OPTIMAL SYSTEMS

enaio®

Software Documentation

enaio® Administration

Version 8.50

optimal-systems.de

Software für Macher.

Copyright 1992 – 2017 by OPTIMAL SYSTEMS GmbH
Cicerostraße 26
D-10709 Berlin

07.04.2017
Version 8.50

Contents

Introduction

About the Manual

This handbook is available as PDF file and as online help.

The PDF file is installed in the documentation directory. Adobe Reader can be used to read the document on-screen, to quickly search for particular terms, or to completely or partially print it.

You can quickly open and look up topics online at your workstation in enaio® administrator using the **F1** key or the Help menu.

The handbook describes enaio® administrator, enaio® enterprise-manager and additional administrative configuration such as logging and encryption as well as installation and configuration of the viewer services and optional components.

About enaio® administrator

With enaio® administrator you can manage the Enterprise Content Management system enaio®. To start using enaio® administrator, you need to have successfully installed enaio®. enaio® administrator can only be started if the database is set up and enaio® server is running.

With enaio® administrator, you can:

§ Set up users and configure various workstations

§ Set up the security system. Distribute access rights to archive objects and administrative applications of enaio®

§ Configure templates and applications for Windows document types

§ control audit-proof archiving. Archiving is an automatic action, which, once configured, can take place at specific times or in cycles

§ Configure the import and export of data. enaio® provides numerous interfaces which can be used, for example, to access, import, and automatically index legacy data or data created in other systems

enaio® administrator is started from the enaio® application group or the `\clients\Admin` directory.

After initial installation, log in with the user name 'root' and the password 'optimal'.

> For security reasons, delete the `root/optimal` user account immediately after having started enaio® administrator for the first time.

enaio® administrator blocks all data spaces which are currently being edited. Other users can view such blocked data spaces but cannot edit it.

enaio® manager-for-log files is used to log all components (see 'Introduction to Logging').

About enaio® enterprise-manager

enaio® enterprise-manager is particularly used to administer enaio® licenses, servers and archiving media for server groups.

On top of that, enaio® enterprise-manager offers significant technical insight into system processes and can therefore be useful for system optimization and problem analysis.

Configuring the Archiving System

Introduction to the Archiving System

The basic configuration of the system is done when installing enaio® via setup. The setup program writes the required data to the registry and to the `as.cfg` configuration file in the `\etc` directory of the data directory.

enaio® administrator allows further configuration only if the enaio® installation has been successful and if the database and enaio® server are running.

Configuration settings of the entire system range from setting up a background image for enaio® client to the integration of libraries, which may, for example, be required for import and export of data.

> Changes to the configuration can have far-reaching consequences. For that reason, only qualified personnel are recommended to perform changes. In case of doubt, please contact the OPTIMAL SYSTEMS support team first.

Entire System Settings

The following tabs allow you to make changes to the entire system:

§ 'Start' tab

§ 'Database' tab

§ 'Additions' tab

§ 'LDAP Configuration' tab

§ 'Documents' tab

§ 'Events' Tab tab

§ 'Web Directory' Tab tab

§ 'Print Labeling' tab

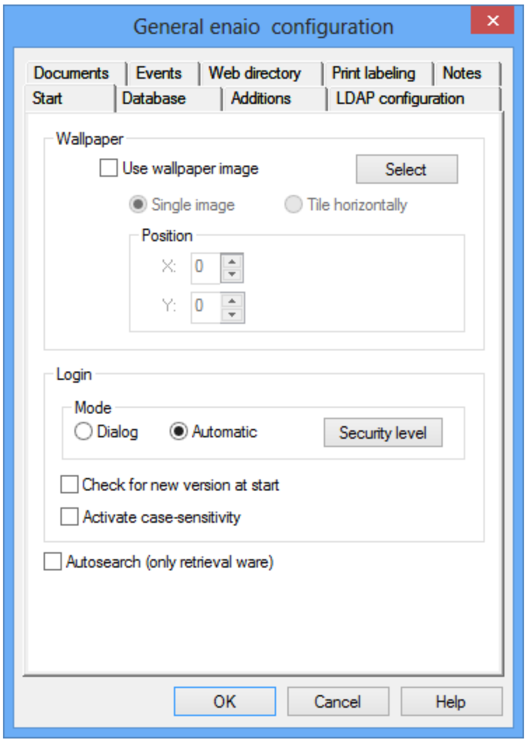
§ 'Notes' tab

You open the tabs with either the Entire system button in the toolbar or via the Entire system entry in the Configuration menu.

The initial settings found in the tabs are either defaults or have been set by the setup program.

'Start' Tab

On the **Start** tab, you can configure the enaio® startup properties, particularly login.



General enaio configuration
Documents | Events | Web directory | Print labeling | Notes
Start | Database | Additions | LDAP configuration
Select
Security level
OK
Cancel
Help

Wallpaper

□ Use wallpaper image

● Single image ○ Tile horizontally

Position

X: 0

Y: 0

Login

Mode

○ Dialog ● Automatic

□ Check for new version at start

□ Activate case-sensitivity

□ Autosearch (only retrieval ware)

You can add a **Wallpaper**. The wallpaper must be a bitmap with a maximum of 24 colors as JPG, TIFF or PNG. The color with the RGB value 255,0,255 is transparent.

The **Select** button will open a file selection dialog to choose the wallpaper. The image file will then be copied to the `\etc` directory of the data directory and, irrespective of the file format, named `background.bmp`.

The two options **Single image** and **Tile horizontally** allow you to customize the view of your wallpaper. In single image mode, you can freely position the image on the workspace. Valid position values range from -10; -10 (top left), and 10; 10 (bottom right).

For user **login** to enaio® client and related applications, choose between the options:

§ **Dialog**

Users enter their enaio® user names and enaio® passwords into a login dialog.

If user passwords are managed with an LDAP directory service (see ''LDAP Configuration' Tab') users enter their LDAP passwords into the login dialog.

§ **Automatic**

Users are automatically logged in with their network login, as long as their network names correspond to enaio® user names. Otherwise, a login dialog will open.

Using the **Security level button**, open the **Configure security level dialog** and select whether the application should be closed after three failed logins, or whether it should be locked.

All enaio® components can check during start whether there is a more recent version available in the `\etc\update` directory of the data directory. If so, the new version is copied to the respective directory and will then start. You can get information on updated versions from Consulting and Support.

You can decide whether passwords are case-sensitive by activating the **Activate case-sensitivity checkbox**.

After receiving an update version, copy it into the respective directory and activate the **Check for new version at start** checkbox. It is recommended to disable the automatic update after its completion, which is performed by starting all components affected by the update once at each workstation.

If you have activated the **Check for new version at start** option, it is possible to specify users in the `as.cfg` file in the `\etc` directory of the data directory for which the automatic update will not be performed.

Add the following entry to the [SYSTEM] section:

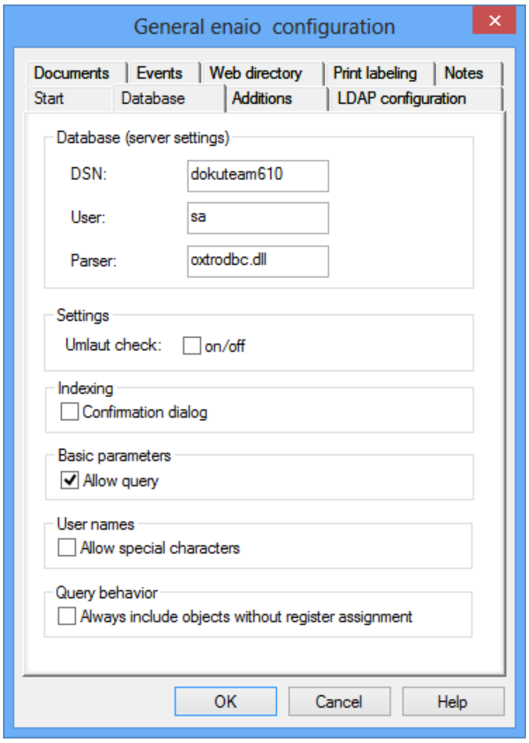
```
NOUPDATEUSER=OSECM user name,OSECM user name
```

When specifying more than one user, separate them by commas.

It is also possible to specify users for whom the automatic update will be performed, even if the **Check for new version at start** option is not activated:

```
UPDATEUSER=OSECM user name,OSECM user name
```

'Database' Tab



Database (server settings)

DSN: dokuteam610

User: sa

Parser: oxtrodbc.dll

Settings

Umlaut check: □ on/off

Indexing

□ Confirmation dialog

Basic parameters

☑ Allow query

User names

□ Allow special characters

Query behavior

□ Always include objects without register assignment

tab

The **Database** tab indicates data source name (DSN), the user account of the database, and the parser. These entries cannot be modified here.

Activate the **Umlaut check** only if the database has been set up with a non-German character set, but enaio® client is using the German character set. The umlaut check will slow down system performance.

The **Confirmation dialog** checkbox activates system-wide confirmation when saving the index data on data sheets. Regular users cannot disable these confirmation dialogs.

Search forms querying **Basic parameters** from the archive area can be hidden if you do not want users to perform this type of query. However, users with the system role 'Administrator: Start' can always query basic parameters.

Instead of disabling searches over basic parameters, you can limit them. In this case, users must leave the fields **Creator**, **Modified**, and **Owner** empty or enter their own names. The **Properties** cannot be limited. This limitation does not apply to users with the system role 'Administrator: Start'.

To do so, add the following line to the [System] section of the `\etc\as.cfg` file of the data directory: `SHOWBASISPARAMETER=2`

User names that contain the special character '@' can cause errors when logging in using the COM interface. For the user account creation in enaio® administrator you can forbid the '@' character usage by deselecting the **Allow special characters** checkbox option.

Do not use the special character '@' or other special characters for the user name as otherwise search queries cannot be carried out correctly.

Define for the **Query behavior** of integrated scripts whether or not to show documents without register assignment – documents that are not contained in any register – in the hit list of a search, which queries register and document data. This setting will not have any effect as long as the query behavior is specified in the script itself.

For searches in enaio® client, users can configure the query behavior in the **Query behavior** section of their personal settings dialog.

Queries in the Index Data History

A query refers to the index data of the current object version. If an index data history for an object type is created with the respective property in enaio® editor, users can query against these data, too.

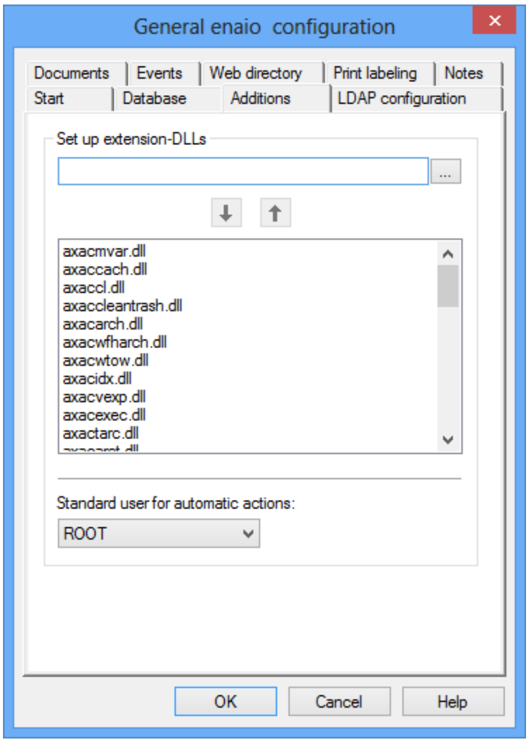
To do so, the Shift key must be pressed while starting the query.

An SQL query can take significantly more time. That is why this feature is deactivated by default.

This feature can be activated with the following entry in the file `\etc\as.cfg` in the data directory:

```
[SYSTEM]

QUERYALLINDEXDATAVERSIONS=1
```

'Additions' Tab



axacmvar.dll
axaccach.dll
axaccl.dll
axaccleantrash.dll
axacarch.dll
axacwfharch.dll
axacwtow.dll
axacidx.dll
axacvexp.dll
axacexec.dll
axactarc.dll

Standard user for automatic actions: ROOT

You use the **Additions** tab to register libraries for automatic actions (see 'Introduction to Automatic Actions') with the system.

The libraries can be found in the …`\clients\admin` directory.

The following libraries are automatically integrated at installation:

axacimp.dll	Data/ document import
axacexp.dll	Data/ document export
axacpdfa.dll	PDF/A validation
axacscript.dll	Run script
axacarch.dll	Archive
axacidx.dll	Full text indexing
axacdirectorysync.dll	Directory synchronization
axacdok2tif.dll	Rendition

Some libraries must be licensed to the workstations via a module assignment (see 'Adding Modules').

Optionally, a **Standard user** can be defined for any automatic action. The information can be evaluated by scripts or external applications which you integrate. A standard user is not evaluated internally.

The user for automatic actions that are started from enaio® administrator is always the logged in user. enaio® start (see 'enaio® start') expects the user name and password when first starting and uses these login details later on.

Users with accounts used for editing documents should close the area with the list of recently edited objects while executing the respective actions in enaio® client. The continuous refreshing of this area would slow the system.

'LDAP Configuration' Tab

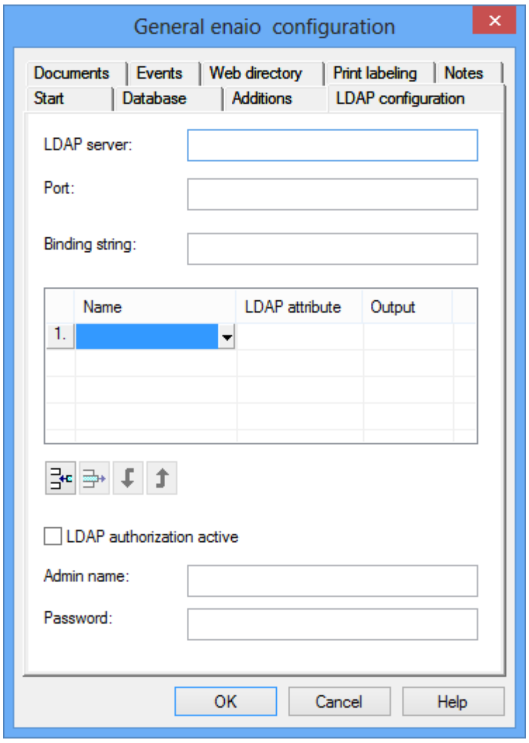
If you use an LDAP directory service, the users can log in with the password administered there – automatically or via a dialog.

It is however necessary to pass the user names to the user administration of the enaio® security system (see 'Setting Up Groups').

Only users who are listed in both the LDAP directory service and the enaio® user administration can log in with LDAP authentication.

You can use the automatic action 'User Import' for the transfer (see 'Import User and Group Data').

Group-specific access rights and system roles can only be specified from within the enaio® security system.



Select the **LDAP Authentication Active** checkbox.

Enter the name of the **LDAP Server** and its **Port**.

Enter the **Binding string**.

You can enter several entries for server, port and binding string, separated by semicolons. Servers will be queried in sequence. Data of the first server that is reached will be used for user administration.

To import users from the directory service into the enaio® user administration, assign the LDAP attribute, which you are using as a unique user indication, to the user indication 'Name'.

Optionally, you can assign the identifiers 'Full name' and 'Comment' to LDAP attributes in order to automatically hand over this data to the enaio® user administration.

Each name to which an LDAP attribute is assigned can be used within the user administration in order to search for those users who are meant to be passed to the security system.

It is possible to set up further assignments when searching for users in the LDAP directory service. However, respective data will not be imported into the user administration.

This is how to create assignments:

1. Click on the first line of the name field.
2. Select an attribute for data handover from the list or enter any other attribute for search purposes.
3. Enter the LDAP attribute in the next column.
4. Select 'yes' or 'no' in the 'Output' column.

   Therewith, you are specifying whether or not to display this attribute in the hit list of an LDAP user search.
5. Add extra lines for additional assignments.

If you select a line by clicking the line number, the following line options will be available:

Insert an empty line below the selected one.

Delete the selected line.

Move the selected line down under the following line.

Move the selected line up above the previous one.

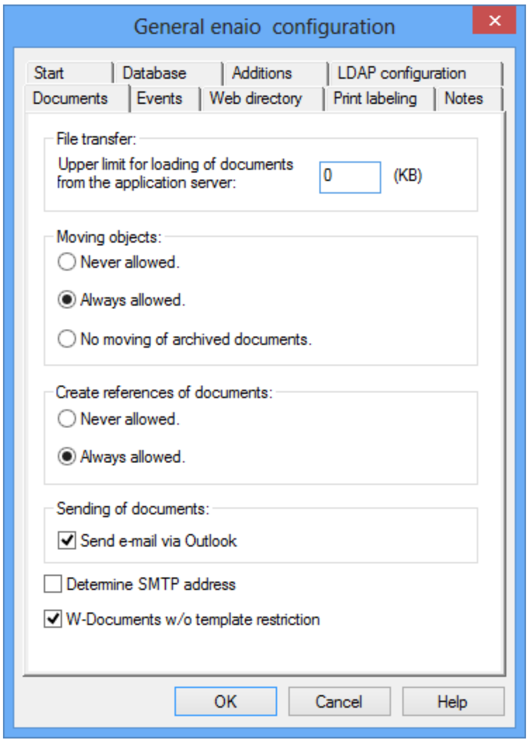
Anonymous access to the LDAP directory service usually is not allowed; as a result, authentication at the LDAP system is required for identification of LDAP users and their rights.

To do so, indicate an LDAP user who has been provided with all required rights. The password will be encrypted before storage.

> If LDAP authentication has been selected, and the LDAP directory service is not available, no user will be able to log in. Therefore, it is recommended that you create at least one user that has the system role 'Supervisor' and an enaio® password. In case the LDAP directory service is not available, this user can start enaio® administrator or enaio® enterprise-manager and change the settings of the user administration. It is still necessary to disable LDAP authorization first. To do this, in the registry file using the key `…\Schemata\4.0\Login`, change the value of

the LoginMode string from '1' to '0.' Then, all users with enaio® passwords will be able to start the applications according to their system roles.

'Documents' Tab



File transfer:

Upper limit for loading of documents from the application server: 0 (KB)

Moving objects:

○ Never allowed.

● Always allowed.

○ No moving of archived documents.

Create references of documents:

○ Never allowed.

● Always allowed.

Sending of documents:

☑ Send e-mail via Outlook

□ Determine SMTP address

☑ W-Documents w/o template restriction

File transfer

In order to reduce network traffic, specify the upper size limit of files to be uploaded in kilobytes. If a user wants to open a file which is larger than the indicated limit, he will be notified and asked for confirmation before the handover is performed.

Set the limit to '0' in order to automatically pass and open all files without further confirmation.

Every user can additionally set an upper file size limit in the personal settings of OS|CLIENT. This personal user setting is always given priority to.

Creating references of documents

It is possible to allow or prohibit the creation of reference documents. This setting applies to the entire system. User may require the system role 'Client: Create reference documents.'

File-related properties of reference documents such as the number of files, the number of pages, and retention times are not updated when there are changes to the document files of the original and must be viewed via the original.

Deleting documents for which reference documents have been created can activate a confirmation dialog notifying the user and this enables the reference documents to be listed.

To enable this function, add the following line to the [System] section of the `\etc\as.cfg file` of the data directory:

```
MUSTCHECKLINKEDDOCUMENTS=1
```

The value '0' turns the function off.

Moving objects

The capability of moving objects can be enabled or disabled; the setting applies to the entire system.

A permission only applies for users who have the system role 'Client: Move objects'.

To perform a move across cabinets, users also require the 'Client: Move across cabinets' system role. Registers and archived documents cannot be moved to a different cabinet, and documents can only be moved one at a time. The index data are transferred from fields with the same internal name.

> Moved documents and reference documents can cause inconsistencies between location, index data, and content, for example, when documents are indexed through add-ons.
> If the move is allowed, documents can also be moved that are checked out by other users or whose index data is edited by other users.

Sending documents

Allows sending documents by e-mail using Microsoft Outlook.

Determining SMTP address

The Exchange server's address book uses the sender names to determine e-mail addresses of internally sent e-mails and also displays and takes over addresses of e-mails in the inbox.

> With very extensive address books, this process may consume a lot of time.

W-Documents without template restriction

Documents can be imported by dragging and dropping. To do so, they must have a document type assigned to them. You can allow users to drag and drop documents with file extensions not recognized by the W-template administration and to specify the W-Document type of the document afterwards. Such documents will be opened by the application, which has been respectively assigned to in the operating system settings. Image documents that are managed with an image module cannot be imported in this way.

> If the file extension is not assigned to any application, the document will not be opened. The user will then receive a notification.

Merging Documents

You can allow the merging of documents throughout the entire system. Two documents are merged in enaio® client by dragging a document onto another with the mouse, while holding the **Ctrl** and **Shift** keys. Both documents must be assigned to the same module. The document which the user has dragged onto another will be moved to the trash can, and the associated file will be assigned to the target document.

> This function is subject to some limitations. For example, annotations on layers may be lost or documents which cannot be displayed correctly may be created as the files of which they are composed are of different formats. You must only enable this option after contacting the consulting department.

To enable this function, add the following line to the [System] section of the `\etc\as.cfg file` of the data directory:

```
DnDMerging=1
```

The value '0' turns the function off.

The function is not documented in the enaio® client handbook. Inform all users if you enable the connection of documents.

Copying Folders and Registers

The **Create copy** function for folders and registers creates a new object, which is indexed with the original object's data. Contents of the original object will not be copied, i.e. that way created objects will be empty.

This function can be turned off:

To do so, add the following line to the `[System]` section of the `\etc\as.cfg` file of the data directory:

```
COPYREGISTER=0
```

The value '1' turns the function back on.

The **Create copy** function for documents is not affected by this setting, nor is the copying of registers and their contents using the mouse and the **Ctrl** key.

Deleting Documents with Variants

If a document with variant administration in enaio® client is deleted from a hit list or a location, the result depends on the status of the document:

§ If the active document is the original, all documents in the variant administration will be deleted.

§ If the active document is a variant, this variant as well as all sub-variants will be deleted and the original becomes the active variant.

Since the variant status of a document in the hit list or location is not shown, the consequence of deleting the document is not immediately recognizable for the user; this functionality can be turned off throughout the entire system. As a result, the document and all documents in the variant administration will always be deleted.

To do so, the following entry in the `\etc\as.cfg` configuration file of the data directory is necessary:

```
[SYSTEM]
```

```
DELETEVARIANTMODE=1
```

The value '0' always reverts to the previous behavior.

The original document cannot be deleted from the variant administration as long as variants exist.

Moves across cabinets

Users can move several documents of the same document type to another cabinet. If there are several document types in this cabinet to which the documents can be assigned, one of these document types can be selected. If there are index data fields with the same internal name, the data is transferred from these fields. Index data of fields that cannot be assigned to other fields with the same internal names are lost and cannot be restored. Mandatory fields und key fields are not verified, events are not executed.

If a user moves a single document to another cabinet, the index data form is opened after the move. If indexing is canceled, the move is not reversed. Canceling can lead to inconsistent data, for example from unpopulated mandatory fields.

You can switch off the function to move several documents simultaneously and opening the index data form when moving a single document.

To do so, you need the following entry in the `\etc\as.cfg` file of the data directory:

```
[CLIENT]

ALLOWONLYONEDOCMOVE=1

OPENDATASHEETIFONEDOCMOVE=0
```

Sharing Documents

Documents can be shared in enaio® client for users who have no or limited access rights. Sharing is limited in time. The access rights granted are specified. The 'Delete object' right and annotations is excluded from sharing.

Sharing functions are switched on throughout the entire system in enaio® enterprise-manager via the 'Sharing active' parameter (cf. 'Security'). A maximum period for sharing is also specified.

Users need corresponding system roles:

- Client: Share documents

  Users can share documents and edit and remove their own sharing.

- Client: Administer sharing

  Users can remove sharing of other users. A condition of this is the access right 'Show index data.'

If a user is editing a shared document, the user can complete their edit even after sharing has expired or been removed.

> A data transfer with enaio® data-transfer is not possible for shared documents.

Quality Setting for Imported Images

If users import JPEG images into enaio® client via the image module from the file system, the images will be checked and transferred in the original.

If imported images are converted, e.g. color JPEG images for the grayscale module into grayscale images, these images are then stored with a default value for compression. You can define the compression value with an entry in the configuration file `\etc\as.cfg` of the data directory.

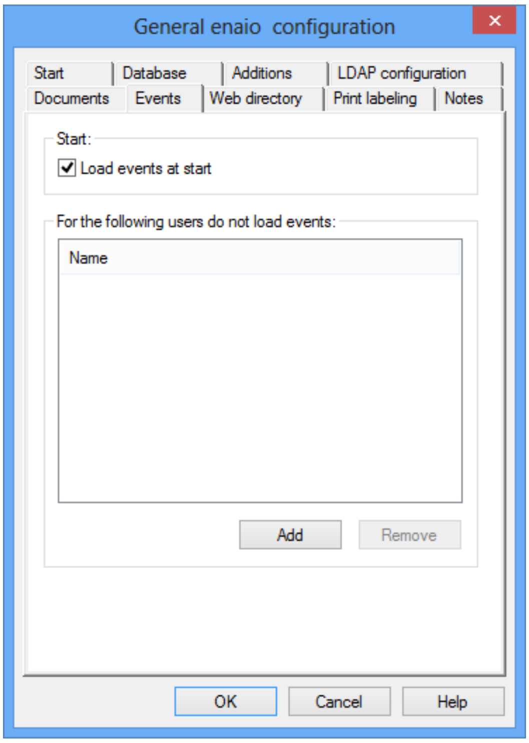
```
[SYSTEM]
```

```
JPEGQUALI=value
```

You enter a value between '2' for maximum quality and '100' for highest compression.

The default value is '20.'

'Events' Tab



☑ Load events at start

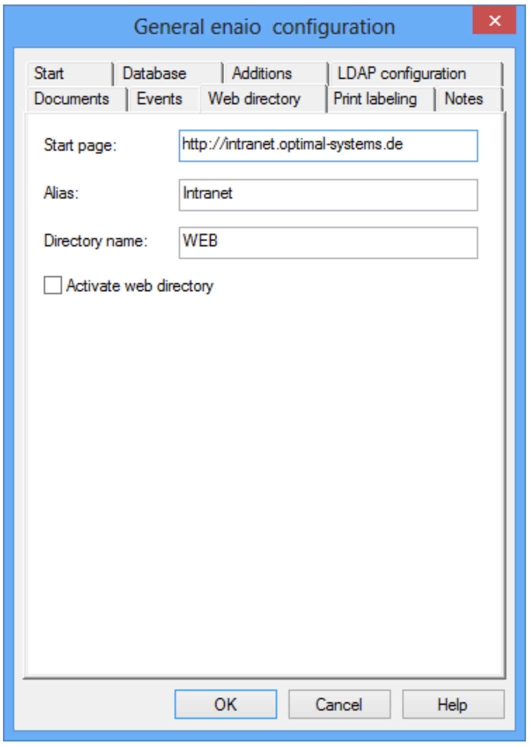
On this tab, you can choose whether to load events at start or not.

If you activate this option, you can additionally set up a list of users for whom events will not be loaded.

If you do not select the option, you can specify a list of users for whom events will still be loaded.

This setting applies only to enaio® client; in enaio® webclient events are always executed for all users.

'Web Directory' Tab



Start page: http://intranet.optimal-systems.de

Alias: Intranet

Directory name: WEB

□ Activate web directory

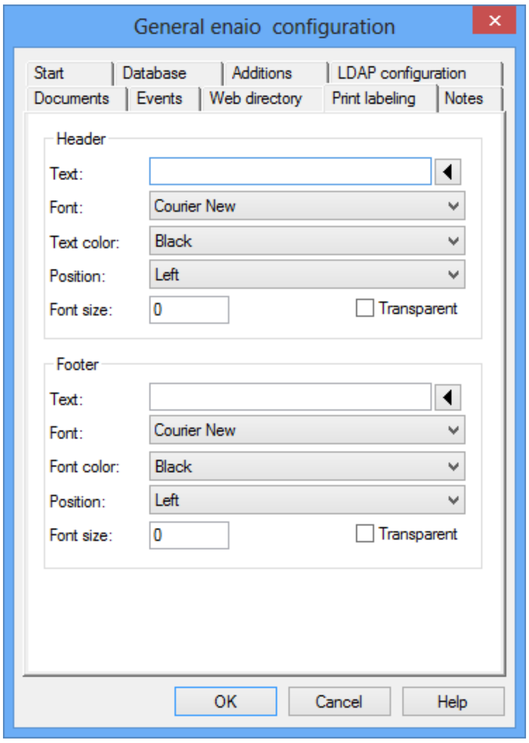
A Web directory can be set up in the users' workspaces. Users can add links to Internet addresses to this directory.

Specify the URL of a **Home screen** on the tab. The home page cannot be changed by users and is labeled with the **Alias** specified here.

Enter a **Directory name** of the Web directory which is used in the workspace of enaio® client.

The checkbox is used to activate or deactivate the Web directory.

'Print Labeling' Tab



Header

Text:

Font: Courier New

Text color: Black

Position: Left

Font size: 0 □ Transparent

Footer

Text:

Font: Courier New

Font color: Black

Position: Left

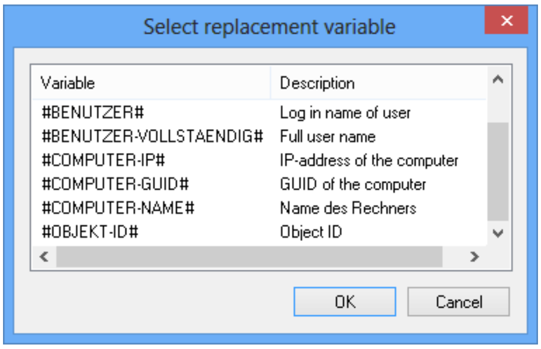
Font size: 0 □ Transparent

Single-line headers and footers can be created when printing image documents and converting image and W-Documents into PDF files. All printouts of image documents will then automatically contain the specified header and footer. They are not shown when the image is viewed on-screen.

Provided that no exceptions were defined, this setting applies to all document types.

If no text is entered, no header or footer will be printed.

The arrow button next to the **Text** field allows you to select variables which can be used in the header and footer.



Variable	Description
#BENUTZER#	Log in name of user
#BENUTZER-VOLLSTAENDIG#	Full user name
#COMPUTER-IP#	IP-address of the computer
#COMPUTER-GUID#	GUID of the computer
#COMPUTER-NAME#	Name des Rechners
#OBJEKT-ID#	Object ID

If environments require more flexibility, scripts allow for precise setup and design of the print labeling. Replacement variables can also be used.

This makes it possible to realize controlled printing scenarios, i.e. print labeling in order to document restrictions regarding the use of documents.

Print labeling is realized with parameters for the 'ConvertDocument' job. These are documented in the server API documentation.

To print documents, users require the system role 'Client: Print documents'.

Defining Exceptions

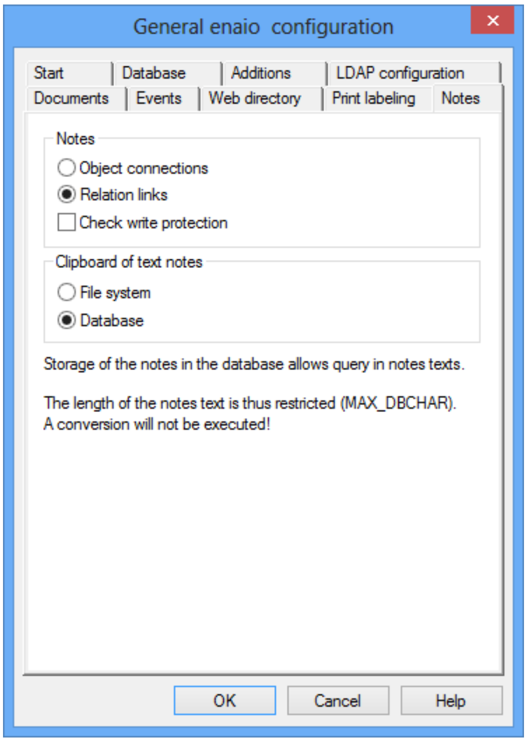
The settings for print labeling apply to all document types as long as you have not defined any exceptions. With an exception you can specify that no print labeling is done for documents of a certain document type if the document has been indexed in an indicated field with a certain value.

For defining exceptions, entries with the following structure must be added to the file `\etc\as.cfg` of the data directory:

```
[PRINTLABELINGEXCLUDE]

Document type ID=Database name,value
```

The ID of the document type and the database name of the fields can be found in enaio® editor; 'value' indicates the value the field has been indexed with.

'Notes' Tab



Notes

○ Object connections

● Relation links

□ Check write protection

Clipboard of text notes

○ File system

● Database

Storage of the notes in the database allows query in notes texts.

The length of the notes text is thus restricted (MAX_DBCHAR).
A conversion will not be executed!

Activate the **Relation link** to no longer link objects by previous notes but by relations, which are defined by users through the relations dialog.

If the **Check write protection** option has been activated, users can only relate two objects provided that they have write access to both objects.

Notes can be administered as text files in the file system, or in the database.

The length of text files is not restricted by enaio® client. The length of notes in the database depends on the maximum length of a database field of the database deployed.

If notes are administered in the database, users can perform searches on the content of these.

Notes can be administered in the database since version 4.10. Existing text files cannot be automatically transferred to the database. They can still be opened. If notes are administered in the database, existing text files that the user modifies and saves will be saved to the database. If a note is longer than the maximum length of a database field, it will be truncated.

System roles are necessary to view or edit notes. The system roles are also required to create or edit links between objects.

License System Configuration

Introduction to the License System

License keys which you have purchased are administered in enaio® enterprise-manager. enaio® enterprise-manager `osecm_entmgr.msc` is a snap-in for the Microsoft Management Console.

The number and type of licenses can be found in the license certificate or the `aslic.dat` file. The file can be examined using enaio® enterprise-manager.

Seat license keys are assigned to particular workstations. Floating license keys must not be assigned to a workstation. To ensure that a module will always be available at a particular workstation, though, they can be assigned as well.

The enaio® server license is only available as a seat license key with a fixed GUID or TCP/IP address. If a server's address changes, you will need a new license file. If you acquire additional licenses, you also receive a new license file with the corresponding license keys.

During the enaio® installation, license files will be passed automatically to the database. New license files are imported into the database using enaio® enterprise-manager. Licenses are only available after they have been imported.

enaio® enterprise-manager allows you to monitor which license keys are assigned to which workstation by enaio® server.

Layer administration is licensed in the 'ADI' module. You must license this module on every workstation on which you want to use it.

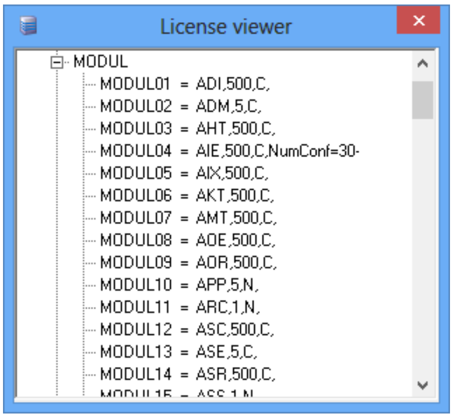
Determining Licenses

The number and the type of licenses can be found in the license certificate or in the file `aslic.dat`. Open this file through the license administration in enaio® enterprise-manager.

The file `aslic.dat` is opened as follows:

1. Start enaio® enterprise-manager.
2. Select the **Administration** > **License settings** entry in the console root.
3. Select **All tasks** > **Show license file** item from the context menu of the **Licenses** entry.

   The `aslic.dat` file will open. It cannot be edited.



```
MODUL
    MODUL01  =  ADI,500,C,
    MODUL02  =  ADM,5,C,
    MODUL03  =  AHT,500,C,
    MODUL04  =  AIE,500,C,NumConf=30-
    MODUL05  =  AIX,500,C,
    MODUL06  =  AKT,500,C,
    MODUL07  =  AMT,500,C,
    MODUL08  =  AOE,500,C,
    MODUL09  =  AOR,500,C,
    MODUL10  =  APP,5,N,
    MODUL11  =  ARC,1,N,
    MODUL12  =  ASC,500,C,
    MODUL13  =  ASE,5,C,
    MODUL14  =  ASR,500,C,
    MODUL15  =  ASS,1,N
```

In the **Globals** area, you will find the address of the computer for which enaio® server is licensed.

The **Module** area lists all licensed modules.

Abbreviated module names, the number of license keys and the license types are indicated there. 'C' stands for a floating license, and 'N' for a seat license.

4. Close the window using the close button on the title bar.

Licenses can have a restricted period of validity. In this case, a respective entry will be included in the **Globals** area. The periodic job 'CheckExpires' (see 'Category: Periodic Jobs') will automatically inform you about the expiration of licenses.

Monitoring the License Utilization

A periodic job is set up to monitor the licenses utilization of enaio® client ('ASC') and enaio® web-client ('WEB') in an interval of one hour. If more than 90% of the licenses 'ASC' or 'WEB' are occupied, the administrator will be notified by an e-mail message.

The utilization of licenses which are assigned to the 'Standard' station is also monitored. If the licenses of the 'Standard' station are assigned to a workstation that logs in or is set up through network setup and if for that reason more than 90% of the available licenses are used, the administrator will also be notified by a respective e-mail message.

Monitoring is configured with two entries in the section **Server properties > Category: General > General parameters**:

Parameters	Value	Description
Monitoring license utilization	90	Enter a value for the license utilization in percent – if this value is exceeded, an e-mail will be sent to the administrator. Enter the value '0' to not monitor the license utilization.
Email to license utilization	Send	Defines whether or not to send an e-mail to the administrator if the value defining the license utilization is exceeded. An exceeding of the utilization value will be written to the flow log if the log level is set to 3.

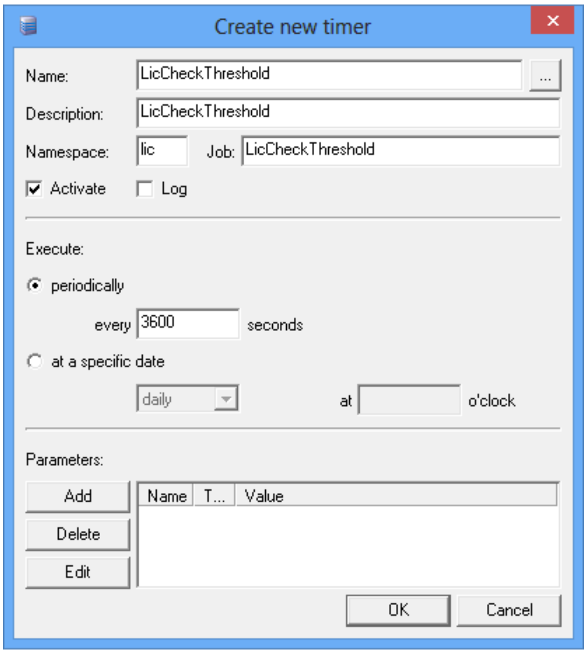
If monitoring is activated, the licenses of the 'Standard' station will be monitored through the network setup when a workstation logs in or is set up.

The parameters of the periodic job 'LicCheckThreshold' additionally define the interval in which licenses are being monitored:

You can change the monitoring interval of this periodic job in the **Periodic jobs** area. An interval of 3600 seconds is preset by default.

The parameter 'Modules' allows you to indicate licenses to check. The licenses of enaio® client and enaio® web-client are preset. You can enter further licenses or remove specified ones.

Details regarding configuration of periodic jobs can be found in the section 'Periodic Jobs.'


Create new timer

Name: LicCheckThreshold

Description: LicCheckThreshold

Namespace: lic Job: LicCheckThreshold

☑ Activate ☐ Log

Execute:

● periodically

every 3600 seconds

○ at a specific date

daily at o'clock

Parameters:

Name	T...	Value

Administering Floating Licenses

Floating licenses are not bound to workstations. You have the possibility to assign them to workstations if you want to assure that a module can always be used at a specific workstation. You administer floating license keys like seat license keys (see 'Administering Seat Licenses').

Floating license keys are assigned to the default station.

Programs that are launched on a workstation will register themselves at enaio® server. enaio® server assigns the license key, which are assigned to the computer address and the free license keys, which are assigned to the default workstation.

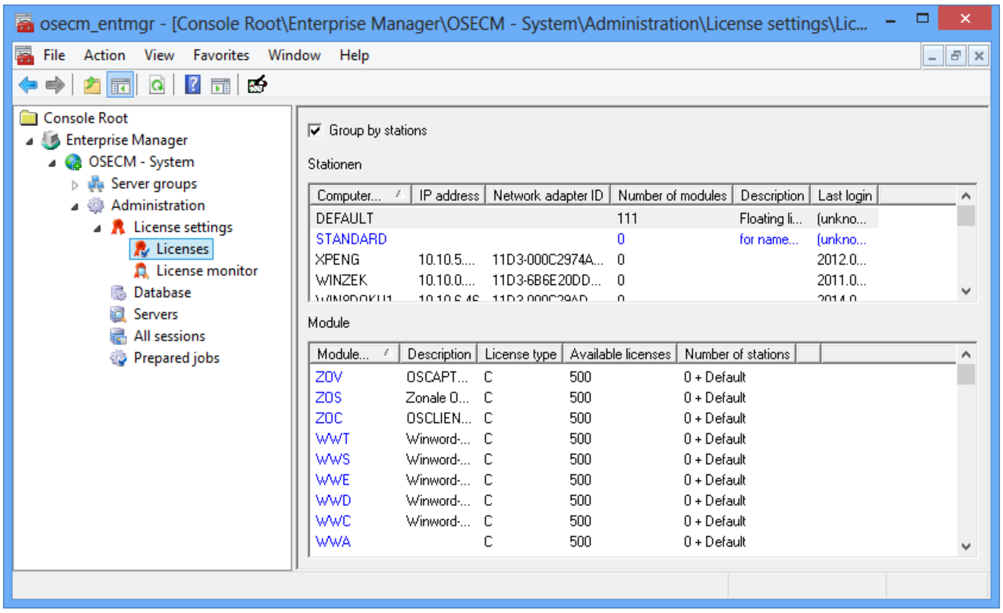
Programs and modules cannot be run unless they are licensed with the respective computer address or the default workstation. Users will be notified about the license conflict by an error message.

In the license files that you have received, all license keys are assigned to the default station. Therefore, you just need to reassign floating license keys, which you had assigned to a station, to the default station.

Follow these work items to assign floating license keys to the default workstation:

1. Select the entry **Administration** > **License settings** > **Licenses** from the console root.

   The license view will be displayed.



osecm_entmgr - [Console Root\Enterprise Manager\OSECM - System\Administration\License settings\Lic...

☑ Group by stations

Stationen

Computer...	IP address	Network adapter ID	Number of modules	Description	Last login
DEFAULT			111	Floating li...	(unkno...
STANDARD			0	for name...	(unkno...
XPENG	10.10.5....	11D3-000C2974A...	0		2012.0...
WINZEK	10.10.0....	11D3-6B6E20DD...	0		2011.0...
WIN8DOKU1	10.10.6.46	11D3-000C29AD...	0		2014.0...

Module

Module...	Description	License type	Available licenses	Number of stations
ZOV	OSCAPT...	C	500	0 + Default
ZOS	Zonale O...	C	500	0 + Default
ZOC	OSCLIEN...	C	500	0 + Default
WWT	Winword-...	C	500	0 + Default
WWS	Winword-...	C	500	0 + Default
WWE	Winword-...	C	500	0 + Default
WWD	Winword-...	C	500	0 + Default
WWC	Winword-...	C	500	0 + Default
WWA		C	500	0 + Default

2. Select the **Default** station.

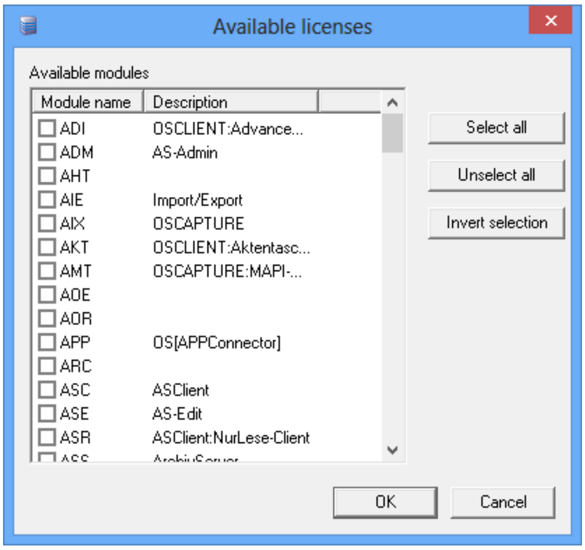
   The assigned modules are listed below in the **Modules** area.

   If the station does not exist anymore, set up a new one by selecting **Add 'Default' station** from the context menu.

3. Select **Add modules** from the context menu

   The **Available licenses** window will open.

   This window lists all available module license keys, which are available through licensing and have not yet been assigned to the default station.



Available licenses

Available modules

Module name	Description
☐ ADI	OSCLIENT:Advance...
☐ ADM	AS-Admin
☐ AHT	
☐ AIE	Import/Export
☐ AIX	OSCAPTURE
☐ AKT	OSCLIENT:Aktentasc...
☐ AMT	OSCAPTURE:MAPI-...
☐ AOE	
☐ AOR	
☐ APP	OS[APPConnector]
☐ ARC	
☐ ASC	ASClient
☐ ASE	AS-Edit
☐ ASR	ASClient:NurLese-Client
☐ ASS	ArchivServer

4. Select the modules you want to assign to the station license key.

5. The **Select all** button will select all modules, the **Deselect all** button will remove selected modules, and the **Invert selection** button will invert the current selection.

6. Confirm with **OK**.

   The changes will be saved.

The selected module license keys will be assigned to the default station and listed in the **Module** area of the license view.

You can print out a module report via the context menu of a module or of several selected modules. In addition to the view data, server data is also printed out.

Administering Seat Licenses

Seat license keys are linked to a workstation. Use enaio® enterprise-manager to include workstations in the license system and to assign module-specific license keys.

Set up the 'Standard' station in order that, when installing local components required for a computer (network setup), any new computer will be entered as workstation and will be provided with all seat license keys that are assigned to the 'Standard' station, as long as license keys are available. In addition, all available seat licenses of the 'Standard' station are assigned to each computer that accesses enaio® and is entered in the workstation list.

To add a workstation through enaio® enterprise-manager, the workstation's IP address or GUID is required. The IP addresses can be determined using enaio® enterprise-manager once the workstations are available in and connected to the network.

> You must either use only GUIDs or only IP addresses to integrate all workstations.

Every computer, from which a user accesses enaio® using enaio® client or another enaio® component, will be listed automatically as a workstation.

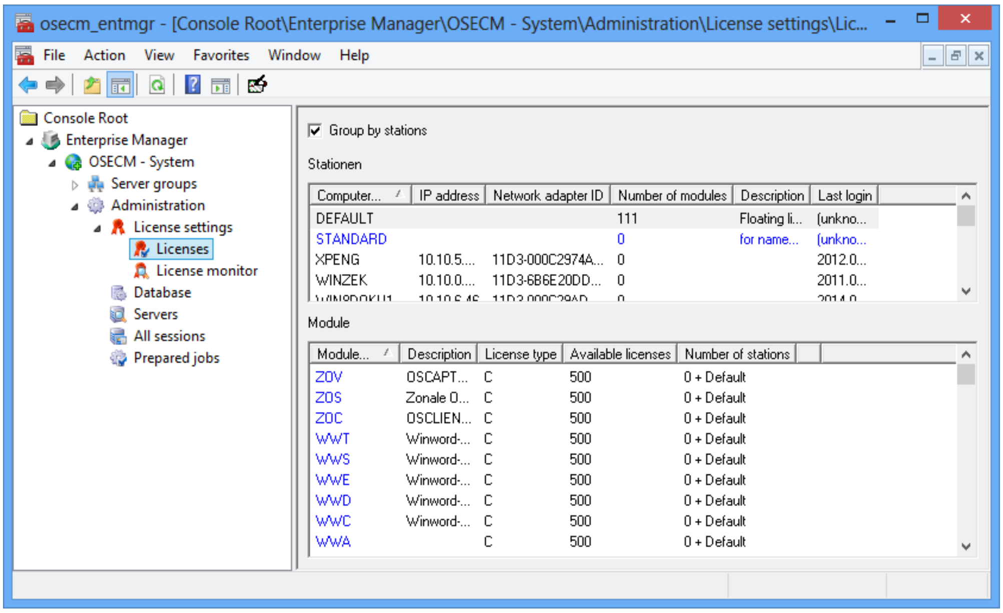
Adding a Workstation

Seat license keys are linked to workstations. These workstations can be added to the enaio® system.

To add a workstation to the system, follow these steps:

1. Select the entry **Administration > License settings > Licenses** from the console root.

   The license view will be displayed.



☑ Group by stations

Stationen

Computer...	IP address	Network adapter ID	Number of modules	Description	Last login
DEFAULT			111	Floating li...	(unkno...
STANDARD			0	for name...	(unkno...
XPENG	10.10.5....	11D3-000C2974A...	0		2012.0...
WINZEK	10.10.0....	11D3-6B6E20DD...	0		2011.0...
WIN8DOKU1	10.10.6.46	11D3-000C29AD...	0		2014.0...

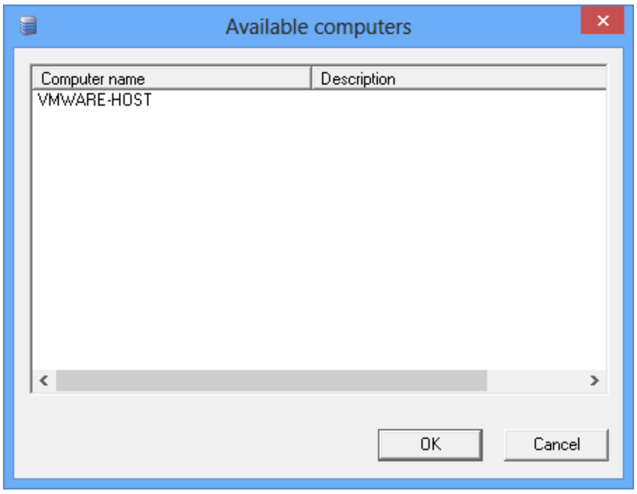
Module

Module...	Description	License type	Available licenses	Number of stations
ZOV	OSCAPT...	C	500	0 + Default
ZOS	Zonale O...	C	500	0 + Default
ZOC	OSCLIEN...	C	500	0 + Default
WWT	Winword-...	C	500	0 + Default
WWS	Winword-...	C	500	0 + Default
WWE	Winword-...	C	500	0 + Default
WWD	Winword-...	C	500	0 + Default
WWC	Winword-...	C	500	0 + Default
WWA		C	500	0 + Default

2. Select **Add stations** from the context menu in the **Stations** section

3. In order to add the 'Standard' station, select the item **Add 'Standard' station** from the context menu').

   The **Available computers** window will open.



Computer name	Description
VMWARE-HOST	

All stations which are accessible through the network, and have not yet been added, are listed in the window.

4. Select one or more stations.

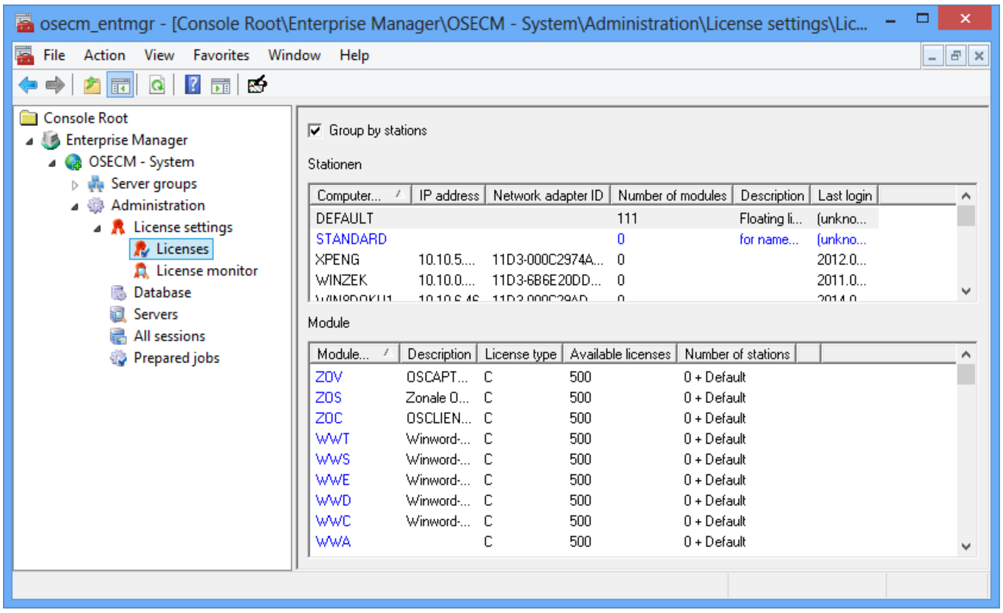
5. Click **OK**.

   The new stations will be shown in the license view. You can assign modules to the stations (see 'Adding Modules').

Follow these steps to manually add a workstation:

1. Select the entry **Administration > License settings > Licenses** from the console root.

   The license view will be displayed.



☑ Group by stations

Stationen

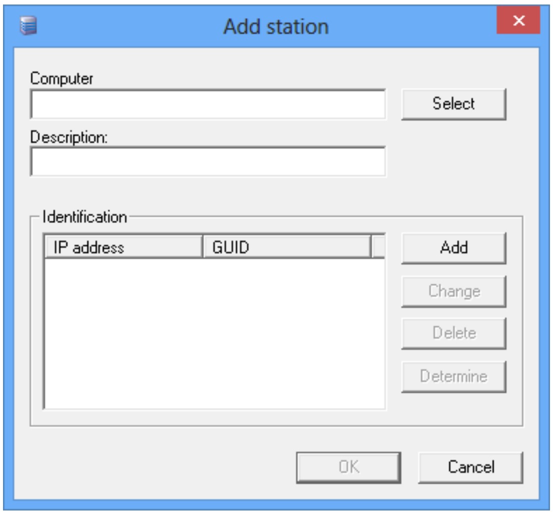
Computer...	IP address	Network adapter ID	Number of modules	Description	Last login
DEFAULT			111	Floating li...	(unkno...
STANDARD			0	for name...	(unkno...
XPENG	10.10.5....	11D3-000C2974A...	0		2012.0...
WINZEK	10.10.0....	11D3-6B6E20DD...	0		2011.0...
WIN8DOKU1	10.10.6.46	11D3-000C29AD...	0		2014.0...

