



IMiS^(R)/Notes Interface Administrator's Guide

Version 8.2.1507

**IMAGING
SYSTEMS**

Imaging Systems Inc.
Brnciceva 41g
Ljubljana
Slovenia

TABLE OF CONTENTS

1	INTRODUCTION.....	4
1.1	Purpose of the guide	4
1.2	Target audience.....	4
1.3	Scope and requirements	4
1.4	Conventions.....	5
1.5	Abbreviations.....	5
2	ADMINISTRATION INTERFACE.....	6
2.1	General	6
2.2	Accessing the administration interface.....	6
2.3	Exiting the administration interface.....	7
2.4	Administration interface view	7
2.4.1	Left view	7
2.4.2	Central view	8
2.5	Access rights.....	8
2.6	Changing settings.....	8
3	STORAGE SERVERS.....	9
3.1	New Storage Server document.....	9
3.2	Description of settings.....	10
3.2.1	General	10
3.2.2	Protocols.....	10
4	ACTIVATED USERS.....	15
4.1	Overview of the user environment.....	17
5	DATABASE PROFILE	18
5.1	References to Notes databases in the Database profile	19
5.2	Migration of Notes databases between Database profiles.....	19
5.3	New Database Profile document	20
5.4	Description of settings.....	20
5.4.1	Basic information.....	20
5.4.2	Basic options	21
5.4.3	Advanced options	22
5.4.4	Document security	25
5.4.5	Object security	27
5.5	Additional settings	29
5.6	Overview of Notes databases.....	31
6	DOCUMENT TYPES.....	31
6.1	Overview of existing document types.....	31
6.2	New document type.....	32
7	LOG EVENTS.....	33
7.1	Log event	34

7.1.1	Basic information.....	34
7.1.2	User information.....	34
7.1.3	Event information	35
7.1.4	Context information	35
8	AUDIT LOG QUERY	35
9	TROUBLESHOOTING	40
9.1	Most frequent errors	40
9.2	List of errors in the event log.....	41

1 INTRODUCTION

This part presents the contents and language of the IMiS®/Admin Administrator's Guide and offers advice on the technical and operation aspects of application management.

1.1 Purpose of the guide

The guide describes administrator tasks required for the management and configuration of the IMiS®/Admin module. It is intended for:

- Management of Notes databases and users.
- Faster error tracing.
- Faster handling and debugging of errors.
- Easier and faster administration of IMiS® modules.
- Faster enabling of IMiS® Design elements in individual Notes databases.
- Faster upgrading, in the sense of achieving compatibility between old and new Notes databases.

1.2 Target audience

The guide is intended for system administrators with a knowledge of IBM Domino/Notes administration.

1.3 Scope and requirements

The guide deals specifically with administrative tasks and option settings for IMiS®/Admin on the IBM Domino/Notes platform.

For information on the installation of IMiS®/Admin, the IMiS® technical support is at your disposal at the email address: support@imis.si.

1.4 Conventions

The Administrator's Guide uses various styles and colors to highlight important information. These are explained below:

Text style	Purpose
Regular	Basic information, description of functionalities
<u>Underlined text</u>	Field values
»Quotation«	Names of headers and tabs, warnings
[Green text]	Names of sections and subsections
[Red text]	Names of actions over the selection, options selectable from the dropdown menu
[Blue text]	Names of Notes document fields

1.5 Abbreviations

The table below shows the abbreviations used in the text and images of this guide:

Abbreviation	Meaning
IMiS®/Admin	Administration interface
IMiS® modules	IMiS® functionalities consolidated into products
IMiS®/ARChive Server	Archive server
IMiS®/OCR Server	OCR server
IMiS®/Net	Object forwarding interface between the application server and the IMiS®/ARChive Server
IMiS® design elements	IMiS® application components that enable IMiS® functionalities
Finereader Engine	Core of the IMiS® module for optical character recognition (OCR)

2 ADMINISTRATION INTERFACE

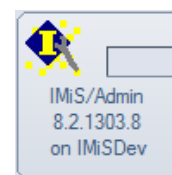
2.1 General

The IMiS®/Admin interface enables the configuring of the IMiS® system. This chapter presents the following topics:

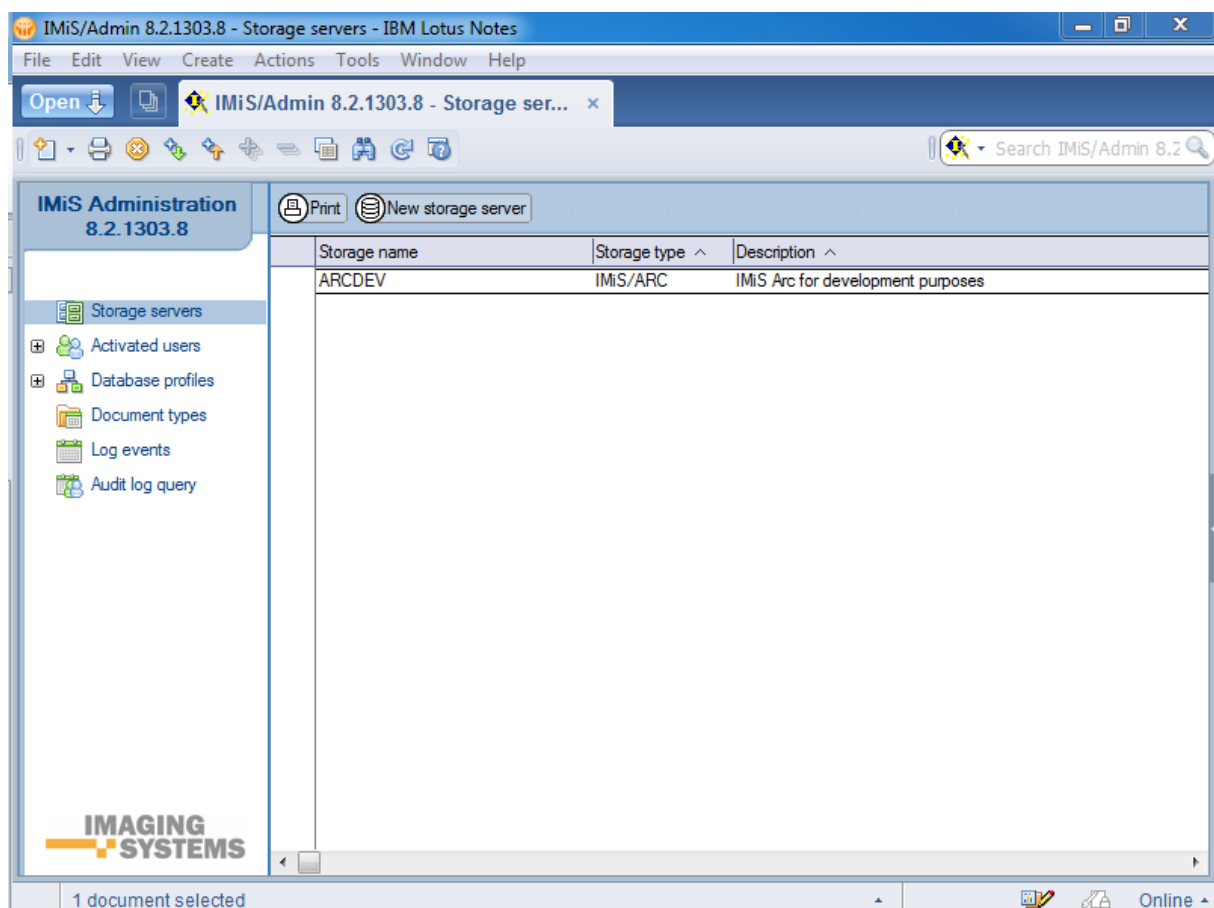
- Accessing the administration interface
- Exiting the administration interface
- Administration interface view.

2.2 Accessing the administration interface


IMiS®/Admin is launched by clicking the IMiS/Admin icon 8.2.1303.8.



The basic administration interface appears on-screen:



2.3 Exiting the administration interface

Exit IMiS®/Admin by clicking the  button in the tab.



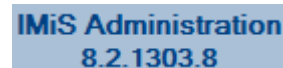
2.4 Administration interface view

The interface consists of two views:

2.4.1 Left view

Left view displays the version number and the left menu.

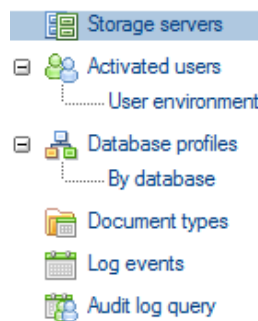
The version of the IMiS®/Admin database is shown on top.



The version number reveals the corresponding design of the administration Notes database.

The version is important in the context of automatic upgrades or data update procedures.

The left menu offers the following options:



[Storage Servers] Manage the settings of IMiS®/ARChive Servers (test or production servers), or other storage servers.

[Activated users] Specify the users of individual IMiS® modules.

[User environment] Monitor the activities of IMiS® module users.

[Database profiles] Specify the profile and resulting properties of individual Notes databases or groups of Notes databases.

[Document types] Table of all authorized document types that are saved as objects on IMiS®/ARChive Servers or other storage servers.

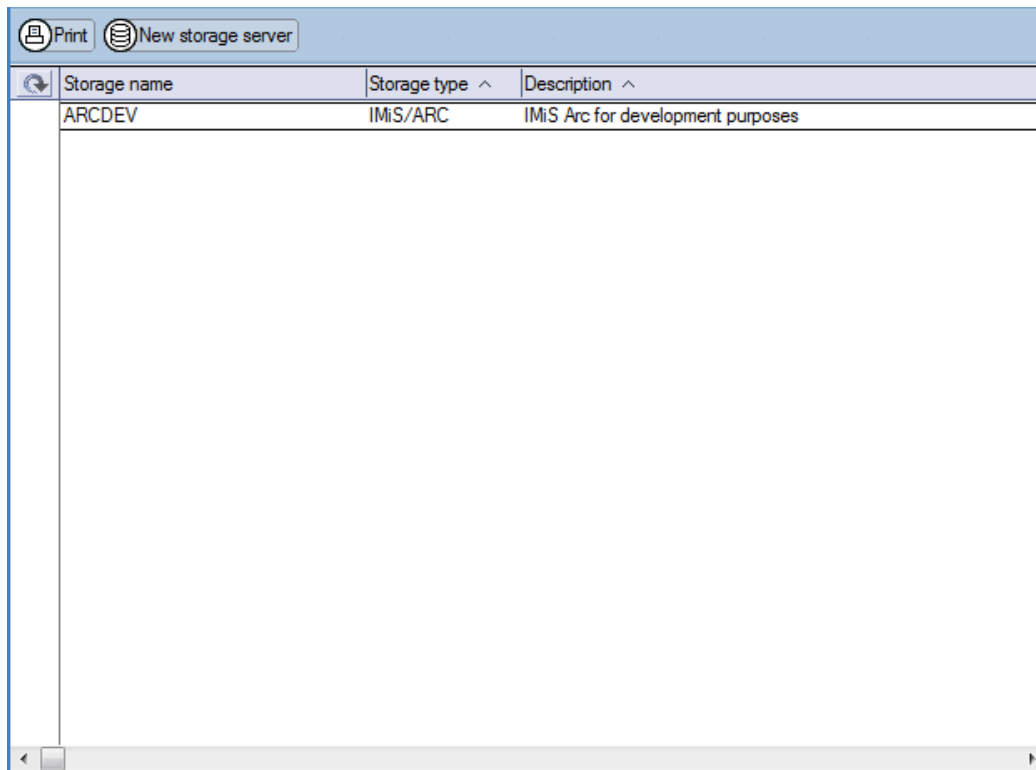
[By database] Overview of Notes databases that include IMiS® functionalities.

