IMiS<sup>(R)</sup>/Client
Manual
Version 9.5.1510

# IMAGING SYSTEMS

# TABLE OF CONTENTS

**TABLE OF IMAGES**

Table of images appearing in the manual

## LIST OF TABLES

Below is a list of tables appearing in the manual:

# 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

## 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 |
| HTML | HyperText Markup Language |
| ID | Identifier |
| IPTC | International Press Telecommunications Council News Feed Format |

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

| Abbreviation | Description |
|---|---|
| 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

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.<br>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

## 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 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.

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.
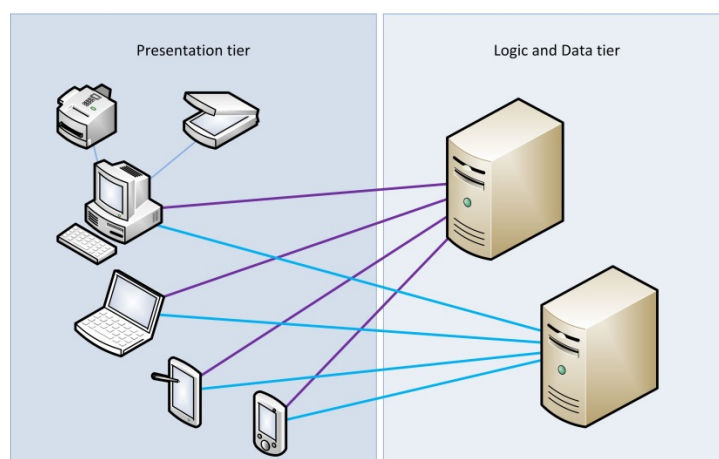


Image 1: Example virtual two-tier document system

## 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 June 2014 IMiS® module release is represented by 1406 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.

- 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 9.1.1406 installation package for 64-bit Windows with .NET 4.0 framework:*

*IMiS.Client.9.1.1406.x64.msi*

## 2.4  Functionalities

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

- Access to any number of IMiS®/ARChive Servers.

- Secure user authentication.

- Access to the records according to a predetermined organization scheme.

- Entry and management of the records metadata according to a predetermined attribute scheme.

- Storage of archive materials of electronic origin, or digitized using the scanner.

- Streaming-mode access to the records.

- 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.

- Printing of records and classification schemes.

- Creation of access reports.

- 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.
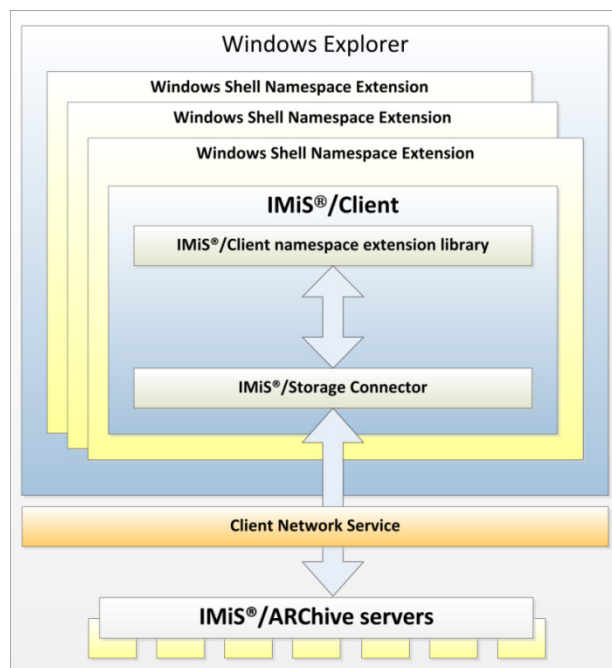


Image 2: Client architecture

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.
- *imisclient.res.net.dll*;  contains additional resources for the client.
- 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.

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:*

*<?xmlversion="1.0"encoding="utf-8"?>*
*<Classxmlns: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">*
*<Descriptionxmlns="">*
*<classification>*
*<classification_code>08</classification_code>*
*<fully_qualified_classification_code>*
*    08*
*</fully_qualified_classification_code>*
*</classification>*
*<place />*
*<title>Test document</title>*
*…*

Image 3: Example XPath notation text

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

*/Class/classification/fully_qualified_classification_code.*

### 3.2.1   File structure

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

[class|file|sub-file|record]_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 (*see chapter 3.2.2  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 |

/<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« and »bcc« of the message according to RFC 2822 specification. | | | | |
| **XMLSchema type:** | String | **Reference:** | eml:ToCC, eml:ToBCC | **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 valid 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« and »bcc« of the message according to RFC 2822 specification. |  |  |  |  |
| **XMLSchema type:** | String | **Reference:** | eml:ToCC, eml:ToBCC | **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:** | 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** | eml:MessageId | **MOREQ2 code:** | M195 |

/<entity_type>/Description/place/current_location

|  | **Required:** | NO | **Number:** | 1 |  |
|---|---|---|---|---|---|
| **Definition:** | Current location of physical records |  |  |  |  |
| **Use:** | **Class:** NO | **Folder:** YES | **Sub-File:**YES | **Record:**YES |  |
| **Commentary:** | The value represents a description of the current location of physical records, when this is not a home location or when physical records is checked out or entrusted to a third party for storage. Enter data that describes the external location of physical records as precisely as possible (address, room, cabinet, folder …). At the same time, make the appropriate modification of the attribute »prm:Status« into »CheckedOut«. |  |  |  |  |
| **XMLSchema type:** | String | **Reference:** | 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:** | 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:** | eml:To | **MOREQ2 code:** | M186 |

/<entity_type>/Description/recipient/name

| | **Required:** | NO | **Number:** | Multiple | |
|---|---|---|---|---|---|
| **Definition:** | Name of email recipient | | | | |
| **Use:** | **Class:** NO | **Folder:** NO | **Sub-File:**NO | **Record:**YES | |
| **Commentary:** | Values represent valid names of email recipients. They are forwarded by the messaging client, which usually acquires them from the message itself, though the precision of the information depends on the client. Values represent the values of the attribute »to« of the message according to RFC 2822 specification. | | | | |
| **XMLSchema type:** | String | **Reference:** | 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:** | 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:** | eml:From | **MOREQ2 code:** | M075 |

/<entity_type>/Description/title

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

/<entity_type>/Event_history/abstract/reclassification_reason

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

/<entity_type>/Event_history/date/checked_in

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

/<entity_type>/Event_history/date/closed

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

/<entity_type>/Event_history/date/created

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

/<entity_type>/Event_history/date/opened

|  | **Required:** | YES | **Number:** | 1 |
|---|---|---|---|---|
| **Definition:** | Date and time of change of attribute »sys:Status« to »Opened« | | | |
| **Use:** | **Class:** YES | **Folder:** YES | **Sub-File:**YES | **Record:**YES |
| **Commentary:** | The value represents the date and time when the attribute »sys:Status« of the entity in question received the value »Opened« *(see chapter 4.3.1 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:** | prm:ReturnDue | **MOREQ2 code:** | M098 |

/<entity_type>/Event_plan/status/permanent

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

/<entity_type>/Identity/system_identifier

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

/<entity_type>/Relation/agent/custodian

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

/<entity_type>/Relation/agent/owner

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

/<entity_type>/Relation/is_child_of

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

/<entity_type>/Relation/retention_and_disposition_schedule

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

/<entity_type>/Relation/disposal_hold

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

/<entity_type>/Use/status/active

|  | **Required:** | YES | **Number:** | 1 |
|---|---|---|---|---|
| **Definition:** | Entity is active | | | |
| **Use:** | **Class:** YES | **Folder:** YES | **Sub-File:**NO | **Record:**NO |
| **Commentary:** | »true« when the attribute »sys:Status« of the entity in question has the value »Opened« (*see chapter 4.3.1 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 phyical record, its format, physical carriers, volume ... | | | |
| **XMLSchema type:** | String | **Reference:** | prm:Description | **MOREQ2 code:** M092 |

/<entity_type>/Custom/AuditTrail

| | 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 tag »Content« contains the XML attribute »hash_algorithm« of »string« type, which contains the name of the hash algorithm and at least one »Value« tag that contains the following attributes: <br><br>• Hash:  hash value of the exported content. <br>• Mime:  data of the type of content. <br>• Description:  description of the content. <br>• Accessed:  time stamp of last access to the content. <br>• Created:  time stamp of content creation. <br>• Modified:  time stamp of last edit of the content. <br>• Extension:  content extension. <br>• Size:  size of the content. <br><br>Each »Value« tag represents exactly one content (file). The value of the »Value« tag represents the name of the exported content. | | | |
| **XMLSchema type:** | complexType | **Reference:** | sys:Content | **MOREQ2 code:** / |

/<entity_type>/Custom/Property

| | Required: | NO | Number: | Multiple |
|---|---|---|---|---|
| **Definition:** | Other attributes (names and values) | | | |
| **Use:** | **Class:** YES | **Folder:** YES | **Sub-File:**YES | **Record:**YES |
| **Commentary:** | List of entity's attributes along with values that are not part of Moreq2 specification. Each »Property« tag contains exactly one »Name« XML tag of »string« type, which contains the title of the attribute and at least one »Value« XML tag. Each »Property« tag contains the following XML attributes: <br><br>• Hash_algorithm:  type »string«, contains name of the hash algorithm. <br>• Value_db_type:  type »string«, contains name of the attribute type in the database. <br>• Value_content_type:  enumerator that represents the type of the attribute. Possible values are: STRING, STRINGMAX, BINARY. | | | |
| **XMLSchema type:** | complexType | **Reference:** | Attribute | **MOREQ2 code:** / |

/<entity_type>/Custom/Property/Value

| | **Required:** | YES | **Number:** | Multiple |
|---|---|---|---|---|
| **Definition:** | Value of the attribute described in tag »/<entity_type>/Custom/Property/Value« | | | |
| **Use:** | **Class:** YES | **Folder:** YES | **Sub-File:**YES | **Record:**YES |
| **Commentary:** | When the value of the »value_content_type« enumerator is STRING, the tag does not contain XML attributes, and the value of the attribute is then written in the XML tag. When the value of the »value_content_type« enumerator is STRINGMAX or BINARY the tag contains the following attributes: <br>• Hash:  hash value of the file with the content of the attribute. <br>• MIME:  data regarding the type of content. <br>The value of the XML tag contains the name of the file storing the attribute content. | | | |
| **XMLSchema type:** | String | **Reference:** | Attribute | **MOREQ2 code:** | / |

/<entity_type>/Custom/TransferredAuditLog

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

/<entity_type>/Custom/Evidence

| | **Required:** | NO | **Number:** | 1 |
|---|---|---|---|---|
| **Definition:** | Evidence of entity's authenticity | | | |
| **Use:** | **Class:** NO | **Folder:** YES | **Sub-File:**YES | **Record:**YES |
| **Commentary:** | 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 attributes are contained: <br>• Hash_algorithm:  »string« type containing the name of the hash algorithm. <br>• Hash:  hash value of file with the authenticity evidence. <br>The value of the XML tag contains the name of the authenticity evidence file. | | | |
| **XMLSchema type:** | String | **Reference:** | trf:Evidence | **MOREQ2 code:** | / |

/<entity_type>/Custom/TemplateId

|  | **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/AdditionalMetadata

|  | **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/ACL

|  | **Required:** | NO | **Number:** | Multiple |
|---|---|---|---|---|
| **Definition:** | List of access rights on the entity (Access Control List) | | | |
| **Use:** | **Class:** YES | **Folder:** YES | **Sub-File:**YES | **Record:**YES |
| **Commentary:** | Every »ACL« tag contains the »User« attribute with a name of a directory entity and one to four sub-tags »Value«, which specify the access rights on the directory entity according to attributes listed here:<br><br>• type: enumerator of the type of access right (see below).<br>• cr: right to edit access rights list.<br>• cse: right to create new child entities.<br>• da: right to delete the entity.<br>• mv: right to move the entity.<br>• ra: right to read the entity.<br>• wa: right to delete the entity.<br>• date_from: date of current access control list validity ( start / valid from).<br>• date_to: date of current access control list validity (end / valid to).<br>Description of enumerator values for the type of access right:<br>• EXPLICIT_ALLOW: explicit permission.<br>• EXPLICIT_DENY: explicit denial.<br>• INHERITED_ALLOW: inherited permission.<br>• INHERITED_DENY: inherited denial. | | | |
| **XMLScheme type:** | complexType | **Reference:** | ACL | **MOREQ2 code:** | / |

/RDS/Description/abstract/description

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

/RDS/Description/mandate

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

/RDS/Description/abstract/reason

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

/RDS/Description/title

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

/RDS/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/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/Event_plan/event_type/disposition_action

|  | **Required:** | YES | **Number:** | 1 |
|---|---|---|---|---|
| **Definition:** | Default action of the retention policy in the implementation phase of the review process. | | | |
| **Commentary:** | Valid values: <ul><li>»Dispose«:  the default action of the retention policy is the disposition of entities.</li><li>»Permanent«:  the default action of the retention policy is the permanent retention of entities.</li><li>»Transfer«:  the default action of the retention policy is the transfer of entities to another system and their disposition after confirmation of successful transfer.</li><li>»Review«:  the default action of the retention policy is to leave the entity for the next review process.</li></ul> | | | |
| **XMLScheme type:** | String | **Reference:** | sys:ret:pol:Action | **MOREQ2 code:** | M014 |

/RDS/Identity/system_identifier/retention_and_disposition_schedule

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

/RDS/Use/status/inheritance

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

Table 5:  Lists of XML tags

### 3.2.3   Format of the additional metadata export file

The additional (user entered) metadata export file is used for the particular requirements of the archiving process. Upon export, each entity may optionally be added additional metadata which is not part of the 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
<?xmlversion="1.0"encoding="UTF-8"?>
<xs:schematargetNamespace="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:elementname="AdditionalMetadataRoot">
<xs:complexType>
<xs:sequence>
<xs:elementname="Entity"minOccurs="0"maxOccurs="unbounded">
<xs:complexType>
<xs:sequence>
<xs:anyprocessContents="skip"maxOccurs="unbounded"/>
</xs:sequence>
<xs:attributename="classification_code"type="xs:string"/>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>
```

Image 4: Example XSD scheme

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

```xml
<moreq2:AdditionalMetadataRootxmlns:moreq2="http://www.dlm-network.org/moreq2/1.04.01">
<Entityclassification_code="03.01">
<!-- add custom XML node entries -->
<A>Metadata A</A>
</Entity>
<Entityclassification_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.
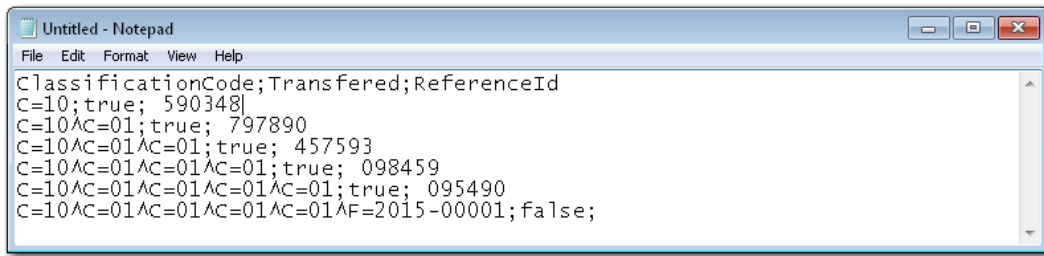
Image 6:  Example of a confirmation file after transfer

# 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.
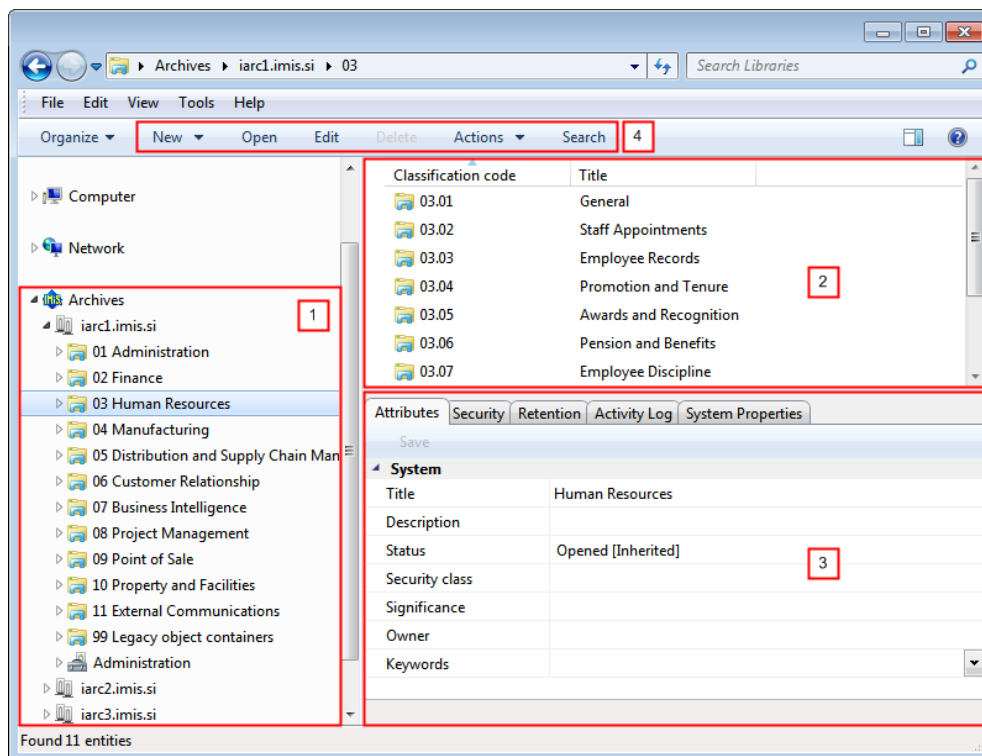


Image 7: User interface of the IMiS®/Client

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.

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 4.1.1. 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 4.1.2. 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 publically accessible entity information, users
can generally view the publically 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
publically 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 4.1.3. 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 4.1.4. The command
bar*.

### 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.
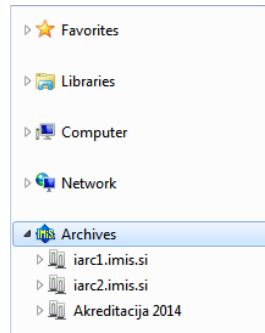


Image 8: Display of the Archives folder when the client is installed in the Desktop folder

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.
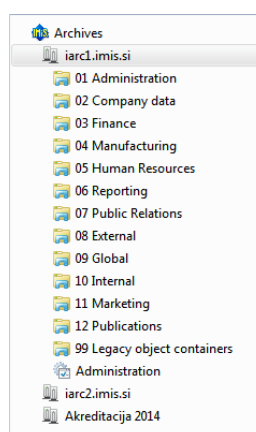


Image 9: Display of an archive's root classes and the Administration system folder

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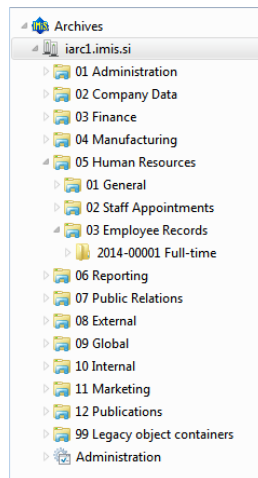


Image 10: Expanded tree view of the classification scheme

*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.*

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.



Image 11: 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.
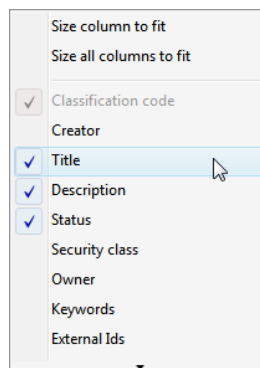


Image 12: Popup menu over a line of displayed attributes

### 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 publically 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.

- »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 publically accessible (*see chapter 4.3.1  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 (*see chapter 4.3.6  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.



Image 13: 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.
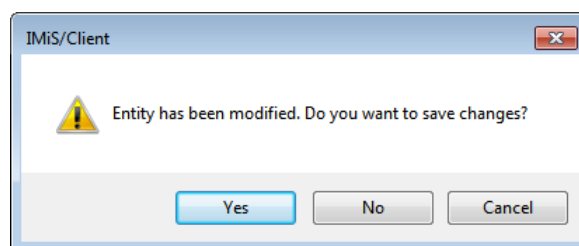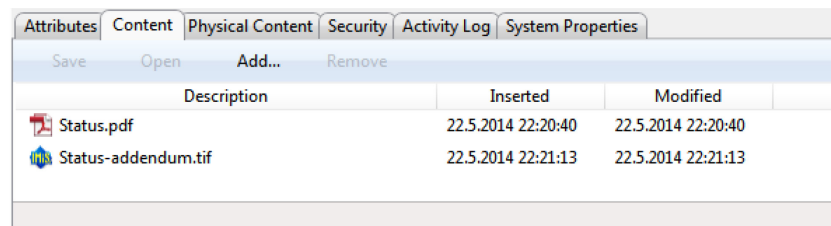


Image 14: Display of the unsaved changes alert prompt

*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.



Image 15: View of the »Content« tab

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

- »Add«:  allows you to add content to the selected entity. These can be existing files of the file system, or files scanned using the separate application IMiS®/Scan.
  The command is available when the selected entity is open in editing mode.

- »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.*

- »Remove«:  allows you to remove content from the selected entity. The command is available when the selected entity is open in editing mode.

### 4.1.3.3    The »Physical Content« tab

The »Physical Content« tab shows users the metadata of physical content corresponding to the selected entity (*see chapter 4.3.7  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 16: View of the »Physical Content« tab

The command bar just under the »Physical Content« tab has a »Save« button that is activated when metadata 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 user's effective access rights on the selected entity.
- The overview and editing of the Access Control List (ACL) or the explicit permissions for groups or users on the entity and its metadata.

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

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

The preview mode shows the title of the selected entity in the »Entity name« field.

Under this field is the list of »Effective permissions« for the chosen user.

The current effective permissions on the entity are displayed for the current user.

This command also enables seeing the other users' effective access rights on the entity.

The access rights also depend on the date and time of the display, since some permissions have a time limit. Permissions marked by a check mark are currently granted to the user.
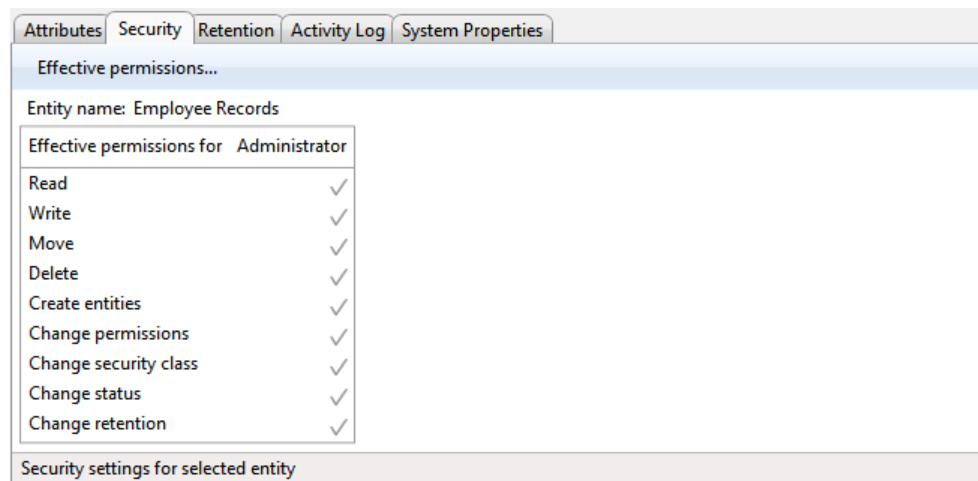
Image 17: View of the »Security« tab in preview mode

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

- »Read«:  the user has permission to read data on the selected entity (view metadata and content files).

- »Write«:  the user has permission to edit entity data (write metadata and add content files).

- »Move«:  the user has permission to move the entity within the classification scheme.

- »Delete«:  the user has permission to delete entity data (delete metadata and remove content files).

- »Create entities«:  the user has permission to create sub-entities inside the selected entity.

- »Change permissions«:  the user has permission to change the effective permissions of other users on the selected entity.

- »Change security class«:  the user has permission to change the security class of the selected entity.

- »Change status«:  the user has the permission to change the status of a selected entity.

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

In the preview mode, the command bar just under the »Security« tab has the »Effective permissions« button. This command allows the overview of effective permissions granted to the selected user, on the selected entity. By clicking the button, a window appears showing all the users registered on the IMiS®/ARChive Server.

The window allows you 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.
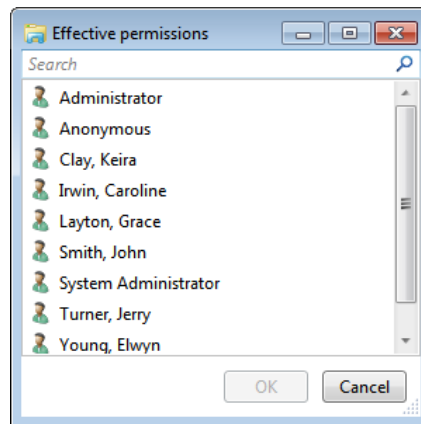


Image 18: User selection window of the »Security« tab in preview mode

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. 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.
The list of effective permissions for the current user is replaced by the list »Group or user names«. This list contains groups and users 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 user«, which shows the current effective permissions of the selected group or user on the entity.
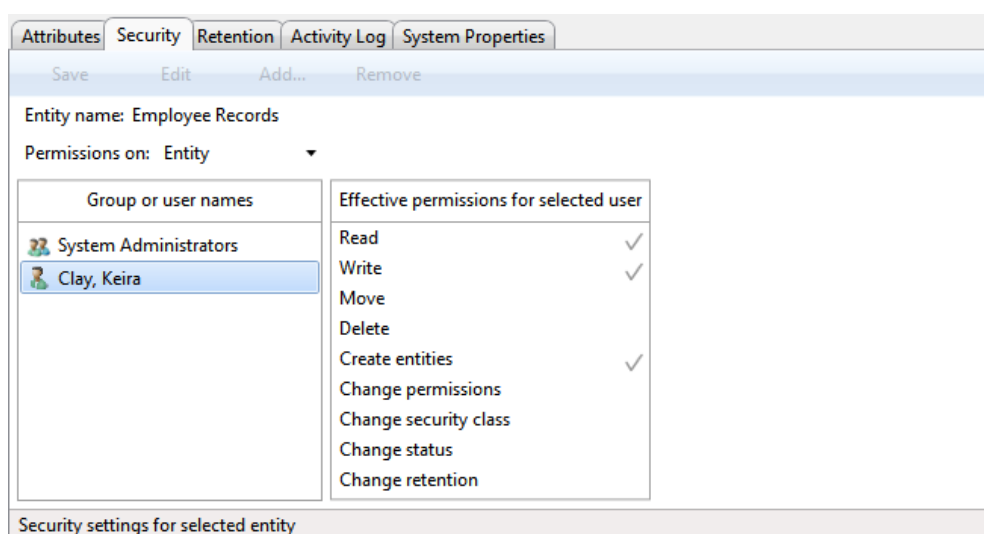


Image 19: Reading mode display of the »Security« tab

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

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

In the editing mode display, when the user has the »Change permissions« access right, 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 entity or metadata chosen in the field »Permissions on«. On the right, a permissions list appears for the selected user.

By checking the »Allow« column, a user authorized to change permissions can grant explicit permissions to the selected group or user, and by checking the »Deny« column deny them permissions. The validity field containing »Valid from« and »Valid to« values allows an authorized user to set time limits for permissions granted to the selected group or user.



Image 20: View of the »Security« tab in editing mode

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 group or user, and when groups or users are added or removed. By using the »Save« command, changes to explicit permissions are saved to the server. Unsaved changes will be discarded.

- »Edit«: enables the editing of the Access Control List for the chosen group or user selected from the list »Group or user names« and the setting of their explicit permissions on the entity or metadata selected in the »Permissions on« field.

- »Add«: enables the adding of users or groups of users 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 groups or users from the »Group or user names« list and the revoking of their explicit permissions on the selected 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.

The tab is available for review to all users with the »Review« role in all view modes for the data of the selected entity. 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 21:  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.
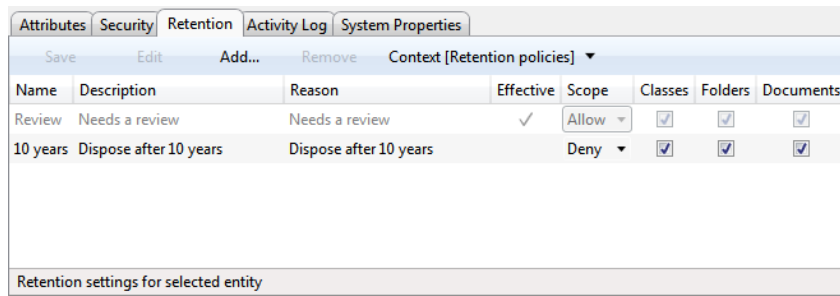
Image 22:  Display of retention periods in the »Retention« tab in editing mode

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.
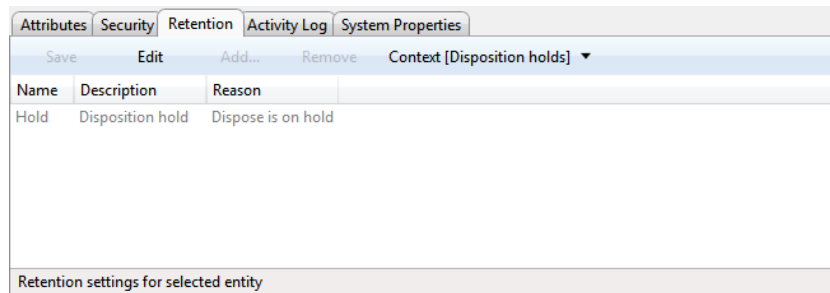


Image 23:  Display of disposition holds in the »Retention« tab in reading mode

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 »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.
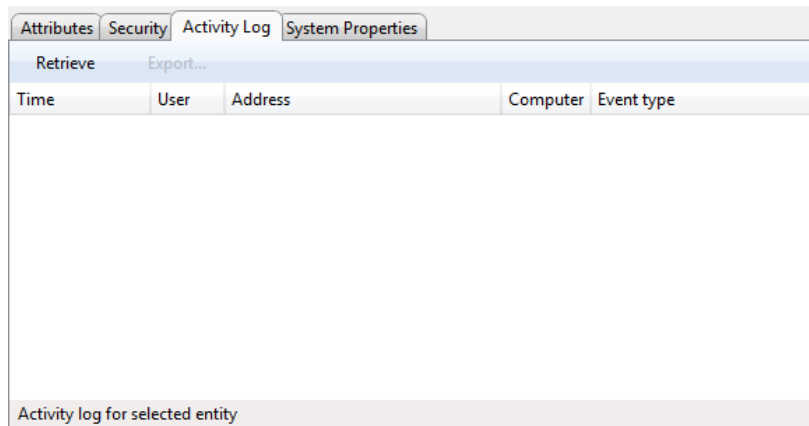
Image 24: View of the »Activity Log« tab prior to retrieving an audit trail

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.
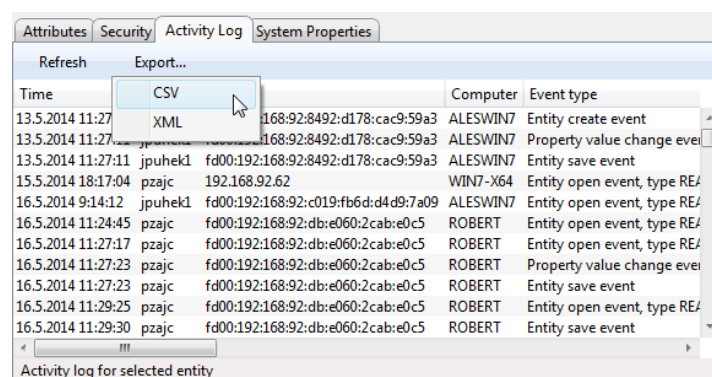


Image 25: View of the »Activity Log« tab with a displayed audit trail

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.

### 4.1.3.7    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 *(see chapter 4.3.1  General system attributes)*.

- »Security class«:  contains metadata on changes done to the entity's security class
  *(see chapter 4.3.2 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 *(see chapter 4.3.3 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 *(see chapter 4.3.5 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.



Image 26: View of the »System Properties« tab

### 4.1.4    The command bar

The command bar under the Windows Explorer menu, above the list of contained entities,
offers different commands in addition to the Windows system command »Organize«.
These depend on the selections of the user.

Above a selected »Archives« folder, the command bar offers the command »Add archive«.
When this command is chosen, a dialog box appears that lets users add archives.
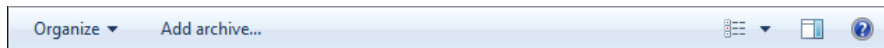


Image 27: Command bar above the selected »Archives« folder

Above a selected archive, the command bar offers the command »Log in« next to the command
»Add archive«. When the »Log in« command is chosen, a dialog box appears in order to
authenticate the user on the IMiS®/ARChive Server.
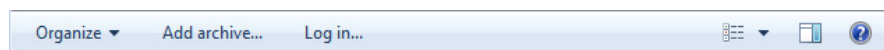


Image 28: Command bar above a selected archive prior to login

When the user successfully logs into the selected archive, the following commands appear on
the bar:

- »Log out«:  enables the user to log out of the archive. This command is only available when
  the user is currently located at the root of the archive, but not when exploring any of the
  contained entities.
- »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.
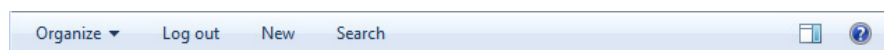


Image 29: Command bar above a selected archive when logged in

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 entiry.

- »Open«: opens the selected entity in the reading mode.

- »Edit«: opens the selected entity in the editing mode.

- »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.

- »Search«: allows searching by the metadata of contained entities and the full text of the selected entity content.
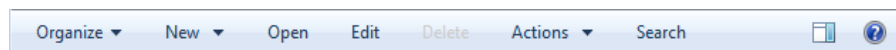


Image 30: Command bar above a selected entity

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«.
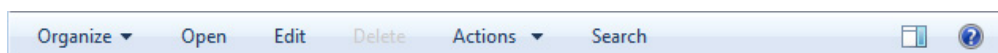


Image 31: Command bar above selected entity in the search folder

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.
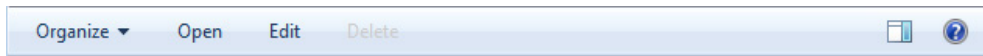


Image 32: Command bar above selected entity in the »Queue« system folder

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.
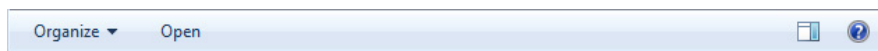


Image 33: Command bar above selected entity in the system folders »Export« and »Import«

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

### 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.
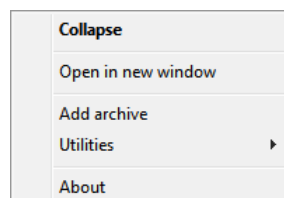


Image 35: Popup menu over the »Archives« folder

The popup menu over a <u>selected archive</u> 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.

- »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.
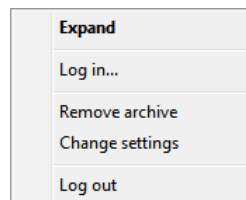


Image 36: Popup menu over the selected archive prior to login

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.
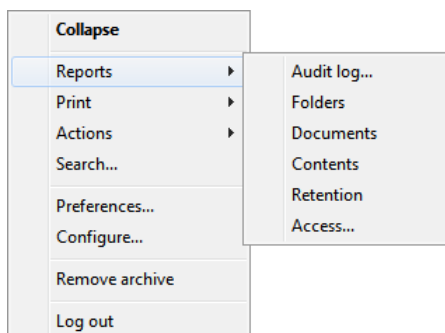
Image 37: Popup menu over the selected archive when choosing the »Reports« command

- »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.
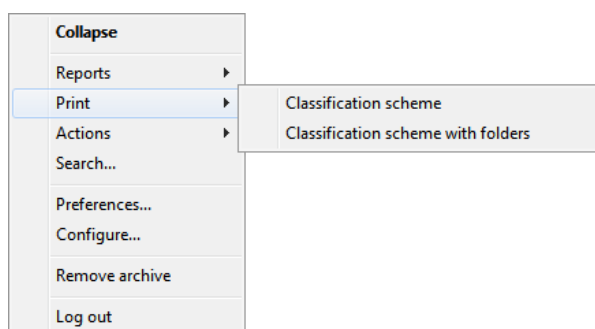


Image 38: Popup menu over the selected archive when choosing »Print«

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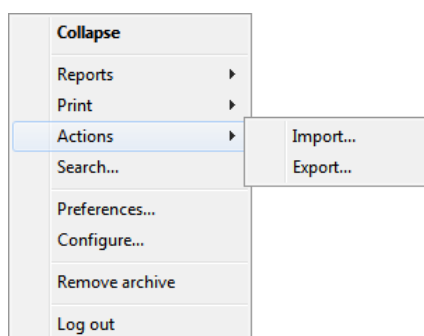


Image 39: Popup menu over the selected archive when choosing »Actions«

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

The popup menu <u>over a selected entity</u> 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.
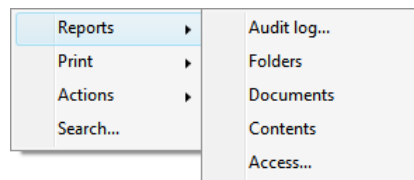


Image 40: Popup menu over the selected entity when choosing »Reports«

- »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.
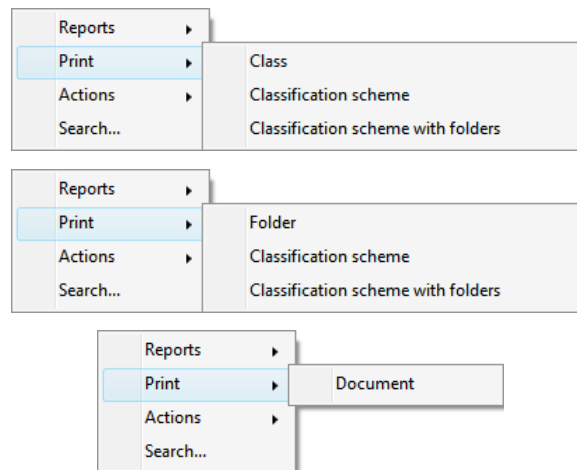
Image 41: Popup menu over the selected entity (class, folder, document) when choosing »Print«

- »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.
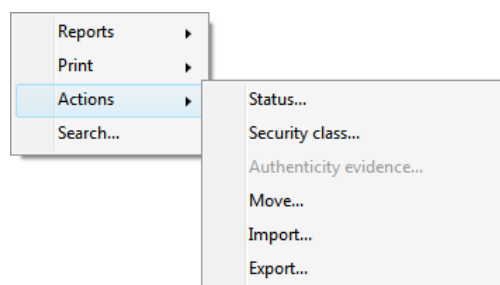


Image 42: Popup menu over the selected entity when choosing »Actions«

- »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.
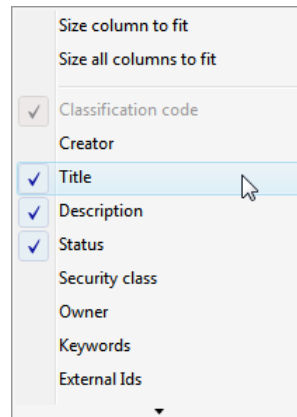


Image 43: Popup menu over a line of displayed attributes

## 4.2  Actions

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

- User login and logout from the archive.