Module

Module...	Description	License type	Available licenses	Number of stations
ZOV	OSCAPT...	C	500	0 + Default
ZOS	Zonale O...	C	500	0 + Default
ZOC	OSCLIEN...	C	500	0 + Default
WWT	Winword-...	C	500	0 + Default
WWS	Winword-...	C	500	0 + Default
WWE	Winword-...	C	500	0 + Default
WWD	Winword-...	C	500	0 + Default
WWC	Winword-...	C	500	0 + Default
WWA		C	500	0 + Default

2. Select **Add station manually** from the context menu in the **Stations** section.

   The **Add station** window will open.



3. Enter a computer name or click on **Choose**.

   Use **Choose** to select an available station across the network.

4. Optionally, you can enter a **Description**. It will be displayed together with the computer name in the license view.

5. Click the **Add** button in the **Identification** area.

   The **Computer identification** window will open.

6. If all computers are to be integrated by IP addresses, enter the **IP address** of the computer.

7. If all computers are to be integrated by GUID, enter the **Network adapter ID** (GUID) of the computer.

8. Confirm with **OK**.

The new station will be shown in the license view. You can assign modules to the station (see 'Adding Modules').

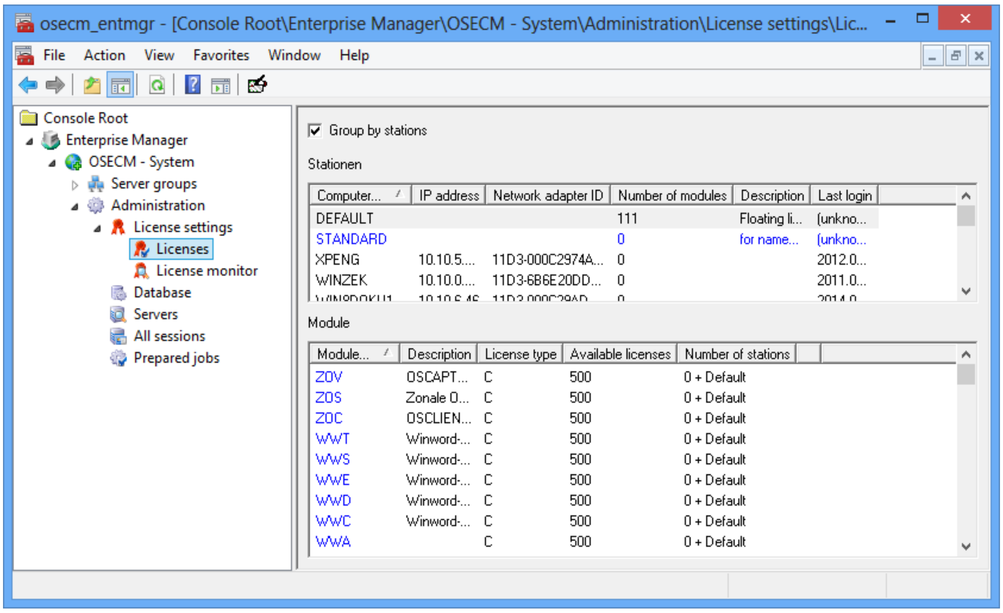
Several IP addresses/GUIDs can be indicated for computer identification.

Modifying and Removing Workstations

Follow these steps to remove a workstation:

1. Select the entry **Administration** > **License settings** > **Licenses** from the console root.

   The license view will be displayed. Set up stations will be listed.



☑ Group by stations

Stationen

Computer...	IP address	Network adapter ID	Number of modules	Description	Last login
DEFAULT			111	Floating li...	(unkno...
STANDARD			0	for name...	(unkno...
XPENG	10.10.5....	11D3-000C2974A...	0		2012.0...
WINZEK	10.10.0....	11D3-6B6E20DD...	0		2011.0...
WIN8DOKU1	10.10.6.46	11D3-000C29AD	0		2014.0

Module

Module...	Description	License type	Available licenses	Number of stations
ZOV	OSCAPT...	C	500	0 + Default
ZOS	Zonale O...	C	500	0 + Default
ZOC	OSCLIEN...	C	500	0 + Default
WWT	Winword-...	C	500	0 + Default
WWS	Winword-...	C	500	0 + Default
WWE	Winword-...	C	500	0 + Default
WWD	Winword-...	C	500	0 + Default
WWC	Winword-...	C	500	0 + Default
WWA		C	500	0 + Default

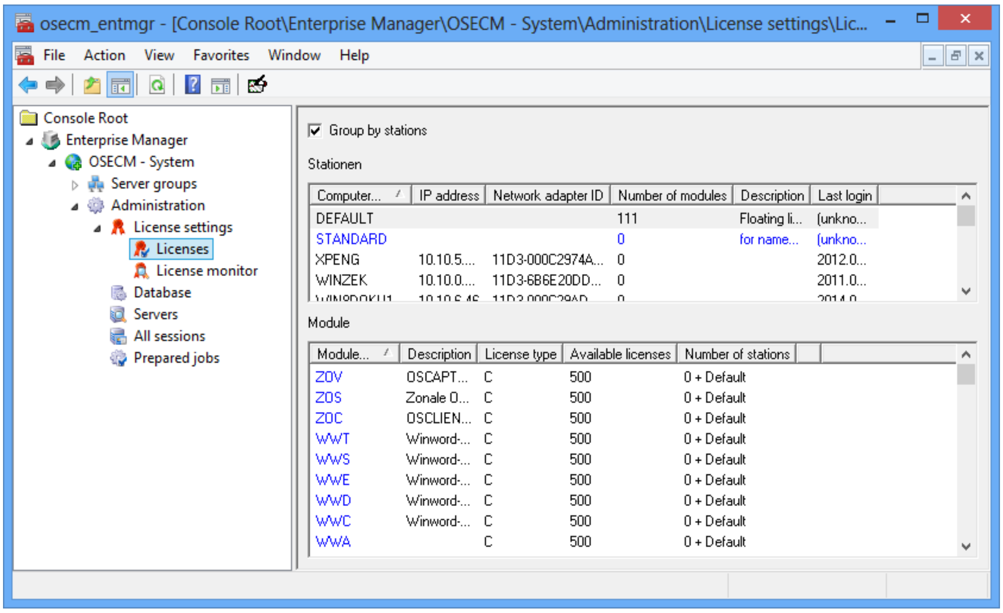
2. Select a station.
3. Select **Remove station** from the context menu.

   The station will be deleted.

Follow these steps to modify a workstation:

1. Select the entry **Administration** > **License settings** > **Licenses** from the console root.

   The license view will be displayed. Set up stations will be listed.



☑ Group by stations

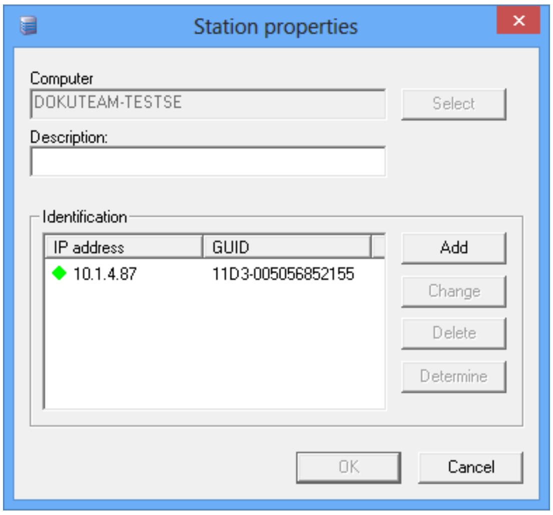
Stationen

Computer...	IP address	Network adapter ID	Number of modules	Description	Last login
DEFAULT			111	Floating li...	(unkno...
STANDARD			0	for name...	(unkno...
XPENG	10.10.5....	11D3-000C2974A...	0		2012.0...
WINZEK	10.10.0....	11D3-6B6E20DD...	0		2011.0...

Module

Module...	Description	License type	Available licenses	Number of stations
ZOV	OSCAPT...	C	500	0 + Default
ZOS	Zonale O...	C	500	0 + Default
ZOC	OSCLIEN...	C	500	0 + Default
WWT	Winword-...	C	500	0 + Default
WWS	Winword-...	C	500	0 + Default
WWE	Winword-...	C	500	0 + Default
WWD	Winword-...	C	500	0 + Default
WWC	Winword-...	C	500	0 + Default
WWA		C	500	0 + Default

2. Select a station.
3. Select **Properties** from the context menu. The **Station properties** window will open.



Computer: DOKUTEAM-TESTSE

Description:

Identification

IP address	GUID
10.1.4.87	11D3-005056852155

You can use the following buttons in the **Identification** area:

- **Add** – to add another computer.
- **Modify** – to change the IP address and the GUID.
- **Delete** – to delete the IP address and the GUID.
- **Determine** – to redetermine the IP address.

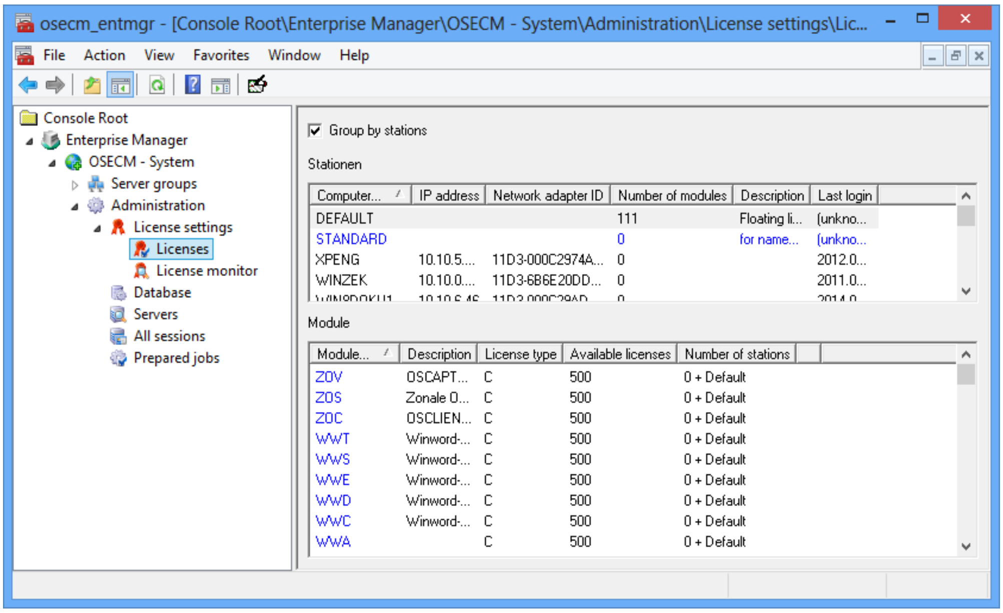
4. Confirm with **OK**.

Adding Modules

Follow these work items to assign license keys to workstations for modules:

1. Select the entry **Administration > License settings > Licenses** from the console root.

The license view will be displayed. Set up stations will be listed.



☑ Group by stations

Stationen

Computer...	IP address	Network adapter ID	Number of modules	Description	Last login
DEFAULT			111	Floating li...	(unkno...
STANDARD			0	for name...	(unkno...
XPENG	10.10.5....	11D3-000C2974A...	0		2012.0...
WINZEK	10.10.0....	11D3-6B6E20DD...	0		2011.0...
WIN8DOKU1	10.10.6.46	11D3-000C29AD	0		2014.0

Module

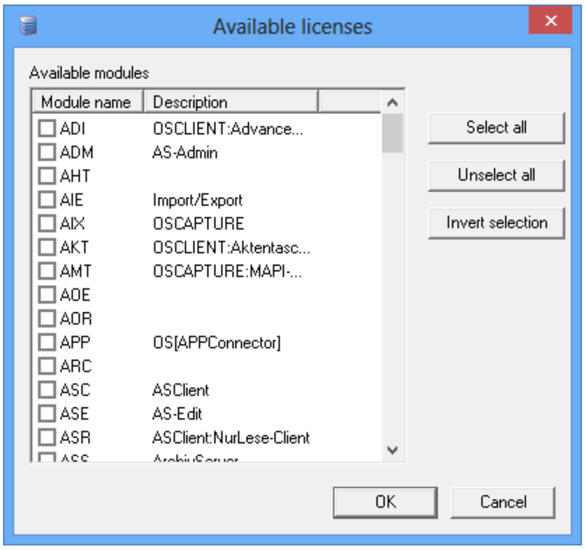
Module...	Description	License type	Available licenses	Number of stations
ZOV	OSCAPT...	C	500	0 + Default
ZOS	Zonale O...	C	500	0 + Default
ZOC	OSCLIEN...	C	500	0 + Default
WWT	Winword-...	C	500	0 + Default
WWS	Winword-...	C	500	0 + Default
WWE	Winword-...	C	500	0 + Default
WWD	Winword-...	C	500	0 + Default
WWC	Winword-...	C	500	0 + Default
WWA		C	500	0 + Default

2. Select the station you want to add module license keys to.

   The license keys which have already been assigned will be listed in the **Modules for selected station** area.

3. Select **Add modules** from the station's context menu.

   All module license keys, which are available through the license file and have not been assigned to the station, will be listed.



Available modules

Module name	Description
☐ ADI	OSCLIENT:Advance...
☐ ADM	AS-Admin
☐ AHT	
☐ AIE	Import/Export
☐ AIX	OSCAPTURE
☐ AKT	OSCLIENT:Aktentasc...
☐ AMT	OSCAPTURE:MAPI-...
☐ AOE	
☐ AOR	
☐ APP	OS[APPConnector]
☐ ARC	
☐ ASC	ASClient
☐ ASE	AS-Edit
☐ ASR	ASClient:NurLese-Client
☐ ASS	ArchivServer

4. Select the modules you want to assign to the station license key.
5. The **Select all** button will select all modules, the **Deselect all** button will remove selected modules, and the **Invert selection** button will invert the selection.
6. Confirm with **OK**.

   The changes will be saved.

The selected module license keys will be assigned to the station and shown in the **Modules** area.

You can print out a module report via the context menu of a module or of several selected modules. In addition to the view data, server data is also printed out.

> Layer administration is licensed in the 'ADI' module. Use this module, a license key must be available at every workstation.

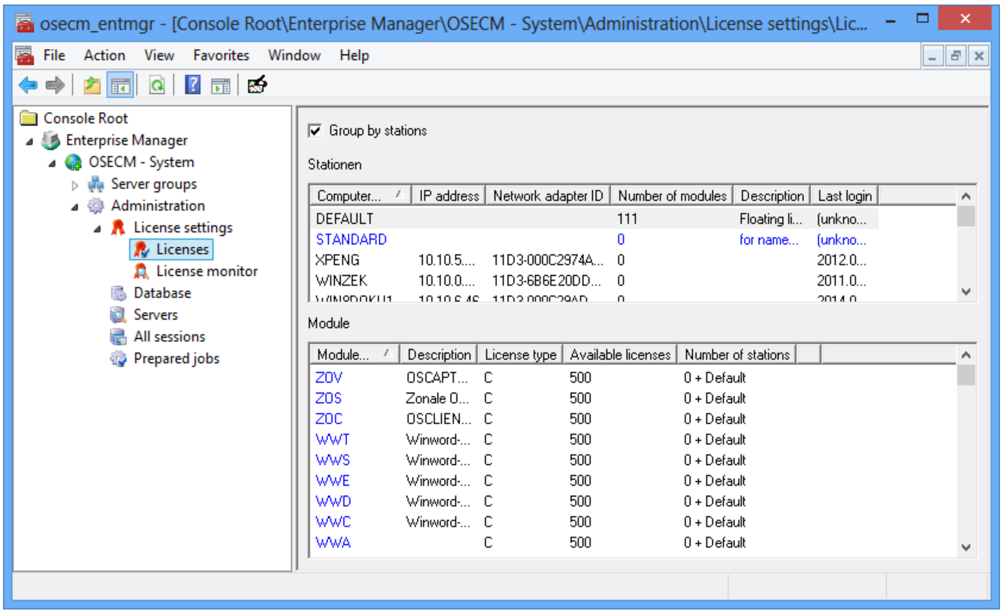
If you assign seat licenses to the 'Standard' station, this seat license will be automatically assigned, as long as they are available, to each station that is integrated with network setup or that logs in.

Deleting Modules

Follow these work items to delete the assignment of a module license key to stations:

1. Select the entry **Administration** > **License settings** > **Licenses** from the console root.

   The license view will be displayed. Set up stations will be listed.



☑ Group by stations

Stationen

Computer...	IP address	Network adapter ID	Number of modules	Description	Last login
DEFAULT			111	Floating li...	(unkno...
STANDARD			0	for name...	(unkno...
XPENG	10.10.5....	11D3-000C2974A...	0		2012.0...
WINZEK	10.10.0....	11D3-6B6E20DD...	0		2011.0...
WIN8DOKU1	10.10.6.46	11D3-000C29AD	0		2014.0

Module

Module...	Description	License type	Available licenses	Number of stations
ZOV	OSCAPT...	C	500	0 + Default
ZOS	Zonale O...	C	500	0 + Default
ZOC	OSCLIEN...	C	500	0 + Default
WWT	Winword-...	C	500	0 + Default
WWS	Winword-...	C	500	0 + Default
WWE	Winword-...	C	500	0 + Default
WWD	Winword-...	C	500	0 + Default
WWC	Winword-...	C	500	0 + Default
WWA		C	500	0 + Default

2. Select a station. The assigned module license keys are listed.
3. Select a module.
4. Select **Remove modules** from the context menu.

The module will be removed from the list of assigned modules.

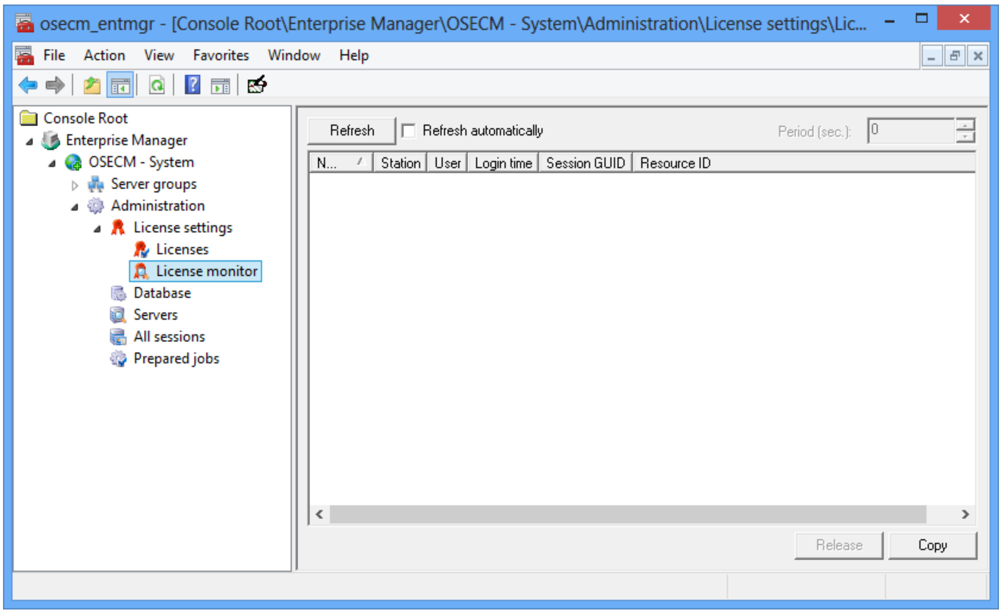
Printing Module Lists

You can select modules and print a module list via the context menu.

License Monitoring

You can use enaio® enterprise-manager to view which workstation currently accesses which license keys.

Select the entry **Administration > License settings > License monitor** from the console tree in order to list the license keys which are being used on which station by which user.



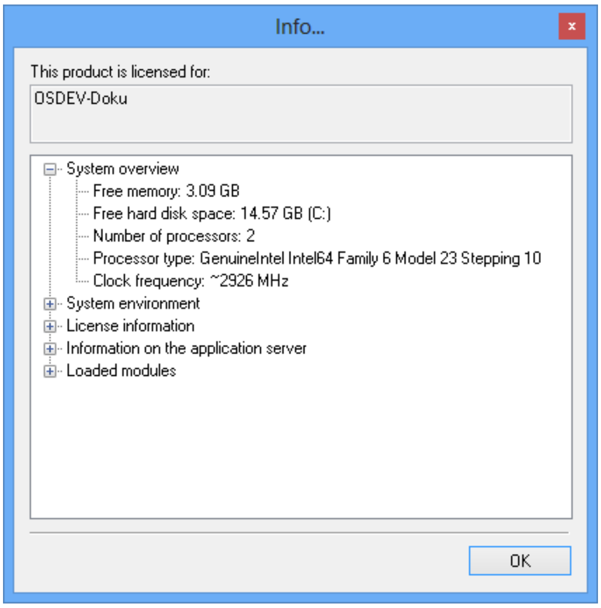
The 'license' service reserves all 'WEB' licenses, which are shown as 'occupied.'

Refresh the list by clicking the **Update** button or by specifying an update interval in seconds.

Release the license key by selecting entries and clicking on **Release**.

By clicking the **Copy** button you can copy the entire list to the clipboard.

The **ENAIO > Information > About** menu of each enaio® client application will open an information dialog, which also contains license information.



Info...

This product is licensed for:

OSDEV-Doku

- System overview
  - Free memory: 3.09 GB
  - Free hard disk space: 14.57 GB (C:)
  - Number of processors: 2
  - Processor type: GenuineIntel Intel64 Family 6 Model 23 Stepping 10
  - Clock frequency: ~2926 MHz
- System environment
- License information
- Information on the application server
- Loaded modules

The **Not licensed modules** area lists all unavailable modules for which no license keys have been imported.

The license errors may be displayed:

600 The maximum number of stations has already logged in.

602 The license entry for this station has not been found.

607 The test license has expired.

609 Test licenses are not supported by this module.

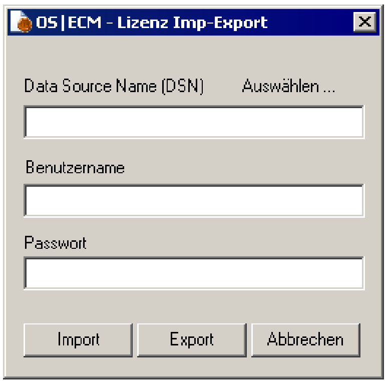
Importing Licenses

The license keys for enaio® server are only available as seat license keys with a fixed GUID or TCP/IP address. If the address changes, you will need a new license file. If you acquire additional license keys, you also get a new license file.

If you work with several servers, each enaio® server (except the family control server) must be restarted after import. You must also restart all applications which are affected by these changes.

You import the license file via enaio® enterprise-manager.

If enaio® server is not running, select the entry **All tasks > Start axliccfgeditor** from the context menu.



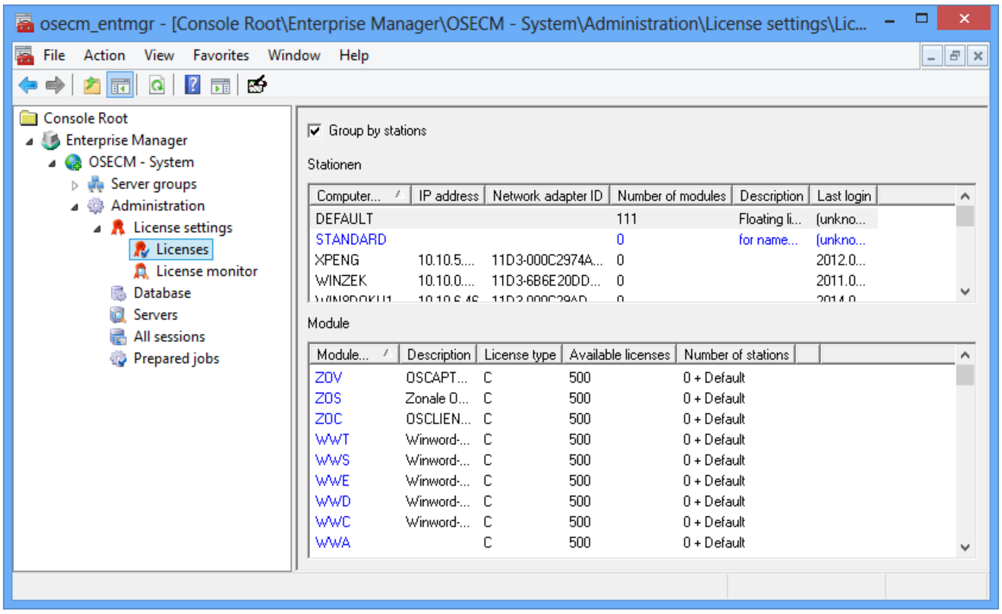
Enter the DSN of the database connection, the user name, and the password, and click on the **Import** button.

Enter the source directory for import. The source directory is the directory in which the license file `aslic.dat` is found.

> The license import with AXLICCFGEDITOR only imports license data and allows you to start enaio® server afterwards. After purchasing new licenses, you have to import the license file `aslic.dat` again through enaio® enterprise-manager so that these licenses can be administered.

Start enaio® server and import licenses directly with enaio® enterprise-manager.

Select the **Administration** > **License settings** > **Licenses** item from the console tree to show the license view.



☑ Group by stations

Stationen

Computer...	IP address	Network adapter ID	Number of modules	Description	Last login
DEFAULT			111	Floating li...	(unkno...
STANDARD			0	for name...	(unkno...
XPENG	10.10.5....	11D3-000C2974A...	0		2012.0...
WINZEK	10.10.0....	11D3-6B6E20DD...	0		2011.0...

Module

Module...	Description	License type	Available licenses	Number of stations
ZOV	OSCAPT...	C	500	0 + Default
ZOS	Zonale O...	C	500	0 + Default
ZOC	OSCLIEN...	C	500	0 + Default
WWT	Winword-...	C	500	0 + Default
WWS	Winword-...	C	500	0 + Default
WWE	Winword-...	C	500	0 + Default
WWD	Winword-...	C	500	0 + Default
WWC	Winword-...	C	500	0 + Default
WWA		C	500	0 + Default

You can import licenses into the database by selecting the entry **All tasks** > **License import** from the context menu of the **Licenses** entry in the console tree.

The configuration file `aslic.cfg` with station and module data can be imported at the same time.

> You can also export license data from the database into a file. It can be useful to the support department for error analysis. The license file is also needed to generate a signature code (see 'Subsequent Creation of Hash Values').
> Moreover, you do not need an exported license file. The configuration file `aslic.cfg` and a report file in which export results are logged will also be exported.

License Overview

The following overview shows which enaio® components require which license modules.

A distinction is made between the following license types:

- S – Server license
- F – Floating license
- E – Enterprise license
- A – Workstation license, named
- C – Workstation license, concurrent

Component	License Type	License
enaio® advanced-dms	S	WW2, WWS, WWT, PDF, WWE, SDE
enaio® annotation	A/F	ADI
enaio® appconnector	S	APP, MOB
enaio® capture-barcode	A	SIC, RER, REK
enaio® capture-barcode-index	A	W2D
enaio® capture-basic	A	AIX
enaio® capture-datamatching	A	OCD
enaio® capture-ocr	A	ZOV, RER
enaio® capture-scan	A	SCA, SFI, STW
enaio® capture-script	A	VBV
enaio® capture-valid	A	VAL, AIE
enaio® client	F/A	ASC, M_D, M_E, M_P, M_M, M_W, M_X, M_A, M_C, SUB, REM, MWC, WW1, OSE, VBX, MAI, GAD
enaio® client-api	S	
enaio® cold	S	COL
enaio® cold-configuration	C	COL
enaio® contentminer	S	OKM
enaio® data2enaio	S	D2E
enaio® data2s	S	D2S, DOC
enaio® directory-services	S	LDP
enaio® dynamics-ax	S	DAX
enaio® dynamics-nav	S	DNA
enaio® editor	E	ASE

enaio® editor-for-events	E	EVE
enaio® SQL queries	E	OSM
enaio® editor-for-workflow	E	WFG
enaio® editor-package	E	ASE, WFG, OSM, EVE, VBE
enaio® exchange	S	OSX
enaio® feedreader	S	FRD
enaio® filesystem	S	OFS
enaio® filesystem-archiver	E	FSA
enaio® fulltext	S	VTX, LIS
enaio® import-export	S	AIE
enaio® import-export-configuration	C	AIE
enaio® jump2enaio	S	J2E
enaio® jump2s	S	J2S
enaio® krypto	S	KRY,SKR
enaio® mail-archiver	S	MAR
enaio® mediamanagement-export	S	DPE
enaio® mediamanagement-import	S	DPI
enaio® mediamanagement-catalog	S	DPK
enaio® ocr	S	VOC, ZOS, ZOC, ZOV
enaio® pagination	S	PAG
enaio® pdfa-dispatcher	S	CLE
enaio® pdfa-validator	S	PDA
enaio® renditionplus	S	REN
enaio® repositorymanager	S	L3R
enaio® scan	A/F	SCC,SCT
enaio® search	S	OSS
enaio® server-20	S	ASS, ADM, AXA, AXK, WFE, WFA, ASW, AVG, CPR, WAH
enaio® server-200	S	ASS, ADM, AXA, AXK, WFE, WFA, ASW, AVG, CPR, WAH
enaio® server-50	S	ASS, ADM, AXA, AXK, WFE, WFA, ASW,

		AVG, CPR, WAH
enaio® server-api	S	
enaio® server-api-access	F	
enaio® server-balance	S	ASS
enaio® server-cluster	S	ASS
enaio® server-ul	S	ASS, ADM, AXA, AXK, WFE, WFA, ASW, AVG, CPR, WAH
enaio® sharepoint-archiv	S	SPA
enaio® sharepoint-dms	S	SPD
enaio® signature-10	S	DIS
enaio® signature-50	S	DIS
enaio® storage-for-centera	S	CEN
enaio® storage-for-emc-celerra	S	NAP
enaio® storage-for-emc-cluster	S	CEM
enaio® storage-for-fast-silent-cubes	S	NAP
enaio® storage-for-grau	S	NAP
enaio® storage-for-netapp	S	NAP
enaio® tapi	S	VBT
enaio® terminal	S	OLT
enaio® text-analysis-multilanguage	S	LIS
enaio® webclient	F	Web
enaio® winapp	S	OLS

Configuration of the Security System

Introduction to the Security System

After applying changes to the security system, the 'adm' engine will be reloaded automatically on all servers in use. Changes affecting other applications will only take effect after restart. Users can update the security system in enaio® client with the key combination **Ctrl+F5**.

The security system for access to archive object types is group-orientated. Access rights to archive objects are distributed to users due to their membership in one or more groups.

Access rights allow the differentiated definition for each type of archive object and can be specified using clauses. Logical expressions enable users to be granted with or denied access to archive object dependent on the objects' indexing. The concept of logical expressions lets you create a structure that allows users to grant with or deny access to archive objects through the objects' indexing in enaio® client, without having to personally modify administrative settings in the security system.

The layers concept is also integrated into the security system. It allows you to provide users with access to documents which before had to be denied in general security systems. For example, personal data in documents can be blackened out on layers for particular user groups. All members of a user group can open such documents, and can print and export them with all blackened areas.

Layer administration is licensed in the 'ADI' module. Use this module, a license key must be available at every workstation.

The security system allows you controlling access to administrative programs for every single user. The access rights to the applications enaio® administrator, enaio® start, enaio® editor, and enaio® capture are assigned to individual users as system roles. Usually, different types of users and user groups receive different system roles. Some functions in enaio® client also require particular system roles.

Additionally, you can create profiles and assign to users. Administering the security system is simpler via the assignment of profiles. It is also possible to make saved searches, extended queries, and links to external applications available to all users with the same profile.

Logging Changes

An additional logging of changes on the security system via the 'Security system' and 'Remote user administration' area can be activated through enaio® enterprise-manager.

You activate the appropriate options via **Server properties > General > Security**.

The log can then be opened in enaio® administrator via the **Extras** menu.

The log can be filtered by categories, free text, and date. The log entries can be grouped by category, time, and user.

> Users require the system role 'Administrator: Configure security system' in order to access the logs and to delete entries.

Global and Local Administration

In enaio®, at least one supervisor is required: a user to whom all system roles have been assigned. This user has access to all programs and data.

Every other user with the system role 'Administrator: Configure security system' fulfills the function of a supervisor as it allows him to grant his profile or any other user any system role, thus providing him with access to all programs and data.

Within complex environments, setting up local administrators with limited rights to change system configuration may be useful.

Within a specified area, local administrators can create users and groups, assign users to groups, give them previously approved system roles, and manage user accounts.

Local administrators cannot establish or edit the group-specific access rights to object types for the groups. This task must be performed by a user with the system role 'Administrator: Configure security system'.

Areas can be created by a supervisor or by a user with the system role 'Administrator: Configure local security groups'.

Users who are meant to perform the functions of a local administrator need the system role 'Administrator: Configure local security groups'.

Users who can create and configure local security groups fulfill the function of a supervisor.

Follow these steps to configure a local administrator:

1. Create an area.
2. Assign groups and users as an option to the area.

   One group is designated as the standard group. New users will automatically become members of this group.
3. Indicate the local administrator.

   The user with this function must be provided with the system role 'Administrator: Configure local security groups'.

The local administrator may be given various rights, which are subject to different limitations.

4. Define which system roles the local administrator is allowed to distribute.

The configuration dialog will be opened through the **Remote user administration** item in the **Configuration** menu or the respective button in the toolbar.

Local administration is carried out in the same manner as global administration in the **Security system** window. The breadth of functionality is respectively limited.

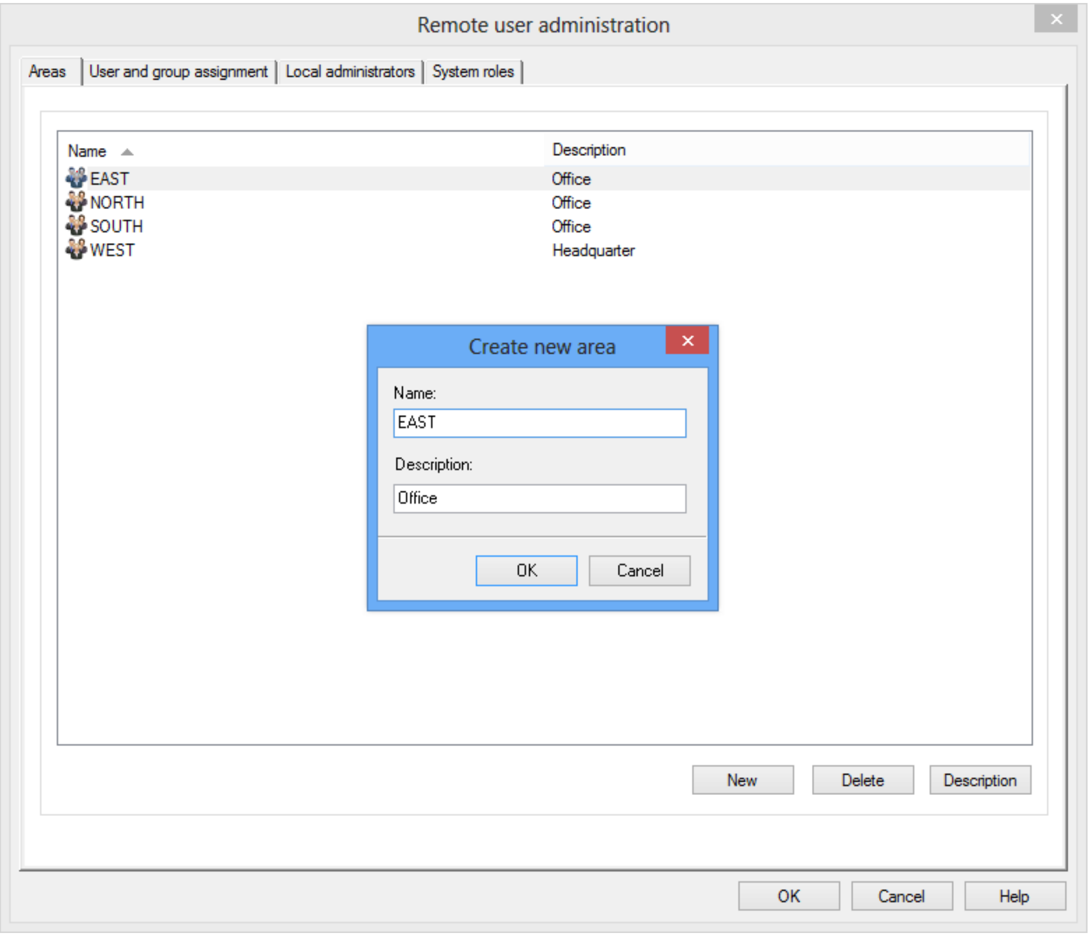
Groups and users need names which are unambiguous across all areas.

Creating Areas

The **Areas** register of the remote user administration allows you to create new areas.

Set up areas are listed on the tab.

Use the **New** button to create a new area with a maximum of 255 characters for the name. A description is optional.



Remote user administration

Areas | User and group assignment | Local administrators | System roles

Name	Description
EAST	Office
NORTH	Office
SOUTH	Office
WEST	Headquarter

Create new area

Name: EAST

Description: Office

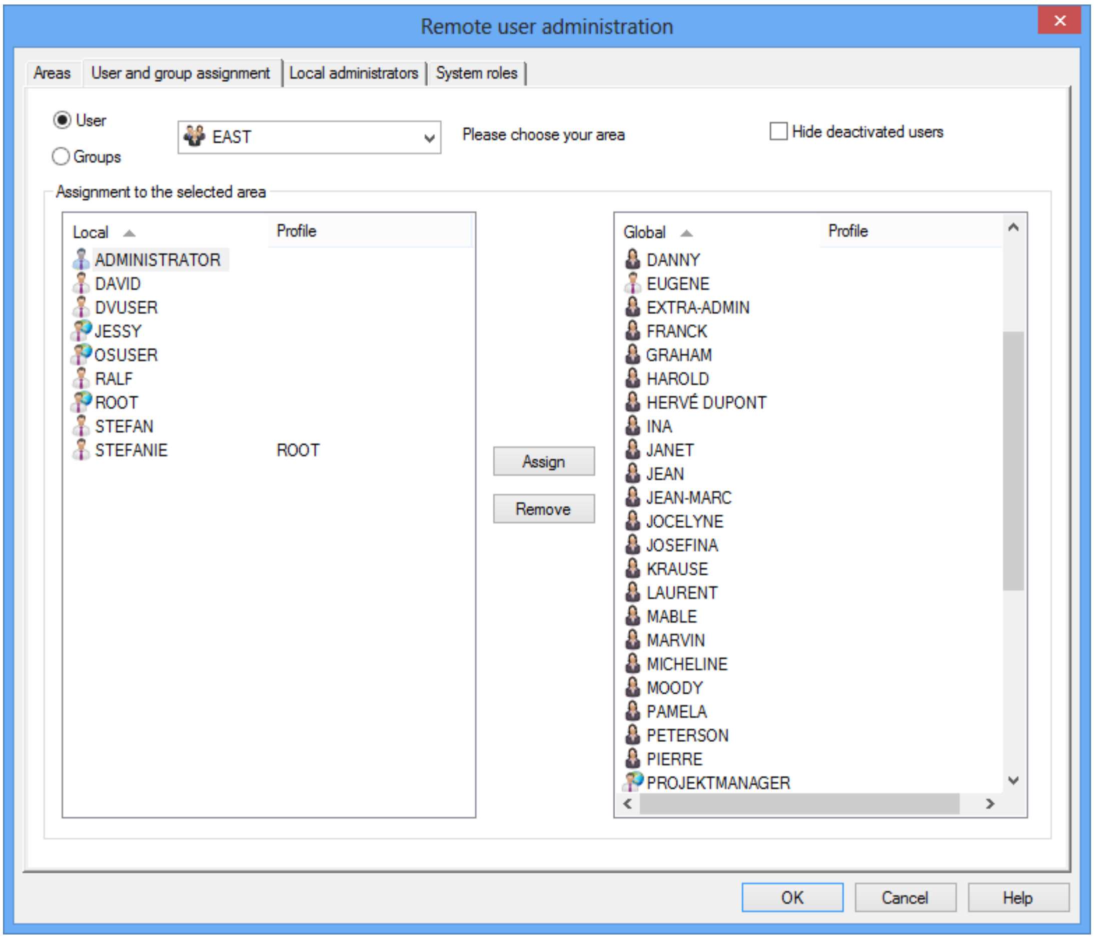
Use the **Delete** button to delete an area. If users or groups are distributed to the area, they will be moved into the global area.

Use the **Description** button to change the description of an area.

Local Groups and Users

On the **User and group assignment** tab of the remote user administration dialog, created users and groups are assigned to an area.

New users and groups are created through the respective functions in the **Security system** dialog, which is described below.



Local	Profile
ADMINISTRATOR	
DAVID	
DVUSER	
JESSY	
OSUSER	
RALF	
ROOT	
STEFAN	
STEFANIE	ROOT

Global	Profile
DANNY	
EUGENE	
EXTRA-ADMIN	
FRANCK	
GRAHAM	
HAROLD	
HERVÉ DUPONT	
INA	
JANET	
JEAN	
JEAN-MARC	
JOCELYNE	
JOSEFINA	
KRAUSE	
LAURENT	
MABLE	
MARVIN	
MICHELINE	
MOODY	
PAMELA	
PETERSON	
PIERRE	
PROJEKTMANAGER	

When selecting an area for which you can create assignments from the drop down menu, all global users and user groups will be listed on the right side of the dialog.

Use the **Assign** and **Remove** button to configure the groups and users for the area.

Groups

In the global area, every new user automatically becomes a member of the 'Standard' group. This group cannot be deleted.

In a local area, the group assigned at first is automatically given the role of the 'Standard' group. To define another group as standard group, select a group in the left dialog area and use the respective item of the context menu. You can remove all groups from an area. However, users cannot be assigned to an area without any groups.

When removing a group, all users who exclusively are members of this group will become members of the standard group.

To remove a group which is set as the standard group, you have to assign this property to another group first. If there are no other groups, all users will become members of the 'Standard' group in the global area.

You will receive a security confirmation dialog which informs you of this fact.

Removed groups will be assigned to the global area.

> A local administrator can create groups without having the system role 'Administrator: Configure security system', but he cannot provide group-specific access rights to object types.

User

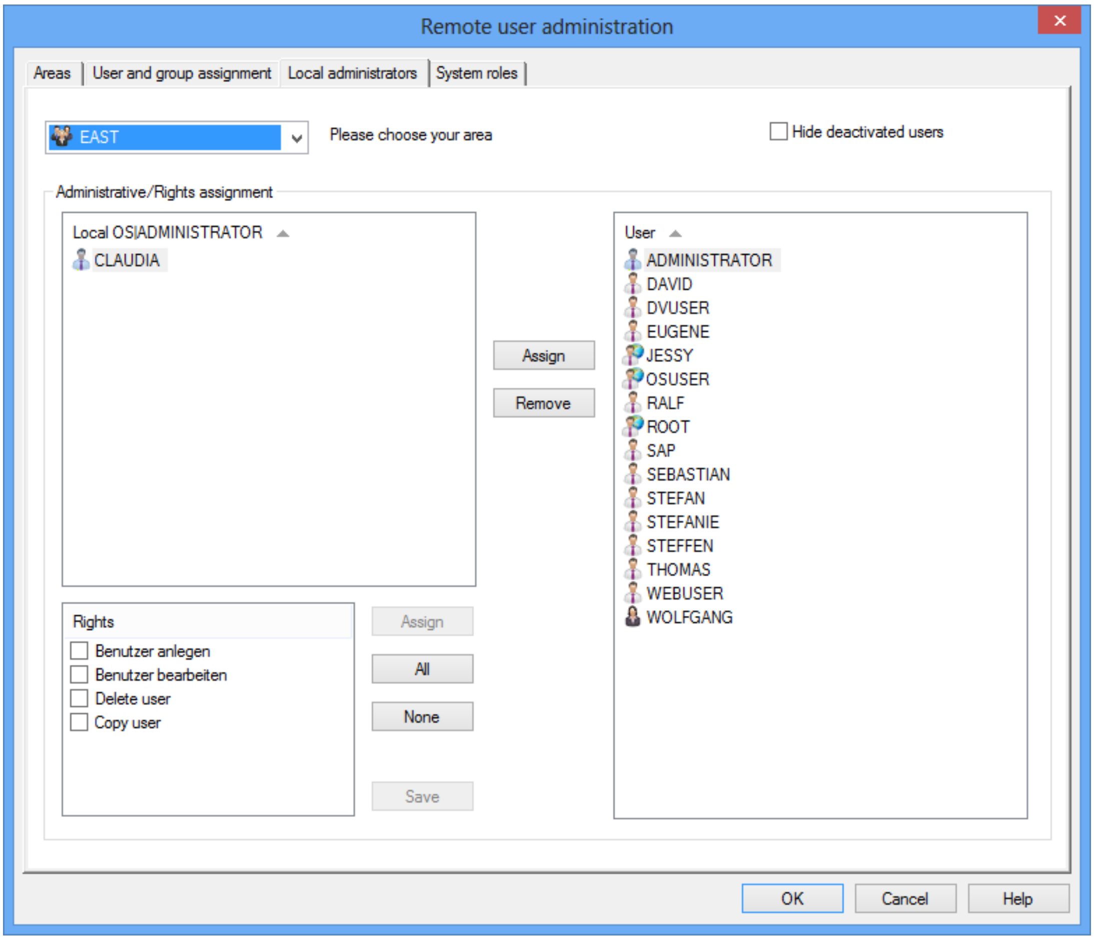
Global users cannot be assigned to an area unless at least one group has been assigned to it. Assigned users automatically become members of the group which is set as the standard group. Users can only be a member of one area.

Local administrators can add new users to their area but cannot move global users into an area.

Local Administrators

The local administrator of an area is set on the **Local administrators** tab.

When selecting an area from the drop down menu, all users with the system role 'Administrator: Configure local security groups' will be listed on the right side of the dialog.



EAST — Please choose your area

□ Hide deactivated users

Administrative/Rights assignment

Local OS|ADMINISTRATOR
CLAUDIA

User
ADMINISTRATOR
DAVID
DVUSER
EUGENE
JESSY
OSUSER
RALF
ROOT
SAP
SEBASTIAN
STEFAN
STEFANIE
STEFFEN
THOMAS
WEBUSER
WOLFGANG

Rights
□ Benutzer anlegen
□ Benutzer bearbeiten
□ Delete user
□ Copy user

You can mark several users as local administrators.

The local administrator may be given various rights, which are subject to different limitations:

- **Create users**

  The local administrator can create new users. This right includes the capability of importing users through synchronizing functions.

- **Edit users**

  Local administrators who do not have the right to edit users can modify system roles but not any other user settings. In particular, local administrators cannot edit group memberships.

- **Delete users**

  The local administrator can delete users.

- **Copy users**

  The copy function allows the local administrator to create a new user who has the same system roles and group memberships as a user who is already a member of the area.

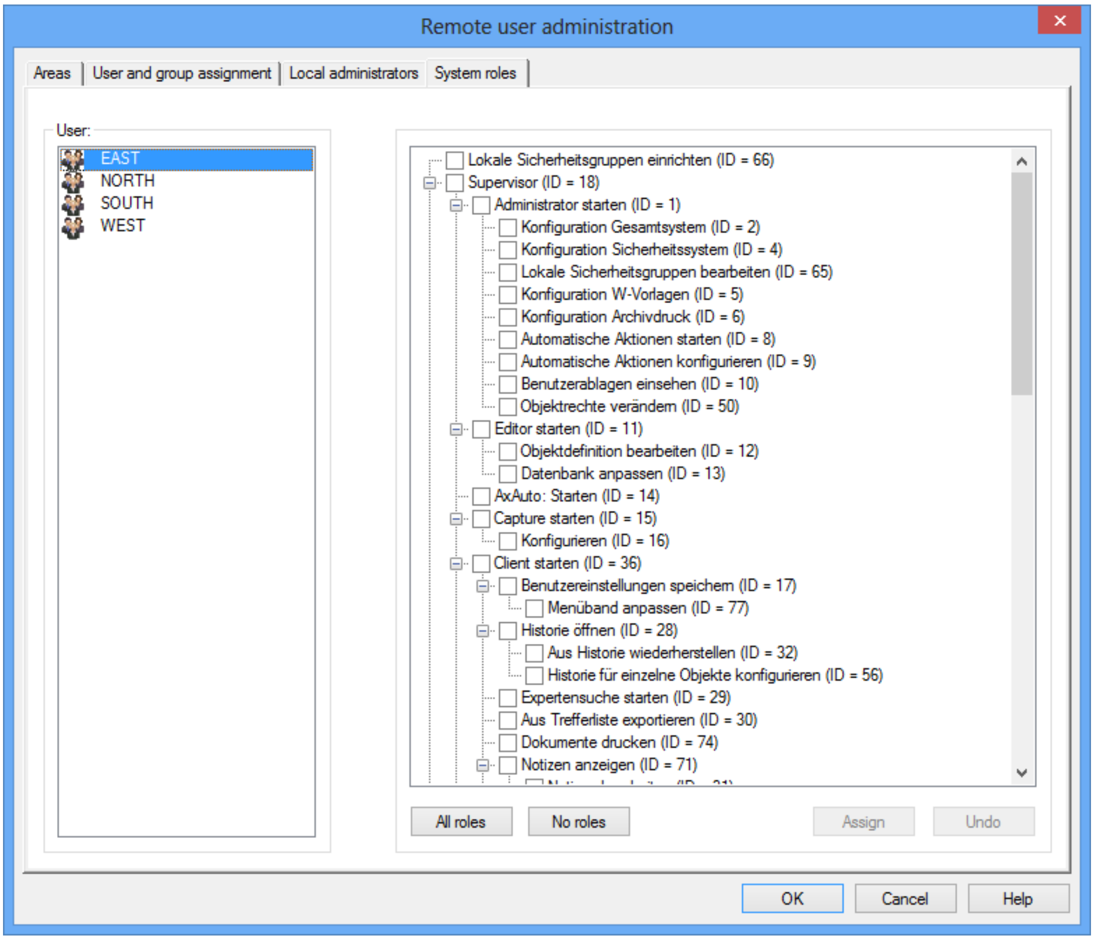
If there are users in an area with system roles other than those which the local administrator is allowed to assign, the local administrator can use the copy function to create users with such system roles, regardless of the locally configured system role assignment.

Once you have selected all necessary rights, you must **Assign** them and then save the settings with **OK**.

Local System Role Assignment

In his area, the local administrator can only assign those rights to users which have been marked on the **System roles** tab in the remote user administration. The same applies to the revocation of rights.

Selected system roles are automatically assigned to every new user in the area.



User:

- EAST
- NORTH
- SOUTH
- WEST

- □ Lokale Sicherheitsgruppen einrichten (ID = 66)
- □ Supervisor (ID = 18)
  - □ Administrator starten (ID = 1)
    - □ Konfiguration Gesamtsystem (ID = 2)
    - □ Konfiguration Sicherheitssystem (ID = 4)
    - □ Lokale Sicherheitsgruppen bearbeiten (ID = 65)
    - □ Konfiguration W-Vorlagen (ID = 5)
    - □ Konfiguration Archivdruck (ID = 6)
    - □ Automatische Aktionen starten (ID = 8)
    - □ Automatische Aktionen konfigurieren (ID = 9)
    - □ Benutzerablagen einsehen (ID = 10)
    - □ Objektrechte verändern (ID = 50)
  - □ Editor starten (ID = 11)
    - □ Objektdefinition bearbeiten (ID = 12)
    - □ Datenbank anpassen (ID = 13)
  - □ AxAuto: Starten (ID = 14)
  - □ Capture starten (ID = 15)
    - □ Konfigurieren (ID = 16)
  - □ Client starten (ID = 36)
    - □ Benutzereinstellungen speichern (ID = 17)
      - □ Menüband anpassen (ID = 77)
    - □ Historie öffnen (ID = 28)
      - □ Aus Historie wiederherstellen (ID = 32)
      - □ Historie für einzelne Objekte konfigurieren (ID = 56)
    - □ Expertensuche starten (ID = 29)
    - □ Aus Trefferliste exportieren (ID = 30)
    - □ Dokumente drucken (ID = 74)
    - □ Notizen anzeigen (ID = 71)

Choose the area on the left and mark all those system roles on the right that the local administrator will be allowed to assign and revoke.

Once you have marked all necessary system roles, you must **Assign** them and then save the settings with **OK**.

Setting Up Groups

The security system that controls access to archive objects is a group-oriented system. Access rights are distributed to users due to their membership in one or more groups.

Every new user is initially a member of the **Standard** group. It is possible to remove a user from the **Standard** group, but the group cannot be deleted.

You can set up groups or transfer existing Windows NT groups into the system.

Within a local area, one group is always set as the standard group in the remote user administration dialog.

Create User Groups

Follow these steps to create a group:

1. Open the **Security system** window.
2. Click on the **User groups (access rights)** tab.
3. Click the **New** button in the **Select user group** area.

   The **Create new user group** dialog will open.
4. Enter a name (using a maximum of 255 characters) and a description for the new group.

   A description is optional.

   You can apply the assignment of objects, including object rights, clauses, and users from the currently selected user group.
5. Confirm with **OK**.

The new group is set up. You can define the group rights (see 'Setting ').

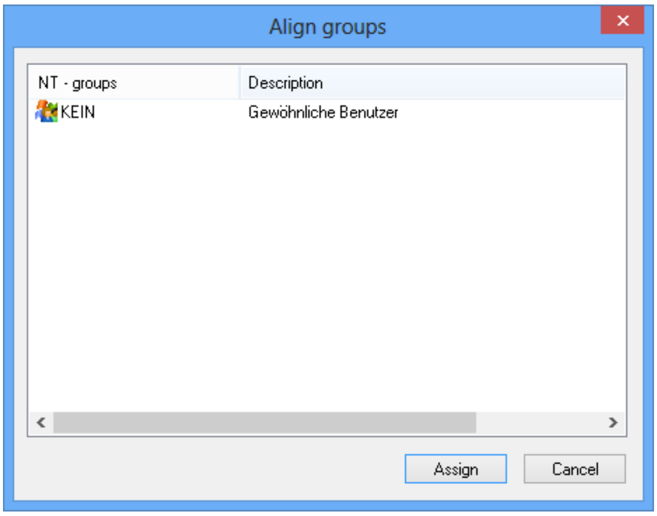
> Within a remote area, local administrators who have no additional rights cannot grant or revoke access rights.

Applying NT Group

Follow these steps to import NT user groups into the enaio® security system:

1. Open the **Security system** window.
2. Click on the **User groups (access rights)** tab.
3. Click the **Synchronize...** button in the **Select user group** area.

   The **Synchronize groups** window will open.