[Log events] Log of errors and warnings recorded during the execution of operations.

[Audit log query] Create an audit log detailing the execution of operations over objects archived on storage servers, based on a query.

2.4.2 Central view

The default central view shows a list of available storage servers and offers several executable actions.



The screenshot shows a web application window with a blue header bar. On the left, there is a vertical sidebar with a search icon and a 'New storage server' button. The main content area contains a table with three columns: 'Storage name', 'Storage type', and 'Description'. The table has one data row with the values 'ARCDEV', 'IMiS/ARC', and 'IMiS Arc for development purposes'. Below the table is a horizontal scrollbar.

Storage name	Storage type ^	Description ^
ARCDEV	IMiS/ARC	IMiS Arc for development purposes

[New storage server] Specify a new storage server for the purposes of administration.

For each storage server (test or production server), information that must be specified is the server's name (**Storage Name**), type of server (**Storage type**) and description of the server or its purpose (**Description**).

2.5 Access rights

The administrator is authorized to access all the settings of IMiS®/Admin and change them (editor). Users need to be granted the right to read and write public documents (Write public documents).

2.6 Changing settings

[Edit] Change or add individual field values.

[Save] Save the settings of the current document.

[Close] Close the current document.

[Print] Print the settings of the selected storage server.

For better performance, settings are written into a memory structure that refreshes every 30 minutes. To activate changes immediately, the IBM Notes client must be restarted.

3 STORAGE SERVERS

This chapter deals with the following topics:

- Specifying the settings of a new document
- Description of settings.

In the **Storage servers** section, it is necessary to create an individual document for each storage server used.

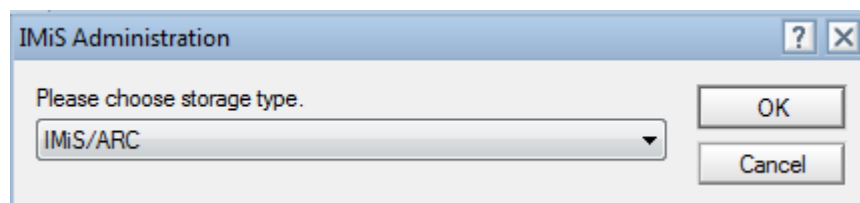
3.1 New Storage Server document

Specify the settings for each storage server. Mandatory fields are: **Name**, **Host name**, **Profile** and **Port**.

[Storage type] Choose the type of the storage server from the menu. The default setting is IMiS/ARC.

The screenshot shows a configuration window titled "STORAGE SERVER (IMiS/ARC)" with the IMAGING SYSTEMS logo in the top right. The window has a toolbar with "Close", "Save", "Storage type", and "Revision history" buttons. The main area is divided into sections: "General" with "Name:" and "Description:" fields; "Protocols" with a tabbed interface showing "Native" and "IMiS/Net"; and "Basic information" with "Host name(s):", "Profile(s):", "Allow audit log queries:" (set to "No"), "Port(s):", and "Authentication type:" (set to "Basic").

For historical/compatibility reasons, several other storage server types are also supported (Storage type): File Server, Lotus Domino.Doc and IBM Content Manager.



3.2 Description of settings

3.2.1 General

Under the »General« header, the name and type of the storage server is specified along with a short description.

STORAGE SERVER (IMiS/ARC)		IMAGING SYSTEMS
General		
Name:	ARCDEV	Description: IMiS Arc for development purposes

[Name] Name of the storage server, logged in the ObjectHandle Prefix.

[Description] A short description of the storage server or its purpose. This field isn't mandatory, but it's useful for optimal clarity in server management.

3.2.2 Protocols

The »Protocols« header specifies the type of access to objects on the IMiS®/ARChive Server. You may choose between direct access (»Native«) and indirect access via web browser (»IMiS®/Net«).

3.2.2.1 Settings

3.2.2.1.1 Basic information

The »Basic information« header specifies basic storage server information.

Protocols	
Native	IMiS/Net
Basic information	
Host name(s):	dev-iarc.imis.si
Profile(s):	Documents
Allow audit log queries:	Yes
Port(s):	16807
Authentication type:	Advanced

[Host name(s)] Set the name and address of the storage server. In case of several Host servers (cluster connections), these are set in succession. When simultaneously using more than one Host server, this requires an equal number of open ports. This field is mandatory.

[Profile(s)] For better management and easier searching, objects on the storage server are classified into profiles. This field requires the listing of all profiles over which we wish to execute administrative tasks, and is mandatory.

[Port(s)] Set the number of ports that allow forwarding of objects from/to the storage server. When using more than one port, the process requires an equal number of Host servers. This field is mandatory.

[Allow audit log queries] By choosing Yes you will monitor events connected to the stored object. The header »Audit log query session information« appears, offering additional settings explained later in the guide.

[Authentication type] Setting the authentication type to Advanced increases object security. The header »Advanced information« appears, offering additional settings presented below. The fields [Key strength](#), [Encryption mode](#), [Encryption algorithm](#) and [Encryption block size](#) are set to default values already, but can be changed.

3.2.2.1.2 Advanced Information

The »Advanced information« header manages the authentication data of user sessions. User sessions are allowed all the operations with the exception of accessing the audit trail. For the purposes of audit trails, the interface uses authentication data from the header »Audit log query session information«.

Advanced information			
Key type:	<input type="text" value="PSK (Pre-shared key)"/>	Key strength:	<input type="text" value="256 bit"/>
Pre-shared key:	<input type="text" value="lQUopiOP6G3C4lpZfhWi7FX"/>	Encryption algorithm:	<input type="text" value="AES (Advanced Encryption Standard)"/>
Encryption mode:	<input type="text" value="CBC (Cipher-block chaining)"/>	Encryption block size:	<input type="text" value="128 bit"/>

[Key type] By setting the key type to PSK (pre-shared key) the interface uses deciphered/encrypted values from the [Pre-shared key](#) field for authentication, as described below.

[Pre-shared key] The pre-shared key is specified by the administrator of the server IMiS®/ARChive Server for the authentication of user sessions that are allowed to access the audit trail. To prevent unauthorized access, the value is stored in an encrypted form and is deciphered by the interface in real time for the duration of the session.

[Encryption mode] The default setting is CBC (Cipher-block chaining). Other possible options are: ECB (Electronic codebook), OFB (Output feedback – 128 bit) and CFB (Cipher feedback – 128 bit). The setting must correspond to one of the allowed types of authentication data encryption, which are set by the administrator of the IMiS®/ARChive Server.

[Key strength] Sets the size of the encryption key and is expressed in bits. Higher values reflect greater key strength and unauthorized access protection. The default value is 256 bit. Other possible options are: 128 bit and 192 bit. The setting must correspond to one of the allowed types of authentication data encryption, which are set by the administrator of the IMiS®/ARChive Server.

[Encryption algorithm] Sets the authentication data encryption algorithm. The default setting is AES (Advanced Encryption Standard), which is also the only possible option. The setting must correspond to one of the allowed types of authentication data encryption, which are set by the administrator of the IMiS®/ARChive Server.

[Encryption block size] Sets the size of the encryption block, expressed in bits. The default setting is 128 bit, which is also the only possible option. The setting must correspond to one of the allowed types of authentication data encryption, which are set by the administrator of the IMiS®/ARChive Server.

3.2.2.1.3 Audit log query session information

The »Audit log query session information« header sets encryption parameters for the authentication data of user sessions authorized to access the audit trail. The interface uses this data whenever a session trying to access the audit trail is started, independently from any other already existing user sessions dealing with other operations over the archived objects. The topic is covered extensively in the IMiS®/ARChive Server user manual, which is separate from this guide.

Audit log query session information	
Key type:	PSK (Pre-shared key) ▾
Pre-shared key:	lqodCTClmo7j3W0ymtx1mw ▾
Encryption mode:	CBC (Cipher-block chaining) ▾
Key strength:	256 bit ▾
Encryption algorithm:	AES (Advanced Encryption Standard) ▾
Encryption block size:	128 bit ▾

[Key type] By setting the key type to PSK (pre-shared key) the interface uses **deciphered** values from the field Pre-shared key for authentication, as described below.

[Pre-shared key] The pre-shared key is specified by the administrator of the server IMiS®/ARChive Server for the authentication of user sessions that are allowed to access the audit trail. To prevent unauthorized access, the value is stored in an encrypted form and is deciphered by the interface in real time for the duration of the session.

[Encryption mode] The default setting is CBC (Cipher-block chaining). Other possible options are: ECB (Electronic codebook), OFB (Output feedback – 128 bit) and CFB (Cipher feedback – 128 bit). The setting must correspond to one of the allowed types of authentication data encryption, which are set by the administrator of the IMiS®/ARChive Server.

[Key strength] Sets the size of the encryption key and is expressed in bits. Higher values reflect greater key strength and unauthorized access protection. The default value is 256 bit. Other possible options are: 128 bit and 192 bit. The setting must correspond to one of the allowed types of authentication data encryption, which are set by the administrator of the IMiS®/ARChive Server.

[Encryption algorithm] Sets the authentication data encryption algorithm. The default setting is AES (Advanced Encryption Standard), which is also the only possible option. The setting must correspond to one of the allowed types of authentication data encryption, which are set by the administrator of the IMiS®/ARChive Server.

[Encryption block size] Sets the size of the encryption block and is expressed in bits. The default setting is 128 bit, which is also the only possible option. The setting must correspond to one of the allowed types of authentication data encryption, which are set by the administrator of the IMiS®/ARChive Server.

3.2.2.2 IMiS®/Net

3.2.2.2.1 Basic information

The »Basic information« header sets the preferred type of access to objects archived on the storage server.

Native IMiS/Net	
Basic information	
Enabled for Web browser:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enabled for Notes client:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Agent URL:	<input type="text"/>
API version:	<input type="text"/>

[Enabled for Web browser] By choosing Yes objects on the storage server may be accessed via web browser. Two additional fields open up, the Agent URL and API version in addition to the new header »Options« with new settings presented in the following paragraph.

[\[Enabled for Notes client\]](#) IMiS®/Admin version 8.2.1303.8 supports access to objects via IMiS®/Net from IBM Notes clients exclusively.

[\[Agent URL\]](#) State the URL address of the agent that serves the object content.

[\[API version\]](#) By setting the URL address version of IMiS®/Net functionality: 1 , 2 , 3 , you enable the generation of an URL address and the calling of this IMiS®/Net functionality. The structure of the URL address changes with time (Notes database ID, document ID, object index, ...) and it is therefore important to create the URL based on current information.

3.2.2.2.2 Options

The »Options« header sets the user authentication and icon display options.

Options	
Authentication type:	<input type="text" value="Yes"/>
User name:	<input type="text" value="James Hunt"/>
Password:	<input type="password" value="*****"/>
View icon URL:	<input type="text"/>
Download icon URL:	<input type="text"/>

[\[Authentication type\]](#) If you'd like to employ additional authentication for the execution of IMiS®/Net functionalities, choose the setting Yes and specify the [User name](#) and [Password](#).

[\[User name\]](#) Set a user name for an extra layer of security.