- Capture of content and classification of records on the archive.

- Bulk capture of content.

- Conversion of content into long-term storage type.

- Access to records on the archive.

- Archiving of email messages.

- Management of physical records metadata.

- Printing of entity metadata, content and reports.

- Import, export and transfer of archived records.

- Moving and deleting of records.

- Search by metadata and search full text of archived records.

- Status changes.

- Security class changes.

- Authenticity evidence retrieval.

- Audit log 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.
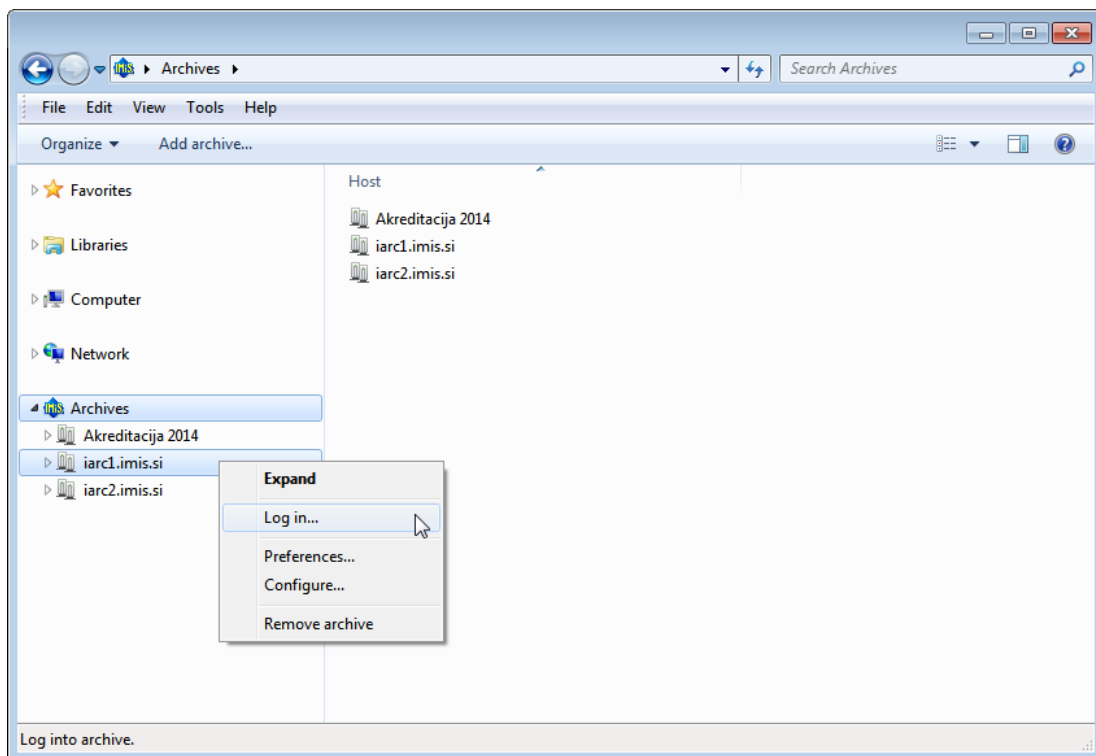


Image 44: Login into the selected archive via the popup menu

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«.
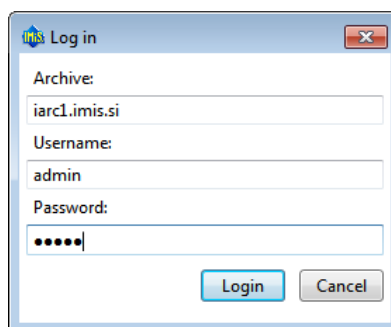


Image 45: Archive login dialog box

After a successful login, the user sees a list of those classes at the root level of the archive's document scheme, user is authorized to access.

Logout from the archive is done by using the »Log out« command in the popup menu or command bar of the selected archive. This prevents access to the IMiS®/ARChive Server.
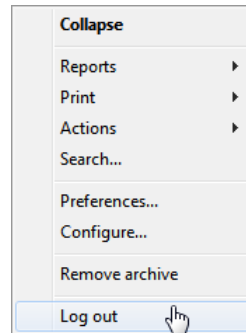


Image 46: Logging out of the selected archive via the popup menu

*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.*

### 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).*
- *…*

*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.
To check the effective access rights of the user on he selected entity *see chapter 4.1 Interface description*  and *chapter 4.1.3.4  The »Security« tab*.
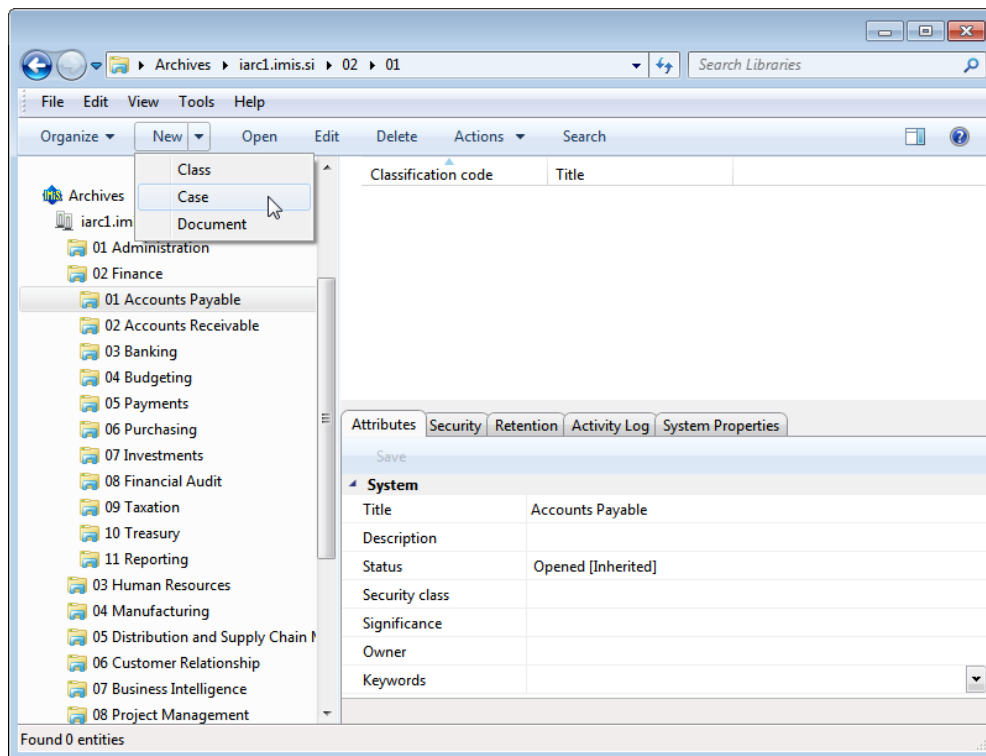
Image 47: Creating a new entity using the command bar

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.

*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.
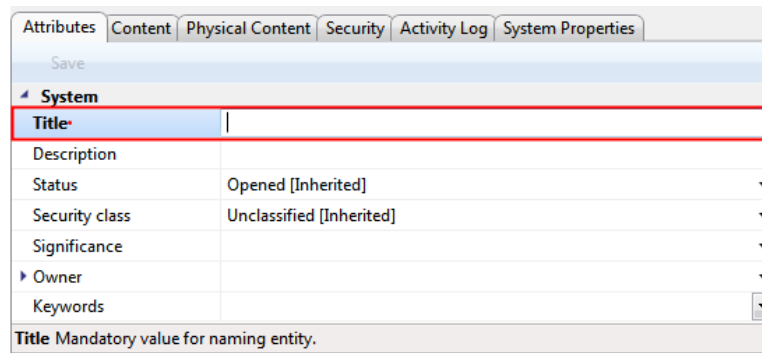
Image 48: Entry of required metadata

The list of attributes is divided into several categories:

- »System« attributes: these are present for all entities.
  See also *chapter 4.3.1 General system attributes*.

- »Email« attributes: these are present when you select a template that contains email
  attributes. See also *chapter 4.3.6 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.

Attribute entry fields are as follows:

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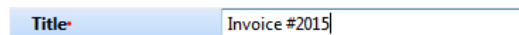


Image 49: Entry of text metadata

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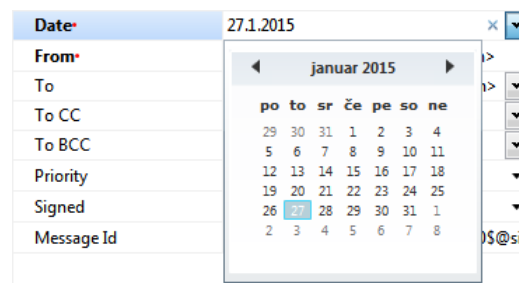


Image 50: Entry of date and time metadata

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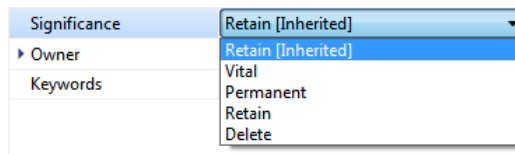


Image 51: Entry of metadata with predefined values

- 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 ( ; ).
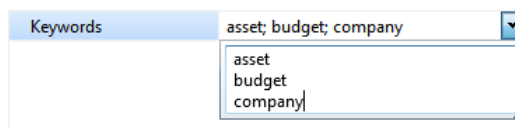


Image 52: Entry of multiple value metadata

*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. 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:

- »Automatic«:  where classification codes of child entities are generated automatically by the IMiS®/ARChive Server. These classification codes appear as successive numbers, with each new child entity increasing the number by one.

- »Manual«:  where classification codes of child entities must be entered manually. This classification code may be any combination of letters and numbers, providing it is unique inside the entire parent class.

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

Image 53: Display of the type of child classification code generation

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



Image 54: Display of the entry of a child entity's classification code

_Example:_  _Inside a class with the classification code »04-02«, the user creates a new folder for which user manually input »ProductX« as the relative part of the classification code. When the folder is saved to the IMiS®/ARChive Server, its full classification code will be »04-02-ProductX«._
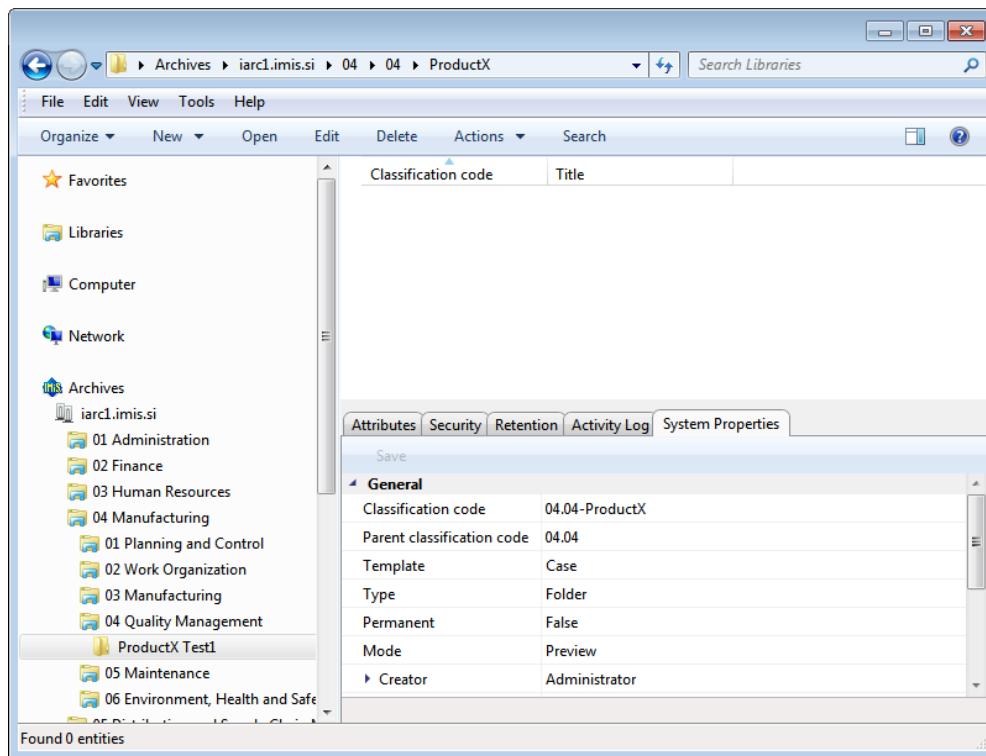
Image 55: Display of manually entered classification code

#### 4.2.2.4 Setting an entity's security class

A user with the appropriate 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.

When the parent entity's security class is not set, the list includes an empty value.

This empty value is used to remove a previously set security class, should you choose to remove it.
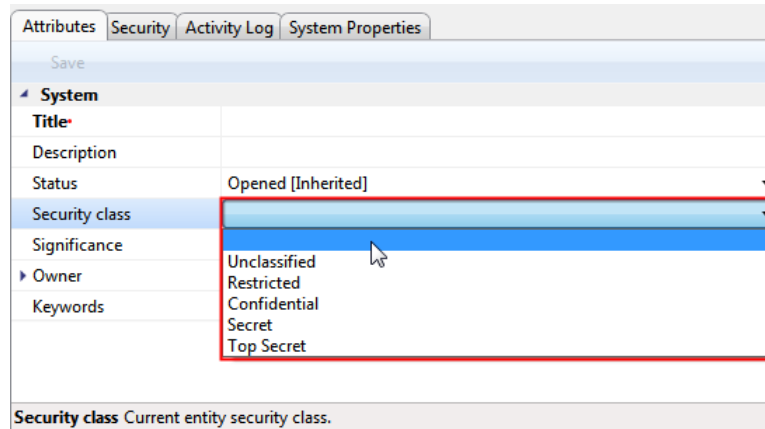


Image 56: Display of setting an entity's security class without inherited value

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].
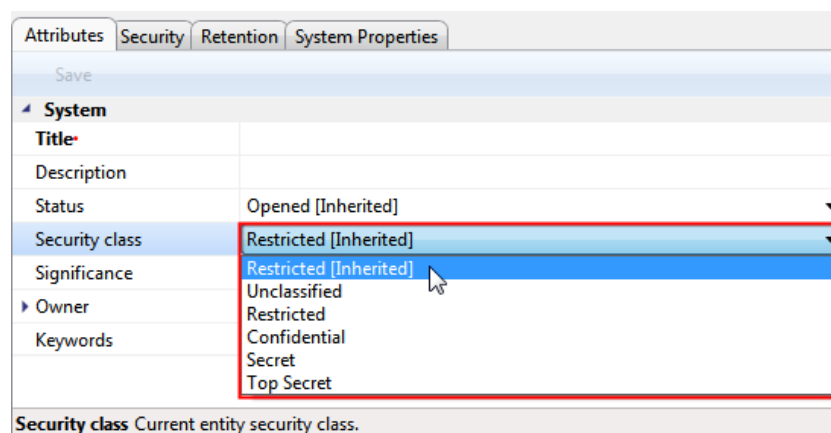


Image 57: Display of setting an entity's security class with inherited value

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 (*see chapter 4.2.17 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.*
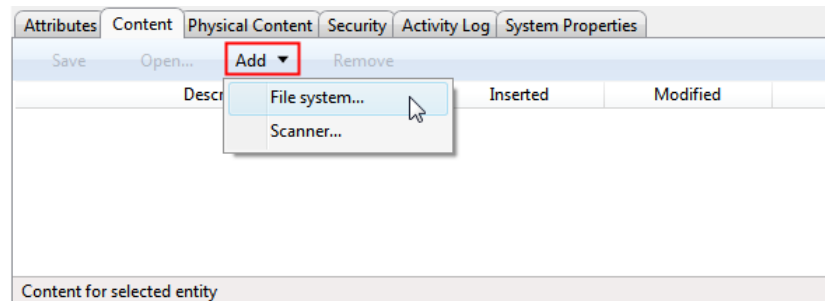


Image 58: Adding files using the file system

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.
  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 user manual of the IMiS®/Scan client*.
  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).

_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.
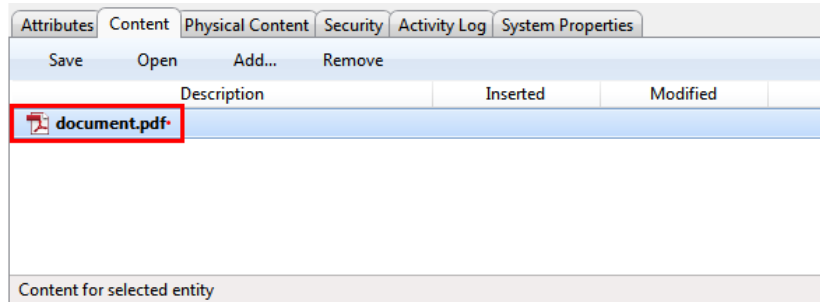


Image 59: Display of added content

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.
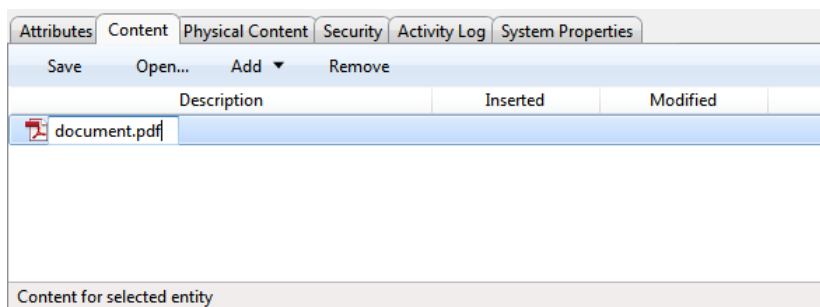


Image 60: Editing the new content's description

The description of the content is changed by clicking its name on the list. Write your

description and press the »Enter« key to confirm it. When you are done capturing all the

content, you can decide to save the entity (_see chapter 4.2.2.8  Saving an entity_)

or proceed to enter data about the physical content.

_Troubleshooting_:  Most frequent issues when capturing content:

- _The file does not exist._
- _Wrong MIME type of file._

### 4.2.2.6    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. See also _chapter 4.2.9  Managing physical content metadata_.

**4.2.2.7    Specifying retention periods**

A condition for successfully saving new entities is the existence of effective retention periods
on the entity.

This condition applies to all types of entities, except for documents in a folder for which
retention periods cannot be specified. 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.

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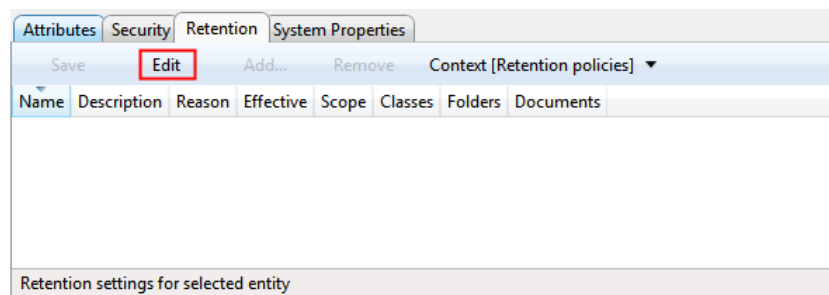


Image 61:  Enables the editing of retention periods and disposition holds

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
(*see chapter 8.4.7.1 Retention policies« subfolder*).

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.
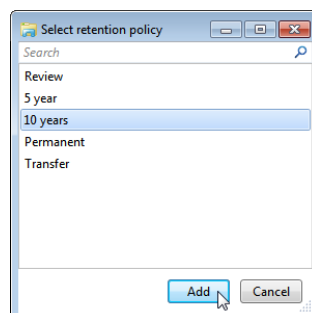


Image 62:  Adding an explicit retention period

73

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.
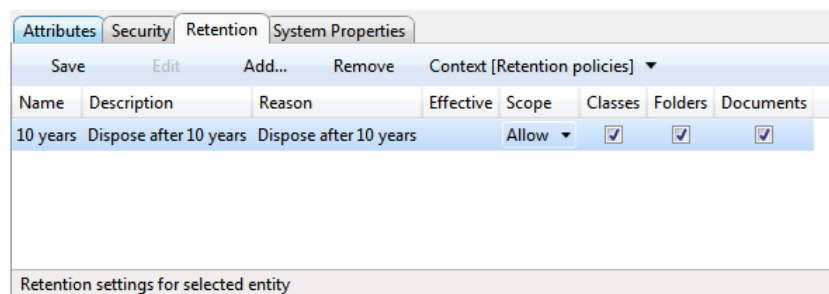
Image 63:  Editing the settings of the explicit retention period

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.
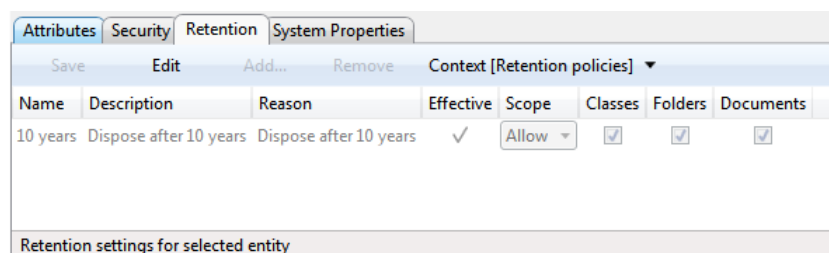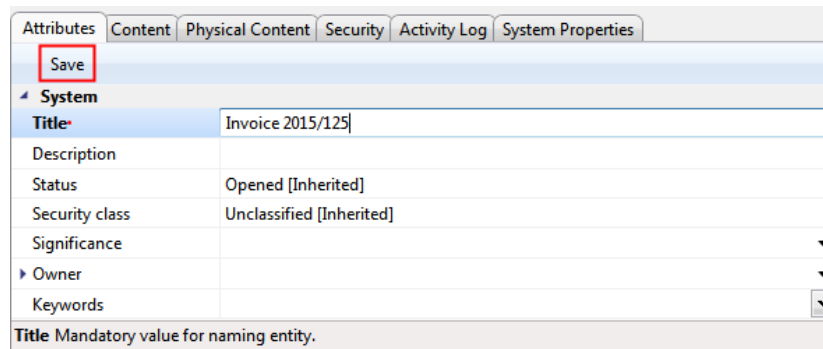
Image 64:  A saved explicit retention period

### 4.2.2.8   Saving an entity

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

Image 65: 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.*

### 4.2.2.9    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 (*see chapter 4.4.2.2 Checking the validity of electronic signatures*).

### 4.2.2.10  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 66: 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.

| ▸ Creator | Administrator |
|---|---|

Image 67: Example creator of entity

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

| Opened | 2.2.2015 11:26:57 |
|---|---|

Image 68: Example date and time an entity was opened

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

| Closed | 2.2.2015 11:41:57 |
|---|---|

Image 69: 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.

| Created | 30.1.2015 13:20:06 |
|---|---|

Image 70: Example date and time an entity was created

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

| Modified | 2.2.2015 11:28:07 |
|---|---|

Image 71: Example date and time of last changes to the entity

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

| Accessed | 2.2.2015 11:41:57 |
|---|---|

Image 72: Example date and time of last access to the entity

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



Image 73: Example entity identifier

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



Image 74: Example external identifiers of an entity

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



Image 75: 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 76: 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 77: Example date of content modification

### 4.2.3   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 4.2.11 Import*.

### 4.2.4   Conversion

For the needs of long-term content storage, the user can convert all files on the document into a long-term storage type.

*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.*

*Warning*:  *The IMiS®/Client and IMiS®/ARChive Server do not enable automatic conversion. Conversion must be done separately using the virtual printer application IMiS®/Convert To PDF-A.*

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).

#### 4.2.4.1    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._
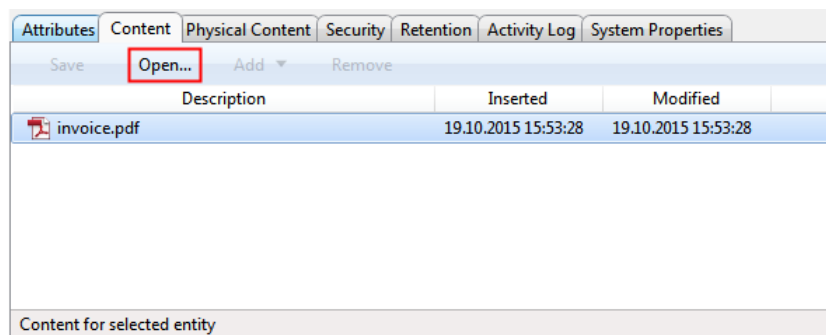


Image 78: Opening content of document in the conversion procedure

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).
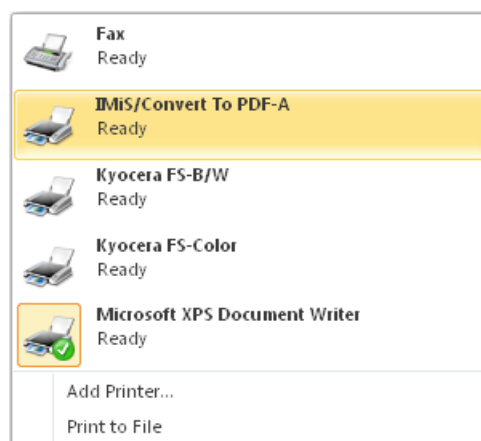


Image 79: Selecting the virtual printer »IMiS Convert To PDF-A«

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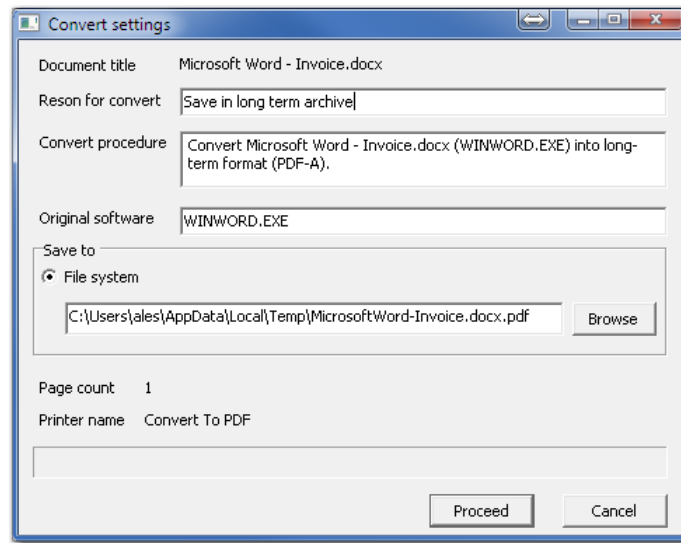


Image 80: Conversion settings via the dialog box

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.

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 *(see chapter 4.2.2.5 Content capturing procedure)*.

### 4.2.5 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.

More information on the security classes is found *in the IMiS®/ARChive Server user manual chapter 3.3.5 Access*. To learn how to change the security class of an entity *see chapter 4.2.16 Changing the security class*.

When logging into the selected archive *(see chapter 4.2.1 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.
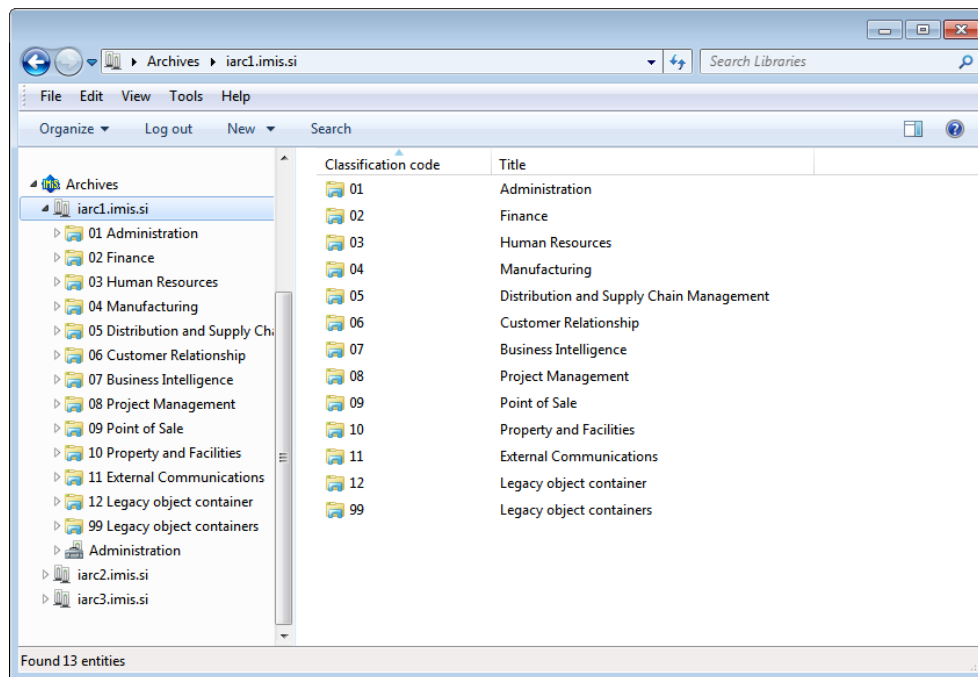


Image 81: Display of root classes when logging into the selected archive

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

- »Attributes«:  contains a list of entity metadata.
- »Security«:  displays the effective access rights of the user on the entity.
- »Activity log«:  shows the audit trail of the entity. The tab is only visible to appropriately authorized users.
- »System properties«:  contains a list of the entity's system properties.

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 a user accesses entities contained in the root classes of the archive.

The tabs initially display only the publically 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.

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 (*see chapter 4.2.7  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.
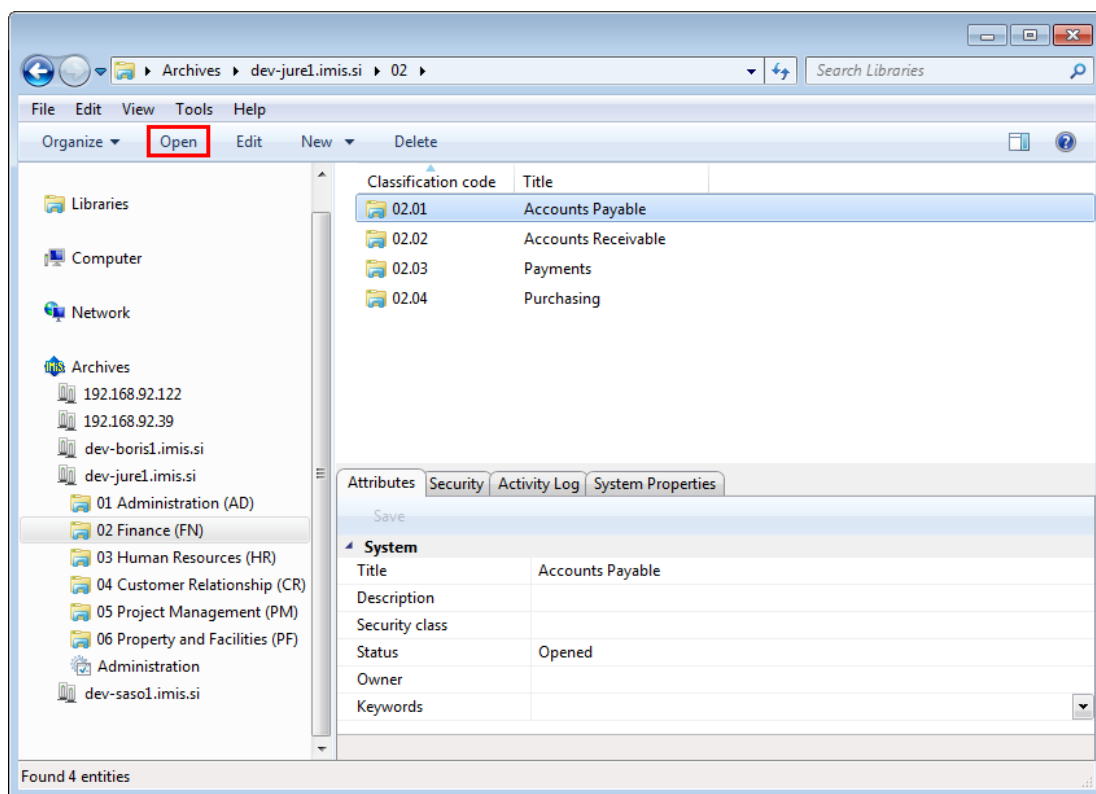


Image 82: Opening the selected entity

### 4.2.6   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.

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.
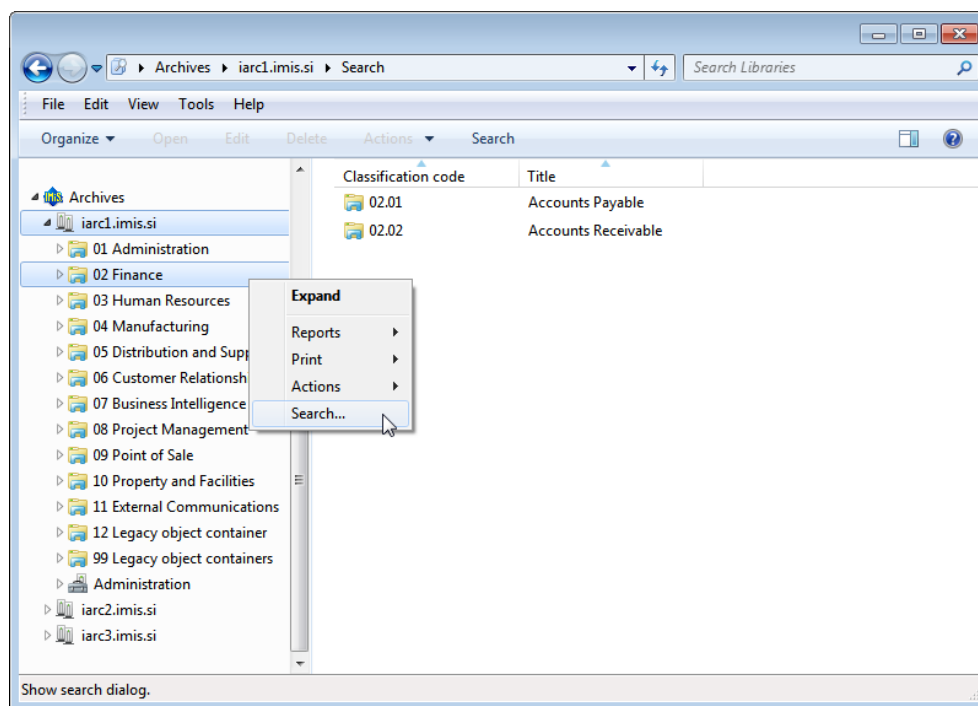


Image 83: Search of the selected entity via the popup menu

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.
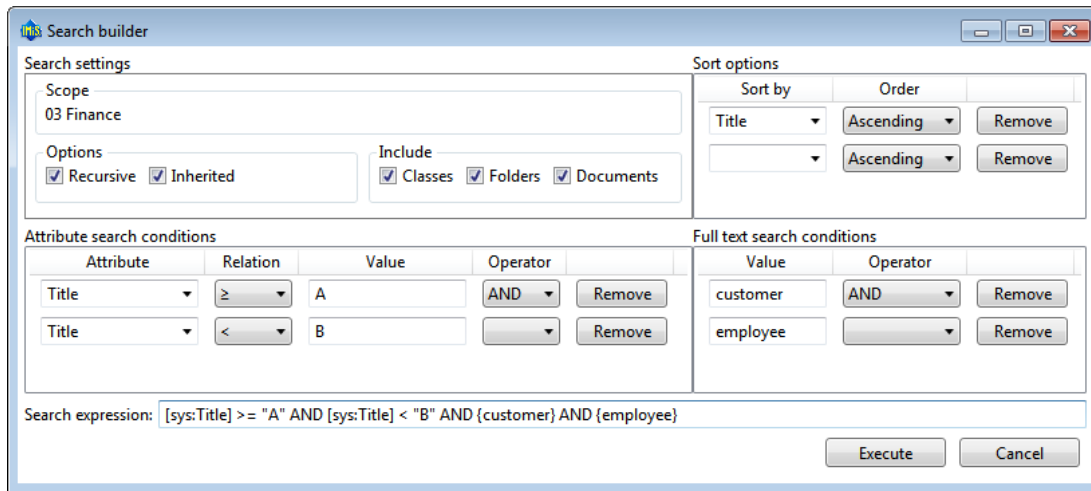


Image 84: Setting search parameters via the dialog box

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«.

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 *(see the IMiS®/ARChive Server user manual chapter 3.5.2 Search string rules)*.

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.
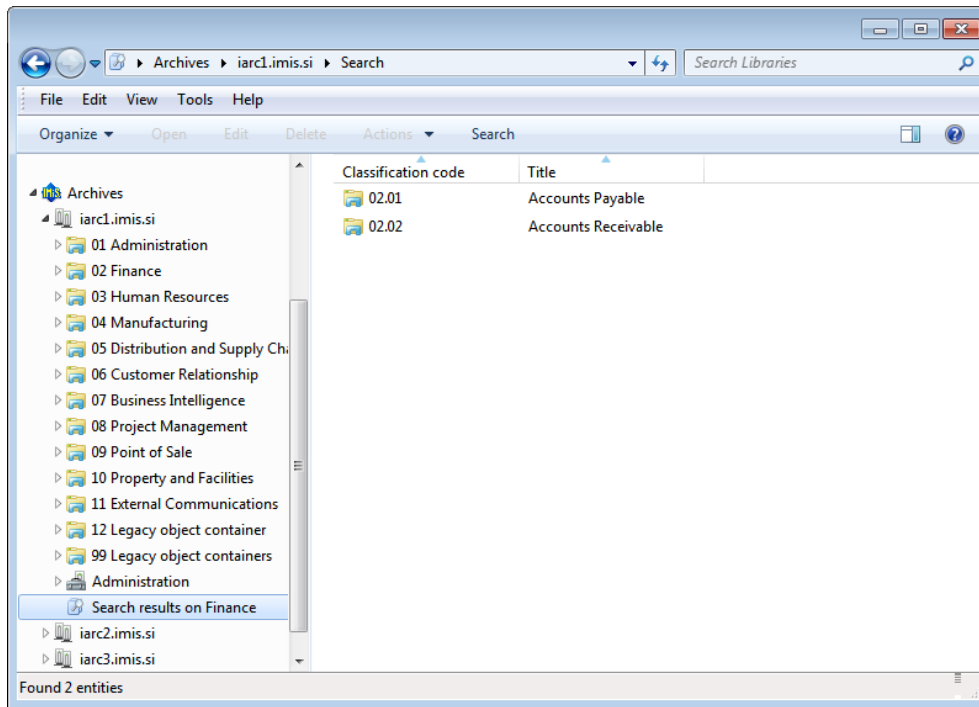


Image 85: Display of search results in the right view of Windows Explorer

### 4.2.6.1    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«.

- »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.