4. Select one or several groups and click the **Assign** button.

The NT groups will be imported. You can define the group rights (see 'Setting ') and enter group members (see 'Assigning Users to Groups').

Only groups of the Primary Domain Controller (PDC) will be shown.

Deleting Groups

All newly created users are initially members of the **Standard** group. You cannot delete the **Standard** group.

Follow these steps to delete a group:

1. Open the **Security system** window.
2. Click on the **User groups (access rights)** tab.
3. Select a user group from the **User group** list.
4. Click on the **Delete** button.

The user group will be deleted. If the selected group has users set up, you will get an error message telling you that the members firstly need to be deleted from the group (see 'Deleting Users'). The group members will also be listed.

Setting Group Access Rights

You define the group rights in the **Security system** window on the **User groups** (access rights) tab. Among others, this tab lists all object types that have been configured in enaio® editor for the archive system. You assign archive object types to the selected group and define the access rights to these archive object types.

Access rights to archive objects can be assigned as follows:

- Show index data (R)
- Write index data (W)
- Delete object (D)

- Output object (X)
  (open, print, export)
- Write object (U)
  (create and modify)

Each of the access rights can also be made dependent on a clause.

In order to delete archived documents, a user requires the system role 'Client: Delete archived documents'. In enaio® enterprise-manager, you can decide whether to not only remove archived documents from the trash can, but also delete them physically from storage media.

To print documents, users require the system role 'Client: Print documents'.

Folder Access Rights

If a user does not have the right 'Show index data' to access folders, the respective search form will not be shown in the archive area. Search forms which are used to retrieve registers and document types contained in folders will not be displayed either. Thus, users cannot retrieve any content of none of the folders.

The folder access right 'Write index data' includes the right to create new folders.

The user needs the folder access right 'Output object' in order to open folders.

Users with the access right 'Delete object' can only delete folders if they additionally have the right to delete all registers and documents within the folder.

The right 'Write object' to access folders does not have any function.

Register Access Rights

If a user does not have the right 'Show index data' to access registers, the respective search form will not be shown in the archive area.

The register access right 'Write index data' includes the right to create new registers.

The user needs the register access right 'Output object' in order to open registers.

A user who wants to open a register through a link, such as a notes window, additionally needs the right 'Output object' to access the folder and the register in which the register to be opened is located.

Users with the access right 'Delete object' can only delete registers if they additionally have the right to delete all registers and documents within the register.

The right 'Write object' to registers does not have any function.

Document Access Rights

If a user does not have the right 'Show index data' to access documents, the respective search form will not be shown in the archive area.

The document access right 'Write index data' includes the right to create new documents without pages. To create a document with pages, the 'Write object' access right is also required.

A user who wants to open a document through a link, such as a notes window, additionally needs the right 'Output object' to access the folder and the register in which the document to be opened is located.

The rights for 'Group annotations' and 'Public annotations' are only relevant for image documents.

Annotation Rights

Users with the right 'Group annotations' are allowed to create, hide, edit, and delete static group layers for documents of the indicated type. If they furthermore have the system role 'Client: Edit static layers of other users', they are allowed to hide, edit and delete all static group layers.

Users with the right 'Group annotations' can create dynamic group layers, but every user can hide, modify, and delete these layers.

The same applies to public layers. Users with the right 'Public annotations' are allowed to create, hide, edit, and delete static public layers for documents of the indicated type. If they furthermore have the system role 'Client: Edit static layers of other users', they are allowed to hide, edit and delete all static group layers.

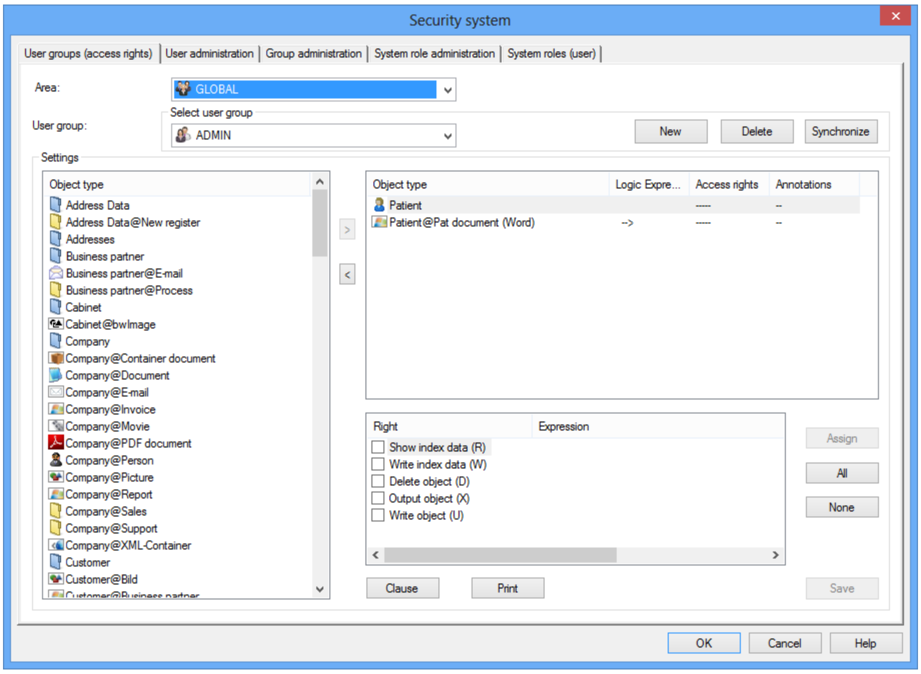
Users with the right 'Public annotations' can create public layers, but every user can hide, modify and delete these layers.

> If users without annotation rights import documents into enaio® client, layers will be burned into indelibly. Users with the right to edit these documents (Write object) will only edit the documents with burned in layers. On check-in, these files will be saved with burned in layers. Burned into layers cannot be removed from the document.
>
> Layers cannot be burned into PDF documents.

Archive Object Type Access Rights

Follow these work items to assign access rights for groups to archive object types.

1. Open the **Security system** window.
2. Click on the **User groups (access rights)** tab.


Security system
User groups (access rights) | User administration | Group administration | System role administration | System roles (user)
New
Delete
Synchronize
Settings
>
<
Assign
All
None
Clause
Print
Save
OK
Cancel
Help

Area: GLOBAL

User group: Select user group ADMIN

Object type
- Address Data
- Address Data@New register
- Addresses
- Business partner
- Business partner@E-mail
- Business partner@Process
- Cabinet
- Cabinet@bwImage
- Company
- Company@Container document
- Company@Document
- Company@E-mail
- Company@Invoice
- Company@Movie
- Company@PDF document
- Company@Person
- Company@Picture
- Company@Report
- Company@Sales
- Company@Support
- Company@XML-Container
- Customer
- Customer@Bild
- Customer@Business partner

Object type	Logic Expre...	Access rights	Annotations
Patient		-----	--
Patient@Pat document (Word)	-->	-----	--

Right	Expression
□ Show index data (R)	
□ Write index data (W)	
□ Delete object (D)	
□ Output object (X)	
□ Write object (U)	

3. Select a user group from the **User group** list.
4. Select the object types on the left to which the group must have access. Use the arrow buttons to move the object types to the right-hand window.
5. Select object types in the right-hand window.
6. Activate the check boxes to select the rights you want to assign.

   Use the **All** button to select all rights and the **None** button to remove all selections.
7. Click the **Assign** button. A summary of the new access rights will be displayed on the right.
8. Click the **OK** button. The rights will be saved.

You can also make the rights dependent on clauses (see 'Clauses for Access Rights').

You can print out the access rights of user groups using the **Print** button. The `Grouplist.xsl` style sheet is used for the printout. You can find this style sheet in the directory`\clients\admin`. You can edit the design.

> Within a remote area, local administrators who have no additional rights cannot grant or revoke group-specific access rights.

Clauses for Access Rights

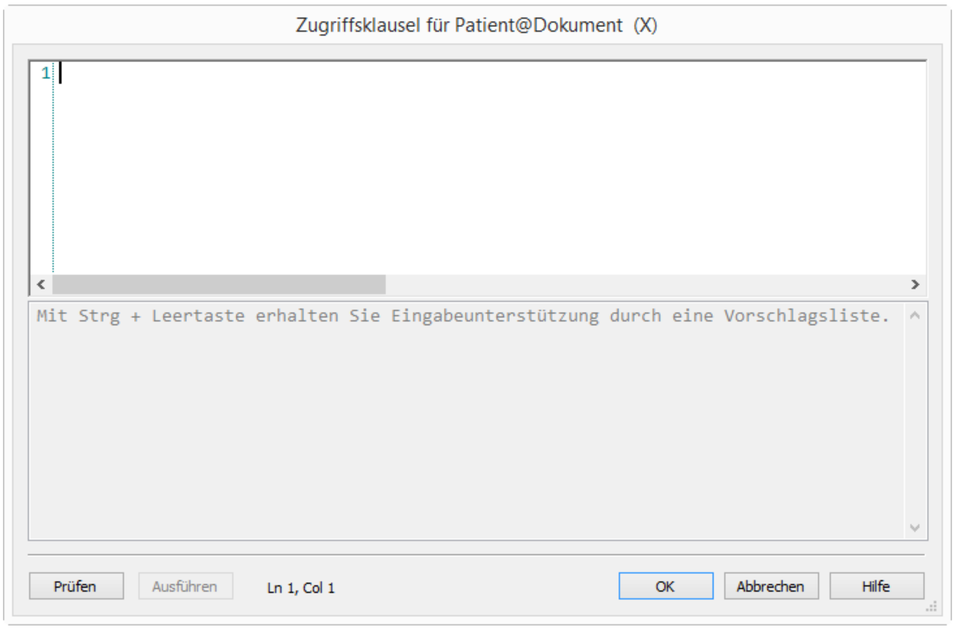
Access rights can be made to depend on logical expressions. A granted right will only be provided when the condition is fulfilled.

Follow these work items to create clauses:

1. Open the **Security system** window.

2. Click on the **User groups (access rights)** tab.
3. Select a user group from the **User group** list, select an object type in the right-hand window and a right to assign in the bottom window.
4. Click the **Clauses** button.

   The editor will open.



Zugriffsklausel für Patient@Dokument (X)

Mit Strg + Leertaste erhalten Sie Eingabeunterstützung durch eine Vorschlagsliste.

5. Create the clause in the editor.

   With **Ctrl+space key** you get input support from a suggestion list.

   Entries can be selected, copied, inserted, and deleted via context menu.
6. Check the clause.

   The check shows the corresponding SQL statement with the current values of variables.

   When you click **Run**, the SQL statement is run. The number of hits will be shown. Meaningfulness depends on the data pool and the current values of variables.
7. Confirm with **OK**.

The clause is shown on the **User group** tab. Save changes to the security system using the **Save** button.

> Logic expressions for access rights can have the effect, for example, that after having changed an object's index data, a user loses his rights to the just modified object and does not find it again after updating the view.

Clause Syntax

A clause consists of a field, an operator, and a constant or variable value. Several clauses can be logically combined and combinations can be structured with brackets.

Fields

The index data fields of an object and basic parameters are available as fields. The editor offers all the object's fields in the suggestion list (**Ctrl+Space**).

Marking:

§ Field names with square brackets ([To:]).

§ Internal names with curly brackets ({MAIL_TO}).

§ Database names without brackets (field1).

§ Basic parameters with 'sys' prefix (sys'creator').

The following basic parameters can be used:

sys'created'	Date of creation
sys'creator'	User who created the object
sys'archiver'	Archivist
sys'archived'	Archive date
sys'flags'	Archiving status
sys'mimetypid'	Mime type ID
sys'modifytime'	Last modification date and time
sys'modifyuser'	User who last modified the object
sys'retention'	Retention time
sys'retention_planned'	Planned retention period
sys'systemid'	ID of the object

Operators

The following operators can be used:

=	equal
!=	unequal
<<New configuration name>>	large
<	less than
>=	greater than or equal
<=	less than or equal
in not in	contained in not contained in

between	within an area
not between	not within an area

a clause in field, operator, and value can also have the prefix 'not.'

Constants

Constants are dependent on the database field type.

Character fields

Type: 'All characters,' 'letters,' 'capital letters,' 'numerals (alphanumeric),' 'patient type,' 'page,' 'gender,' 'questions.'

Constants for character fields are enclosed in single quotes. They may contain placeholders.

The placeholder '*' represents one character exactly, the placeholder '?' for any number of characters. Placeholders can be inside, as well as at the beginning and at the end.

> Placeholders can only be used for the operators 'equal' and 'unequal.'

If constants are meant to contain the characters '*' or '?', they must be masked with '\'. Single quotes and the escape character '\' must also be masked.

Values for the 'in' operator are listed in brackets:

```
field1 in ('a,' 'b,' 'c')
```

The area for the 'between' operator is specified thus:

```
field1 between 'a' and 'c'
```

Date/Time fields

Type: 'date,' 'date/time,' and 'time.'

Constants for date fields have the prefix `date`. The date is enclosed in single quotes. Notation: `YYYY-MM-DD`

Example: `date1 = date'2016-09-30'`

Constants for date/time fields have the `datetime` prefix. The value is enclosed in single quotes: Notation: `YYYY-MM-DD HH-MM-SS`

Example: `zahl1 = datetime'2016-09-30 11:31:55'`

Constants for date/time fields have the `datetime` prefix. The value is enclosed in single quotes: Notation: `HH-MM-SS`

Example: `number1 = time'11:31:55'`

The last elements can be omitted successively so that the clause refers to values independently of these elements.

Example: `number1 = datetime'2016'`

Decimal/Numeric fields

Type: 'Decimal' and 'numerals (numeric)'

Constants for decimal field and numeric fields are not enclosed in brackets.

Examples:

```
number1 >= 400
```

```
number1 between 300 and 400
```

```
real1 in (1.2,2.3,3.4)
```

Variables

The following variables can be used.:

#DATE#	current date
#DATETIME#	Current date and time
#TIME#	current time
#USER#	Name of the logged-on user
#COMPUTERNAME#	Name of the logged-on computer
#COMPUTERGUID#	GUID of the logged-on computer
#COMPUTERIP#	IP of the logged-on computer
#GROUPS#	Groups of which the logged-on user is a member. Operator is always 'in' or 'not in.'
#RIGHTGROUP#	Right groups or user name of the logged-on user. The specified field must be indexed via the right group add-on. Operator is always 'in' or 'not in.'

Date information can be subtracted (-) or added (+) to #DATE# and #DATETIME#. Information for years, months, weeks, and days is optional.

Example: `number1 = #datetime#-1y2m3w4d`

1 year, 2 months, 3 weeks, and 4 days are subtracted from the current datetime.

Example: `number1 = #DATETIME#+2m4d`

Two months and 4 days are added to the current datetime.

Empty fields

Clauses to empty fields are formulated thus:

```
field1 is zero
```

```
field1 is not zero
```

The clause is independent of whether zero values are allowed in the database.

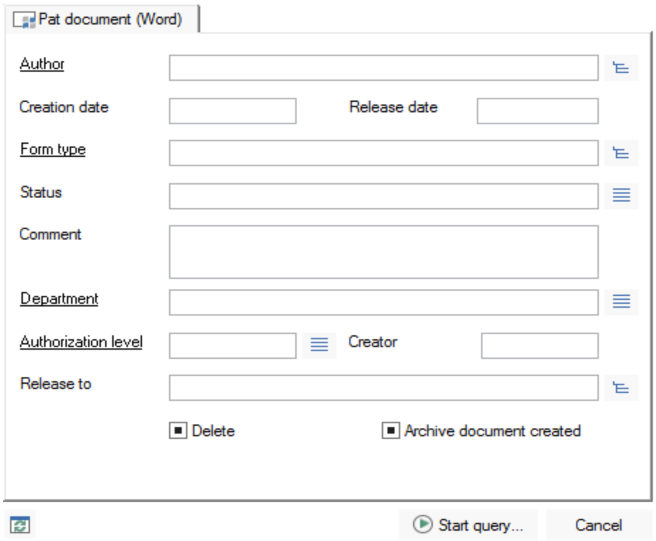
Owner

A simple clause can be used to assign access only to the user, the owner of the object is:

```
isowner
```

Example of Expressions

In the following example, the right is only assigned to the current user if the user is either the creator or if the creator has entered the current user’s name into the 'Share with' index field, given that the date indicated in the 'Sharing date' field has already been reached or expired.



The data sheet contains the fields 'Creator,' 'Document sharing date,' and 'Share with.' These fields are used in the logic expression.

Use the expression editor to create the logic expression. It reads as follows:

```
[Creator] = #USER# or ([share with] = #USER# and [Sharing date] <=
#DATE#)
```

The check shows the clause with the current values of the variables `#USER#` and `#DATE#`.

Clauses in Previous Versions

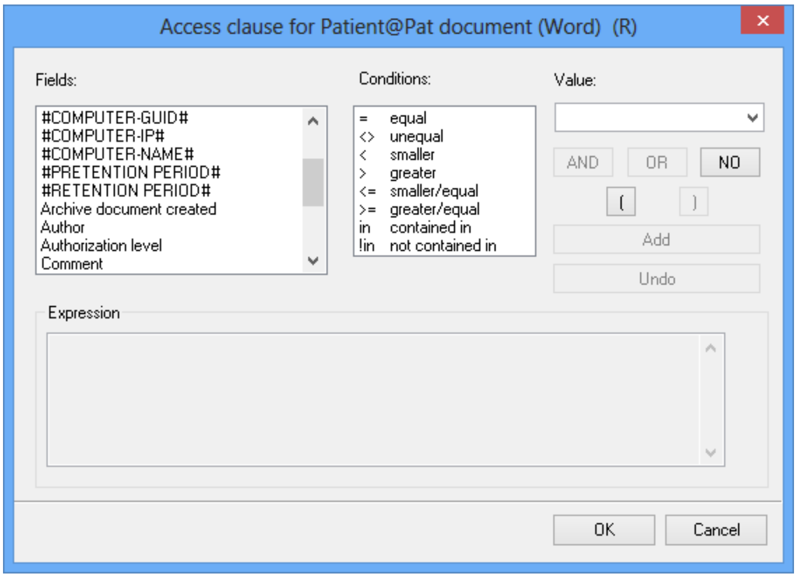
Up to version 8.10, clauses were created with a clause editor. Existing clauses in these versions can still be used, edited, and recreated in the old format. Once converted to the current format, the clause editor is no longer available.

Follow these work items to create an expression with the clause editor in the version up to 8.10:

1. Open the **Security system** window.
2. Click on the **User groups (access rights)** tab.

3. Select a user group from the **User group** list, select an object type in the right-hand window and a right to assign in the bottom window.
4. Click the **Clauses** button.

   The expression editor will open.



The **Fields** area will list the index data fields of the selected object type. Select the field for which you want to create a logical expression.

The following values will also be listed:

- `#Computer-IP#` – the IP address of the user's computer,
- `#Computer-GUID#` – the GUID of the user's computer,
- `#Computer-Name#` – the name of the user's computer.

For documents, the following basic parameters are available:

- `#Creation date#`, `#Creator#`, `#Archivist#`, `#Archiving date#`, `#Owner#`, `#Retention time#`, `#PRetention time#`.

5. The **Links** area will list all available operators. Select an operator.
6. Enter a value for the selected field into the **Value** area.

   '*' can be used as a placeholder for any string of characters and '?' can be used as a placeholder for any single character.

   The following variables can additionally be used:

- `#User#` – the current user name,
- `#Date#` – the current date,
- `#Zero#` – no entry in the field,
- `#Groups#` – the groups of which the user is a member. Use the operators 'in' and '!in'.
- `#Computer-IP#` – the IP address of the user's computer,
- `#Computer-GUID#` – the GUID of the user's computer,

- `#Computer-Name#` – the name of the user's computer.
- `#Right group#` – groups and users who are entered into the field via the 'Right group' add-on. Use the operators 'in' and '!in'.

For documents, the following basic parameters are available:

- `#Creation date#`, `#Creator#`, `#Archivist#`, and `#Archiving date#`.
- Planned retention period `#PRetention period#` and retention period `#Retention period#` are additionally available.

7. Then click on the **Add** button.

   By combining the field, the operator and the value, you have thus formed an expression. This expression can furthermore be logically combined with other expressions. The entire expression is shown in the field below. You cannot edit the entries in the **Clause** field. If you want to delete or correct entries, press the **Undo** button.

8. Confirm with **OK**.

The clause is shown on the **User group** tab. Save changes to the security system using the **Save** button.

Access to User Lists

In some contexts, users have the possibility to open a list of all users. For example, in search forms of portfolios and basic parameters, in configuration dialogs of view filters, in configuration dialogs of subscriptions and follow-ups, and in other contexts.

Such access is not always desirable or required, hence you can reduce the list to those users who are members of at least one of the groups in which the user who opens the list is a member.

To do so, you need the following entry in the `\etc\as.cfg` file of the data directory:

```
[CLIENT]

HideOthers=1
```

You can add another line to the section in order that other individual users are included even if they do not share group membership with the current user:

```
Exclude=User1;User2
```

Change the value of 'HideOthers' to '0', to turn off this function.

> Users who are members of the 'Standard' group will always see all users in user lists. Similarly, users who are members of the standard group in an area of the remote user administration will see all other members of the area.
> Users with the system role 'Client: Show system trash can' always see all users in the trash can user list.

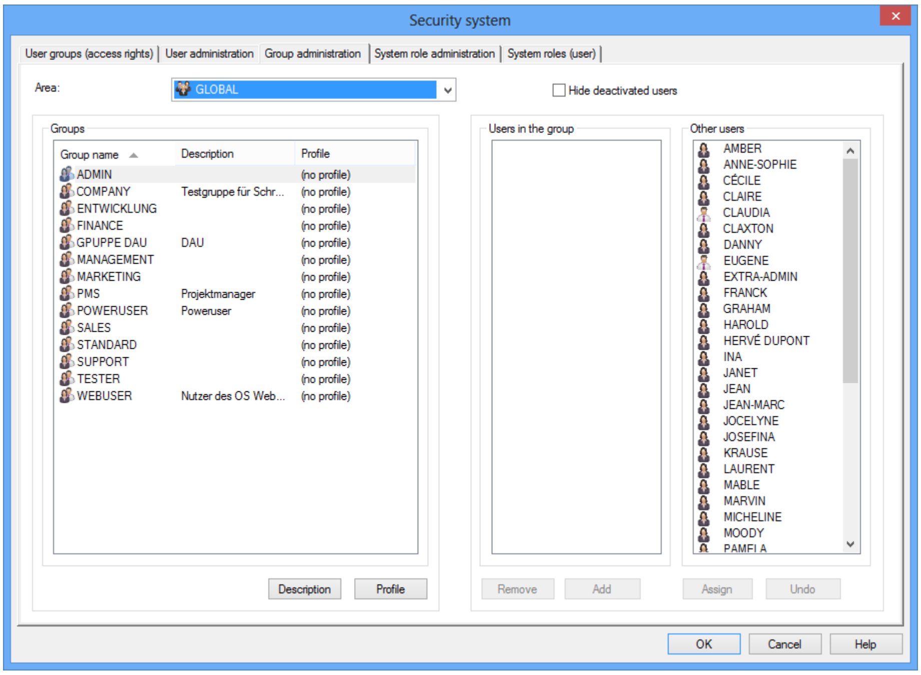
Assigning Users to Groups

You can assign users to several groups. The user is always given the most far-reaching access rights from all assigned groups.

Functions of local administrators within an area can be limited significantly.

Follow these steps to assign users to groups:

1. Open the **Security system** window.
2. Click on the **Group administration** tab.



Area: GLOBAL

□ Hide deactivated users

Group name	Description	Profile
ADMIN		(no profile)
COMPANY	Testgruppe für Schr...	(no profile)
ENTWICKLUNG		(no profile)
FINANCE		(no profile)
GPUPPE DAU	DAU	(no profile)
MANAGEMENT		(no profile)
MARKETING		(no profile)
PMS	Projektmanager	(no profile)
POWERUSER	Poweruser	(no profile)
SALES		(no profile)
STANDARD		(no profile)
SUPPORT		(no profile)
TESTER		(no profile)
WEBUSER	Nutzer des OS Web...	(no profile)

Other users:
AMBER
ANNE-SOPHIE
CÉCILE
CLAIRE
CLAUDIA
CLAXTON
DANNY
EUGENE
EXTRA-ADMIN
FRANCK
GRAHAM
HAROLD
HERVÉ DUPONT
INA
JANET
JEAN
JEAN-MARC
JOCELYNE
JOSEFINA
KRAUSE
LAURENT
MABLE
MARVIN
MICHELINE
MOODY
PAMELA

3. All groups are listed in the **Groups** area. If you select a group, all users in the **Users in the group** area are shown.
4. You can choose not to display deactivated users.
5. Select a user from the group and double-click or press the **Remove** button to remove it from the group. The user will be listed in the **Other users** area.
6. Select a user from the **Other users** list and double-click or press the **Add** button to enter it into the currently selected group. The user will be listed in the **Users in the group** area.
7. Click the **Assign** button to save the changes.
8. Click the **Undo** button to undo all changes.

The group's access rights to archive objects are configured on the **User groups** tab.

Users which have been configured as profiles are not shown here.

Exporting and Importing Group Settings

You can export and import the settings of group administration, for example to transport changes to the rights system, which you have created on a test system, to the production system. The settings are saved in an XML file during export.

The following changes can be transported:

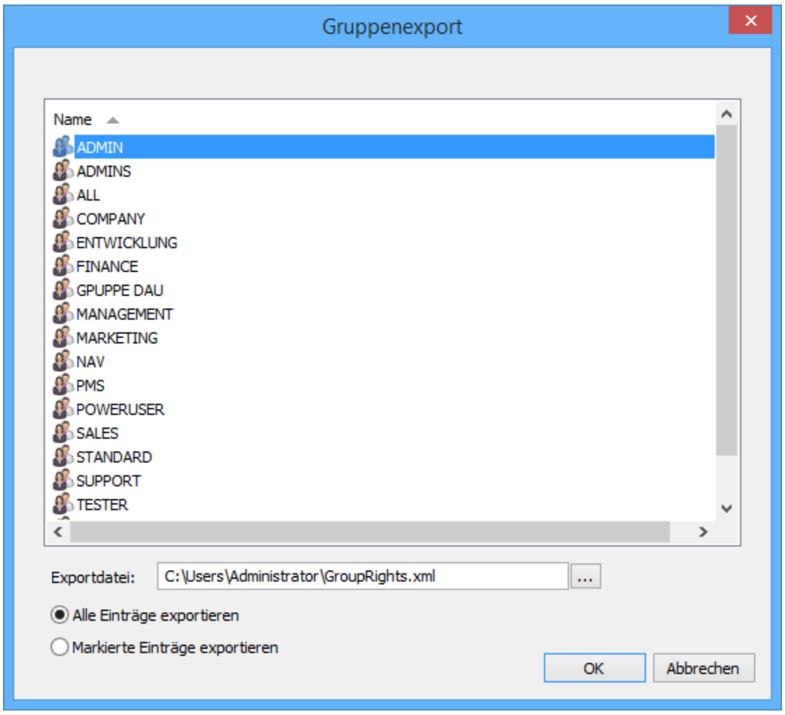
- New groups (identified by name)
- Assignments of rights to groups
- New, deleted, and amended clauses

The following changes are not transported:

- Deleted and amended groups
- User
- Assignments of users to roles, groups, and rights.

Follow these work items to export group settings:

1. Open the **Security system** window.
2. Click on the **Group administration** tab.
3. Click the **Export** button and



Name

ADMIN
ADMINS
ALL
COMPANY
ENTWICKLUNG
FINANCE
GPUPPE DAU
MANAGEMENT
MARKETING
NAV
PMS
POWERUSER
SALES
STANDARD
SUPPORT
TESTER

Exportdatei: C:\Users\Administrator\GroupRights.xml

● Alle Einträge exportieren

○ Markierte Einträge exportieren

select **Export all entries** if you want to export all settings or

select **Export selected entries** if you want to select and export specific entries.

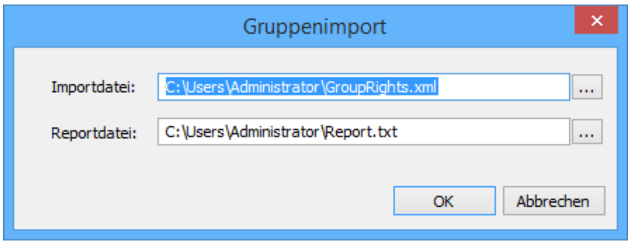
4. Select a name and a location in the file system for the export file. The default path is 'C:\Users\Administrator\GroupRights.xml'.
5. Click **OK**.

The group settings are exported and stored.

Follow these work items to import group settings:

Export and back up the settings of a production system before you import new settings. You cannot reverse settings once they have been imported!

1. Open the **Security system** window.
2. Click on the **Group administration** tab.
3. Click the **Import** button.



Gruppenimport

Importdatei: C:\Users\Administrator\GroupRights.xml

Reportdatei: C:\Users\Administrator\Report.txt

4. Select an existing import file from the file system.
5. Select a location for a report file. The changes installed are logged in the report file.
6. Click **OK**.

   The group settings are imported.

Set Up Users

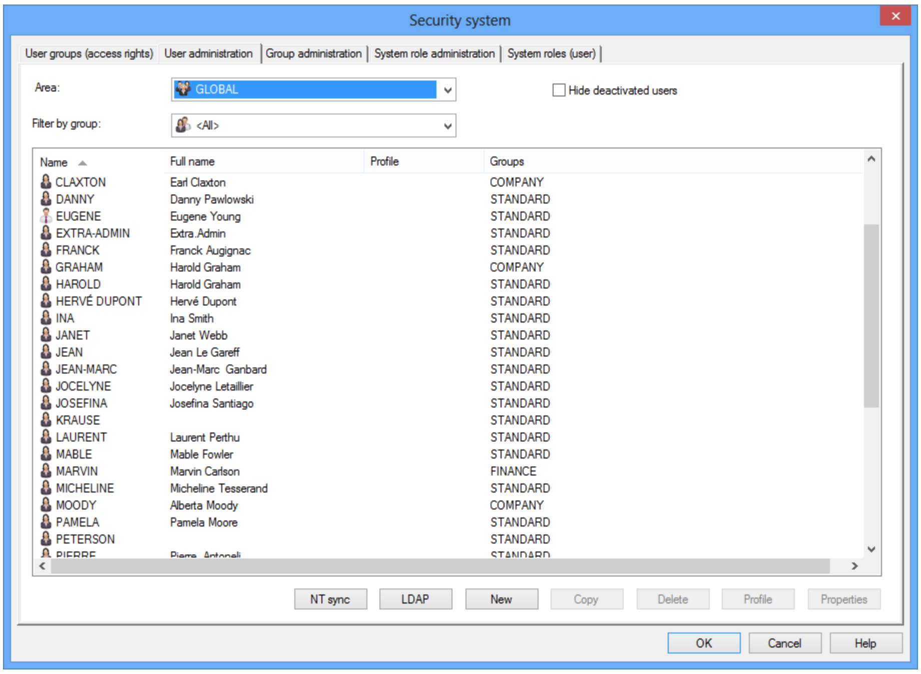
During the installation of enaio®, a user with the user name 'root' and the password 'optimal' will be created. This user has the system role 'DMS: Supervisor'. You must delete this user account instantly on first login to enaio® administrator, or at least change the password, and create a new supervisor.

There must always be at least one user with the system role 'DMS: Supervisor'.

Users with the system role 'DMS: Supervisor' are flagged with a special icon:

Follow these work items to set up users:

1. Open the **Security system** window.
2. Click on the **User administration** tab.



Area: GLOBAL

□ Hide deactivated users

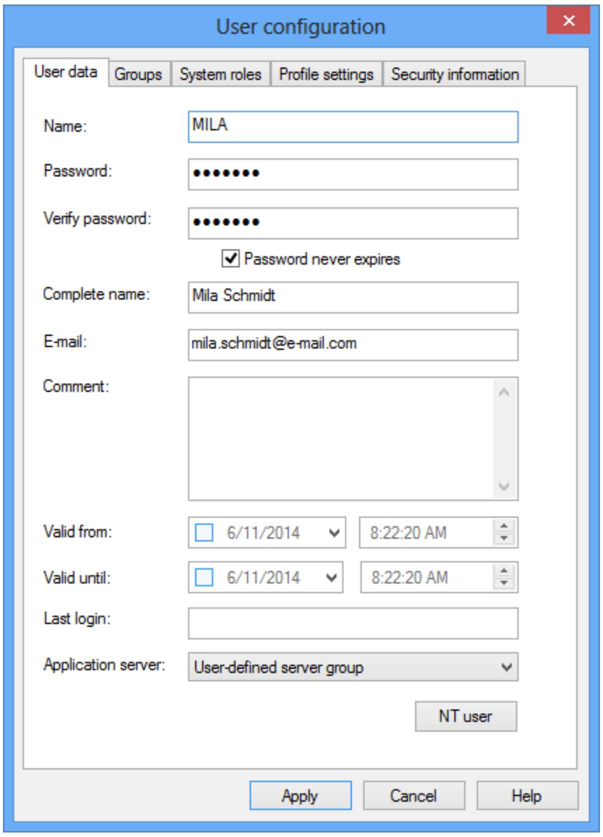
Filter by group: <All>

Name	Full name	Profile	Groups
CLAXTON	Earl Claxton		COMPANY
DANNY	Danny Pawlowski		STANDARD
EUGENE	Eugene Young		STANDARD
EXTRA-ADMIN	Extra.Admin		STANDARD
FRANCK	Franck Augignac		STANDARD
GRAHAM	Harold Graham		COMPANY
HAROLD	Harold Graham		STANDARD
HERVÉ DUPONT	Hervé Dupont		STANDARD
INA	Ina Smith		STANDARD
JANET	Janet Webb		STANDARD
JEAN	Jean Le Gareff		STANDARD
JEAN-MARC	Jean-Marc Ganbard		STANDARD
JOCELYNE	Jocelyne Letaillier		STANDARD
JOSEFINA	Josefina Santiago		STANDARD
KRAUSE			STANDARD
LAURENT	Laurent Perthu		STANDARD
MABLE	Mable Fowler		STANDARD
MARVIN	Marvin Carlson		FINANCE
MICHELINE	Micheline Tesserand		STANDARD
MOODY	Alberta Moody		COMPANY
PAMELA	Pamela Moore		STANDARD
PETERSON			STANDARD
PIERRE	Pierre Antoneli		STANDARD

All existing users will be listed.

You can filter users by groups and hide users whose accounts are disabled.

3. Click on the **New** button.
4. The **User configuration** window will open.
5. Set up a new user on the **User data** tab.



Name: MILA

Password: •••••••

Verify password: •••••••

☑ Password never expires

Complete name: Mila Schmidt

E-mail: mila.schmidt@e-mail.com

Comment:

Valid from: □ 6/11/2014 8:22:20 AM

Valid until: □ 6/11/2014 8:22:20 AM

Last login:

Application server: User-defined server group

6. Enter a user name with a maximum of 255 characters in the **Name** field.

   The special character '@' as part of a user name leads to login errors. To avoid errors, the 'Database can check whether the '@' character is contained in a user name.

   You can transfer individual NT users. Click on the **NT user** button and select a user from the list. Click the **Apply** button to transfer the selected user name to the **Name** field.

   You can transfer multiple NT users using the **NT sync** function on the **User administration** tab (see below).

7. Enter a password for the user with a maximum of 100 characters in the **Password** field. It can be changed (see 'Change password').

   In enaio® enterprise-manager, you can set rules for password syntax using regular expressions. These rules must be followed both when passwords are given administratively and when users change their passwords in enaio® client.

   A password can expire after a predefined period (see 'Login'). This function can be turned off for users.

   Use the 'Start' tab to specify whether or not to check the case sensitivity of passwords.

8. Enter the password a second time into the **Password verification** field.

9. You can decide whether or not to fill out the fields **Complete name**, **E-mail** address, and **Comments**.

   A period of validity can be entered for each user account.

10. To fill out the **Application server** field, select the OS server to which the user usually logs on. Independent of the here set entry, every user can log on to every server of the server group.

11. Click the **Apply** button.

The new user will be entered into the user list. He will automatically become a member of the 'Standard' group, have the standard system role 'Client: Save own settings' but not any profile assigned.

You can edit the user properties (see 'Set User Properties').

The **Copy** button on the **User administration** tab allows you to create a user that has the same settings as an already-existent user. You just need to enter the user data. Group memberships, profile properties and system roles will be copied from the selected user.

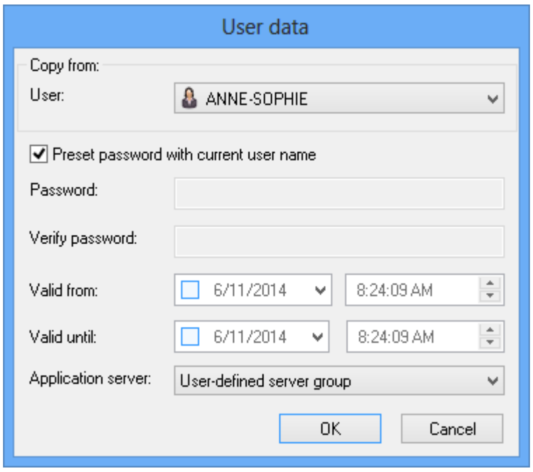
> Functions of local administrators within an area can be limited significantly.

NT Synchronization

The **NT sync** function on the **User administration** tab imports multiple NT users into user administration.

If you click the corresponding button, a list of all the users in the current domain is listed. Select the required users and click the **Assign** button.

The **User data** dialog will open.



Copy from:

User: ANNE-SOPHIE

☑ Preset password with current user name

Password:

Verify password:

Valid from: □ 6/11/2014 8:24:09 AM

Valid until: □ 6/11/2014 8:24:09 AM

Application server: User-defined server group

You can either enter a password for every selected NT user or preset the password of each user with its user name. Password verification is then unnecessary.

It is also possible to choose an OS user from the user list, from whom the user data will be copied and assigned to the selected NT users:

- group membership,
- profile assignment,
- system roles,
- account state (whether the account is open or blocked).

Confirm with **OK** to transfer users together with their data.

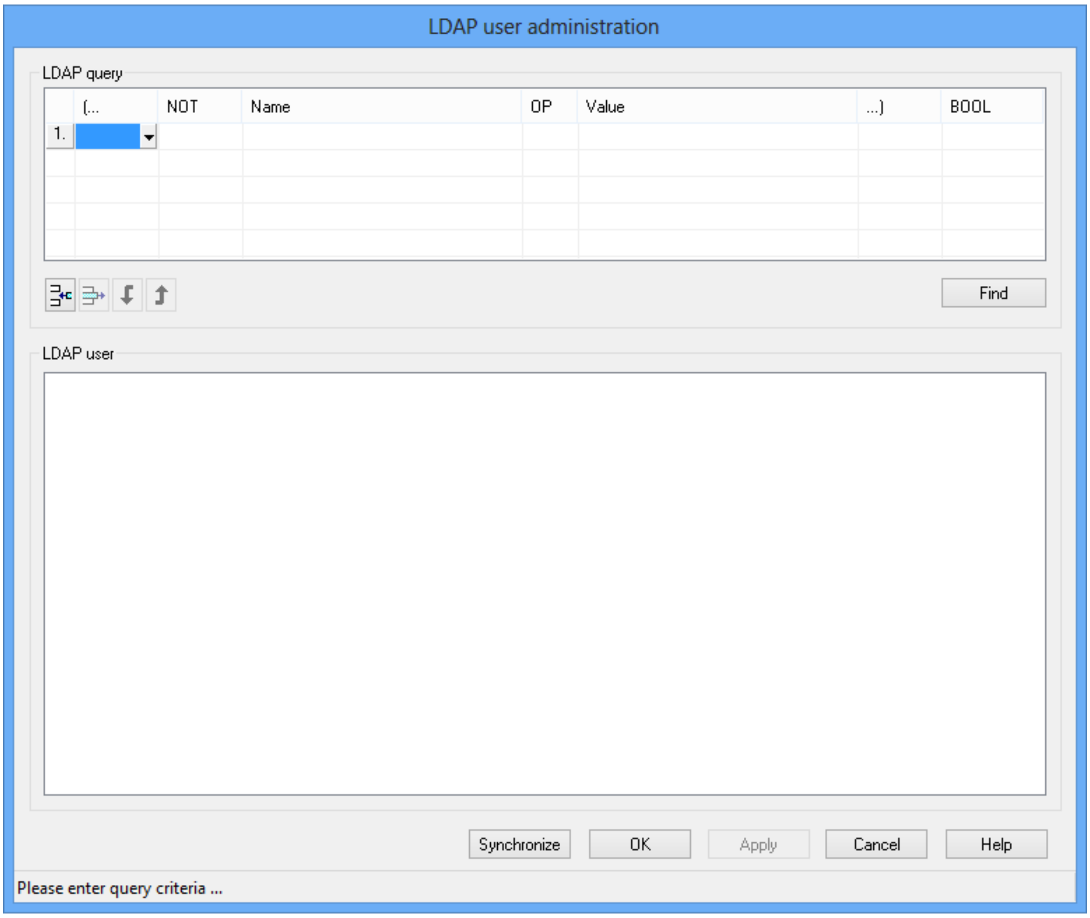
LDAP Users

For an LDAP authentication (see 'LDAP Configuration), LDAP user namestransferred to user administration.

Use an LDAP query to determine all LDAP users.

> Anonymous access to the LDAP directory service usually is not allowed; as a result, authentication at the LDAP system is required for identification of LDAP users and their rights. You must have an LDAP user with the appropriate rights. Name and password are entered on the 'LDAP Configuration.

Click the **LDAP** button on the **User administration** tab in order to open the dialog.



Please enter query criteria ...

In the **LDAP query** area, names, operators, and values are combined to form a search expression. You can combine multiple search expressions with the Boolean operators and change their logical order by adding parentheses.

The **Name** column lists the names to which you have assigned LDAP attributes (see "LDAP Configuration), while the **OP** column offers the logic operators that can be used for LDAP queries. In the **Value** column, enter a value for the search expression.

The details of the LDAP query syntax can be found in the LDAP documentation.

If you select a line by clicking the line number, the following line options will be available:

Insert an empty line below the selected one.

Delete the selected line.

Move the selected line down under the following line.

Move the selected line up above the previous one.

You start the query with the **Find** button. The search result will be an LDAP user list. The columns and the order in which they are shown are set on the **LDAP configuration** tab (see "LDAP Configuration

If you click on the **Apply** button, selected users will be cached. Even after new LDAP queries, you can pass users more than once and finally add all of them to the user administration by clicking **OK**.

Click **OK** in order to pass all selected and cached users together with associated data to the user administration.

Use the **Synchronize** button to delete all those users who have been removed from the LDAP directory service. You will be asked to confirm the deletion for each user that can no longer be found in the LDAP directory.

LDAP Version

For LDAP controlled export enaio® uses the LDAP interface provided by Microsoft operation systems.

If LDAP version 2 is used on operation systems earlier than Windows Server 2008 R2, nodes with more than 1,000 users cannot be exported completely, as the operation system does not support result paging.

Nevertheless, to fully export all users with LDAP version 2, follow these steps:

§ Add paging to the operation system.

Operation systems with Windows Server 2008 R2 or later support paging by default, and Microsoft additionally offers respective updates for earlier operation system versions.

§ When updates are not installed, running the automatic action will present you with an error message stating that a critical extension is mission.

Set the `HKEY_LOCAL_MACHINE\SOFTWARE\OPTIMAL SYSTEMS\SCHEMATA\4.0\Login\LDAP` registry key to the value '3.'

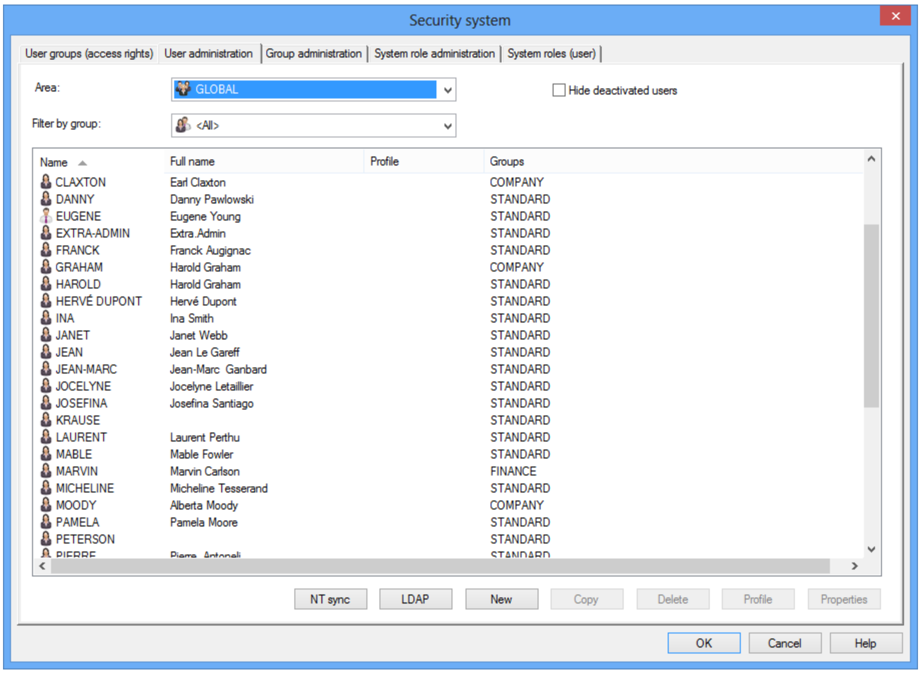
You can then completely export users regardless of the number of users per node.

Since LDAP version 3 and Windows Server 2008 R2 this adaption is not necessary.

Deleting Users

Follow these steps to delete a user:

1. Open the **Security system** window.
2. Click on the **User administration** tab.



Area: GLOBAL

☐ Hide deactivated users

Filter by group: <All>

Name	Full name	Profile	Groups
CLAXTON	Earl Claxton		COMPANY
DANNY	Danny Pawlowski		STANDARD
EUGENE	Eugene Young		STANDARD
EXTRA-ADMIN	Extra.Admin		STANDARD
FRANCK	Franck Augignac		STANDARD
GRAHAM	Harold Graham		COMPANY
HAROLD	Harold Graham		STANDARD
HERVÉ DUPONT	Hervé Dupont		STANDARD
INA	Ina Smith		STANDARD
JANET	Janet Webb		STANDARD
JEAN	Jean Le Gareff		STANDARD
JEAN-MARC	Jean-Marc Ganbard		STANDARD
JOCELYNE	Jocelyne Letaillier		STANDARD
JOSEFINA	Josefina Santiago		STANDARD
KRAUSE			STANDARD
LAURENT	Laurent Perthu		STANDARD
MABLE	Mable Fowler		STANDARD
MARVIN	Marvin Carlson		FINANCE
MICHELINE	Micheline Tesserand		STANDARD
MOODY	Alberta Moody		COMPANY
PAMELA	Pamela Moore		STANDARD
PETERSON			STANDARD
PIERRE	Pierre Antoneli		STANDARD

Using the property dialog of a user, you can view on the **User data** tab when this user was last logged in.

3. Select a user name from the user list.
4. Click on the **Delete** button.
5. A confirmation dialog will appear.

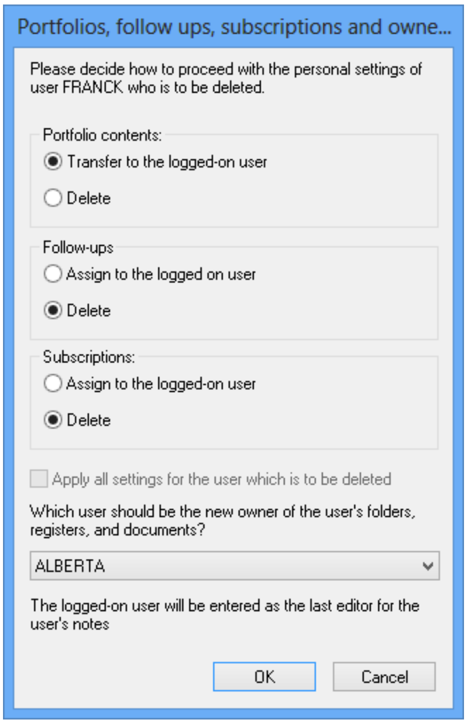
In enaio®, there must always be at least one user with the system role 'DMS: Supervisor'. Users with this system role are flagged with a special icon: .

Administrative users cannot be deleted, you must remove his administrative rights (system role) first.

You can synchronize transferred LDAP users via LDAP user administration (see 'LDAP Users').

Specify how portfolios, follow-ups, subscriptions, and owner rights of the user to be deleted will be managed in the presented dialog.

The portfolios, follow-ups and subscriptions that were set up for other users are not deleted.



Portfolios, follow ups, subscriptions and owne...

Please decide how to proceed with the personal settings of user FRANCK who is to be deleted.

Portfolio contents:

● Transfer to the logged-on user

○ Delete

Follow-ups

○ Assign to the logged on user

● Delete

Subscriptions:

○ Assign to the logged-on user

● Delete

□ Apply all settings for the user which is to be deleted

Which user should be the new owner of the user's folders, registers, and documents?

ALBERTA

The logged-on user will be entered as the last editor for the user's notes

Set User Properties

Every user is a member of one or more groups and is granted access rights to archive objects through their group memberships. Either to the individual user or by use of profile administration, users can be provided with system roles, i.e. rights to use administrative programs or access additional features in enaio® client.

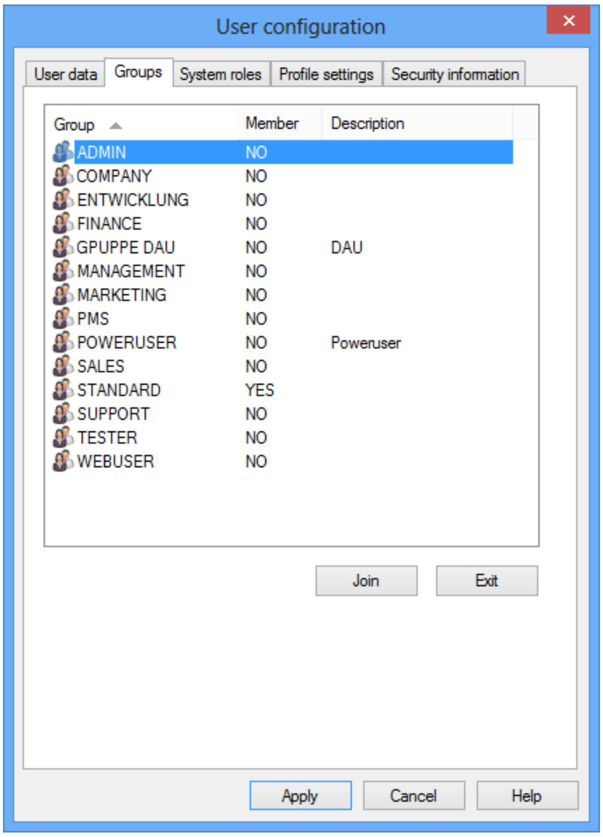
Functions of local administrators within an area can be limited significantly.

Group Membership

Follow these steps to add or remove a user from a group:

1. Open the **Security system** window.
2. Click on the **User administration** tab.
3. Select a user from the **User list** and click on the **Properties** button.

   The **User configuration** window will open.
4. Open the **Groups** register.



Group	Member	Description
ADMIN	NO	
COMPANY	NO	
ENTWICKLUNG	NO	
FINANCE	NO	
GPUPPE DAU	NO	DAU
MANAGEMENT	NO	
MARKETING	NO	
PMS	NO	
POWERUSER	NO	Poweruser
SALES	NO	
STANDARD	YES	
SUPPORT	NO	
TESTER	NO	
WEBUSER	NO	

5. Select the groups from the list into which you want to enter the selected user and click on the **Join** button.
6. Select the groups from the list from which you want to remove the selected user and click on the **Leave** button.
7. Click the **Apply** button to apply the changes.

The changes to group membership will be saved and shown on the **User administration** tab.

You can assign users to a group via the **Group administration** tab (see 'Assigning Users to Groups').

System Roles

By default, new users are only provided with the client system roles.

With the system role 'Client: Save own settings' users can perform and save the following changes within enaio® client:

- Make changes to the **Settings** tabs.
- Make changes to the archive area or to the search bar.

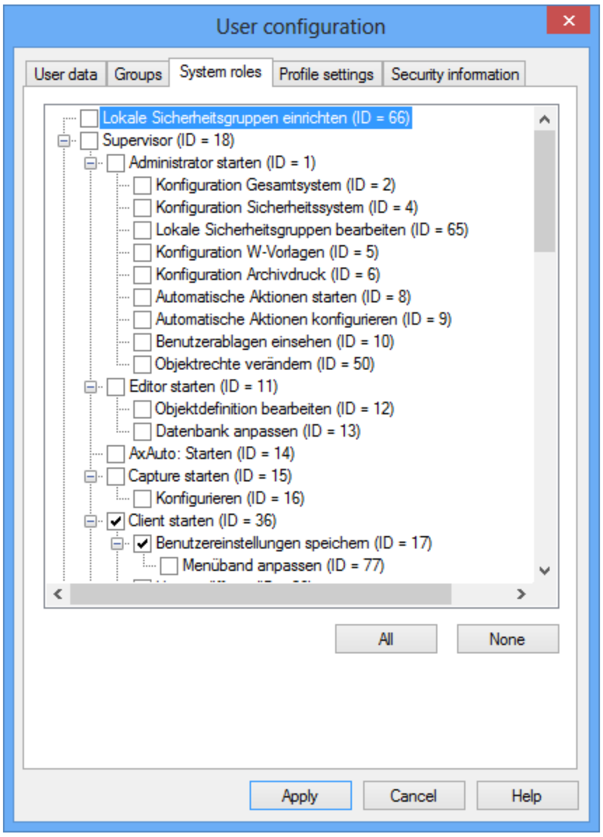
> This is a basic right which is only to be taken from users if you are the one who configures the archive area and search bars using the profile administration, thus making sure that users cannot change your configurations.

> The corresponding client system roles that users receive by default are required for the archive and search areas. Without access to the archive area, users cannot run an index data search.

Follow these steps to assign a system role to a user:

1. Open the **Security system** window.
2. Click on the **User administration** tab.
3. Select a user from the **User list** and click on the **Properties** button.

   The **User configuration** window will open.
4. Open the **System roles** register.