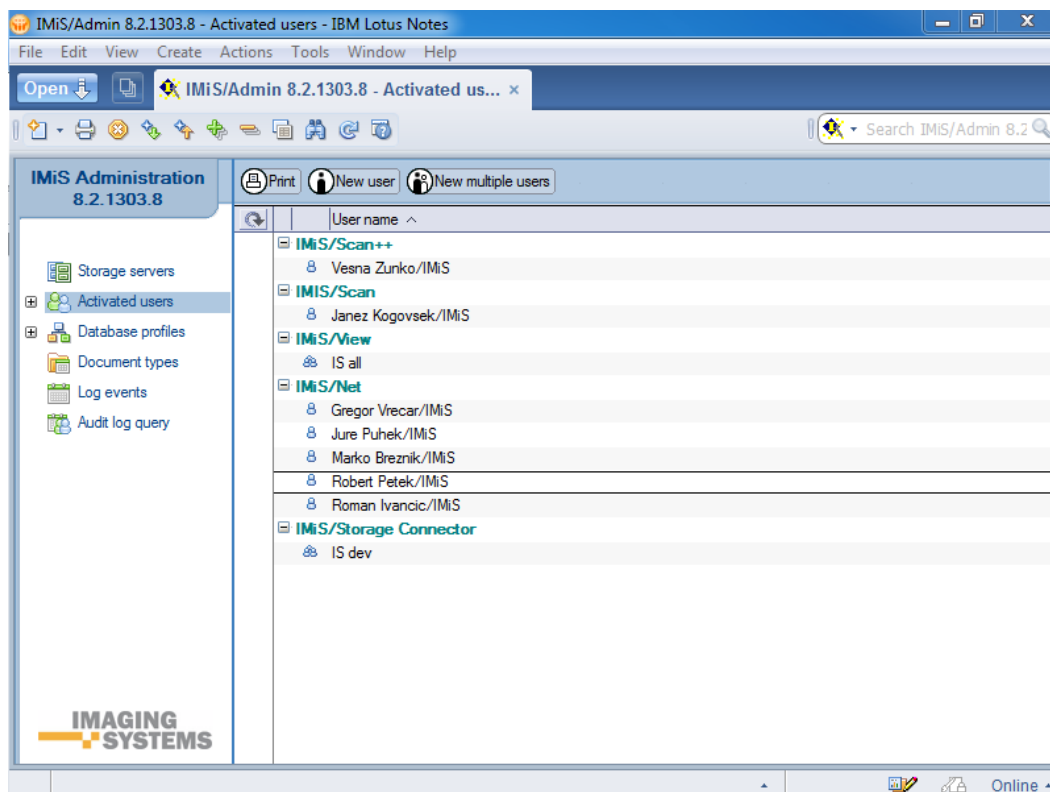
[\[Password\]](#) Set a password for an extra layer of security.

[\[View icon URL\]](#) Enter the path to the GIF file of your custom "View" icon that suits the appearance of the application. If no path is entered, the default icon will be used.

[\[Download icon URL\]](#) Enter the path to the GIF file of your custom "Download" icon that suits the appearance of the application. If no path is entered, the default icon will be used.

4 ACTIVATED USERS

The **Activated users** section specifies the users of various IMiS® functionality sets.



[New user] Choose a user, group of users or a server from the menu (**User name**) and specify the set of IMiS® functionalities they will use (**Client type**).

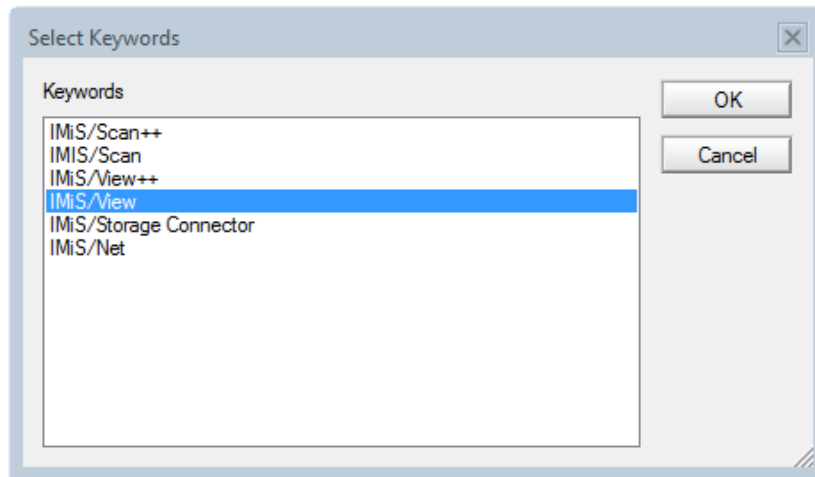
Users are arranged into groups for easier maintenance and administration.

Choosing a user name is mandatory.

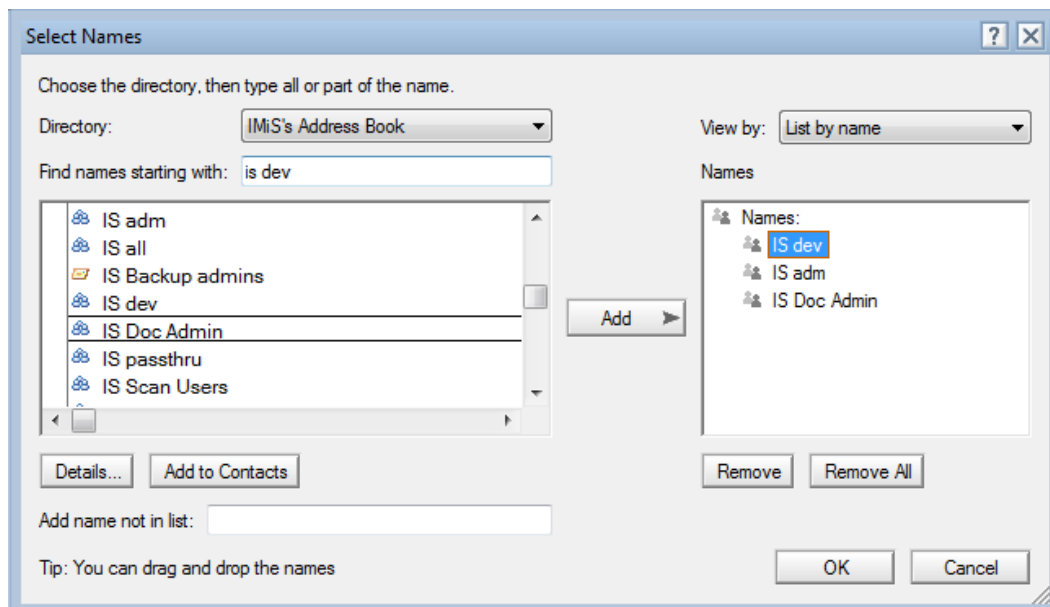
ACTIVATED USER	
<div>IMAGING SYSTEMS</div>	
<div>Basic information</div>	
User name: <input type="text" value="Bine Zerko/IMiS"/> - <input type="text" value="Person"/>	Client type: <input type="text" value="IMiS/Scan"/>

In most cases, after the user name has been selected, the type of user (Person, Group, Server) is automatically entered into the field if you click on it when it's empty. When the type of user cannot be precisely specified from the address book, you need to enter it manually.

Choose the type of user for one of the available options (IMiS®/Scan++, IMiS®/Scan, IMiS®/View++, IMiS®/View, IMiS®/StorageConnector, IMiS®/Net).

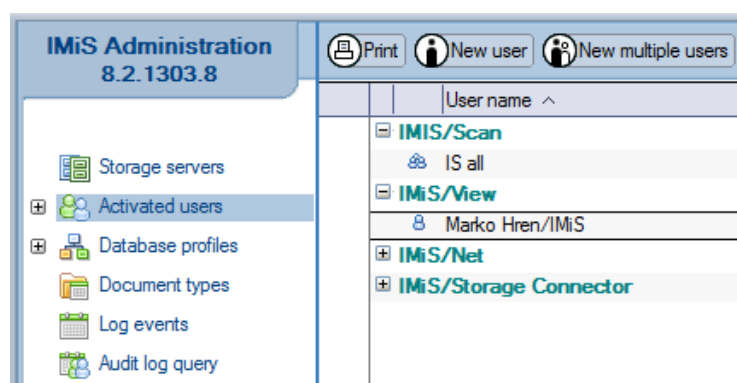


[New multiple users] Choose users, groups of users or servers from the menu and specify the set of IMiS® functionalities they will use.



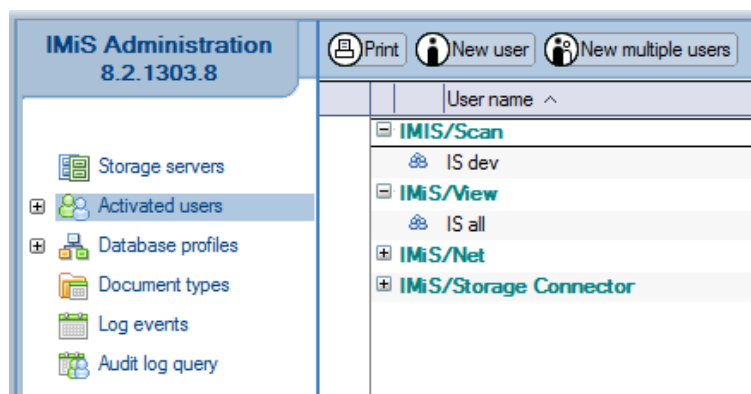
If a user is not listed as the user of a particular IMiS® module, or is not part of a group of users of a particular IMiS® module, or if a server is not listed as active for the purposes of particular IMiS® functionalities, they are not authorized to use them.

If a user is specifically named in connection to a particular IMiS® module (e.g. IMiS®/View), his potential membership in a group (e.g. IS all) will not be taken into account, even when he is the member of a group that is authorized to use an IMiS® module with a broader set of functionalities (e.g. IMiS®/Scan).



If a user is listed in several groups at once (e.g. »IS all« and »IS dev«) he is authorized to use the IMiS® module with the broadest set of functionalities between the groups (in this case »IS all«).

Example: The user is a member of the following groups: »IS all« and »IS dev«. Members of the group »IS all« are authorized to use the functionalities of the module IMiS®/View, while members of the group »IS dev« are authorized to use a broader set of functionalities provided by the module IMiS®/Scan. Such a user may use the module IMiS®/Scan as well.




4.1 Overview of the user environment

The **User Environment** subsection allows you to monitor information of IMiS® module users, which includes:

- Name of user or computer
- Version of the IBM Notes client or IBM Domino server
- Platform and version
- Name of IMiS® module
- Version of IMiS® module
- Date of last login/use of IMiS® module.

