check if the username and password are correct (characters are case sensitive, check for unwanted spaces ...etc.).
If you believe the username and password are correct, please verify if the user is registered on the IMiS®/ARChive Server with these exact characters.

Error when saving a new folder (»New folder cannot be saved on archive.«)

Likely cause 1: You are trying to create a folder on a sub-level that is too deep in the classification scheme. When a new folder is saved, a classification code will automatically be created, and the IMiS®/ARChive Server code generator only supports numbers up to a certain sub-level of the classification scheme.

Solution 1: Try to save the folder to a higher sub-level of the classification scheme.

Likely cause 2: The folder's required metadata has not been entered. When saving a new folder, the IMiS®/ARChive Server will return an error stating that required metadata is missing.
A description appears in the expanded error window.

Solution 2: Complete all the required metadata fields for the folder.

2018 © Imaging Systems, Inc., All rights reserved.

Error when saving a new document (»New document cannot be saved on archive.«)

Likely cause: The document's required metadata has not been entered. When saving a new document, the IMiS®/ARChive Server will return an error stating that required metadata is missing. A description appears in the expanded error window.

Solution: Complete all the required metadata fields for the document.

Error when editing an existing entity (»[Class, Folder, Document] <classification code> cannot be saved on archive.«)

Likely cause: The entity's required metadata has not been entered correctly, or has been removed. When saving an edited entity, the IMiS®/ARChive Server will return an error stating that required metadata is missing. A description appears in the expanded error window.

Solution: Complete all the required metadata fields for the entity.

Error when trying to edit a closed entity (»Closed [class, folder, document] <classification code> cannot be edited.«)

Likely cause: The entity's status is »Closed«. A closed entity cannot be edited.

Solution: Verify if the closed entity should indeed be edited. If yes, change the status of the entity into »Opened« using the »Change status« action, and then reopen the entity.

Error when opening an entity in editing mode (»[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.

Error when opening an entity in reading mode (»[Class, Folder, Document] <classification code> cannot be opened.«)

See »Error when accessing an archive«, listed above

2018 © Imaging Systems, Inc., All rights reserved.

Error when opening an entity in editing mode. User does not have sufficient rights. (»[Class, Folder, Document] <classification code> cannot be edited. User has insufficient rights to edit entity.«)

Likely cause: The user wants to edit an entity they are not allowed to edit.

Solution: A user with sufficient rights grants the current user rights to edit the entity.

Error when opening an entity in reading mode. User does not have sufficient rights. (»[Class, Folder, Document] <classification code> cannot be opened. User has insufficient rights to open entity.«)

Likely cause: The user wants to open an entity they are not allowed to open.

Solution: A user with sufficient rights grants the current user rights to open the entity.

Cannot delete folder/class. (»[Class, Folder] <classification code> cannot be deleted on archive.«)

Likely cause: The class or folder still contains entities and therefore can't be deleted.

Solution: Every entity inside the class or folder you wish to delete must be deleted individually. When the class or folder is empty, you can delete it.

Cannot delete entity. User does not have sufficient rights. (»[Class, Folder, Document] <classification code> cannot be deleted on archive. User has insufficient rights to open entity.«)

Likely cause: The user does not have permission to delete the entity.

Solution: A user with sufficient rights grants the current user rights to delete the entity.

Cannot delete entity. Entity is closed. (»Closed [class, folder, document] <classification code> cannot be deleted.«)

Likely cause: The entity's status is »Closed«. Closed entities cannot be deleted.

Solution: Verify if the closed entity should indeed be deleted. If yes, change the status of the entity into »Opened« using the »Change status« action, and then delete the entity.

2018 © Imaging Systems, Inc., All rights reserved.

9.3 Less frequent errors

Error when closing an entity. (»[Class, Folder, document] <classification code> cannot be set in preview state.«)

Likely cause: An entity was open in reading or editing mode. When the user finished working on the entity, user selected another entity. This resulted in the IMiS®/Client's automatic attempt to close the previous entity, which it was unable to do. The error's cause is probably a failure to access the archive.

Solution: See section »Error when accessing an archive«.

Error when reading entity metadata. (»Error while retrieving entity property.«)

Error description: When saving, opening or closing an entity, metadata was not successfully retrieved by the client.

Likely cause: Type of the entity's metadata is different from the type expected by the IMiS®/Client.

Possible solution: Make sure the currently installed version of the IMiS®/Client is compatible with the currently installed version of the IMiS®/Archive Server.

Error when opening content files in editing mode. (»File <content description> is already open in another application. Close the other application and try again.«)

Likely cause: The user is trying to open the content of an entity which is already open in another application.

Solution: Close the application where the content is already open, then try to reopen the content.

Error when capturing content with the scanner. (»Attachment cannot be added from scanner.«)

Error description: An error occurred during communication with the virtual scanner.

Likely cause 1: The IMiS®/Scan application is not installed on the computer, or is not compatible with the current version of the IMiS®/Client.

Solution 1: Contact the administrator and get the IMiS®/Scan application to work on the computer.

2018 © Imaging Systems, Inc., All rights reserved.

Likely cause 2: After a scanned document was saved by the IMiS®/Scan application, the IMiS®/Client was unable to open it.

Solution 2: Contact IMiS® support at the following email address: support@imis.eu.

Likely cause 3: An error occurred during the transfer of the scanned document to the IMiS®/ARChive Server.

Solution 3: See section »Error when accessing an archive«.

Error when scanning the content files of a document. (»File <file path> cannot be attached to content.«)

Error description: An error can sometimes occur while adding files from the file system.

Likely cause 1: The file you are trying to add does not exist in the file system, or the name or path of the file is wrong.

Solution 1: Make sure the path and the file name and format are correct.

Likely cause 2: The MIME type of content files cannot be recognized by the IMiS®/Client or the IMiS®/ARChive Server.

Solution 2: Try to convert the file to another format, change the extension of the file manually, or contact IMiS® support at: support@imis.eu.

Error when moving an entity. (»[Class, Folder, document] <classification code> cannot be moved.«)

Error description: An error occurred while trying to move the entity.

Likely cause 1: The user does not have sufficient rights to move the entity.

Solution 1: A user with sufficient rights grants the current user rights to move the entity.

Likely cause 2: The user does not have a »move« permission on the server.

Solution 2: An IMiS®/ARChive Server user with sufficient rights grants the current user a »move« permission on the server.

2018 © Imaging Systems, Inc., All rights reserved.