User configuration

User data | Groups | System roles | Profile settings | Security information

- ☐ Lokale Sicherheitsgruppen einrichten (ID = 66)
- ☐ Supervisor (ID = 18)
  - ☐ Administrator starten (ID = 1)
    - ☐ Konfiguration Gesamtsystem (ID = 2)
    - ☐ Konfiguration Sicherheitssystem (ID = 4)
    - ☐ Lokale Sicherheitsgruppen bearbeiten (ID = 65)
    - ☐ Konfiguration W-Vorlagen (ID = 5)
    - ☐ Konfiguration Archivdruck (ID = 6)
    - ☐ Automatische Aktionen starten (ID = 8)
    - ☐ Automatische Aktionen konfigurieren (ID = 9)
    - ☐ Benutzerablagen einsehen (ID = 10)
    - ☐ Objektrechte verändern (ID = 50)
  - ☐ Editor starten (ID = 11)
    - ☐ Objektdefinition bearbeiten (ID = 12)
    - ☐ Datenbank anpassen (ID = 13)
  - ☐ AxAuto: Starten (ID = 14)
  - ☐ Capture starten (ID = 15)
    - ☐ Konfigurieren (ID = 16)
  - ☑ Client starten (ID = 36)
    - ☑ Benutzereinstellungen speichern (ID = 17)
      - ☐ Menüband anpassen (ID = 77)

5. Check the system roles that you want the selected user to have.
6. Uncheck all those system roles you do not want the selected user to have.
7. Click the **Apply** button to apply the changes.

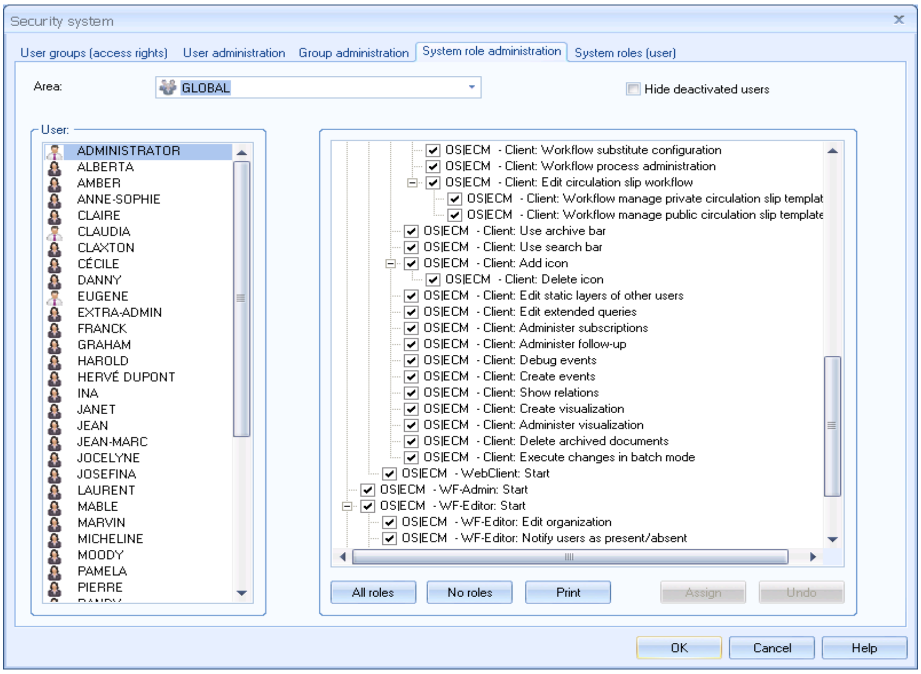
The changes to the system roles will be saved.

Users with the system role 'DMS: Supervisor' are flagged with a special icon: . There must always be at least one supervisor.

You can administer the system roles for several users more simply using the tabs **System role administration** or **System roles (user)**.

1. Open the **Security system** window.

2. Click on the **System role administration** tab.



Area: GLOBAL

☐ Hide deactivated users

User:

ADMINISTRATOR
ALBERTA
AMBER
ANNE-SOPHIE
CLAIRE
CLAUDIA
CLAXTON
CÉCILE
DANNY
EUGENE
EXTRA-ADMIN
FRANCK
GRAHAM
HAROLD
HERVÉ DUPONT
INA
JANET
JEAN
JEAN-MARC
JOCELYNE
JOSEFINA
LAURENT
MABLE
MARVIN
MICHELINE
MOODY
PAMELA
PIERRE

☑ OS|ECM - Client: Workflow substitute configuration
☑ OS|ECM - Client: Workflow process administration
☑ OS|ECM - Client: Edit circulation slip workflow
☑ OS|ECM - Client: Workflow manage private circulation slip templat
☑ OS|ECM - Client: Workflow manage public circulation slip template
☑ OS|ECM - Client: Use archive bar
☑ OS|ECM - Client: Use search bar
☑ OS|ECM - Client: Add icon
☑ OS|ECM - Client: Delete icon
☑ OS|ECM - Client: Edit static layers of other users
☑ OS|ECM - Client: Edit extended queries
☑ OS|ECM - Client: Administer subscriptions
☑ OS|ECM - Client: Administer follow-up
☑ OS|ECM - Client: Debug events
☑ OS|ECM - Client: Create events
☑ OS|ECM - Client: Show relations
☑ OS|ECM - Client: Create visualization
☑ OS|ECM - Client: Administer visualization
☑ OS|ECM - Client: Delete archived documents
☑ OS|ECM - Client: Execute changes in batch mode
☑ OS|ECM - WebClient: Start
☑ OS|ECM - WF-Admin: Start
☑ OS|ECM - WF-Editor: Start
☑ OS|ECM - WF-Editor: Edit organization
☑ OS|ECM - WF-Editor: Notify users as present/absent

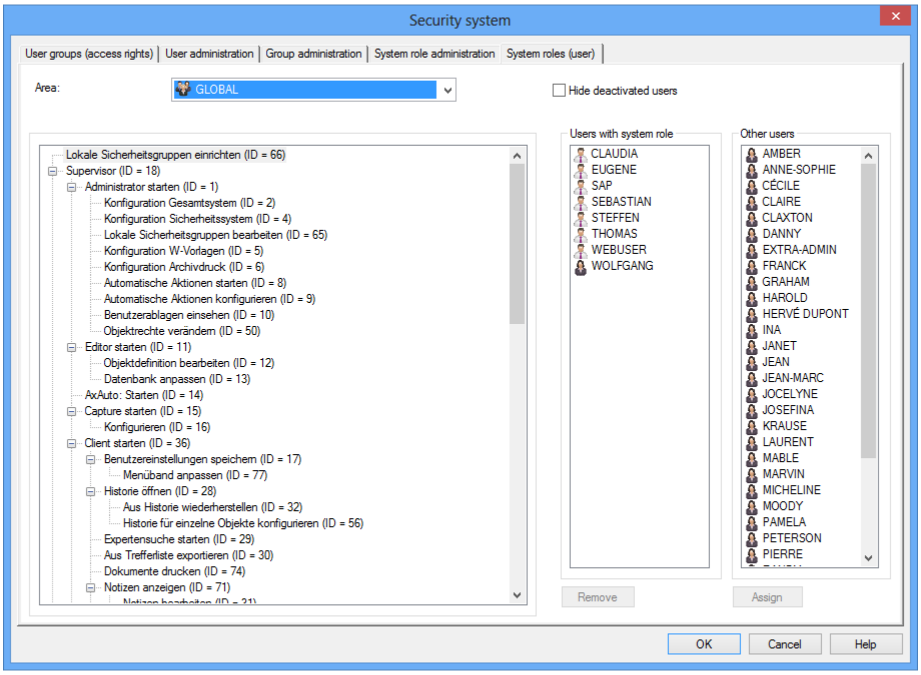
All **Users** are listed on the left and all **System roles** on the right.

3. Select a user from the list on the left.
4. Check the system roles that you want the selected user to have.
5. Uncheck all those system roles you do not want the selected user to have.
6. Click the **Assign** button.
7. Click on the **OK** button to save the system role changes.

The system roles of users can be printed using the **Print** button. The `userrights.xsl` style sheet is used for the printout. You can find this style sheet in the directory`\clients\admin`. You can edit the design.

Users which have been configured as profiles are not shown on the **System role administration** tab.

On the **System roles (user)** tab, all system roles are listed on the left. Select a system role to see to which users it has been assigned. You can take or assign a system role to multiple users with this tab.



Area: GLOBAL

□ Hide deactivated users

- Lokale Sicherheitsgruppen einrichten (ID = 66)
- Supervisor (ID = 18)
  - Administrator starten (ID = 1)
    - Konfiguration Gesamtsystem (ID = 2)
    - Konfiguration Sicherheitssystem (ID = 4)
    - Lokale Sicherheitsgruppen bearbeiten (ID = 65)
    - Konfiguration W-Vorlagen (ID = 5)
    - Konfiguration Archivdruck (ID = 6)
    - Automatische Aktionen starten (ID = 8)
    - Automatische Aktionen konfigurieren (ID = 9)
    - Benutzerablagen einsehen (ID = 10)
    - Objektrechte verändern (ID = 50)
  - Editor starten (ID = 11)
    - Objektdefinition bearbeiten (ID = 12)
    - Datenbank anpassen (ID = 13)
  - AxAuto: Starten (ID = 14)
  - Capture starten (ID = 15)
    - Konfigurieren (ID = 16)
  - Client starten (ID = 36)
    - Benutzereinstellungen speichern (ID = 17)
      - Menüband anpassen (ID = 77)
    - Historie öffnen (ID = 28)
      - Aus Historie wiederherstellen (ID = 32)
      - Historie für einzelne Objekte konfigurieren (ID = 56)
    - Expertensuche starten (ID = 29)
    - Aus Trefferliste exportieren (ID = 30)
    - Dokumente drucken (ID = 74)
    - Notizen anzeigen (ID = 71)
      - Notizen bearbeiten (ID = 31)

Users with system role: CLAUDIA, EUGENE, SAP, SEBASTIAN, STEFFEN, THOMAS, WEBUSER, WOLFGANG

Other users: AMBER, ANNE-SOPHIE, CÉCILE, CLAIRE, CLAXTON, DANNY, EXTRA-ADMIN, FRANCK, GRAHAM, HAROLD, HERVÉ DUPONT, INA, JANET, JEAN, JEAN-MARC, JOCELYNE, JOSEFINA, KRAUSE, LAURENT, MABLE, MARVIN, MICHELINE, MOODY, PAMELA, PETERSON, PIERRE

For local administrators within an area, the right to assign or revoke system roles may be limited to single system roles, which are being specified using the remote user administration.

The following system roles can be assigned to individual users in enaio® administrator:

ID	System role	Description
66	DMS: Set up local security groups	Configuration of remote areas
18	DMS: Supervisor	All system roles except for Workflow functions, enaio® enterprise-manager, and 'Server: Server: Switch job context'
1	Administrator: Starting	Start enaio® administrator
2	Administrator: Configuration of entire system	Configuration of the entire system (LDAP, automatic actions etc.)
4	Administrator: Configuration of security system	Configuration of the security system (user and rights administration)
65	Administrator: Configuration local security groups	Enables restricted configuration of the security system for remote areas.
5	Administrator: Configuration of W-templates	Administration of the W-templates (configuration of W-templates and assigned applications)
6	Administrator: Configuration of Archive Print	Configuration of the archive print
8	Administrator: Start automatic actions	Start installed automatic actions

9	Administrator: Configure automatic actions	Set up and configure automatic actions
10	Administrator: View user tray	View private trays of all users in enaio® administrator
50	Administrator: Change object rights	Specify other users or transfer object ownership itself
11	Editor: Starting	Start enaio® editor
12	Editor: Edit object definition	Change and modify object definition This role alone does not enable you to save changes in the database.
13	Editor: Adjust database	Make adaptations to the database
14	Start: Starting	Start enaio® start to run automatic actions
15	Capture: Starting	Start enaio® capture
87	Capture: Edit filing	Access to filing in enaio® capture
16	Capture: Configure	Set up configurations for enaio® capture
36	Client: Starting	Starting enaio® client
70	WebClient: Starting	Start enaio® webclient
17	Client: Save own settings	Make individual user settings and save queries and/or documents in the archive area of clients
80	Client: Configure external applications	Integrate external applications into clients
77	Client: Adjust ribbon	Adjust ribbon
28	Client: Open history	View editing history, where activated
32	Client: Restore data from history	Restore earlier data through editing history (Condition: System role 'Client: Open history' is available)
56	Client: Configure history of individual objects	Configuration of the history for an individual document, where included in the object definition (Condition: System role 'Client: Open history' is available)
29	Client: Start expert mode	Advanced search for objects
30	Client: Export from hit list	Export index data and document files from a hit list
74	Client: Print documents	Print documents via clients
71	Client: Open notes	Show notes on objects
31	Client: Edit notes	Create and edit notes on objects
33	Client: Show personal trash can	Show the personal trash can from which deleted data can be restored.
37	Client: View system trash can	Show system trash can in which the deleted

		objects of all users are visible (Condition: System role 'Client: Show personal trash can' is available)
40	Client: Delete objects from the trash can	Permanently delete objects in the trash can (Condition: System role 'Client: Show personal trash can' is available)
34	Client: Run SQL queries	Run SQL queries
85	Client: Share documents	Share documents with users with limited access rights
86	Client: Administer sharing	Remove sharing of other users
35	Client: Send content as e-mail	Send objects by e-mail to a recipient not set up in the enaio® system
44	Client: Open property	Show property dialog for an object
63	Client: Move objects	Move objects, provided this is allowed in enaio® administrator
83	Client: Assign other locations	Assign another location to documents
84	Client: Create reference documents	Create reference documents from documents
79	Client: Move across cabinets	Move documents across cabinets
19	Client: Use workflow	Use workflows
61	Client: Workflow substitute configuration	Set up workflow substitute for oneself
62	Client: Workflow process administration	Restricted administration of running processes from clients
67	Client: Edit workflow circulation slip	Edit workflow circulation slip
68	Client: Manage workflow of private circulation slip templates	Manage and delete templates for private circulation slips
69	Client: Manage workflow of public circulation slip templates	Manage and delete templates of public circulation slips
51	Client: Use object search	Show 'Object Search' area
52	Client: Use Navigation	Show 'Navigation' area
78	Client: Run default search	If users should run searches exclusively through saved searches, the default search (search by index data and full text search) can be switched off.
59	Client: Add icon	Include icons in the system's data pool
60	Client: Delete icon	Remove icons from the system's data pool
64	Client: Edit static layers of other users	Edit static layers not created by oneself
38	Client: Edit SQL queries	Create and edit SQL queries

39	Client: Administer subscriptions	Administer and delete subscriptions of all users and set up subscriptions for other users
55	Client: Administer follow-ups	Administer and delete follow-ups of all users
45	Client: Debug events	Run events for the client in debug mode
49	Client: Create events	Edit events for client and server
46	Client: Depict relations	Show relations/relations list where relation links are set up in the system
47	Client: Create visualization	Visualize relations and save the visualization in the assigned document type
48	Client: Administer visualization	General configuration for relation visualization
75	Client: Change archiving status	Give documents the property 'archivable' or 'non-archivable'
53	Client: Delete archived documents	Delete documents with the 'archived' status
57	Client: Carry out collective changes	Carry out collective changes for several selected objects in a hit list
73	Client: Always show variant administration	Users who have no write permissions for index data or objects can open the variant administration in read-only mode, but are not allowed to create new variants or assign the 'active variant' status to other variants.
76	Client: Show favorites	For every user, favorites are managed and their objects are accessible on mobile devices via enaio® apps as favorites.
81	Client: View preview annotations	Show annotations in the PDF preview
82	Client: Edit preview annotations	Create, edit, and delete annotations in the PDF preview
20	WF-Admin: Starting	Start enaio® administrator-for-workflow
21	WF-Editor: Starting	Start enaio® editor-for-workflow
22	WF-Editor: Edit organization	Edit workflow organization
58	WF-Editor: Record users as present/absent	Set presence of other workflow users
23	WF-Editor: Create model	Create workflow model
24	WF-Processes: Start by import	Start workflow processes via a system import, which is run by the automatic action 'Data/document import'
25	WF-Simulation: Starting	Start a workflow simulation
26	WF-Script: Starting	Start runtime environment for workflow scripts
27	Enterprise-Manager: Starting	Start enaio® enterprise-manager

72	Server: Switch job context	
88	Server: Run Ado jobs	

By using the **Extras** option in the menu bar you can show or hide system role IDs of the system roles in the remote user administration and the configuration dialog of the security system.

Change password

Follow these steps to change a user's password:

1. Open the **Security system** window.
2. Click on the **User administration** tab.
3. Select an individual user and click on the **Properties** button.
4. Enter a new password in the **Password** field on the **User data** tab. Enter the password a second time into the **Password verification** field.

   A maximum of 100 characters may be used for a password.
5. Click the **Apply** button.

The changes will be saved.

In enaio® enterprise-manager, you can set rules for password syntax using regular expressions. You must stick to these rules.

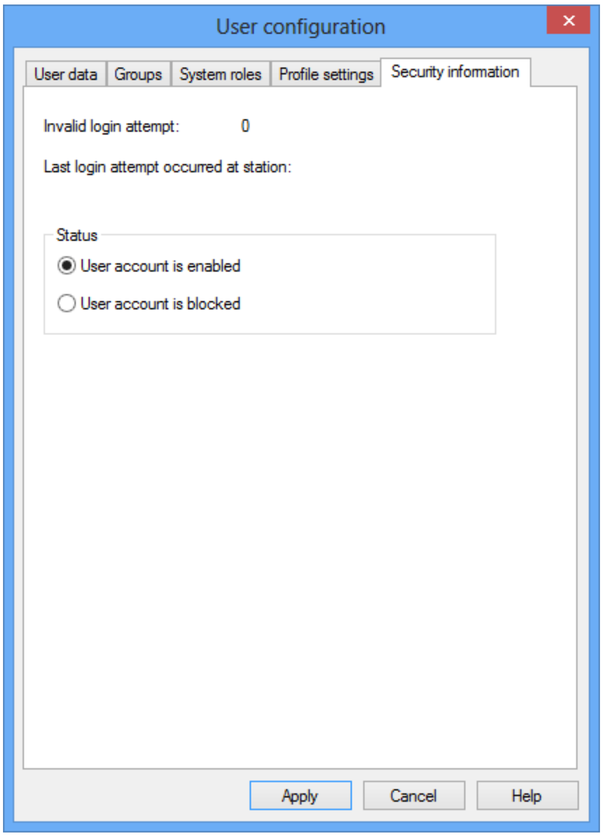
Use the 'Start to specify whether or not to check the case sensitivity of passwords.

Enabling and Locking User Account

On the **START** tab, you can choose to have user accounts locked after three failed login attempts.

A user account is enabled as follows:

1. Open the **Security system** window.
2. Click on the **User administration** tab.
3. Select an individual user and click on the **Properties** button.
4. Select the **Security information** tab and click on the **User account is enabled** radio button in the **Status** area.



Invalid login attempt: 0

Last login attempt occurred at station:

Status

● User account is enabled

○ User account is blocked

Provided that the security level **Blocking of user account** was specified (see ''Start' Tab' Tab'), invalid login attempts and the workstations where the attempt was made will be shown here.

5. Click the **Apply** button.

The user account is enabled again.

You can use the same dialog to lock a user account.

Users can use their settings in enaio® client to establish that users whose account was locked via the **Security information** tab are not shown in user lists.

Blocked users are never shown in user lists in enaio® webclient.

> Blocked users are not automatically blocked in the workflow system.

Set up Profiles

The creation of profiles may facilitate the administration of the security system. You can assign a profile to users and at the same time enter them in several groups and define the system roles. By changing a profile, you can modify group memberships and system roles for all those users that have the same profile.

It is also possible to create saved searches, extended queries, and links to external applications for all users with the same profile.

Profiles contain the following settings:

§ all settings that users can select in the settings dialog in enaio® client:

  - Settings for hit lists, i.e. configuration of the columns and hierarchical folder hit lists, as well as hit list layout
  - Ribbon settings
  - inbox configuration
  - Language
  - etc.
- Saved searches
- SQL queries
- Links to external applications, limited to the first 15
- Settings for the archive area
- Settings for the search bar
- positions of windows and bars

  (for screen resolutions smaller and bigger/equal to 1024 × 768)
- System roles
- Group membership
- Predefined labels for annotations on layers

Through profile administration, the scanner settings of enaio® client and enaio® capture are distributed as well.

> When assigning a profile to a user, the user’s settings and rights will be overwritten. Whether group memberships and system roles are overwritten or added is specified when distributing a profile.
>
> Group memberships and system roles of user having the system role 'DMS: Supervisor' will not be changed.

If a user has the system role 'Client: Save own settings', he can customize the profile settings assigned to him in enaio® client.

A profile is created like a new user, but the new user is marked as a profile template. The profile gets a user name and a password. It can be used to log in to enaio® client, for example, in order to create saved queries, links to external programs, and to configure the workspace and the search bars.

Group memberships and system roles of the profile and its assignment to users are set up in enaio® administrator in the same way as for regular users.

If you change the settings of a profile, it must be redistributed specifically in order to update the settings of the profile’s users.

In addition to the described individual profiles, it is possible to create group profiles.

Group profiles contain:

- Saved searches,
- SQL queries,

§ Links to external applications, limited to the first 15.

This profile is assigned to a group and will take effect on all current and future members of the group. Individual settings of group members will not be overwritten.

> Group profiles do not allow you to administer the access rights to archive objects, system roles and scanner settings.

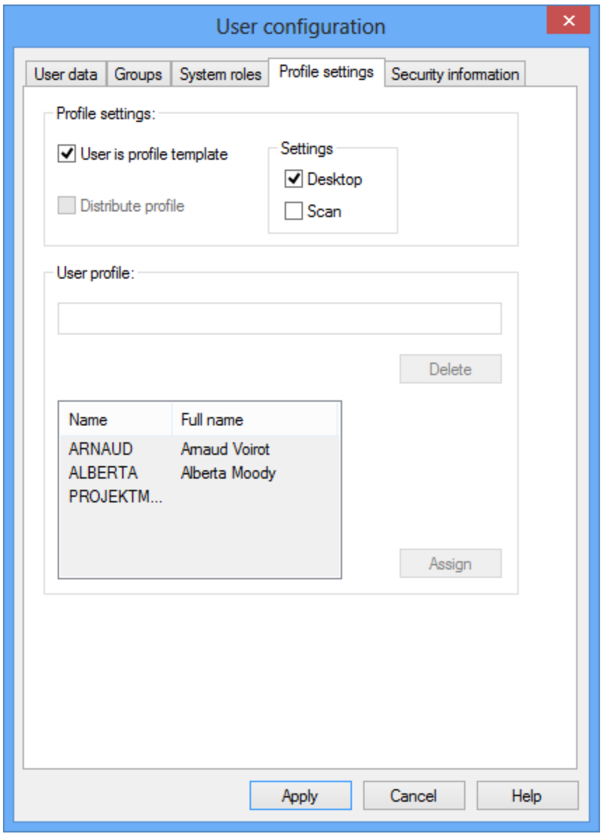
Creating Profiles

A profile is created on the **User administration** tab in the security system. You create it like a new user. It gets a user name and a password. This user name is used in enaio® client to configure the default settings for saved queries, links to external programs and search bars.

An already created user can also be used as a profile template.

Follow these steps to create a profile:

1. Open the **Security system** window.
2. Click on the **User administration** tab.
3. Select an individual user and click on the **Properties** button.
4. Select the **User is a profile template** option on the **Profile setting** tab.



Profile settings:

☑ User is profile template

□ Distribute profile

Settings

☑ Desktop

□ Scan

User profile:

Name	Full name
ARNAUD	Arnaud Voirot
ALBERTA	Alberta Moody
PROJEKTM...	

5. Choose whether to use the desktop and/or scanner settings of enaio® client and enaio® capture.

6. Click the **Apply** button.

The user will be shown with the profile icon in the user list on the **User administration** tab.

You can assign the profile to users (see 'Assigning a Profile to Users').

If you change the settings of a profile, it must be redistributed in order to update the changes with the assigned users (see 'Distributing Profiles').

Profiles which are not assigned to individual users but are used to assign saved searches, SQL queries, and links to external applications to groups, must be members of one group only.

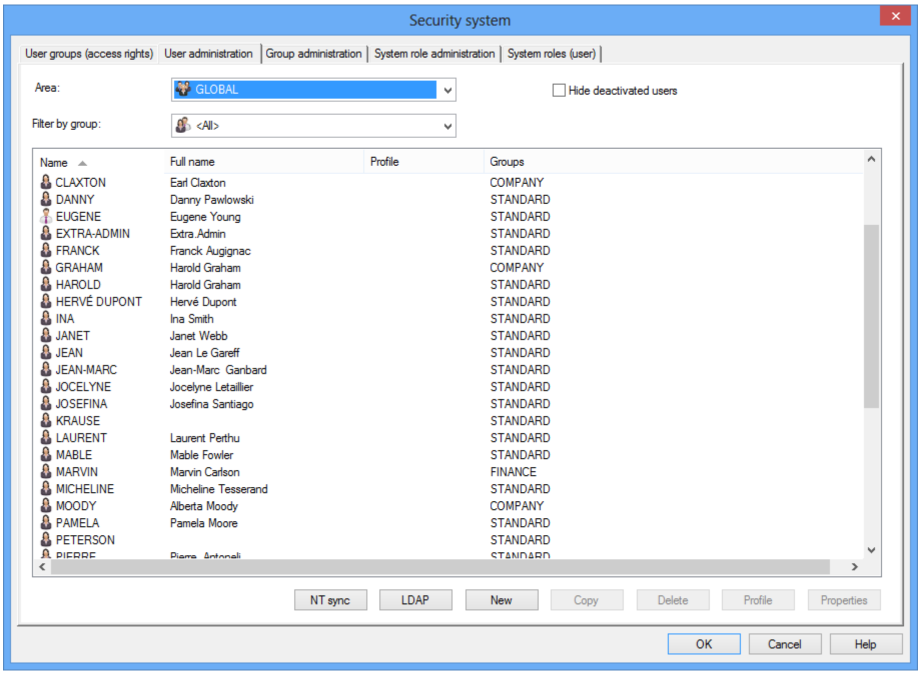
Assigning a Profile to Users

You can assign exactly one profile to a user. The user's settings will be then replaced by those specified in the profile. Whether group memberships and system roles are overwritten or added is specified when distributing a profile (see 'Distributing Profiles').

If you assign a profile to a supervisor, his system roles will not be changed.

Follow these steps to assign a profile to users:

1. Open the **Security system** window.
2. Click on the **User administration** tab.



Security system
User groups (access rights) | User administration | Group administration | System role administration | System roles (user)

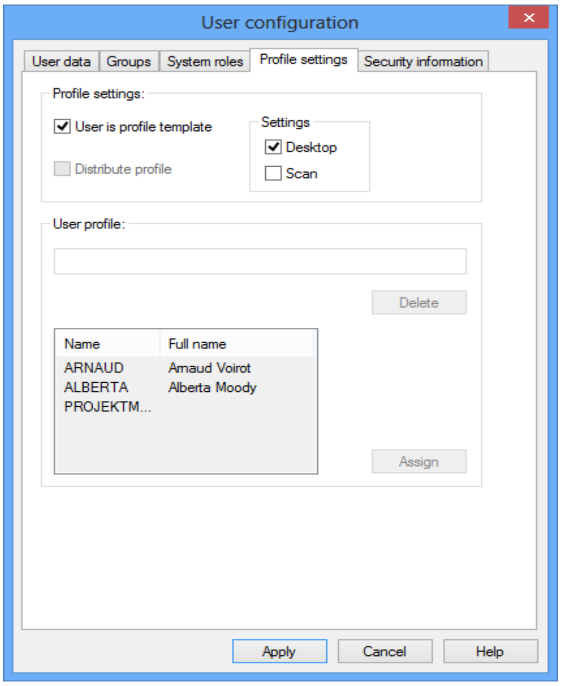
Area: GLOBAL

☐ Hide deactivated users

Filter by group: <All>

Name	Full name	Profile	Groups
CLAXTON	Earl Claxton		COMPANY
DANNY	Danny Pawlowski		STANDARD
EUGENE	Eugene Young		STANDARD
EXTRA-ADMIN	Extra.Admin		STANDARD
FRANCK	Franck Augignac		STANDARD
GRAHAM	Harold Graham		COMPANY
HAROLD	Harold Graham		STANDARD
HERVÉ DUPONT	Hervé Dupont		STANDARD
INA	Ina Smith		STANDARD
JANET	Janet Webb		STANDARD
JEAN	Jean Le Gareff		STANDARD
JEAN-MARC	Jean-Marc Ganbard		STANDARD
JOCELYNE	Jocelyne Letaillier		STANDARD
JOSEFINA	Josefina Santiago		STANDARD
KRAUSE			STANDARD
LAURENT	Laurent Perthu		STANDARD
MABLE	Mable Fowler		STANDARD
MARVIN	Marvin Carlson		FINANCE
MICHELINE	Micheline Tesserand		STANDARD
MOODY	Alberta Moody		COMPANY
PAMELA	Pamela Moore		STANDARD
PETERSON			STANDARD
PIERRE	Pierre Antoneli		STANDARD

3. Select one or more users.
4. Click the **Profile** button.
5. The **User configuration** window with the **Profile setting** tab will open.



User configuration

User data | Groups | System roles | Profile settings | Security information

Profile settings:

☑ User is profile template

□ Distribute profile

Settings

☑ Desktop

□ Scan

User profile:

Name	Full name
ARNAUD	Arnaud Voirot
ALBERTA	Alberta Moody
PROJEKTM...	

6. Select a profile.
7. Click the **Assign** button.

The profile will be assigned to the selected users. The user's settings will be then replaced by those specified in the profile. According to profile distribution settings group memberships and system roles are extended or overwritten.

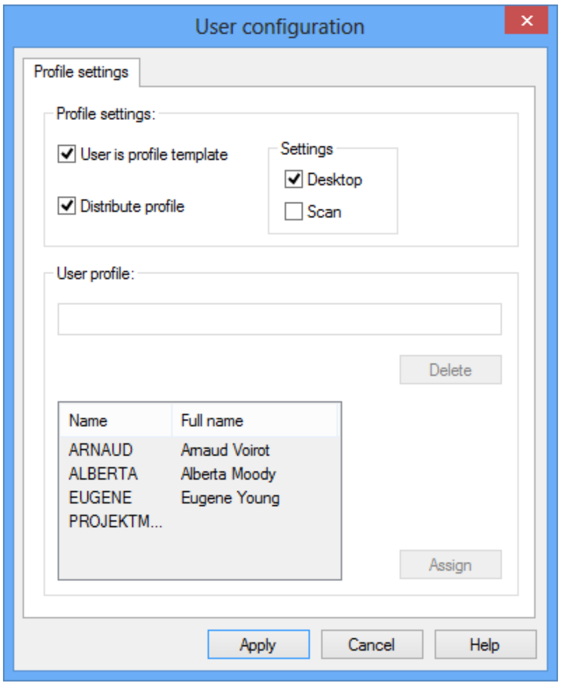
You remove the assignment of a profile to a user by clicking the **Delete** button on the **Profile setting** tab.

Distributing Profiles

If you change the settings of a profile in enaio® client or in the security system, these changes will only take effect on assigned users after the profile has been redistributed.

Follow these steps to distribute a profile:

1. Open the **Security system** window.
2. Click on the **User administration** tab.
3. Select a profile and click on the **Properties** button.
4. Activate the **Profile settings** tab in the **User configuration** window.
5. Select the **Distribute profile** option.



User configuration

Profile settings

Profile settings:

☑ User is profile template

☑ Distribute profile

Settings
☑ Desktop
□ Scan

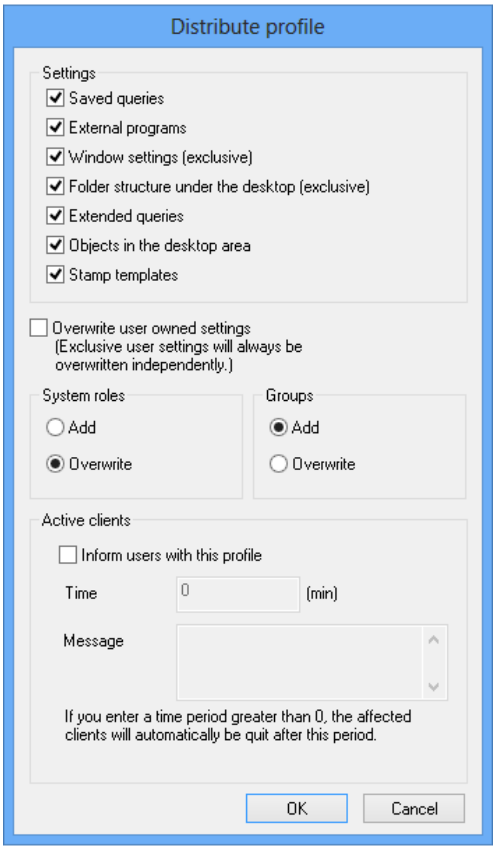
User profile:

Name	Full name
ARNAUD	Arnaud Voirot
ALBERTA	Alberta Moody
EUGENE	Eugene Young
PROJEKTM...	

This option is available only if the profile settings differ from the settings of the previously distributed profile.

6. Click the **Apply** button.

   The **Distribute profile** dialog will open.



Distribute profile

Settings
☑ Saved queries
☑ External programs
☑ Window settings (exclusive)
☑ Folder structure under the desktop (exclusive)
☑ Extended queries
☑ Objects in the desktop area
☑ Stamp templates

□ Overwrite user owned settings
(Exclusive user settings will always be overwritten independently.)

System roles
○ Add
● Overwrite

Groups
● Add
○ Overwrite

Active clients
□ Inform users with this profile
Time 0 (min)
Message

If you enter a time period greater than 0, the affected clients will automatically be quit after this period.

7. Select the settings you want to distribute.

8. If you distribute **Window settings** and **Folder structure under the desktop**, these settings always overwrite the users' setting.

   You can decide whether the users' settings will be overwritten for the selected non-exclusive settings.

9. To have more than the selected user-specific settings with the profile's settings, activate the **Overwrite user-own settings option**. These are particularly the object-type specific options and settings, which the user configures using the settings dialogs in enaio® client.

   For groups and system roles you can choose to only add new groups and system roles or to completely overwrite them with the groups and system roles of the profile.

   System roles are never overwritten when the user has the system role 'DMS: Supervisor'.

10. Confirm with **OK**.

Changes to the profile will apply to all assigned users.

To distribute the profile to logged-in users, you must inform them. Select this option if you cannot rule out users being logged in.

You can enter a period in minutes after which the logged in clients will be closed automatically. After restart, changed settings will be available.

If you do not enter a time and, instead, leave the setting at the value 0, the changed settings will become available after enaio® client has been closed and restarted by the user.

Assigning Profiles to Groups

If you assign a profile to a group, you are therefore providing all current and future members of this group the saved queries, the SQL queries, and the links to external applications assigned to this profile. Other settings will not be modified. Saved queries and links created by the user will not be replaced.

A profile to be assigned to a group is created in the same way as a profile to be assigned to individual users (see 'Set up Profiles'). However, the profile must only be a member of the group that you want to assign it to and must only use desktop settings.

If you change the saved queries, SQL queries, and the links to external applications assigned to this profile, these changes are only applied to the group if you distribute the profile (see 'Distributing Profiles').

Follow these steps to assign a profile to a group:

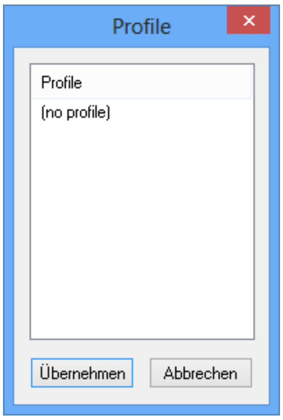
1. Open the **Security system** window.
2. Click on the **Group administration** tab.
3. Select a group.
4. Click the **Profile** button.

   The **Profile** window will open.

5. Select a profile from the list of available profiles.

   Only the profiles that can be assigned to the selected group will be listed.

6. Click the **Apply** button.



The saved queries, SQL queries, and links to external applications are assigned to the group.

If you want to delete the profile assignment to a group, select the entry **(No Profile)** in the **Profile** window and click **Apply**.

Exporting and Importing User and Group Data

Data from the enaio® security system – user and group data as well as corresponding workflow information – can be exported and imported. For instance, it is possible to export data from a productive system, modify them in a test system and then import them into the productive system.

Export and import are carried out as automatic actions. You integrate automatic actions via the **Complete system/Additions** tab (see ''Additions' Tab'). You can then create configurations for the actions and execute them manually using enaio® administrator or periodically using enaio® start (see 'Setting Up Automatic Actions').

This action does not require an additional license keys.

Export User and Group Data

For the 'Export users/groups' action, you incorporate the `axacdirectorysync.dll` library.

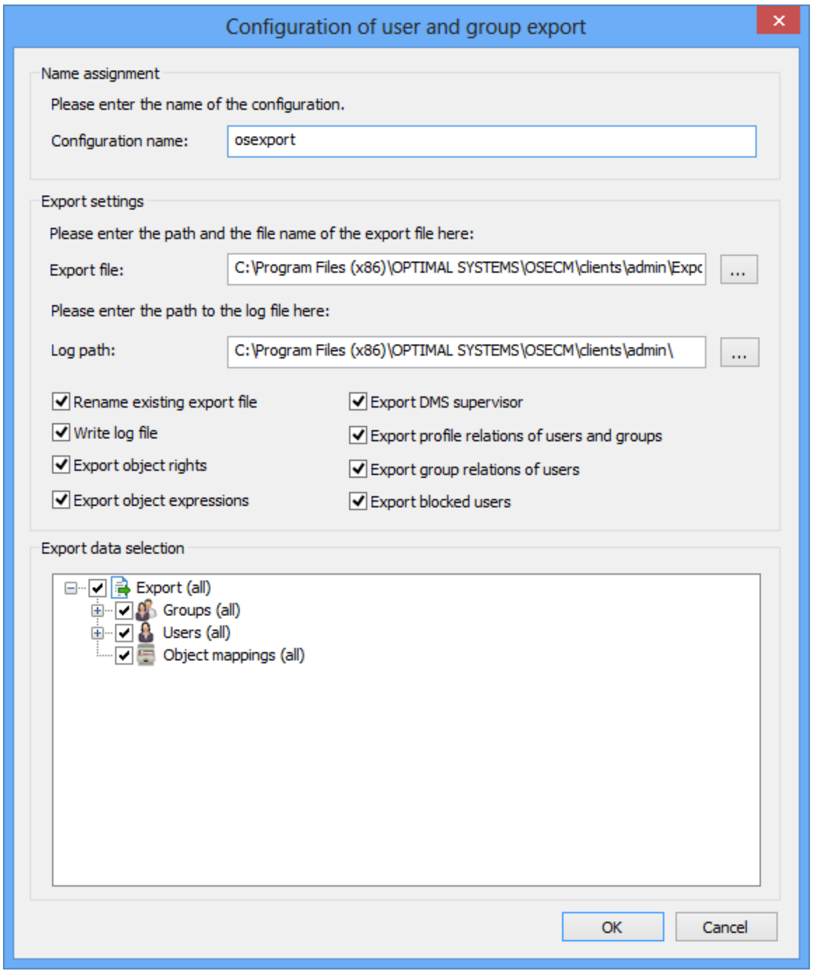
Once this is done, add the action using the **Automatic actions** dialog and create a configuration.

Configuration Data

A configuration name is entered on the configuration dialog. The name must be unique. Special characters are allowed.

Then specify a path and name to the export file and an optional log file path. The log file is only generated if you enable the checkbox **Write log file**. The log file receives the name of the export file with the suffix 'log'. Both files are XML files.

This kind of logging takes place independently from enaio® logging.



Configuration of user and group export

Name assignment

Please enter the name of the configuration.

Configuration name: osexport

Export settings

Please enter the path and the file name of the export file here:

Export file: C:\Program Files (x86)\OPTIMAL SYSTEMS\OSECM\clients\admin\Expc

Please enter the path to the log file here:

Log path: C:\Program Files (x86)\OPTIMAL SYSTEMS\OSECM\clients\admin\

☑ Rename existing export file

☑ Write log file

☑ Export object rights

☑ Export object expressions

☑ Export DMS supervisor

☑ Export profile relations of users and groups

☑ Export group relations of users

☑ Export blocked users

Export data selection

☑ Export (all)

☑ Groups (all)

☑ Users (all)

☑ Object mappings (all)

If you execute a configuration, an export file will be created. If an export file already exists at the given location, it will be overwritten.

Activate the checkbox **Rename existing export file** to rename any existing log file by prepending its date of creation rather than replacing it by the new log.

Export Data

Select the data that you want to export in the **Export data selection** area. Therein, all groups, users and object types will be listed for the assignment from the security system.

§ Groups and object assignments

Select one or all those groups that you want to export.

Export data related to groups include the names, descriptions and profile assignments.

All further data must be explicitly specified for export.

- Groups are assigned to object types. These assignment data will be exported if you select the respective object types, cabinets or all object assignments.
- Object rights (access rights) are assigned to object types. If you want to export this data, activate the checkbox **Export object rights**.
- Object expressions may make object rights conditional on conditions. If you want to export these data, activate the checkbox **Export object clauses**.
- A profile can be assigned to a group. If so, the user data of the assigned profiles can also be exported. To do so, activate the checkbox **Export profile relations of users and groups**.
- User

  Select one or all those users whose data you want to export.

  A user's export data contain the information that was displayed on the **User data** tab upon user creation. Password is encrypted.

  Data related to the assignment of system roles, group memberships and the information whether a user’s account is blocked or enabled can also be exported.

  - Users whose account is deactivated will only be exported when the respective check box is activated.
  - Users with the system role 'DMS: Supervisor' will only be exported when the respective check box is activated.
  - If a profile is assigned to a user, the user data of the assigned profile can also be exported. To do so, activate the checkbox **Export profile relations of users and groups**.
  - By default, the data related to the users’ group memberships contain only group names. Activate the checkbox **Export group memberships of users** so that the descriptions and profile assignments of the groups are exported in which the exported users are members.
  - Just like to groups, profiles can be assigned to users. Activate the checkbox **Export profile relations of users and groups** to export the user data that are created only as profiles for exported users.

Click **OK** to confirm the configuration. All data will be saved and the import can be instantly performed with enaio® administrator or at a scheduled time with enaio® start.

Import User and Group Data

Integrate the library `axacdirectorysync.dll` for the 'User/Group Import' action.

Once this is done, add the action using the **Automatic actions** dialog and create a configuration.

Always back up all of the current user and group data before performing an import of user and group data. Importing data that have been erroneously configured or modified can lead to violation of the data protection regulations.
In case remote user administration areas have been configured, user and group data cannot be imported.

Configuration Data

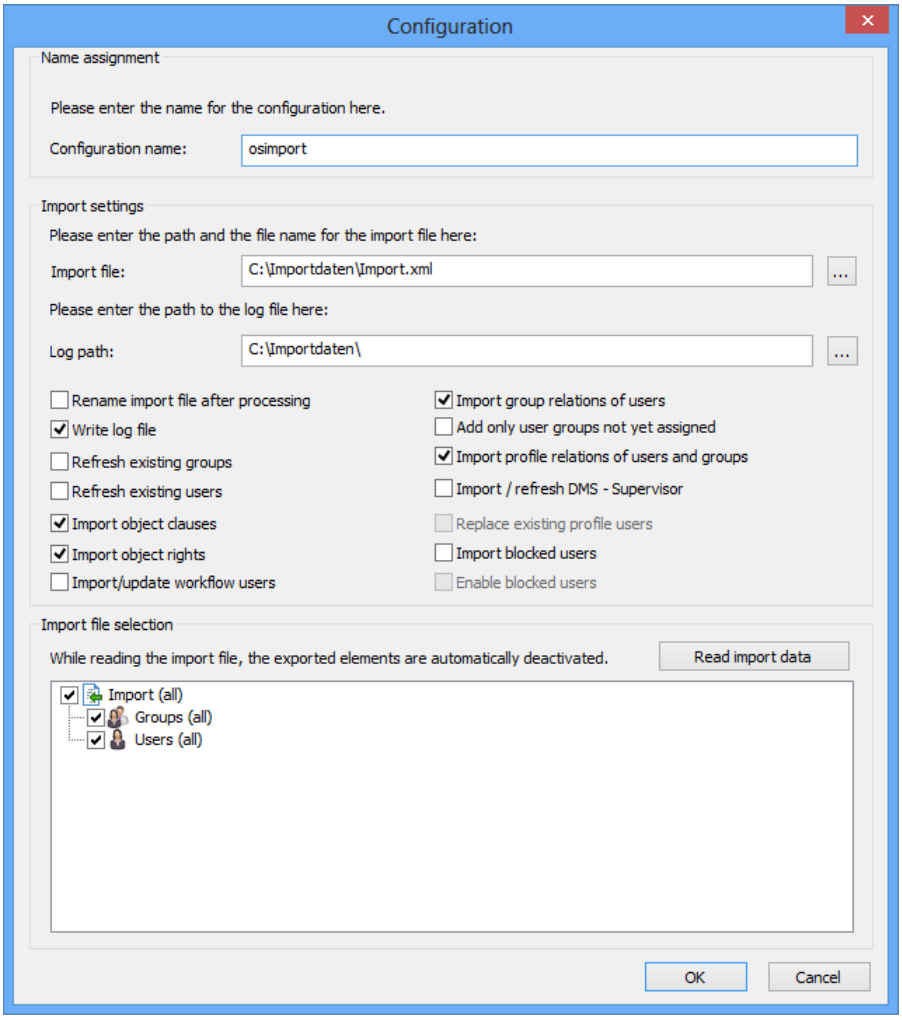
A configuration name is entered on the configuration dialog. The name must be unique; special characters are possible.

Then, enter the path and the name to the import file. You can specify the name syntax with the help of placeholders. If you enter a folder name, the import will check all XML files in the folder.

You can only import user and group data from files which have been created by one of the two automatic actions 'User and group export'.

A path for a log file is optional. The log file is only generated if you select the checkbox **Write log file**. The log file receives the name of the import file with the prefix 'log'. The log file is an XML file.

This kind of logging takes place independently from enaio® logging.



Configuration

Name assignment

Please enter the name for the configuration here.

Configuration name: osimport

Import settings

Please enter the path and the file name for the import file here:

Import file: C:\Importdaten\Import.xml ...

Please enter the path to the log file here:

Log path: C:\Importdaten\ ...

☐ Rename import file after processing
☑ Write log file
☐ Refresh existing groups
☐ Refresh existing users
☑ Import object clauses
☑ Import object rights
☐ Import/update workflow users
☑ Import group relations of users
☐ Add only user groups not yet assigned
☑ Import profile relations of users and groups
☐ Import / refresh DMS - Supervisor
☐ Replace existing profile users
☐ Import blocked users
☐ Enable blocked users

Import file selection

While reading the import file, the exported elements are automatically deactivated.

☑ Import (all)
☑ Groups (all)
☑ Users (all)

Activate the checkbox **Rename import file after processing** to rename any existing log file by prepending its date of creation rather than replacing it by the new log.

Import Data

If you have indicated exactly one import file, you can show this data via the **Read import data** button in the **Import data selection** area.

All groups and users available in the import file will be then listed. You can either select all users, all groups or both depending on whose data you want to import.

If you just enter a folder name or a path syntax using placeholders, you can choose whether to import single or all users.

§ Groups

Group data consist of names, descriptions and profile assignments. They may include object assignments, object rights and object expressions. Object assignments will always be imported if the objects exist in the import system.

For importing groups, specify:

§ whether or not data of existing groups will be updated.

- If you do not select this option, group data will not be imported in case a group with the same name exists.
- whether or not object expressions will be imported.
- If object assignments and object rights are imported, object expressions can also be imported. Select the corresponding checkbox.
- Logic expressions refer to object fields. If these object fields do not exist in the system, the expression will not be imported.
- This option has to be disabled during Active Directory synchronization.
- Specify whether object rights will be imported.
- If the import data include object assignments, they will always be imported. Object assignments not existing in the system will not be imported. Object rights will not be imported unless the respective check box is activated.
- This option has to be activated during Active Directory synchronization.
- Specify whether workflow information of users will be imported.
- Unique assignment of users to the workflow organization structure is only possible if the XML file to be imported contains: wf-name, wf-surname, wf-email, wf-login, is-wf-user, wf-organization (name, wf-org-id, wf-user-id), wf-role (name, wf-role-id, wf-org-id').
- Import requires workflow organization structures and internal IDs of both the source and the target system to be identical. Otherwise enaio® user data will be imported without workflow information because it is impossible to uniquely assign users to the workflow organization.
- To transfer the organizational workflow structure to the target system, just use the export/import feature of enaio® editor for workflow.
- Specify whether or not the profile relations of groups will be imported.
- A profile can be assigned to groups. If so, data of the profile user will be required. If this data is not available, the profile property of the group to be imported will be deleted in order to avoid inconsistencies.
- If profile user data is part of the import data, you can either select the respective user when selecting import data or activate the option **Import profile relations of users and groups** in order to automatically import the data of users who have been defined as profile for other groups or users.

  - If the import data do not contain profile user data, the system checks whether the necessary profile user data are already in the user administration. If so, the profile property will be retained; otherwise, the profile property will be deleted.

- User

  User data contain the information that was shown on the **User data** tab upon user creation as well as the unique GUID of the user. Password is encrypted. Data related to assigned system roles and group memberships will also be imported.

  For importing users, specify:

  - whether or not data of existing users will be updated.

    If you do not select this option, user data will not be imported in case a user with the same name already exists.

  - whether users with the system role 'DNS: Supervisor' will be imported or updated.

  - whether or not users whose accounts are blocked will be imported.

    If you do not select this option, only users whose accounts are not blocked will be imported.

    If you import these users, you can enable their accounts by activating the checkbox **Enable blocked users**.

  - Specify whether or not the profile relations of users will be imported.

    A profile can be assigned to users. If so, data of the profile user will be required. If this data is not available, the profile property of the group to be imported will be deleted in order to avoid inconsistencies.

    If profile user data is part of the import data, you can either select the respective user when selecting import data or activate the option **Import profile relations of users and groups** in order to automatically import the data of users who have also been defined as profile for other groups or users. The default settings are used for profile assignment, i.e. system roles are overwritten and group memberships added. The default behavior cannot be changed.

    If the import data do not contain profile user data, the system checks whether the necessary profile user data are already in the user administration. If so, the profile property will be retained; otherwise, the profile property will be deleted.

  - If a user has a profile function in the import system but becomes a user without a profile function through an import update, you must select the checkbox **Replace existing profile user**. The profile assignments will be deleted. The settings of users to which the profile has been assigned will not be changed. Only the user who now has no profile function any more loses the profile function.

If you do not activate the checkbox **Replace existing profile users**, data of profile users is not updated with data of users who do not have a profile function.

§ Activate the checkbox **Import group memberships of users** so that the descriptions and profile assignments of the groups are imported in which the imported users are members.

§ When activating the **Add only unassigned user groups** checkbox option, existing group assignments will not be modified, but unassigned groups will be added to user accounts and groups.

Click **OK** to confirm the configuration. All data will be saved and the import can be instantly performed with enaio® administrator or at a scheduled time with enaio® start.

Automatic Directory Synchronization

The automatic action 'Directory synchronization' automatically executes synchronization with all Directory systems, e.g. Novell eDirectory and Active Directory.

Doing so, user and group data of an enaio® system and the Directory system are exported and synchronized. New and changed user data of the directory system are then imported into the enaio® system.

If synchronization is carried out with remote user administration, data is synchronized only to a limited degree: Only user group assignments and user changes are synchronized. This means that users may be deleted from the administration area of a local administrator, no longer be visible for him/her, and appear in the administration area of another local administrator.

To configure the action, use a configuration wizard.

To use this automatic action, add the `axacdirectorysync.dll` library.

The action uses style sheets for the XSLT transformation, which are delivered as standard with the setup. Copy the `components\DirectorySync-XSLT` directory with the installation data into a `...clients\admin` subdirectory of the application data.

As in the automatic action 'User and group import' (see 'Import User and Group Data') users cannot be deleted and user names cannot be changed. Users who have been deleted from the Directory system are disabled in enaio®. They are not deleted or disabled in the workflow organization.

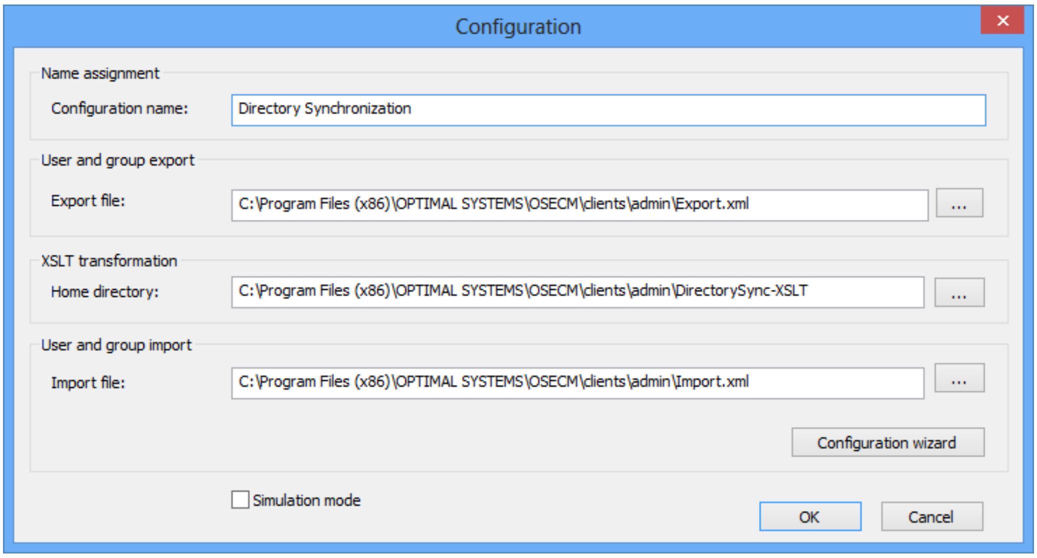
If remote user administration is used, then data within the remote areas is synchronized only to a limited degree: Only user group assignments and user changes are synchronized. This means that users may be deleted from the administration area of a local administrator.

In addition to the automatic action 'Directory Synchronization,' the automatic action 'XSLT Directory Synchronization' is also available. It is also integrated via the `axacdirectorysync.dll` library.

The XSLT Directory Synchronization does not use a wizard but enables directory data to be called up very flexibly via a command line and enables configuration files and style sheets to be integrated for XSLT transformation.

Configuration Data

When setting up the automatic action, enter the configuration name and the paths for the export files from the enaio® system and the directory system.