Data in the above fields can have multiple values (multivalue). When one of the first five types of the above data is modified, an updated line appears, as shown in the following image:

USER ENVIRONMENT Jure Puhek/IMiS



Basic information

Last seen online:	22.08.2014 07:57:43	
-------------------	---------------------	--

Computer name	Lotus Notes/Domino version	Platform version	IMiS client type	IMiS client version	Created
JURE	Release 8.5.2, August 10, 2010, Build 379	Windows/7 6.1 Intel Pentium	IMiS/Scan++	8.6.1211.397	29.03.2013 14:32
JURE	Release 8.5.2, August 10, 2010, Build 379	Windows/7 6.1 Intel Pentium	IMiS/Scan++	8.6.1306.406	19.07.2013 13:25
JURE	Release 7.0.4, March 23, 2009, Build 267	Windows/NT 6.1 Intel Pentium	IMiS/Scan++	8.6.1306.406	13.09.2013 13:23

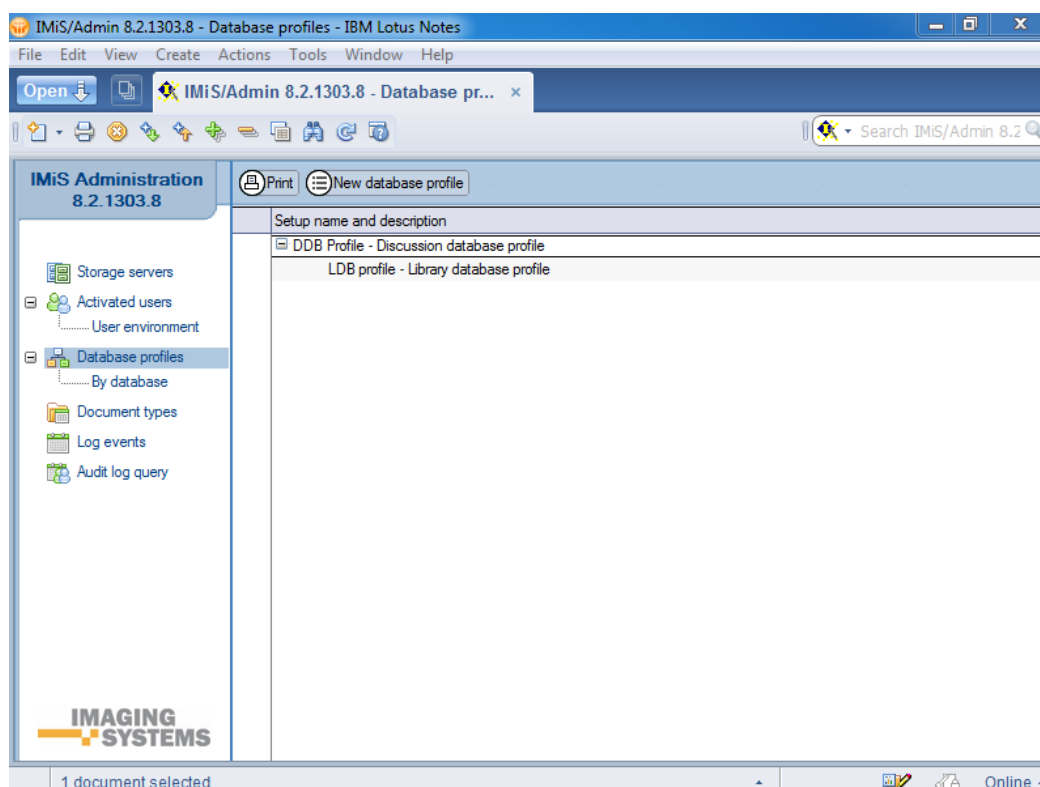
5 DATABASE PROFILE

The **Database profile** section lets you create profile documents and associate Notes databases with them.

This makes administering Notes databases easier. Administration commands apply to the settings of the modules IMiS®/ARChive Server and IMiS®/OCR Server, audit trails, document security and object security for each individual Notes database.

IBM Domino/Notes applications typically use several Notes databases. In the IMiS®/Design version 7.x certain settings were being repeated in configurations with more than one Notes database, and administrators had to be careful to execute all the changes correctly. Since it was difficult to know which Notes databases contain IMiS® Design elements, the Setup agent had to be started up for each individual Notes database to avoid any mistakes.

To enable easier Notes database management and provide a centralized overview of IMiS® enabled Notes databases, the new IMiS®/Admin allows you to set up a single Database profile and associate several Notes databases with it.



5.1 References to Notes databases in the Database profile

The »Databases using this profile« header sets the Notes databases individual Database profiles are associated with.

Databases using this profile		
<input type="button" value="Add"/> <input type="button" value="Remove"/>		
Database server	Database file path	Database title
IMiSDev/IMiS	dev\marko\discussion.nsf	Discussion

[Add] Select the appropriate databases from a directory of Notes databases and assign them to this Database profile.

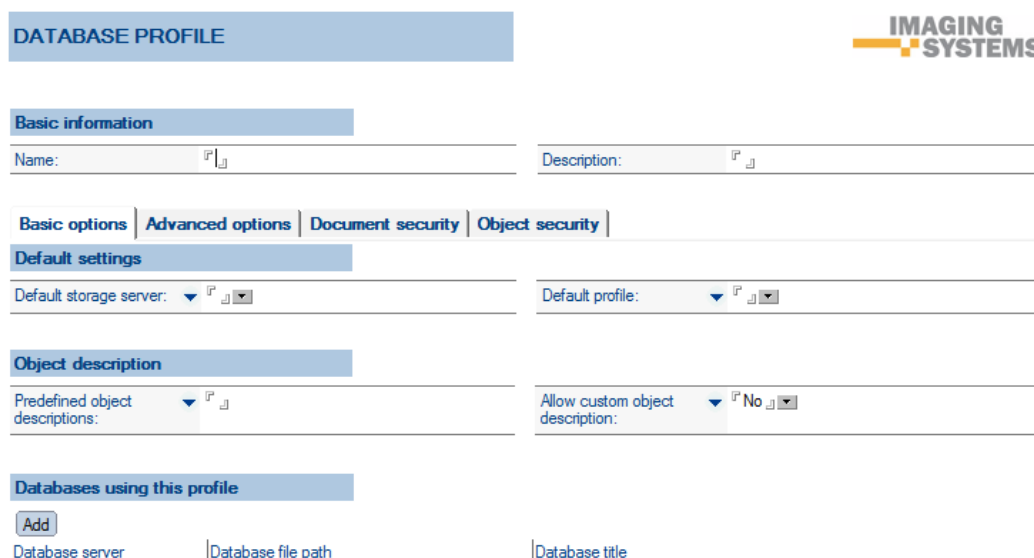
[Remove] Remove one or more Notes databases from the list of this Database profile.

5.2 Migration of Notes databases between Database profiles

A specific Notes database may only be assigned to one Database profile. To transfer databases between profiles, use the **Add** button. From the selection of available Notes databases, choose the one you wish to transfer to another Database profile. When you do so, you will receive the warning »Database is already using database profile« to let you know it was removed from another profile.

5.3 New Database Profile document

Specify the settings for each Database profile. When creating a new Database profile, first select the type of profile (**Main** or **Child**). The central view will then display appropriate information.



DATABASE PROFILE

Basic information

Name: Description:

Basic options | **Advanced options** | **Document security** | **Object security**

Default settings

Default storage server: Default profile:

Object description

Predefined object descriptions: Allow custom object description:

Databases using this profile

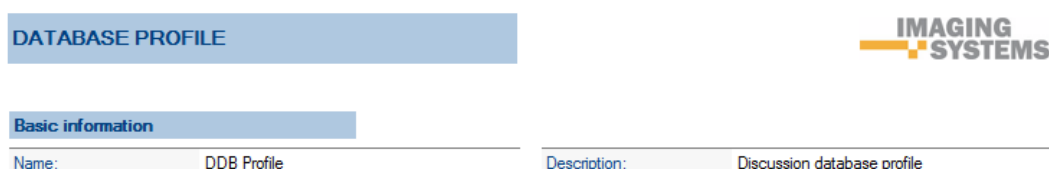
Add

Database server	Database file path	Database title
-----------------	--------------------	----------------

5.4 Description of settings

5.4.1 Basic information

The »Basic information« header lets you input names and descriptions of Database profiles.



DATABASE PROFILE

Basic information

Name: DDB Profile Description: Discussion database profile

[Name] State the name of the Database profile. This is a mandatory field.

[Description] Write a short description of the Database profile or its purpose. This field isn't mandatory, but it's recommended for easier profile management.

Once this is done, you can continue to the additional settings in the tabs »Basic options«, »Advanced options«, »Document security« and »Object security«.

5.4.2 Basic options

5.4.2.1 Default settings

The »Default settings« header lets you set default values for the [Default Storage server](#) and the [Default profile](#). All created objects are saved to the default storage server and the default profile.

Basic options	Advanced options	Document security	Object security
Default settings			
Default storage server: ▼ <input type="text" value="ARCDEV"/>		Default profile: ▼ <input type="text" value="Documents"/>	

[\[Default storage server\]](#) Choose a server from the selection of available storage servers and make it the default server.

[\[Default profile\]](#) Choose a profile from the selection of available profiles and make it the default profile. To best organize things when administering bigger locations, separate the profiles according to the expected inflow of objects.

5.4.2.2 Object description

The »Object description« header lets you set names for document types.

Object description	
Predefined object descriptions: ▼ <input type="text" value="Letter"/> Invitation Quotation form Purchase Order Invoice	Allow custom object description: ▼ <input type="text" value="Yes"/>

[\[Predefined object descriptions\]](#) You can predefine document types that are scanned on a regular basis (inbound mail, outbound mail, invoice, purchase order, ...). This lets you save time and avoid input mistakes.

[\[Allow custom object descriptions\]](#) The default setting is Yes and allows additional changes (custom descriptions) to the type of document even when you already have a predefined document set.

5.4.3 Advanced options

5.4.3.1 Audit trail

The »Audit trail« header enables the audit trail and lets you specify the required reasons for accessing objects.

Basic options		Advanced options		Document security		Object security	
Audit trail							
Enabled:	▼	Yes	▼	Allow unspecified reason:	▼	Yes	
Reasons:	▼	1st level approval		Allow custom reason:	▼	Yes	
		2nd level approval		Prompt in case of single reason:	▼	Yes	
		Management approval		Use effective user name:	▼	No	

[Enabled] The default setting Yes enables the recording of an audit trail for actions performed over IMiS® objects. Additional settings then appear, which are presented below.

[Reasons] Enter the required reasons for performing actions in IBM Domino/Notes applications.

[Allow unspecified reason] The default setting Yes allows users of Notes databases to perform chosen actions in the IBM Domino/Notes application without stating a reason.

[Allow custom reason] The default setting Yes allows users of Notes databases to enter their own reasons in order to perform chosen actions in the IBM Domino/Notes application.

[Prompt in case of single reason] The default setting Yes prompts users of Notes databases to confirm their reason for performing an action in the IBM Domino/Notes application even when a single reason is stated.

[Use effective user name] The setting Yes is used for web applications. Since the code runs on the server, it can run in the name of the person who signed the code or in the name of the user who executed either the agent or some web service method. By selecting Yes the audit trail will record the name of the user who actually executed the specific functionality within the framework of the web application. The default setting is No.

5.4.3.2 IMiS®/OCR Server settings

The »IMiS®/OCR server settings« header manages the settings of the IMiS®/OCR Server module.

IMiS/OCR server settings	
Enabled:	<input checked="" type="checkbox"/> Yes
Type:	<input checked="" type="checkbox"/> Mail-in
Address:	<input checked="" type="checkbox"/> OCR Server/IMiS
Engine version:	<input checked="" type="checkbox"/> Finereader Engine 9
Use IMiS administration database:	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Full text indexing enabled:	<input checked="" type="checkbox"/> Yes
Send disposition:	<input checked="" type="checkbox"/> As objects
Default language:	<input checked="" type="checkbox"/> Slovenian
Default output format:	<input checked="" type="checkbox"/> DOCX

[Enabled] The default setting Yes enables the administration of the IMiS®/OCR Server module and associated Notes databases. Additional options then appear, which are described below.

[Type] Select the Mail-in type. Scanned documents are sent by email to the IMiS®/OCR Server for recognition. The IMiS®/OCR Server then replies with email containing recognized text in the format selected in the »Default output format« field. In the future, we are looking into the possibility of supporting web service functionalities within the framework of the IMiS®/OCR Server.