#### 4.2.6.1.1   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 86: Sample search string for searching by title of the content

List of entities that shows the matching search results.

| Classification code | Title | Content descriptions |
|---|---|---|
| 02-2015-00001/00001 | Business reports | Business report_2013.xltx; Business report_2014.xlsx |
| 02-2015-00001/00002 | Agreements | Employment Agreement.docx; Equity Transfer Agreement.docx; Manufacturing Agreement.docx |

Image 87: Results of searching by title of the content

### 4.2.6.2   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.

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 4.2.6.1  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).

### 4.2.6.3   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«.

### 4.2.7   Editing entity data

Changing 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.
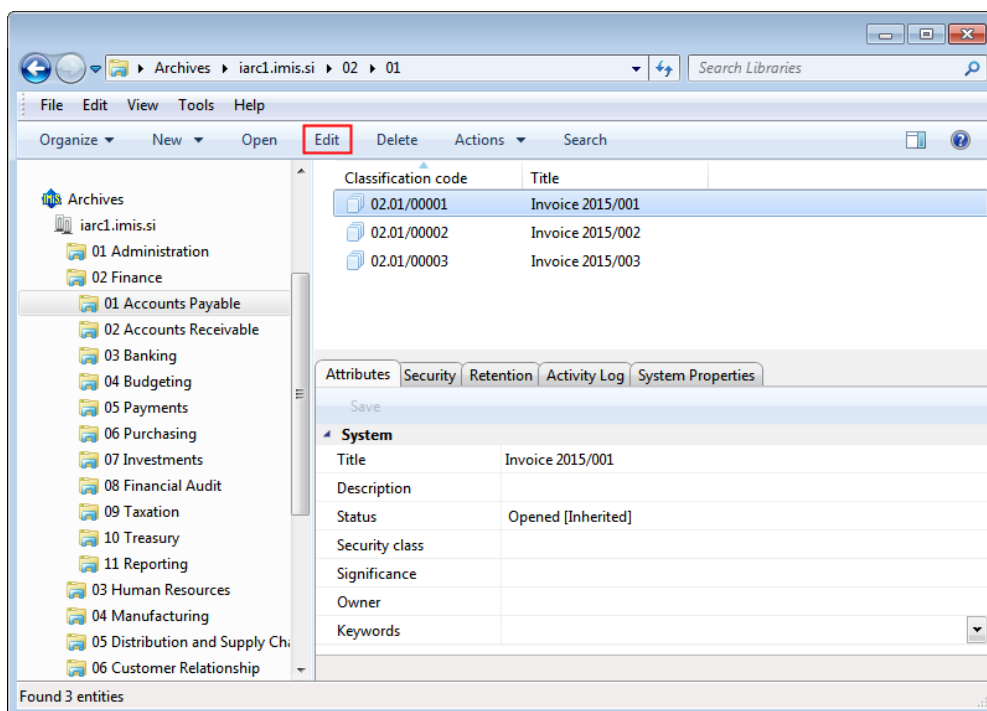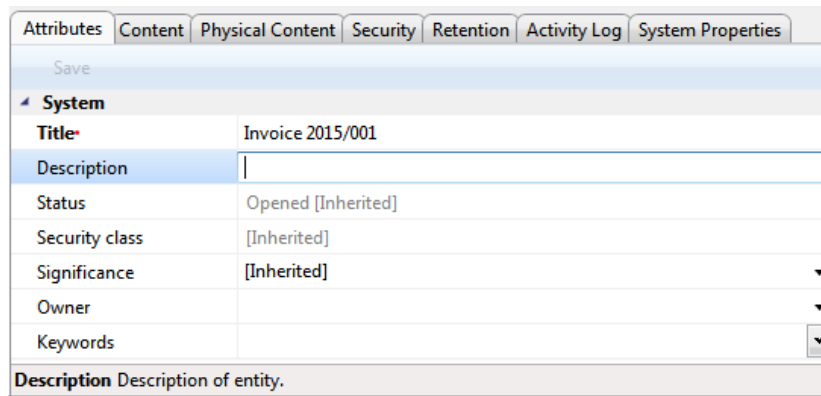


Image 88: Editing an entity via the command bar

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.

Image 89: Entering or editing entity metadata

Changes to an entity also involve the adding *(see chapter 4.2.2 Document capture)*, deleting and modifying of the entity's content. The user performs these actions through the »Content« tab.
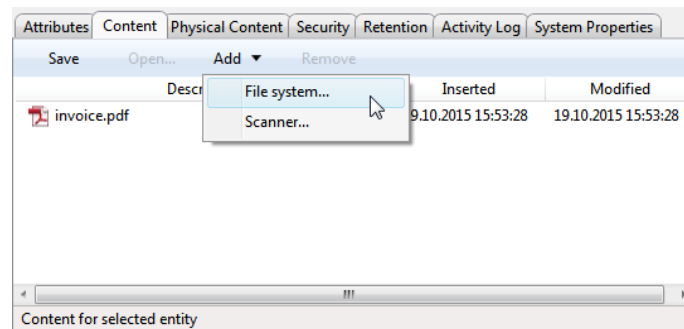


Image 90: Adding content to an entity via the file system

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 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.

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



Image 91: Opening the entity in editing mode.

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



Image 92: Opening content in the default application.

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.
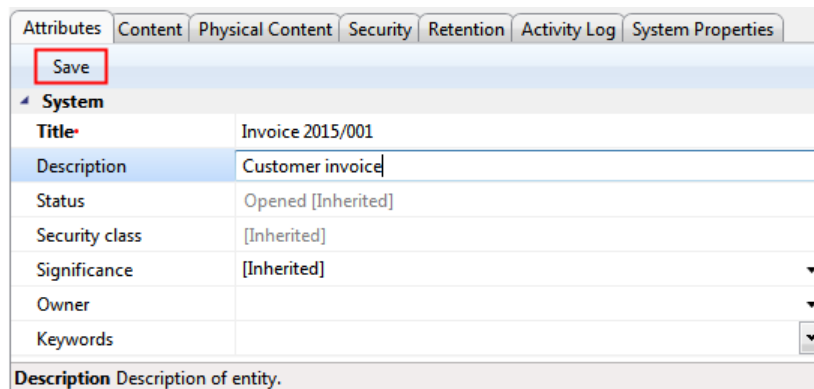


Image 93:  Display of the modified content after modification in the default application
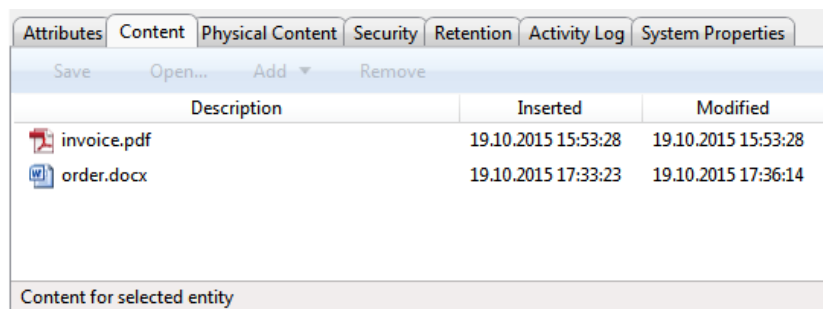
Changes to the entity are confirmed using the »Save« command in the bottom command bar.
If you wish to discard changes, simply select another entity and click »Don't save« in the save
prompt.



Image 94: Saving changes to the entity

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



Image 95:  When saving the modified content, the »Modified« date is also changed

### 4.2.8   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 *(see chapter 4.3.6  Email attributes)*.

### 4.2.8.1   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.

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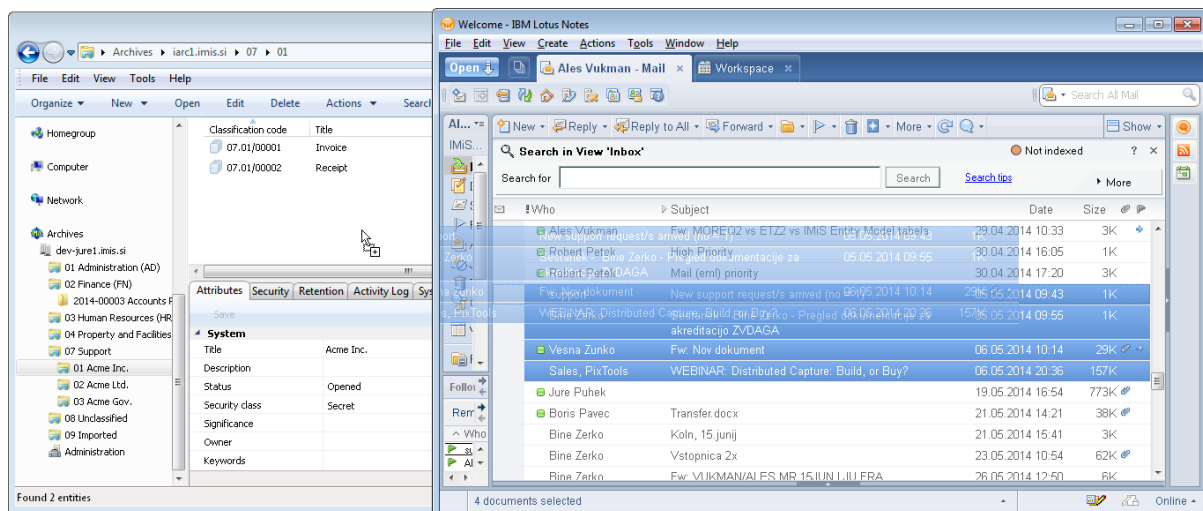


Image 96:  Transferring email messages from the email client to the selected class

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.
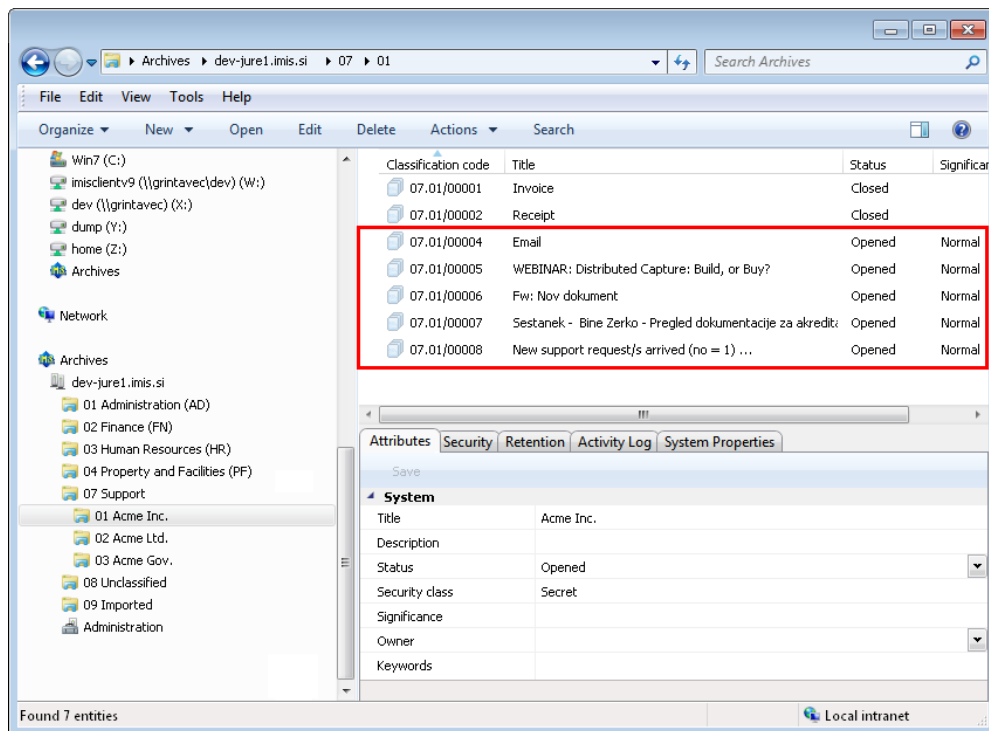
Image 97: Display of transferred email messages

*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.
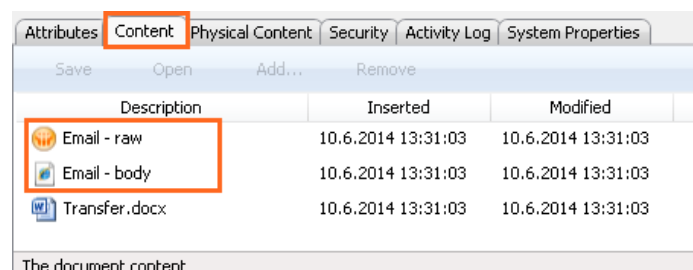


Image 98: Automatically created email attachments

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

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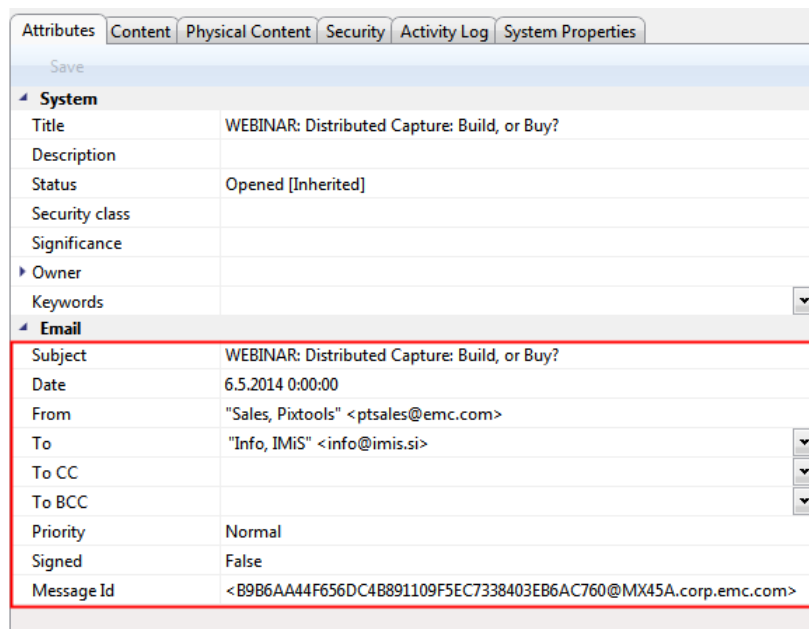
The selected email messages are copied to the specified location in the classification scheme, in the form of an EML file. For each email message, the IMiS®/Client creates a new document containing the original message, the metadata and any captured content.

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.



Image 99: Example metadata extracted from an email message

### 4.2.9   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.

If you want to perform the entry of physical content metadata during capture (*see chapter 4.2.2  Document capture*) or later on, select the »Physical Content« tab. Find the appropriate class or folder in the classification scheme (*see chapter 4.1.1 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 (*see also chapter 4.1  Interface description*).
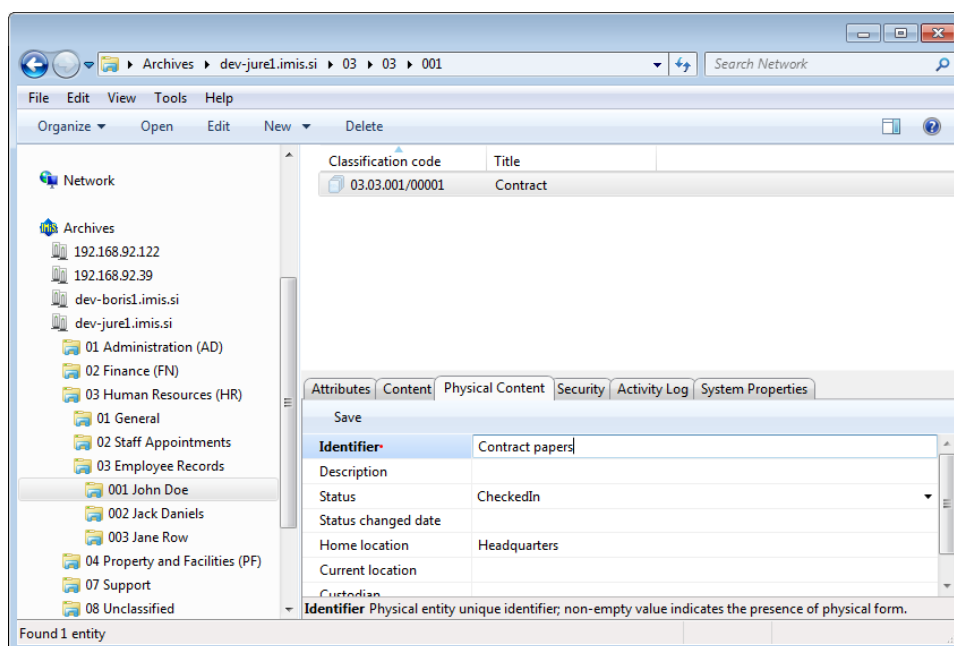


Image 100: Display of entering physical content metadata

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 a description of physical content metadata *see chapter 4.3.7  Physical content attributes*.

## 4.2.10  Print

Printing functionalities are divided into:

- Printing the content of a document.

- Performing print functions via the popup menu.


### 4.2.10.1   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.


Select the archive server in the left view of Windows Explorer and locate the folder containing

the content you wish to print.
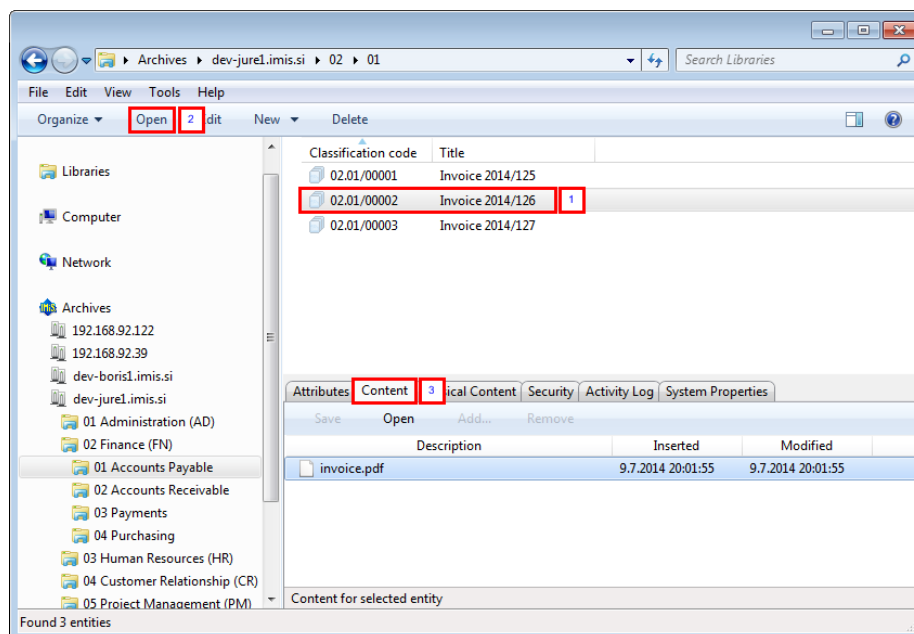


Image 101: Access to the content of a selected document


In the top right view, select the document (number 1 in the above image). 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 (number 2 in the image above) 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 (number 3 in the image above).
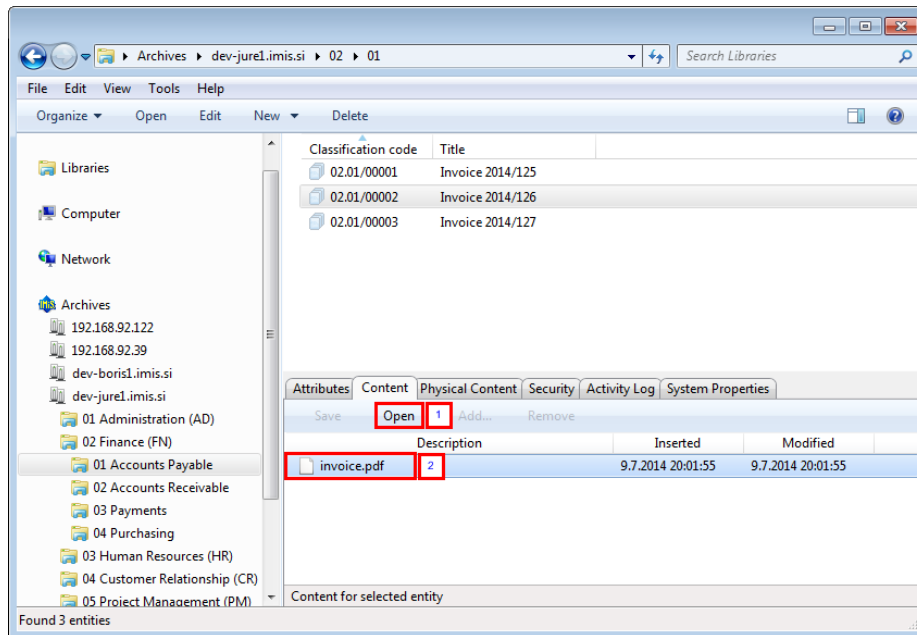
Image 102: Opening the content »invoice.docx« in its default application MS Word

The selected content (number 2 in the image above) is opened in the default application for the corresponding content type by choosing the »Open« command in the top command bar (number 1) or by double clicking. Once the application is open, you can print the content. Repeat this procedure for all content in the document.

### 4.2.10.2  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.
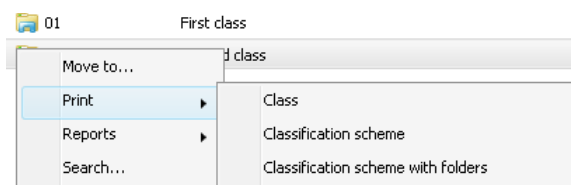


Image 103: Selecting print options via the popup menu

### 4.2.10.3 Printing metadata, document security settings and properties

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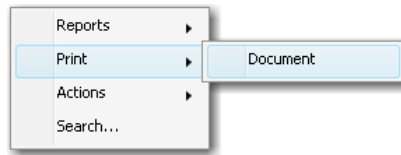


Image 104: Selection of metadata print options for the chosen document

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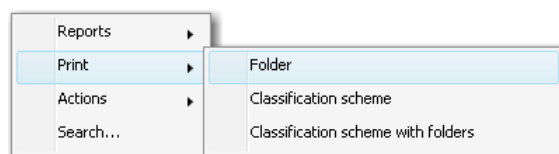


Image 105: Selection of metadata print options for the chosen folder

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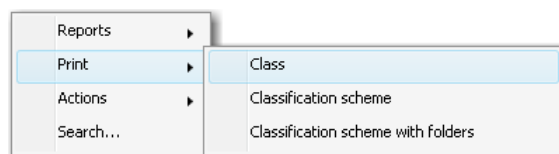


Image 106: Selection of metadata print options for the chosen class

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.*
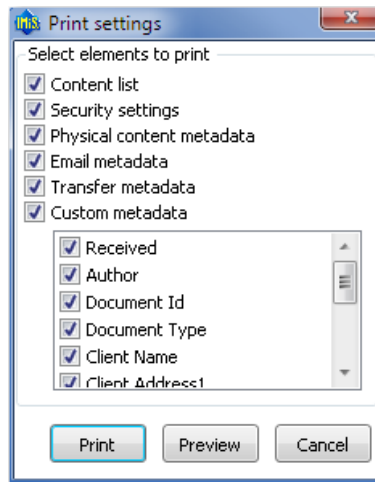
Image 107: Print settings dialog box

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.

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.
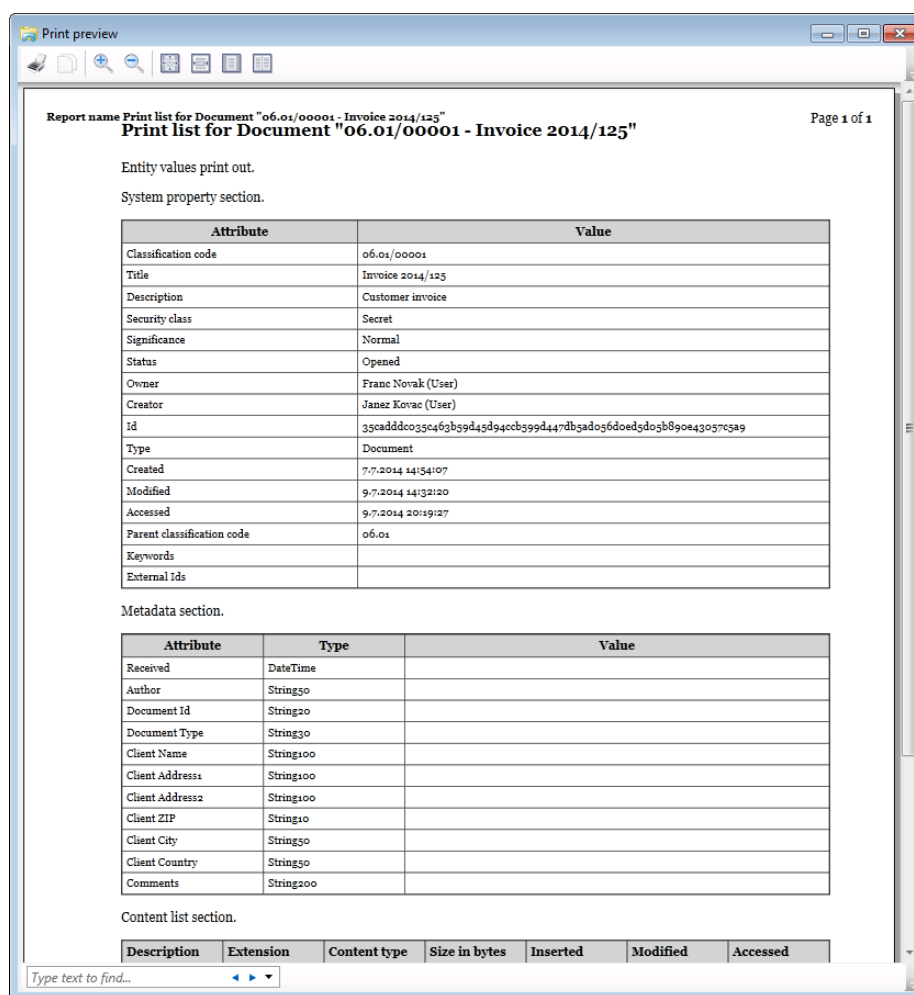
Image 108: Example document print preview

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.
- 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.

### 4.2.10.4 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«.
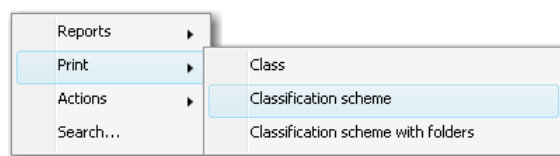


Image 109: Selection of classification scheme printing options

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

Image 110: Example classification scheme print

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

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

### 4.2.10.5  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 111: Selection of classification scheme printing options

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



Image 112: Example classification scheme with folders print from the preview

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

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

### 4.2.10.6  Printing retention periods of the review process

Prior to printing, the user selects the review under which he will be printing the retention periods.

Each review created is located in the »Reviews« folder contained in the »Administration« system folder. This folder can only be accessed by users who have been assigned the »Review« role. For more information on roles *see chapter 4.3 Roles*.

By right-clicking on the selected review, the user is shown a pop-up menu. The user selects the »Print - Retention policies« command.
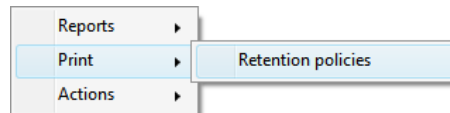
Image 113: Selecting the option of printing retention periods

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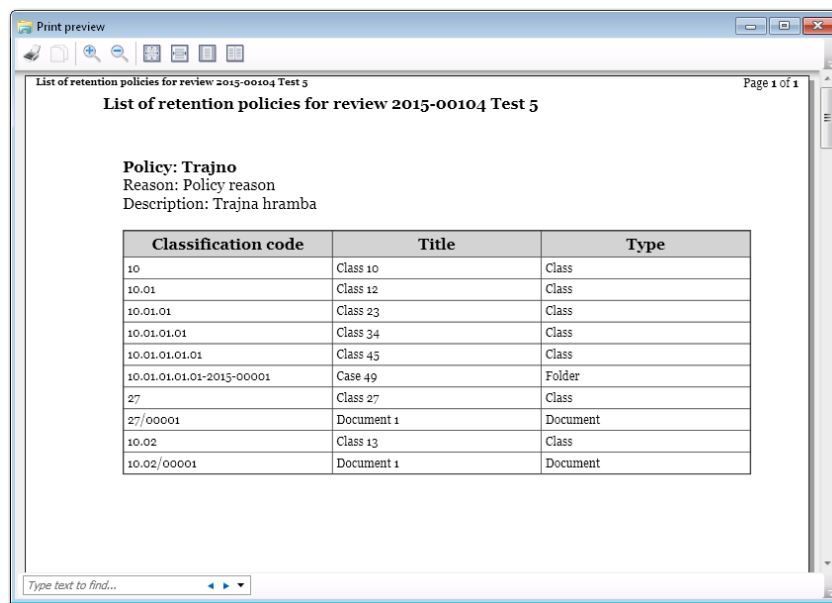


Image 114:  Example of printing selected entities classified by retention policies

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 longer description of the retention period.

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

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

## 4.2.11  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 3.2  Format of the import / export file*. More info on server roles / permissions is found *in the IMiS®/ARChive Server manual chapter 3.3.5  Access*.

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).
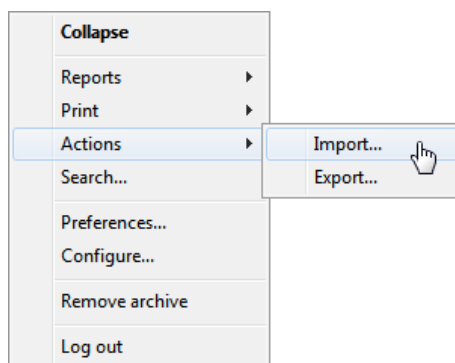


Image 115: Importing content via the popup menu

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«.
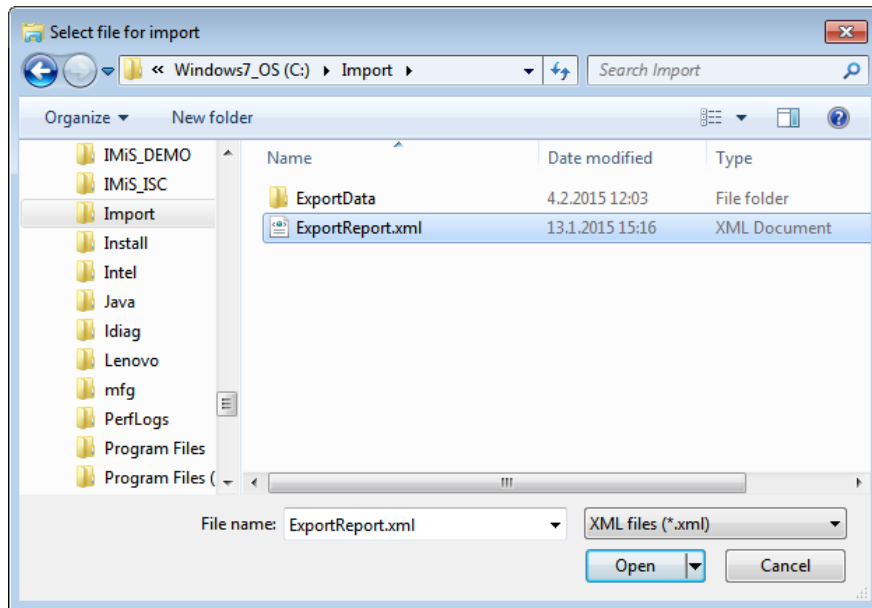
Image 116: Selection of the XML import list

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.
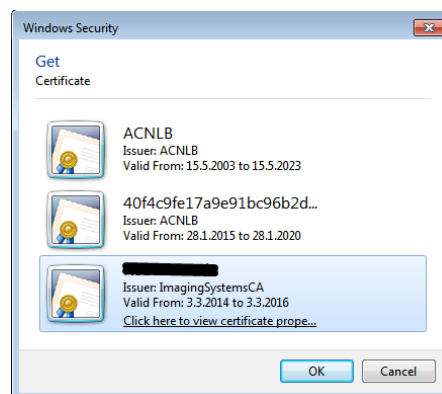


Image 117: Selecting a digital certificate when importing

*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.
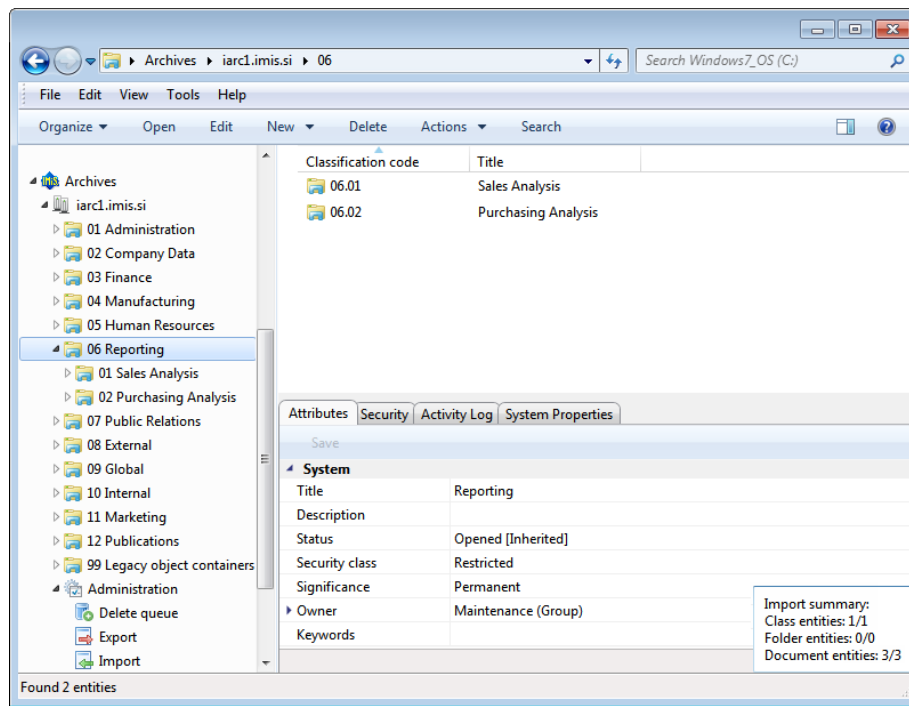


Image 118: Display of the import complete message with success rate statistics

### 4.2.11.1   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.

- »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.
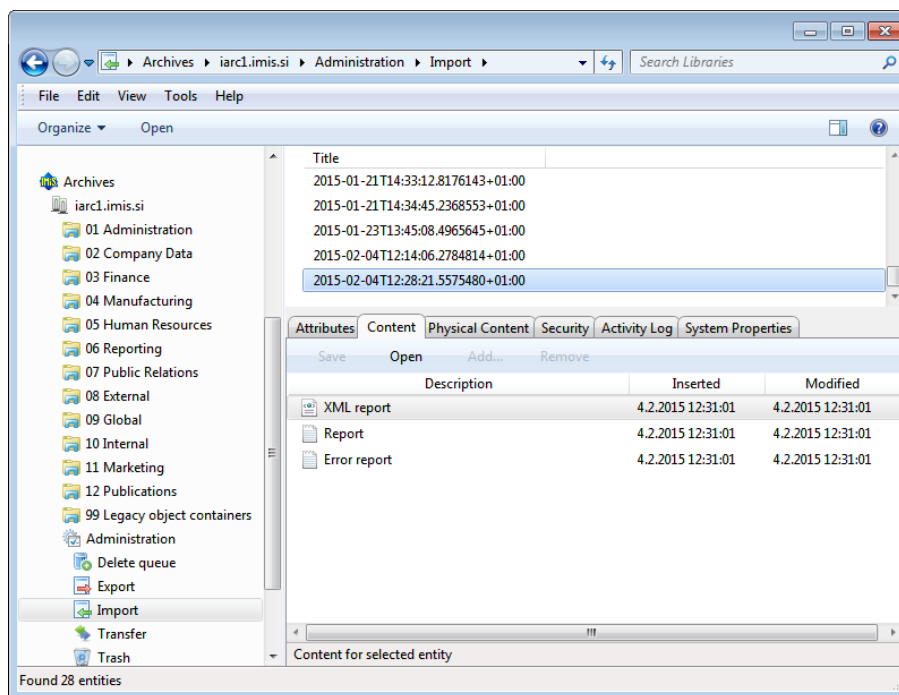


Image 119: Display of the import report in the »Import« system folder

### 4.2.12 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 3.2 Format of the export / import file*.

For more information on server roles *see the IMiS®/ARChive Server user manual chapter 3.3.5 Access*.

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).
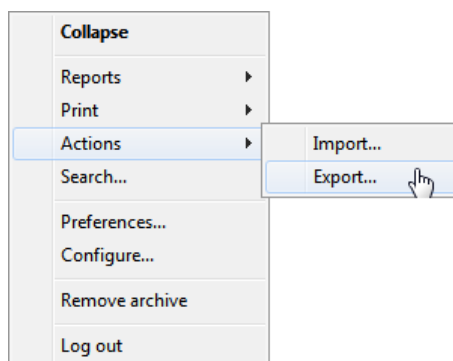


Image 120: Exporting records via the popup menu

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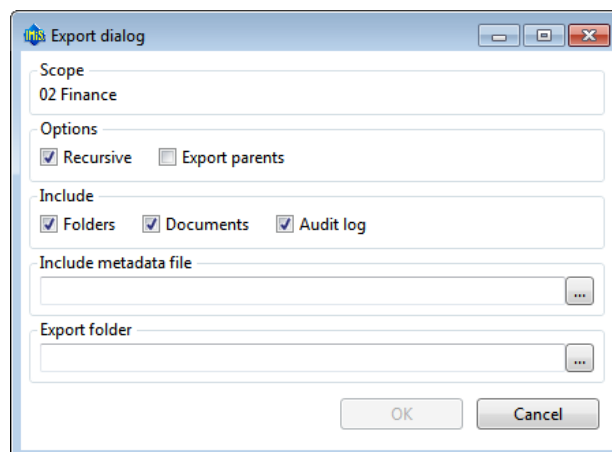


Image 121: Export settings in the dialog box

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 3.2.3  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.