Name assignment

Configuration name: Directory Synchronization

User and group export

Export file: C:\Program Files (x86)\OPTIMAL SYSTEMS\OSECM\clients\admin\Export.xml

XSLT transformation

Home directory: C:\Program Files (x86)\OPTIMAL SYSTEMS\OSECM\clients\admin\DirectorySync-XSLT

User and group import

Import file: C:\Program Files (x86)\OPTIMAL SYSTEMS\OSECM\clients\admin\Import.xml

□ Simulation mode

Specify the home directory in the …`clients\admin\` subdirectory into which the XSLT transformation data were copied.

At last, enter the path of the XML file to be imported with the updated user and group data which are automatically imported into the enaio® system.

The automatic action can be run in simulation mode. This will include all steps as far as import of the updated user and group data. Once simulation is done, the new XML file with updated user and group data will open for checking. Provided that simulation has been successful and you want the automatic action to run productively, reopen the automatic action for configuration and deactivate the simulation mode.

With enaio® start, you can execute the automatic action in a time-controlled manner so that user data are automatically synchronized and updated on a regular basis.

The Configuration Wizard

In the configuration wizard you can customize XSLT transformation settings. This way, no further customization of files is necessary.

Start the configuration assistant using the button in the configuration dialog.

DSDE Queries

In this step, you enter the server IP address and port as well as the LDAP path as parameters for the data query in the Directory.

Notation:

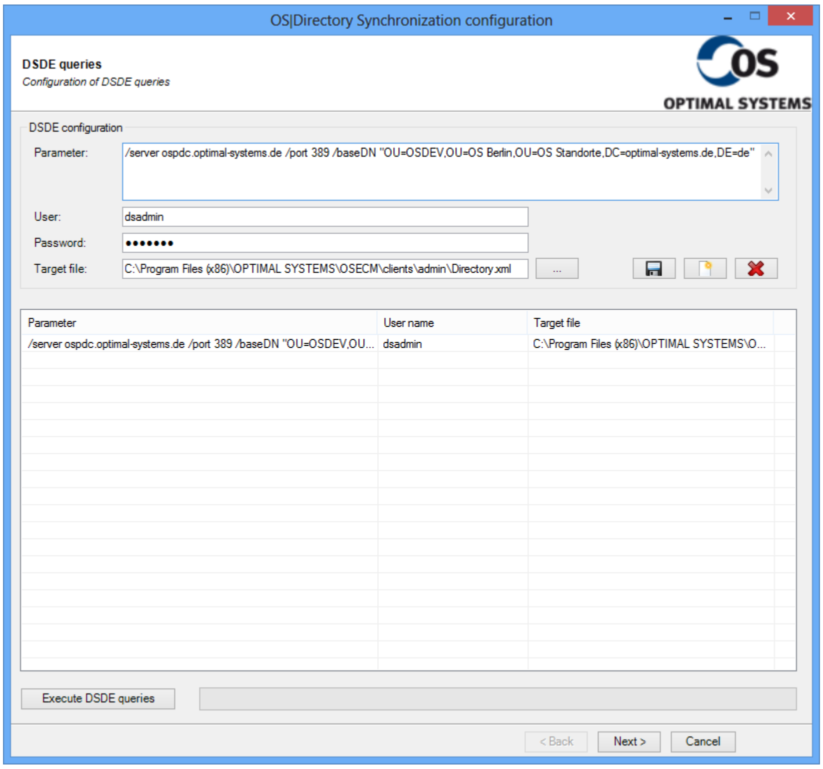
```
/server <Name or IP> /port <Port> /baseDN "<LDAP-Path>"
```

The parameter information must be in DSDE expected notation. Details can be found in the Microsoft documentation.

Specify as user name and password the access data of the domain account, which will be used for the AD query and which has the corresponding rights in the domain.

As the target file specify the name and path for the file where the data from the directory will be exported.

After entering this data, click the **Save** button. The data will be transferred to the query list. You can create multiple queries. Each query must be saved to a separate file. If you select a query in the list, the data will be shown. You can edit and save this data or delete it again by clicking the **Delete** button. Click the **New** button to create a new query.



DSDE queries
Configuration of DSDE queries

DSDE configuration

Parameter: /server ospdc.optimal-systems.de /port 389 /baseDN "OU=OSDEV,OU=OS Berlin,OU=OS Standorte,DC=optimal-systems.de,DE=de"

User: dsadmin

Password: •••••••

Target file: C:\Program Files (x86)\OPTIMAL SYSTEMS\OSECM\clients\admin\Directory.xml

Parameter	User name	Target file
/server ospdc.optimal-systems.de /port 389 /baseDN "OU=OSDEV,OU...	dsadmin	C:\Program Files (x86)\OPTIMAL SYSTEMS\O...

After having created the queries, you must execute the DSDE query. The respective data will be displayed in the following steps.

Then click **Next** to continue with the configuration.

Group mappings

Assign a directory group to an OS group. To do so, select an OS group and a directory group. Only directory groups that have members are displayed here.

Enter additional parameters and click the **Save** button. The assignment is entered in the assignment list.

The group lists can be filtered. If you enter a character sequence in a **Filter** field, only the groups that contain the character sequence will be shown. Remove the filter again using the **Update** button. Updating is also necessary if you have added or modified queries in the previous step.

You can specify the following parameters for an assignment:

§ Password for members of this group

Users who have not yet been a member of an OS group receive this password.

If you do not specify a password, the password 'optimal' is entered.

§ User profile for members of this group

New members receive this profile, whereas it is assigned to existing members. However, in the latter case it must be redistributed in enaio® administrator.

§ Roles

Specify the IDs of the desired system roles.

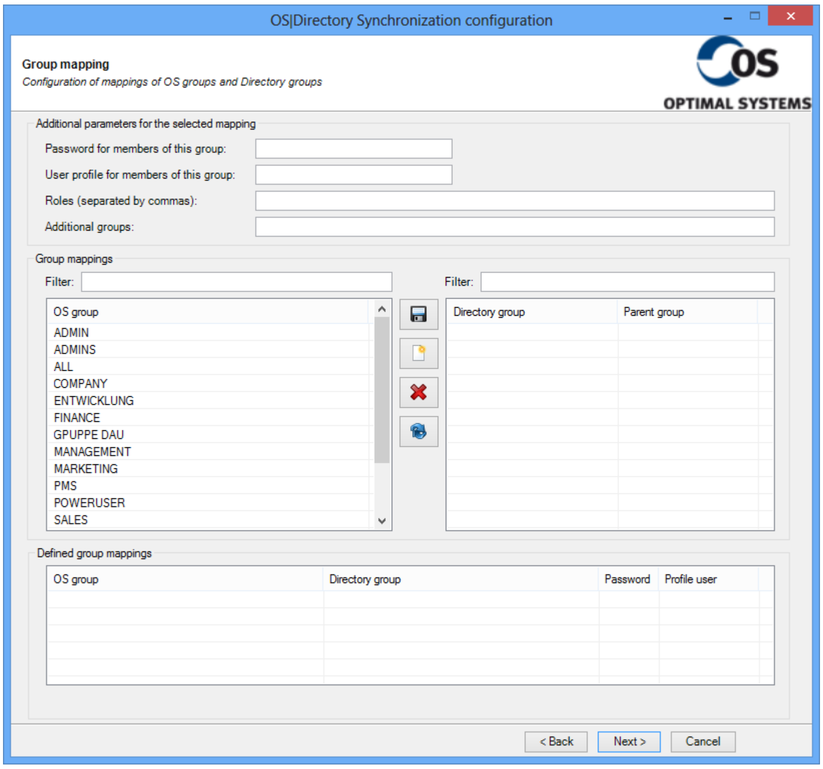
All members are assigned the specified system roles, any existing roles are deleted.

In enaio® administrator, you can choose to show the IDs of the system roles via the **EXTRAS** menu within the user administration.

§ Additional groups

Additional groups are assigned to all members.

> These parameters may depend on other parameters that are specified in the user and group import configuration in a later step.



OS|Directory Synchronization configuration

Group mapping

Configuration of mappings of OS groups and Directory groups

Additional parameters for the selected mapping

Password for members of this group:

User profile for members of this group:

Roles (separated by commas):

Additional groups:

Group mappings

Filter:

OS group
ADMIN
ADMINS
ALL
COMPANY
ENTWICKLUNG
FINANCE
GPUPPE DAU
MANAGEMENT
MARKETING
PMS
POWERUSER
SALES

Filter:

Directory group	Parent group

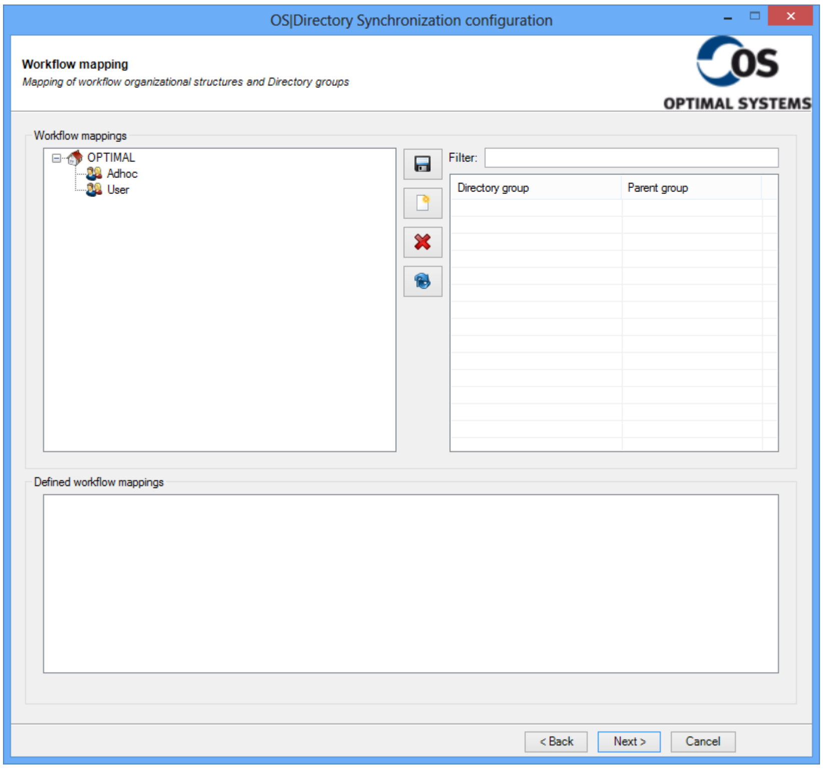
Defined group mappings

OS group	Directory group	Password	Profile user

Then click **Next** to continue with the configuration.

Workflow mapping

Assign a Directory group to an OS organizational class 'Role'. To do this, select an OS role and a directory group and click on the **Save** button. The assignment is entered in the assignment list.


OS|Directory Synchronization configuration
Workflow mapping
Mapping of workflow organizational structures and Directory groups
OPTIMAL SYSTEMS
Workflow mappings
OPTIMAL
Adhoc
User
Filter:
Directory group
Parent group
Defined workflow mappings
< Back
Next >
Cancel

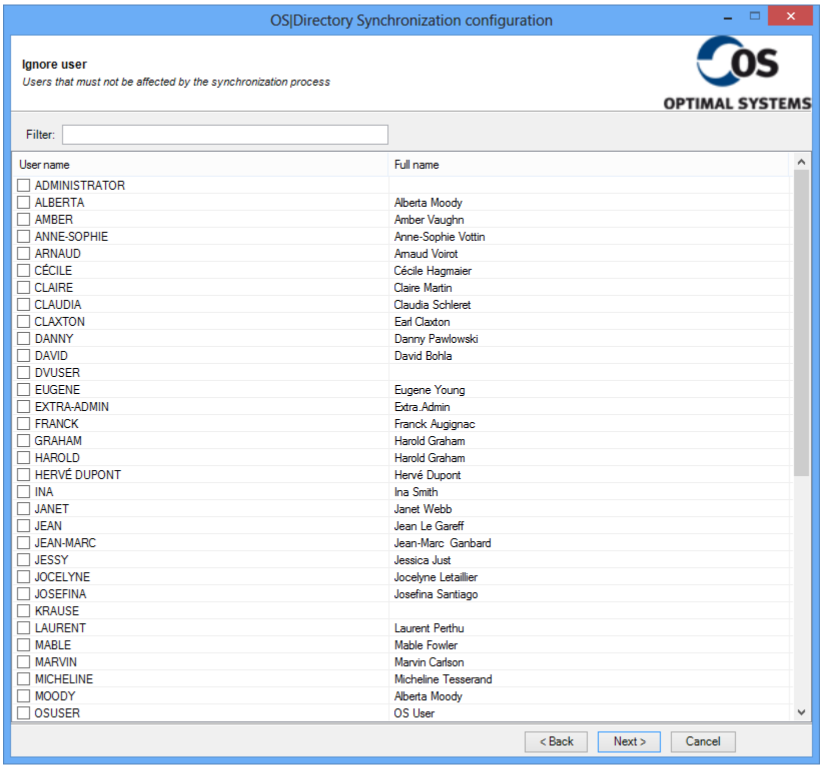
Then click **Next** to continue with the configuration.

Ignore users

Here you can activate all OS users whose data you do not want to be changed by the synchronization.

> Activate all users here that are not to be deleted because they are only in the OS user administration.

All existing OS users are listed. The view can be filtered. If you activate the checkbox for a user, the data of this user will not be changed.



Ignore user

Users that must not be affected by the synchronization process

Filter:

User name	Full name
□ ADMINISTRATOR	
□ ALBERTA	Alberta Moody
□ AMBER	Amber Vaughn
□ ANNE-SOPHIE	Anne-Sophie Vottin
□ ARNAUD	Amaud Voirot
□ CÉCILE	Cécile Hagmaier
□ CLAIRE	Claire Martin
□ CLAUDIA	Claudia Schleret
□ CLAXTON	Earl Claxton
□ DANNY	Danny Pawlowski
□ DAVID	David Bohla
□ DVUSER	
□ EUGENE	Eugene Young
□ EXTRA-ADMIN	Extra.Admin
□ FRANCK	Franck Augignac
□ GRAHAM	Harold Graham
□ HAROLD	Harold Graham
□ HERVÉ DUPONT	Hervé Dupont
□ INA	Ina Smith
□ JANET	Janet Webb
□ JEAN	Jean Le Gareff
□ JEAN-MARC	Jean-Marc Ganbard
□ JESSY	Jessica Just
□ JOCELYNE	Jocelyne Letaillier
□ JOSEFINA	Josefina Santiago
□ KRAUSE	
□ LAURENT	Laurent Perthu
□ MABLE	Mable Fowler
□ MARVIN	Marvin Carlson
□ MICHELINE	Micheline Tesserand
□ MOODY	Alberta Moody
□ OSUSER	OS User

Then click **Next** to continue with the configuration.

User and group import configuration

You can specify the following import parameters:

§ Write log file

You can set up additional logging. You must specify the path for this logging file. The file gets the name `axacuimp.log.xml`.

§ Rename import file after processing

Activate the checkbox **Rename import file after processing** to rename any existing log file by prepending its date of creation rather than replacing it by the new log.

§ Refresh existing groups

If you do not select this option, group data will not be imported in case a group with the same name exists.

§ Refresh existing users

If you do not select this option, user data will not be imported in case a user with the same name already exists.

§ Import object expressions

Clauses for the access rights to objects are imported at the same time.

§ Import object rights

Access rights to objects are imported at the same time.

§ Import/update workflow users

The workflow assignment is only evaluated if you select this option.

§ Add only not yet assigned user groups

At import, belonging of a user to a group is not deleted but added.

§ Import profile relations from users and groups

If you activate this option, the data of users serving as a profile for other groups or users will also be imported automatically.

§ Import/update DMS supervisor

Data of users having the system role 'DMS: Supervisor' are only included if this option is activated.

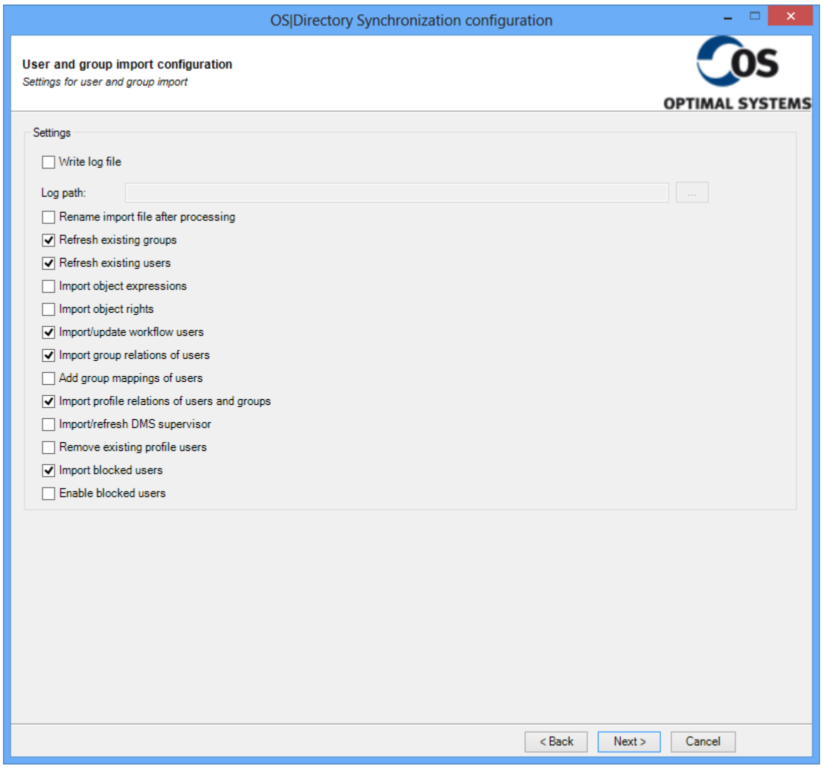
§ Replace existing profile users

You must select the checkbox **Replace existing profile users** if a user who is a profile user in the import system would become a user without profile function due to an import update. The profile assignments will be deleted. The settings of users to which the profile has been assigned will not be changed. But the settings of the user account that now is a user without profile function are lost.

§ Import blocked users

If you do not select this option, only users whose accounts are not blocked will be imported.

If you import these users, you can enable their accounts by activating the checkbox **Enable blocked users**.



OS|Directory Synchronization configuration

User and group import configuration

Settings for user and group import

Settings

☐ Write log file

Log path:

☐ Rename import file after processing

☑ Refresh existing groups

☑ Refresh existing users

☐ Import object expressions

☐ Import object rights

☑ Import/update workflow users

☑ Import group relations of users

☐ Add group mappings of users

☑ Import profile relations of users and groups

☐ Import/refresh DMS supervisor

☐ Remove existing profile users

☑ Import blocked users

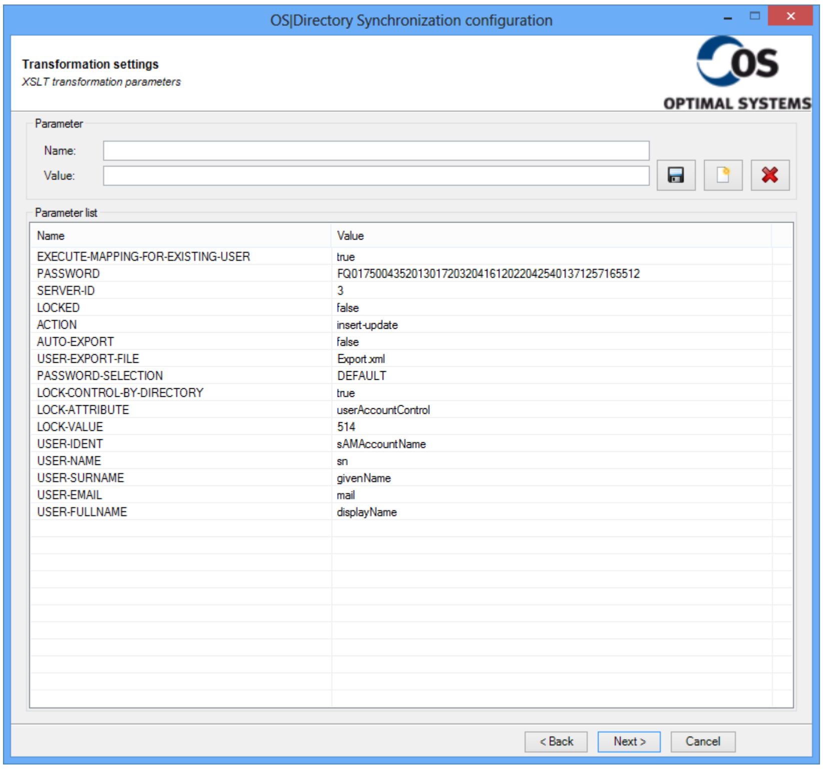
☐ Enable blocked users

Then click **Next** to continue with the configuration.

Transformation settings

The XSLT transformation parameters are displayed in this step.

If necessary, they must be adapted to the data of your Directory.



Transformation settings

XSLT transformation parameters

Parameter

Name:

Value:

Parameter list

Name	Value
EXECUTE-MAPPING-FOR-EXISTING-USER	true
PASSWORD	FQ017500435201301720320416120220425401371257165512
SERVER-ID	3
LOCKED	false
ACTION	insert-update
AUTO-EXPORT	false
USER-EXPORT-FILE	Export.xml
PASSWORD-SELECTION	DEFAULT
LOCK-CONTROL-BY-DIRECTORY	true
LOCK-ATTRIBUTE	userAccountControl
LOCK-VALUE	514
USER-IDENT	sAMAccountName
USER-NAME	sn
USER-SURNAME	givenName
USER-EMAIL	mail
USER-FULLNAME	displayName

Then click **Next** to continue with the configuration.

On the following page some configuration data are displayed. You can complete or cancel the configuration or go back to previous steps.

The configuration is saved as `configuration.xml`. If a configuration already exists, it is saved as `configuration.date.time.xml`.

XSLT Directory Synchronization

The automatic action 'XSLT Directory Synchronization' is also integrated via the `axacdirectorysync.dll` library.

The action does not include a configuration wizard.

The process logic corresponds to the 'Directory Synchronization' action:

§ Export of user and group data from enaio®

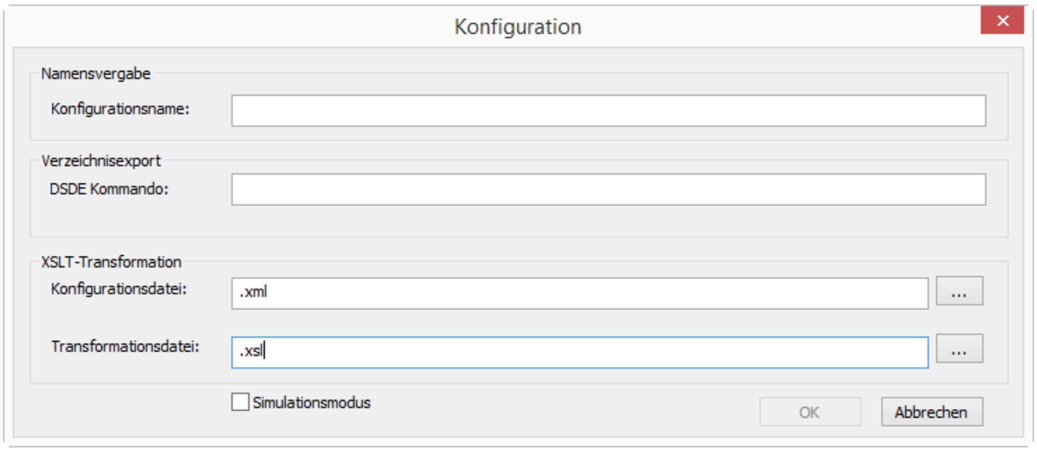
§ Export of data from an Active Directory

§ Transformation of data

§ Import of data into enaio®

Unlike the 'Directory Synchronization' action, data is exported from an Active Directory via a command line call and through which more complex mechanisms are possible than with DSDE queries.

Include an XML configuration file and an XSLT style sheet for the transformation.



Konfigurationsname:

DSDE Kommando:

Konfigurationsdatei: .xml

Transformationsdatei: .xsl

□ Simulationsmodus

The automatic action can be run in simulation mode. This will include all steps as far as import of the updated user and group data.

You can find sample files and further information in the directory …`components\XSLT Directory Synchronization logic`.

Please contact the support team or consulting team at OPTIMAL SYSTEMS if you want to use the 'XSLT Directory Synchronization' action.

Configuring the W-Module

Introduction to the W-Module

You must assign users or user groups and Windows templates in enaio® administrator for W-Document types set up in enaio® editor. A user can then choose between the configured Windows templates when creating a W-Document.

Templates can also be assigned to module-spanning document types.

You need the system roles 'Configuration of W-Module' and 'Configuration of security system' for W-template administration.

Windows templates link a Windows application with a file that is used as a template file and is opened when the Windows application starts. You can either specify the application during configuration or let enaio® client automatically determine it using the registered extension of the template file.

If the Windows template is linked with Microsoft Word, the template file may contain replacement fields. enaio® data-transfer can automatically replace these empty fields with index or archive data, or data from other archive documents.

To enable access to Windows templates, assign access rights to users and groups.

enaio® server administers template files in the `\etc\Templates` directory, making them available to users.

If you are working with multiple server groups, you have to copy the templates into the templates directory of each server group.

It is also possible to drag and drop W-Documents without having configured any application for a template, i.e. a file type. When opened, the operating system uses the file extension to determine the application to which the document must be handed over.

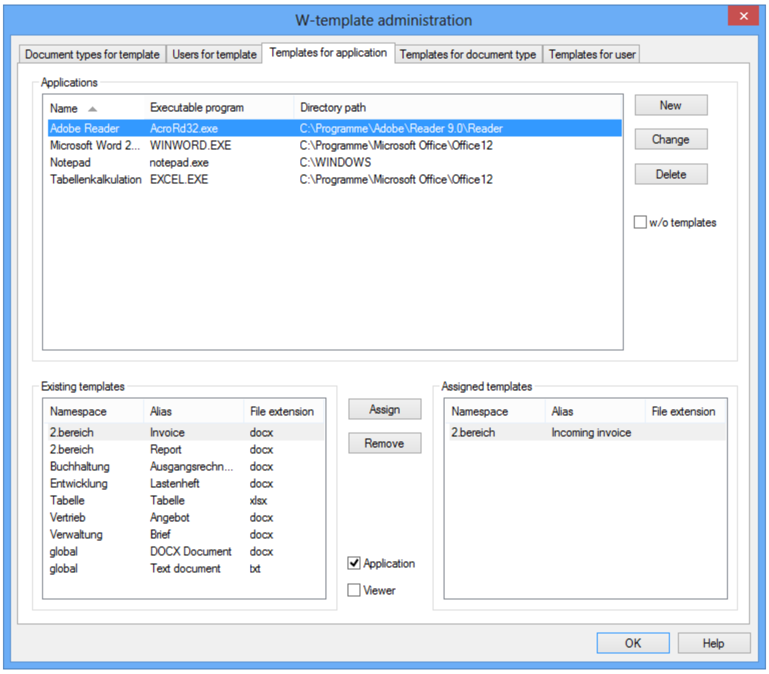
However, if there is no such association, the document cannot be opened.

This feature is enabled on the 'Documents.

Setting Up a Windows Application

Follow these work items to set up a Windows application:

1. Open the **W-template administration** window using the toolbar button W-module or the **Set up W-modules item** in the **Configuration** menu.
2. Open the **Template for application** tab.



W-template administration

Document types for template | Users for template | Templates for application | Templates for document type | Templates for user

Applications

Name	Executable program	Directory path
Adobe Reader	AcroRd32.exe	C:\Programme\Adobe\Reader 9.0\Reader
Microsoft Word 2...	WINWORD.EXE	C:\Programme\Microsoft Office\Office12
Notepad	notepad.exe	C:\WINDOWS
Tabellenkalkulation	EXCEL.EXE	C:\Programme\Microsoft Office\Office12

New | Change | Delete

□ w/o templates

Existing templates

Namespace	Alias	File extension
2.bereich	Invoice	docx
2.bereich	Report	docx
Buchhaltung	Ausgangsrechn...	docx
Entwicklung	Lastenheft	docx
Tabelle	Tabelle	xlsx
Vertrieb	Angebot	docx
Verwaltung	Brief	docx
global	DOCX Document	docx
global	Text document	txt

Assign | Remove

☑ Application

□ Viewer

Assigned templates

Namespace	Alias	File extension
2.bereich	Incoming invoice	

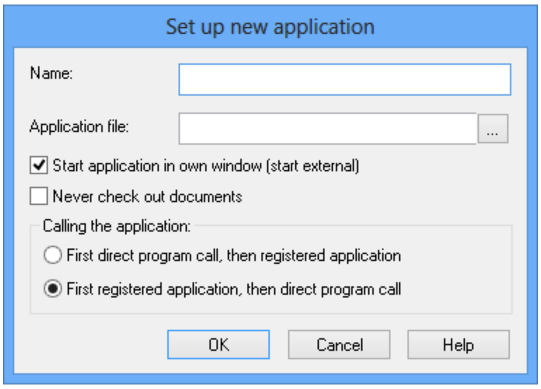
OK | Help

In the **Applications** area of this tab, you will find all applications that have already been set up.

The **Existing templates** section lists all templates that have been set up and the **Assigned templates** section lists all templates that are assigned to the selected application.

3. Click the **New** button in the **Applications** area.

   The **Set up new application** window will open.



Set up new application

Name:

Application file: ...

☑ Start application in own window (start external)

□ Never check out documents

Calling the application:

○ First direct program call, then registered application

● First registered application, then direct program call

OK | Cancel | Help

4. Enter a name and select a file using the file selection dialog.

   Applications can be started internally or externally. Externally, the application runs in a separate window, while internally it is integrated into the application window of enaio® client.

   Internally started applications do not offer to use enaio® office-utilities during document processing. We recommend to process files only in externally started applications and to use internally running applications as document viewers.

   If documents are not to be modified in the application, for example PDF files which are displayed by Acrobat Reader, you must activate the option **Never check out documents**.

Both the indicated path to the application and the registered file extension allow you to directly open an application.

If you choose to have the application started directly, it must be available at each workstation using the indicated path.

> Note: Select the option **First registered application, then direct application call** if you use MS Office applications, particularly in conjunction with enaio® office-utilities.

5. Confirm your entries with **OK**.

The data is saved and is displayed on the **Template for application** tab.

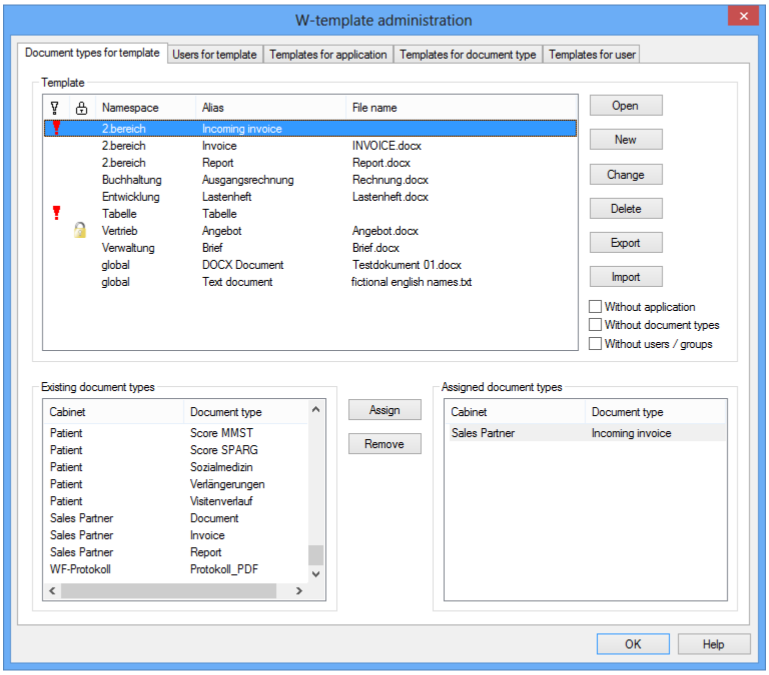
You can **Change** and **Delete** the applications. Before deleting the application entry, you must remove assigned templates.

You can assign templates to the applications.

Creating Windows Templates

Follow these work items to create a Windows template:

1. Open the **W-template administration** window using the toolbar button W-module or the **Set up W-modules item** in the **Configuration** menu.
2. Open the **Document types for template** tab.



		Namespace	Alias	File name
❗		2.bereich	Incoming invoice	
		2.bereich	Invoice	INVOICE.docx
		2.bereich	Report	Report.docx
		Buchhaltung	Ausgangsrechnung	Rechnung.docx
		Entwicklung	Lastenheft	Lastenheft.docx
❗		Tabelle	Tabelle	
	🔒	Vertrieb	Angebot	Angebot.docx
		Verwaltung	Brief	Brief.docx
		global	DOCX Document	Testdokument 01.docx
		global	Text document	fictional english names.txt

☐ Without application
☐ Without document types
☐ Without users / groups

Cabinet	Document type
Patient	Score MMST
Patient	Score SPARG
Patient	Sozialmedizin
Patient	Verlängerungen
Patient	Visitenverlauf
Sales Partner	Document
Sales Partner	Invoice
Sales Partner	Report
WF-Protokoll	Protokoll_PDF

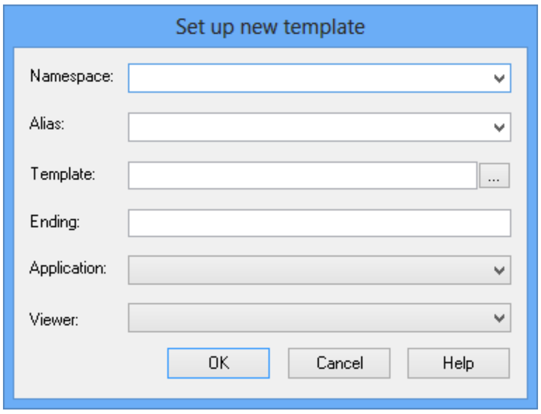
Cabinet	Document type
Sales Partner	Incoming invoice

In the **Template** area of the tab you will find the namespace and alias for each available template. Templates with a template file that has not been stored in enaio® server will be flagged with a red exclamation point in the first column. Templates with a template file that has been opened and not yet written back are flagged with a yellow lock (see 'Modifying Windows Templates').

In the **Existing document types** area, all available W-Document types and module-spanning document types are listed, while the **Assigned document types** area lists all document types that are assigned to the selected template.

3. Click the **New** button in the **Template** area.

   The **Set up new template window** will open.



4. Enter a **Namespace** and an **Alias**. Existing names can be chosen from the list. These names allow the user to select a template.
5. Select a template file using the file selection dialog (see 'Creating Template Files'). If you do not select a template file, the template will be flagged in the list with a red exclamation point.

   The extension of the selected template file will be preset in the **Ending** field.
6. Select the application to be run from the **Application** list. All applications that have been set up are shown in the list (see 'Setting Up a Windows Application').

   If you do not select an application, enaio® client will start the application automatically using the registered file extension of the template.

   The viewer is used once a W-Document is opened by a user who does not have the right to modify the document. Select the viewer from the list of all set up applications. If you do not select a viewer, the application will be used as viewer by default.

   The **Templates for application** tab also allows you to assign templates and applications.
7. Confirm your entries with **OK**.

The data will be saved and the new template will be shown on the **Document types for template** tab.

You can assign document types to the template here or on the **Application for document types** tab.

Both the **Users for template** and the **Templates for users** tab allow you to assign users and user groups to the template.

Creating Template Files

You must create the template file, which is indicated upon template creation, with the application that the template is assigned to.

The template file is the file that will start the application when being opened.

enaio® administrator copies template files to the `\etc\Templates` directory of the data directory and enaio® server makes them available to users.

For W-Templates that are associated with the Microsoft Word application, you can create template files containing replacement fields.

The 'Data transfer' macro will replace the replacement fields with content of index data fields or document content.

Further information can be found in the 'enaio® data-transfer' handbook.

> If you are working with multiple servers, you have to copy the templates into the templates directory of each server.

Assigning Windows Templates to a W-Document Type

A user can only create W-Documents if the W-Document type has at least one assigned Windows-template. Due to Windows templates, a Windows application is connected with a file that is used as a template and opened when starting the Windows application.

The **W-template administration** dialog offers the **Document types for template** tab on which you can assign document types to a template. You can assign templates to a document type on the **Templates for document type** tab.

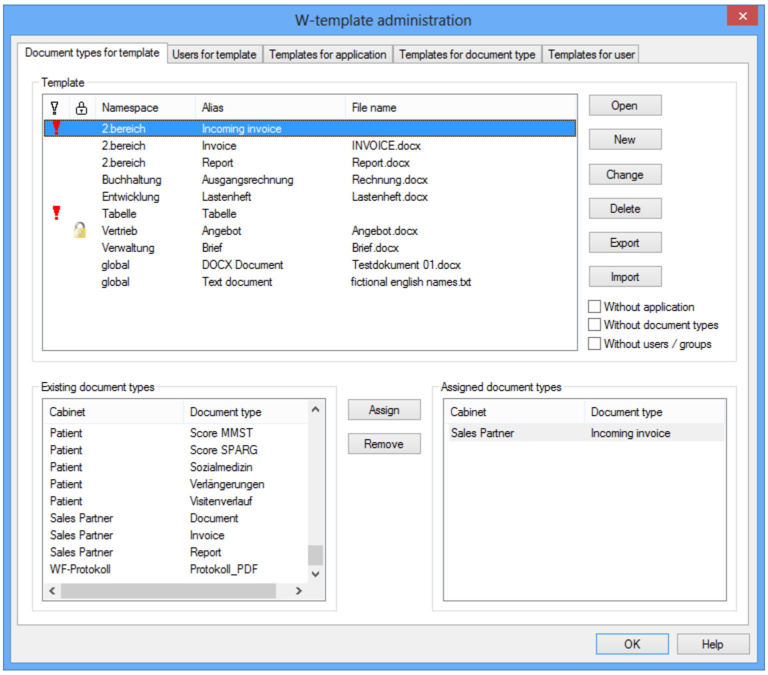
Templates can also be assigned to module-spanning document types.

> The assignments are automatically saved in the database.

Document Types for Template

You set up and edit templates in the **Template** area in the **Document types for template** tab.

All available templates are listed in this area. Use checkboxes to restrict the list to templates **Without application**, templates **Without document types**, and templates **Without users/groups**.


W-template administration
Document types for template
Users for template
Templates for application
Templates for document type
Templates for user
Open
New
Change
Delete
Export
Import
Assign
Remove
OK
Help

Template

		Namespace	Alias	File name
!		2.bereich	Incoming invoice	
		2.bereich	Invoice	INVOICE.docx
		2.bereich	Report	Report.docx
		Buchhaltung	Ausgangsrechnung	Rechnung.docx
		Entwicklung	Lastenheft	Lastenheft.docx
!		Tabelle	Tabelle	
	🔒	Vertrieb	Angebot	Angebot.docx
		Verwaltung	Brief	Brief.docx
		global	DOCX Document	Testdokument 01.docx
		global	Text document	fictional english names.txt

□ Without application
□ Without document types
□ Without users / groups

Existing document types

Cabinet	Document type
Patient	Score MMST
Patient	Score SPARG
Patient	Sozialmedizin
Patient	Verlängerungen
Patient	Visitenverlauf
Sales Partner	Document
Sales Partner	Invoice
Sales Partner	Report
WF-Protokoll	Protokoll_PDF

Assigned document types

Cabinet	Document type
Sales Partner	Incoming invoice

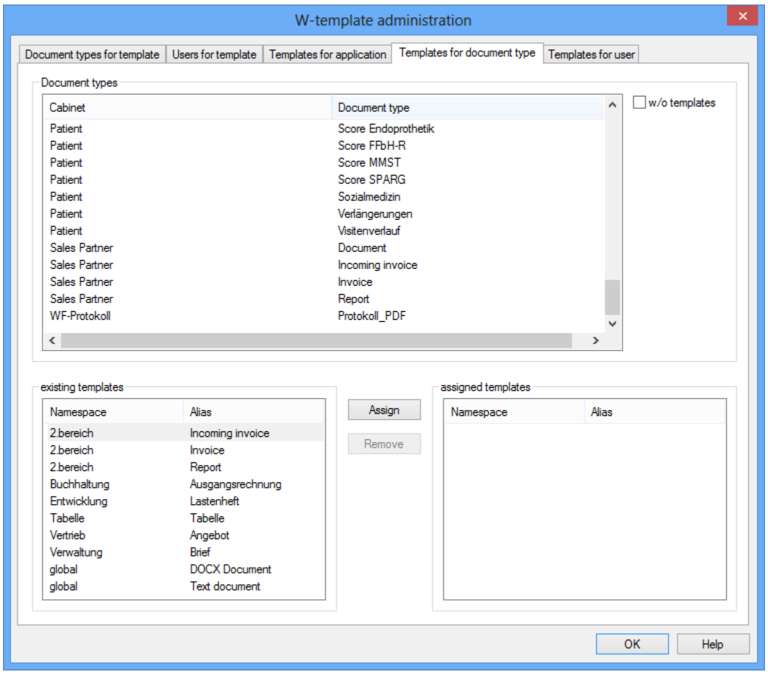
All configured W-Document types and module-spanning document types will be listed in the **Existing document types** area.

Use the **Assign** button to assign to a selected template the selected document types from the **Existing document types** area. They will be displayed in the **Assigned document types** area.

Use the **Remove** button to undo the document type assignment to a template.

Templates for Document Type

All W-Document types and module-spanning document types are listed in the **Document types** area on the **Templates for document type** tab. Use the checkbox **Without template** to limit the list to document types to which no template is assigned.


W-template administration
Document types for template
Users for template
Templates for application
Templates for document type
Templates for user
Document types
existing templates
assigned templates
Assign
Remove
OK
Help

□ w/o templates

Cabinet	Document type
Patient	Score Endoprothetik
Patient	Score FFbH-R
Patient	Score MMST
Patient	Score SPARG
Patient	Sozialmedizin
Patient	Verlängerungen
Patient	Visitenverlauf
Sales Partner	Document
Sales Partner	Incoming invoice
Sales Partner	Invoice
Sales Partner	Report
WF-Protokoll	Protokoll_PDF

Namespace	Alias
2.bereich	Incoming invoice
2.bereich	Invoice
2.bereich	Report
Buchhaltung	Ausgangsrechnung
Entwicklung	Lastenheft
Tabelle	Tabelle
Vertrieb	Angebot
Verwaltung	Brief
global	DOCX Document
global	Text document

Namespace	Alias

All available templates will be listed in the **Existing templates** area.

Use the **Assign** button to assign to a selected document type the selected templates from the **Existing templates** area. They will be listed in the **Assigned templates** area.

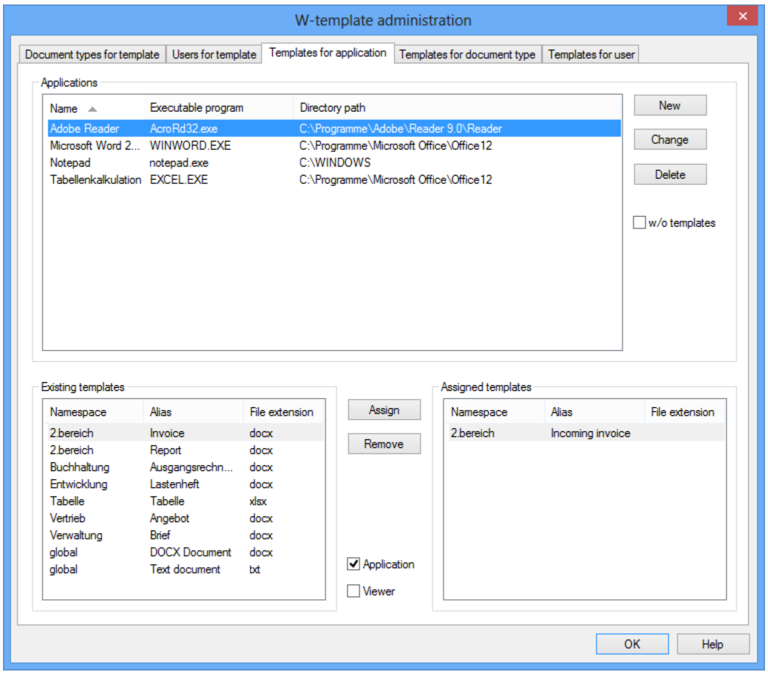
Use the **Remove** button to undo the template assignment to a document type.

Assigning a Windows Template to an Application

You can either assign an application and a viewer to Windows templates directly in the configuration dialog (see 'Setting Up a Windows Application') or on the **Templates for application tab**.

If you do not assign any application to a template, the application will start using the registered file extension of the template. If you do not select any viewer, the application will be used as viewer by default.

On the tab in the **Applications** area you can find a list of applications set up. Use the checkbox **Without template** to limit the list to applications to which no template is assigned.


W-template administration
Document types for template
Users for template
Templates for application
Templates for document type
Templates for user
New
Change
Delete
Assign
Remove
OK
Help

Applications

Name	Executable program	Directory path
Adobe Reader	AcroRd32.exe	C:\Programme\Adobe\Reader 9.0\Reader
Microsoft Word 2...	WINWORD.EXE	C:\Programme\Microsoft Office\Office12
Notepad	notepad.exe	C:\WINDOWS
Tabellenkalkulation	EXCEL.EXE	C:\Programme\Microsoft Office\Office12

☐ w/o templates

Existing templates

Namespace	Alias	File extension
2.bereich	Invoice	docx
2.bereich	Report	docx
Buchhaltung	Ausgangsrechn...	docx
Entwicklung	Lastenheft	docx
Tabelle	Tabelle	xlsx
Vertrieb	Angebot	docx
Verwaltung	Brief	docx
global	DOCX Document	docx
global	Text document	txt

☑ Application

☐ Viewer

Assigned templates

Namespace	Alias	File extension
2.bereich	Incoming invoice	

The **Existing templates** section lists all templates that have been set up and the **Assigned templates** section lists all templates that are assigned to the selected application as **Application** or as **Viewer**.

Use the **Assign** button to assign to a selected application the selected templates from the **Existing templates** area as **Application** or as **Viewer**. They will be listed in the **Assigned templates** area.

Use the **Remove** button to undo the template assignment to an application.

The assignments are automatically saved in the database.

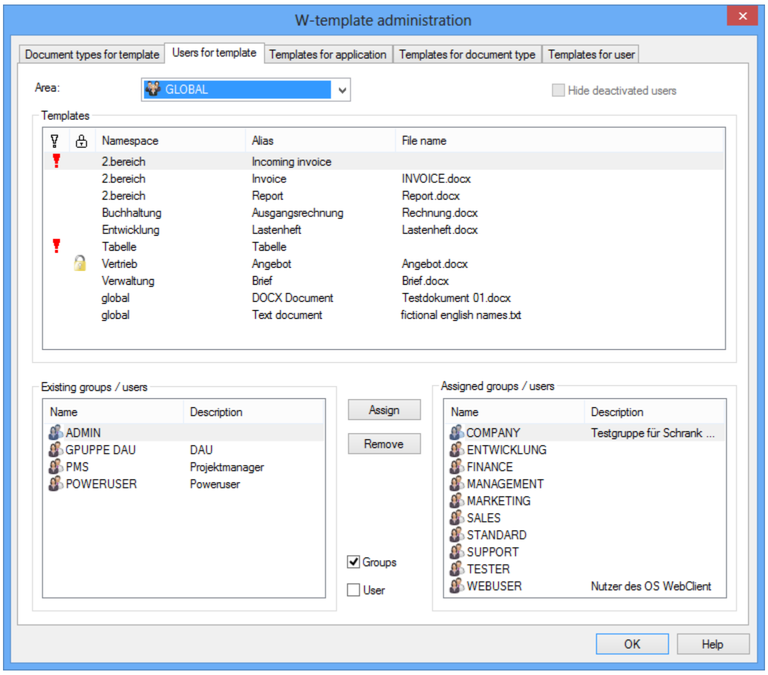
Assigning Windows Templates to Users

You assign Windows templates to user groups or individual users on the **Users for template** or on the **Templates for users** tab.

The assignments are automatically saved in the database.

The Users for Template Tab

All available templates will be listed in the **Templates** area of the **Users for template** tab.


W-template administration
Document types for template
Users for template
Templates for application
Templates for document type
Templates for user
Assign
Remove
OK
Help

Area: GLOBAL

☐ Hide deactivated users

Templates

		Namespace	Alias	File name
!		2.bereich	Incoming invoice	
		2.bereich	Invoice	INVOICE.docx
		2.bereich	Report	Report.docx
		Buchhaltung	Ausgangsrechnung	Rechnung.docx
		Entwicklung	Lastenheft	Lastenheft.docx
!		Tabelle	Tabelle	
	🔒	Vertrieb	Angebot	Angebot.docx
		Verwaltung	Brief	Brief.docx
		global	DOCX Document	Testdokument 01.docx
		global	Text document	fictional english names.txt

Existing groups / users

Name	Description
ADMIN	
GPUPPE DAU	DAU
PMS	Projektmanager
POWERUSER	Poweruser

☑ Groups

☐ User

Assigned groups / users

Name	Description
COMPANY	Testgruppe für Schrank ...
ENTWICKLUNG	
FINANCE	
MANAGEMENT	
MARKETING	
SALES	
STANDARD	
SUPPORT	
TESTER	
WEBUSER	Nutzer des OS WebClient

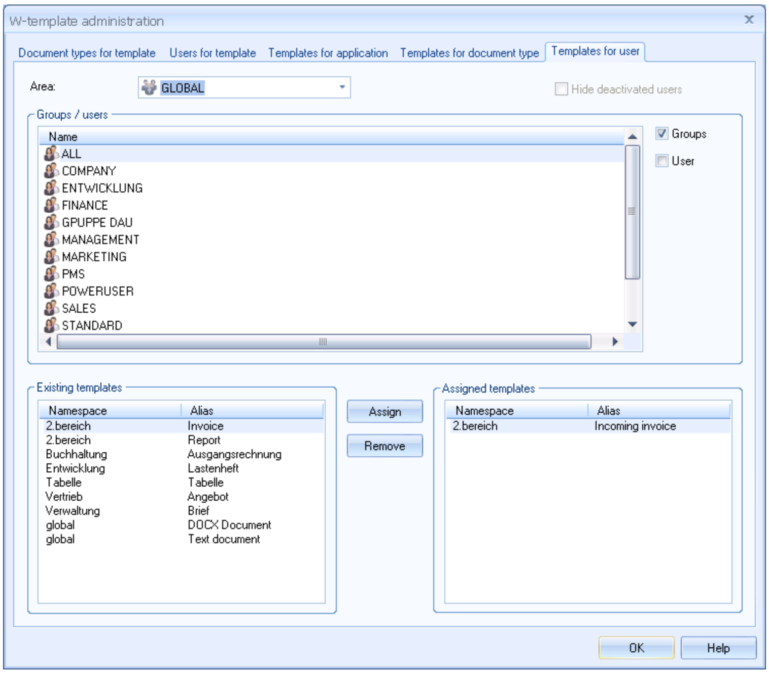
Either all available groups, users or both will be listed in the **Existing groups/users** and **Assigned groups/users** areas.

Use the **Assign** button to assign to a selected template the selected groups and users from the **Existing groups/users** area. They will be shown in the **Assigned groups/users** area.

Use the **Remove** button to undo the template assignment to groups and users.

The Templates for User Tab

Either all available groups, users or both will be listed in the **Groups/users** on the **Templates for users** tab.


W-template administration
Document types for template
Users for template
Templates for application
Templates for document type
Templates for user
Assign
Remove
OK
Help

Area: GLOBAL

☐ Hide deactivated users

Groups / users

Name
ALL
COMPANY
ENTWICKLUNG
FINANCE
GPUPPE DAU
MANAGEMENT
MARKETING
PMS
POWERUSER
SALES
STANDARD

☑ Groups

☐ User

Existing templates

Namespace	Alias
2.bereich	Invoice
2.bereich	Report
Buchhaltung	Ausgangsrechnung
Entwicklung	Lastenheft
Tabelle	Tabelle
Vertrieb	Angebot
Verwaltung	Brief
global	DOCX Document
global	Text document

Assigned templates

Namespace	Alias
2.bereich	Incoming invoice

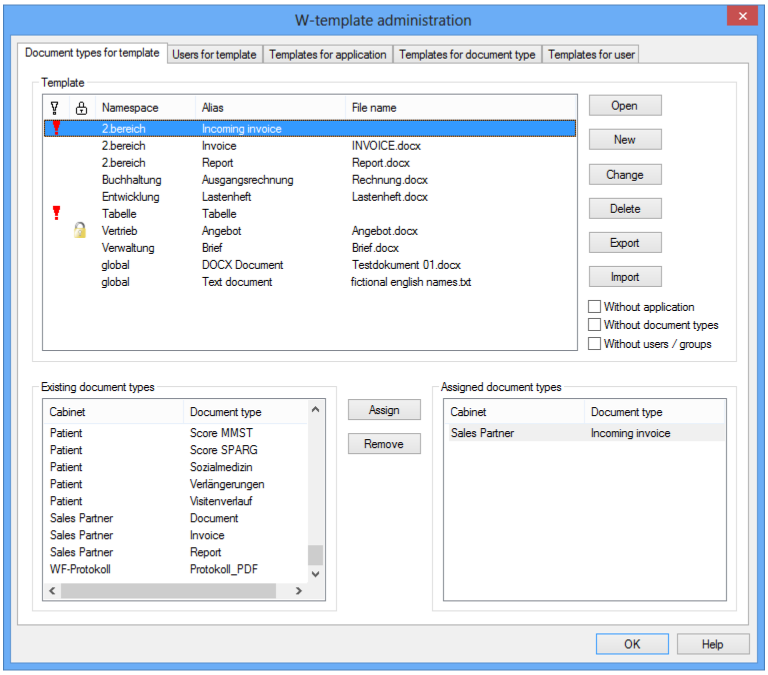
All available templates will be listed in the **Existing templates** area.

Use the **Assign** button to assign to a selected user or a selected group the selected templates from the **Existing templates** area. They will be listed in the **Assigned templates** area.

Use the **Remove** button to undo the template assignment to groups and users.

Modifying Windows Templates

Click the **Set up W-module** item in the **Configuration** menu to open the W-template administration in which you will find all templates set up in the **Template** area on the **Document types for template** tab. Use checkboxes to restrict the list to templates **Without application**, templates **Without document types**, and templates **Without users/groups**.