[Address] State the address of the IMiS®/OCR Server.

[Engine version] Choose the appropriate Finereader Engine version, from a choice ranging between 4 and 10. The Finereader Engine version dictates the range of functionalities of the IMiS®/OCR Server.

[Use IMiS administration database] In case you wish, due to architectural or other reasons, for the IMiS®/OCR Server to use another administration Notes database, its location can be stated in this field. The default setting is empty, which means the IMiS®/OCR Server is using the current administration Notes database.

[Full text indexing enabled] The default setting No disables the text indexing of the scanned document. By choosing Yes you enable the IMiS®/OCR Server to convert text recognized by optical character recognition into the format that is chosen in the Default output format field. A text representation is entered into the Notes document, thus enabling the FTS framework to build a full text index.

[Send disposition] When sending a document (object) into recognition to the IMiS®/OCR Server via email, you must refer to an IMiS® object. Choose between the options As attachment and As objects. The first option detaches the IMiS® object and attaches it to the email.

The second option asks you to describe the object by stating where (in which Notes database and which document) the object is found, and the index of the object (object ID). For optimal performance you are advised to select the option **As object** so you don't need to make attachments.

[Default language] Choose your preference from the selection of available languages.

This language becomes the default language of optical character recognition (OCR) for the text.

[Default output format] Choose your preferred output format from the available selection.

This format becomes the default output format of recognized text.

5.4.3.3 Storage server specific settings

The »Storage server specific settings« header configures parameters applying to the selected storage server. These are specific settings that vary according to the type of selected server.

As a result, the set of parameters changes according to the parameters of the storage server.



The screenshot shows a web interface for 'Storage server specific settings'. At the top is a blue header bar with the text 'Storage server specific settings'. Below it is a white box with a blue border containing the text 'IMiS/ARChive'. Underneath is a label 'Object ID format:' followed by a dropdown menu. The dropdown menu is open, showing the selected option 'Long - Base 16 (64 characters)' and a small arrow icon to the right.

[Object ID format] This parameter sets the size and format of the object identifier generated when new objects are archived through the Notes interface. Choose the value that best suits the connected applications.

***Example:** If you connect IBM Domino/Notes applications to a SAP R/3 environment and wish to maintain the availability of objects created in IBM Domino/Notes applications in SAP R/3 as well, you must set the format to Short – Base 85 due to limitations of the ArchiveLink data table of the subsystem. Namely, this table is only able to store object IDs up to 30 characters in length. The default setting is Long – Base 16 (64 characters). The other choices are Long – Base 40 and 43 character format, and Short – Base 30, 32 and 48 character format.*

5.4.4 Document security

5.4.4.1 Actions

The »Actions« header lets you configure the settings of actions performed over IMiS® objects.

Basic options	Advanced options	Document security	Object security
Actions			
Scan:	<input type="checkbox"/> Yes <input type="checkbox"/> No	View:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Edit:	<input type="checkbox"/> Yes <input type="checkbox"/> No	IMiS Menu:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Copy:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Paste:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Delete:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Duplicate:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Change description:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Import attachment(s):	<input type="checkbox"/> Yes <input type="checkbox"/> No
Import file(s):	<input type="checkbox"/> Yes <input type="checkbox"/> No	Attach:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Export:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Rich Text item name:	<input type="checkbox"/> Body
Send:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Send for OCR:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Audit log:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Send for PDF:	<input type="checkbox"/> Yes <input type="checkbox"/> No

[Scan] The default setting Yes enables the scanning of documents in the IBM Domino/Notes application. The user must be listed as an authorized user of the IMiS®/Scan functionality in the [Activated users](#) section.

[View] The default setting Yes allows the viewing of IMiS® objects.

[Edit] The default setting Yes allows the editing of IMiS® objects.

[IMiS Menu] The default setting Yes enables the display of the IMiS® menu.

[Copy] The default setting Yes enables the copying of IMiS® objects to several Notes documents. When this is done, two or more documents refer to the same Object ID.

[Paste] The default setting Yes enables the pasting of IMiS® objects.

[Delete] The default setting Yes enables the deletion of a reference to the IMiS® object.

In this case, the object is not physically deleted, since several Notes documents may be bound to the same IMiS® object.

[Duplicate] The default setting Yes enables the duplication of an IMiS® object.

When this is done, a new copy of the object is created with a different Object ID.

[Change description] The default setting Yes enables changes to the description of an IMiS® object.

[Import file(s)] The default setting Yes enables the import of files on the basis of which IMiS® objects are created.

[Export] The default setting Yes enables the export of IMiS® objects into a file.

In case there are several IMiS® objects associated with the Notes document, the »Export all« option is available to export them all together, under the same conditions as [Export](#).

[\[Import attachment\(s\)\]](#) The default setting [Yes](#) enables the creation of IMiS® objects from imported attachments located in the Rich text field of the Notes document. If you wish to import all the files together, choose the »Import all« option which has the same conditions as [Import](#).

[\[Attach\]](#) The default setting [Yes](#) allows you to create a file from an IMiS® object and attach it to a Rich Text field. The [Rich Text item name](#) option is there so you can choose which Rich text field you are attaching it to.

[\[Rich Text item name\]](#) State the name of the Rich Text field where you wish to attach the file you received from the IMiS® object by using the [Attach](#) command.

[\[Send\]](#) The default setting [Yes](#) enables the sending of IMiS® objects.

[\[Send for OCR\]](#) The default setting [Yes](#) enables the sending of IMiS® objects for the purposes of optical character recognition (OCR). This option is only available when the [Enabled](#) field is set to [Yes](#) under the header of »IMiS®/OCR server settings« in the tab »Advanced options«.

[\[Send for PDF\]](#) The default setting [Yes](#) enables the sending of IMiS® objects with the purpose of creating a PDF document. This option is only available when the [Enabled](#) field is set to [Yes](#) under the header of »IMiS®/OCR server settings« in the tab »Advanced options«.

[\[Audit log\]](#) The default setting [Yes](#) enables the creation of an audit trail for the selected object.

5.4.4.2 Options

The »Options« header manages the settings of option selection displays.

Options	
Hide disabled actions: <input type="button" value="v"/> <input type="button" value="No"/>	Hide selection for single option: <input type="button" value="v"/> <input type="button" value="No"/>

[\[Hide disabled actions\]](#) The default setting [No](#) keeps menu options that are currently unused visible (they are grayed out).

[\[Hide selection for single option\]](#) When there is only one IMiS® object on the Notes document, the setting [Yes](#) makes the application automatically open and show the object instead of offering you the selection. The default setting is [No](#).

5.4.5 Object security

The »Object security« header lets you manage the rights of users with regard to documents, document pages and annotations. When a document is opened, the settings are forwarded to the IMiS® client through the IBM Domino/Notes application. A precondition for changing settings under the headers »Document pages permissions« and »Annotations permissions« is to set [Edit document](#) to Yes under the header »Document permissions«.

5.4.5.1 Document permissions

The »Document permissions« header lets you set actions allowed over documents opened in the IMiS® client.

Basic options	Advanced options	Document security	Object security
Document permissions			
Edit document:	<input type="button" value="v"/> Yes <input type="button" value="d"/>	Send document:	<input type="button" value="v"/> Yes <input type="button" value="d"/>
Print document:	<input type="button" value="v"/> Yes <input type="button" value="d"/>	OCR document:	<input type="button" value="v"/> Yes <input type="button" value="d"/>

[\[Edit document\]](#) The default setting Yes allows the editing of documents opened in the IMiS® client.

[\[Print document\]](#) The default setting Yes allows the printing of documents opened in the IMiS® client.

[\[Send document\]](#) The default setting Yes allows the sending of documents opened in the IMiS® client.

[\[OCR document\]](#) The default setting Yes allows the optical character recognition of documents opened in the IMiS® client.

5.4.5.2 Document pages permissions

The »Document pages permissions« header lets you set actions allowed over document pages opened in the IMiS® client.

Document pages permissions	
Create new pages:	<input type="button" value="v"/> Yes <input type="button" value="d"/>
Delete pages:	<input type="button" value="v"/> Yes <input type="button" value="d"/>
Move pages:	<input type="button" value="v"/> Yes <input type="button" value="d"/>
Copy image to clipboard:	<input type="button" value="v"/> Yes <input type="button" value="d"/>

[\[Create new pages\]](#) The default setting Yes allows the creation of new pages (scanning, pasting) in documents opened in the IMiS® client.

[\[Delete pages\]](#) The default setting Yes allows the deletion of pages in documents opened in the IMiS® client.

[\[Move pages\]](#) The default setting Yes allows the moving of pages in documents opened in the IMiS® client.

[\[Copy image to clipboard\]](#) The default setting Yes allows the copying of selected pages or images in documents opened in the IMiS® client to the clipboard.

5.4.5.3 Annotations permissions

The »Annotations permissions« header lets you set permissions for reviewing and changing document annotations on documents opened in the IMiS® client.

To change these settings, you must have editing privileges for annotations. A precondition for pasting annotations from the clipboard is to set the [Create new pages](#) field to Yes under the header »Document pages permissions«.

Annotations permissions	
Edit text annotations:	<input type="checkbox"/> Yes ▾
Edit popup annotations:	<input type="checkbox"/> Yes ▾
Edit highlight annotations:	<input type="checkbox"/> Yes ▾
Edit bitmap annotations:	<input type="checkbox"/> Yes ▾
Edit under document redactions:	<input type="checkbox"/> Yes ▾
View text annotations:	<input type="checkbox"/> Yes ▾
View popup annotations:	<input type="checkbox"/> Yes ▾
View highlight annotations:	<input type="checkbox"/> Yes ▾
View bitmap annotations:	<input type="checkbox"/> Yes ▾
View document redactions:	<input type="checkbox"/> Yes ▾

[\[Edit text annotations\]](#) The default setting Yes allows the editing and changing of text annotations to documents open in the IMiS® client.

[\[Edit popup annotations\]](#) The default setting Yes allows the viewing and editing of comments to documents open in the IMiS® client.

[\[Edit highlight annotations\]](#) The default setting Yes allows the viewing and editing of highlight annotations to documents opened in the IMiS® client.

[\[Edit bitmap annotations\]](#) The default setting Yes allows the viewing and editing of image (bitmap) annotations to documents opened in the IMiS® client.

[\[Edit document redactions\]](#) The default setting Yes allows the viewing and editing of document redactions to documents open in the IMiS® client.

[\[View text annotations\]](#) The default setting Yes allows the viewing of text annotations to documents opened in the IMiS® client.


[\[View popup annotations\]](#) The default setting Yes allows the viewing of popup annotations to documents opened in the IMiS® client.

[\[View highlight annotations\]](#) The default setting Yes allows the viewing of highlight annotations to documents opened in the IMiS® client.

[\[View bitmap annotations\]](#) The default setting Yes allows the viewing of image (bitmap) annotations to documents opened in the IMiS® client.

[\[View document redactions\]](#) The default setting Yes allows the viewing of document redactions to documents opened in the IMiS® client.

5.5 Additional settings

For fields with the  icon, you can choose one of the following options:

- Inherit from parent
- Enter or choose value(s)
- Enter @formula.

The option **Inherit from parent** is only available when you've chosen the relation **Child** when creating a new Database profile. It's suitable when you wish to transfer most of the settings from the parent profile and change just a few on your own. When the **Inherit from parent** option is on, any changes to the settings of parent profiles will automatically be applied to all the corresponding child documents. An alternative to the creation of corresponding documents and the **Inherit from parent** option is the use of the @formula described below.