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.
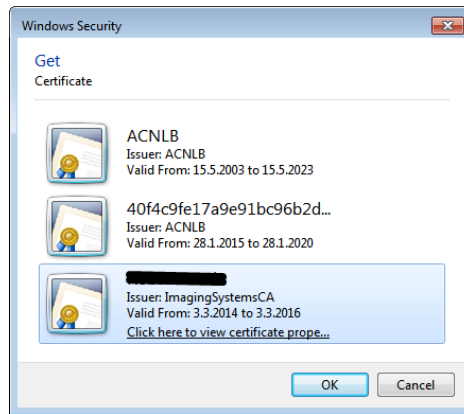
Image 122: Selecting a digital certificate when exporting

_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.
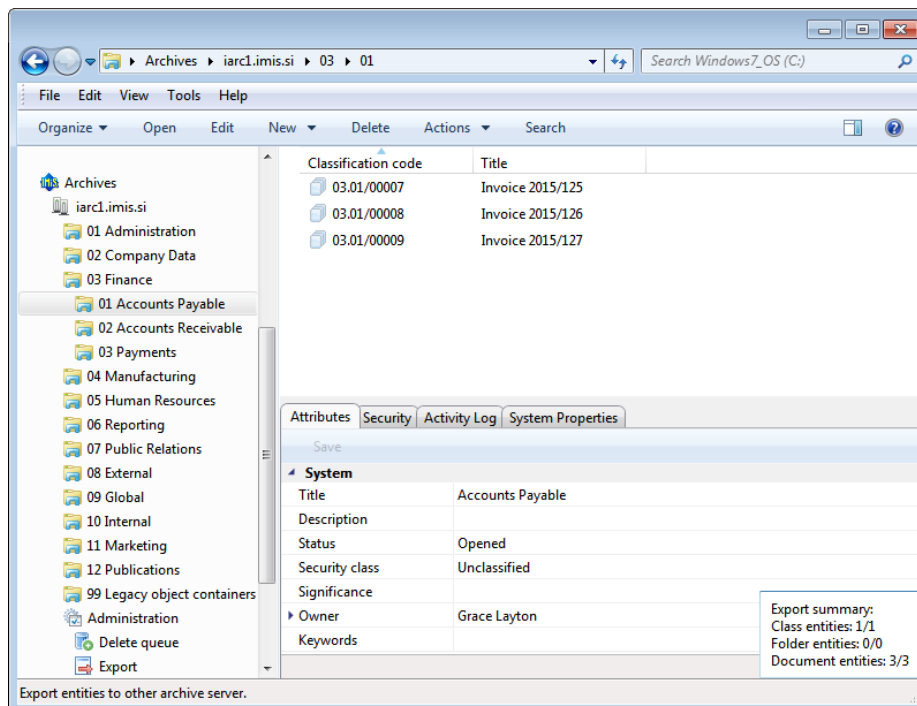


Image 123: Display of the export complete message with success rate statistics

*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.*

### 4.2.12.1  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.

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.
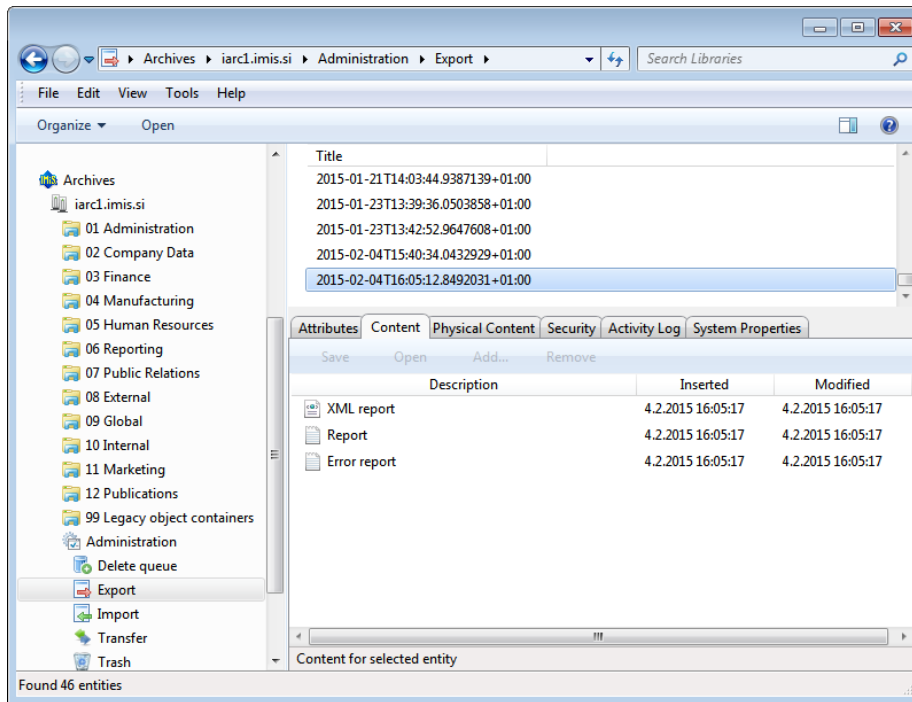
Image 124: Display of the export report in the »Export« system folder

### 4.2.13 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.
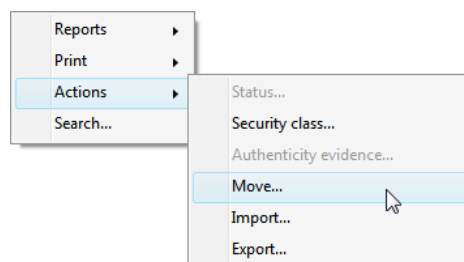


Image 125:  Popup menu where the »Move« command is found

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.
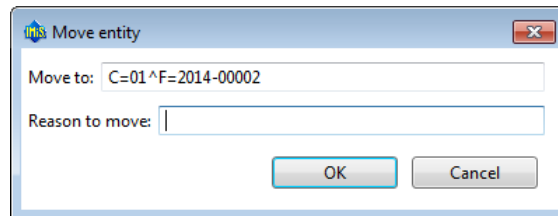


Image 126: Move entity dialog box

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 2014-01, which is located inside class 002, which is located inside class 01 looks like this: C=01^C=002^F=2014-01^D=0001*

For more information on classification codes in canonical form *see the IMiS®/ARChive user manual chapter 3.3.5  Access*.

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 (*see chapter 4.3.3 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.*

## 4.2.14  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).

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

### 4.2.14.1  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 4.1.3  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«).*
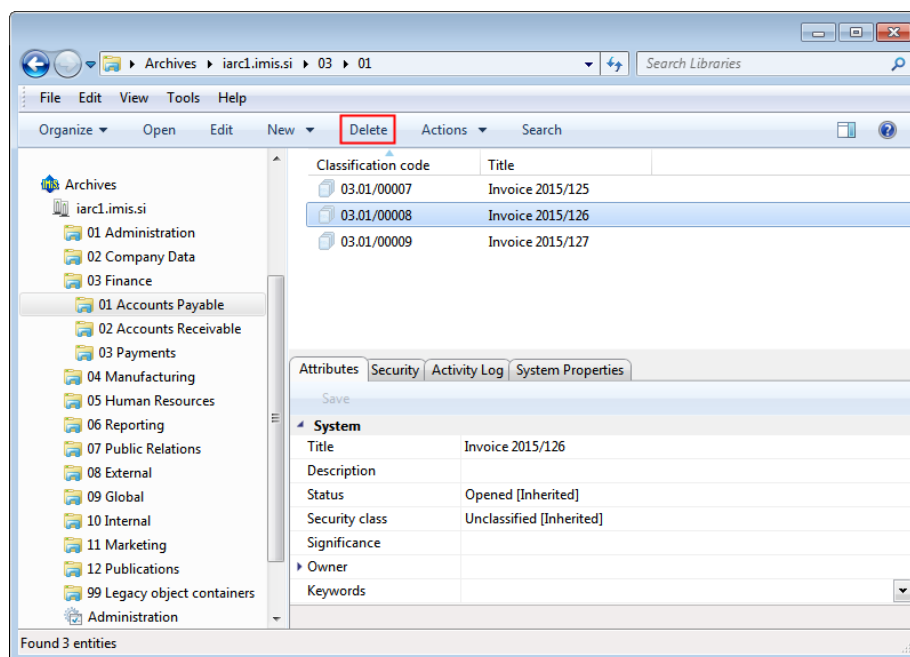


Image 127: Deleting an entity via the command bar

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.
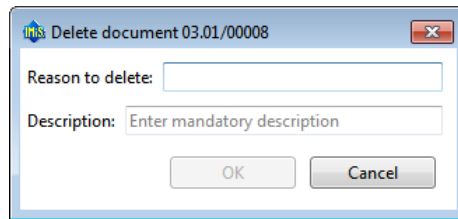


Image 128: Entity deletion dialog box

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.



Image 129: 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.

**4.2.14.2  Marking an entity for later deletion**

If the user has the »Write« access right on the entity, but does not have the »Delete« access right, user is able to mark the entity for later deletion, which will be performed by a user with the »Deletion« role on the server. For the display of a user's current effective access rights *see chapter 4.1.3  Entity information*.

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.
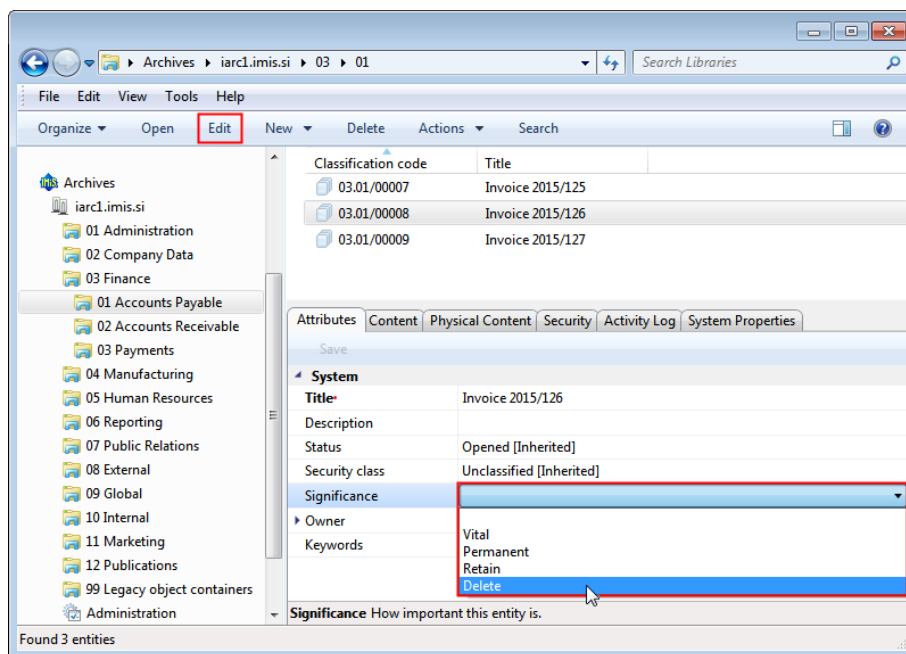


Image 130: Marking an entity for later deletion

**4.2.14.3  Managing the delete queue**

Entities whose »Significance« attribute is set to »Delete« appear in the list of entities waiting for deletion. This list is found in the »Queue« folder in the »Trash« folder in the »Administration« system folder. The »Trash« folder can only be accessed by users who have a »Deletion« role on the server.
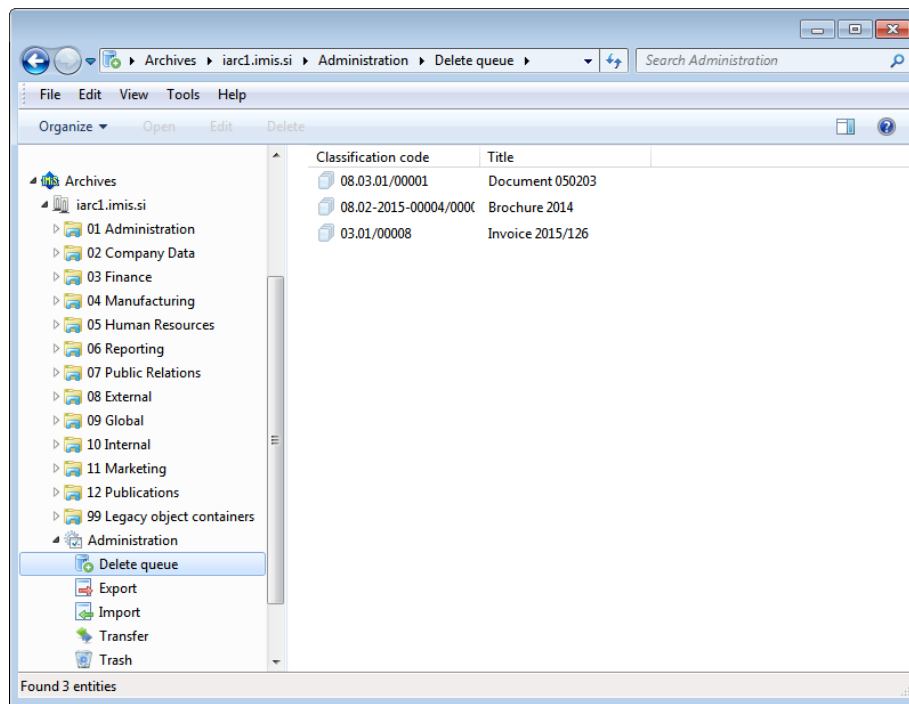
Image 131: List of entities marked for deletion in the »Queue« folder

More information on server roles is available in *the IMiS®/ARChive Server user manual chapter 3.3.5 Access*.

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 with a »Deletion« role on the server 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 4.2.14.1 Immediate deletion of an entity*.

If a user with a »Deletion« role on the server 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 with a »Deletion« role on the server 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.
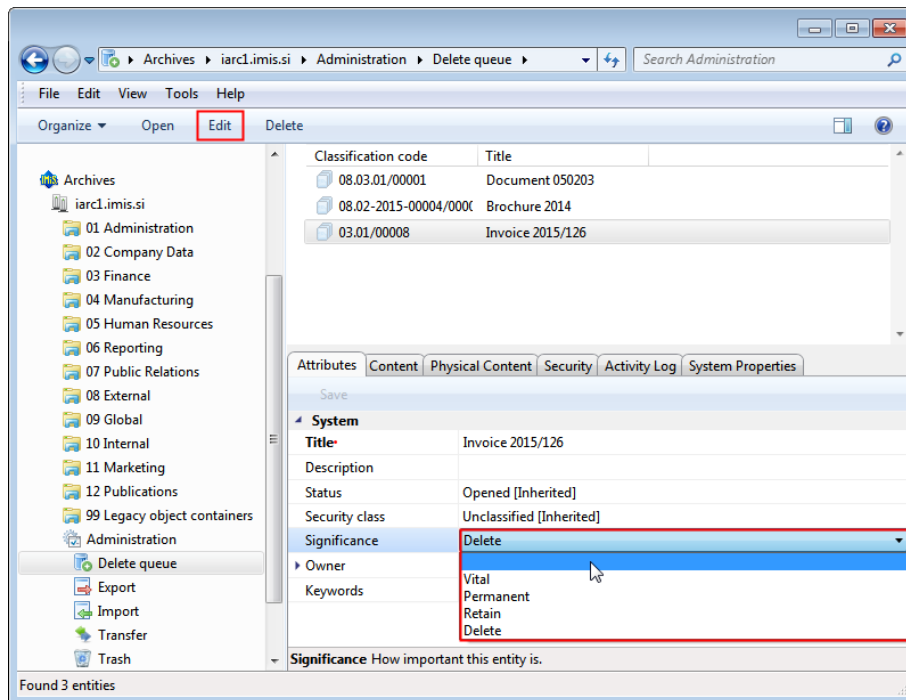


Image 132: Removing an entity from the delete queue list

Once you refresh the delete queue list, the entity will no longer appear there. You can still find it in its old location in the classification scheme.

### 4.2.15  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.
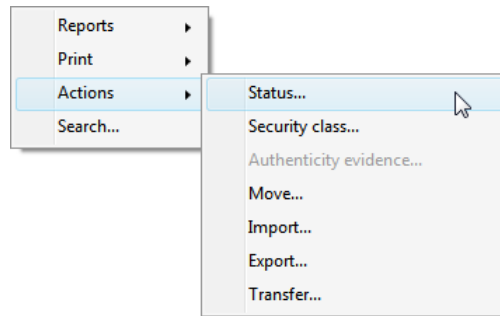
Image 133: Popup menu for choosing the »Status« command

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.
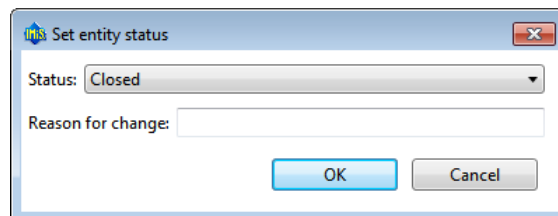


Image 134: Status change dialog box

### 4.2.16  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.
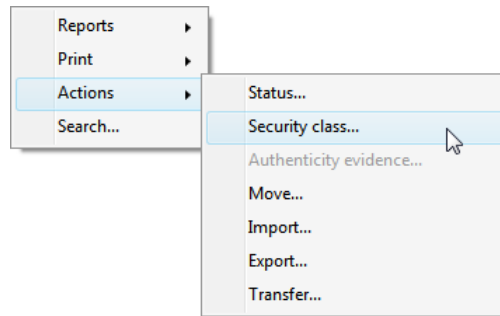
Image 135: Popup menu for choosing the »Security class« command

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.

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.
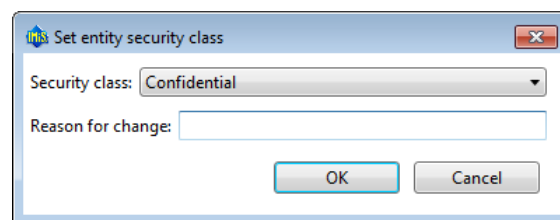


Image 136: Dialog box for changing the security class

### 4.2.17 Acquiring authenticity evidence

Authenticity evidence is created on the IMiS®/ARChive Server for those entities whose »Status« attribute value is changed to »Closed« by a user, and which contain at least one metadata or content intended for evidence creation.

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.
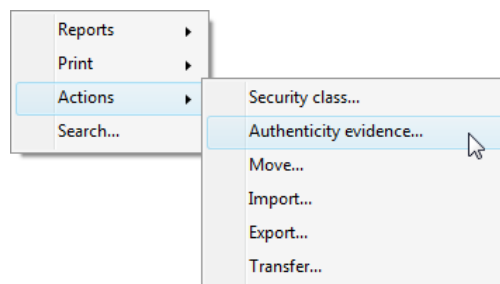


Image 137: Popup menu for choosing the »Authenticity evidence« command

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.
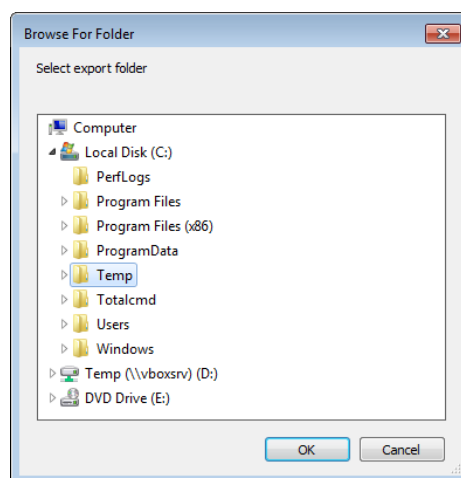


Image 138: Dialog box for selecting the export folder of authenticity evidence files

_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.

```xml
<?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:ContentId="sys:Content">
<aip:ContentValue>
<ds:DigestMethodAlgorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>0NPJp3qfSkFm...T5irpOT+SrJMp+VE=</ds:DigestValue>
</aip:ContentValue>
</aip:Content>
</aip:AIP>
```

Image 139: Example archive information package

```xml
<?xml version="1.0" encoding="UTF-8"?>
<EvidenceRecord xmlns="http://www.setcce.org/schemas/ers" Version="1.0">
<ArchiveTimeStampSequence>
<ArchiveTimeStampChain Order="1">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<ArchiveTimeStamp Order="1">
<HashTree>
<Sequence Order="1">
<DigestValue>RiHMqrhrGATA/fDYJVO2lVg4fTw=</DigestValue>
<DigestValue>dawWHxN2luddA7O+NGHYNd3ApG8=</DigestValue>
</Sequence>
<Sequence Order="2">
<DigestValue>vqBElqW7kGPUaFB/g6tfUFWwylE=</DigestValue>
</Sequence>
</HashTree>
<TimeStamp>
<TimeStampToken Type="XMLENTRUST">
<dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Id="TimeStampToken">
<dsig:SignedInfo>
```

```
<dsig:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<dsig:Reference URI="#TimeStampInfo-13ED106F54C2C33ED420000000000007BD7">
<dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<dsig:DigestValue>fWwSCkWO4udY+/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>7949411139179750976</ts:Nonce>
</ts:TimeStampInfo>
</dsig:Object>
</dsig:Signature>
</TimeStampToken>
<CryptographicInformationList>
<CryptographicInformation Order="1" Type="CERT">
MIIEHDCCAwSgBAgIE... z9Oz6gk/2vorAfGEhuB9nBxVeoQp
</CryptographicInformation>
<CryptographicInformation Order="2" Type="CRL">
MIISKTCCERECAQEwDQYJ.... pYO2SYQMkw819LR9I/YOFg
</CryptographicInformation>
</CryptographicInformationList>
</TimeStamp>
</ArchiveTimeStamp>
</ArchiveTimeStampChain>
</ArchiveTimeStampSequence>
</EvidenceRecord>
```

Image 140: Example evidence record

## 4.2.18  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.
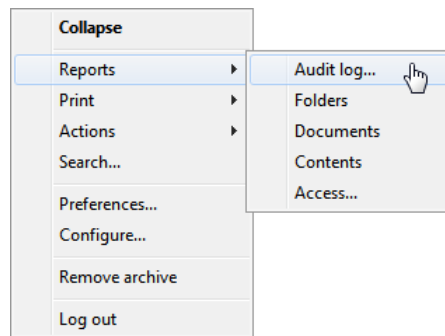
Image 141: Popup menu for selecting the »Audit log« command

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«.

- »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.
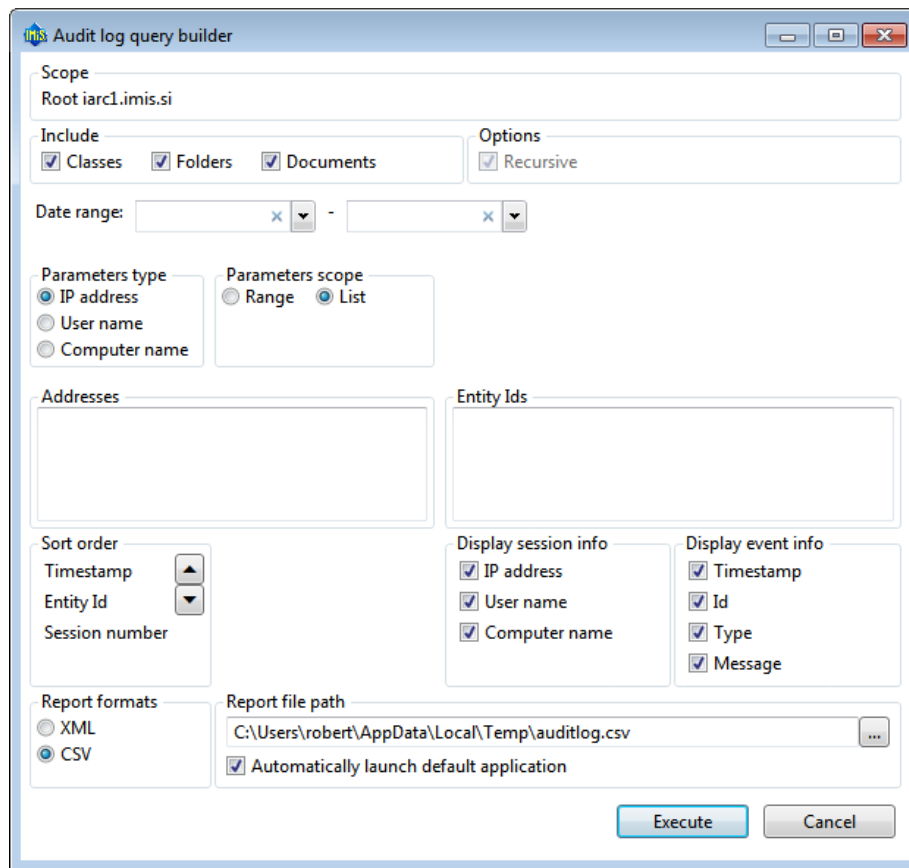
Image 142: Configuring the audit trail query

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

## 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 publically 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.

### 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.<br><br>*Example:*  *The classification code 01-2014-00004/00001 represents document 00001, located inside folder 2014-00004, located inside class 01. The classification code is a publically 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. |

| Name | Description |
|---|---|
| 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. <br>The possible values are:<br>• »Opened«: the entity can be edited by a user with the appropriate effective access rights (the right to write)<br>• »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:<br>• »Vital«: entity is vital.<br>• »Permanent«: entity is permanent.<br>• »Retain«: entity should be retained.<br>• »Delete«: entity is queued for deletion. |
| Security class | Saves/contains the security class of the entity. The security class is optional metadata for all new entities. Once it is set, it cannot be modified without stating a reason for change. The security class is a public metadata that enables inheriting and enables search. <br>The possible predefined values are:<br>• »Unclassified«: entity is freely accessible.<br>• »Restricted«: entity is of an internal nature. Can only be accessed by users with clearance level »Restricted« or higher.<br>• »Confidential«: entity is confidential. Can only be accessed by users with clearance level »Confidential« or higher.<br>• »Secret«: entity is secret. Can only be accessed by users with clearance level »Secret« or higher.<br>• »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. |

| Name | Description |
|------|-------------|
| 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. <br> The possible values are: <br> • »Opened«:  the entity can be edited by a user with the appropriate effective access rights (the right to write). <br> • »Closed«:  the entity cannot be edited. |
| External Ids | Saves/contains external identifiers of the entity. This attribute can have multiple unique values and is a public metadata that enables search. <br><br> _Warning:  When entering values, keywords should be separated using the »Enter« key or the semicolon character ( ; )._ |
| Save  log | Contains a report on the verification of the electronic signature for digitally signed content. This attribute can have multiple, added values. It is a public metadata that enables search |

Table 7:  Description of general system attributes

### 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

### 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.

| 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: <br><br> - »CheckedIn«: the physical content is stored at its home location. <br><br> - »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. <br> Valid values: <br><br> • »Reviewing«: the value represents the action of reviewing entities in the review process and does not influence the server. <br><br> • »Complete«: the value represents the action of completing the review process on the server. <br><br> • »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. <br> In the event of an error during the preparation or implementation phase of the review process. Also recorded in the attribute is the successful completion of the review process. |

| Name | Description |
|------|-------------|
| State | This value is set by IMiS®/ARChive Server during the review process.<br>Valid values:<br>• »Unknown«: this value represents an invalid state of the review process.<br>• »Created«: this value is set by the server when the user creates a new review.<br>• »Preparing«: this value is set by the server during the content creation phase for the review process.<br>• »InReview«: this value is set by the server after successfully creating the entities for the review process.<br>• »Completing«: this value is set by the server when beginning of the review process.<br>• »Completed«: this value is set by the server after successfully implementing the review process.<br>• »Discarded«: this value is set by the server after successfully canceling the review process.<br>• »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.<br>This value is copied from the effective retention policy. |
| Comment | Contains a random comment which is entered during the transfer process. |
| Transfered | This attribute value states whether the entity transfer was successful or not.<br>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

## 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.

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.

### 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. 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.
*(see the IMiS®/Scan and IMiS®/View user manual chapter 6.21 Electronic signatures)*.

### 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.
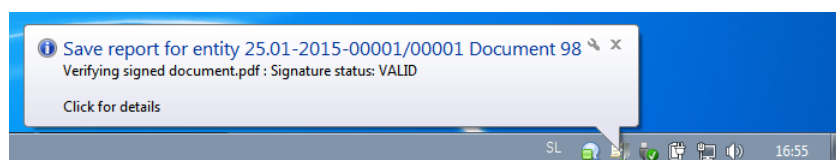


Image 143:  Example of a pop-up window containing the result of the document's electronic signature verification.

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.
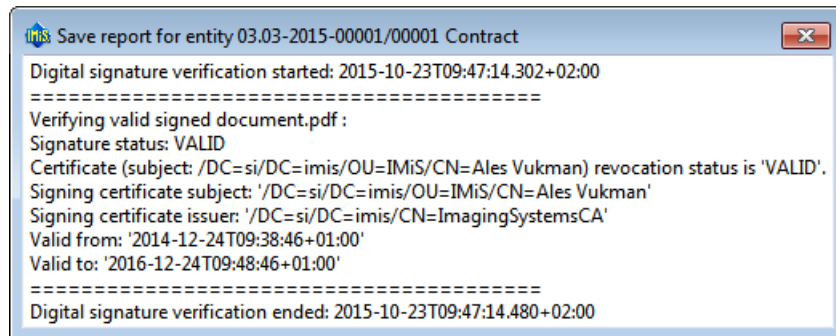


Image 144: Example of a report for a valid electronic signature of a document
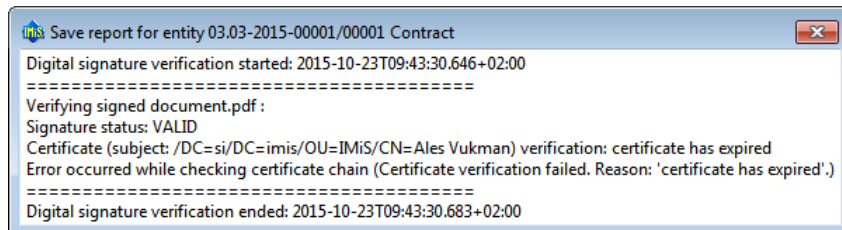


Image 145: Example of a valid electronic signature and an expired digital certificate
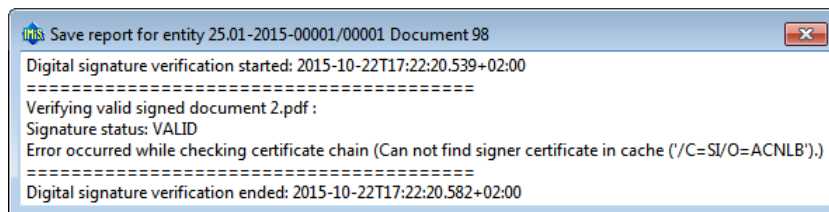


Image 146: Example of a valid electronic signature
for which the certification authority could not be verified.
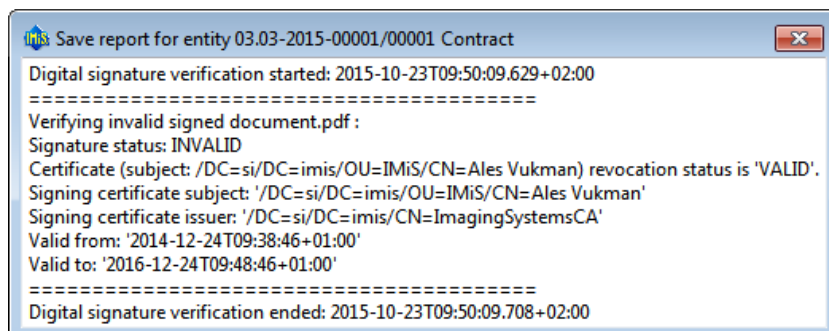


Image 147: Example of an invalid electronic signature due to a modification of the document after signing.

## 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.
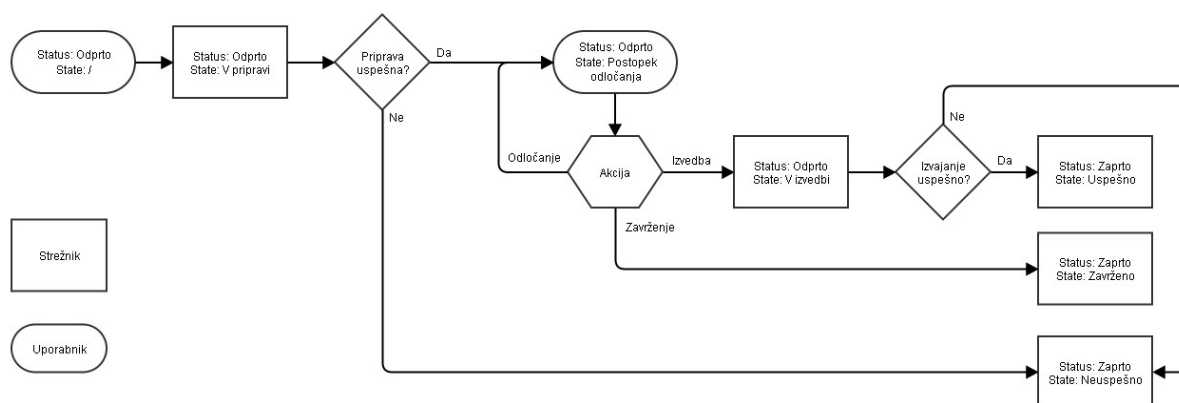


Image 148: Schematic of the review process

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.

The review process can be implemented by users with the »Review« role and the appropriate access rights for reviewing. These access rights are set by the administrator when setting the access rights in the »Configure« interface and the »Reviews« context.

*More information on roles is available in the chapter 3.3.5.2.4 Roles in the IMiS®/ARChive Server user manual.*

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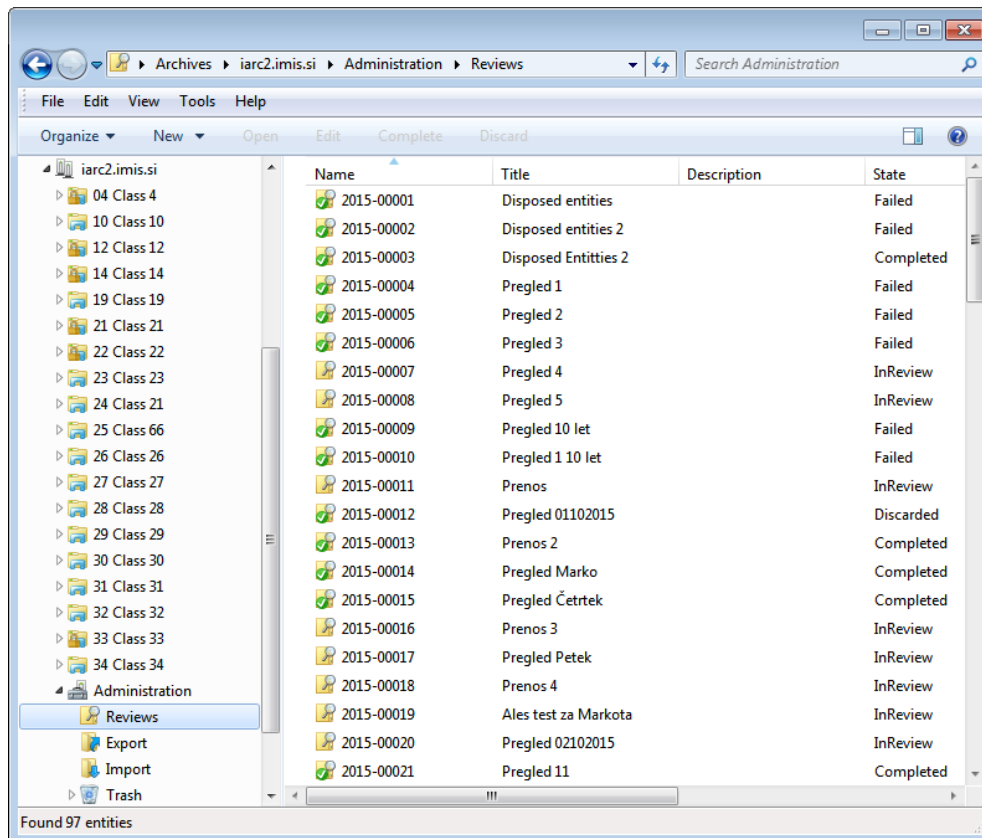


Image 149:  Display of reviews created in the review processes

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.
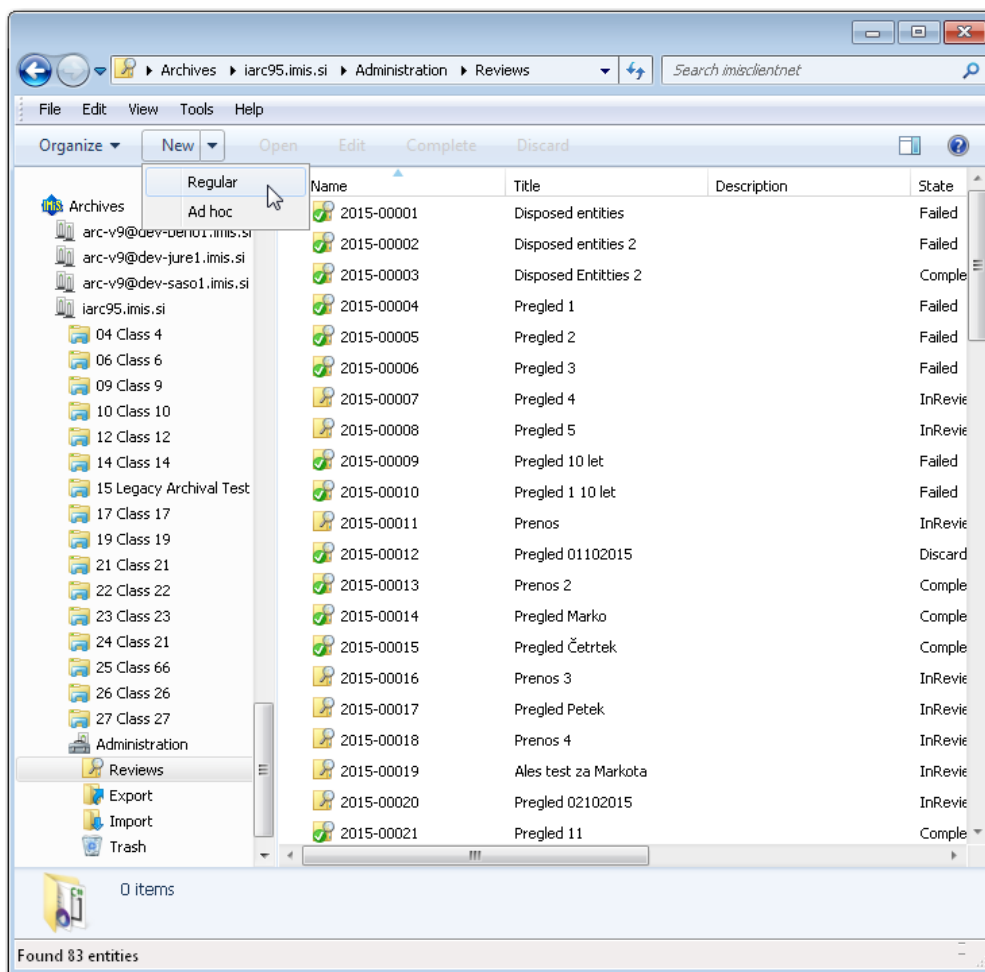
Image 150:  Creating a new regular review in the preparation phase

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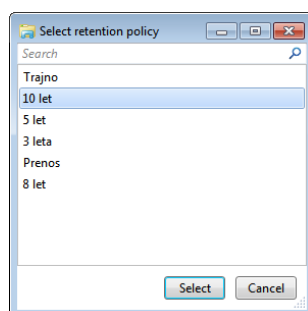


Image 151:  Dialog box for selecting retention periods

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 152:  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 4.2.6. Search functions*.
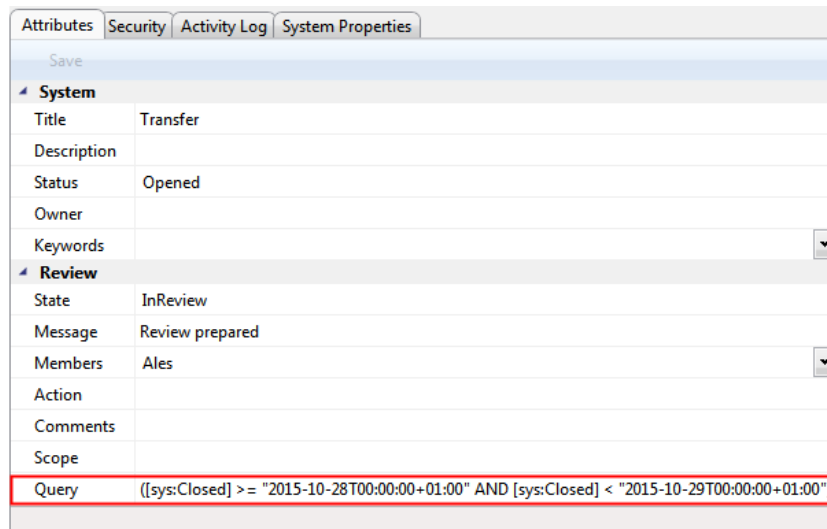


Image 153:  Example of creating a list of entities which were closed on a specific date

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 154:  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 4.2.2.2 Entry of metadata*.