		Namespace	Alias	File name
!		2.bereich	Incoming invoice	
		2.bereich	Invoice	INVOICE.docx
		2.bereich	Report	Report.docx
		Buchhaltung	Ausgangsrechnung	Rechnung.docx
		Entwicklung	Lastenheft	Lastenheft.docx
!		Tabelle	Tabelle	
	🔒	Vertrieb	Angebot	Angebot.docx
		Verwaltung	Brief	Brief.docx
		global	DOCX Document	Testdokument 01.docx
		global	Text document	fictional english names.txt

□ Without application
□ Without document types
□ Without users / groups

Cabinet	Document type
Patient	Score MMST
Patient	Score SPARG
Patient	Sozialmedizin
Patient	Verlängerungen
Patient	Visitenverlauf
Sales Partner	Document
Sales Partner	Invoice
Sales Partner	Report
WF-Protokoll	Protokoll_PDF

Cabinet	Document type
Sales Partner	Incoming invoice

Templates can be flagged with the following icons:

🔒 The template file has been opened for editing and has not yet been closed. Using the **Edit template** dialog, reassign the edited template file.

! Either no template file has yet been specified for the template or the assigned template file is not available in the templates directory. Using the **Edit template** dialog, specify a template file.

You can perform the following operations on selected templates:

Open – The template file will be opened in the specified application and can be modified. In the list, the template will be marked with a yellow lock. Having modified the template file, save it to any location and open the **Edit template** dialog in order to reassign it to the template. The yellow lock with then disappear.

Change – The **Edit template** dialog will open in which you can change the template settings.

Delete – The selected template will be removed from the template administration. If document types are assigned, you must firstly remove the assignment.

Export – The configuration of the W-template administration can be exported. Use the export dialog to specify in detail which settings from the W-template administration settings are to be exported. Export files will be saved in XML format.

Import – A configuration file of the W-template administration can be imported. Assignments will only be imported if the name as well as the internal name of a W-Document type in the export file corresponds exactly to the W-Document type in the import system.

Changes are automatically saved in the database. If you delete templates from the template administration, the template files in the `\etc\Templates` template directory will not be deleted.

Configuration of the Archive Print

Introduction to the Archive Print

A user can place W-Documents as image documents into the archive with the enaio® printer.

Printer drivers for black and white printing and for color printing can be installed optionally during the installation of enaio® client.

The printer driver for black and white printing creates a black and white image from a W-File in TIFF G4 format or a PDF file. The printer driver for color printing creates a color image in JPEG format or a PDF file. PDF files created in this way are images integrated into the PDF format.

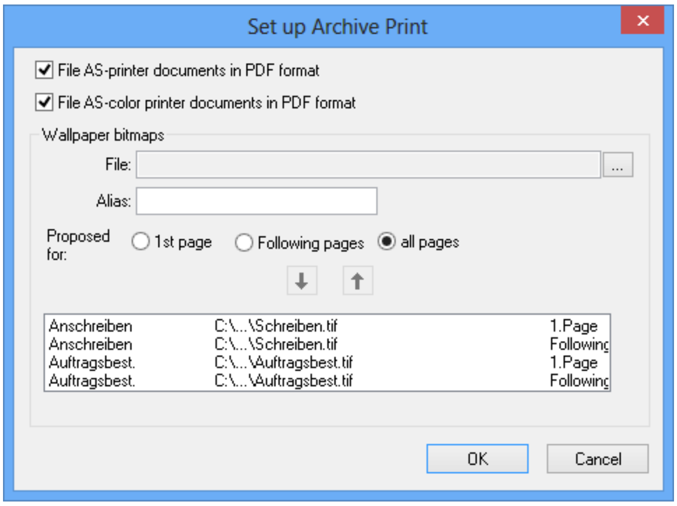
For black and white printing, you can provide the user with background images that they can integrate. These background images must be available as black and white bitmaps in TIFF G4 format and have the same size as the document pages.

When a user uses the printer driver to save a W-Document to the archive as an image document, he must specify the location, choose the document type and index the document.

Archive Print Formats

The archive print dialog allows you to select the format for black and white as well as for color prints.

Open the dialog by selecting the **Set up archive print** item from the **Configuration** menu.



Set up Archive Print

☑ File AS-printer documents in PDF format

☑ File AS-color printer documents in PDF format

Wallpaper bitmaps

File:

Alias:

Proposed for: ○ 1st page ○ Following pages ● all pages

Anschreiben	C:\...\Schreiben.tif	1.Page
Anschreiben	C:\...\Schreiben.tif	Following
Auftragsbest.	C:\...\Auftragsbest.tif	1.Page
Auftragsbest.	C:\...\Auftragsbest.tif	Following

Select **File AS-printer documents in PDF format** to create a black and white copy of the document in PDF format.

Select **File AS-color printer documents in PDF format** to create a color copy of the document in PDF format.

Having selected the PDF format, the user can open a confirmation dialog available in his settings menu in enaio® client and, instead of PDF, select TIFF G4 for black-and-white prints and JPEG for color prints with the AS printer before printing. If you want to enable users to select these options in the confirmation dialog, add the following entry in the `[ASPRINT]` section of the `as.cfg` file of the `etc` directory:

```
DDOCFORMAT=1
```

```
PDOCFORMAT=1
```

Using PDF format, the user can assign the document to a W document type or a module-spanning document type. If you want to make image document types available to users, add the following entry in the `[ASPRINT]` of the `as.cfg` file of the `etc` directory:

```
PDFForInternView=1
```

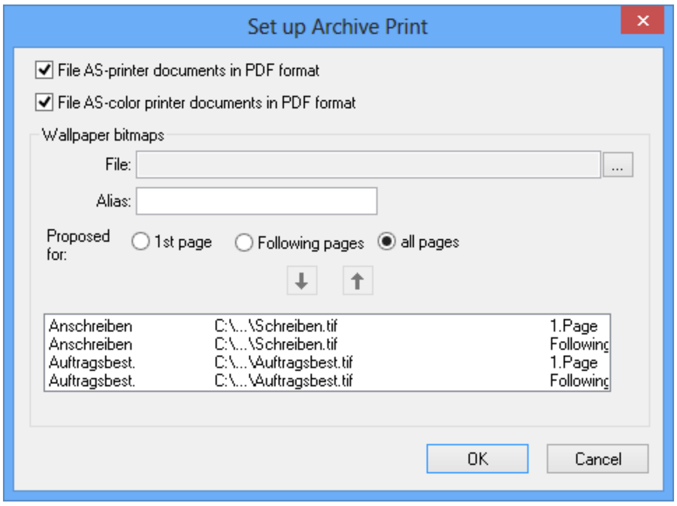
For black and white printing with enaio® printer the user will only be proposed D document types or, respectively, P document types for color printing.

Integrating Background Images

Follow these work items to integrate background images for black and white printing:

1. Open the **Configuration** menu and select the **Set up archive print** item.

   The archive print dialog will open for setup.



☑ File AS-printer documents in PDF format

☑ File AS-color printer documents in PDF format

Proposed for: ○ 1st page ○ Following pages ● all pages

Anschreiben	C:\...\Schreiben.tif	1.Page
Anschreiben	C:\...\Schreiben.tif	Following
Auftragsbest.	C:\...\Auftragsbest.tif	1.Page
Auftragsbest.	C:\...\Auftragsbest.tif	Following

2. Use the file selection dialog to enter a file into the **File** field, which will be integrated as a background.

   The file must be available in TIFF G4 format and have the same size as the document pages. The file must be accessible to all users at the specified location.

3. In the **Alias** field enter an alias, which users can use to select a background.

4. Define whether the file is to be used as the background for the **1st page**, the **Following pages** or **All pages**.
5. Transfer the entries to the list with the arrow buttons.
6. Confirm your entries with **OK**.

You can delete a background image by selecting it in the list and transferring it out of the list with the arrow button.

> Background images are only available for black and white printing by use of enaio® printer.

Configuring the XML Module

Introduction to the XML Module

The XML module is used to administer XML data in the archive. XML data are displayed in a browser using corresponding style sheets.

To each XML document type you can assign any number of style sheets. One of these must be defined as the default style sheet. When opening an XML document, the default style sheet is used for display in enaio® client. You can choose a different style sheet from the list of assigned style sheets.

> The Microsoft XML Parser 4.0 or higher is used. The library required for this purpose is saved to the system directory and registered when enaio® is installed. Internet Explorer must also be installed at the workstation.

In order to define that the XML module is not available for module-spanning document types, add the following entry to the `\etc\as.cfg` configuration file of the data directory:

```
[SYSTEM]

XMLOBJECTMENUMODE=1
```

Style Sheet Administration

Style sheets are assigned to document types by adding entries in the `as.cfg`file.

The `as.cfg` file is found in the directory `\etc` of the data directory. You can edit the file with any editor.

Style sheets also require the object type of a document type. Either use enaio® editor or the **Object information** in enaio® client to determine the object type.

Add the section [XML] to the `as.cfg` configuration file, indicate the object types and assign style sheets to them. The sequence of the entries in the section is not important.

Example:

```
[XML]
objekt(458752)=Tabelle,Grafik
Tabelle=tabelle.xsl;html
Grafik=grafik.xsl;svg
default(458752)=Grafik
```

Use the object type to indicate a document type and, as shown in the second line of the example above, assign all style sheets to it.

Enter the file name of each style sheet in a separate line. Indicate the file type of the output file, separated by semicolon, behind the file name. All style sheets are to be saved to the \etc\templates directory of the data directory.

You can optionally indicate a default style sheet for each object type in a separate line.

The Electronic Signature

Introduction to the Electronic Signature

OPTIMAL SYSTEMS GmbH has issued a manufacturer declaration, declaring the enaio® signature module to be a signature component which allows you to provide data for the creation or validation process of qualified digital signatures and to verify qualified electronic signatures or qualified certificates and to show the results of these examinations, meeting all requirements of the signature law and the signature decree.

Make sure that in Adobe Reader under **Edit > Preferences > Internet** the option **Show PDF in browser** is activated at each workstation where documents are signed. If this option is disabled, the signature module will not open.

Different signature modules are available: Mentana, SecSigner, and Governikus.

Functionality:

	Mentana	SecSigner	Governikus
Image module	Internal signature of a PDF	External signature	Internal signature of a PDF
Windows module	External signature if not already present as PDF	External signature	External signature if not already present as PDF
Video module	No signature	No signature	No signature
E-mail module	External signature	External signature	External signature
XML module	External signature	External signature	No signature
Container module	No signature	No signature	No signature
Sign several documents as batch in succession	Yes	no	Yes

Do not switch from one digital signature module to another as this will cause errors. Please contact Consulting if you need to switch the signature module.

A password prompt may appear when documents are opened in signature mode for Mentana. For this, enter the following in the `as.cfg` file in the `\etc` directory of the data directory:

```
[Signature]

PwdForSigning=1
```

Mentana

An electronic signature including the information on the signature type can be appended to documents in PDF format.

Image documents that are not available as PDFs will be converted into PDF and signed by the features provided by Acrobat Reader. W-Documents which are not in PDF format, are signed using an external signature.

External signatures can also be appended to e-mail documents and XML documents.

For electronically signing of image documents, signature types are set up. When signing, users can then select a signature type from a list. The electronic signature is appended by the signature feature provided by the Acrobat Reader. The Acrobat Reader version 6 or greater is at least required.

When appending external signatures to W-Documents, e-mail documents and XML documents, the user does not need to choose a signature type.

If a card-reading device for digital signatures is installed at the workstation, the user needs a signature card and must enter a PIN.

The license key 'DIS' is additionally required at the workstation.

On 1 July 2008 the validity of the hash algorithm SHA-1 expired. Since enaio® Version 6.0 SPI all required components are updated automatically by the enaio® setup; the latest version of the Mentana certificate manager must be manually installed. The certificate manager must be obtained directly from Mentana.

According to the used hash algorithm, the `HashAlgo` entry in the `[Signature]` section in the `as.cfg` file of the `\etc` directory must be altered. The entry is preset with '1' and allows hash values with SHA-256. Changing the entry can generate hash values with SHA-386 ('2') or SHA-512 ('3'). The appended numbers indicate the length of the hash value, respectively. If required, enable the previously used hash algorithm SHA-1 by setting the `HashAlgo` value to '-1' or '0'.

Archived documents cannot be signed. External signatures are only archived during archiving if document histories are created and archived. You can specify this in enaio® editor.

Users can print a signature at verification. The style sheet `\clients\client32\verify.xsl` is used for the print.

SecSigner

With SecSigner, only external signatures are created. For this purpose, image documents are converted into PDF files, but other document types are not converted.

For external signatures, signature types are not available.

SecSigner requires appropriate soft- and hardware. These must be installed according to the manufacturer's instructions. Additionally, you must indicate the path to the SecSigner installation directory using the 'Path' environment variable.

Both for signing and verification, the external SecSigner components will be run.

The license key 'DIS' is additionally required at the workstation.

> Archived documents cannot be signed. External signatures are only archived during archiving if document histories are created and archived. You can specify this in enaio® editor.

To use SecSigner, open the **Electronic signature configuration** dialog and integrate the signature module 'SecCommerce SecSigner.' Further information is not necessary.

Governikus Signer Integration Edition

Governikus creates external signatures. Image documents are integrated into a PDF and signed internally like existing PDF documents. A signature type can be assigned to internally signed documents.

XML documents, container documents, and film documents are not signed.

You need the appropriate software and hardware for the Governikus Signer Integration Edition. These must be installed according to the manufacturer's instructions. Governikus Signer must be started before a signature.

External Governikus components are used both for the signature and for verification.

The license key 'DIS' is additionally required at the workstation.

> Archived documents cannot be signed. External signatures are only archived during archiving if document histories are created and archived. You can specify this in enaio® editor.

For Governikus, use the **Electronic signature configuration** dialog to integrate the 'Governikus' signature module. You can create signature types with signature text.

You can specify in the configuration file `GovernikusConfig.xml` in the `etc` directory of the data directory how many files a user must have viewed so that a signature is possible. 2% is preset. You can change this value.

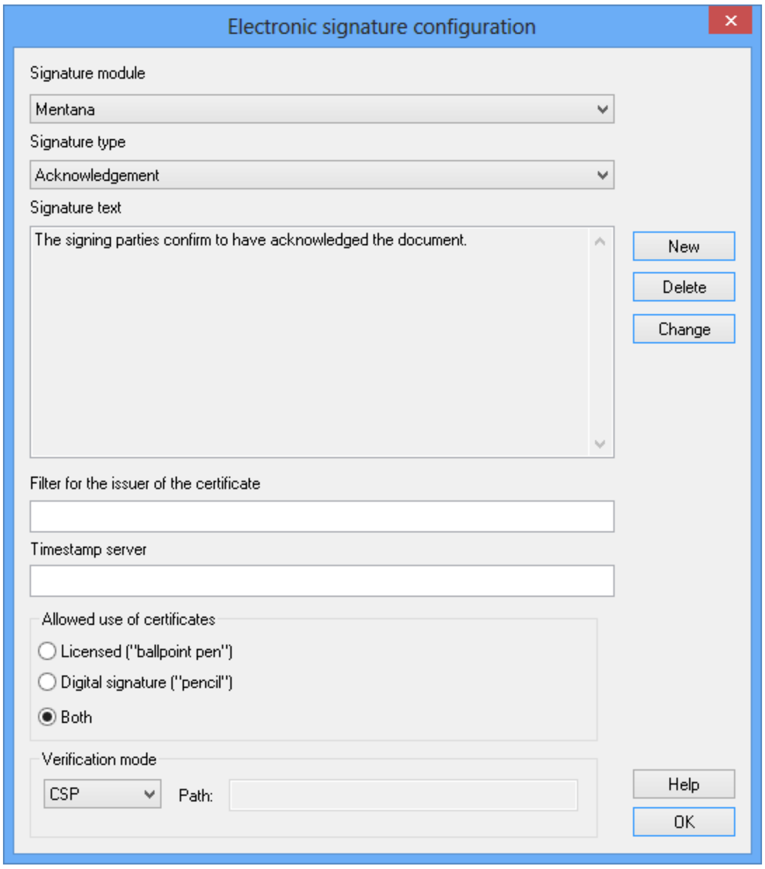
Configuration of Signature Types

You create signature types for the 'Mentana' signature module using the **Electronic signature** toolbar or using the **Electronic signature** item in the **Configuration** menu.

The **Electronic signature configuration** dialog will open in which you can enter the signature module and create and edit signature types.

1. Select the signature module by Mentana GmbH.

   You can create **New** signature types, delete or change them.



Electronic signature configuration

Signature module: Mentana

Signature type: Acknowledgement

Signature text: The signing parties confirm to have acknowledged the document.

Filter for the issuer of the certificate:

Timestamp server:

Allowed use of certificates

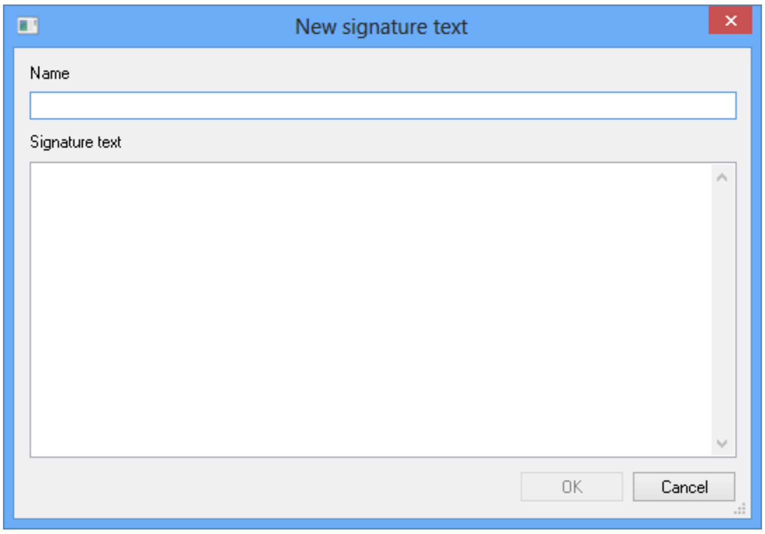
○ Licensed ("ballpoint pen")

○ Digital signature ("pencil")

● Both

Verification mode: CSP Path:

To create a new signature type, enter a **Name** with a maximum of 100 characters in the **New signature text** dialog and enter the **Signature text**. The maximum length of a signature text is equal to the maximum length of a field in your database. You can enter a line break in the field by pressing **Ctrl+Enter**.



New signature text

Name:

Signature text:

2. Confirm with **OK** to save the signature type.

Depending on the qualification of the signature, it may be necessary to integrate a timestamp server which is used to synchronize a signature's time stamp. The URL of the timestamp server is to be entered into the respective field.

If multiple certificates from different certificate providers are accessible, you can activate a filter for users in enaio® client. By entering text, only the certificates of those providers whose names are part of the entered text will be displayed in enaio® client.

What is more, you can decide whether to show certificates for which the valid properties **Licensed ('ballpoint pen'), Digital signature ('pencil')** or **Both** is selected.

There are the following options for the verification mode:

- CSP

  Certificate Status Protocol
- OCSP

  Online Certificate Status Protocol
- LDAP

  Indicate the path to the directory service when selecting this protocol.
- HTTP

  Indicate the path to the directory service when selecting this protocol.

Indicate just the signature type and signature text with no information about certificates for Governikus Signer Integration Edition.

Administration of enaio® client

Introduction to enaio® client Administration

Some settings in OS|Client cannot be modified by users and must be configured by an administrator. In addition to the settings on the 'Start' tab that are defined in enaio® administrator (see ''Start' Tab'), administrators can adjust configuration files and, if necessary, distribute them to the users.

Start Parameters for enaio® client

The following parameters can be specified when starting enaio® client:

`-uid`	User name
`-user`	For user names with spaces: value in quotation marks, mask with quotation marks
`-pwd`	Password
`-password`	For passwords with spaces: value in quotation marks, mask with quotation marks
`-srv`	Server#Port
`-n`	No startup screen
`-i`	Register

Example:

```
ax.exe -uid user -password " My PW" -srv osserver#4040 -n
```

In order to register under Microsoft Windows Vista, the logged in user needs administrative rights. In addition, the User Account Control must be disabled.

Information Page in enaio® client

An information page in German, English, and French is available. It is displayed by default after the client starts up, and it is shown in the content and display preview if no hit list or index data form of an object is open. The respective language version of the information page is displayed according to the language setting in enaio® client.

The files `os_defaultinfo.htm`, `os_defaultinfo_en.htm`, , and `os_defaultinfo_fr.htm` can be found in the directory …`\clients\client32`.

The information pages can be individualized. To do so, create separate pages and replace the files in the directory …`\clients\client32`.

Search Area

A query in enaio® client is done via the current version of the objects' index data. If object types are configured in enaio® editor in such a way that different index data versions are saved, the user can extend the search to all versions. To do so, press and hold Shift when you start the query.

This feature is not available for searches against basic parameters, multiple fields, tables, the full text and for combined searches.

You can enable this feature with an entry in the configuration file `as.cfg` in the directory `\etc` of the data directory:

```
[SYSTEM]
QUERYALLINDEXDATAVERSIONS=1
```

Value '0' turns the extension of the search area off.

This feature is available only in enaio® client, it cannot be used in enaio® web-client and with interfaces. The feature is not described in the enaio® client handbook.

Due to the memory- and processor-intensive access to the database, a significantly higher scaling of the system might be necessary.

Before extending the search area, please consider the following:

§ An index from the osguid column in the `osobjhist` table should be created.

  Example: `create index osobjhist_osguid on osobjhist(osguid)`

§ In all shadow tables of all objects in which the index data history is maintained (e.g. root4s, object6s, …) an index at the `osguid` column should be created.

§ Similar to the search fields in the project-specific tables (e.g. root4, object6), the fields which users will search for in the index data history (e.g. root4s, object6s, …) should be indexed as well.

  By doing so, the size of the respective tables changes significantly and thus the requirements for backup and hardware equipment so adjustments need to be made where necessary.

§ The respective database settings for indexing cannot be made in enaio® editor.

§ Creating indexes affects all writing operations of index data sets which can cause longer processing times when performing mass imports. In enaio® client, the performance of writing operations is not affected considerably.

Default search

Users have many options for searching for objects in enaio® client. The default search is a search for object-type-specific index data forms and a full-text search.

If users and user groups should only be able to search using saved queries, the default search can be switched off for the users and user groups concerned using the 'Run default search' system role.

Then all object types are not shown in the **Object search** area and all corresponding functions are hidden on the **START** tab in enaio® client.

Display of OS Files

OS files, i.e. references to documents managed in enaio® are opened via the `AxOutlookPreview.exe` display module.

The display module is automatically installed with enaio® client into the directory…`\clients\client32` and registered by enaio®-Setup. enaio® client is then used as a default application for showing OS files. This way, OS files will always be opened with enaio® client.

If more than one enaio® client application are installed on the same workstation, the most recently installed application is used to open OS files.

The display module enables you to determine the applications used to display documents managed in enaio®.

There are the following options:

§ Default programs

Documents will be opened with the default programs that were configured on the workstation for the respective file extensions. For example, MS Office Word will open DOC and DOCX files, and MS Office PowerPoint will open PPT files.

§ enaio® client

Documents will be opened in enaio® client.

§ enaio® webclient

Documents will be opened in enaio® webclient.

§ enaio® documentviewer

Documents will be opened in enaio® documentviewer.

The respective applications for document display can be specified in the configuration file `AxOutlookPreview.exe.config`. This file can also be found in the directory …`\clients\client32` and can be edited with any editor.

In the `appsettings` section the following parameters are available:

Parameters	Values	Function
Mode	0=default programs 1=enaio® client 2=enaio® webclient 4=enaio® documentviewer	Only one mode can be set up. If no mode is set, enaio® documents will be opened in enaio® client. Depending on the mode, further parameters can be

		necessary.
ClientPath	Program path to enaio® client	For mode 1: The application path to enaio® client must be indicated if the `ax.exe` and `AxOutlookPreview.exe` files are not located in the same directory.
ContentViewerMode	0=documents and index data 1=documents 2=index data	For mode 4: You define which information is displayed in enaio® documentviewer.
OsEcmWebClientBaseUrl	Home URL for enaio® webclient	For mode 2: This URL is opened by the default browser. Example: http://www.optimal-systems.de/documentviewer/app/viewer
DocumentViewerBaseUrl	Service endpoint of DocumentViewer	The URL must not be indicated for use in the production system as it is read from the client registry file. You can, however, indicate the URL for mode 4 for redirecting by enaio® documentviewer, e.g. for test purposes. This URL to enaio® documentviewer is opened by the default browser.
Server	IP of enaio® server	For mode 0: IP address of enaio® server
Port	port of enaio® server	For mode 0: port of enaio® server
User	Name of the user who can log in to enaio® server.	For mode 0: User name of an enaio® user who has respective rights.
Password	User password	For mode 0: enaio® user password

As for enaio® documentviewer, it is not necessary to indicate the service endpoint of enaio® webservice for use in the production system because it is read from the client registry file. You can, however, indicate the URL in the `system.serviceModel` section for mode 0 to redirect enaio® webservice, e.g. for test purposes.

Example:

```
<client>
  <endpoint address="<Server-IP>:<Port>/osws/services/EcmWsMtom"
    binding="basicHttpBinding"
bindingConfiguration="EcmWsMtomSoapServiceSoapBinding"
    contract="WebService.OsecmWsPortType"
name="EcmWsMtomSoapBinding" />
</client>
```

Changes to service endpoints are not automatically transferred to the client registry file. To synchronize the client registry file with the values of the server registry file, perform an update of the client installation either with the enaio® setup, or synchronize both registry files with the tool `OS.UpdateLocalServiceRegistry.vbs` from the directory …`\clients\client32\samples`. In systems with multiple servers the registry entries are transferred by the server with the highest probability of connection, or, if the probability of connection is less than 50% for all servers, they are transferred by the server in the last line of the `[SERVERS]` section in the `asinit.cfg` file of the client.

Moreover, the display module `AxOutlookPreview.exe` can be deployed for integrating the preview files into e-mails (see 'Integration in Microsoft Outlook').

For more information about enaio® documentviewer and enaio® contentviewer, refer to the sections 'enaio® documentviewer' and 'enaio® contentviewer' in the 'Viewing Services' chapter.

The logging of `axoutlookpreview.exe` is also set up via`axoutlookpreview.exe.config`.

OS Files and Annotations on Layers

References to image documents from e-mail programs that open the image document in enaio® client, for example, can call up the layer administration when the image is displayed so that users can immediately create annotations.

A new dynamic, public layer is created and an annotation tool can be preselected.

The following entries in the `as.cfg` file in the `etc` directory of the data directory are required for this:

`[SYSTEM]`

`AUTOCREATEANNOTATION=1`

`AUTODEFANNOBJ=n`

The entry 'AUTODEFANNOBJ' is optional for an annotation tool:

Value	Tool

`0`	No preselection (default)
`1`	Freehand line
`2`	Text
`3`	Filled rectangle
`4`	Rectangle
`5`	Arrow
`6`	Ruler
`7`	Line
`8`	Highlighter
`9`	Note
`10`	Stamp
`11`	Link

The user requires the appropriate rights to dynamically public layers.

If no annotations are created, the layer is not saved when closed. If users wish to create a different type of layer, they must close and re-open the layer administration.

Archiving

Introduction to Archiving

Audit-proof archiving is one of the most important administrative tasks.

Audit-proof archiving is configured as an automatic action in enaio®. After configuration, automatic actions can automatically be run at regular intervals. This will reduce the administrative effort required after configuration.

The interaction of all corresponding factors is essential in order to guarantee that archiving duly meets the legal requirements. This just as much includes the procedures to be applied as the hardware deployed or the various software components.

It is recommended to have all aspects coming into question be regulated and evidenced by process documentation That is created by the liable operator. If required, OPTIMAL SYSTEMS can provide project support in this matter.

For all compliance storage solutions certified by OPTIMAL SYSTEMS enaio® provides archiving processes that fulfill legal requirements. Correct archiving of documents and physical retention periods are subject to restrictions of the storage system in use. If, for example, a compliance storage system is able to manage retention periods only until 2038, such a restriction cannot be compensated by an archiving software solution like enaio®.

To guarantee simple configuration and secure operation, enaio® provides tools and means for different certified archive storage systems. Nevertheless, keep in mind to follow the configuration steps described in the respective interface manuals.

It is therefore recommended to coordinate, realize, document, and test the planning of retention periods, the selection of an archive storage system and its configuration, the configuration of retention periods as well as necessary archive storage system settings in enaio®, and the correct configuration and execution of archiving processes with our consulting department.

Archive

Audit-proof archiving is set up as an automatic action (see 'Introduction to Automatic Actions'). The action 'Archiving' accesses the settings which you have configured in enaio® enterprise-manager. During configuration you have to specify which enaio® server archives which documents on which media.

Perform the following settings before configuring the automatic action 'Archive:'

§ Register the library `axacarch.dll`with the system (see ''Additions Tab').

§ Open the media administration in enaio® enterprise-manager and indicate the paths to media, set up media sets, assign media to media sets, and assign media sets to document types.

§ Furthermore define archiving options and configure the integrity checks in enaio® enterprise-manager.

Changes to media and archiving settings in enaio® enterprise-manager will usually apply after server restart.

All archiving processes will be logged. This log can be used to verify if archiving processes were successful.

If an e-mail server is available, the administrator can automatically be notified about complete archiving processes by e-mail.

Before archiving, the integrity of the documents to be archived can be verified by performing a hash check (see Validating Document Integrity').

Integration of Virtual Archives: iTernity/Centera/iXOS

An iTernity, Centera or iXOS system available in the network can also be used for archiving.

If so, create a virtual archive for the connection, set up a media set and assign document types to this media set for the available solution.

Media and paths to the media are not configured.

In the manner of archiving with enaio® server, the archiving process itself is carried out as an automatic action.

The following constraints apply:

§ The archiving options in enaio® enterprise-manager regarding the media and space management are not taken into account. enaio® server simply transfers the documents to the integrated system.

The integration of virtual archives requires an additional license key.

For NetApp and GRAU DATA, you set up media and media sets as with internal media management.

Retention periods

For documents enaio® manages two types of information in terms of retention periods: the retention period and the scheduled retention period. If this information is available for a document, it can be viewed in the **Object information** in enaio® client.

The retention period is set in the course of archiving with iTernity, Centera or NetApp system. In doing so, the scheduled retention period is entered as retention period. If no scheduled retention period is indicated, the retention period is determined according to the specified retention days. Using iTernity or Centera, retention days are specified when configuring the virtual archive drivers, and when using NetApp during the configuration of the media paths.

The planned retention period is assigned via scripts. It can be indicated and changed for archived as well as not yet archived documents. An evaluation is also possible via scripts and the COM interface.

The retention period of documents in Centera archives cannot be changed, the retention period of documents that are filed in a NetAPP, GRAU DATA Archive or iTernity archive can be changed by using the automatic action 'Edit retention period'.

> Please note that, if retention periods extend beyond 2038, NetApp archives may be prone to the year 2038 problem. To avoid this problem, select the appropriate option in the server properties (see 'Archiving').

Media Management in enaio® enterprise-manager

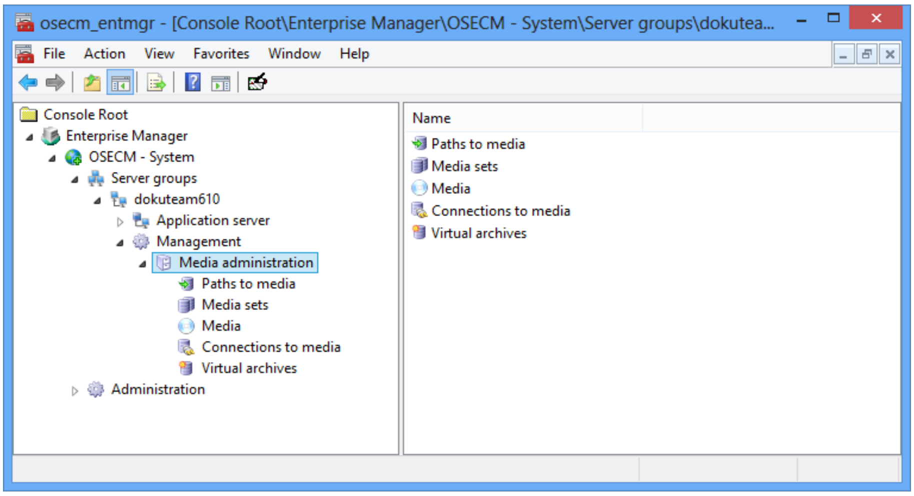
If the archiving is performed with a server or a server group, you must indicate the paths to the media on which the documents can be archived.

Within a server group, one server must be designated as the group control server. This server will be then used to query and modify media data.

The family control server of only one available server group is by default designated as the group control server. If there is a second server group, open the context menu of the intended server and designate it as the group control server with the item **All tasks > Set group control server**.

Media sets must be created and set up. Media sets are assigned to media on which archiving is done and the document types, which are archived on the assigned media.

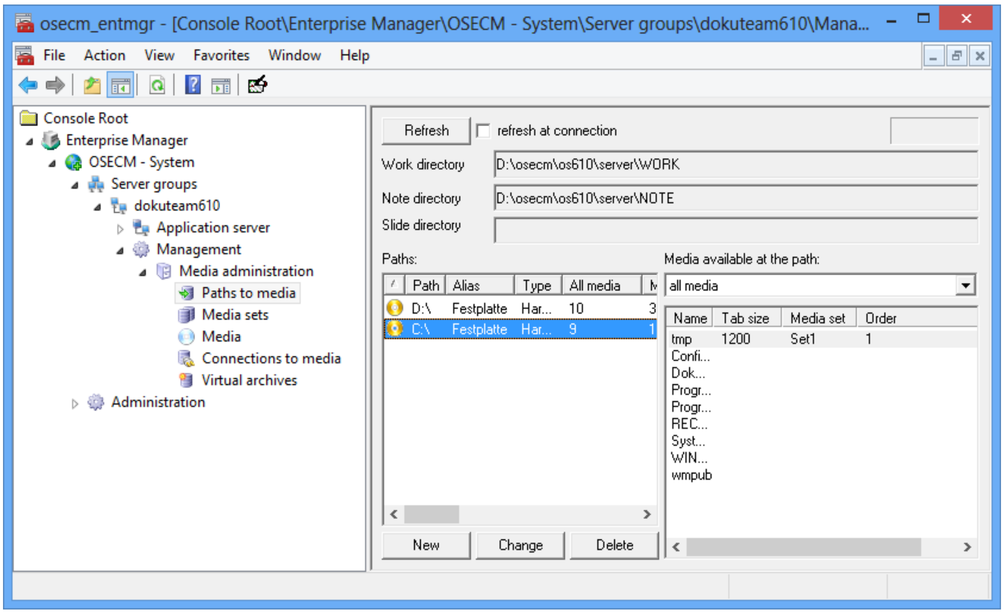
It is not necessary to assign document types to a media set for a server or a server group because other servers/server groups that are configured as main servers can archive the document types, given that the document type assignment has been set up. Auxiliary servers only ever archive their own documents (see 'Archiving options').



Paths to media

If you select **Paths to media** in the console root, the paths already set up to media are listed. If there are no entries, click the Refresh button to update the list.

All media found at the selected path will also be listed.



☐ refresh at connection

Work directory: D:\osecm\os610\server\WORK

Note directory: D:\osecm\os610\server\NOTE

Slide directory:

Paths:

Path	Alias	Type	All media	N
D:\	Festplatte	Har...	10	3
C:\	Festplatte	Har...	9	1

Media available at the path: all media

Name	Tab size	Media set	Order
tmp	1200	Set1	1
Confi...			
Dok...			
Progr...			
Progr...			
REC...			
Syst...			
WIN...			
wmpub			

You can filter the list of media according to:

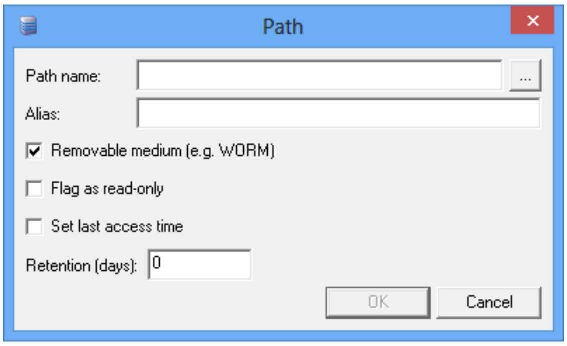
- **media entered in the database**

  The list will only offer media found at the selected path which have already been configured.

- **media not entered in the database**

  The list will only offer media found at the selected path which have not yet been configured.

Set up a new path via the **New** button.



Path name:

Alias:

☑ Removable medium (e.g. WORM)

☐ Flag as read-only

☐ Set last access time

Retention (days): 0

Enter a path name and an alias. Multiple aliases of a path allow you to set up archiving processes with different retention periods to the same path.

> Make sure that no other enaio® server archives into this area.

If you are working with removable media, select the respective option.

You can activate the property **Read-only** for all files that are filed to this path. The property may be required by other systems that you are working with, e.g. hierarchical storage management systems. This function requires a license key.

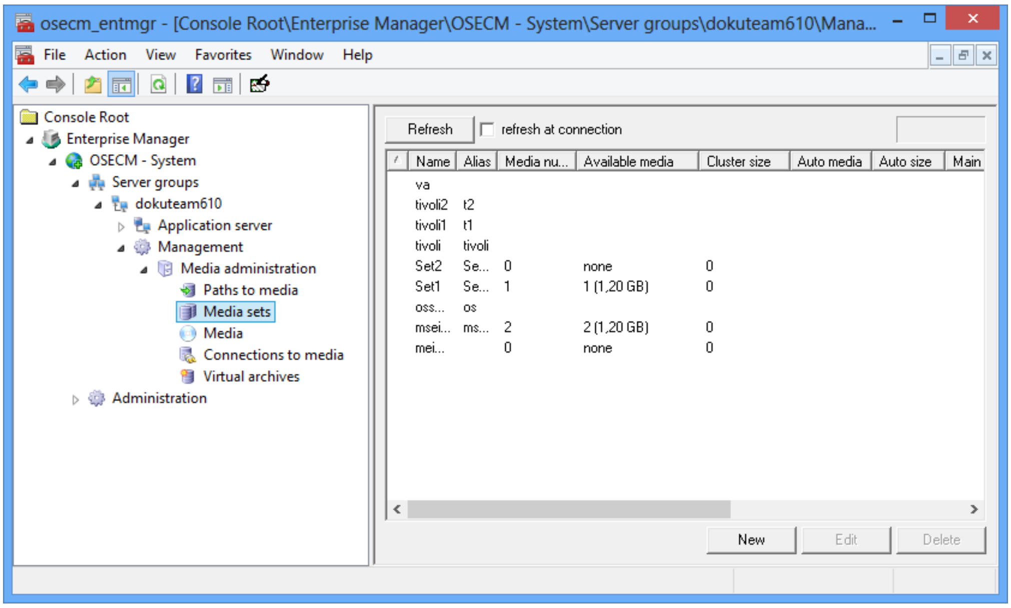
A retention period (in days) is necessary for the use of GRAU DATA and NetApp storage solutions. NetApp must be configured for the administration of retention periods.

Activate the property **Set last access time** for all paths which lead to GRAU DATA and NetApp storage media.

> You can only delete paths to media if neither media nor document types are configured for them.

Media Sets

If you select **Media sets** in the console root, media sets already set up are shown. If there are no entries, click the Refresh button to update the list.

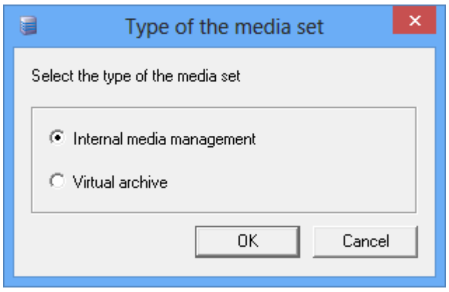


□ refresh at connection

Name	Alias	Media nu...	Available media	Cluster size	Auto media	Auto size	Main
va							
tivoli2	t2						
tivoli1	t1						
tivoli	tivoli						
Set2	Se...	0	none	0			
Set1	Se...	1	1 (1,20 GB)	0			
oss...	os						
msei...	ms...	2	2 (1,20 GB)	0			
mei...		0	none	0			

Media sets are set up using the **New** button in the **Media sets** area.

You can choose whether to create a media set for internal media management using enaio® server or a media set for a virtual archive (see below).

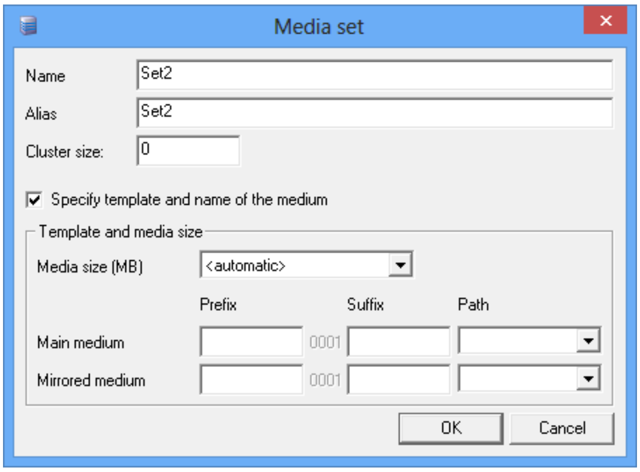


Select the type of the media set

● Internal media management

○ Virtual archive

For internal media management, the following dialog will open:



Media set

Name: Set2

Alias: Set2

Cluster size: 0

☑ Specify template and name of the medium

Template and media size

Media size (MB): <automatic>

	Prefix		Suffix	Path
Main medium		0001		
Mirrored medium		0001		

Enter a **Name** and optionally an **Alias**, and the **Cluster size**.

When archiving via a hard disk system or XenTERA, you can specify a **Template for the media name**. Media are thus not need to be set up.

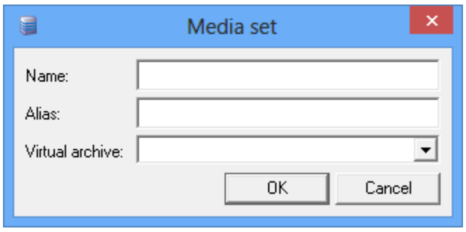
To define the template, select the **Media size** and enter the **Path**. The Main medium path just needs to be selected from the list which offers all already configured paths to media. Do not select a path to a **Mirrored medium** if you do not want mirrored media to be created.

Both media are named with a serial decimal number starting from `0001`. You can specify a prefix and a suffix for the name.

> Make sure that media names as well as environments with differing paths to media and several archiving server are unique throughout the entire system.

Media Sets for Virtual Archives

If you want to use a virtual archive as archiving location, you must set up a media set for it.



Media set

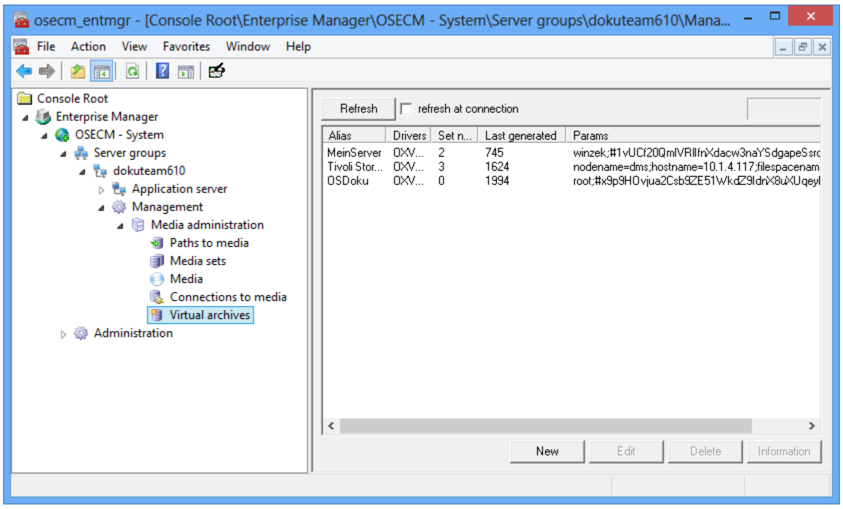
Name:

Alias:

Virtual archive:

To do so, enter a **Name** and optionally an **Alias**, then choose the virtual archive which has been set up.

The virtual archive is set up in the area **Media management > Virtual archives**.



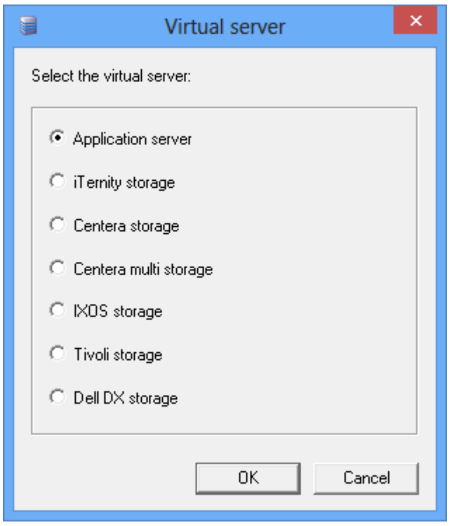
☐ refresh at connection

Alias	Drivers	Set n...	Last generated	Params
MeinServer	OXV...	2	745	winzek;#1vUCf20QmlVRllfnXdacw3naYSdgapeSsrc
Tivoli Stor...	OXV...	3	1624	nodename=dms;hostname=10.1.4.117;filespacenam
OSDoku	OXV...	0	1994	root;#x9p9HOvjua2Csb9ZE51WkdZ9IdnX8uXUqeyl

You need a license key to integrate virtual archives.

If you select a virtual archive that has already been set up, you get detailed information about the virtual archive via the **Information** button.

You create a new virtual archive using the **New** button. First, you must select the virtual archive type:



Select the virtual server:

● Application server

○ iTernity storage

○ Centera storage

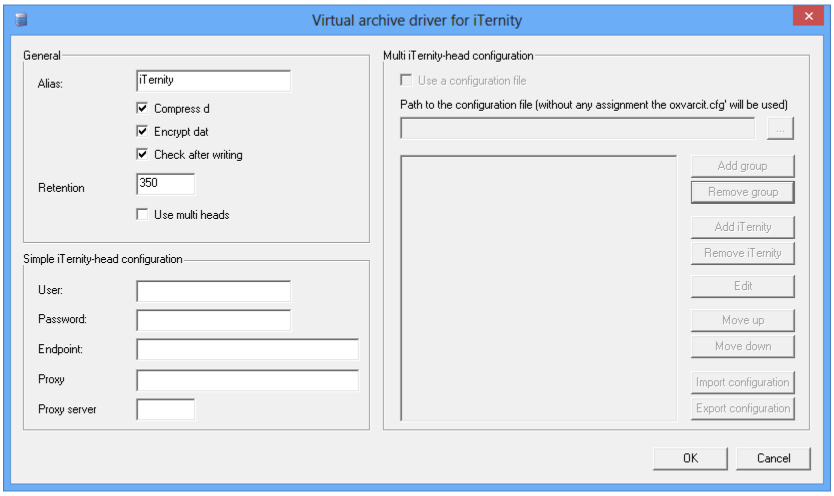
○ Centera multi storage

○ IXOS storage

○ Tivoli storage

○ Dell DX storage

iTernity:



Virtual archive driver for iTernity

General

Alias: iTernity

☑ Compress d

☑ Encrypt dat

☑ Check after writing

Retention 350

□ Use multi heads

Simple iTernity-head configuration

User:

Password:

Endpoint:

Proxy

Proxy server

Multi iTernity-head configuration

□ Use a configuration file

Path to the configuration file (without any assignment the oxvarcit.cfg' will be used)

Insert in the **Endpoint** field the URL of the Web service through which you can access iTernity.

The URL's structure is as follows:

```
http://<IP address>/iTernity/iTernity.asmx
```

Indicate `https` as the protocol if encrypted handover has been configured for iTernity users.

Enter the URL in your browser to check the connection. If the Web service is accessible, a page containing the documentation of the iTernity server will be displayed.

It is possible to compress the data before saving and to encrypt them. To prevent failures, you can have the data checked after storage by use of hash values in order to determine transmission errors.

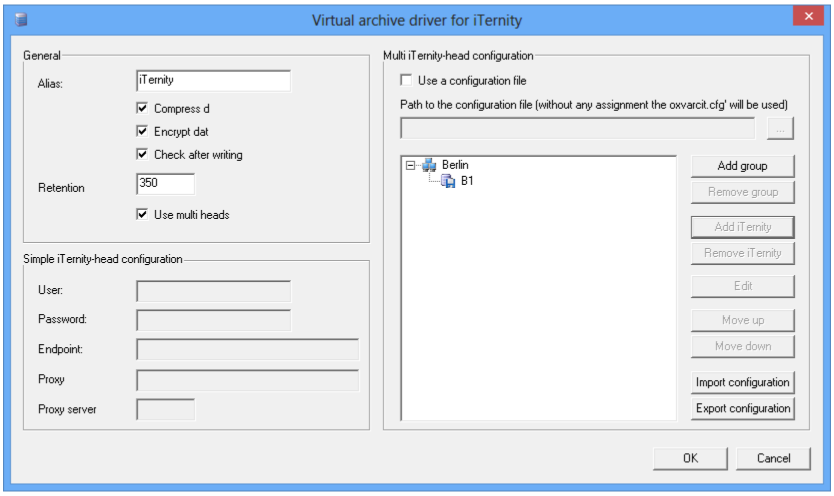
Documents can only be deleted once the retention period has expired.

If connections must be provided by a proxy server, indicate the server's port.

Use multi heads

Set up a configuration in case you use a multi head system. The configuration will be saved to the database and applies to all enaio® servers.

Different configurations for several enaio® servers must be set up in configuration files. Every server will access the configuration file that is indicated here. For this case, you thus need identically named configuration files which, in relation to respective server, are accessible at the path entered. If you do not indicate any path or file name, a configuration file named `oxvarcit.cfg` will be searched for in the …`\server` directory of all servers. You create configuration files by exporting a configuration.



Virtual archive driver for iTernity

General

Alias: iTernity

☑ Compress d

☑ Encrypt dat

☑ Check after writing

Retention 350

☑ Use multi heads

Simple iTernity-head configuration

User:

Password:

Endpoint:

Proxy

Proxy server

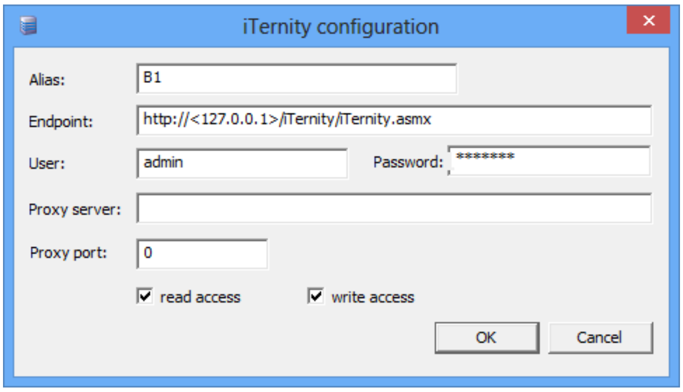
Multi iTernity-head configuration

☐ Use a configuration file

Path to the configuration file (without any assignment the oxvarcit.cfg' will be used)

Berlin
- B1

You create at least one group and assign at least one head to the group with the **Add iTernity** button:



iTernity configuration

Alias: B1

Endpoint: http://<127.0.0.1>/iTernity/iTernity.asmx

User: admin Password: ********

Proxy server:

Proxy port: 0

☑ read access ☑ write access

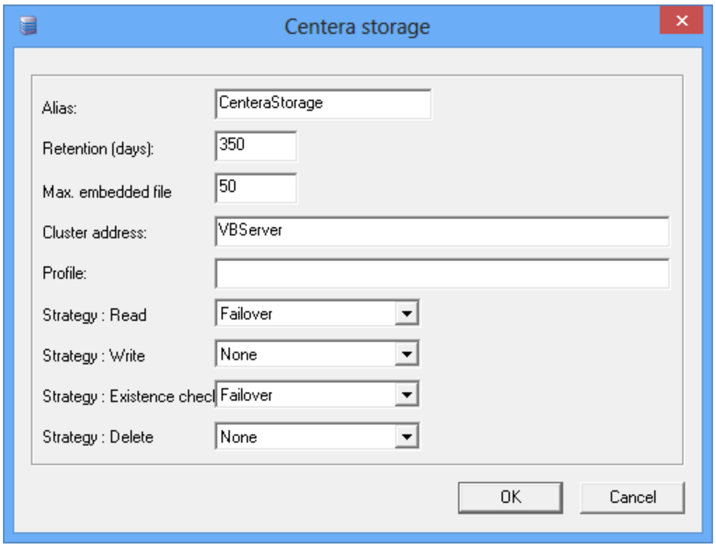
Decide whether you want to use the head for read access, write access or both.

The head of the first group is always used for read-only access and balances the load automatically. The head of the second group will attempt to access in case the head of the first group is not available.

Write access always takes place in the order of the groups and the heads in the groups. The server load is not balanced for write access.

You can save a configuration as a file using the **Export configuration** button.

Centera storage



Centera storage

Alias:	CenteraStorage
Retention (days):	350
Max. embedded file	50
Cluster address:	VBServer
Profile:	
Strategy : Read	Failover
Strategy : Write	None
Strategy : Existence checl	Failover
Strategy : Delete	None

Documents can only be deleted once the retention period has expired. The deadline begins with the date of archiving.

The maximum size for the storage of files in the content description files is indicated in KB. The value '0' deactivates the storage function. Files with a size up to 100 KB can be stored. If 'single instance storage' is activated, the storage of documents can have an impact on the system performance.

Enter the IP or the computer name as the **Cluster address**. Separate multiple addresses by comma in Centera multi cluster environments.

Insert the path and the name of a Centera access profile file into the **Profile** field. The path has to be entered relatively to the enaio® directory `\server`.

> If more than one enaio® server is applied, the Centera access profile file has to be copied to the respective directory of each enaio® server.

This file is needed to identify enaio® server as a user and to grant the necessary rights.

Specify strategies for read and write access, the existence check and deletion. The choice of the strategy depends on your Centera system.

§ Failover: If the action fails using the first address, it is repeated using the next address.