The option @formula (**Enter @formula**) lets you enter a Notes @formula, evaluated within the context of the document over which an IMiS® action is being performed. Normally you want to use the @formula when you wish to select specific cases where the action is available to the user. Consequently, the result of the @formula must be a Boolean value (true / false). @Formula can also be used when you wish to program the available set of IMiS® object descriptions. In that case, the result of the @formula must be a string array.

Examples of @formulas:

Form = »invoice«

The action is available for documents that represent an invoice.

@IsMember ("[Administrator]"; @UserRoles)

The action is available to authorized users, in this case those with the role of [Administrator].

@If (Form = "invoice"; "invoice"; "credit note"; "invoice copy"; "correspondence"; "invitation"; "contract")

In the case of an invoice, the selection of possible descriptions is »invoice«, »credit note« and »invoice copy«, while other cases include »correspondence«, »invitation« and »contract«.

Additionally, the @formula allows the use of reserved keywords \$IMiSActionType, \$IMiSClientType and \$IMiSSourceType, where the selection of values is the following:

\$IMiSSourceType:
"1" - IMiS/Scan++
"2" - IMIS/Scan
"3" - IMiS/View++
"4" - IMiS/View
"5" - IMiS/Net
"6" - IMiS/Storage Connector



\$IMiSActionType:
"1" - Scan
"2" - View
"3" - Edit
"4" - Menu
"5" - Copy
"6" - Paste
"7" - Remove
"8" - Duplicate
"9" - Import file
"10" - Import attachment
"11" - Export
"12" - Attach
"13" - Send
"14" - Send for OCR
"15" - Audit log

\$IMiSClientType:
"1" - Document
"2" - View

5.6 Overview of Notes databases

In the subsection **By database** you can browse all the IMiS® enabled Notes databases.

When you're dealing with many databases, the overview makes for easier management and administration.

 			
Server name ^	Database file path ^	Database title ^	Setup name ^
IMiSDev/IMiS	dev\marko\discussion.nsf	Discussion	DDB Profile
IMiSDev/IMiS	dev\marko\library.nsf	Library	DDB Profile

[Server name] Name of the server where the Notes database is stored.

[Database file path] Path and name of the Notes database.

[Database title] Title of the Notes database.

[Setup name] Name of the profile the Notes database is associated with.

[Validate] This command lets you validate a Notes database. Following the validation procedure, a popup window with the following message appears: »Databases using database profiles are validated. Please look at log events for more information«. Furthermore, a log document is created, recording any changes.

6 DOCUMENT TYPES

The section **Database types** manages the types of documents stored on the IMiS®/ARChive Server. The server will only store those documents that have been previously listed in the document type table.

6.1 Overview of existing document types

Specify the types of documents that can be stored on each individual IMiS®/ARChive Server. The most important document types are already listed.

Print New document type		
Extension	MIME type ^	Description ^
7Z	application/x-7z-compressed	7-Zip compressed file
ACE	application/x-ace-compressed	ACE compressed file
ARJ	application/x-arj-compressed	ARJ compressed file
AVI	video/avi	Video AVI file
BMP	image/bmp	Bitmap picture
DOC	application/msword	Microsoft Word document
DOCM	application/vnd.ms-word.document.macroEnabled.12	Microsoft Word 2007 (macros)
DOCX	application/vnd.openxmlformats-officedocument.docx	Microsoft Word 2007
	application/vnd.openxmlformats-officedocument.wordprocessingml.document	
DOT	application/msword	Microsoft Word template
DOTM	application/vnd.ms-word.template.macroEnabled.12	Microsoft Word 2007 template (macros)
DOTX	application/vnd.openxmlformats-officedocument.dotx	Microsoft Word 2007 template
	application/vnd.openxmlformats-officedocument.wordprocessingml.template	
EML	message/rfc822	RFC822 email message (EML)
GIF	image/gif	GIF file
HTM	text/html	HTML file
JPG	image/jpeg	JPEG image
MDI	image/vnd.ms-modi	Microsoft Imaging
MP3	audio/mp3	Audio MP3
MPEG	video/mpeg	Video MPEG file
MSG	application/vnd.ms-outlook	Microsoft Outlook mail
ODC	application/vnd.oasis.opendocument.chart	ODF Chart document
ODF	application/vnd.oasis.opendocument.formula	ODF Formula document

The following command is available:

[New document type] Specify a new document type.

6.2 New document type

The »New document type« header lets you specify settings for new types of documents.

These are created by entering the **Description**, the file **Extension** and the **MIME type**.

DOCUMENT TYPE		IMAGING SYSTEMS
Basic information		
Description:	JPEG image	
Extension(s):	JPG JPEG	MIME type(s): image/jpeg

[Description] Describe the type of document.

[Extension(s)] State the extension or document type marker. This field can contain multiple values (multivalue).

[MIME type(s)] The MIME type is a text description of the file type. Each type of file has its corresponding MIME type. The structure of the IMiS®/ARChive Server requires the MIME type to be registered when an object is stored on the server. Since the only available info you have is the file extension, you need a translation table between extensions and MIME types which is found in the section **Document types**. This field can contain multiple values (multivalue).

DOCUMENT TYPE

Basic information

Description:	XML document	MIME type(s):	application/xml text/xml
Extension(s):	XML		



7 LOG EVENTS

The section **Log events** contains a log of errors and warnings that occurred while actions were being performed over Notes databases. This helps you establish the circumstances of the error and find the appropriate solution.

Event time	User name ^	Database server ^	Database file path ^	Event information ^
04.12.2013				
04.12.2013 11:22:41	Marko Hren/IMiS	IMiSDev/IMiS	dev\marko\imisadmin.ntf	10257 - Host name must be specified.
04.12.2013 11:33:15	Marko Hren/IMiS	IMiSDev/IMiS	dev\marko\imisadmin.ntf	10261 - At least one profile must be specified.
04.12.2013 11:42:44	Marko Hren/IMiS	IMiSDev/IMiS	dev\marko\imisadmin.ntf	10258 - Port must be specified.
04.12.2013 11:43:13	Marko Hren/IMiS	IMiSDev/IMiS	dev\marko\imisadmin.ntf	10250 - Storage name must be specified.
04.12.2013 14:16:43	Marko Hren/IMiS	IMiSDev/IMiS	dev\marko\imisadmin.ntf	10260 - Number of host names must match number of ports.
04.12.2013 14:17:08	Marko Hren/IMiS	IMiSDev/IMiS	dev\marko\imisadmin.ntf	10260 - Number of host names must match number of ports.
03.12.2013				
03.12.2013 10:20:58	Janez Kogovsek/IMiS	IMiSDev/IMiS	dev\marko\imisadmin.ntf	10263 - Pre-shared key must be specified.
03.12.2013 10:31:53	Janez Kogovsek/IMiS	IMiSDev/IMiS	dev\marko\imisadmin.ntf	10275 - Setup name must be specified.
03.12.2013 10:32:34	Janez Kogovsek/IMiS	IMiSDev/IMiS	dev\marko\discussion.nsf	12295 - IMiS is not activated for current user.
03.12.2013 10:33:28	Janez Kogovsek/IMiS	IMiSDev/IMiS	dev\marko\discussion.nsf	14085 - Error copying object to storage (Client error 61523).
03.12.2013 10:38:18	Janez Kogovsek/IMiS	IMiSDev/IMiS	dev\marko\discussion.nsf	14085 - Error copying object to storage (Client error 61523).
03.12.2013 10:56:21	Janez Kogovsek/IMiS	IMiSDev/IMiS	dev\marko\imisadmin.ntf	10279 - Field 'Agent URL' must be specified.
03.12.2013 11:37:58	Janez Kogovsek/IMiS	IMiSDev/IMiS	dev\marko\imisadmin.ntf	12034 - Error executing query (61523).

[Event time] States the time of the event.

[User name] States the name of the user.

[Database server] States the name of the server storing the Notes database.

[Database file path] States the path and name of the Notes database.

[Event information] States event information (error number and event description).

By clicking an individual event, a window appears containing the »Basic information«, »User information«, »Event information« and »Context information« headers.

7.1 Log event

7.1.1 Basic information

LOG EVENT (Warning)



Basic information

User name:	Janez Kogovsek/IMiS	Event time:	03.12.2013 10:20:58
Database location:	IMiSDev/IMiS dev\marko\imisadmin.ntf	Database title:	IMiS/Admin 8.2.1303.8

[User name] States the name of the user that accessed a particular Notes database.

[Database location] States the server, path and name of the Notes database.

[Event time] States the time of the event.

[Database title] States the title of the Notes database.

7.1.2 User information

User information

Notes client version:	Release 7.0.2, September 26, 2006, Build 265	Platform version:	Windows/XP 5.1 Intel Pentium
IMiS design version:	8.2.1303.8	IMiS client version:	
Database access level:	Manager	Database roles:	[AuditLogQuery]

[Notes client version] States the version, release date and edition of the IBM Notes client.

[IMiS design version] States the IMiS®/Design version.

[Database access level] States the access level of the user that caused the event. Examples: Manager, Designer, Editor, Author, Reader, Depositor.

[Platform version] States the platform and version of the user's operation system.

[IMiS client version] States the version of the IMiS® client used during the time of the event. In case an event occurs as a result of application code that isn't connected to the use of the IMiS® client, this field can be empty.

[Database roles] States the user roles of the user that caused the event within the framework of the Notes database.


7.1.3 Event information

Event information	
Error number/message:	10263 - Pre-shared key must be specified.
Stack trace:	IMiSLSAdmin.CheckFieldsUser (3634) IMiSLSAdmin.QuerySave (3220)

[\[Error number/message\]](#) States the number and short message of the error.

[\[Stack trace\]](#) The stack of application calls that caused the event to occur. Each call consists of the title of object, type of method, and number of line in the source code.

7.1.4 Context information

Context information	
Message:	cn=imis_n1/o=imis!is/pelikan/pelikan.nsf - NT0001C0E2 Račun (ISARC/b8586...fb0b1)
Document link:	

[\[Message\]](#) States information that helps you identify the document in the context of which the error occurred. Optionally, can also state additional context information if the programmer assessed it will be useful in order to pinpoint the cause of the event.

Example: when an error occurs during an operation executed over an archived object, it is sensible to record its object ID as part of the event. Namely, the source Notes document can store several archived objects, and the administrator cannot know precisely which one caused the event.