The list of attributes is divided into several categories:
- »System«:  attributes are present on all entities.
  *See chapter 4.3.1  General system attributes*.
- »Review«:  attributes are present only when the entity is undergoing the review process.
  *See chapter 4.3.8  Review process attributes*.

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 155:  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.

*Problems:  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 the chapter 3.7.4 Filtering process in the IMiS®/ARChive Server user manual.*

While the review process is in the preparation phase, it cannot be modified.

During that time its »State« attribute shows the »Preparing« value.

Image 156:  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.
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.
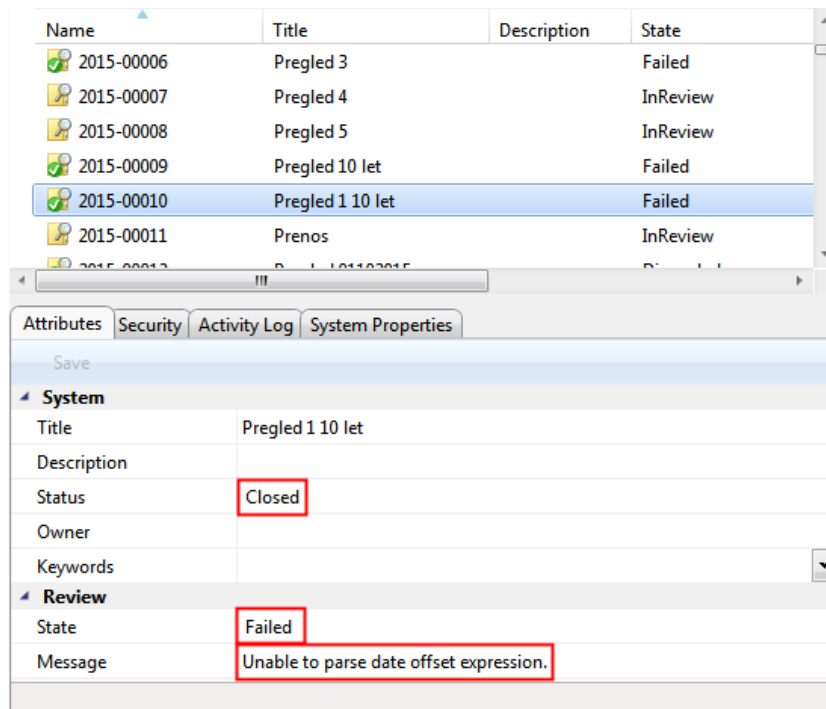
Image 157:  Display of an error which occurred during the preparation phase of the review process

### 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 who have been assigned the »Review« role.

*More information on roles is available in the chapter 3.3.5.2.4 Roles in the IMiS®/ARChive Server user 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.
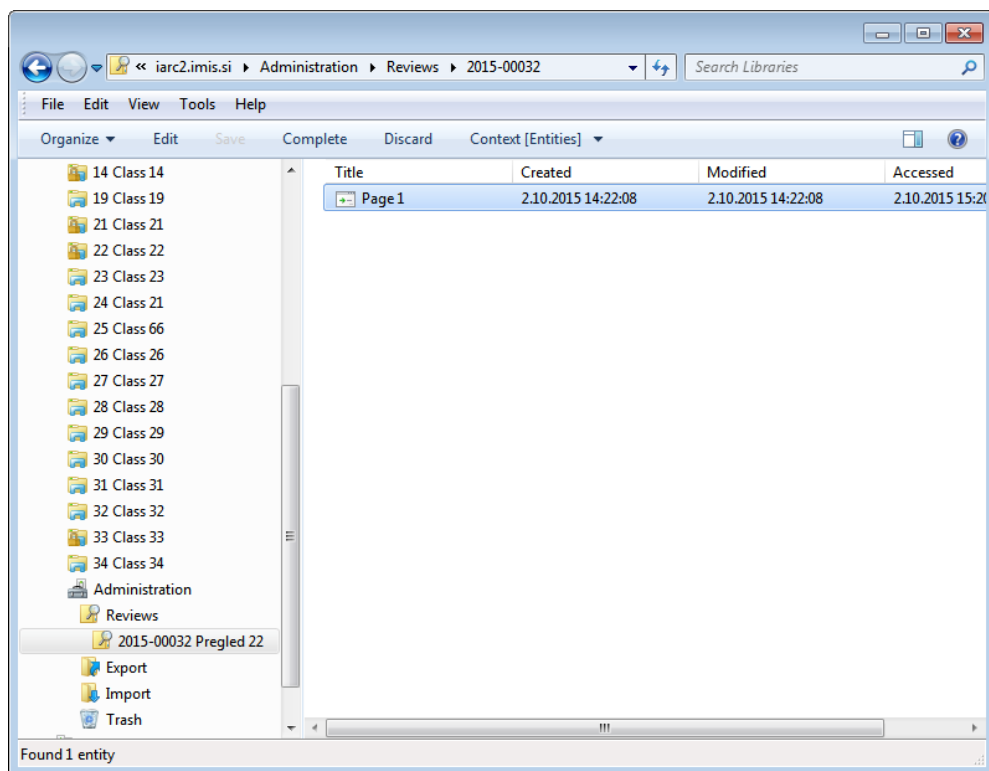
Image 158:  Display of the review page

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.

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.
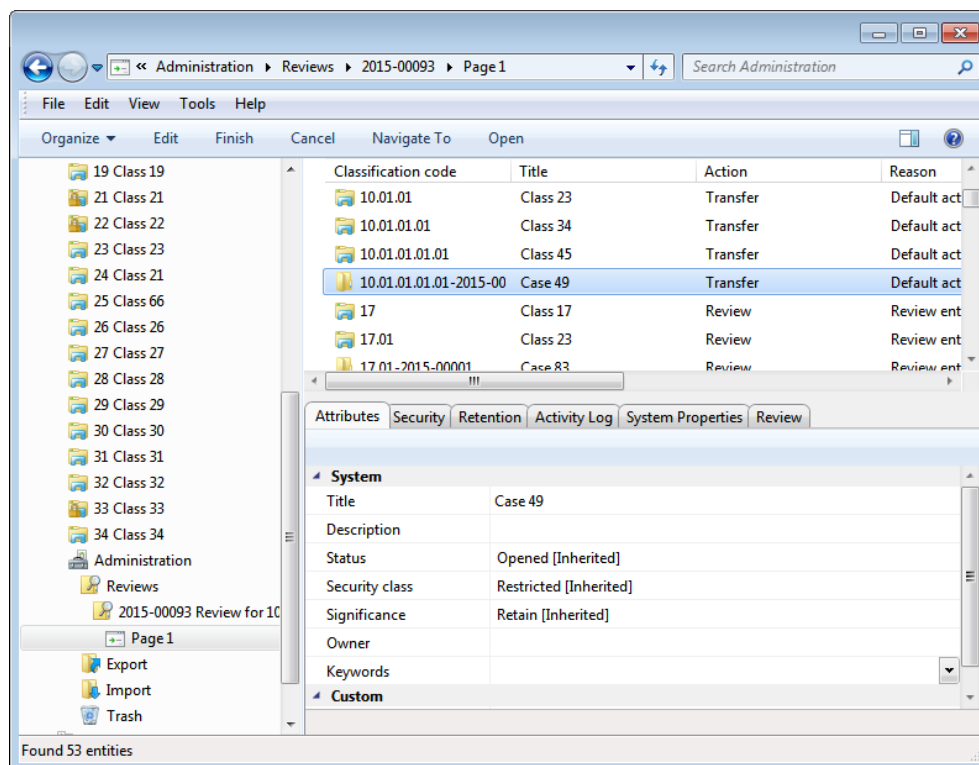


Image 159:  Display of entity tabs during the decision-making process

An entity which is included on the list of an individual review page has the following tabs:

- Attributes  *(see chapter 4.3.1 General system attributes)*.

- System Properties  *(see chapter 4.3.1 General system attributes)*.

- Review *(see chapter 4.3.9 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.


### 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.
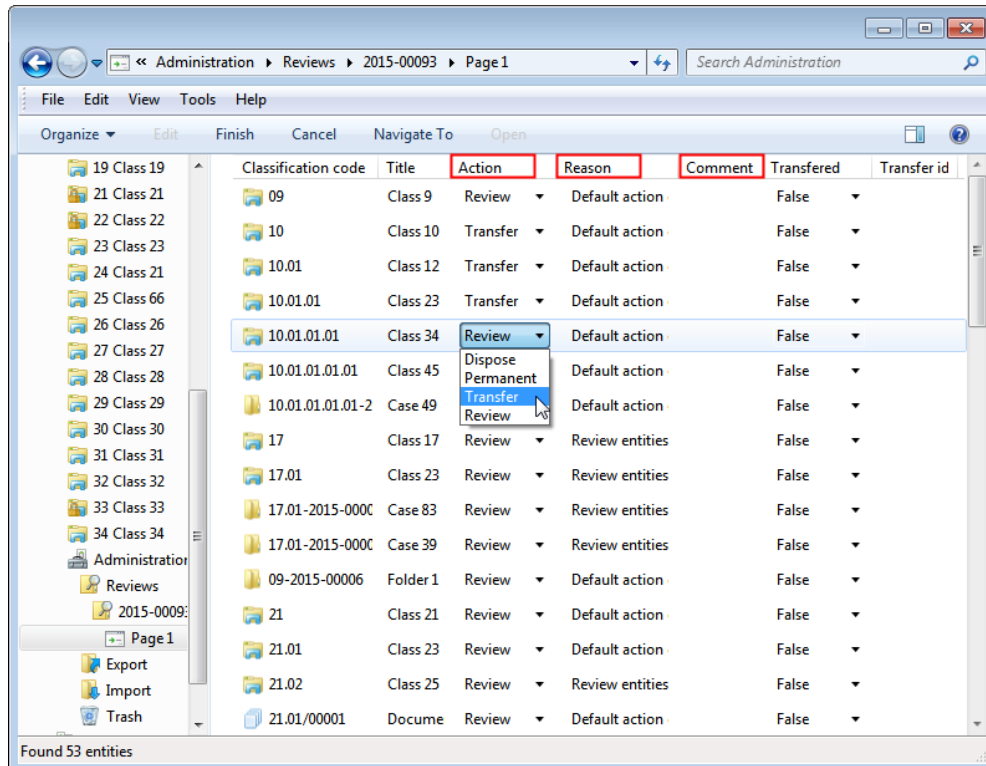


Image 160:  List of entities in modification mode

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 *(see chapter 4.3.9 Entity attributes in the decision-making process)*

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.
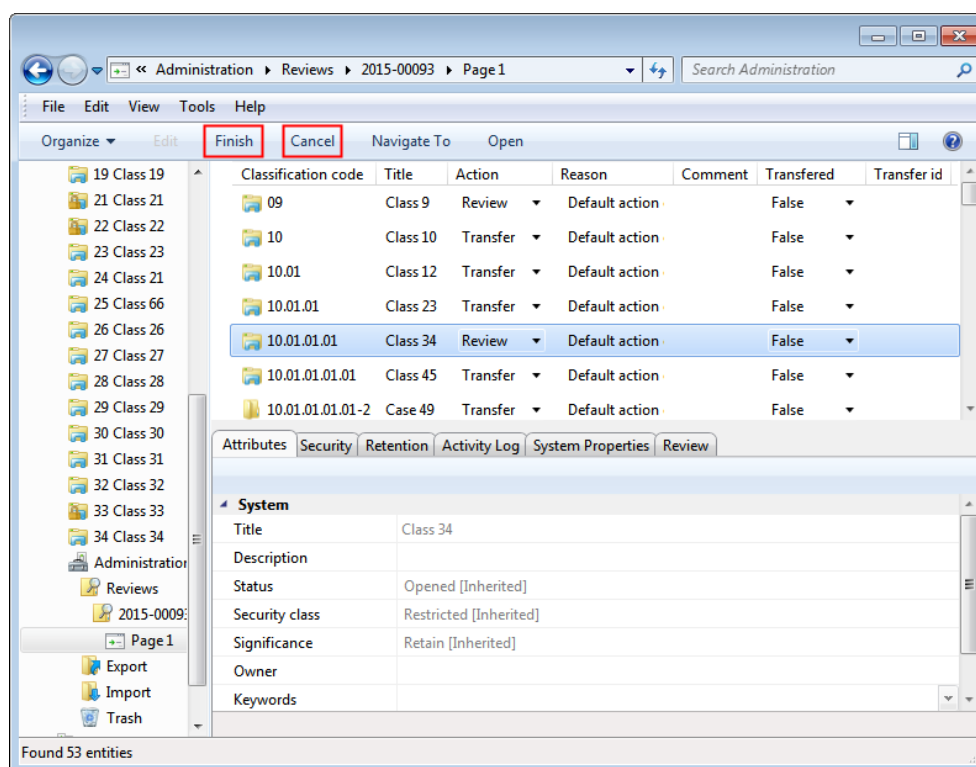
Image 161:  Display of the »Finish« and »Cancel« button


If the page has been modified, its title is written in bold in the view.
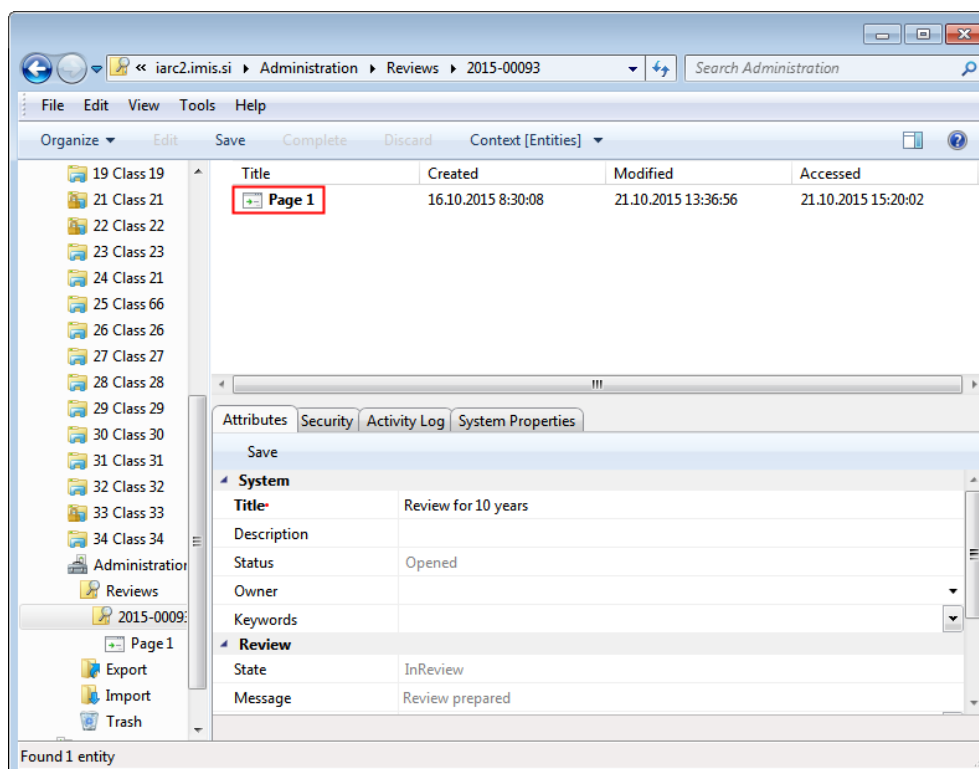


Image 162:  Display of the page which has been modified

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.
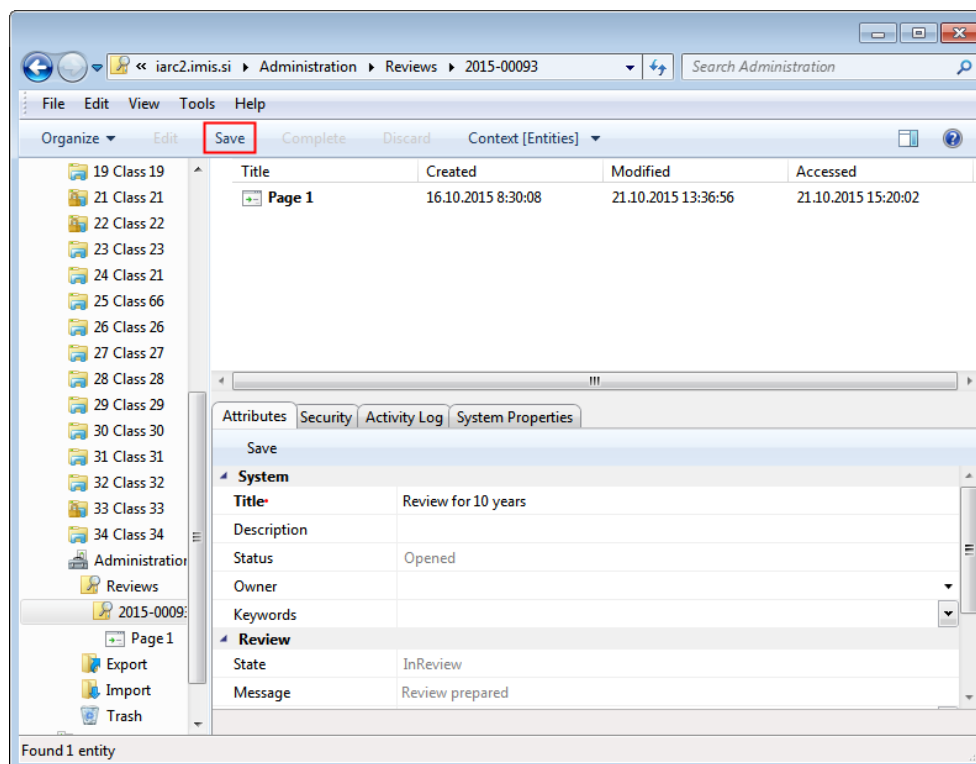


Image 163:  Display of the »Save« command in the review process

### 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.
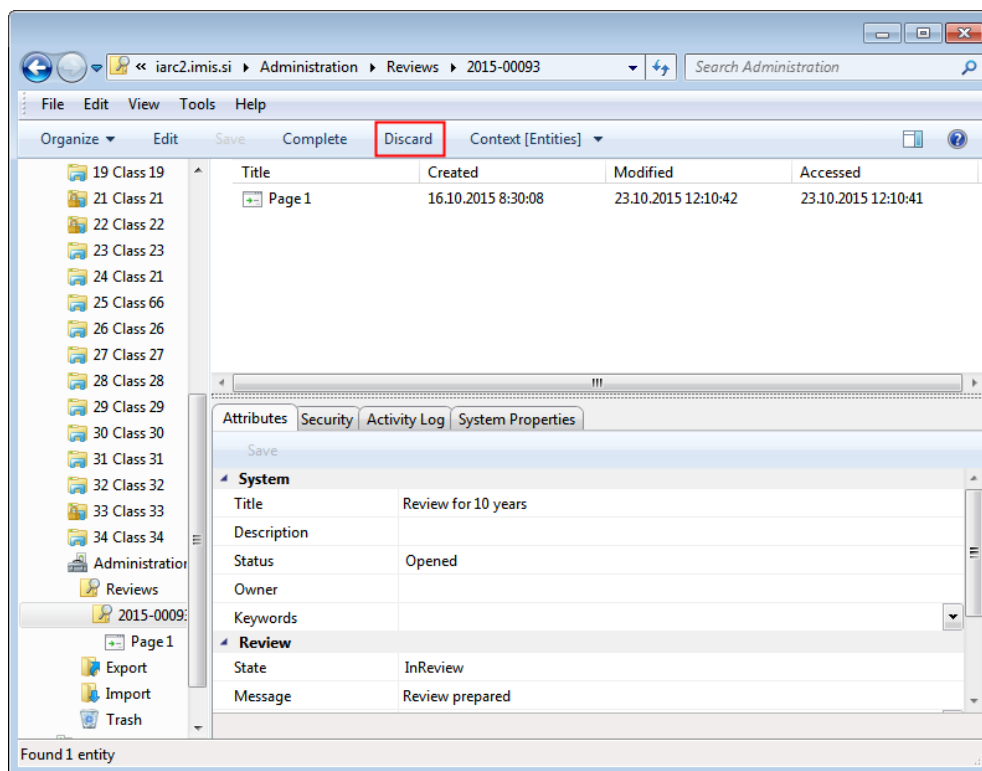
Image 164:  Cancellation of the review process using the »Discard« command

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.

### 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.
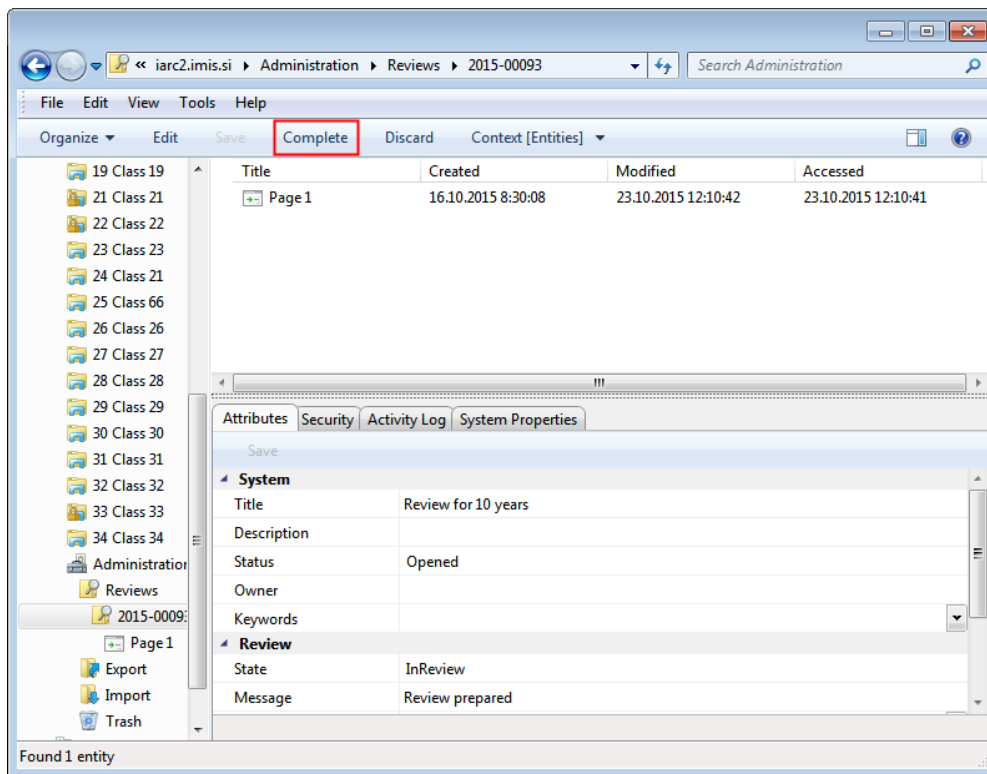
Image 165:  Starting the implementation phase by selecting the »Complete« command

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 4.1.5  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.

### 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.
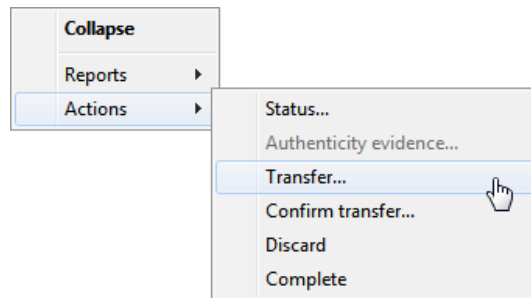


Image 166:  Transfer of entities in the review process

After selecting the command, the user is shown a dialog box for setting the transfer parameters.
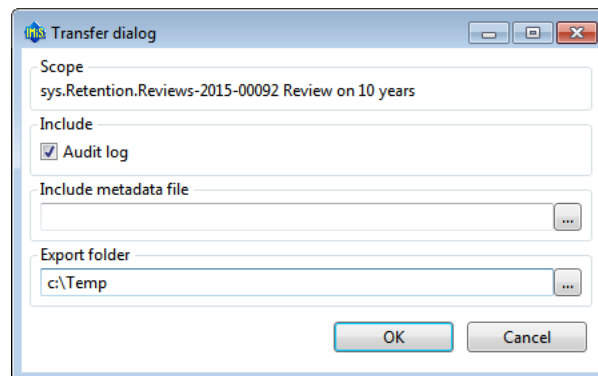


Image 167:  Setting the transfer parameters

By selecting the »Audit log« option, the audit log for an individual transferred entity can be included in the transfer.

*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 3.2.3  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.
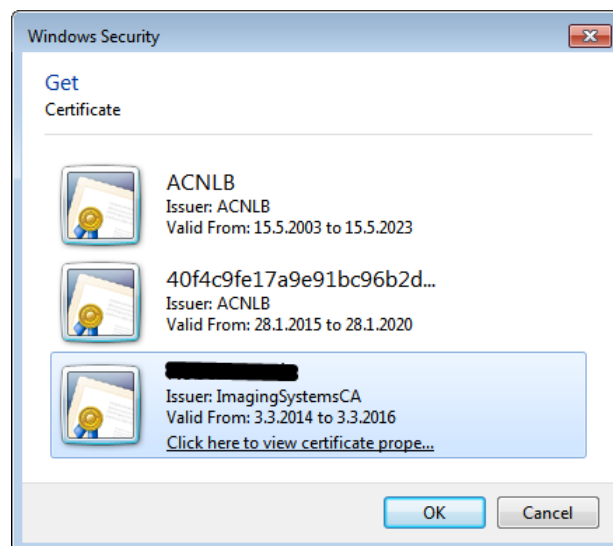


Image 168:  Selecting a digital certificate during export

*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.*

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.
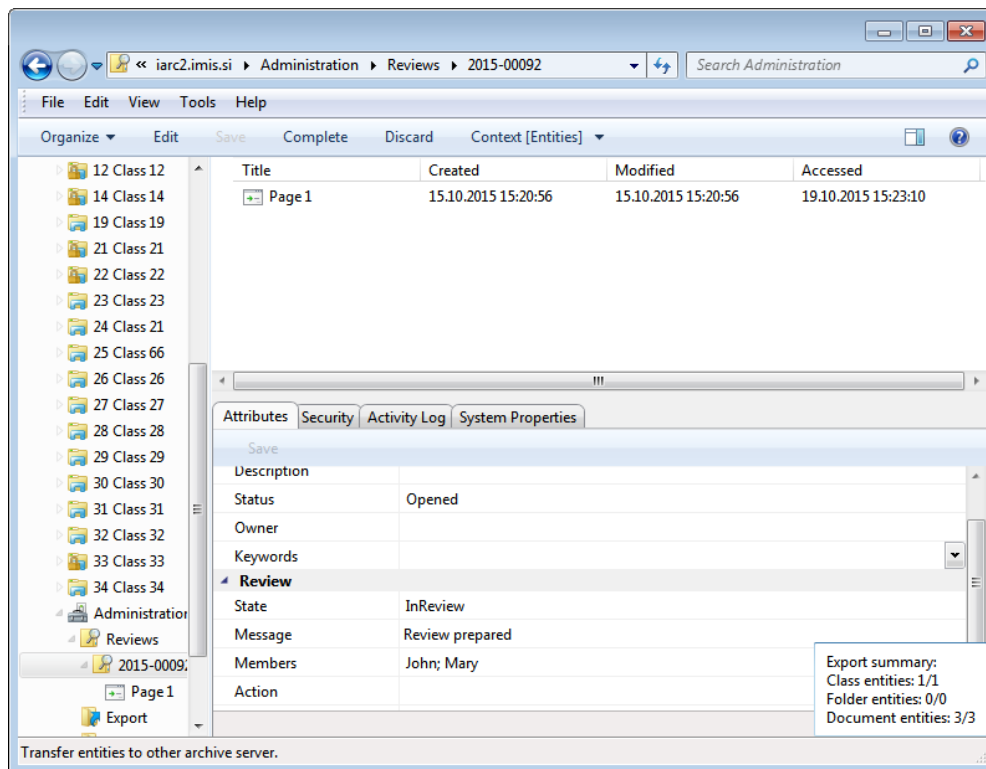
Image 169:  Display of the export complete message with success rate statistics

*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.*

### 4.5.4.1.1   Export phase

At the start of export IMiS®/Client creates a new review document.

For more information  *see chapter 4.1.5  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.

### 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 (*see chapter 3.3 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 *(see chapter 4.1.2.1 Modification of action on an individual entity)*.
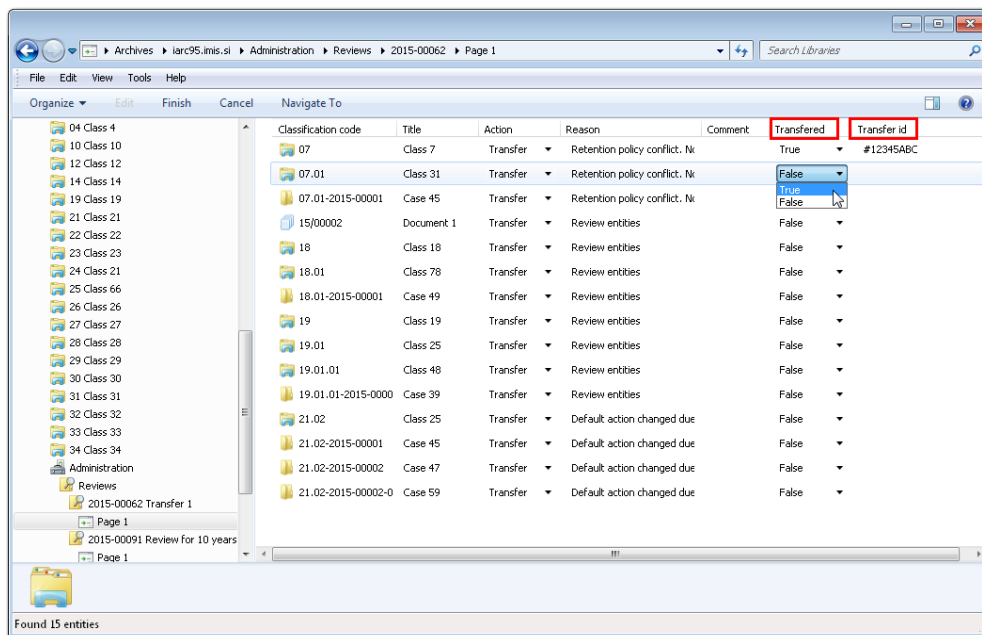


Image 170: Manual transfer confirmation for an individual entity

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.
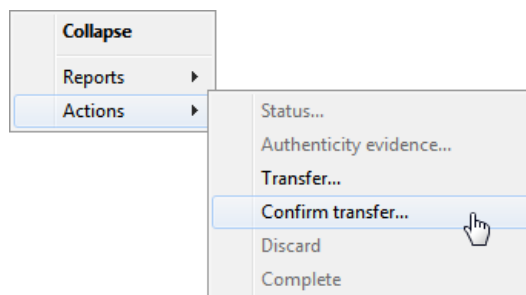
Image 171:  Transfer confirmation using a confirmation file.

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.
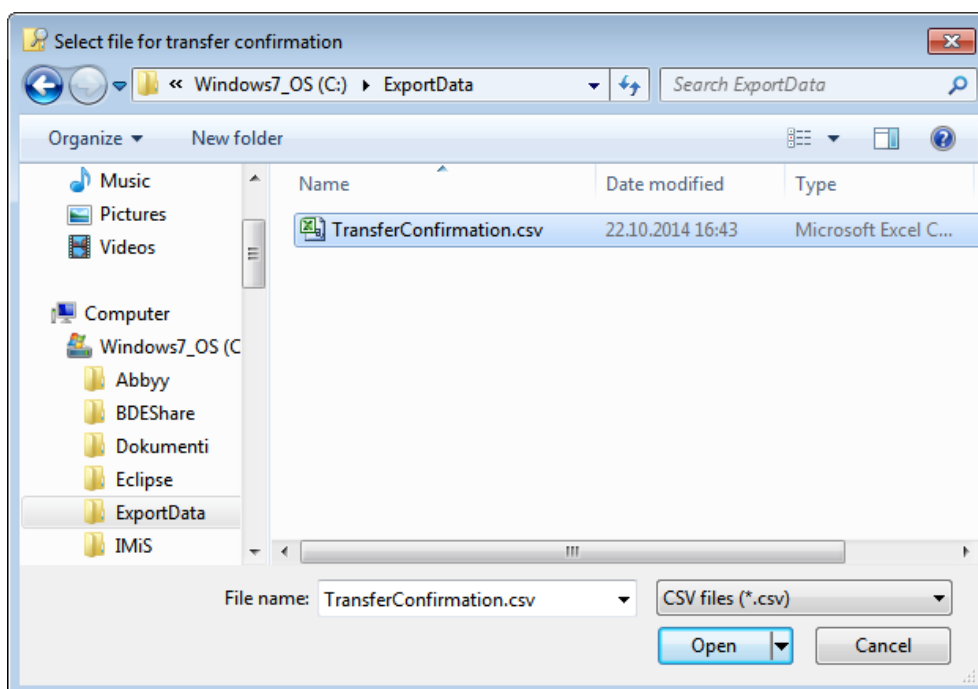


Image 172:  Selecting the confirmation file

The confirmation of all entities recorded in the confirmation file begins to be executed.

For more information *see chapter 3.3  Format of the confirmation file during transfer*.

With the »Cancel« command team members cancel the selection of the confirmation file.