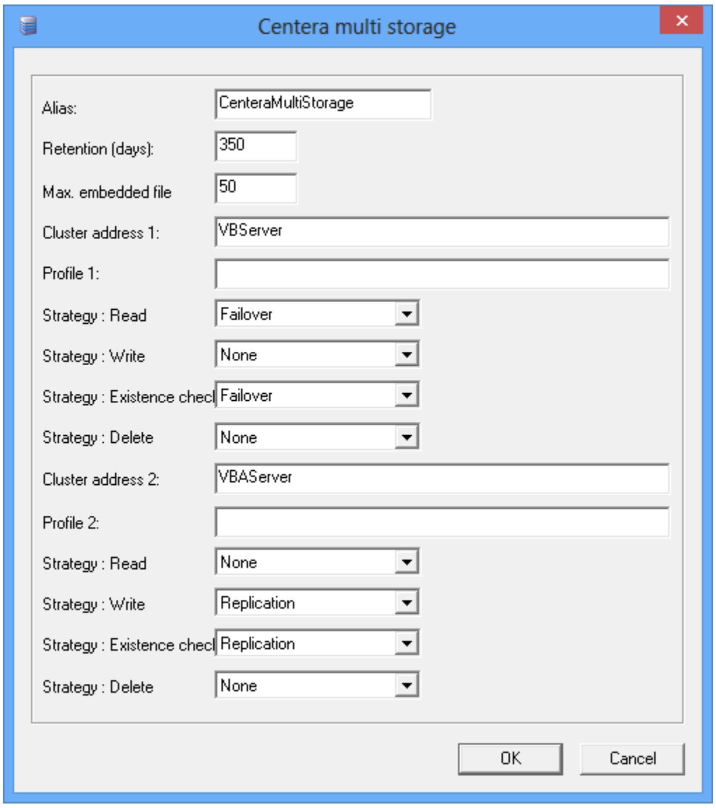
§ Replication: The action will always be repeated using the following cluster address.

§ None: The action is always exclusively executed using the first address.

Further information can be found in the section 'Multi cluster strategies' in the Centera documentation 'Programmer's guide'.

These strategies set up the communication between enaio® server and Centera. The strategies concerning failure safety and data security within a Centera system are not dependent hereof.

Centera multi storage

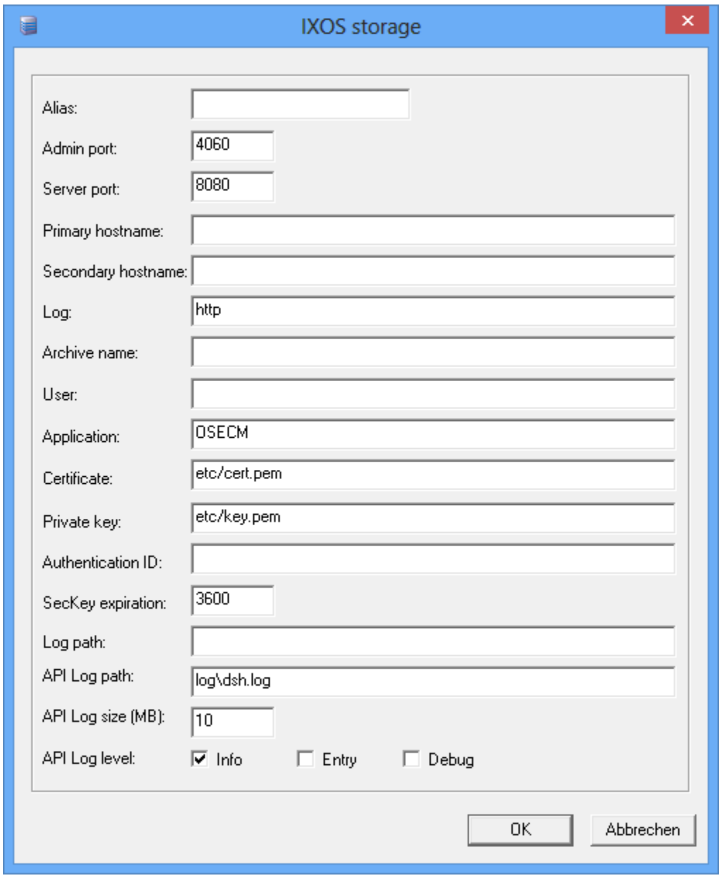


Alias:	CenteraMultiStorage
Retention (days):	350
Max. embedded file	50
Cluster address 1:	VBServer
Profile 1:	
Strategy : Read	Failover
Strategy : Write	None
Strategy : Existence checl	Failover
Strategy : Delete	None
Cluster address 2:	VBAServer
Profile 2:	
Strategy : Read	None
Strategy : Write	Replication
Strategy : Existence checl	Replication
Strategy : Delete	None

When using two Centera systems which are independent of each other choose the virtual server **Centera multi storage**.

Alias, amount of retention days and maximum size for the storage of documents in the content description files are equal for both Centera systems, but addresses, profiles and strategies need to be entered separately for both systems.

iXOS



Alias:	
Admin port:	4060
Server port:	8080
Primary hostname:	
Secondary hostname:	
Log:	http
Archive name:	
User:	
Application:	OSECM
Certificate:	etc/cert.pem
Private key:	etc/key.pem
Authentication ID:	
SecKey expiration:	3600
Log path:	
API Log path:	log\dsh.log
API Log size (MB):	10
API Log level:	☑ Info ☐ Entry ☐ Debug

Insert the communication data which enable the archiving with iXOS. Details can be found in the iXOS documentation.

The paths to the files which contain the certificate and the private key can be optionally entered relatively to the enaio® directory `\server`.

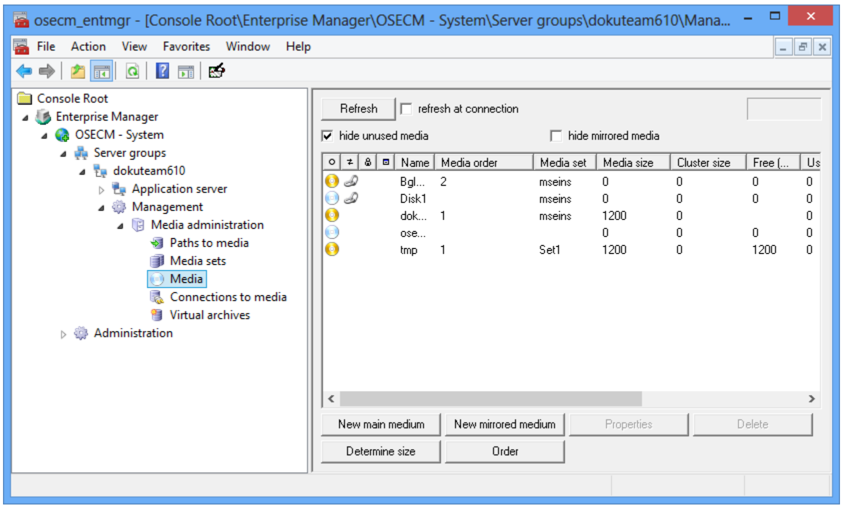
Storages

If you cannot automatically generate the media using templates for the media sets, configure the media.

If you select **Media** in the console root, all accessible media are listed.

> Media that a template has created automatically will also be listed here.

Mirrored media and unused media can be hidden.



□ refresh at connection

☑ hide unused media   □ hide mirrored media

○	≠	🔒	▣	Name	Media order	Media set	Media size	Cluster size	Free (...	Us
●	🔗			Bgl...	2	mseins	0	0	0	0
○	🔗			Disk1		mseins	0	0	0	0
●				dok...	1	mseins	1200	0		0
○				ose...			0	0	0	0
●				tmp	1	Set1	1200	0	1200	0

Media can be set up as ● Main media or as ○ Mirrored media and 🔗 assigned to each other.

If a document cannot be found on the main medium, it will be then searched for on the mirrored medium. Optionally and in case of failure, an e-mail is sent to the administrator (see the 'Archiving Option' **Send e-mail when archiving**').

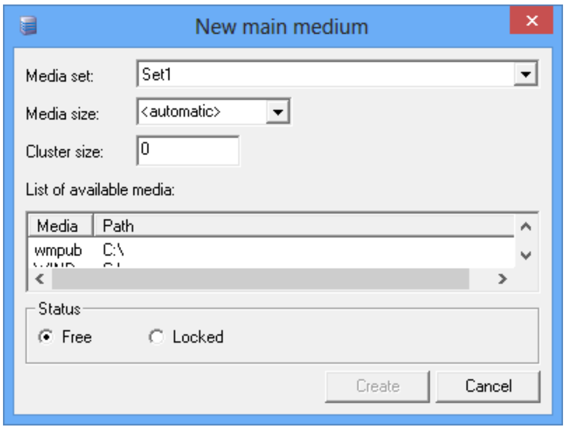
At storage, documents are first written to the main medium and then to the mirrored medium. If a document cannot be saved to one or more media, the document is not classified as archived and both media will be blocked. At renewed archiving, a document will only be written to a medium if it is not found on it.

Media are assigned to a media set in which they can be sequenced, at the same time defining the order in which they are written to.

It is possible to lock all main media that you do not want to use for further archiving.

Click the button **New main medium** to open the **New main medium** dialog. From the list of available media, select the medium you want to use as the main medium, choose a media set, the cluster size and a media size. The size can be selected from the list or inserted as a value in MB.

For removable media, you can choose **Automatic** as the size to automatically detect the size.



Media set: Set1

Media size: <automatic>

Cluster size: 0

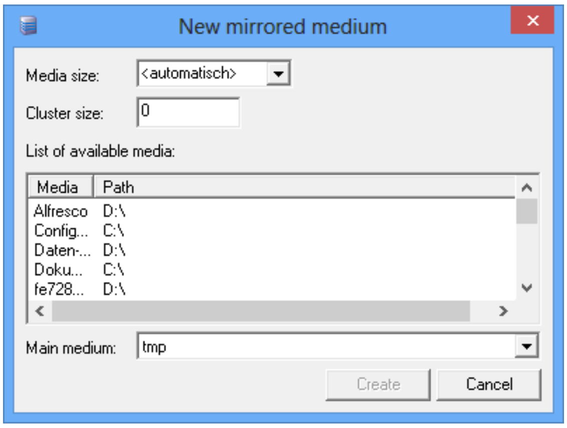
List of available media:

Media	Path
wmpub	C:\

Status

● Free   ○ Locked

Click the button **New mirrored medium** to open the **New mirrored medium** dialog. In this dialog, select a medium, enter a medium size and a cluster size and choose the main medium to which the mirrored medium will be assigned.



Media size: <automatisch>

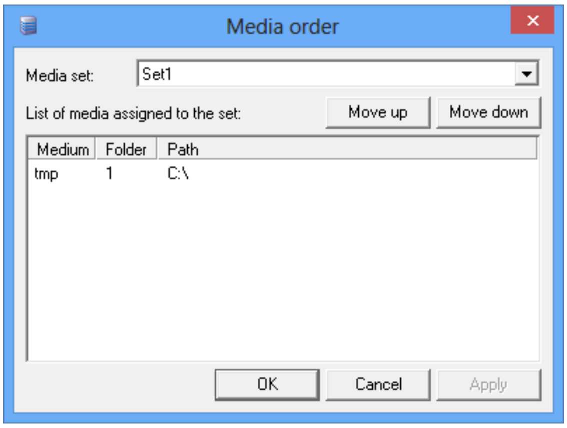
Cluster size: 0

List of available media:

Media	Path
Alfresco	D:\
Config...	C:\
Daten-...	D:\
Doku...	C:\
fe728...	D:\

Main medium: tmp

Use the **Order** button to specify the sequence in which main media are described.



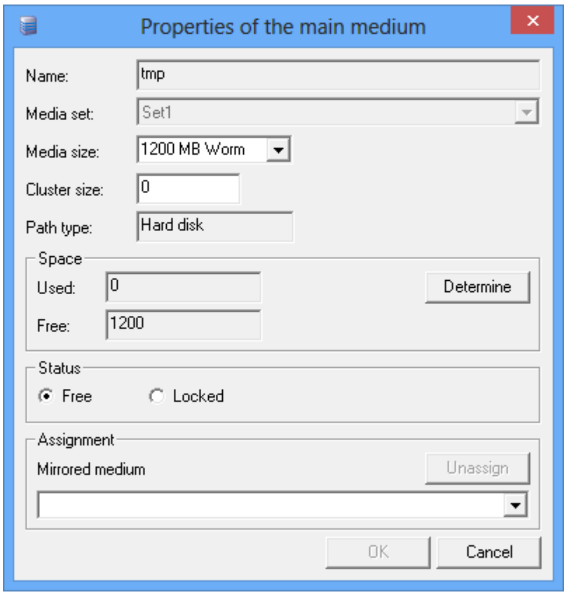
Media set: Set1

List of media assigned to the set:

Medium	Folder	Path
tmp	1	C:\

It is possible to lock all main media that you do not want or no longer want to use for archiving. The assigned mirrored medium is also automatically locked.

Use the **Properties** button to open the properties dialog of a medium and you can lock a main medium.



Properties of the main medium

Name: tmp

Media set: Set1

Media size: 1200 MB Worm

Cluster size: 0

Path type: Hard disk

Space

Used: 0

Free: 1200

Status

● Free ○ Locked

Assignment

Mirrored medium

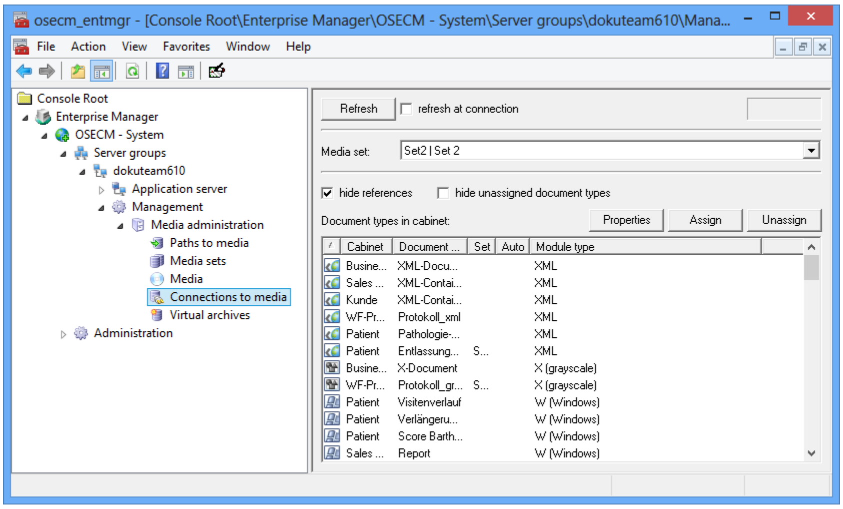
If you lock a main medium, the assigned mirrored medium will be automatically locked as well. Mirrored media cannot be locked through the properties dialog.

Assignments between main and mirrored media can be undone and set up anew.

Connection to Media

Document types are assigned to media sets as their documents will be stored on the media of the set.

If you select **Connection to media** in the console root, the document types will be listed. Existing assignments to media sets will be displayed.



osecm_entmgr - [Console Root\Enterprise Manager\OSECM - System\Server groups\dokuteam610\Mana...

□ refresh at connection

Media set: Set2 | Set 2

☑ hide references □ hide unassigned document types

Document types in cabinet:

Cabinet	Document ...	Set	Auto	Module type
Busine...	XML-Docu...			XML
Sales ...	XML-Contai...			XML
Kunde	XML-Contai...			XML
WF-Pr...	Protokoll_xml			XML
Patient	Pathologie-...			XML
Patient	Entlassung...	S...		XML
Busine...	X-Document			X (grayscale)
WF-Pr...	Protokoll_gr...	S...		X (grayscale)
Patient	Visitenverlauf			W (Windows)
Patient	Verlängeru...			W (Windows)
Patient	Score Barth...			W (Windows)
Sales ...	Report			W (Windows)

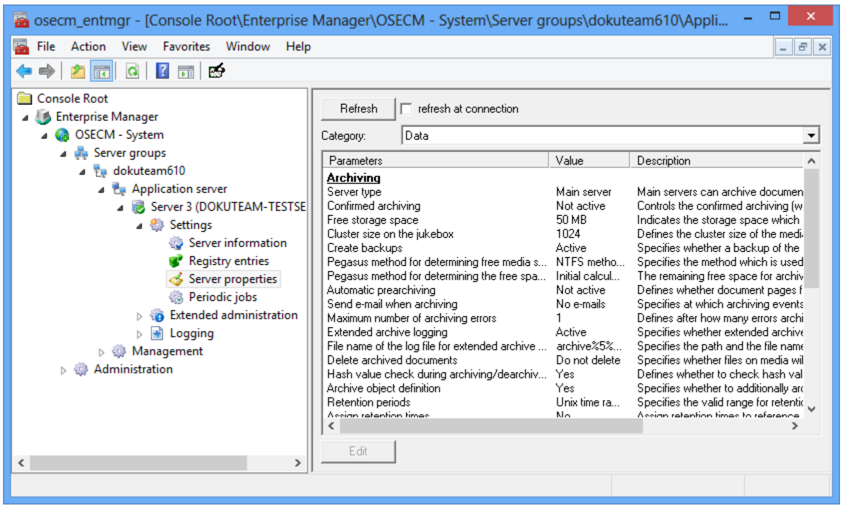
To connect document types with media sets, choose the **Media set**, select **Document types**, and click on the **Assign** button.

You can hide and show references (documents without pages) in the list of document types. Documents without pages cannot be archived – such an assignment would not fulfill any function.

You can also hide unassigned document types.

Archiving options

General archiving options can be set with enaio® enterprise-manager for the archiving enaio® server using the **Server > Settings > Server properties > Category: Data** area.



□ refresh at connection

Category: Data

Parameters	Value	Description
Archiving		
Server type	Main server	Main servers can archive documen
Confirmed archiving	Not active	Controls the confirmed archiving (w
Free storage space	50 MB	Indicates the storage space which
Cluster size on the jukebox	1024	Defines the cluster size of the medi
Create backups	Active	Specifies whether a backup of the
Pegasus method for determining free media s...	NTFS metho...	Specifies the method which is used
Pegasus method for determining the free spa...	Initial calcul...	The remaining free space for archiv
Automatic prearchiving	Not active	Defines whether document pages f
Send e-mail when archiving	No e-mails	Specifies at which archiving events
Maximum number of archiving errors	1	Defines after how many errors archi
Extended archive logging	Active	Specifies whether extended archive
File name of the log file for extended archive ...	archive%5%...	Specifies the path and the file name
Delete archived documents	Do not delete	Specifies whether files on media wil
Hash value check during archiving/dearchiv...	Yes	Defines whether to check hash val
Archive object definition	Yes	Specifies whether to additionally arc
Retention periods	Unix time ra...	Specifies the valid range for retentic
Assign retention times	No	Assign retention times to reference

Changes will only become effective after the respective server was restarted or the corresponding 'std' engine reloaded.

You can find the following parameters in the **Archiving** area:

§ **Server type**

Main servers can archive documents of other servers; sub-servers can only archive their own documents. In case no media assignment has been set up for a given document type at the server that manages the corresponding documents, a main server will archive the documents of other main and sub-servers.

All servers of a server group must have the same server type.

§ **Activate confirmed archiving**

In order to confirm that the documents were successfully archived, a file is created for every document type containing the data of the archived documents.

These files are saved in the `\server\archive` directory. They are named according to the following syntax: 'OSDDMMYY.'MainType''SubType''.

§ **Free storage space**

You can define how much storage space in MB will remain free on the archiving medium in order to save the index data and data related to the object definition. This data will also be written to the media at archiving events.

The default value is 50 MB. Increase the value if you use systems with more extensive object definitions and index data.

§ **Cluster size on the jukebox**

The cluster size is used to determine the available space on media. The default value is '0' and the cluster size is thus automatically determined. The utilization of media capacity in jukeboxes, in particular in older jukebox models, can be improved by specifying the cluster size in MB. A size specified in the media administration takes precedence over the default value.

§ **Create backups**

It is possible to create backups of the archived documents and to save them to the `\server\backup` directory. The backup of a document is written to a subdirectory which is named after the medium on which the document has been archived.

§ **Pegasus method for determining free media space**

The default setting is the 'NTFS Method' and the free space is thus determined with the WinApi32 function 'GetDiskFreeSpaceEx'.

When archiving to a Pegasus jukebox, the NTFS method used to determine free space on a medium may in parts not be reliable. As a result, it may occur that a significant part of the medium capacity is not utilized.

The 'Pegasus method 1' is a method from InveStore which determines free space by reading the '!FSFREE.###' file. This method is geared for media larger than 4 GB.

The 'Pegasus method 2' is a method from InveStore which determines free space by reading the 'FSFREE__.###' file. This method is suitable for media smaller than 4 GB.

§ **Pegasus method for determining the free space for the next document to be archived**

The remaining free space for archiving on Pegasus media can be calculated based on the initially free space or determined anew each time.

§ **Automatic prearchiving**

When a main server archives documents of another server, all documents to be archived can be passed before the archiving event to the main server for preparation. Performant network connections make this prearchiving step unnecessary.

§ **Sending e-mails during archiving**

If an e-mail server is available, the administrator can be automatically notified about complete archiving processes by e-mail.

The following values are available:

'No e-mails'

''If no of archiv. docs > 0 (w/o rep. file)'

'For each archiving process (w/o rep. file)'

''If no of archiv. docs > 0 (with rep. file)'

'For each archiving process (with rep. file)'

'In case that errors occurred'

§ **Maximum number of errors during archiving**

You can specify after how many archiving errors the archiving process will stop. Insert '0' to not cancel the archiving process.

Note that updating the enaio® server will reset this value to '1'.

§ **Extended archive logging**

You can establish whether extended archive logging remains activated. Thus, a detailed XML log file will be created. In addition to general data, the results of the hash and signature checks are listed in detail as well as the environment data concerning the archiving.

§ **Path und file name for extended archive logging**

Specify the path and the name of the log file for extended archiving.

§ **Delete archived documents**

You can specify whether or not to remove archived documents from the archiving medium. Depending on the used medium, this is not invariably possible.

Deleting archived documents requires the appropriate system role.

§ **Hash value check during archiving/dearchiving**

Define whether or not to check the hash values during archiving or dearchiving processes. This ensures correct handover but is detrimental to performance.

This check is independent of the document integrity's validation.

§ **Archive object definition**

Specifies whether to additionally archive the corresponding object definition during each archiving process.

If this option is deactivated, you have to ensure the equality of index data and the corresponding data model according to your procedural documentation.

§ **Retention periods**

Specifies the valid range for retention periods.

32 bit systems may require you to limit the valid retention date period. To do so, select the unix time range. As a result it will be impossible to specify retention dates beyond Jan 19, 2038.

If the file system in use allows retention periods beyond 2038 without further ado, select the continuous time range.

When using NetApp archives, select the extended time range. As a result, the valid time range for retention dates extends to Jan 19, 2071.

For GRAU DATA, select the continuous time range.

§ **Transfer retention periods**

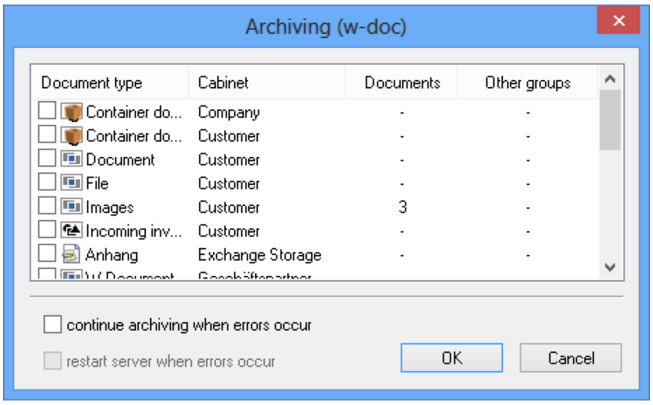
For reference documents, the retention times are transferred from the originals.

Retention periods of already archived documents are not transferred to new reference documents.

'Archiving' Action

You set up the 'Archiving' action in the same way as the other actions by using the **Automatic actions** window (see 'Setting Up Automatic Actions'). It is possible to set up several configurations for the 'Archiving' action.

The configuration dialog of the 'Archiving' action allows you to select the document types. In the dialog, all document types which are assigned to a media set will be listed. The number of archivable documents is indicated for each document type. This number also includes documents from all other servers that can be archived using the current server.



Archiving (w-doc)

Document type	Cabinet	Documents	Other groups
□ Container do...	Company	-	-
□ Container do...	Customer	-	-
□ Document	Customer	-	-
□ File	Customer	-	-
□ Images	Customer	3	-
□ Incoming inv...	Customer	-	-
□ Anhang	Exchange Storage	-	-
□ W-Document	Geschäftspartner		

□ continue archiving when errors occur

□ restart server when errors occur

Select the document types whose documents you want to archive.

The following options are available:

§ **Continue archiving despite error**

In case of error, the archiving event will not be canceled, instead the attempt to archive the respective document type will be renewed.

> If errors continue to occur, new archiving attempts will also continue to be started. In such a case, the action must be stopped manually.

If the option is not selected and after an error with a document type, an attempt to archive the next document type will be made.

§ **Restart server when errors occur**

If, in case of error, the archiving action is to be continued, this option is used to restart enaio® server before the new archiving attempt is performed. The action then waits two minutes for the server to restart and then renews the archiving attempt of the respective document type.

Confirm with **OK**.

The action is shown in the **Automatic actions** window. You can start the action manually or schedule a time for enaio® start to automatically start the action (see 'enaio® start').

If you want to terminate the action before it ends, you can create a file with the name `canceljob.$$$` in the server directory `...\server\ostemp`.

> Make sure that the documents of the selected document type are not currently being accessed by the full text indexing feature.
> The documents of the selected document type are written to the media of the assigned media set. All earlier document versions of those document types that have the property 'Archive document versions' will also be filed. Variants of W-Documents are also archived if they are released for archiving.

Alternatively, you can create a list with document IDs. In each case, you specify the document ID and the document type ID.

Structure: `<objectid>,<objecttypid>;<objectid>,<objectypid>;…`

Variants of documents thus specified will not be archived either.

The Archiving Log

The 'Archiving' action writes a log named `osDDMMYY.rep` to the server's log directory, irrespective of the log settings. The letters `DDMMYY` stand for the date. If the archiving action is carried out over more than one day, for example from 11 p.m. to 2 a.m. of the following day, the name will comprise a beginning and the end date.

The log has the following structure:

```
Application server report 10.08.2006, 13:00:29

=========================================================

The Automatic Action 'Archiving'

=========================================================

00:00:00 | Action started.......

00:00:00 | GetArchDocs

00:00:00 | 28 documents found

00:00:00 | For medium MEDIUM1, no mirror medium is defined.

00:00:00 | No register available.

00:00:00 | Media were determined. Primary Medium: MEDIUM1,

00:00:14 | 28 of 28 documents of type Contracts were successfully
archived.

----------------------------------------------------------

Result:

Automatic action archiving successfully completed (value = 0)
(10.08.2006, 13:00:43)

----------------------------------------------------------

00:00:14 | ------------------------------------------------------

00:00:14 | ---------------------------Statistics------------------

00:00:14 | 28 documents with a total of 29 files were processed.

00:00:14 | Average of 1.04 files per document, 107.31 KB per file
```

```
00:00:14 | 0.50 s / document, 0.48 s per file, 222.29 KB / s
transfer
```

The storage space that remained available on the medium will also be inserted into the log.

Contains the error message log, please contact Support.

The name of the archiving log cannot be defined exactly using parameters, but it is possible to switch between the formats `osDDMMYY.rep` and `osYYMMDD.rep`. To do so, edit the designation format in the `oxrpt.cfg` file, which is found in the server directory, in terms of flow logging. If the parameter '%6' (DD) is not before '%7' (MM) and '%5' (YY), the designation format `osYYMMDD.rep` is used.

You can find details with respect to the logging configuration in the chapter 'Introduction to Logging.'

Extended archive logging also creates an archiving log containing more details, in particular on hash value, signature, and environment data.

The path and the file name can be set using enaio® enterprise-manager. The default file name is `archive%5%7%6%8%9%10.xml`.

`%5` stands for the year, `%7` for the month, `%6` for the day, `%8` for the hour, `%9` for the minute, `%10` for the second.

The file will be written to the `\server\log` directory.

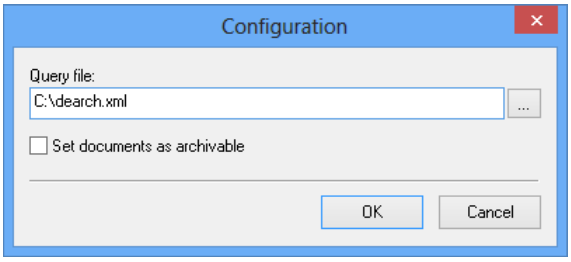
The style sheet `archive.xsl` is used for display. This file is written to the `\server` directory and copied into the respective directory in which the extended archiving log file is created.

'Dearchiving' Action

The automatic action 'Dearchiving' copies documents which have already been archived in an audit-proof way of a given type from the archiving media into the work area and marks the documents as 'not archived.' These documents can be afterwards modified or newly archived using a different configuration.

Integrate the library for the 'Dearchiving' action`axacunac.dll` (see ''Additions').

When setting up the automatic action (see 'Setting Up Automatic Actions'), specify a configuration name and choose a query file in the configuration dialog. Specify whether variants should also be dearchived, and whether the dearchived documents should be given the property 'approved for archiving.'



Configuration

Query file: C:\dearch.xml

☐ Set documents as archivable

The query file is used to select which documents are to be dearchived.

The settings of the server properties **Category: Integrity** establish whether a hash value check and a signature check take place after dearchiving.

You can start the action manually or schedule a time for enaio® start to automatically start the action (see 'enaio® start').

Only documents of one document type can be dearchived via a query field of the 'Dearchiving' action. All earlier document versions of those document types that have the property 'Archive document versions' will also be dearchived.

You can create the query file with any arbitrary text editor. It has the following structure:

`[ANFRAGE]`	The file begins with the 'query' section.
`SCHRANK=cabinet name`	Enter the name of the cabinet that the documents originate from into the first line.
`DOKUMENT=document type name`	The document type of the documents comes in the second line.

`KLAUSEL1=Objekt@Feld=Wert`
`...`
`KLAUSELn=Objekt@Feld=Wert`
	Optional logic expressions allow you to limit the selection to those documents that fulfill these conditions.
	Logical expressions must be numbered consecutively.

Use internal names and enclose the name in percent signs.

Alternatively, you can create a list with document IDs for dearchiving. In each case, you specify the document ID and the document type ID.

Structure: `<objectid>,<objecttypid>;<objectid>,<objectypid>;…`

Variants of documents specified through IDs are not dearchived. Versions are dearchived.

Logical Expressions

Optional logic expressions allow you to limit the selection to those documents that are indexed with the indicated value in the indicated field.

Example:

```
Klausel1=Kunde@Status=abgeschlossen
```

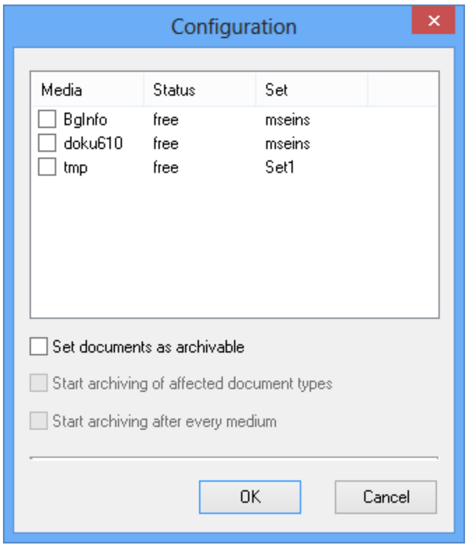
Documents of the indicated document type will be dearchived only if the index data of the archive object type 'Customer', e.g. a folder, contains the value 'completed' in the field 'Status'.

'Media Dearchiving' Action

The automatic action media dearchiving copies all documents which have already been archived in an audit-proof way of any type from the archiving medium to the work area and marks the documents as 'not archived.' These documents can be afterwards modified and newly archived using a different configuration, for example on different media.

Integrate the library for the 'Media dearchiving' action`axacunac.dll` (see ''Additions').

When setting up the automatic action (see 'Setting Up Automatic Actions'), specify a configuration name and select the required media in the configuration dialog.



Media	Status	Set
□ BgInfo	free	mseins
□ doku610	free	mseins
□ tmp	free	Set1

□ Set documents as archivable

□ Start archiving of affected document types

□ Start archiving after every medium

You can also decide whether the dearchived documents are given the 'approved for archiving' property.

Activate the **Start archiving of affected document types** option so that after the dearchiving process of all selected media, the archiving of those document types that are located on the selected media starts automatically. Current connections to media are then used for the document types.

If you activate the **Start archiving after every medium** option, the document types from every individual medium will be re-archived immediately after the medium has been dearchived. Current connections to media are then used for the document types.

If you have not provided connections to media for a dearchived document type, this document type will not be archived. If the document type has the property 'Archive document versions,' all old versions of the documents will also be dearchived and rearchived.

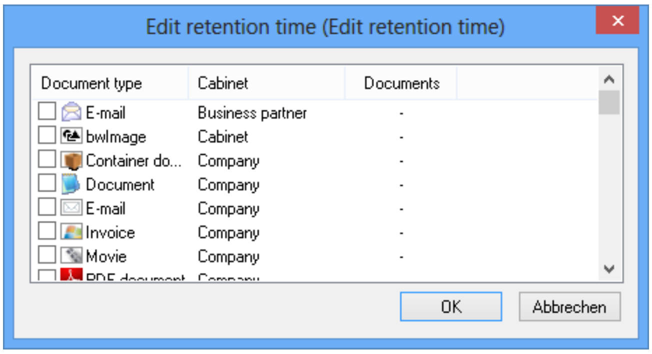
The action creates an additional log file in the log directory. This file is named `UnArchive_YYYYMMDD.txt`.

'Adjust Retention Period' Action

The automatic action 'Adjust retention period', `axacadjr.dll`, collects the retention period scheduled for all archived documents that are stored on a NetApp or iTernity archive, inserts it as the retention period and modifies the retention period of the document on the storage media.

If the scheduled retention period is shorter than the retention period, the information will not be changed. If the retention period was not specified, the scheduled retention period will be inserted as the retention period. If the scheduled retention period is in the past nothing will be changed.

During the configuration of the automatic action 'Edit retention period' the intended document type is specified for which the action will be executed. The number of archived documents will be then displayed.



Edit retention time (Edit retention time)

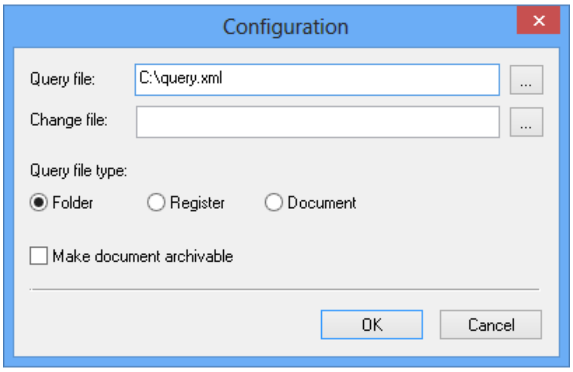
Document type	Cabinet	Documents
□ E-mail	Business partner	-
□ bwImage	Cabinet	-
□ Container do...	Company	-
□ Document	Company	-
□ E-mail	Company	-
□ Invoice	Company	-
□ Movie	Company	-
□ PDF document	Company	

Please note that, if retention periods extend beyond 2038, NetApp archives may be prone to the year 2038 problem. To avoid this problem, select the appropriate option in the server properties (see 'Archiving'). Adjustments need to be made for NetApp archives and other archives if the indicated retention period exceeds the year 2038.

'Non-Technical Retention Scheme' Action

The automatic action 'Non-technical retention scheme' `axacaret.dll`, using a query file, finds documents and determines a date based on the index data which is set as the planned retention period for the documents. If desired, a change file can be used to modify the index data of the object that the date was taken from.

The planned retention period is only entered if up until then no planned retention time was specified or a retention time already entered is before the new date for the planned retention time. Reference documents are processed only if they are managed by a virtual server. The retention period of documents located in several folders or registers may be checked more than once before being modified.



Configuration

Query file: C:\query.xml

Change file:

Query file type:

● Folder ○ Register ○ Document

□ Make document archivable

The query file has the following structure:

`[ANFRAGE]`	The file begins with the 'query' section.
`SCHRANK=cabinet name`	Enter the name of the cabinet that the documents

	originate from into the first line.
`DOKUMENT=document type name`	The document type of the documents comes in the second line.

`KLAUSEL1=Objekt@Feld=Wert`
`...`
`KLAUSELn=Objekt@Feld=Wert`
	Optional logic expressions allow you to limit the selection to those documents that fulfill these conditions.
	Logical expressions must be numbered consecutively.

`Datenfelder=1`	Preset entry
`[Queryfields]`	Specify the field containing the planned retention date.
`Feld0=field name`	The indicated field must contain a date and be a field of the object type that is found by the query.

Use internal names and enclose the name in percent signs.

Following query types are available:

- **Document query**

  The fields with the date and the optional index data modification are located on the document's data sheet.

- **Register query**

  The fields with the date and the optional index data modification are located on the register type's data sheet. The planned retention period will be set for all documents in a register which are determined by the query.

- **Folder query**

  The fields with the date and the optional index data modification are located on the folder type's data sheet. The planned retention period will be set for all documents in a folder which are determined by the query.

The optional change file has the following structure:

`[UPDATE]`	The file begins with the section 'Aktualisieren' (update).
`SCHRANK=cabinet name`	Enter the name of the cabinet that the documents originate from into the first line.
`DOKUMENT=document type name`	The document type of the documents comes in the second line.
`DOKUMENT-ID=%OBJECT-ID%`	Preset entry
`FELD1=field name=value`	Enter the field and the value to be changed.
`MODE=1`	Specifies whether all other field will not be modified.

You can also specify whether the documents are given the 'approved for archiving' property.

Actions for Checking Archiving

enaio® provides a number of automatic actions which can be used to check not archived documents which are saved to an archiving medium or the WORK area.

§ Archive consistency

You can check if documents which are registered by the database really exist.

§ Archive system reparation

If during the archive consistency check inconsistencies are found, this action can reintegrate all documents which are flagged as 'archived' and stored in the cache area but have not been archived into the system.

§ Work directory synchronization

You can check if documents which were archived or deleted and must therefore be deleted from the WORK area have remained in the WORK area.

§ Archive control

Due to archiving errors, documents that have been stored on archiving media may still have the 'approved for archiving' property. You can find out which documents these are with the 'Archive control' action.

§ Directory comparison

You can compare the contents of directories, e.g. an archiving medium with the corresponding mirrored medium.

These actions extensively log the check results. Some actions can be used to manipulate data. Data must only be manipulated after prior consultation with the support or consulting department.

> These actions cannot check archiving processes on virtual archives or NetApp and GRAU DATA archives. Equally, document types with the property 'Combine and Compress' cannot be checked.

All actions are part of the `axactarc.dll` library. This library can be integrated using the 'Additions. Then you can create configurations for the actions and run the configured actions (see 'Setting Up Automatic Actions').

Action logs are saved in the directory which is specified in the log configuration file `oxrpt.cfg` located in the application directory.

In addition, all actions are logged by the enaio® logging function.

'Archive Consistency' Action

This action is used to check the WORK area and the archive area.

If you check the WORK area, it is verified according to the data found in the database if for each document which is not archived a corresponding document file exists in the WORK area.

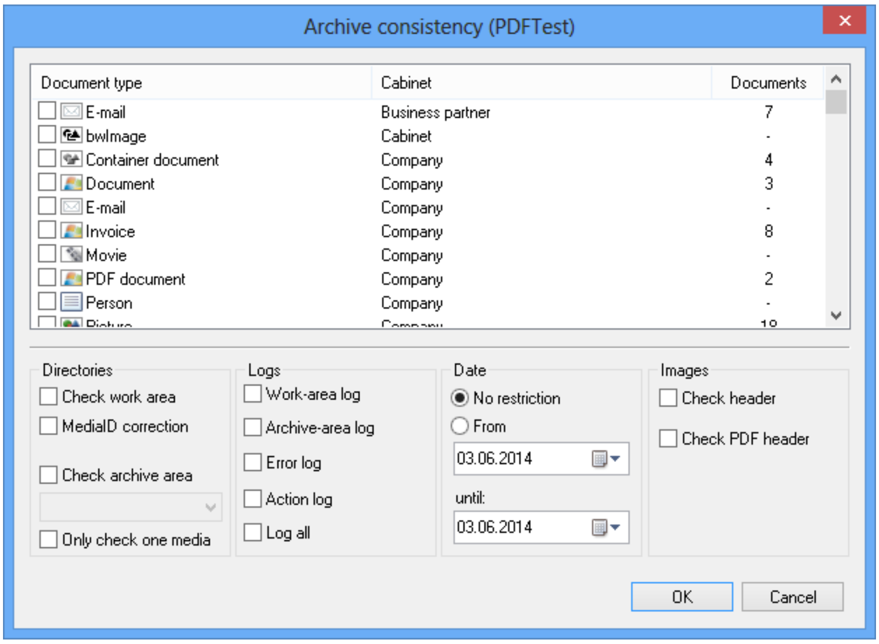
Invalid IDs of documents in the WORK area can be corrected.

> Usually, this ID does not need to be corrected and may only be manipulated after prior consultation of the support or consulting department.

If you check the archive area, it is verified according to the data found in the database if for each archived document a corresponding document file exists on the media. The check for archived documents can be restricted to documents of one medium.

The **Check header** option can be enabled for the work area and the archive area. Then, each image file is checked if the file contains a valid header of an enaio® image format. The header for PDF files can also be checked.

> Checking only this aspect of a file does not guarantee its integrity.



Document type	Cabinet	Documents
□ E-mail	Business partner	7
□ bwImage	Cabinet	-
□ Container document	Company	4
□ Document	Company	3
□ E-mail	Company	-
□ Invoice	Company	8
□ Movie	Company	-
□ PDF document	Company	2
□ Person	Company	-
□ Picture	Company	10

Directories
□ Check work area
□ MediaID correction
□ Check archive area
□ Only check one media

Logs
□ Work-area log
□ Archive-area log
□ Error log
□ Action log
□ Log all

Date
● No restriction
○ From 03.06.2014
until: 03.06.2014

Images
□ Check header
□ Check PDF header

Enter the document types for which you want to perform the archive consistency check in the configuration dialog. You can restrict the selection to documents that were created within a specific period of time.

These kinds of logs can be created:

- **Work area log**

  This log contains a detailed list of all documents which were found in the WORK area. This log does not contain any errors.

  `TarchWork_[configuration name]_[YYYYMMDD_HHMMSS].rep`

- **Archive area log**

  This log contains a detailed list of all archived documents which were found on archiving media. This log does not contain any errors.

  `TarchArchiv_[configuration name]_[YYYYMMDD_HHMMSS].rep`

- **Error log**

This log contains a detailed list of all documents which are registered by the database but could not be found on the available media.

If a document cannot be found because media cannot be accessed, this problem will not be listed in the error log.

`TarchError_[configuration name]_[YYYYMMDD_HHMMSS].rep`

- **Action log**

  The log contains an overview of the performed checks. It lists how many documents of which document type were checked.

  `TarchAction_[configuration name]_[YYYYMMDD_HHMMSS].rep`

- **Log all**

  The action log contains a list of all actions which were performed for the 'Archive consistency' action. It also logs access to non-available media.

  `TarchProtokoll_[configuration name]_[YYYYMMDD_HHMMSS].rep`

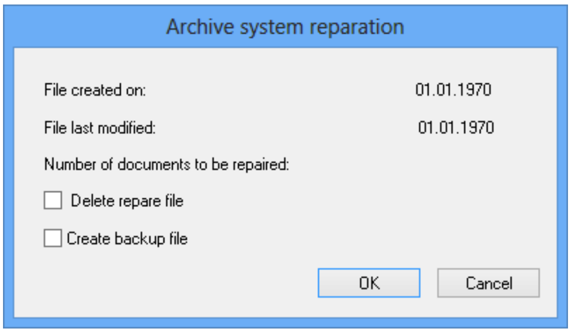
'Archiving System Reparation' Action

If the 'Archive consistency' check of an archive area finds documents which instead of being stored on the archive medium are stored in the cache area, a log file named `Repair.sys` will be created.

Using the information in the log file, the 'Archive system reparation' action can copy the document files found to the work area and give the documents the 'approved for archiving' property. The documents are then available in enaio® again, and can be opened, edited, and rearchived.

> The action checks the integrity of the found document files.

The action is only executed if the log file `Repair.sys` is available.



Archive system reparation

File created on: 01.01.1970

File last modified: 01.01.1970

Number of documents to be repaired:

☐ Delete repare file

☐ Create backup file

The number of found documents will be displayed in the configuration dialog.

Specify if you want the file `Repair.sys` to be deleted after the action and if a backup of the file `Repair.sys` will be created.

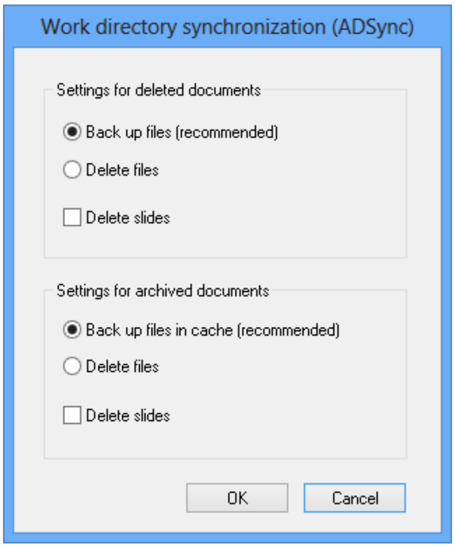
The log in the specified log directory has the following name:

`TarchRepair.txt`

'Work Directory Synchronization' Action

If a user creates a document in enaio® the document file is saved in the WORK area. If the document is archived or deleted, the document file is deleted from the WORK area.

The 'Work directory synchronization' action checks if document files of archived or deleted documents have remained in the WORK area. Such files can be deleted by this action.



Work directory synchronization (ADSync)

Settings for deleted documents

● Back up files (recommended)

○ Delete files

□ Delete slides

Settings for archived documents

● Back up files in cache (recommended)

○ Delete files

□ Delete slides

You can create configurations for deleted or archived documents. Specify for document files of deleted documents in the configuration dialog if the document files will be backed-up or deleted. Slide files which can be used as quicklooks in enaio® client can also be deleted.

If you back up document files of deleted documents, they are moved from the directory `\server\WORK` into the directory `\server\WBACKUP`.

If you back up document files of archived documents, they are moved into the directory `\server\CACHE`. Copies of archived documents are stored in this cache area for quicker file access.

The log in the specified log directory has the following name:

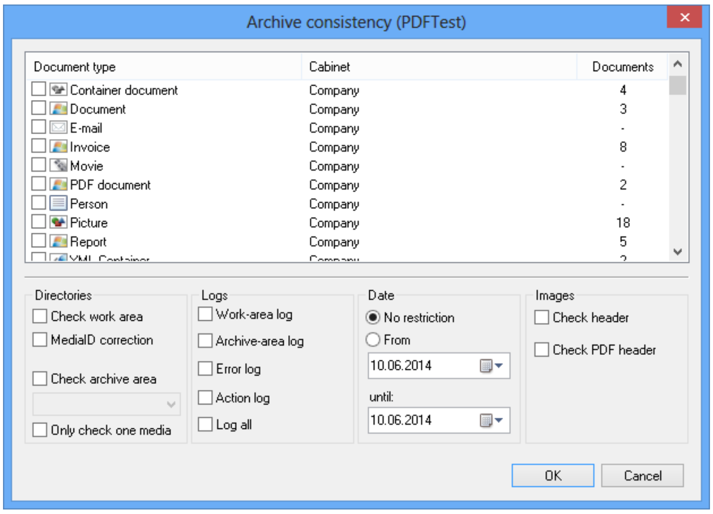
```
TarchWorkKons_[configuration name]_[YYYYMMDD_HHMMSS].rep
```

'Archive Control' Action

During archiving, it is possible that a document may be transferred to an archiving medium, but that archiving errors have occurred, so that the status of the document is not changed from 'approved for archiving' to 'archived.' If writable media is archived in one go or if the media is duly configured, it is not possible to archive the document again on the same medium.

The 'Archive control' action searches for this kind of document, i.e. documents that have the status 'approved for archiving' but are stored on the current archiving medium and cannot therefore be saved again on this medium.

You can identify such documents using the log and check them. The action itself does not check whether the documents on the archiving media have errors.



Archive consistency (PDFTest)

Document type	Cabinet	Documents
□ Container document	Company	4
□ Document	Company	3
□ E-mail	Company	-
□ Invoice	Company	8
□ Movie	Company	-
□ PDF document	Company	2
□ Person	Company	-
□ Picture	Company	18
□ Report	Company	5
□ XML Container	Company	2

Directories
□ Check work area
□ MediaID correction
□ Check archive area
□ Only check one media

Logs
□ Work-area log
□ Archive-area log
□ Error log
□ Action log
□ Log all

Date
● No restriction
○ From 10.06.2014
until: 10.06.2014

Images
□ Check header
□ Check PDF header

Enter the document types for which you want to perform the archive check in the configuration dialog. You can specify a medium which is checked and include the corresponding mirrored medium.

The option 'Move archive flag in the database' must not be selected. If you find document containing errors with the 'Archive control' action, please contact the support or consulting department.

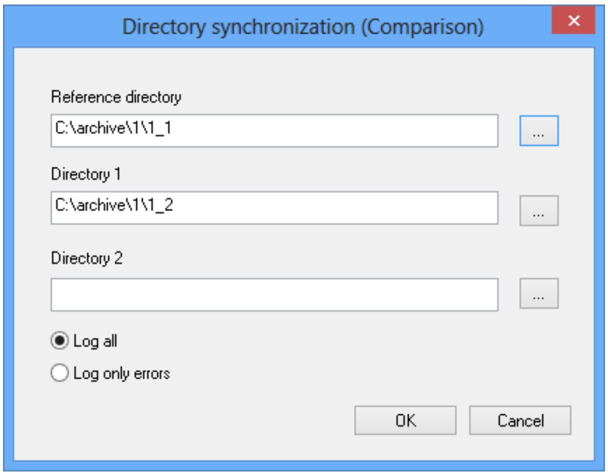
The log in the specified log directory has the following name:

```
TarchArchivControl_[configuration name]_[YYYYMMDD_HHMMSS].rep
```

'Directory Comparison' Action

The action is used to compare the archiving media with the corresponding mirrored media and backup directories. You can compare any directories too. The number of files inside the directories including all subdirectories, the file size and the file's creation date are compared.

The result is written into the log file `TarchCompareProt.rep` in the specified log directory `\clients\admin`.



Directory synchronization (Comparison)

Reference directory: C:\archive\1\1_1

Directory 1: C:\archive\1\1_2

Directory 2:

● Log all
○ Log only errors

Specify a reference directory and up to two directories to which the directory is compared. If the comparison directories contain files which the reference directory does not contain, this information is not logged.

You can also specify in the dialog whether to log all data or errors only.

Missing files, different file size and a different file date are recognized as errors.

Automatic Actions

Introduction to Automatic Actions

Automatic actions can be used to archive documents in an audit-proof way, to export or import data, or to automatically perform system maintenance tasks.

Automatic actions are configured as individual actions or as action sequences. You can start automatic actions manually from within enaio® administrator or schedule them to be automatically executed by enaio® start.

Automatic actions are integrated in a modular manner by use of libraries. You register libraries with enaio® using the **Complete system** and the **Additions** tab (see ''Additions' Tab'). They are located in the …`\clients\admin` directory.

Automatic actions can only be configured once this has been done. Some automatic actions are automatically integrated at installation.

The following automatic actions are available:

Action	Function	Library	License
Import and export of data and document files (see 'enaio® import-export Manual')			
Data/ Document import	Creates archive objects from many external data formats. A wizard facilitates the configuration.	`axacimp.dll`	AIE
Data/ Document export	Index data and document files can be exported. A wizard facilitates the configuration.	`axacexp.dll`	AIE
AXCOLD Import	COLD data consists of background images, text and position specifications. First of all, images are created from this data for display.	`axcold.dll`	COL
ASFax Import	Imports data from a fax server and stores it as archive objects.	`axfax.dll`	FAX
DICOM Import	Imports DICOM data	`axacdcm.dll`	

	from a DICOM server.		
XML Tag Extraction	This action generates delimited ASCII files from XML files.	`axacxmle.dll`	
XML transformation	Performs conversion of XML files into other XML formats.	`axacxmlc.dll`	
Actions for archiving			
Archive	Archiving documents on media.	`axacarch.dll`	
Dearchiving	Dearchives documents.	`axacunac.dll`	
Media dearchiving	Dearchives the data from media.	`axacunme.dll`	
Archive consistency	Checks the WORK area and the archive area.	`axactarc.dll`	
Archive system reparation	If during the archive consistency check inconsistencies are found, this action can reintegrate all documents which are flagged as 'archived' but have not been archived into the system.	`axactarc.dll`	
Work directory synchronization	Checks the work directory.	`axactarc.dll`	
Archive control	Checks whether there are documents that have the status 'approved for archiving' and are already stored on archiving media.	`axactarc.dll`	
Directory comparison	Directory comparison, in particular one medium with the assigned mirrored medium.	`axactarc.dll`	
Adjust retention period	Enter scheduled retention period as retention period.	`axacadjr.dll`	
Actions for document management			

Document retrieval	Retrieves documents from another server group.	`axacpref.dll`	
Object encryption	The action encrypts and decrypts document files.	`axaccrypt.dll`	KRY / SKR
Pagination	Labels image files which are assigned to each other.	`axacpage.dll`	PAG
Full text indexing	Performs full text indexing on pre-existing archive objects (see 'enaio® fulltext Manual').	`axacidx.dll`	
Full-text export at object level	Also indexes pre-existing archive objects which are specified in a configuration file which contains the search criteria for documents to be indexed (see 'enaio® fulltext Manual').	`axacvexp.dll`	
Database query	Performs SQL database queries and allows for the requested documents to be arranged as portfolios.	`axacreq.dll`	
Run script	Executes VB script code.	`axacscript.dll`	
Rendition	Creates variants in 'TIFF' or 'PDF' file format for module-spanning W-Documents.	`axacdok2tif.dll`	
Actions for System Maintenance			
Subscription maintenance	Deletes subscription entries according to specified rules.	`axacabo.dll`	
Updating database	Updates the database statistics.	`axacdbst.dll`	
Cleanup of configuration and log	Deletes old configuration versions	`axaccl.dll`	

files	and logs according to specified rules.		
Cache maintenance	Deletes files from the server cache. The server cache contains document files of which the originals are either in the work directory of another server group or stored on archiving media.	`axaccach.dll`	
History maintenance	Deletes entries from the editing history, e.g. entries for deleted documents.	`axachist.dll`	
Follow-up maintenance	Deletes follow-up entries according to specified rules.	`axacwdvl.dll`	
Cleaning history workflow	Deletes the history entries of workflow processes according to specified rules.	`axacwfhclear.dll`	
System check	Checks for and corrects inconsistencies in the database.	`axacsysc.dll`	
Start external application	Starts external Windows applications.	automatically integrated	
COM action interface	Can encapsulate COM libraries and makes them accessible as automatic actions.	`axaccom.dll`	
Execute SQL command	Enables direct execution of SQL commands and handover of results to VB scripts in the form of record sets.	`axacolfr.dll`	
Creation of multi-page TIFF	Converts TIF's of a given document type to multi-page TIF's.	`axacmtif.dll`	
Empty trash can	Empties the trash can according to specified rules.	`axaccleantrash.dll`	
Sign	This action creates	`axacsign.dll`	

	hash values for pre-existing documents. Hash values can also be signed at this point. Hash values are needed to secure document integrity and to check for identical documents.		
Hash check	This action checks the hash values of documents stored on archiving media or in the WORK area.	`axachash.dll`	
Hash check on object level	This action checks the hash value of documents that are specified in a query file.	`axachashd.dll`	
Delete objects	This actions deletes all objects that are specified in a query file from enaio® server.	`axacdel.dll`	
Calculate MIME Type	Adds MIME type and size of document files. These data are automatically stored since version 5.20.	`axacmtype.dll`	
Actions for controlling automatic actions			
Action sequence	Can be used to build sequences of automated actions.	automatically integrated	
Start external program from command line	Starts external windows applications and batch files, and allows return codes to be read back.	`axacexec.dll`	
Synchronization	Enables the synchronization of automatic actions with external applications.	`axacsync.dll`	

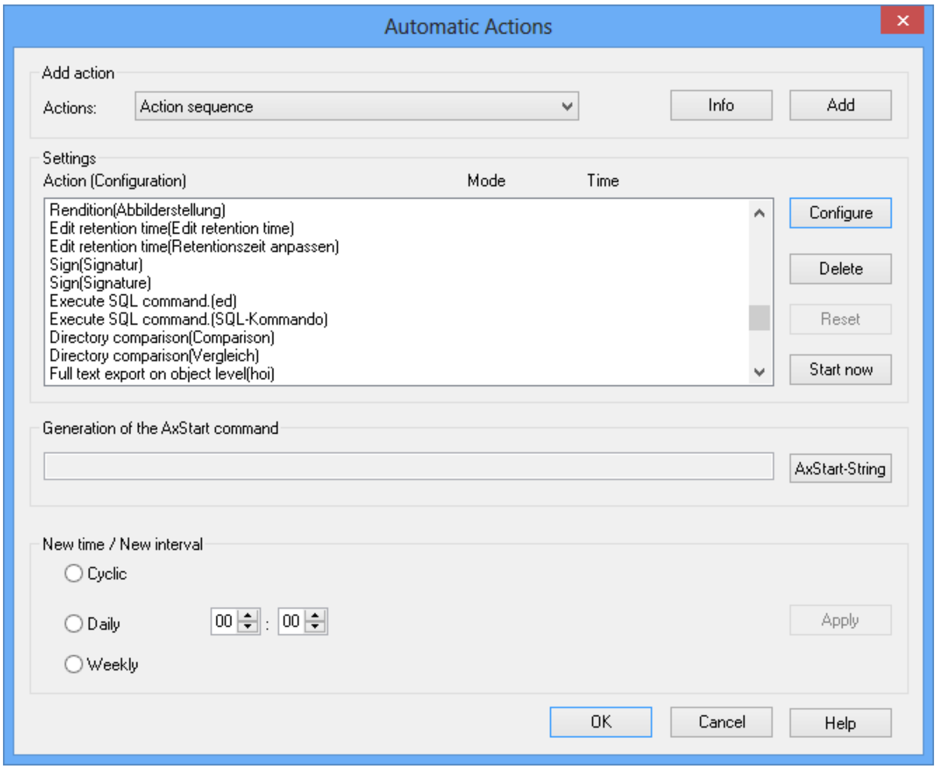
If automatic actions are run, the corresponding license keys for the workstations must be available (see 'Adding Modules').