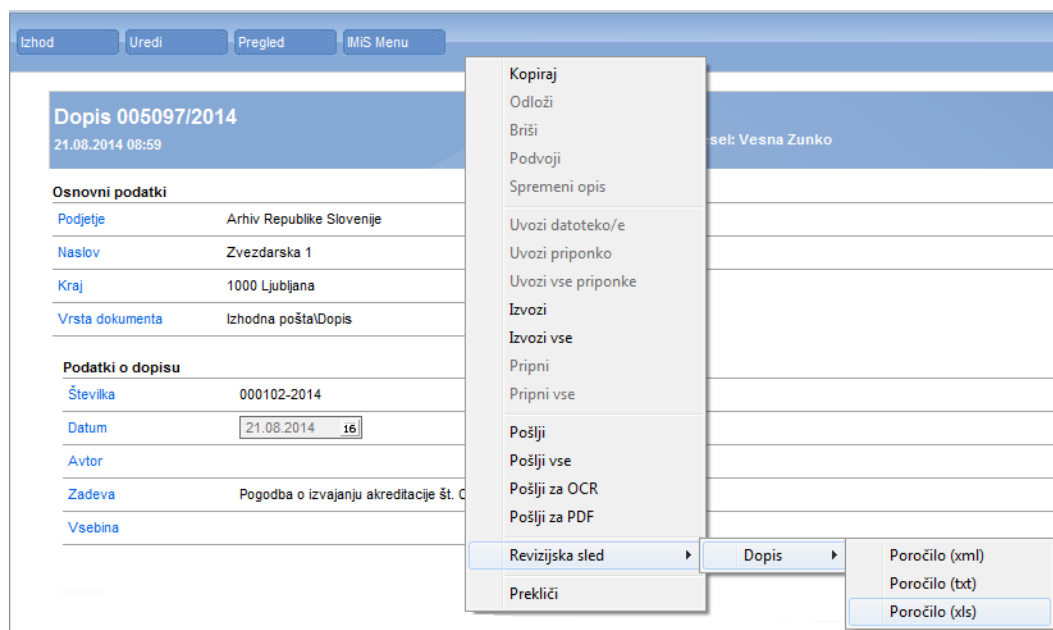
[\[Document link\]](#) Specifies the source document in which the event originated. This is typically a Notes document within the framework of which an error occurred. This data is useful for debugging purposes.

8 AUDIT LOG QUERY

The section [Audit log query](#) supplies you with information explaining events that affected specific objects, based on the selected conditions. In other words, you can query for an audit trail of a specific set of objects. There are two ways to obtain an audit trail.

The first way is querying for a context audit trail, which can be done when you know which document exactly is problematic.

In this case you can obtain an audit trail for IMiS® objects within a given Notes database by selecting the document in question and choosing “Audit log” from the IMiS® menu.



timestamp	user name	IP address	computer name	type	message
21.8.2014 9:01:17	vzunko	192.169.92.84	VESNA	Object create event	Document creation
21.8.2014 9:01:17	vzunko	192.169.92.84	VESNA	Object create event	Values for the following properties have changed: sys:Content, sys:Creator, sys:Description, sys:Opened, sys:Significance, sys:Status, sys:Title
21.8.2014 9:01:17	vzunko	192.169.92.84	VESNA	Object save event	Document creation
21.8.2014 9:01:17	vzunko	192.169.92.84	VESNA	Object open event, type READ-WRITE	Document creation
21.8.2014 9:01:17	vzunko	192.169.92.84	VESNA	Object open event, type READ-WRITE	Property values sys:Content changed.
21.8.2014 9:01:17	vzunko	192.169.92.84	VESNA	Object save event	Document creation
21.8.2014 11:27:49	bzerko	192.169.100.21	BINE	Object open event, type READ-ONLY	Contract review

The second way is to specify the set of documents you are interested in and query for an audit trail of all the corresponding objects located in these Notes documents. In this case, the user must have an **AuditLogQuery** authorization in the IMiS®/Admin database in order to be able to perform the query.

AUDIT LOG QUERY

Database: Document:

View:

IMiS/ARC server: Date range: -

Session parameter scope:

☐ IP address ☒ user name ☐ computer name

ID type:

☒ IMiS/ARC object ID ☐ event ID

User names:

Object IDs:

Report file path or directory:

Report format:

☐ xml ☐ txt ☒ xls

Report sort order:

☐ session - timestamp - ID ☒ timestamp - ID - session
☐ session - ID - timestamp ☐ ID - session - timestamp
☐ timestamp - session - ID ☐ ID - timestamp - session

Display session info:

☒ IP address ☒ user name ☒ computer name

Display event info:

☒ timestamp ☒ ID ☒ type ☒ message

Report options:

☐ Validate result set ☒ Automatically launch

timestamp	user name	IP address	computer name	ID	type
21.8.2014 7:16:13	CN=Roman Ivancic/O=IMiS	192.169.92.63	ROMAN	b264aa026c43489816734ad873046c1fd8cf3321a19e7f7a2c235f520b394c07	Object create event
21.8.2014 7:16:13	CN=Roman Ivancic/O=IMiS	192.169.92.63	ROMAN	b264aa026c43489816734ad873046c1fd8cf3321a19e7f7a2c235f520b394c07	Object save event
21.8.2014 9:53:54	CN=Mitja Nikolic/O=IMiS	192.169.92.73	MITJA	b264aa0268d274da54a66f5e7ba3732a4d9499f4439770cd4225d4ba01d3e2e5	Object open event, type READ-ONLY
21.8.2014 15:26:41	CN=Mitja Nikolic/O=IMiS	192.169.92.73	MITJA	b264aa0279f5902a6aa1fc3db91f6f649395feca2f1bcdaa4799f72ed79712e9	Object create event
21.8.2014 15:26:41	CN=Mitja Nikolic/O=IMiS	192.169.92.73	MITJA	b264aa0279f5902a6aa1fc3db91f6f649395feca2f1bcdaa4799f72ed79712e9	Object save event
21.8.2014 15:26:52	CN=Mitja Nikolic/O=IMiS	192.169.92.73	MITJA	b264aa0279f5902a6aa1fc3db91f6f649395feca2f1bcdaa4799f72ed79712e9	Object open event, type READ-ONLY
21.8.2014 15:29:13	CN=Mitja Nikolic/O=IMiS	192.169.92.73	MITJA	b264aa027a9978ad11b6a0b4e1036ee4281d72e31cdc19a7856f5bcad53a2779	Object open event, type READ-ONLY

You can obtain information about events concerning a specific IMiS® object by choosing the appropriate Notes [Database](#), the relevant [View](#) and the appropriate document.

The screenshot shows a web interface with two main sections. On the left, under 'Database:', there is a dropdown menu set to 'IMiSDev/IMiS' and a text field containing 'dev\marko\discussion.nsf'. Below this, under 'View:', there is a dropdown menu set to 'By Category'. On the right, under 'Document:', there is a dropdown menu set to 'IMIS_OBJ' and a list box showing a document path: 'ARCDEV/b264aa0291d5dee3fe8b07e0e9f7031613b7d4a431afd500730a5e4833e407a6'. Below the list box, the text 'ARCDEV/' is visible.

[Database] From the list of available Notes databases, choose the database for which you wish to obtain audit log information.

[View] Select the view where the document is found.

[Document] From the list of available documents, choose the document for which you wish to obtain audit log information. The window below the document selection field shows you the values of individual document attributes.

The second way to access information about events affecting a specific IMiS® object is by entering the User name.

The screenshot shows a web interface with several sections. At the top left, 'IMiS/ARC server:' has a dropdown menu set to 'ARCDEV'. To its right, 'Date range:' has two date pickers set to '01.12.2013' and '15.12.2013'. Below 'IMiS/ARC server:', there are two sections: 'Session parameter scope:' with radio buttons for 'IP address' (selected), 'user name', and 'computer name'; and 'IP address scope:' with radio buttons for 'range' and 'individual' (selected). To the right of these, 'ID type:' has radio buttons for 'IMiS/ARC object ID' (selected) and 'event ID'. At the bottom left, 'IP addresses:' has a large empty text area. At the bottom right, 'Object IDs:' has a list box showing several object IDs, including 'to je en lep opis - ARCDEV/b264aa0291d5dee3fe8b07', 'x4.tif - ARCDEV/b264aa029065d62a1478ce8b128c82', 'x3.tif - ARCDEV/b264aa0293bafd80b4c3dd312ceef3d', and 'x2.tif - ARCDEV/b264aa02921ae3e3d18e1052709fb5f'. Below the list box, there is a pagination control showing '111'.

[IMiS/ARC server] Choose the server storing the Notes database you are querying about from the list of available IMiS®/ARChive Servers.

[Session parameter scope] Choose one of the possible parameters of the audit log:

IP address, User name or computer name.

[IP address scope] Select one of the available parameters: individual IP addresses (individual) or their range (range). When choosing individual [IP addresses](#), enter the specific addresses you wish to query for the purposes of creating the audit log. When choosing range you will receive a window where you can enter the range of IP addresses you wish to cover.

[ID type] Select one of the available parameters: IMiS®/ARC object ID or event ID.

When choosing the IMiS®/ARC object ID, the window **Object IDs** lets you select the objects you will query for the purposes of creating the audit log.

When choosing event ID, you receive the window **Event ID scope** with an additional selection of possible parameters: individual or range. When choosing range, the **Event ID range** window lets you input the range of ID numbers, where each number represents a type of event.

The screenshot shows a configuration window with the following elements:

- Date range:** Two date pickers, both set to 16, separated by a minus sign.
- ID type:** Two radio buttons: IMiS/ARC object ID (unselected) and event ID (selected).
- Event ID scope:** Two radio buttons: range (selected) and individual (unselected).
- Event ID range:** Two empty text input boxes separated by a minus sign.

The last window of the view configures settings related to the display of results.

The screenshot shows a configuration window with the following elements:

- Report file path or directory:** A text input field.
- Report format:** Three radio buttons: xml (selected), txt (unselected), and xls (unselected).
- Report sort order:** Six radio buttons arranged in two columns:
 - Left column: session - timestamp - ID (unselected), session - ID - timestamp (unselected), timestamp - session - ID (unselected).
 - Right column: timestamp - ID - session (selected), ID - session - timestamp (unselected), ID - timestamp - session (unselected).
- Display session info:** Three checked checkboxes: IP address, user name, and computer name.
- Display event info:** Three checked checkboxes: timestamp, ID, and message.
- Report options:** Two checkboxes: Validate result set (unchecked) and Automatically launch (checked).

[Report file path or directory] State the path or directory where you wish to save the report file.

[Report sort order] State the sort order of the reports in the audit log. The default setting is timestamp-ID-session. The other options let you sort these three parameters in any other order.

[Report options] Set the options for the creation of the audit log report.

The default setting is Automatically launch which means the report is created automatically.

The other available setting is Validate result set which means the results must be reviewed and confirmed prior to creating the report.

[Report format] Choose one of the available audit log formats: xml, txt or xls. When choosing txt or xls you can specify the type of session or event in the fields [Display session info](#) and [Display event info](#).

[Display session info] Specify which session information will be displayed in the audit log.

You can choose between the following: IP address, user name and computer name.

[Display event info] Specify which event information will be displayed in the audit log.

You can choose between the following: timestamp, ID, event type and message.

9 TROUBLESHOOTING

This section covers the most frequent errors encountered by users and lists all the errors that appear in the event log.

9.1 Most frequent errors

Below are some of the most frequent error numbers and titles encountered by users, along with a short description.

ERR 12289 »Database is not IMiS enabled.«

The selected Notes database is not assigned to a Database profile in the IMiS®/Admin database.

ERR 12295 »IMiS is not activated for current user.«

The user is not listed as an active user of the IMiS®/Admin database.

ERR 12804 »Object description can not contain any of the following characters: < > : " / \ | ? * ; <control character>.«

The object description must not contain any of the listed characters.

ERR 14084 »Error copying object from storage (Client error <error code>).«

The IMiS® object cannot be copied from the IMiS®/ARChive Server. This usually means the IMiS® object ID is wrong, or that the IMiS®/ARChive Server is unresponsive.

ERR 14088 »Scan process has not finished properly (<error code>).«

An error occurred during scanning. Usually, this means the user has somehow interrupted the operation.

ERR 14091 »Invalid object ID.«

The IMiS® API method sometimes does not return a valid object ID. You are advised to restart the IBM Notes client.

ERR 16401 »Action is not supported on installed client.«

The current version of the IMiS® client does not support the particular operation.