## 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.
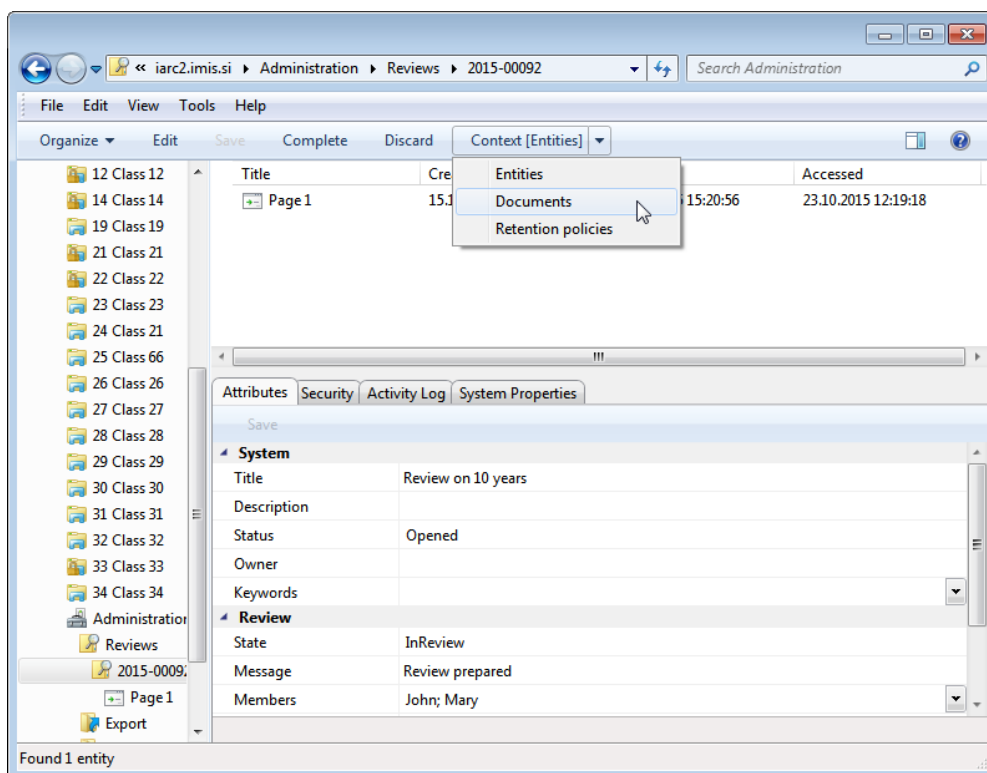


Image 173: Changing the context during the review of classified contents

_Examples_ of classified contents:

- _Report on the implementation phase of the review process._
- _Transfer report._
- _Custom document._
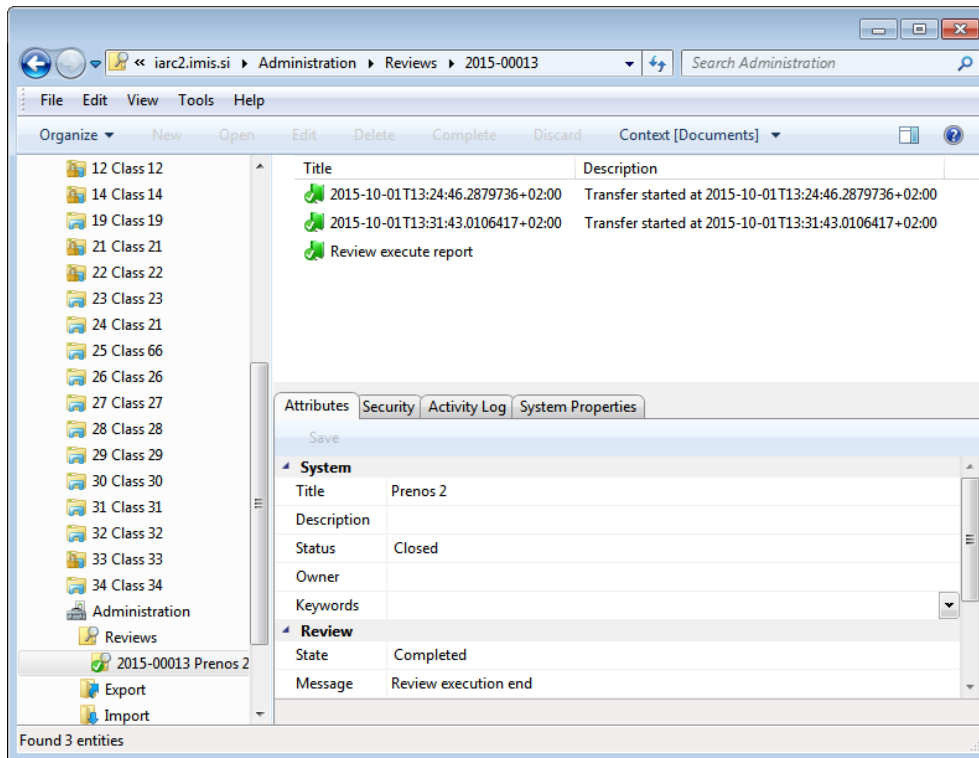
Image 174:  Example of displaying inserted documents in »Documents« context

For updating and viewing contents *see chapter 4.1.3  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 4.2.2.2  Entry of metadata*.

### 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.
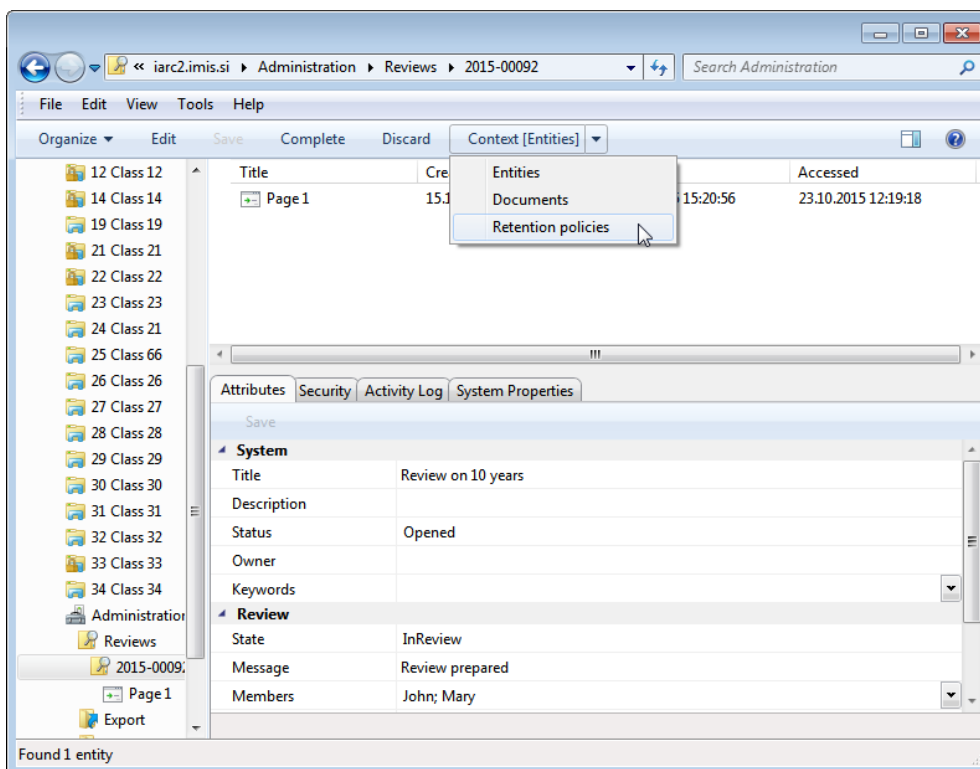
Image 175:  Changing the context in retention policies

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 4.3.8 Review process attributes*.
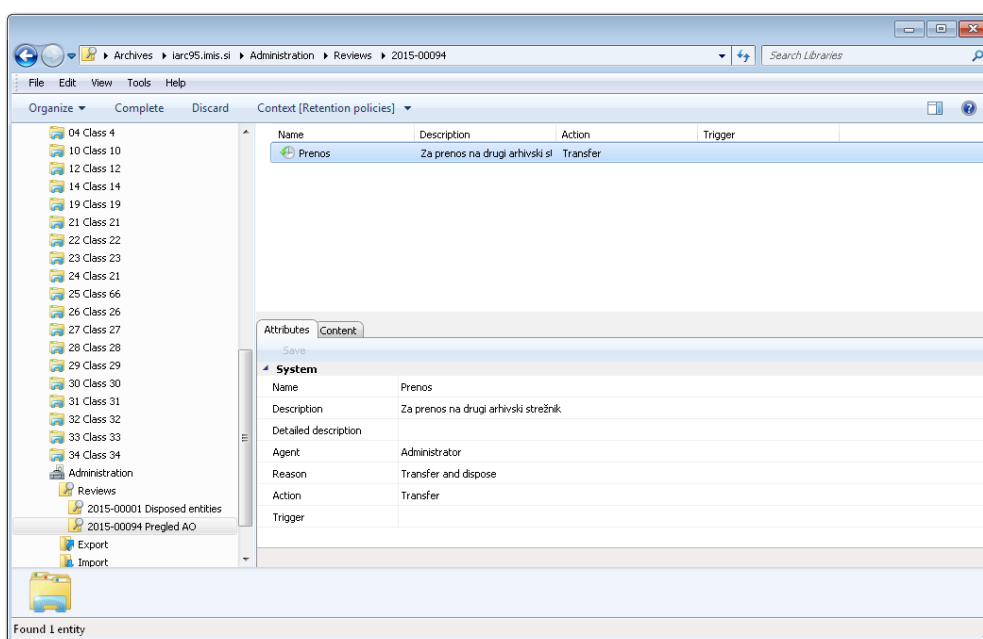


Image 176:  Display of the retention policy

## 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.

### 4.6.1   Import

Every import action *(see chapter 4.2.11 Import)* 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.

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 *IMiS®/ARChive Server manual chapter 3.3.5  Access*.

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.
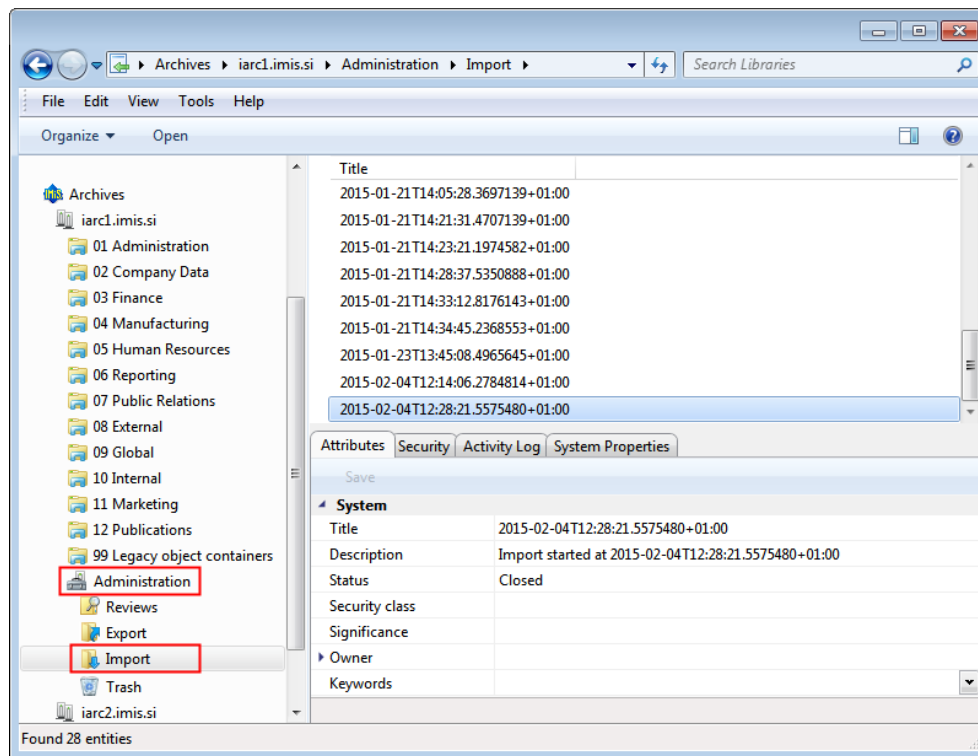
Image 177: Display of the »Import« folder in the »Administration« system folder

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 178: 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.



Image 179: Example signed »XML Report« file with a record of import actions
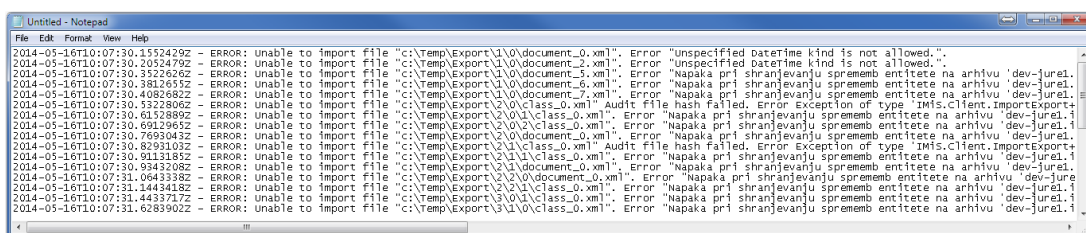


Image 180: Example »Error report« log with a list of import errors
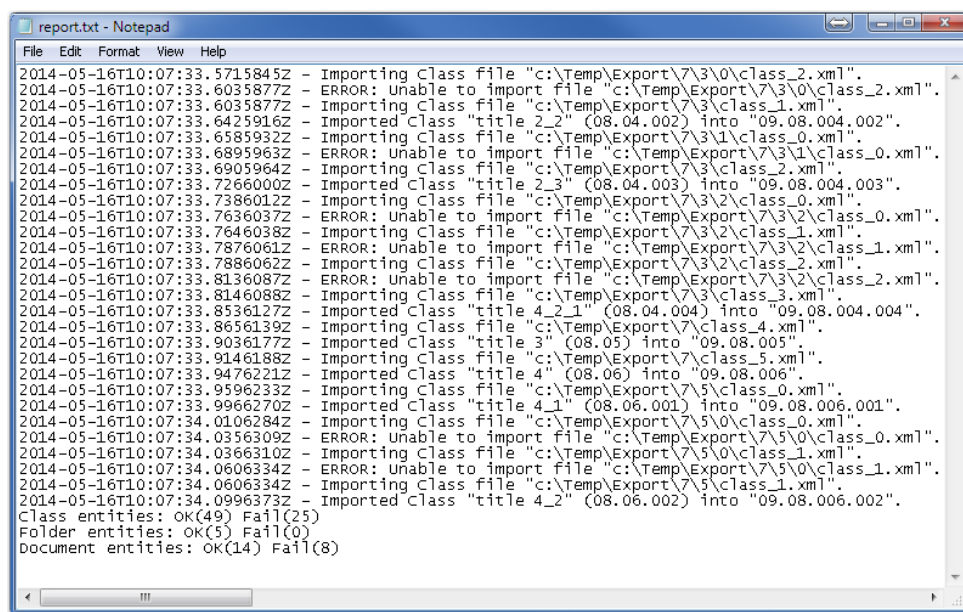
Image 181: Example »Report« log with a list of errors and the overall import success rate

### 4.6.2   Export

Every export action *(see chapter 4.2.12  Export)* 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.
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 *IMiS®/ARChive Server manual*
*chapter 3.3.5  Access procedures*.

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.
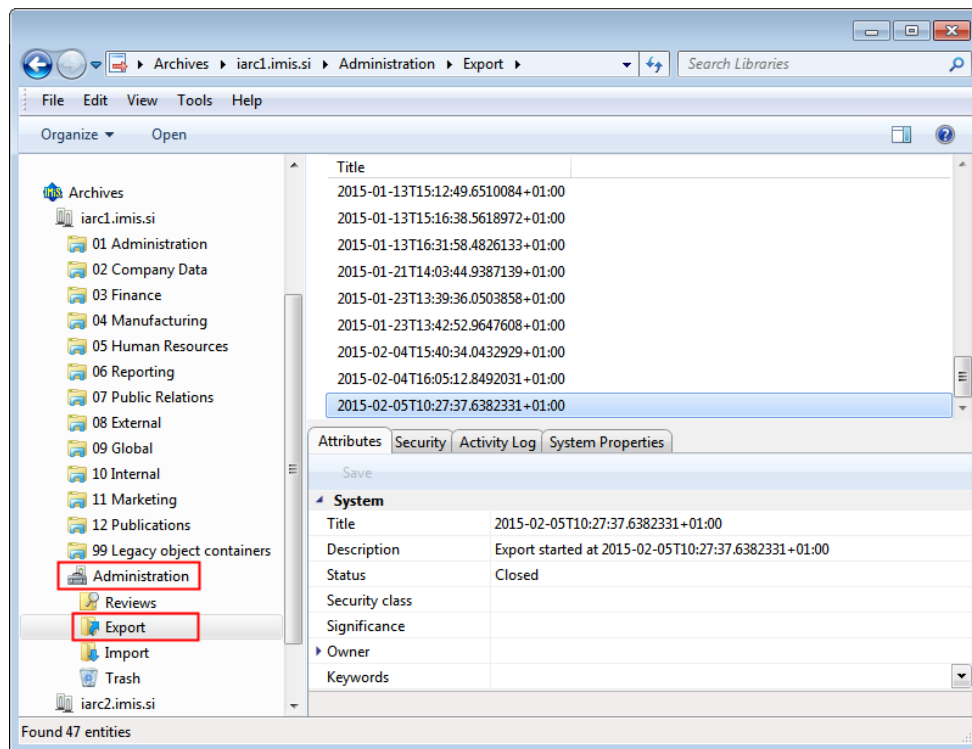
Image 182: Display of the »Export« folder in the »Administration« system folder

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.



Image 183: 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.



Image 184: Example »XML Report« file with a record of export actions
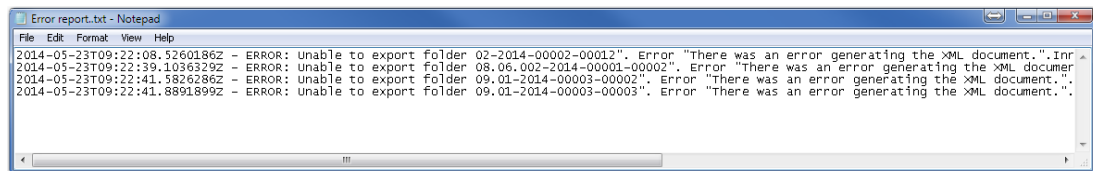


Image 185: Example »Error report« log with a list of export errors
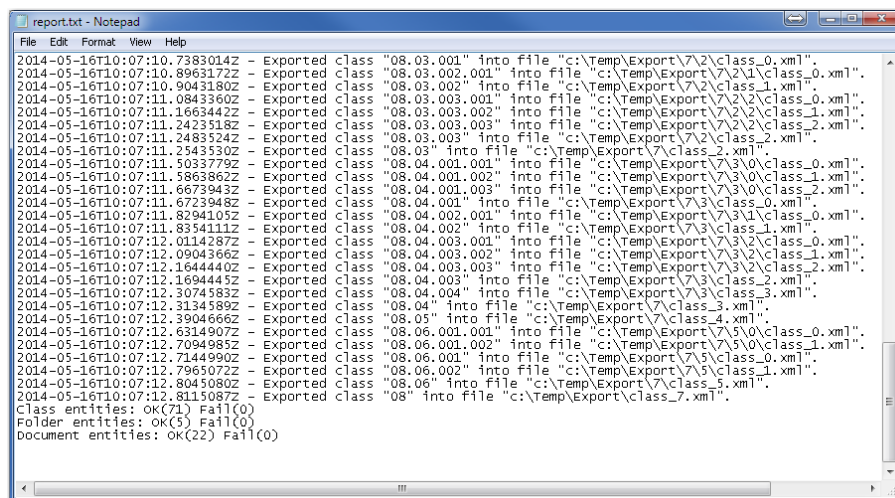


Image 186: Example »Report« log with a list of export actions and the overall export success rate

### 4.6.3    Deletion

Entities deleted by users with a »Deletion« role on the serverappear in the »Trash« folder inside the »Administration« system folder, in their raw form.

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.
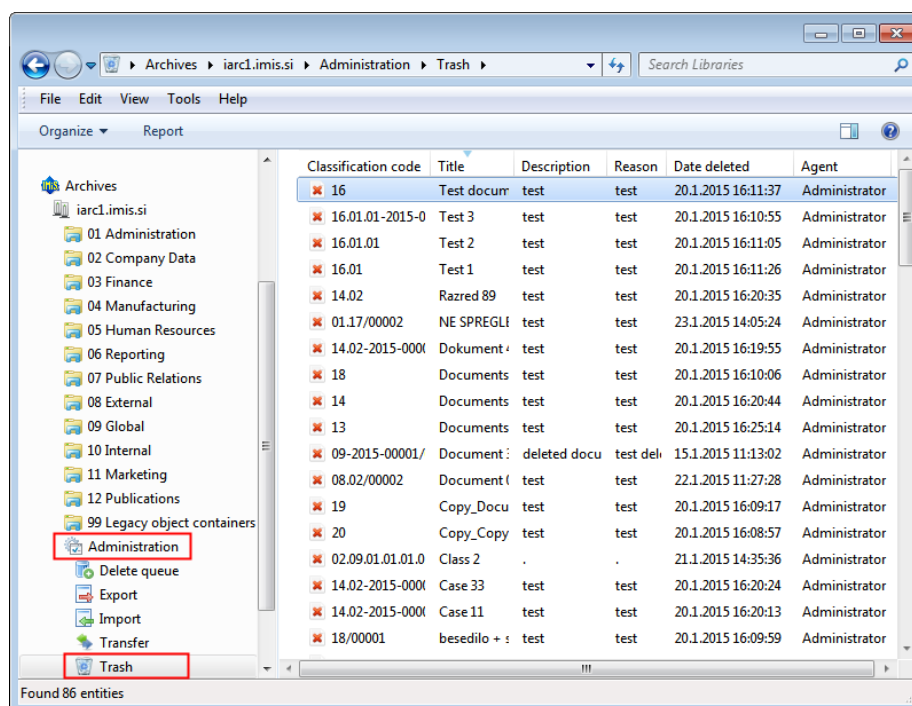


Image 187: Display of the »Trash« folder in the »Administration« system folder

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 »deletion« authorized 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.

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | ClassificationCode | Title | Description | Reason | Deletion date | Agent |
| 2 | 99 | Legacy object containers | Class holding legacy object containers | test | 23.9.2015 16:29 | Administrator |
| 3 | 01 | Class 1 | TEST | TEST | 8.10.2015 8:49 | Administrator |
| 4 | 02 | Class 2 | TEST | TEST | 8.10.2015 8:49 | Administrator |
| 5 | 02-2015-00001 | Folder 1 | TEST | TEST | 8.10.2015 8:48 | Administrator |
| 6 | 02-2015-00001/00001 | Document 1 | TEST | test | 8.10.2015 8:48 | Administrator |
| 7 | 05-2015-00002 | Folder 2 | test | test | 1.10.2015 9:18 | Administrator |
| 8 | 05-2015-00003 | Folder 3 | test | test | 1.10.2015 9:19 | Administrator |
| 9 | 05-2015-00003/00001 | Document 1 | test | test | 1.10.2015 9:19 | Administrator |
| 10 | 05-2015-00001/00001 | Filed 1 | test | test | 1.10.2015 9:28 | Administrator |
| 11 | 06 | Class 6 | test | test | 15.10.2015 12:18 | Administrator |
| 12 | 06.01 | Class 23 | test | test | 15.10.2015 12:18 | Administrator |
| 13 | 06.01-2015-00001 | Case 27 | test | test | 15.10.2015 12:17 | Administrator |
| 14 | 06.01-2015-00001/00001 | Document 38 | test | test | 15.10.2015 12:17 | Administrator |
| 15 | 10 | Class 10 | test | test | 2.11.2015 9:11 | Ron Salazar |
| 16 | 10.01 | Class 12 | test | test | 2.11.2015 9:11 | Ron Salazar |
| 17 | 10.01.01 | Class 23 | test | test | 2.11.2015 9:11 | Ron Salazar |
| 18 | 10.01.01.01 | Class 34 | test | test | 2.11.2015 9:10 | Ron Salazar |
| 19 | 10.01.01.01.01 | Class 45 | test | test | 2.11.2015 9:10 | Ron Salazar |
| 20 | 01-2015-00005 | Folder 5 | test | corrupted entities | 8.10.2015 8:45 | Administrator |
| 21 | 01-2015-00006 | Folder 6 | test | corrupted entities | 8.10.2015 8:44 | Administrator |
| 22 | 01-2015-00005/00001 | Document 1 | test | corrupted entities | 8.10.2015 8:44 | Administrator |
| 23 | 01-2015-00005/00002 | Document 2 | test | corrupted entities | 8.10.2015 8:44 | Administrator |

Image 188: 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.

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.
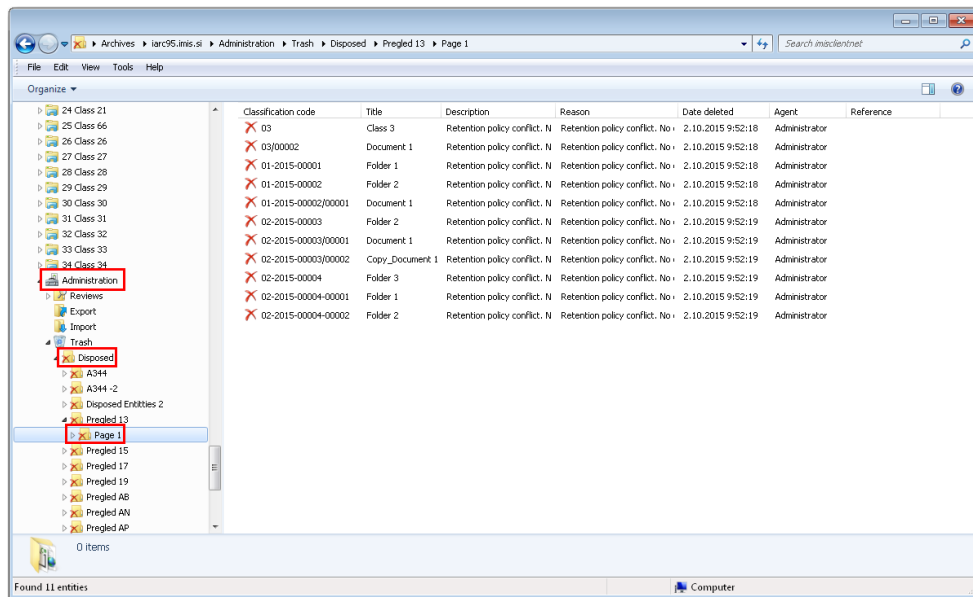
Image 189:  Display of the list of disposed entities

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.
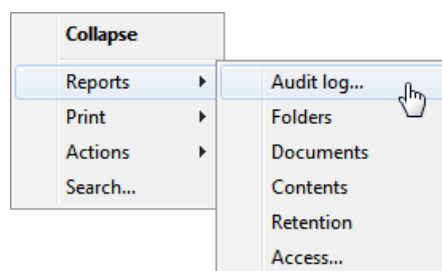


Image 190: Selecting an audit log report via the popup menu

Within the framework of audit log search settings *(see chapter 4.2.19  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 *(see the IMiS®/ARChive Server user manual chapter 3.3.8.5  Report format)*.
- 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.

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.

| | A | B | C | D | E | F | G | H | I | J |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Time | UserName | Address | ComputerNa | Id | ClassificationCode | EventType | EventMessage | | |
| 2 | 23.5.2014 8:14 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | fJ75#wiQv&JhF | C=02^F=2014-00003^D=00002 | Entity open event, type READ-ONLY | | | |
| 3 | 23.5.2014 8:17 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | fJ75#wiQv&JhF | C=02^F=2014-00003^D=00002 | Entity open event, type READ-WRITE | | | |
| 4 | 23.5.2014 8:17 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | fJ75#wiQv&JhF | C=02^F=2014-00003^D=00002 | Property value changed event | Values for the following pr | | |
| 5 | 23.5.2014 8:17 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | fJ75#wiQv&JhF | C=02^F=2014-00003^D=00002 | Entity save event | | | |
| 6 | 23.5.2014 8:17 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | fJ75#wiQv&JhF | C=02^F=2014-00003^D=00002 | Entity open event, type READ-ONLY | | | |
| 7 | 23.5.2014 8:18 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Entity open event, type READ-ONLY | | | |
| 8 | 23.5.2014 8:18 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Entity open event, type READ-ONLY | | | |
| 9 | 23.5.2014 8:18 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Entity open event, type READ-WRITE | | | |
| 10 | 23.5.2014 8:18 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Property value changed event | Values for the following pr | | |
| 11 | 23.5.2014 8:18 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Entity save event | | | |
| 12 | 23.5.2014 8:18 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Entity open event, type READ-WRITE | | | |
| 13 | 23.5.2014 8:19 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Entity save event | | | |
| 14 | 23.5.2014 8:19 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Property value changed event | Values for the following pr | | |
| 15 | 23.5.2014 8:19 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Entity open event, type READ-WRITE | | | |
| 16 | 23.5.2014 8:19 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Entity open event, type READ-ONLY | | | |
| 17 | 23.5.2014 8:20 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Entity open event, type READ-WRITE | | | |
| 18 | 23.5.2014 8:20 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Entity save event | | | |
| 19 | 23.5.2014 8:20 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Property value changed event | Values for the following pr | | |
| 20 | 23.5.2014 8:20 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Entity open event, type READ-WRITE | | | |
| 21 | 23.5.2014 8:20 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Property value changed event | Values for the following pr | | |
| 22 | 23.5.2014 8:20 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Entity save event | | | |
| 23 | 23.5.2014 8:20 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Entity open event, type READ-WRITE | | | |
| 24 | 23.5.2014 8:20 | jpuhek1 | fd00:192:168:9 | ALESWIN7 | 637`u!9ycQN?r | C=02^F=2014-00003^D=00003 | Property value changed event | Values for the following pr | | |

Image 191: 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 192: Selecting a folder report via the popup menu

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 | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| 1 | ClassificationCode | Title | Template | Status | Significance | SecurityClass | CurrentLocation | HomeLocation | DocumentCount |
| 2 | 35.01.01.01.01-2015-00001 | Case 49 | Case | Opened | | | | | 1 |
| 3 | 35.02.01.01.01-2015-00002 | Case 49 | Case | Opened | | | | | 1 |
| 4 | 35.14-2015-00001 | Case 91 | Case | Opened | | | | | 0 |
| 5 | 35.14-2015-00002 | Case 93 | Case | Opened | | | | | 0 |
| 6 | 35.21.01.01.02-2015-00001 | Case 45 | Case | Opened | | | | | 2 |
| 7 | 35.21.01.01.02-2015-00002 | Case 47 | Case | Opened | | | | | 0 |
| 8 | 35.21.01.01.02-2015-00002-00001 | Case 59 | Case | Opened | | | | | 0 |
| 9 | 35.22-2015-00001 | Case 75 | Case | Opened | | | | | 0 |
| 10 | 35.22-2015-00001-00001 | Case 29 | Case | Opened | | | | | 2 |
| 11 | | | | | | | | | |
| 12 | | | | | | | | | |

Image 193: 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.

Image 194: 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 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 | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| 1 | ClassificationCode | Title | Template | Status | Significance | CurrentLocation | HomeLocation | ContentCount |
| 2 | 35.01.01.01.01-2015-00001/00001 | TEST FTI | FiledDocument | | | | | 2 |
| 3 | 35.01.02/00001 | Document 1 | Document | Opened | | | | 1 |
| 4 | 35.02.01.01.01-2015-00002/00001 | TEST FTI | FiledDocument | | | | | 2 |
| 5 | 35.02.02/00001 | Document 1 | Document | Opened | | | | 1 |
| 6 | 35.16/00001 | Dokument 57 | Document | Closed | | | | 15 |
| 7 | 35.17/00001 | IMiS/Client build 72 | Email | Opened | | | | 2 |
| 8 | 35.17/00002 | IMiS/Client build 72 | Email | Opened | | | | 2 |
| 9 | 35.17/00003 | IMiS/Client build 72 | Email | Opened | | | | 2 |
| 10 | 35.20/00001 | Dokument 59 | Document | Closed | | | | 7 |
| 11 | 35.21.01.01.01/00001 | Document 59 | Document | Opened | Retain | | | 0 |
| 12 | 35.21.01.01.01/00002 | Document 61 | Document | Opened | Retain | | | 0 |
| 13 | 35.21.01.01.01/00003 | Document 63 | Document | Opened | Retain | | | 0 |
| 14 | 35.21.01.01.02-2015-00001/00001 | Document 67 | FiledDocument | | | | | 0 |
| 15 | 35.21.01.01.02-2015-00001/00002 | Document 49 | FiledDocument | | | | | 0 |

Image 195: Example document report

### 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.
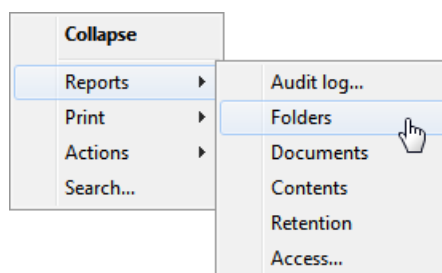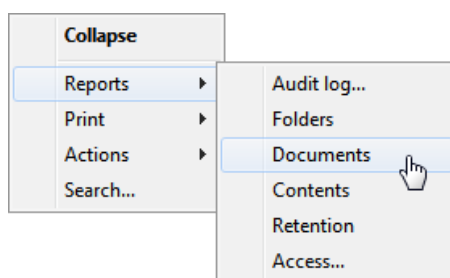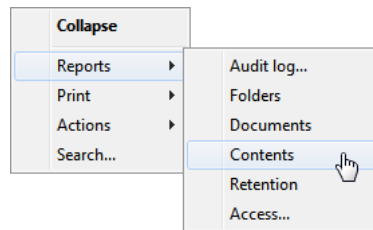


Image 196: Selecting a content report via the popup menu

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.

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | ClassificationCode | Title | Template | ContentDescription | ContentType | ContentSize |
| 2 | 35.01.01.01.01-2015-0001/00001 | TEST FTI | FiledDocument | signed document.pdf | application/pdf | 61708 |
| 3 | 35.01.01.01.01-2015-0001/00001 | TEST FTI | FiledDocument | signed document.pdf | application/pdf | 61708 |
| 4 | 35.01.02/00001 | Document 1 | Document | signed document.pdf | application/pdf | 61708 |
| 5 | 35.02.01.01.01-2015-0002/00001 | TEST FTI | FiledDocument | signed document.pdf | application/pdf | 61708 |
| 6 | 35.02.01.01.01-2015-0002/00001 | TEST FTI | FiledDocument | signed document.pdf | application/pdf | 61708 |
| 7 | 35.02.02/00001 | Document 1 | Document | signed document.pdf | application/pdf | 61708 |
| 8 | 35.16/00001 | Dokument 57 | Document | Balance Sheet.docx | application/vnd.openxmlformats-officedocument.v | 5812 |
| 9 | 35.16/00001 | Dokument 57 | Document | Budget Tracking Template. | application/vnd.openxmlformats-officedocument.s | 81413 |
| 10 | 35.16/00001 | Dokument 57 | Document | Business report_2013.xltx | application/vnd.openxmlformats-officedocument.s | 89341 |
| 11 | 35.16/00001 | Dokument 57 | Document | Business report_2014.xlsx | application/vnd.openxmlformats-officedocument.s | 77037 |
| 12 | 35.16/00001 | Dokument 57 | Document | Certification of Incorporati | application/vnd.openxmlformats-officedocument.v | 16277 |
| 13 | 35.16/00001 | Dokument 57 | Document | Company Overview.pdf | application/pdf | 88549 |
| 14 | 35.16/00001 | Dokument 57 | Document | Decision Structure.jpg | image/jpeg | 19710 |
| 15 | 35.16/00001 | Dokument 57 | Document | Distribution and Marketing | application/vnd.openxmlformats-officedocument.v | 28686 |
| 16 | 35.16/00001 | Dokument 57 | Document | Employment Agreement.d | application/vnd.openxmlformats-officedocument.v | 22285 |
| 17 | 35.16/00001 | Dokument 57 | Document | Equity Transfer Agreement | application/vnd.openxmlformats-officedocument.v | 23560 |
| 18 | 35.16/00001 | Dokument 57 | Document | EU Stats_August 2011.xlsx | application/vnd.openxmlformats-officedocument.s | 21640 |
| 19 | 35.16/00001 | Dokument 57 | Document | EU Stats_July 2011.xlsx | application/vnd.openxmlformats-officedocument.s | 21095 |
| 20 | 35.16/00001 | Dokument 57 | Document | Finance Log_April 2014.xls | application/vnd.openxmlformats-officedocument.s | 17554 |

Image 197: 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.
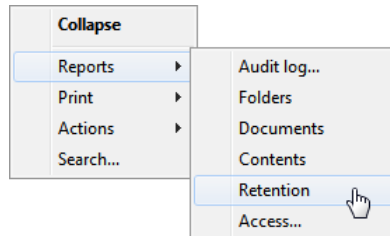


Image 198:  Selecting the retention report via the pop-up menu

Information on retention is listed in the following columns:

- »ClasssificationCode«:  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).
- »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 |
|---|---|---|---|---|---|---|---|
| 1 | ClassificationCode | Title | Type | Policy/Hold | Name | Reason | Description |
| 2 | 23 | Class 23 | Class | Retention policy | 3 leta | Hramba za 3 leta po zaprtju entitete | Review entities after 3 years |
| 3 | 23 | Class 23 | Class | Retention policy | 8 let | Pregled 8 let od zaprtja entitet | Review entities after 8 years |
| 4 | 23 | Class 23 | Class | Retention policy | 3 leta | Hramba za 3 leta po zaprtju entitete | Review entities after 3 years |
| 5 | 23 | Class 23 | Class | Retention policy | 8 let | Pregled 8 let od zaprtja entitet | Review entities after 8 years |
| 6 | 23.01 | Class 28 | Class | Retention policy | 3 leta | Hramba za 3 leta po zaprtju entitete | Review entities after 3 years |
| 7 | 23.01 | Class 28 | Class | Retention policy | 8 let | Pregled 8 let od zaprtja entitet | Review entities after 8 years |
| 8 | 23.01-2015-00001 | Case 38 | Folder | Retention policy | 3 leta | Hramba za 3 leta po zaprtju entitete | Review entities after 3 years |
| 9 | 23.01-2015-00001 | Case 38 | Folder | Retention policy | 8 let | Pregled 8 let od zaprtja entitet | Review entities after 8 years |
| 10 | 23.01-2015-00001-00001 | Case 29 | Folder | Retention policy | 3 leta | Hramba za 3 leta po zaprtju entitete | Review entities after 3 years |
| 11 | 23.01-2015-00001-00001 | Case 29 | Folder | Retention policy | 8 let | Pregled 8 let od zaprtja entitet | Review entities after 8 years |
| 12 | 23.01-2015-00001-00001/00001 | Document 56 | Document | Retention policy | 3 leta | Hramba za 3 leta po zaprtju entitete | Review entities after 3 years |
| 13 | 23.01-2015-00001-00001/00001 | Document 56 | Document | Retention policy | 8 let | Pregled 8 let od zaprtja entitet | Review entities after 8 years |
| 14 | | | | | | | |

Image 199:  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.
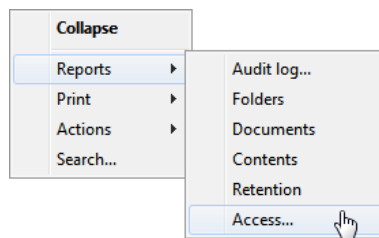


Image 200: Creating an access report on the selected user

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.
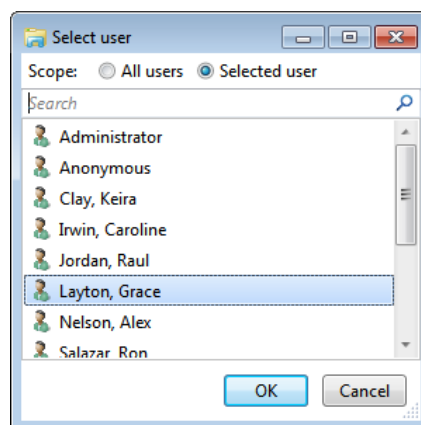


Image 201:  Selecting a user or all users

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.
- »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 | CurrentLocation | HomeLocation | User | Read | Write | Delete | Move | CreateSubEntities | ChangeRights | ChangeSecurityClass | ChangeStatus | ChangeRetention |
| 2 | 19.01.01-2015-00004 | Case 31 | Folder | Case | Opened | | | | | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |
| 3 | 19.01.01-2015-00004/00001 | Document 42 | Document | FiledDocument | | | | | | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |
| 4 | 19.01.01-2015-00004/00002 | Dokument 43 | Document | FiledDocument | | | | | | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |
| 5 | 19.01.01-2015-00004/00003 | Dokument 44 | Document | FiledDocument | | | | | | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |
| 6 | 19.01.01-2015-00004/00004 | Dokument 45 | Document | FiledDocument | | | | | | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |
| 7 | 19.01.01-2015-00004/00005 | Dokument 46 | Document | FiledDocument | | | | | | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |
| 8 | 19.01.01-2015-00005 | Case 32 | Folder | Case | Opened | | | C78 | B32 | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |
| 9 | 19.01.01-2015-00005-00001 | Case 26 | Folder | Case | Opened | | | | | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |
| 10 | 19.01.01-2015-00005-00001 | Case 39 | Folder | Case | Opened | | | | | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |
| 11 | 19.01.01-2015-00005-00001 | Case 49 | Folder | Case | Opened | | | | | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |
| 12 | 19.01.01-2015-00005-00001 | Case 56 | Folder | Case | Opened | | Restricted | | | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |
| 13 | 19.01.01-2015-00005-00001 | Case 61 | Folder | Case | Opened | | Restricted | | | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |
| 14 | 19.01.01-2015-00006 | Case 33 | Folder | Case | Opened | | | | | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |
| 15 | 19.01.01-2015-00006-00001 | Case 23 | Folder | Case | Opened | | | G54 | Z788 | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |
| 16 | 19.01.01-2015-00006-00001 | Case 38 | Folder | Case | Opened | | | | | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |
| 17 | 19.01.01-2015-00006-00001 | Case 46 | Folder | Case | Opened | | | | | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |
| 18 | 19.01.01-2015-00006-00001 | Case 52 | Folder | Case | Opened | | | | | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |
| 19 | 19.01.01-2015-00006-00001 | Case 65 | Folder | Case | Opened | | | | | Keira Clay | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE | FALSE |

Image 202: 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.