Example: the client IMiS®/View cannot perform the operation of scanning. In order to scan documents you have to install the IMiS®/Scan client.

9.2 List of errors in the event log

Below is a list of possible user errors with numbers and titles.

ERR 8192 »Error building empty database.«

ERR 8193 »Replacement parameter must be of type string.«

ERR 8194 »Error retrieving temporary filename.«

ERR 8195 »Error retrieving home server.«

ERR 8196 »Error translating string to platform MultiByte string.«

ERR 8197 »Error building names list.«

ERR 8198 »Error locking names list structure.«

ERR 8199 »Error <error code> opening file.«

ERR 8200 »Error retrieving default import/export/detach directory.«

ERR 8201 »Error retrieving platform information string.«

ERR 8202 »Error <error code> getting file version info size. (Library is missing, No permission to access the library or library has no version info).«

ERR 8203 »Error <error code> reading file version info.«

ERR 8204 »Error <error code> reading translated entry from version info.«

ERR 8205 »Error <error code> reading file version entry.«

ERR 8206 »Win64 specific files don't match required version. Please contact system administrator.«

ERR 8207 »Error installing new version of imisdsgn.dll (library is already loaded).«

ERR 8208 »Error <error code> deleting directory.«

ERR 8209 »Error retrieving machine name.«

ERR 8447 »Unsupported platform.«

ERR 8448 »Error <error code> building popup menu.«

ERR 8449 »Error <error code> creating window.«

ERR 8450 »Error <error code> retrieving the cursor's position.«

ERR 8451 »Error <error code> creating an empty rectangle.«

ERR 10240 »Document can not be edited.«

ERR 10241 »User name must be specified.«

ERR 10242 »User name is already defined as activated user.«

ERR 10243 »User type must be specified.«

ERR 10244 »Client type must be specified.«

ERR 10245 »All users were not created successfully.«

ERR 10246 »Extension(s) must be specified.«

ERR 10247 »Document type with this extension is already defined.«

ERR 10248 »MIME type(s) must be specified.«

ERR 10249 »Document type with this MIME type is already defined.«

ERR 10250 »Storage name must be specified.«

ERR 10251 »Storage name can not contain any of the following characters: ; # & ~ @ <control character>.«

ERR 10252 »Storage server with this name is already defined.«

ERR 10253 »Storage description must be specified.«

ERR 10254 »Directory path must be specified.«

ERR 10255 »Counter must be specified.«

ERR 10256 »Counter must be number.«

ERR 10257 »Host name must be specified.«

ERR 10258 »Port must be specified.«

ERR 10259 »Port must be whole number between 1 and 65535.«

ERR 10260 »Number of host names must match number of ports.«

ERR 10261 »At least one profile must be specified.«

ERR 10262 »Authentication type must be specified.«

ERR 10263 »Pre-shared key must be specified.«

ERR 10264 »Error encrypting pre-shared key.«

ERR 10265 »Path to library must be specified.«

ERR 10266 »Server name must be specified.«

ERR 10267 »Admin user name must be specified.«

ERR 10268 »Password must be specified.«

ERR 10269 »Error encrypting password.«

ERR 10270 »API version must be specified.«

ERR 10271 »Agent URL must represent fully qualified URL.«

ERR 10272 »Authentication type must be specified.«

ERR 10273 »User name must be specified.«

ERR 10274 »Password must be specified.«

ERR 10275 »Setup name must be specified.«

ERR 10276 »Database profile with this name is already defined.«

ERR 10277 »Setup description must be specified.«

ERR 10278 »Database profile must be saved.«

ERR 10279 »Field '<field name>' must be specified.«

ERR 10280 »Field '<field name>' must contain @formula.«

ERR 10281 »Field '<field name>' contains invalid @formula... <error message>.«

ERR 10282 »Configuration document doesn't match required version.«

ERR 11776 »IMiS/ARC server must be specified.«

ERR 11777 »Beginning IP address must also be specified.«

ERR 11778 »Beginning IP address is not valid.«

ERR 11779 »Ending IP address must also be specified.«

ERR 11780 »Ending IP address is not valid.«

ERR 11781 »Maximum number of IP addresses is 20.«

ERR 11782 »At least one IP address is not valid.«

ERR 11783 »Maximum number of user names is 20.«

ERR 11784 »Maximum number of computer names is 20.«

ERR 11785 »Year in beginning date must be between 1970 and 2037 (inclusive).«

ERR 11786 »Year in ending date must be between 1970 and 2037 (inclusive).«

ERR 11787 »Beginning date must also be specified.«

ERR 11788 »Ending date must also be specified.«

ERR 11789 »Beginning date can not be greater than ending date.«

ERR 11790 »Beginning time can not be greater than ending time.«

ERR 11791 »Maximum number of object IDs is 20.«

ERR 11792 »At least one object ID does not correspond to selected IMiS/ARC server.«

ERR 11793 »Beginning event ID must also be specified.«

ERR 11794 »Beginning event ID is not valid (long integer).«

ERR 11795 »Ending event ID must also be specified.«

ERR 11796 »Ending event ID is not valid (long integer).«

ERR 11797 »Beginning event ID can not be greater than ending event ID.«

ERR 11798 »Maximum number of event IDs is 20.«

ERR 11799 »At least one event ID is not valid (long integer).«

ERR 11800 »At least one search condition must be specified.«

ERR 11801 »Report file path or directory is not valid.«

ERR 11802 »Maximum length of report file path is 260 characters.«

ERR 11803 »Maximum length of report directory is 240 characters.«

ERR 11804 »Report file is already opened.«

ERR 11805 »Report file already exists and should not be replaced.«

ERR 11806 »At least one display info must be specified.«

ERR 12032 »Invalid user name used for server authentication.«

ERR 12033 »Invalid crypto authentication options used.«

ERR 12034 »Error executing query (<error code>).«

ERR 12035 »Storage server <storage name> is not configured.«

ERR 12036 »Storage server <storage name> is not configured for Audit log queries.«

ERR 12288 »Database does not exist.«

ERR 12289 »Database is not IMiS enabled.«

ERR 12290 »Admin database is not specified.«

ERR 12291 »Admin database can not be opened.«

ERR 12292 »Document is not specified.«

ERR 12293 »Document does not belong to the specified database.«

ERR 12294 »Error retrieving session ID for specified database (<database file path>).«

ERR 12295 »IMiS is not activated for current user.«

ERR 12296 »IMiS client type is not supported.«

ERR 12297 »One or more config documents don't match required version. Please contact
system administrator.«

ERR 12298 »MIME type for extension can not be determined (<extension>).«

ERR 12299 »Extension for MIME type can not be determined (<MIME type>).«

ERR 12300 »Database setup document must be closed (<database profile name>).«

ERR 12545 »Storage does not exist (<storage name>).«

ERR 12546 »Storage type is not supported (<storage type>).«

ERR 12800 »Object open mode is invalid.«

ERR 12801 »Object is closed.«

ERR 12802 »Object is already opened.«

ERR 12803 »Object description is not specified.«

ERR 12804 »Object description can not contain any of the following characters: < > : " / \ | ? * ;
<control character>».«

ERR 12805 »Object description does not belong to the list of predefined object descriptions.«

ERR 12806 »MIME type is not specified.«

ERR 12807 »MIME type is not supported (<MIME type>).«

ERR 12808 »Source object is closed.«

ERR 12809 »Source object open mode is invalid.«

ERR 12810 »Destination object is closed.«

ERR 12811 »Destination object open mode is invalid.«

ERR 13056 »Object ID is not specified.«

ERR 13057 »Object description is not specified.«

ERR 13058 »Object does not exist in database.«

ERR 13059 »Object already exists in database.«

ERR 13060 »Database index is invalid.«

ERR 13061 »Document IMiS metadata structure is invalid.«

ERR 13312 »Parameter does not exist (<parameter name>).«

ERR 13313 »Profile does not exist (<profile name>).«

ERR 13568 »Method is not implemented.«

ERR 13569 »Storage type is not supported (<storage type>).«

ERR 13570 »Storage can not be opened (<error code>: <error message>).«

ERR 13571 »IMiS Storage Connector version does not meet required minimum version
3.1.1202.15.«

ERR 13572 »Invalid crypto mode.«

ERR 13573 »Client parameters are invalid.«

ERR 13574 »Error resolving System Directory variable.«

ERR 13575 »IMiS Imaging Client (Scan/View) is not installed.«

ERR 13576 »Current version of <client type> <client version> doesn't meet the minimum
requirements ERR for accessing archived content. Upgrade to a newer version.«

ERR 13824 »Method is not implemented.«

ERR 13825 »Error setting configuration parameter (<error code>).«

ERR 13826 »Document can not be created (<error code>: <error message>).«

ERR 13827 »Document can not be opened (<error code>: <error message>).«

ERR 13828 »Current version of <client type> <client version> has no support for notifying
Storage Server of reason for activity and its parameters. Upgrade to a newer
version to add this functionality.«

ERR 13829 »IMiS/Net protocol for storage server <storage name> is not enabled.«

ERR 14080 »Method is not implemented.«

ERR 14081 »Object is closed.«

ERR 14082 »Buffer type must represent byte array.«

ERR 14083 »Index is out of bounds.«

ERR 14084 »Error copying object from storage (Client error <error code>).«

ERR 14085 »Error copying object to storage (Client error <error code>).«

ERR 14086 »MIME can not exceed 64 characters.«

ERR 14087 »Stream is already opened.«

ERR 14088 »Scan process has not finished properly (<error code>).«

ERR 14089 »Error retrieving IMiS object (<error code>).«

ERR 14090 »Extension for MIME type can not be determined (<MIME type>).«

ERR 14091 »Invalid object ID.«

ERR 14092 »Error setting configuration parameter (<error code>).«

ERR 14093 »Current version of <client type> <client version> has no support for selecting object ID format. Upgrade to a newer version to add this functionality.«

ERR 15872 »Parameters must be of type string or string array.«

ERR 16128 »Error evaluating setup @formula.«

ERR 16384 »Action aborted.«

ERR 16385 »IMiS Menu is not available.«

ERR 16386 »Helper database does not exist.«

ERR 16387 »OCR type is not supported.«

ERR 16388 »Error executing audit log query. <error message>.«

ERR 16389 »Action can not be performed since you already have this document opened.«

ERR 16390 »Action is not allowed due to security settings.«

ERR 16391 » Object index is out of bounds.«

ERR 16392 »Clipboard is empty.«

ERR 16393 »Audit trail message is invalid.«

ERR 16394 »Action is only supported for users using Notes mail system.«

ERR 16395 »Format index is out of bounds.«

ERR 16396 »Number of object descriptions must match number of file paths.«

ERR 16397 »Number of object descriptions must match number of attachment names.«

ERR 16399 Action type must be of type integer.

ERR 16400 »Action type is not supported (<action type>).«

ERR 16401 »Action is not supported on installed client.«

ERR 16402 »System error when sending databases (MAPI error <error code>).«

ERR 16403 »Invalid parameter type (<recipients type>).«

ERR 16404 »There are no archived objects available.«

ERR 16405 »Helper database doesn't match required version. Please contact system administrator.«

ERR 16640 »Error constructing IMiSLSUIDocument object instance.«

ERR 16896 »A document must be selected.«

ERR 16897 »You cannot update the selected document since you are not listed as an allowable Author for this document.«

ERR 16898 »This operation is disabled for the selected document.«

ERR 16899 »Selected document can not be saved (probably someone else edited and saved the document in the meanwhile).«