- »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.

- »Deletion«:  this role enables the viewing of entities that have been flagged for deletion.
  Users with the »Deletion« role can access the »Disposed«, »Deleted« and »Queue« folders in the »Trash« folder under the »Administration« folder of the archive.

- »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.

- Review:  this role allows the reviewing and editing of retention policies and disposition holds on entities, and the review and implementation phases of review processes.
  Users with a »Review« role may access the »Retention« tab when reviewing entity information; while the »Reviews« folder is available in the »Administration« folder.

# 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).

### 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:

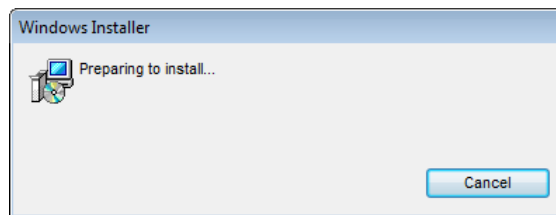_IMiS.Client.9.1.1406.x64.msi_

The following window appears:



Image 203: Preparing to install

Next, a dialog box with the install wizard is shown, prompting the administrator to continue with the installation or cancel it.
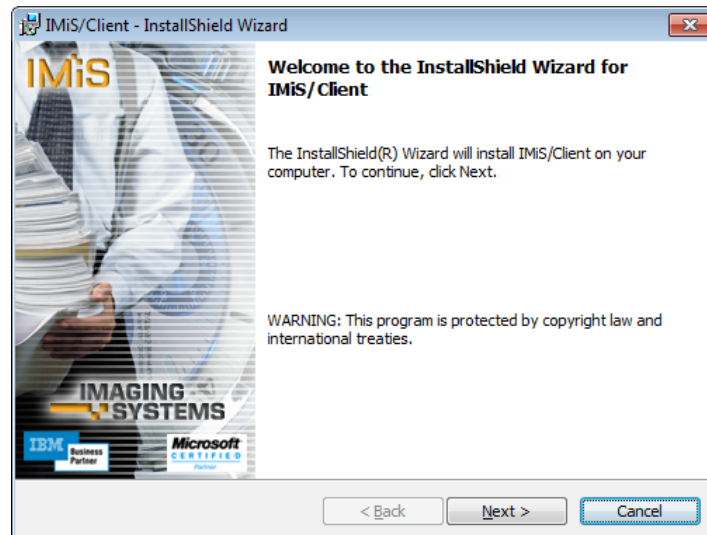
Image 204: Beginning the IMiS®/Client installation procedure

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.
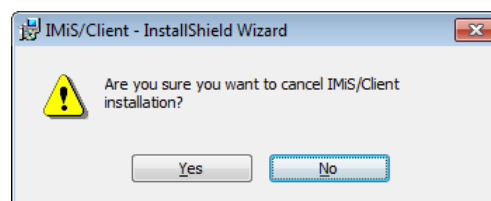


Image 205: Cancelling the IMiS®/Client installation procedure

If the installation procedure is cancelled, any already installed files and Windows registry settings are deleted.

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 206: 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«.
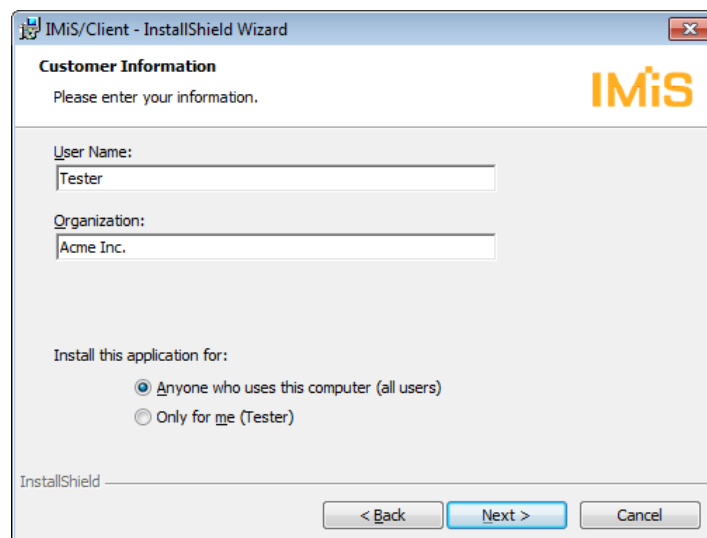


Image 207: Customer information dialog box

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.
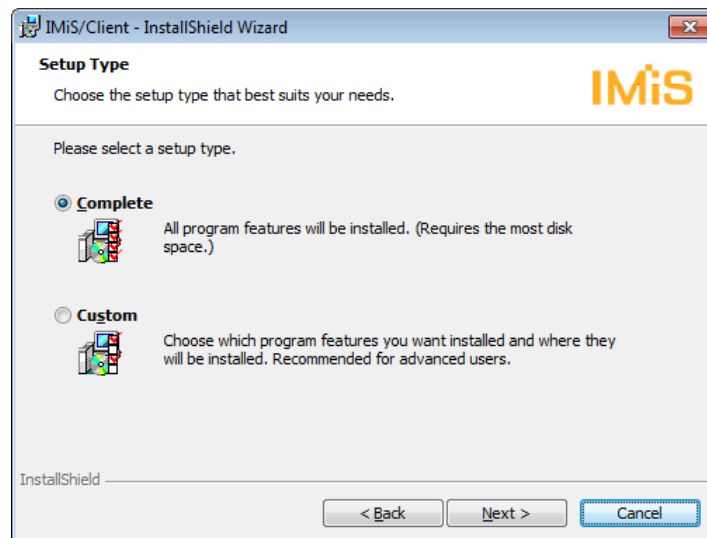


Image 208: Choice between complete and custom installation

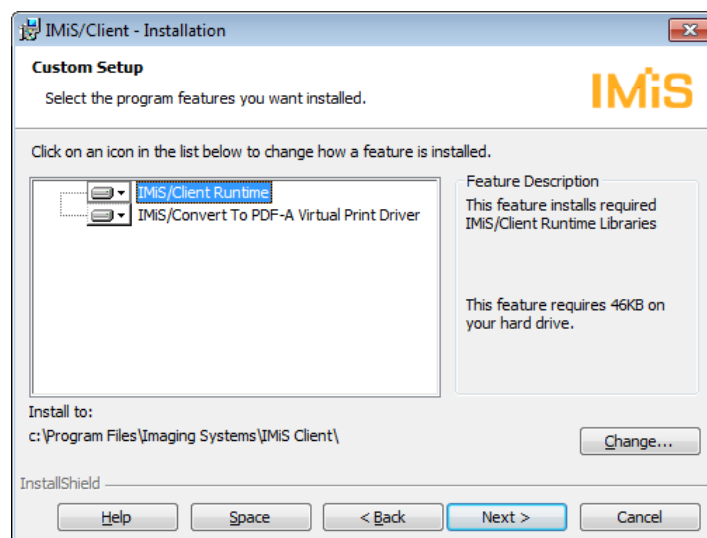When choosing the »Custom« setup type, you will receive the following dialog box:



Image 209: Selecting the elements and location of IMiS®/Client installation

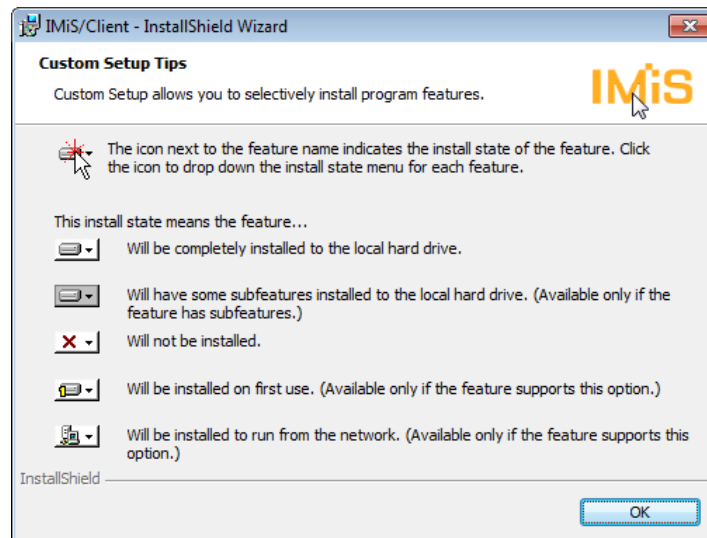Choosing the »Help« command will open the following setup tips:



Image 210: 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
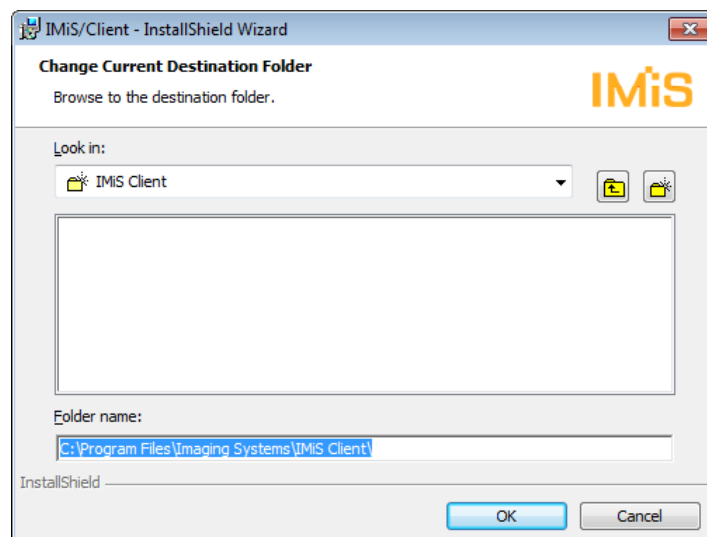
confirmed using the »OK« button.



Image 211: Selecting the destination folder

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.

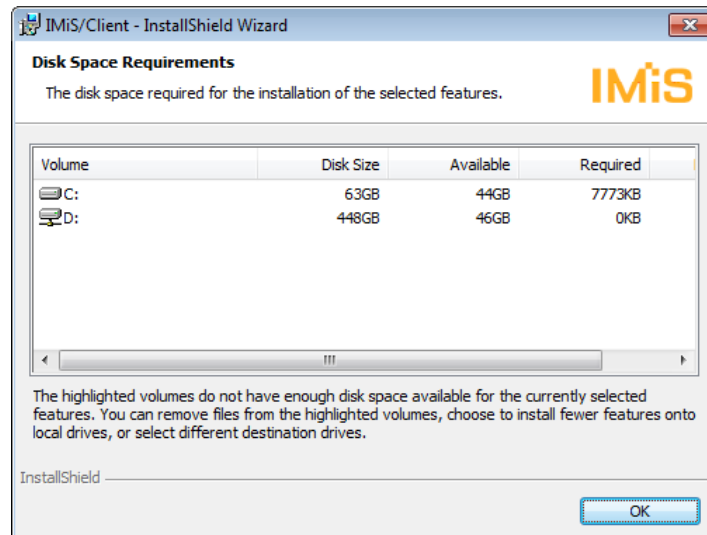Disks with insufficient space are highlighted.

Image 212: 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.

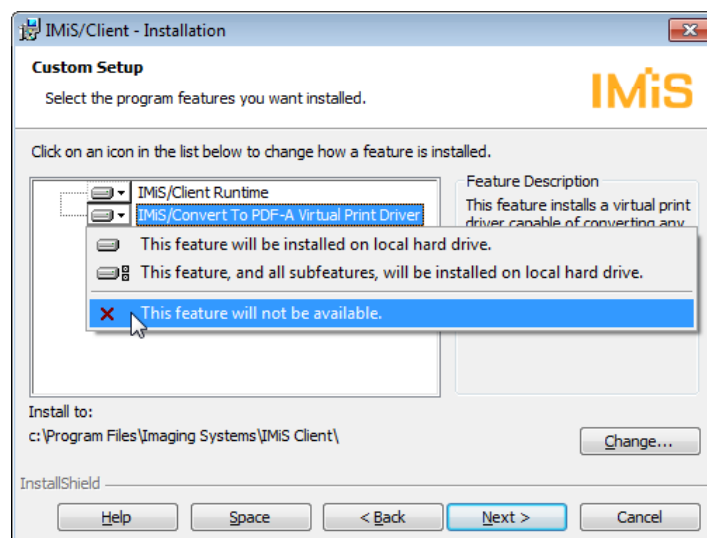  This element can be removed through a popup menu.



Image 213: 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.
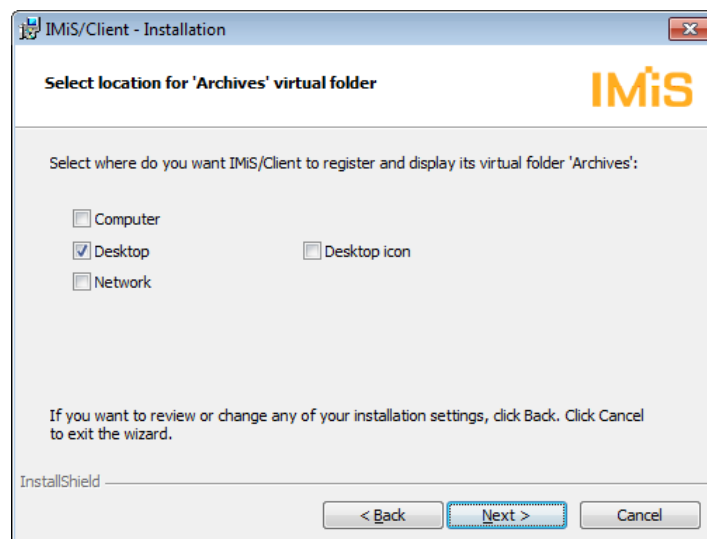- »Network«:  the Archives folder is installed under the »Network« folder.



Image 214: Selecting the location of the Archives folder

The next step prompts you to confirm the selected settings and begin installation by clicking »Install«.
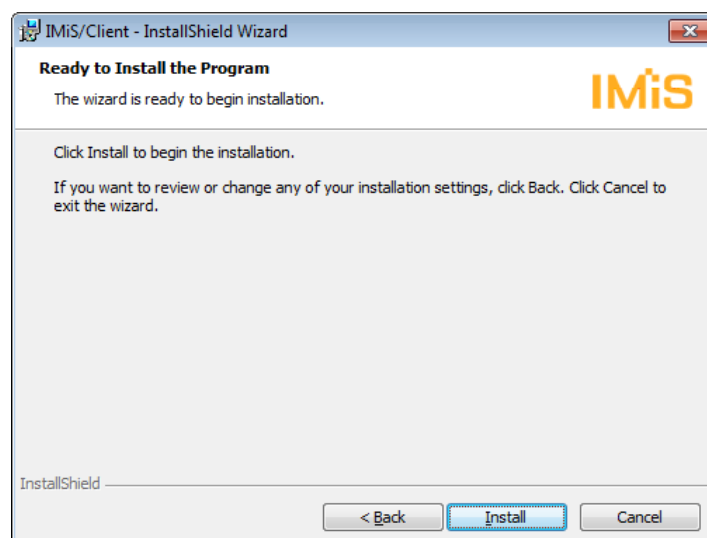


Image 215: Confirming settings to begin installation

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.
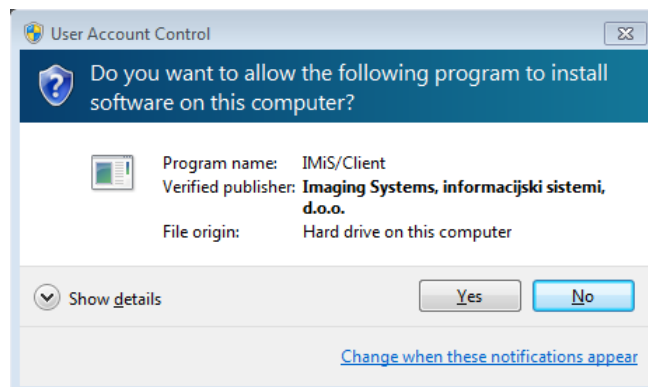


Image 216: Security warning notification

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.
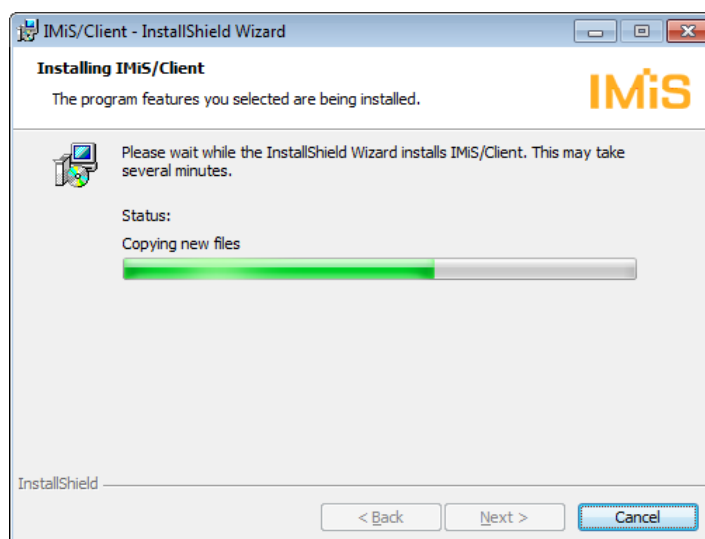


Image 217: Installation progress bar

Installation is completed by clicking »Finish« in the final dialog box.



Image 218: 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
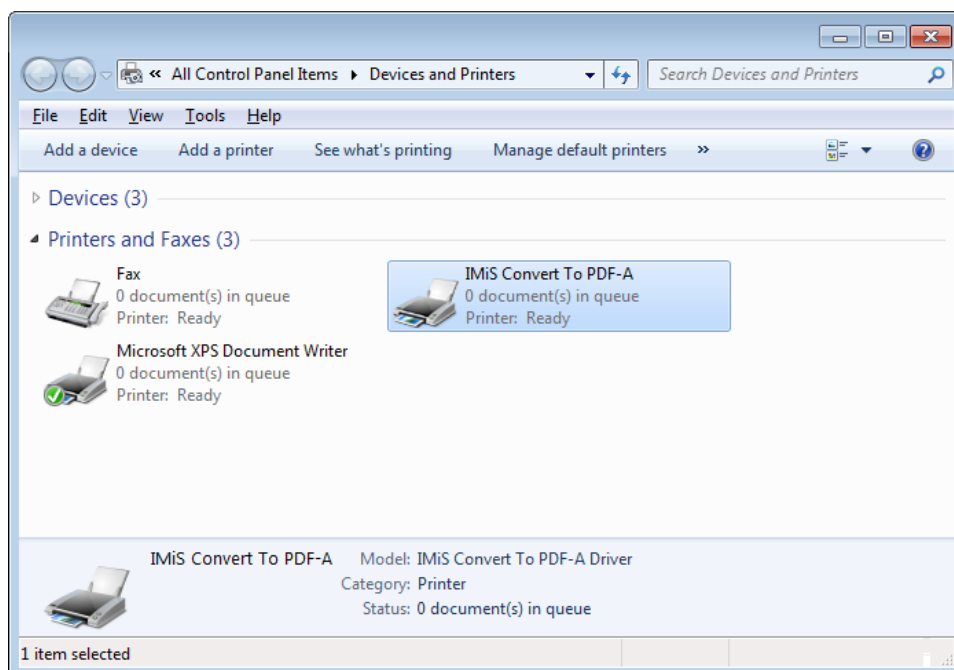choice.



Image 219: Virtual printer

# 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.
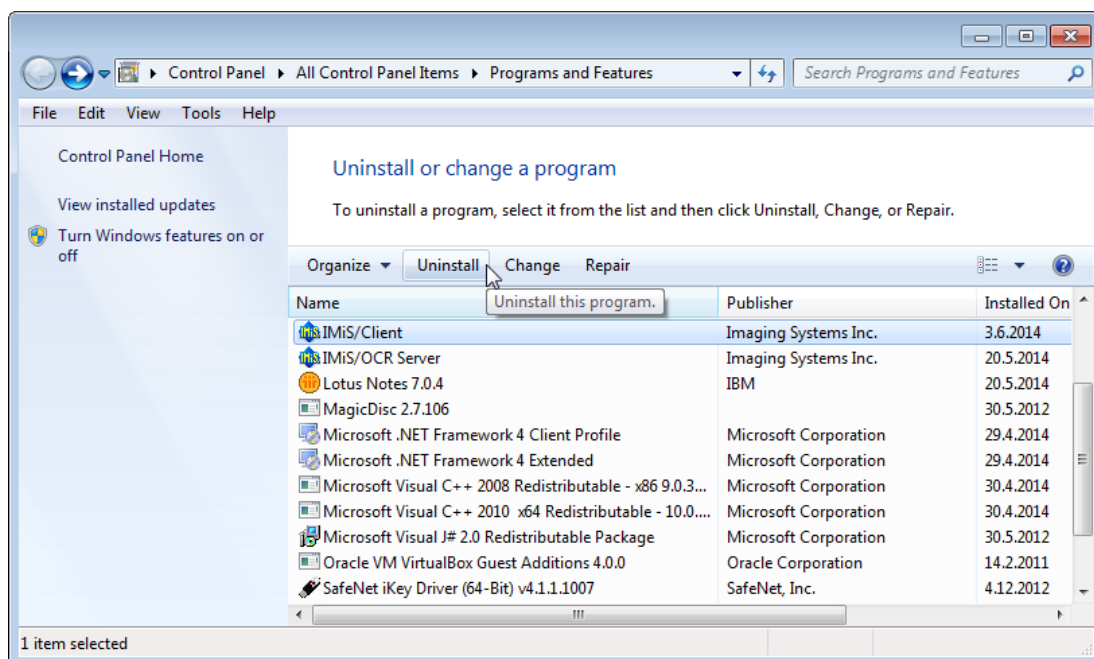


Image 220: Uninstalling the IMiS®/Client

By choosing the »Uninstall« command in the top command bar, a dialog box is opened where the administrator confirms uninstallation by choosing »Yes«, or cancels it by choosing »No«.
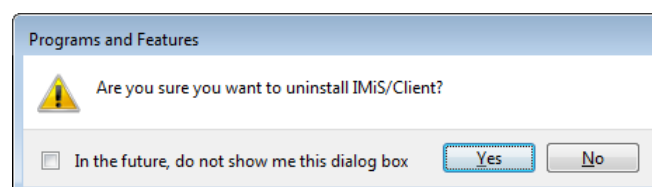


Image 221: Confirming uninstallation

If 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 222: Uninstallation progress bar

The uninstall removes all files and settings that were created by the installation package.

IMiS®/Client can also be removed using the »Change« command, which opens the initial window of the install wizard where modification, repair or removal of the client can be started by selecting »Next«.
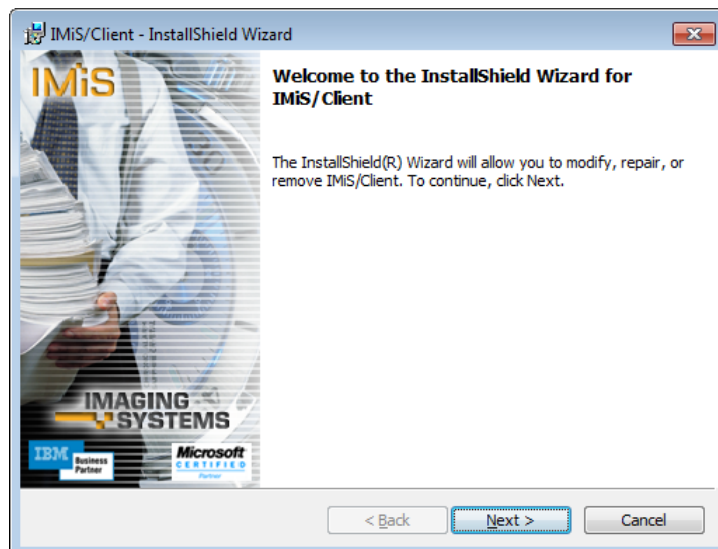


Image 223: Opening the IMiS®/Client program maintenance

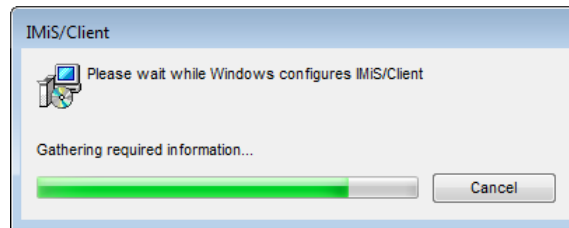If the administrator continues the procedure, the next dialog box offers the option to modify, repair or remove the client, which can be uninstalled using the »Remove« and then »Next« command.
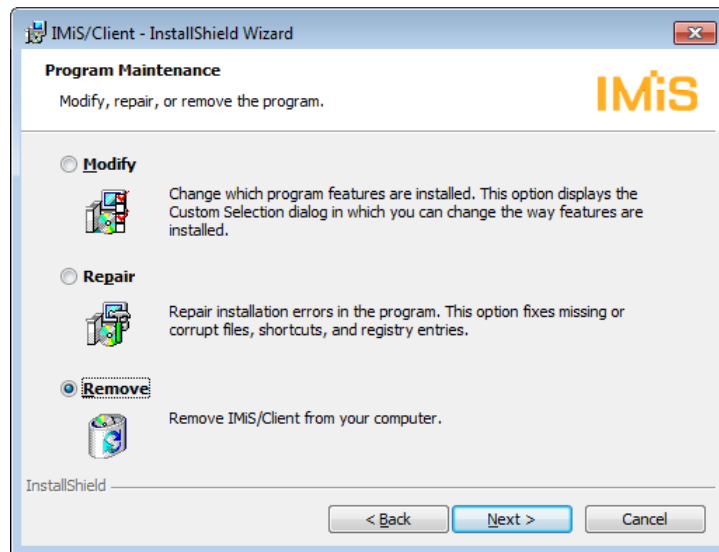


Image 224: Selecting a program maintenance action for the IMiS®/Client

At the next step, uninstallation is confirmed by clicking »Remove«.
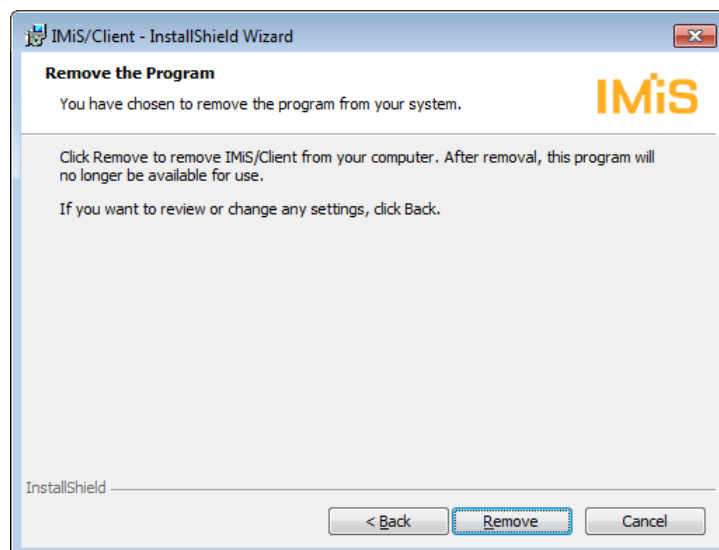


Image 225: Confirming IMiS®/Client uninstallation

If the »User Access Control« window appears during uninstallation, you must select »Yes« to agree to the uninstallation or it will be aborted.
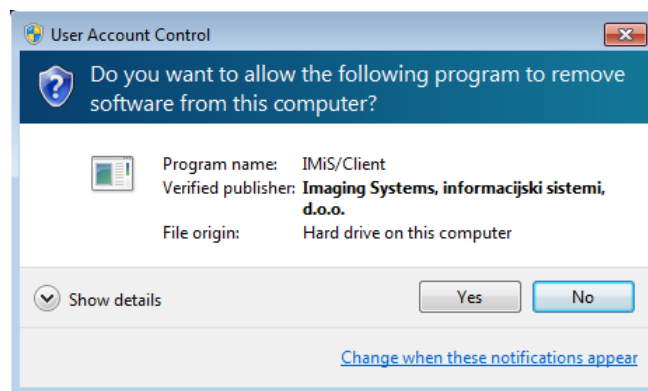
Image 226: Security warning prompt

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.



Image 227: 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.
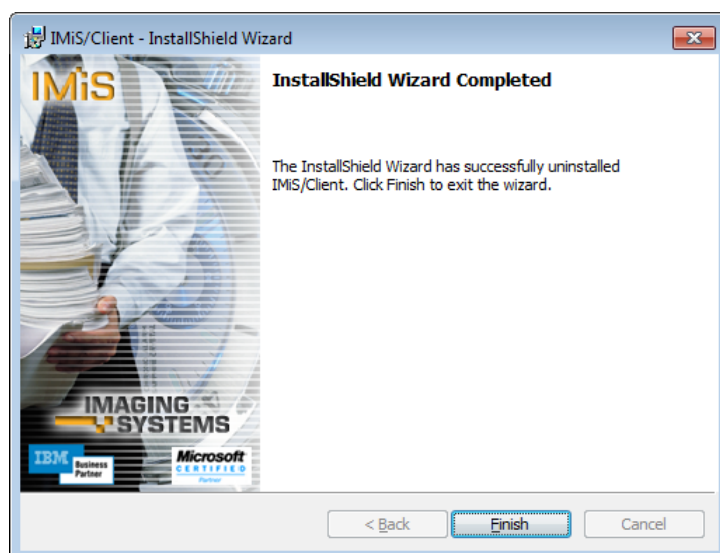For more information on this procedure *see chapter 8.3.1  Adding an IMiS®/ARChive Server*.
Users must log in before they can access the archive.
For more information *see chapter 4.2.1 Login and logout*.

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.*

## 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.
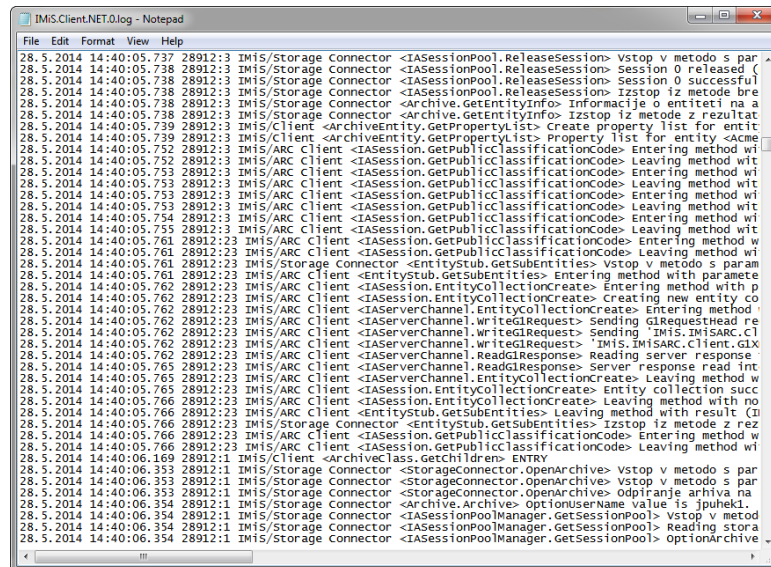


Image 228: Example log file

If there is an error in the client's operation, the entry continues with the:

- Error message, which briefly describes the error or issue.

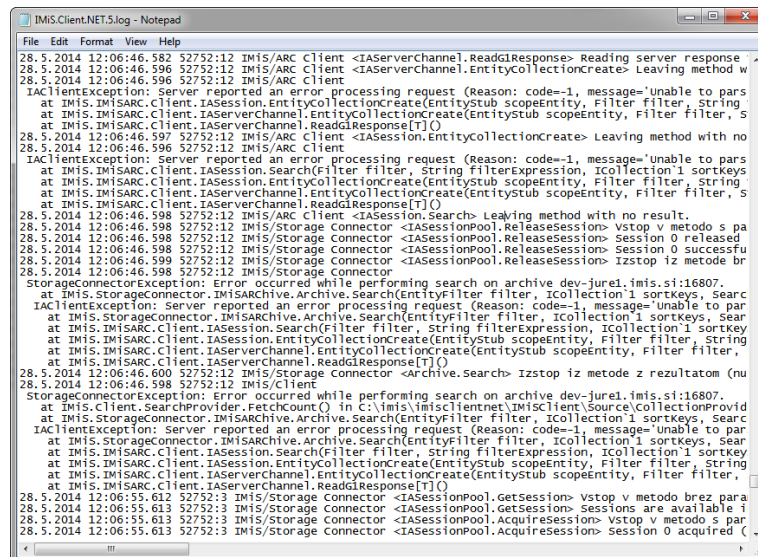- Error stack trace, which contains a detailed description of the reason for error.



Image 229: 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.
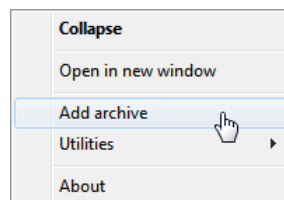


Image 230: Adding an archive via the popup menu

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, where the IP address and the name of the IMiS®/ARChive Server are entered.
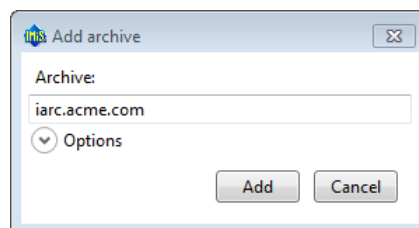


Image 231: Add archive dialog box

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.*

When the server is added, it will appear in the »Archives« folder.
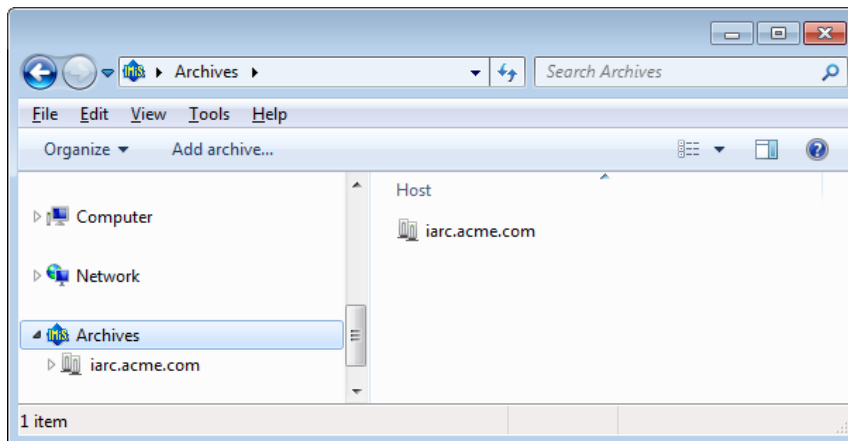


Image 232: Display of newly added archives

Users that wish to access the archive must first log into it *(see chapter 4.2.1 Login and logout)*.

### 8.3.2 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.
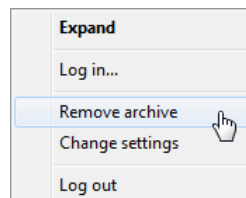


Image 233: Removing an archive via the popup menu

This will open a dialog box asking for confirmation to remove the selected IMiS®/ARChive Server.
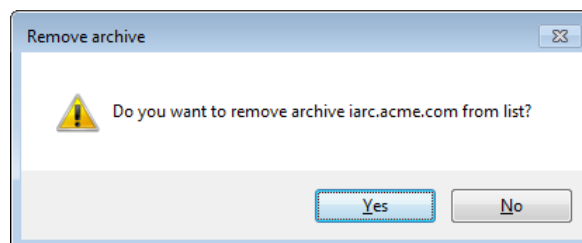


Image 234: Remove archive dialog box

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 8.3 Configuring in the IMiS®/ARChive Server manual.*

## 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.
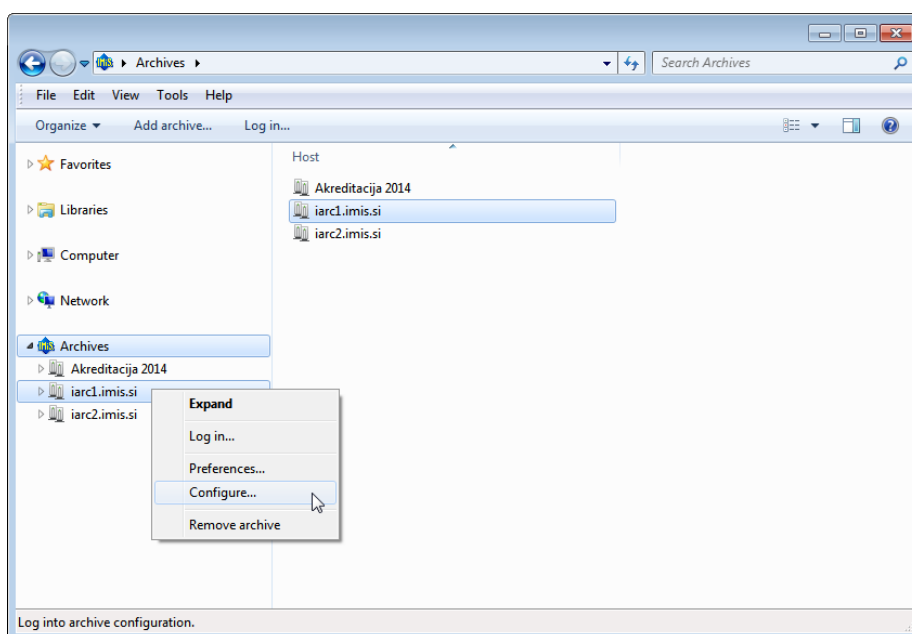


Image 235: Choosing the »Configure« command before the user has logged into the archive

The user can also configure the IMiS®/ARChive Server after he has already logged into the archive.
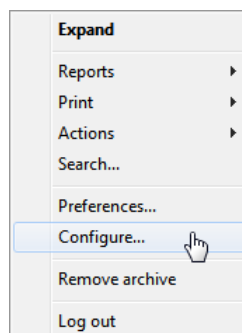


Image 236: Choosing the »Configure« command after the user has logged into the archive

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«.
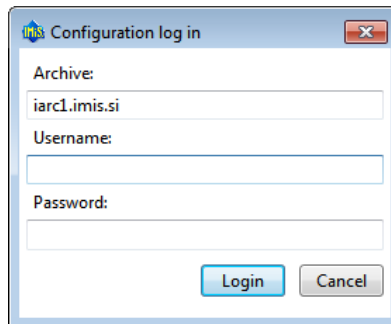


Image 237: Dialog box for entering username and password

Following a successful authentication, a list of configuration folders is displayed in the right view:
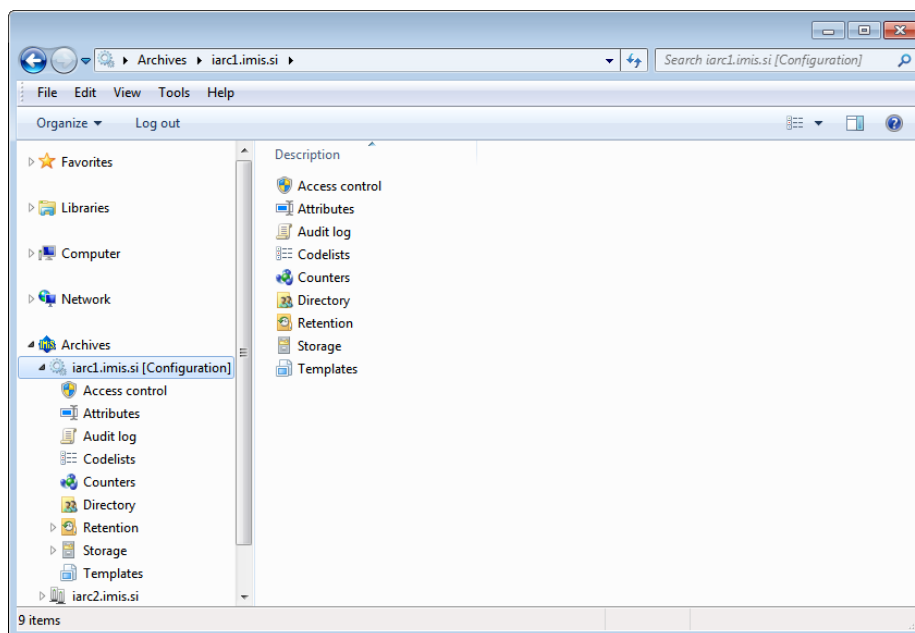


Image 238: List of available folders displayed after logging into the archive configuration

The availability of the configuration folders depends on the user's roles.

201

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.

- »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.

- »Codelists«:  contains a list of attributes, which are used to set the value range.

- »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.

- »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.

- »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.


The following commands are displayed in the command bar next to the »Organize« Windows system command:

- »Edit«:  the selected entity/objects opens 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.



Image 239: Example of a command bar in the 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 240: 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.
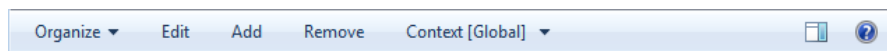


Image 241: Command bar in the »Access control« configuration folder

### 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.



Image 242: 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 243: Choosing the context in the »Access control« configuration folder

The user can choose between the following contexts:

- »Global«:  contains rights for accessing the entities and attributes on the level of the entire archive.
- »Import«:  contains rights for accessing the entities and attributes in the »Import« system folder *(see chapter 4.2.1 Import)*.
- »Export«:  contains rights for accessing the entities and attributes in the »Export« system folder *(see chapter 4.2.2  Export)*.
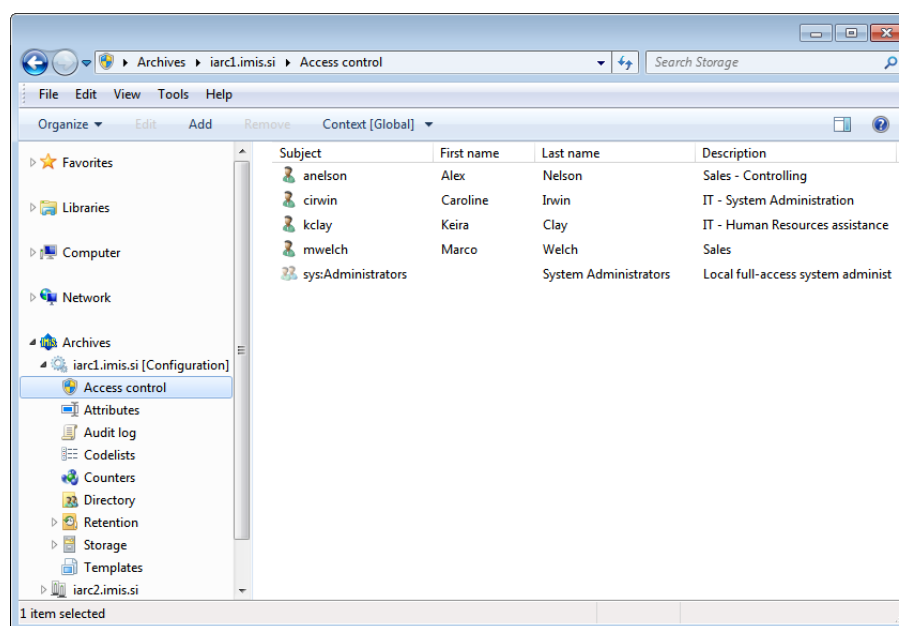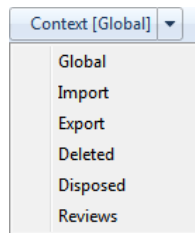- »Deleted«:  contains rights for accessing the entities and attributes in the »Deleted« folder in the »Trash« system folder *(see chapter 4.2.3 Deletion)*.
- »Disposed«:  contains rights for accessing the entities and attributes in the »Disposed« folder in the »Trash« system folder *(see chapter 4.2.4 Disposition)*.
- »Reviews«:  contains rights for accessing the reviews in the »Reviews« system folder *(see chapter 4.1 Review process)*.

### 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.

<u>»Entity rights« tab</u>

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.



Image 244: Access rights to entities

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.*

<u>»Property rights« tab</u>

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 can allow the following actions over the attributes, 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 245: 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 »Reviews«, »Export«, »Import« and »Trash«

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 »Reviews«, »Export«, »Import« and »Trash«.

Rights are described in the *chapter 8.4.1.1 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    »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.
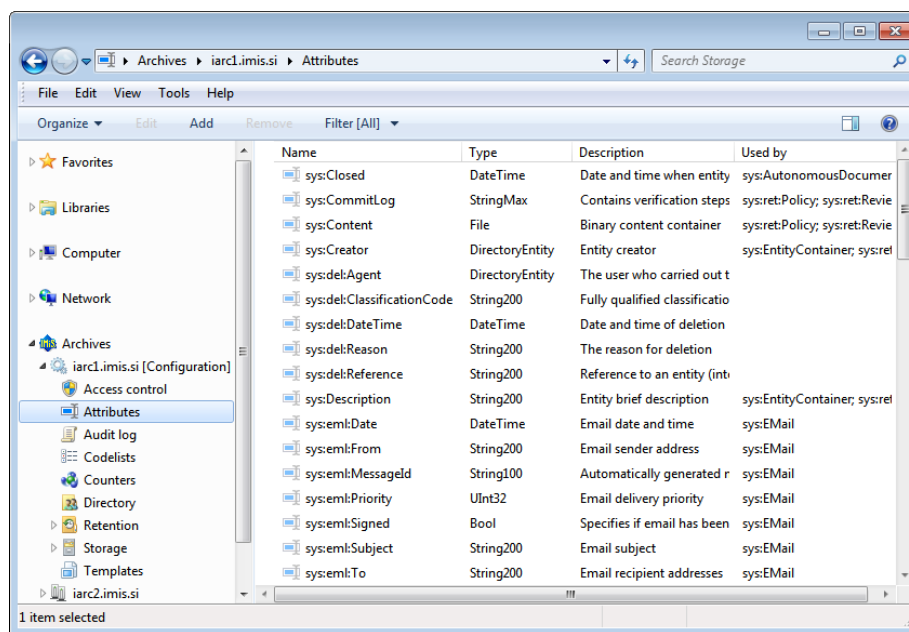


Image 246: Attribute list in the »Attribute« configuration folder

By choosing the »Filter« command in the upper command bar, the user with appropriate access rights can set the view content.
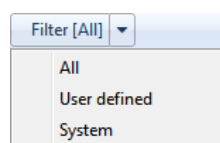


Image 247: Selecting the filter in the »Attribute« configuration folder

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.

- »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.



Image 248: Attribute properties

<u>»Use under« tab</u>

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 *(see chapter* 8.4.7 *Templates)*.



Image 249: Templates, in which the attribute is used

### 8.4.3   »Audit log« folder

The »Audit log« folder contains the audit log parameters.

<u>»Properties« tab</u>

By clicking the »Audit log« folder, the right view of Windows Explorer shows the following value settings under the »Properties« tab:

- »User name«:  requires the entering of a user name for the audit log.
- »Computer name«:  requires the entering of a computer name for the audit log.
- »Private address«:  requires the entering of a private IP address for the audit log.
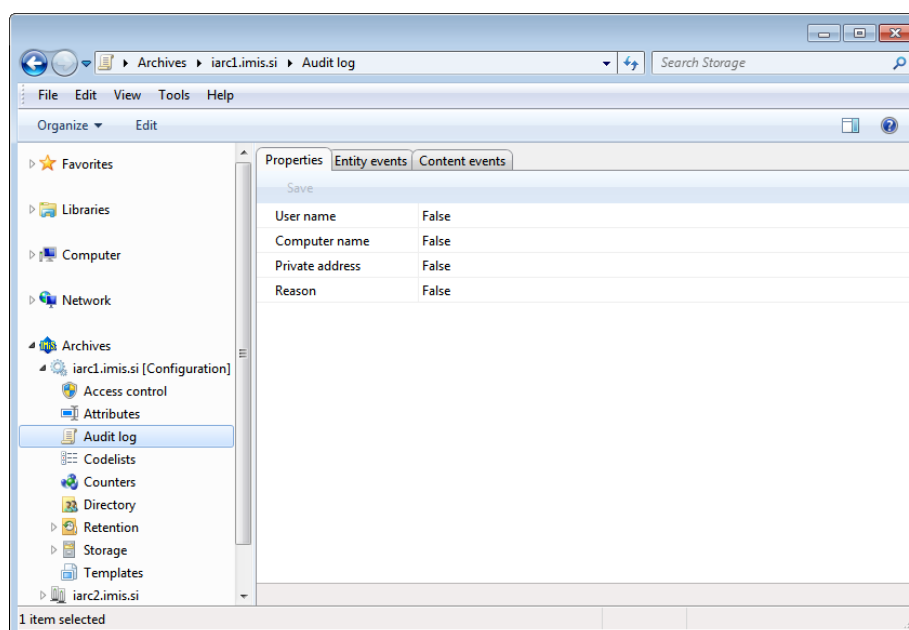- »Reason«:  requires the entering of a reason for the action which is recorded in the audit log.



Image 250:  List of properties in the »Audit log« configuration folder

<u>»Entity events« tab</u>

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.
- »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.
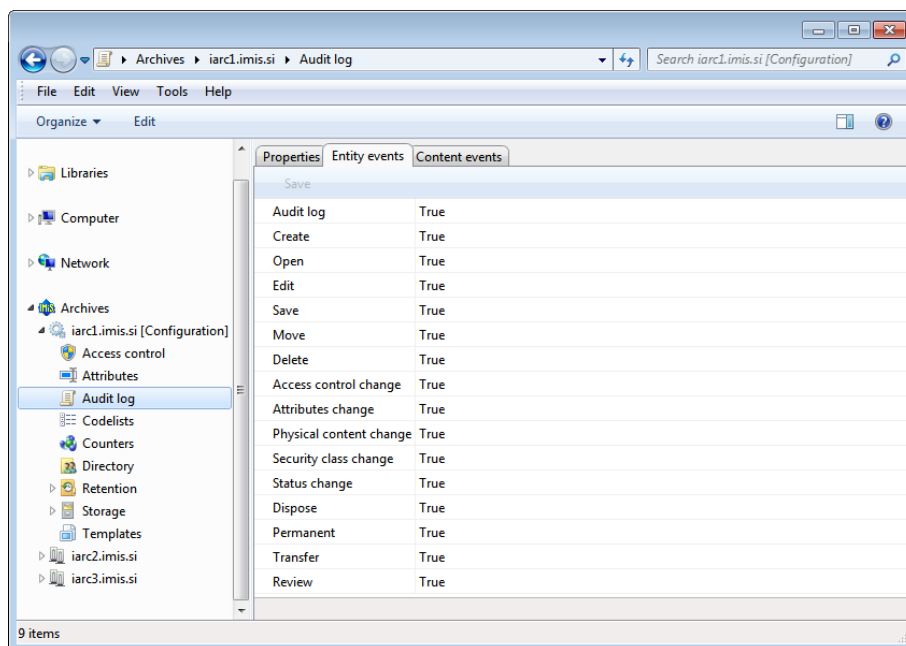
Image 251:  List of entity events in the »Audit log« configuration folder

<u>»Content events« tab</u>

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.

- »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.
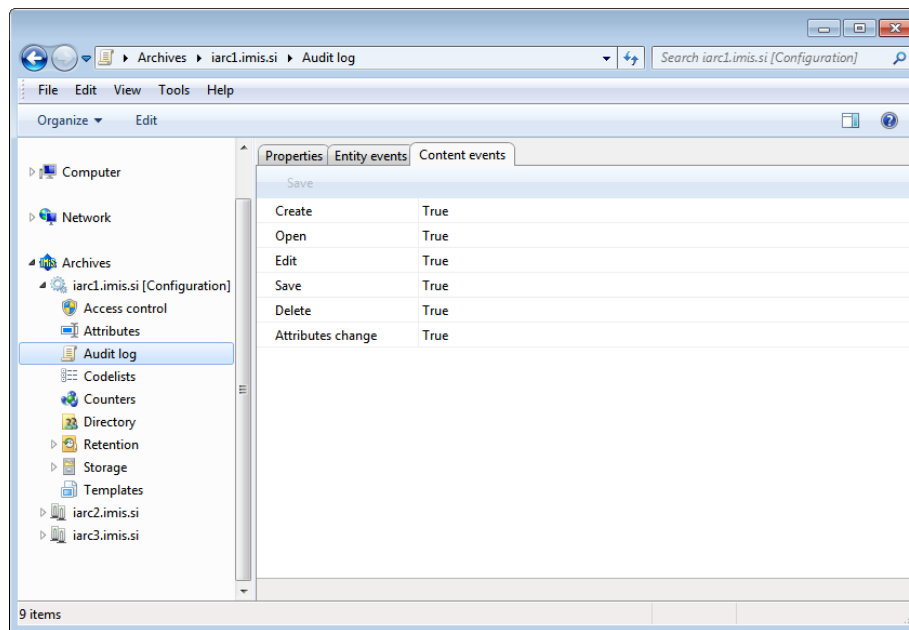
Image 252:  List of content events in the »Audit log« configuration folder

### 8.4.4    »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.
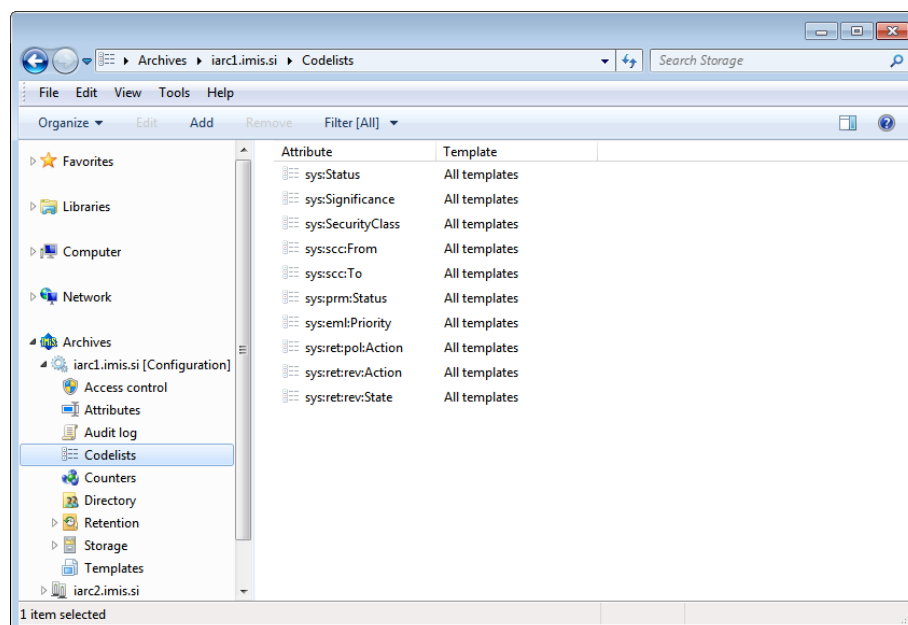- »Template«:  template, to which the codelist is tied.



Image 253: 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.
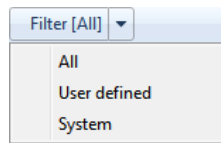


Image 254: Selecting the filter in the »Codelists« folder

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.

»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.
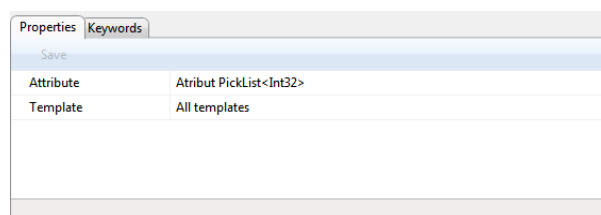


Image 255: Codelist properties

»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.*
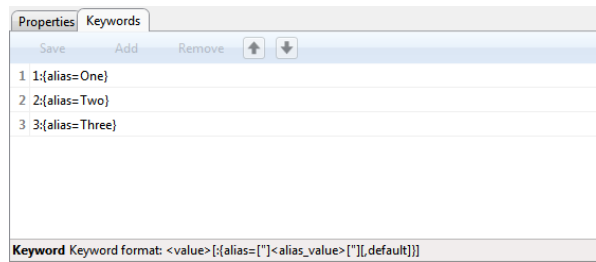
Image 256: Available attribute values

_Warning_:  It is required to restart the IMiS®/ARChive Server in order to effect changes of the value settings in the »Codelists« folder.

### 8.4.5   »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 users or user groups 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.
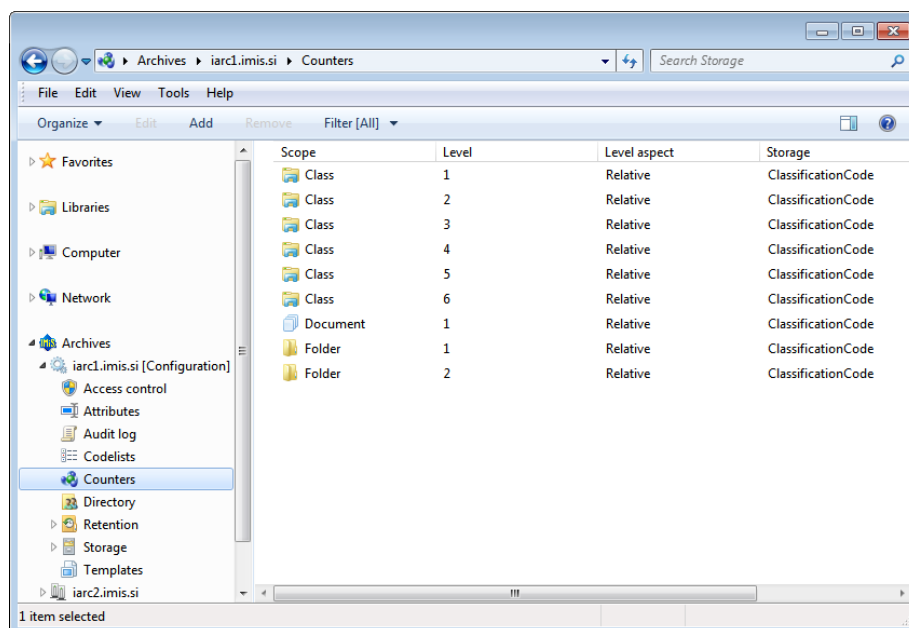- »Unique within«:  defines the uniqueness of the counter within the selected context.



Image 257: 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.
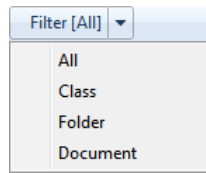


Image 258: Selecting the filter in the »Counters« folder


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.


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 subentities.


<u>»Properties« bar</u>

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 subentity 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.

| Properties | |
| --- | --- |
| Save | |
| Scope | Class |
| Level | 1 |
| Level aspect | Relative |
| Storage | ClassificationCode |
| Unique within | Parent |
| Initial value | 1 |
| Increment | 1 |
| Format | %02@count@ |

Image 259: Counter properties for the class on the first level


### 8.4.6    »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.

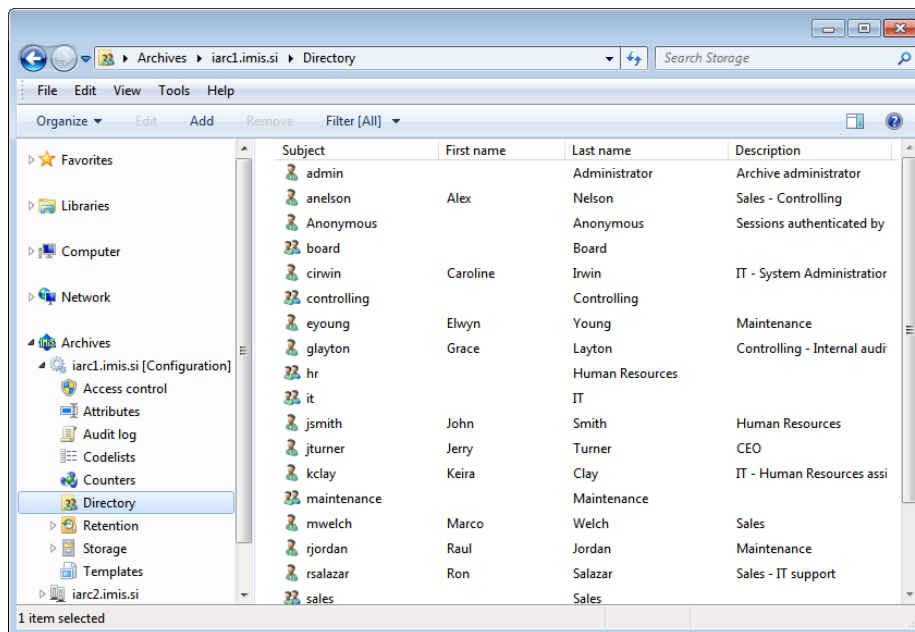- »Description«:  a short description of the user or user group.

Image 260: 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.
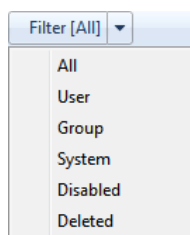


Image 261: Selecting the filter in the »Directory« folder

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.

<u>»Properties« bar</u>

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.

- »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.

- »Enabled«:  if the selected value is »True«, the user is active. When changing the value to »False«, the user with appropriate access rights can deny access to the archive.

- »Member in groups«:  contains a list of groups, in which the user is a member.
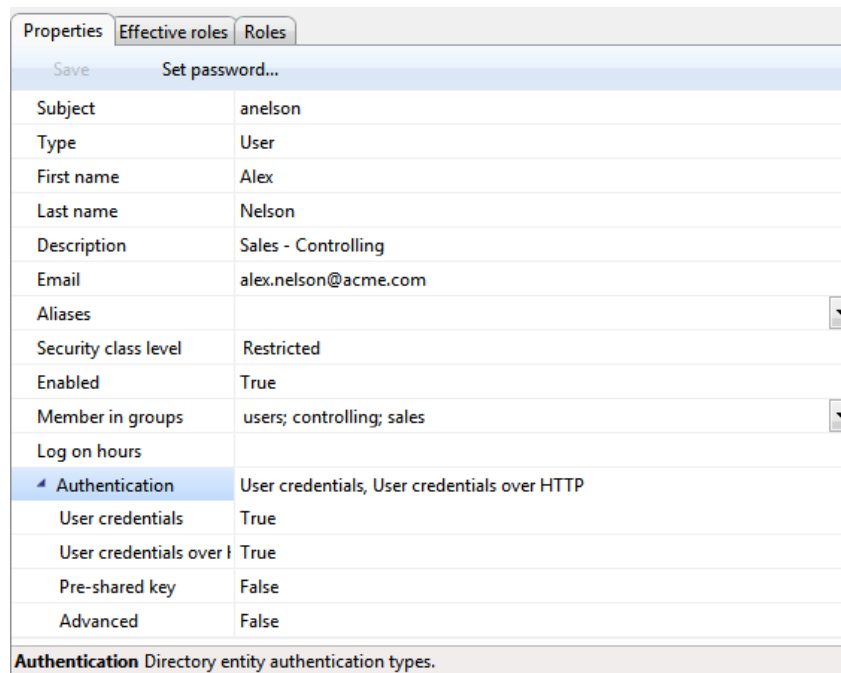
Image 262: User group properties

The fields listed above are available for users as well as for user groups. The additional value settings are displayed for the users:

- »Log on Hours«: contains an expression representing hours of the day, when the user can access the archive.
- »Authentication«: the user with appropriate access rights can set the following authentication options:
  - »User name/password«: authentication is done using the SRP-6a protocol.
  - »User Credentials over http«: authentication is done using the HTTP protocol.
  - »Pre-shared key«: authentication is done using the shared pre-set key.
  - »Advanced«: authentication is done by establishing a session with the server that foresees mandatory and optional client metadata.

  The values can be set to »True« or »False«.



Image 263: 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.

Image 264: Effective roles of the user

<u>»Roles« tab</u>

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

- Deletion

- Reports

- Review.

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 265: Explicit roles for the user

Users can access and change the following configuration folders in the »Configuration« folder:

- Access Control

- Attributes

- Codelists

- Counters

- Directory

- Profiles

- 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.*

»Members« tab

The »Members« tab  is visible only to user groups. By clicking the »Members« tab in the bottom right view of Windows Explorer, the user with appropriate access rights is shown all the members of the user group.



Image 1:  Displaying of users in a group

A user can add group members with the »Add« command or remove them with the »Remove« command.

### 8.4.7   »Retention« folder

The »Retention« folder contains the »Retention policies« and the »Disposition holds« folders.

### 8.4.7.1    »Retention policies« subfolder

The »Retention policies« subfolder contains a list of retention policies. 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 default reason for the existence of the retention policy which is used in the decision-making phase of the review process.
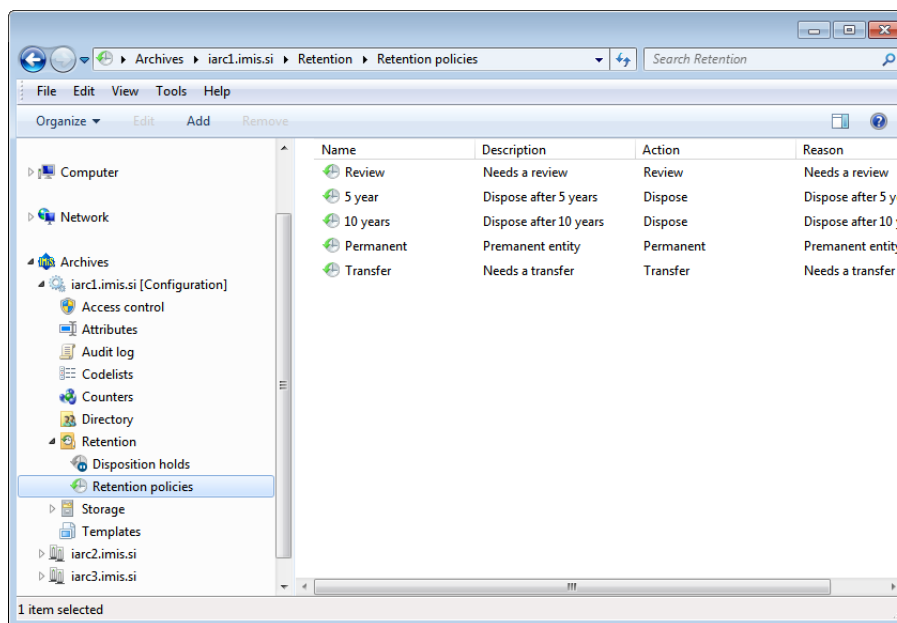


Image 266:  List of retention policies in the »Retention policies« folder

<u>»Properties« tab</u>

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:

- »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.



Image 267: 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 268: Display of retention policy mandates

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.
- »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.

### 8.4.7.2 »Disposition holds« subfolder

The »Disposition holds« folder contains a list of disposition holds.

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.



Image 269: 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:

- »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.

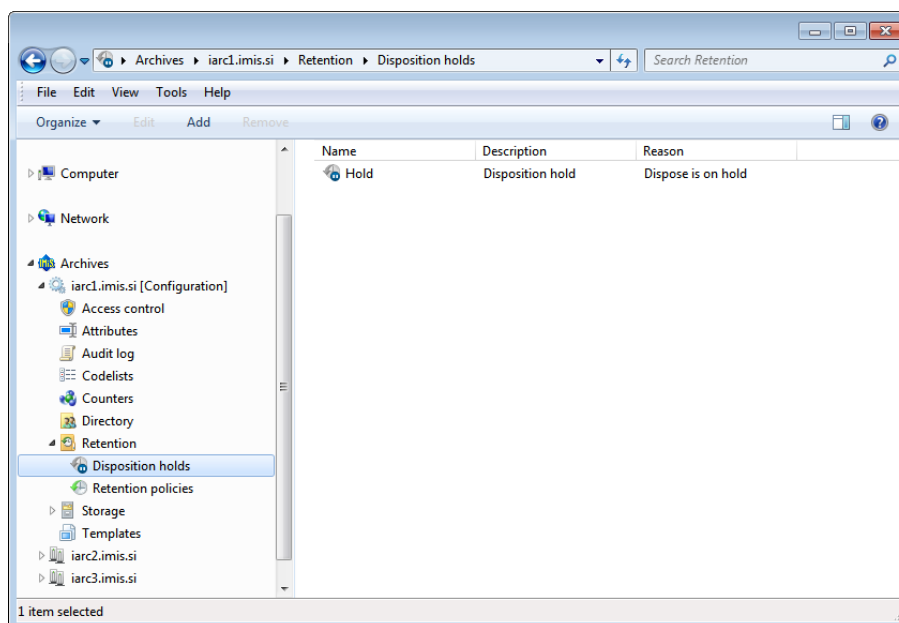- »Reason«: the default reason for the disposition hold in the implementation phase of the review process.

- »Author«: user (author) of the disposition hold.

- »Created«: the date and time when the disposition hold was created.

Image 270: Display of disposition hold mandates

### 8.4.8    »Storage« folder

The »Storage« folder contains the »Profiles« and »Volumes« subfolders.

### 8.4.8.1    »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).

- »Read only«:  if the selected value is »True«, settings can not be changed. When changing
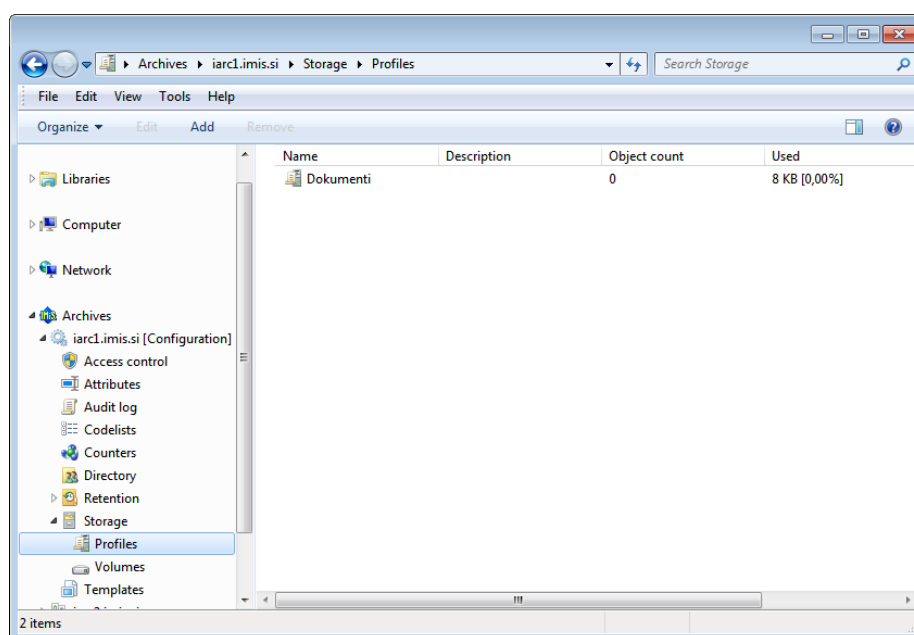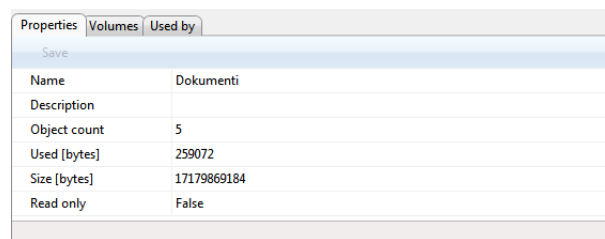the value to »False«, the user with appropriate access rights can change the settings.



Image 271: Attribute list in the »Profiles« folder

<u>»Properties« tab</u>

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.
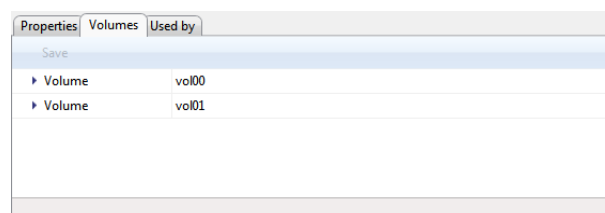


Image 272: Profile properties

<u>»Volumes« tab</u>

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 273: Volumes, which are tied to the profile

<u>»Use under« tab</u>

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 274: Using the profile under the root class of the archive

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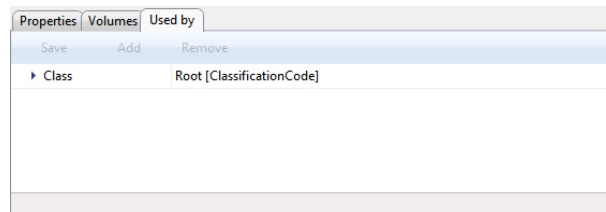. When the identifier value is not set, the profile is used on the level of the archive. Otherwise the profile is used only under the selected class. The user can enter either the classification code, the internal or external class identifier. The new class is saved by choosing the »Save« command.

The class is removed by choosing the »Remove command«.
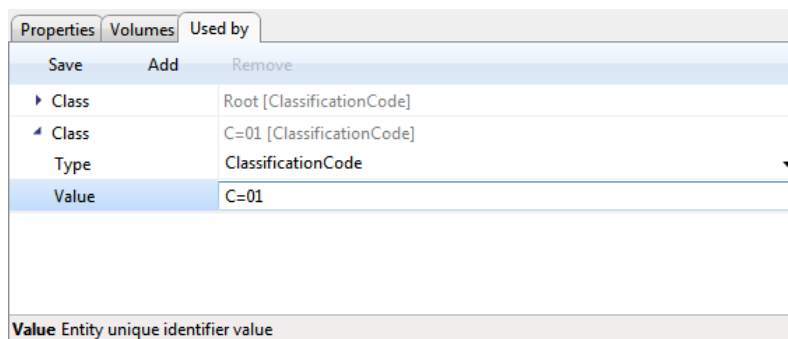


Image 275: Entering the class for profile

_Warning:  It is required to restart the IMiS®/ARChive Server in order to effect changes of the value settings in the »Storage« folder._

### 8.4.8.2    »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.
The »Properties« tab content is the same as the content of the »Volumes« tab in the »Properties« configuration subfolder.
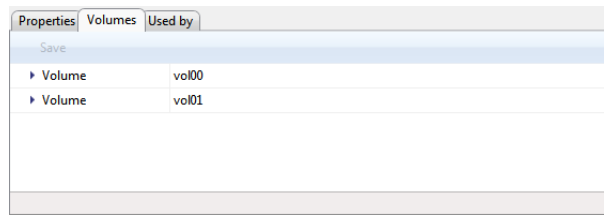
Image 276: Volumes, which are tied to the profile

»Properties« tab

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. After the value has been saved for the first time, it becomes immutable.

- »Description«:  contains a short description of the volume.

- »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.

Image 277: 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.

### 8.4.9    »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.



Image 278: 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.
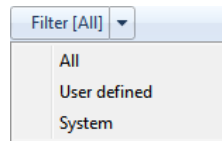


Image 279: Selecting the filter in the »Attribute« configuration folder

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.

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.

- »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 280: Template properties

<u>»Attributes« tab</u>

All attributes tied to the template, including their properties are listed in the »Attributes« tab in the lower right view of the Windows Explorer.

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.

- »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 281: List of attributes used in the template

*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.*

<u>»Use under« tab</u>

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 282: 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.

# 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.

**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.

**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

**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.

## 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.  *(see section »Error when accessing an 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.

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. *See section »Error when accessing an archive«*.

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.

238