Setting Up Automatic Actions

Follow these work items to set up automatic actions:

1. Click the **Automatic actions** button.

   The **Automatic actions** window will open.



Actions: Action sequence

Rendition(Abbilderstellung)
Edit retention time(Edit retention time)
Edit retention time(Retentionszeit anpassen)
Sign(Signatur)
Sign(Signature)
Execute SQL command.(ed)
Execute SQL command.(SQL-Kommando)
Directory comparison(Comparison)
Directory comparison(Vergleich)
Full text export on object level(hoi)

00 : 00

2. Select an action from the list of actions.
3. Click the **Add** button.

   The action will be added to the list of actions and the configuration dialog will open.
4. Configure the action in its configuration dialog or select an existing configuration.
5. Enter (optional) a time for when enaio® start is scheduled to start the action automatically and click on the **Apply** button. The specified time will thus be added to the list of actions.

You can run the action immediately using the **Start now** button or by starting enaio® start (see 'enaio® start'). enaio® start then runs the action at the specified time. The enaio® start application file is located in the same directory as enaio® administrator.

> enaio® start must be running at the time when the action is scheduled to be started. enaio® start requires the license key 'AXA,' otherwise the action will not run. If available, enaio® start can start any number of actions.

enaio® start can be started using other applications, scheduled tasks, batch files or the command line. To determine the parameters which will be sent to enaio® start when it starts up in order to trigger an automatic action, select an action and click on the **AxStart-String** button. The path and the start parameters are displayed in the **Generation of the AxStart command** field.

> Be aware of the fact that the generated start parameters may contain umlauts which possibly lead to problems with subject to the used character sets (ANSI, OEM). If you create a batch processing file, it must be saved in OEM format. The last line has to be followed by a line break.

If errors occur while enaio® is running, these are logged and enaio® is automatically closed. If you add the '/Verbose' parameter to the generated start parameters, enaio® start will not be automatically closed in the event of an error, but will wait for user input. If you add the parameter '/X' to the generated start parameters, the value '0' will not be returned every time in the event of an error; instead a value for the action during which the error occurred will be returned (see 'Error Return Values for Actions'). This allows the relevant action to be identified in a series of actions.

Automatic actions can be selected from the list in the field **Action (configuration)**, and edited using the following buttons:

§ **Delete**

The automatic action will be removed from the list.

§ **Reset**

The scheduled time will be deleted.

§ **Configure**

The configuration dialog will open. You can change the configuration.

enaio® start

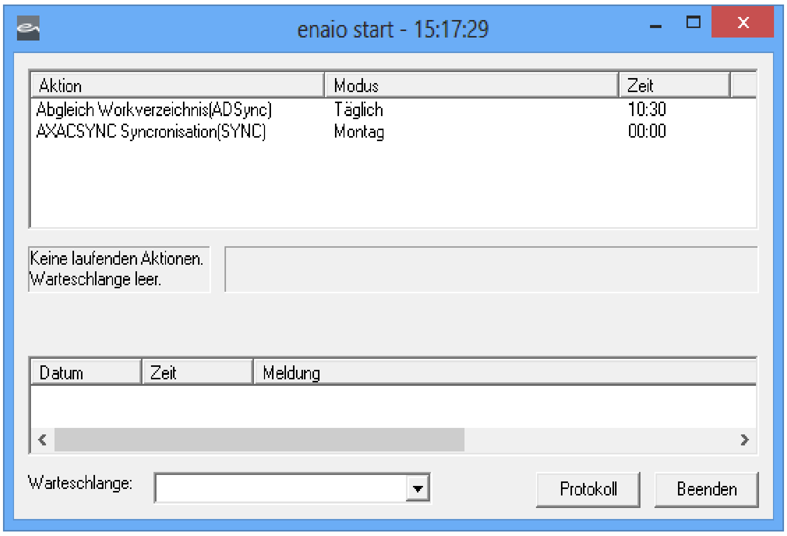
enaio® start handles the start of automatic actions, which you have scheduled. The actions themselves cannot be manipulated in enaio® start.

Actions that are configured to be performed in **Cyclic** mode will be run for the first time shortly after the launch of enaio® start. They will then be executed again after the specified period has expired. If you close enaio® start, no data regarding the execution times of automatic actions will be saved. Just after the next launch of enaio® start all periodic actions will be run again.

The enaio® start application (`axauto.exe`) is found in the folder `clients\admin`.

> When enaio® start is started for the first time, it must be started manually from the application directory. It also requires entering a user name and a password. The data is saved in the registry. This user account is then designated to launch the program.

When launching enaio® start, a window will open which lists all actions for which execution times have been specified.



enaio start - 15:17:29

Aktion	Modus	Zeit
Abgleich Workverzeichnis(ADSync)	Täglich	10:30
AXACSYNC Syncronisation(SYNC)	Montag	00:00

Keine laufenden Aktionen.
Warteschlange leer.

Datum	Zeit	Meldung

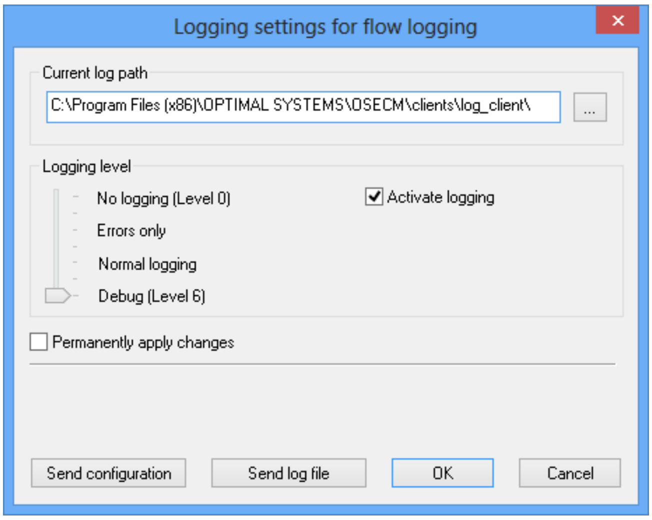
Warteschlange:

Actions are put in a queue if other actions are also processed at the same execution time.

Logging data of running actions is displayed in the lower area of the window. The log is automatically written to the file `osDDMMYY.prt`. `DDMMYY` stands for the date. Logs are saved to the configured log directory (see 'Introduction to Logging'). You can open old logs using the **Log** button.

The logs will not be deleted automatically. At regular intervals, you must manually remove logs which are no longer needed.

Irrespective of this logging process, enaio® logging takes place according to the settings in the `oxrpt.cfg` configuration file. With respect to this logging process you can set up the logging level of the default channel for the period of a session. The change of the logging level will immediately apply; enaio® start does not have to be reloaded.



Logging settings for flow logging

Current log path: C:\Program Files (x86)\OPTIMAL SYSTEMS\OSECM\clients\log_client\

Logging level:
- No logging (Level 0)
- Errors only
- Normal logging
- Debug (Level 6)

☑ Activate logging

☐ Permanently apply changes

Click the **Log settings** entry in the context menu of the title bar to open the dialog.

The **Send configuration** button is used to send the currently set logging configuration `oxrpt.cfg` by e-mail. In doing so, all log files (`*.evn`) of the current day and the configuration file will be sent as a ZIP archive.

Users with the system role 'Administrator: Configuration complete system' can permanently adopt the logging level settings.

You can end enaio® start with the **End** button. Any action which is still running will be completed. Actions in the queue will not be executed.

Actions for controlling automatic actions

Automatic actions can be run sequentially according to an action sequence. External programs can be started by an action sequence; such action sequences allow to be synchronized with applications which run independently of automatic actions.

Action Sequences

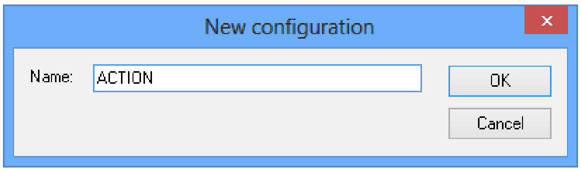
You can combine several automatic actions to be run in a consecutive sequence. For example, this may be necessary when an external application needs to be started to generate the input for the next automatic action in the sequence.

Follow these steps to create an action sequence:

1. Click the **Automatic actions** button.

   The **Automatic actions** window will open.
2. Select the entry **Action sequence** from the list of actions.
3. Click the **Add** button.

   The **Action sequence** window will open.



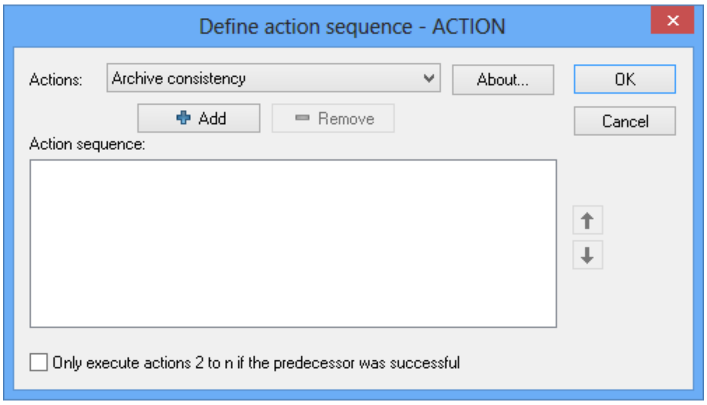
New configuration

Name: ACTION

4. Click on the **New** button, enter a name for the new action sequence in the dialog, and confirm the entry by clicking **OK**.

   The name of the new action sequence will be entered in the **Action sequence** window.
5. Click the **Edit** button.

   The **Define action sequence** window will open.


Define action sequence - ACTION
Actions:
Archive consistency
About...
OK
Add
Remove
Cancel
Action sequence:
□ Only execute actions 2 to n if the predecessor was successful

6. Select an action from the list of actions.
7. Click **Add**.

   The action will be added to the list of actions in the **Action sequence** field, and the configuration dialog will open.
8. Configure the action in the respective configuration dialogs or select an existing configuration.
9. Select more actions for the action sequence.

   Use the arrow buttons to sort the actions.
10. Select the option **Only execute action 2 to n if the predecessor was successful** if you want the action sequence to be canceled in case of error.
11. Then click on the **OK** button.

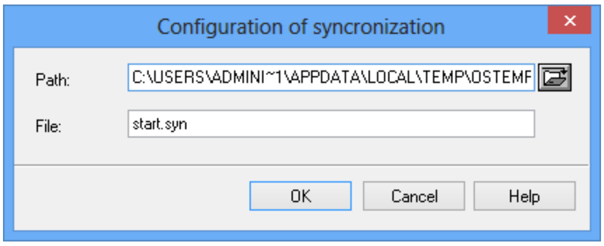
The action sequence will be displayed in the **Automatic actions** window. You can schedule the action sequence to be carried out automatically by enaio® start, or you can start it manually.

'Synchronization' Action

The 'AXACSYNC Synchronization' action creates an empty file for which you must specify a name and location in the action's configuration dialog. The action will not be stopped until the file is deleted or renamed. Within an action sequence, the subsequent automatic action will be started only then.

This file's availability may serve as trigger for other applications to start which operate independently from the action sequence. If an application deletes the file, the action 'AXACSYNC Synchronization' is terminated and the subsequent action which is contained in the action sequence started.

Enter the path and the file name in the configuration dialog to set up the 'AXACSYNC Synchronization' action.



Path: C:\USERS\ADMINI~1\APPDATA\LOCAL\TEMP\OSTEMF

File: start.syn

Confirm your entries with **OK**.

To use this action, add the `axacsync.dll` library.

'Start External Program from Command Line' Action

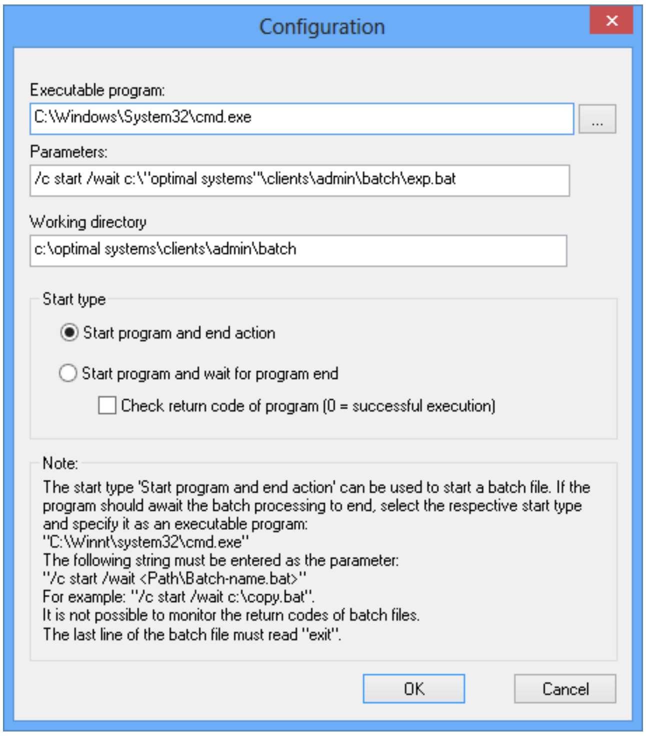
The 'Start external application from command line' action starts an external application. The action can end immediately or wait for the application to end and evaluate whether the program completed without errors.

You can also start batch files.

To use this action, add the `axacexec.dll` library. This action can also be used independently from any activity sequence.

The 'Start external application' action is also available. This action starts an external program and ends immediately without waiting for return values from the program. It cannot be used within action sequences.

To configure the action 'Start external program from the command line'', indicate the designated program, any start parameters (optional) and a working directory.



Configuration

Executable program: C:\Windows\System32\cmd.exe

Parameters: /c start /wait c:\"optimal systems"\clients\admin\batch\exp.bat

Working directory: c:\optimal systems\clients\admin\batch

Start type

● Start program and end action

○ Start program and wait for program end

□ Check return code of program (0 = successful execution)

Note:
The start type 'Start program and end action' can be used to start a batch file. If the program should await the batch processing to end, select the respective start type and specify it as an executable program:
"C:\Winnt\system32\cmd.exe"
The following string must be entered as the parameter:
"/c start /wait <Path\Batch-name.bat>"
For example: "/c start /wait c:\copy.bat".
It is not possible to monitor the return codes of batch files.
The last line of the batch file must read "exit".

You can select as a start type:

- **Start program and end action**

  The external program will be started and the action immediately ended; the action sequence will be continued.

- **Start application and wait for application end**

  The action will end if the external process is no longer running; the action sequence will continue.

- **Check return code of application**

The action will end as soon as the external program ends. If the external program ended with an error, the action 'Action sequence' will also terminate with an error. If the action sequence is carried out with the active option **Only execute actions 2 to n if the predecessor was successful**, the action sequence will be canceled.

Batch Files

You can also start batch files via using the 'Start external applications from the command line.'

Enter 'exit' into the last line of the batch file.

If you do not want to wait for the batch file to end, insert the path and the file name into the **Executable application** field and select the **Start application and end action** start type.

If you want to wait for the batch file to end, start the batch file through the command line interface. Enter the following into the **Executable application** field:

```
C:\WINDOWS\system32\cmd.exe.
```

The parameters and the batch file (including its path) are entered into the parameter field as follows:

```
/c start /wait <path\batchname.bat>
```

If file paths contain space characters, you must enclose them in double quotation marks.

Select as start type **Start application and wait for end of application**.

> The return code cannot be checked. In case of error, the action sequence will not be notified.

Actions for System Maintenance

The following actions are geared to maintain the system. They are integrated by importing libraries but do not require additional license keys.

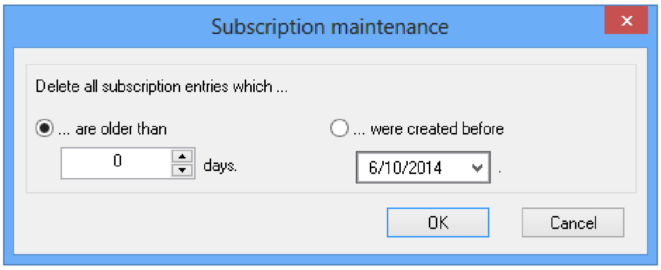
- 'Subscription Maintenance' Action
- 'Follow-up Maintenance' Action
- 'History Maintenance' Action
- 'Cleanup of Configuration and Log Files' Action
- 'Database Statistics Update' Action
- 'Cache Maintenance' Action
- 'System Checks' Action
- 'Prearchiving' Action
- 'Document Retrieval' Action
- 'Creation of Multi-Page TIFF' Action
- 'Cleaning Workflow History' Action

- § 'Process Archiving Workflow' Action
- § 'Empty Trash Can' Action
- § 'Delete Objects' Action
- § 'Calculate MIME Type' Action

Use the 'Additions to integrate the libraries.

'Subscription Maintenance' Action

With the automatic action 'Subscription maintenance' you can remove subscription entries relating to all archive objects from the database according to particular date criteria.



Subscription maintenance

Delete all subscription entries which ...

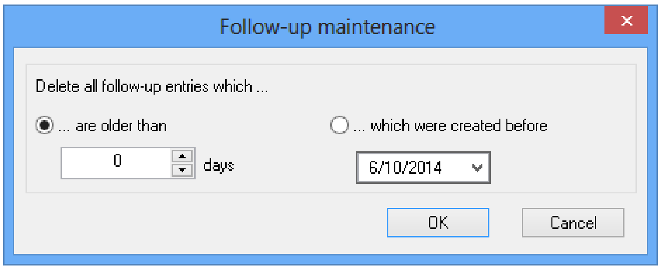
● ... are older than 0 days.

○ ... were created before 6/10/2014 .

To use this action, add the `axacabo.dll` library.

'Follow-up Maintenance' Action

With the automatic action 'Follow-up maintenance' you can remove follow-up entries relating to all archive objects from the database according to particular date criteria.



Follow-up maintenance

Delete all follow-up entries which ...

● ... are older than 0 days

○ ... which were created before 6/10/2014

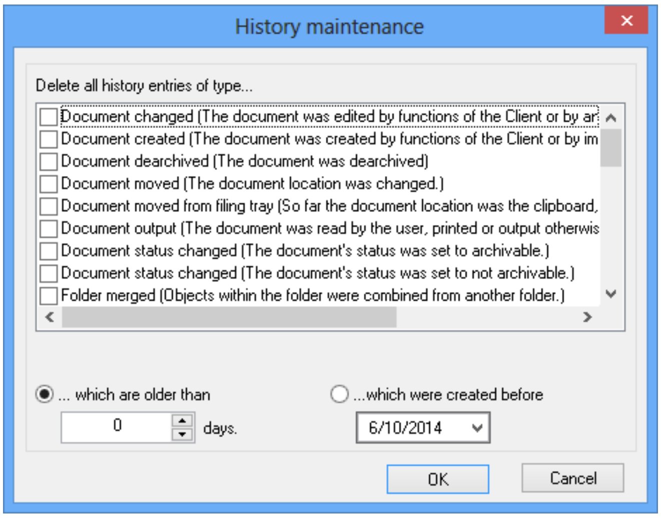
To use this action, add the `axacwdvl.dll` library.

'History Maintenance' Action

enaio® automatically maintains an editing history for all archive objects: folders, registers, and documents. In enaio® editor, an index data history concerning folder and register types, and a document history concerning document types can be set up.

The data for the editing history, the index data history and the document history are saved to the database, whereas documents relating to the document history are saved in the file system. This data may occupy a large amount of storage space in the database and file system.

The 'History maintenance' automatic action can be used to remove data of the editing history from the database and documents from the document history according to specified date criteria.



Delete all history entries of type...

- □ Document changed (The document was edited by functions of the Client or by ar
- □ Document created (The document was created by functions of the Client or by im
- □ Document dearchived (The document was dearchived)
- □ Document moved (The document location was changed.)
- □ Document moved from filing tray (So far the document location was the clipboard,
- □ Document output (The document was read by the user, printed or output otherwis
- □ Document status changed (The document's status was set to archivable.)
- □ Document status changed (The document's status was set to not archivable.)
- □ Folder merged (Objects within the folder were combined from another folder.)

● ... which are older than 0 days.

○ ...which were created before 6/10/2014

The following types of history entries can be deleted:

- **User info**

  Database entries concerning additional information specified by users will be deleted.

- **Owner of the object changed**

  Database entries concerning object owners will be deleted.

- **Document archived**

  Database entries concerning archiving processes will be deleted.

- **Document moved from filing tray**

  Database entries concerning moving actions from the filing tray will be deleted.

- **Document output**

  Database entries concerning document, register and folder output will be deleted.

- **Document created**

  Database entries concerning document, register, and folder creation by the client or an import process will be deleted.

- **Document modified**

  Database entries concerning changes to documents, registers and folders will be deleted.

- **Document deleted**

  Database entries concerning document, register and folder deletion will be deleted.

- **Document moved**

  Database entries concerning changed locations will be deleted.

- **Document status modified**

  Database entries concerning state modification of documents, registers and folders will be deleted.

- **Index data modified**

  The database entries concerning changes to the index data of documents, registers and folders will be deleted. Versions of the index data will also be deleted.

- **Content changed**

  Database entries concerning changes to documents, registers, and folders will be deleted.

- **Acknowledgement of notification confirmed**

  Database entries concerning information about confirmation of notice will be deleted.

- **Object deleted permanently**

  Database entries concerning permanent deletion of objects will be deleted.

- **Object restored**

  Database entries concerning object recovery from the trash can will be deleted.

- **Object flagged for deletion**

  Database entries concerning information about trash can objects will be deleted.

- **Object info**

  Database entries concerning business logic log entries will be deleted.

- **Folders merged**

  Database entries concerning object merging into a folder will be deleted.

- **Register moved**

  Database entries concerning changed register locations will be deleted.

- **Registers merged**

  Database entries concerning object merging into a register will be deleted.

- **Signed document deleted**

  Database entries concerning deletion of signed documents will be deleted.

- **SQL query**

  Database entries concerning information about data queried through SQL statements will be deleted.

- **SQL command**

  Database entries concerning information about data changed through SQL statements will be deleted.

- **Assign type to typeless object**

Database entries concerning object type assignments to typeless objects will be deleted.

- **Variant activated**

  Database entries concerning defining a document as the active variant will be deleted.

- **Variant created**

  Database entries concerning variant creation will be deleted.

- **Variant disabled**

  Database entries concerning removing the 'active variant' status from a document will be deleted.

- **Variant deleted**

  Database entries concerning variant deletion will be deleted.

- **Link terminated**

  Database entries concerning reference deletion will be deleted.

- **Link about notes**

  Database entries concerning notes link creation will be deleted.

- **Version created**

  Database entries concerning document version creation will be deleted.

- **Version deleted**

  Database entries concerning document version deletion will be deleted.

- **Reference document created**

  Database entries for creation of reference documents will be deleted.

- **Full-text query**

  Database entries concerning full text queries against the data pool will be deleted.

- **Restored from version**

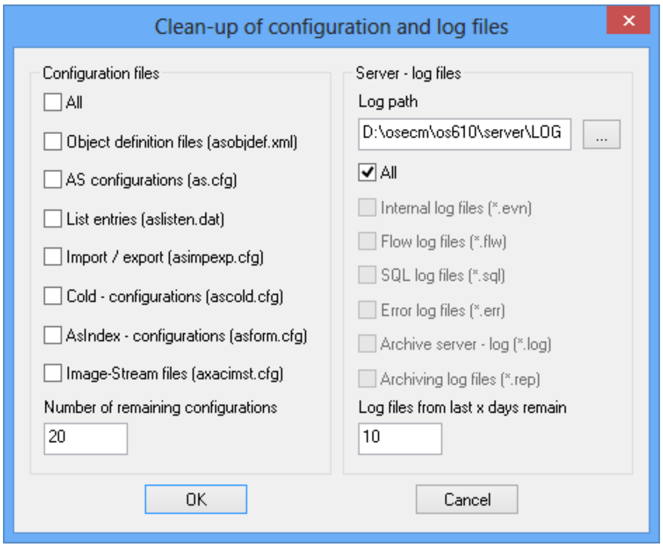
  Database entries concerning document recovery on the basis of previous document versions will be deleted.

> Data which refer to digital signatures cannot be deleted.

To use this action, add the `axachist.dll` library.

'Cleanup of Configuration and Log Files' Action

The 'Cleanup of configuration and log files' action deletes old configuration versions and server log files.



Clean-up of configuration and log files

Configuration files

- □ All
- □ Object definition files (asobjdef.xml)
- □ AS configurations (as.cfg)
- □ List entries (aslisten.dat)
- □ Import / export (asimpexp.cfg)
- □ Cold - configurations (ascold.cfg)
- □ AsIndex - configurations (asform.cfg)
- □ Image-Stream files (axacimst.cfg)

Number of remaining configurations: 20

Server - log files

Log path: D:\osecm\os610\server\LOG

- ☑ All
- □ Internal log files (*.evn)
- □ Flow log files (*.flw)
- □ SQL log files (*.sql)
- □ Error log files (*.err)
- □ Archive server - log (*.log)
- □ Archiving log files (*.rep)

Log files from last x days remain: 10

In the **Configuration files** area, select the file types from which old versions are to be deleted and enter how many versions must be kept.

In the **Server log files** area enter the path to the log directory, select the log types of which old logs are to be deleted and specify the period of time of which logs will be kept.

To use this action, add the `axaccl.dll` library.

'Database Statistics Update' Action

Database statistics should be regularly updated for optimal access performance to the database.

The 'Database statistics update' action uses the SQL command `update statistics on database` to update the index statistics.

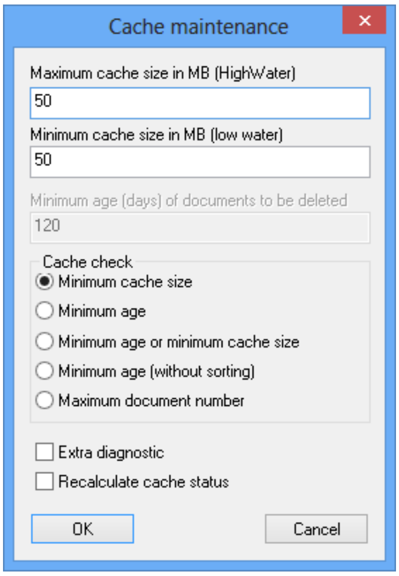
No configuration is required for this action.

To use this action, add the `axacdbst.dll` library.

'Cache Maintenance' Action

The 'Cache maintenance' action lets you manage the cache. Copies of archived documents which have been recently used and documents of other server groups which were handed over by the automatic action 'Document retrieval' are stored to the cache area in order to allow for quick access. The documents remain in the cache until the maximum cache size is exceeded. At that point, the oldest documents will be deleted from the cache until the minimum cache size is reached. The 'Cache maintenance' action can be used to actively clear the cache rather than leaving it to enaio® server.

To use this action, add the `axaccach.dll` library.



Cache maintenance

Maximum cache size in MB (HighWater)
50

Minimum cache size in MB (low water)
50

Minimum age (days) of documents to be deleted
120

Cache check
● Minimum cache size
○ Minimum age
○ Minimum age or minimum cache size
○ Minimum age (without sorting)
○ Maximum document number

□ Extra diagnostic
□ Recalculate cache status

Enter a **HighWater mark**, a **LowWater mark**, a **Minimum age** for the documents to be deleted, and a priority:

- **Minimal cache size**

  Is the priority set to the minimum cache size, exceeding the high water mark causes documents to be deleted from the cache in descending order of age until the low water mark is reached. This may involve the deletion of documents which have not yet reached the minimum age.

- **Minimum age**

  Is the priority set to the minimum age, all documents older than the minimum age will be deleted, irrespective of the cache size. This is intended to ensure that at least the documents of the specified period are available in the cache. The low water mark does not have to be reached.

- **Minimum age or minimum cache size**

  This option deletes documents either if the specified minimum age is reached or the specified cache size exceeded.

- **Minimum age (without sorting)**

  This corresponds to the **Minimum age** option. Without sorting, it may happen that instead of entire documents individual document pages are deleted. For very large caches, clearing the cache without sorting is significantly faster.

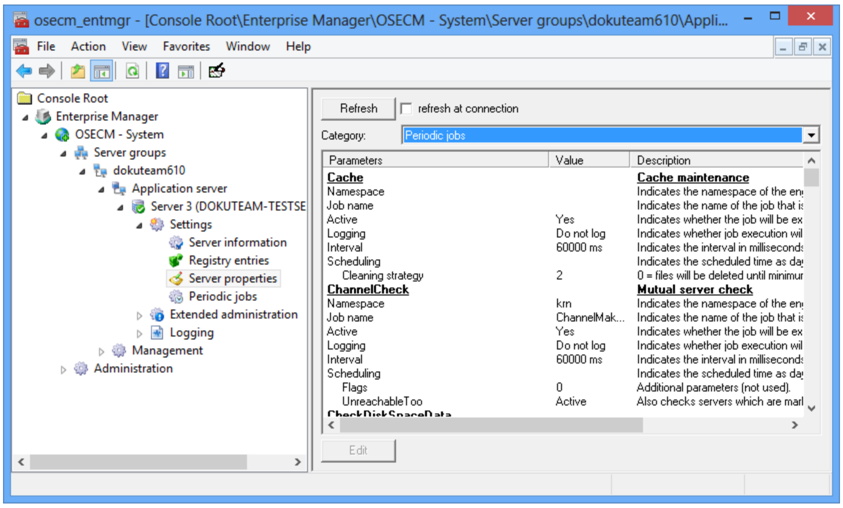
- **Maximum document number**

  Is the priority set to the maximum document number, the specified number of documents will be kept in the cache. Enter a value into the first field. It will be multiplied by 1000.

Independently from the configured logging, the 'Cache maintenance' action writes a report with the name `cleanup.rep` to the server's root directory. If you select the option **Extra diagnostics**, the report will list all documents that have been deleted. With the activated **Recalculate cache status** option, the cache status will be recalculated after the cache has been cleared. The cache state lists data such as the cache size, available storage space and the number of cached documents.

Cache maintenance can also be run automatically. To do so, you have to configure respective registry entries with enaio® enterprise-manager.

Using the **Settings > Server properties > Category: Periodic jobs** area, you can configure automatic cache maintenance:



□ refresh at connection

Category: Periodic jobs

Parameters	Value	Description
Cache		**Cache maintenance**
Namespace		Indicates the namespace of the en
Job name		Indicates the name of the job that i
Active	Yes	Indicates whether the job will be ex
Logging	Do not log	Indicates whether job execution wil
Interval	60000 ms	Indicates the interval in millisecond
Scheduling		Indicates the scheduled time as da
Cleaning strategy	2	0 = files will be deleted until minimu
ChannelCheck		**Mutual server check**
Namespace	krn	Indicates the namespace of the en
Job name	ChannelMak...	Indicates the name of the job that i
Active	Yes	Indicates whether the job will be ex
Logging	Do not log	Indicates whether job execution wil
Interval	60000 ms	Indicates the interval in millisecond
Scheduling		Indicates the scheduled time as da
Flags	0	Additional parameters (not used).
UnreachableToo	Active	Also checks servers which are mar
CheckDiskSpaceData		

Double clicking an entry will open a dialog which allows you to change the value.

You can insert the following values as parameters for the **Cleaning strategy**:

0 priority according to cache size

1 priority according to minimum age

2 priority according to the condition first met

Duly specify an upper limit in MB (**HighWater**), a lower limit in MB (**LowWater**)and a minimum age in days.

The parameter **Active** is used to switch cache maintenance on or off.

The parameter **Logging** is used to switch cache maintenance logging on or off.

The execution is further configured by specifying a period of time in milliseconds using the **Interval** parameter and a scheduled point of time that follows the syntax 'day of the week:hours:minutes' through the **Scheduling** parameter.

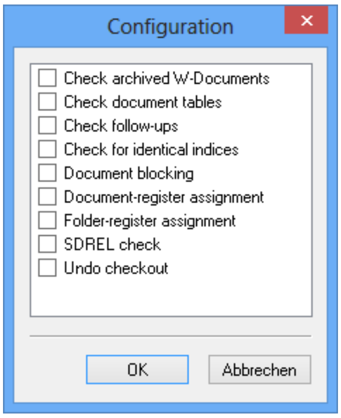
If you want the cache to be cleared periodically at a specific time, use the **Settings > Periodic jobs** area to configure it.

'System Checks' Action

The 'System checks' action makes functions available which allow you to remove inconsistencies found in the archive and in database tables. This function must only be used after careful analysis and after being asked to do so by the support team.

To use this action, add the `axacsysc.dll` library.

The 'System checks' action can also be used in order to remove the 'checked out' property of all W-Documents if, for example, it is impossible for a user to check his documents back in. However, it must be used carefully because users who have opened W-Documents will not be able to save their changes if, in the meantime, you have removed the 'checked out' property from all W-documents.



□ Check archived W-Documents
□ Check document tables
□ Check follow-ups
□ Check for identical indices
□ Document blocking
□ Document-register assignment
□ Folder-register assignment
□ SDREL check
□ Undo checkout

The configuration dialog offers the following functions:

- **Check archived W-Documents**

  Archived W-documents that incorrectly remain in the work area and could have been edited are given the status 'approved for archiving.'

- **Check for identical indices**

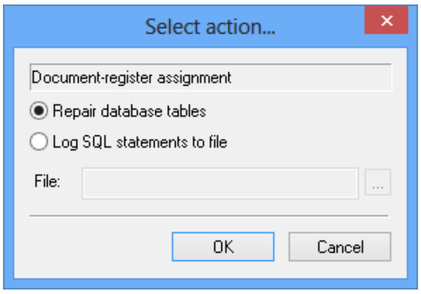
  It is checked whether objects have identical object ID's.

- **Cancel checkout**

  The 'checked out' property is removed for all documents.

- **Document register assignment**

  Storage locations of documents in registers which have been deleted but by mistake remained in the database tables will be deleted from the database.

  Document-register assignment
  ● Repair database tables
  ○ Log SQL statements to file
  File:

  Instead of immediately repairing database tables, you can have the check result written to a file.

- **Document blocking**

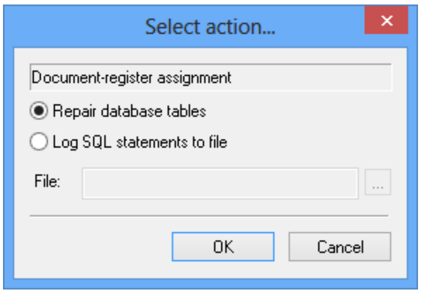
  This function checks whether the 'checked out' property is consistently used in the database tables.

- **Check document tables**

  Documents that have been deleted from the location tables but by mistake remained in the object tables will be deleted from the object tables.

- **Folder-register assignment**

The filing locations of registers in folders which have been deleted but by mistake remained in the database tables will be deleted from the database



Instead of immediately repairing database tables, you can have the check result written to a file.

§ **SDREL check**

It is checked whether document ID, folder ID or register ID/register type are entered more than once in the SDREL table. If so, they are deleted, keeping only one single.

§ **Unbound documents**

Documents that have no location because of errors are placed in the filing tray of the specified user.

§ **Orphaned reference documents**

If documents that refer to reference documents are deleted, the reference documents are not deleted with them. The action creates a file with information – ID and object type ID – about all reference documents without a reference. During configuration, specify the folder where the file is saved.

The file has the name 'SYSCHECK13-YYYYMMDD-HHMMSS.txt.'

File name and path are written to the flow log.

§ **Check follow-ups**

References to documents that have been deleted but mistakenly remained in the follow-up tables will be deleted from the database.

'Prearchiving' Action

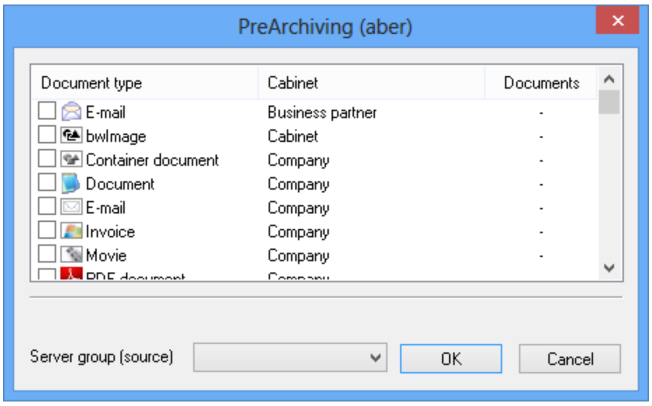
The 'Prearchiving' action passes all of a server group's documents that are not yet archived to the server group through which the automatic action is run. The documents are passed to the WORK area; and the modified server group assignment is inserted into the database.

This transfer can be useful if the documents with this server group are to be archived.

Only documents released for archiving are transferred.

To use this action, add the `axacwtow.dll` library (see ''Additions').

When setting up the automatic action (see 'Setting Up Automatic Actions'), in the configuration dialog, specify a configuration name and select the document types whose documents are to be transferred. Also specify of which server group the documents will be passed.



Document type	Cabinet	Documents
□ E-mail	Business partner	-
□ bwImage	Cabinet	-
□ Container document	Company	-
□ Document	Company	-
□ E-mail	Company	-
□ Invoice	Company	-
□ Movie	Company	-
□ PDF document	Company	

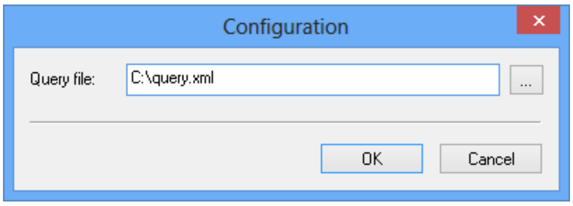
'Document Retrieval' Action

The 'Document retrieval' action transfers documents from all server groups to the cache area of the server group that carries out the automatic action.

In environments comprising multiple server groups, documents which are requested by a client but managed by another server group are passed between the server groups. If the server groups are connected by a slow telecommunication facility, these transfers may cause high network load and thus require long access times. If, for example, documents are created within one server group and viewed within another one, the 'Document retrieval' action can be used to have the documents be passed at a time network load is reduced. The documents are then passed to the cache area of the respective server group.

To use this action, add the `axacpref.dll` library (see ''Additions').

When setting up the automatic action (see 'Setting Up Automatic Actions'), specify a configuration name and choose a query file in the configuration dialog.



Query file: C:\query.xml

The query file is used to select which documents are to be handed over.

You can create the query file with any arbitrary text editor. It has the following structure:

`[ANFRAGE]`	The file begins with the 'query' section.
`SCHRANK=cabinet name`	Enter the name of the cabinet that the documents originate from into the first line.
`DOKUMENT=document type name`	The document type of the documents comes in the second line.

`KLAUSEL1=Objekt@Feld=Wert`
`...`
	Optional logic expressions allow you to limit the selection to those documents that fulfill these

`KLAUSELn=Objekt@Feld=Wert`	conditions. Logical expressions must be numbered consecutively.

Use internal names and enclose the name in percent signs.

Logical Expressions

Optional logic expressions allow you to limit the selection to those documents that are indexed with the indicated value in the indicated field.

Example:

```
Klausel1=Kunde@Status=abgeschlossen
```

Documents of the indicated document type will be passed only if the index data of the archive object type 'Customer', e.g. a folder, contains the value 'completed' in the field 'Status'.

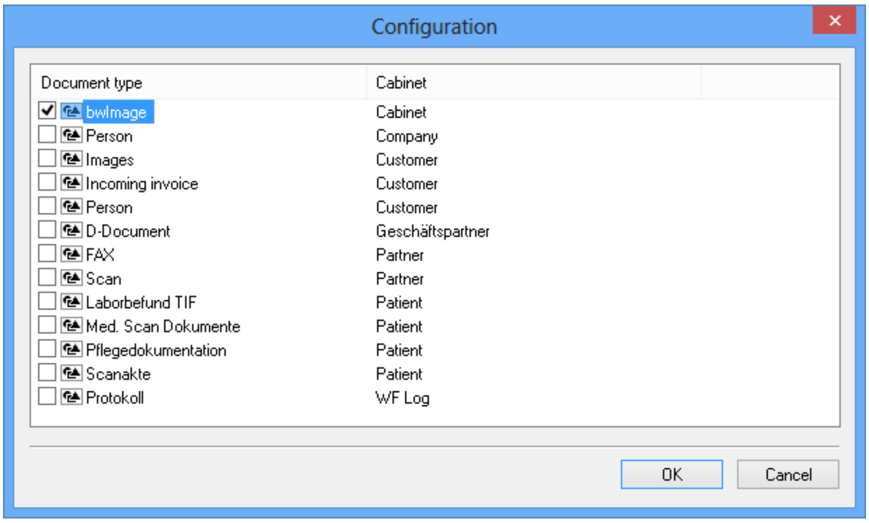
'Creation of Multi-Page TIFF' Action

The 'Creation of multi-page TIFF' action converts image files of black and white documents to multi-page TIF's.

Administering black and white images of a document as individual TIF's requires significantly more space than multi-page TIF's. It may therefore be useful, particularly before the archiving process, to compile individual images of a document to a multi-page TIF.

To use this action, add the `axacmtif.dll` library (see ''Additions').

When setting up the automatic action (see 'Setting Up Automatic Actions'), specify a configuration name and choose the black and white document types you want to run the action for.



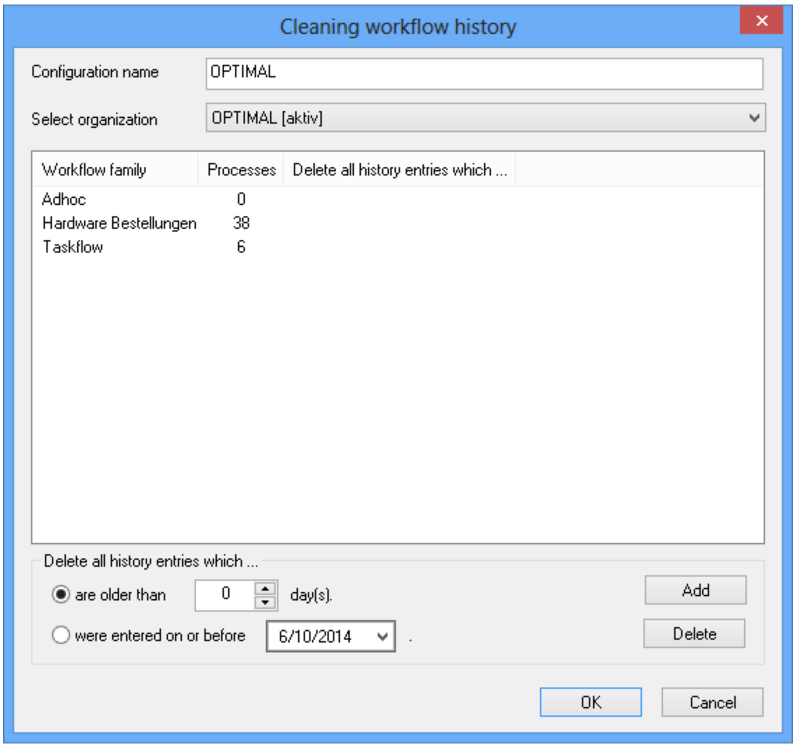
Document type	Cabinet
☑ bwImage	Cabinet
□ Person	Company
□ Images	Customer
□ Incoming invoice	Customer
□ Person	Customer
□ D-Document	Geschäftspartner
□ FAX	Partner
□ Scan	Partner
□ Laborbefund TIF	Patient
□ Med. Scan Dokumente	Patient
□ Pflegedokumentation	Patient
□ Scanakte	Patient
□ Protokoll	WF Log

'Cleaning Workflow History' Action

The history entries of completed workflow processes can be individually deleted from the database using enaio® administrator for workflow or according to specific criteria using the 'Cleaning workflow history' action.

To use this action, add the `axacwfhclear.dll` library (see ''Additions').

In the configuration dialog, enter a configuration name and select the organization to which the processes are assigned.



Cleaning workflow history

Configuration name: OPTIMAL

Select organization: OPTIMAL [aktiv]

Workflow family	Processes	Delete all history entries which ...
Adhoc	0	
Hardware Bestellungen	38	
Taskflow	6	

Delete all history entries which ...

● are older than 0 day(s).

○ were entered on or before 6/10/2014 .

All workflow families that are assigned to the selected organization will be listed.

Select a workflow family, enter a period of time in days or a date in the past and click **Add**. You can delete the configuration data of the selected family by clicking the **Delete** button.

The action will then delete history entries which are older than or were entered before the indicated date.

Confirm with **OK**. The configuration will be saved and the action can be performed by use of enaio® administrator or scheduled using enaio® start.

'Process Archiving Workflow' Action

The 'Process archiving workflow' action saves information on expired processes as XML or PDF document in enaio®.

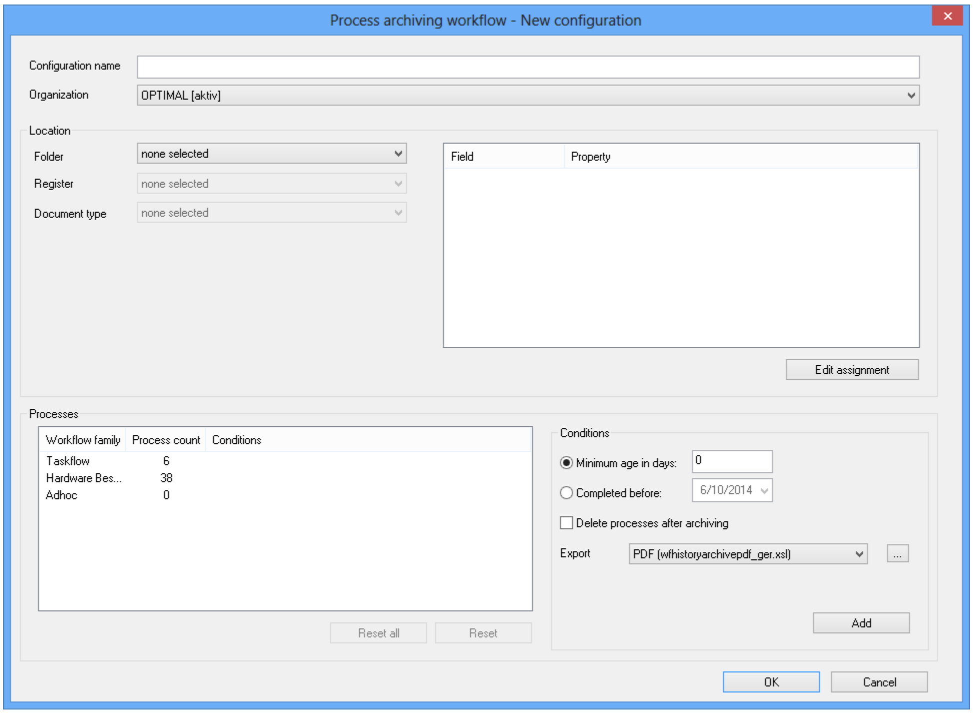
The following information on a process is grouped:

- All activities with time of creation, end time, and editor.
- All global variables and their last values.
- The workflow log with the information on all steps including date, time, activity, editor, and action.
- All deadlines with assignment to activities.
- All events with assignment to activities.

Specify folder, register and document type, assign the process' basic data to the index data fields of objects and define the processes of which you want the data to be saved.

To use this action, add the `axacwfharch.dll` library (see ''Additions').

In the configuration dialog, enter a configuration name and select the organization to which the processes are assigned. After that, define the location and the processes.



Configuration name:

Organization: OPTIMAL [aktiv]

Location

Folder: none selected

Register: none selected

Document type: none selected

Field	Property

Processes

Workflow family	Process count	Conditions
Taskflow	6	
Hardware Bes...	38	
Adhoc	0	

Conditions

● Minimum age in days: 0

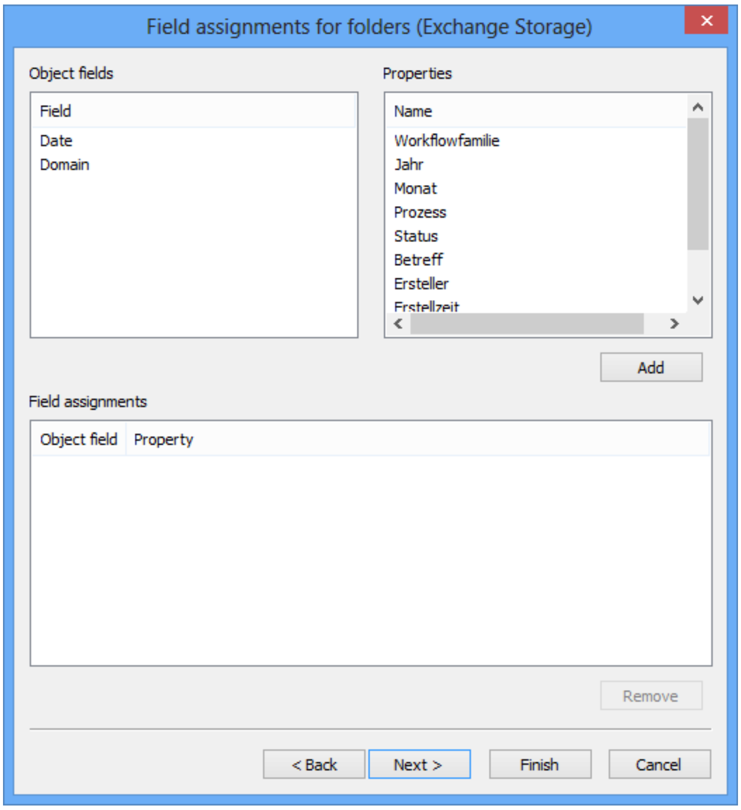
○ Completed before: 6/10/2014

□ Delete processes after archiving

Export: PDF (wfhistoryarchivepdf_ger.xsl)

Select the folder, register, and document type in the **Location** area. Process data can be saved as XML or PDF documents. Select a document type which is suited for the administration of the file format.

Create and edit the assignments of the processes' basic data to the index data fields of objects in enaio® through the **Edit assignment** button:



> Fields can be assigned only to enaio® fields of the database type 'all characters' and with internal field names. Fields on page controls are not yet available.

In the **Object fields** area, at first select an index data field of the folder type and, in the **Properties** field, a basic property of the process. Click on the **Add** button to pass the assignment to the **Field assignments** area.

After assigning the object fields to the folder type, click the **Next** button to assign them to the register type and, if it has not been specified, to the document type.

Click the **Finish** button to complete the assignments. The assignment dialog will close and all data shown in the configuration dialog.

In the **Processes** area, workflow families with their number of available processes are listed.

Select an entry and create a condition by specifying a minimum age in days or a by date. You can additionally define whether to delete process data of archived processes.

Then select XML or PDF as the format of the export file. The XML format is suited for XML document types, whereas the PDF format is recommended to be chosen for image document types and W-Document types.

When selecting the PDF format, an XSL style sheet must be specified, which is intended to be used to format the data. The style sheet `wfhistoryarchivepdf_ger.xsl` from the `\clients\admin` directory is specified by default. In addition to the German version, the directory also contains an English version of the style sheet.

To add the condition to the list of workflow families, click on the **Add** button.

To delete a condition, select an entry of the list of workflow families and click the **Reset** button.

Confirm with **OK**. The configuration will be saved and the action can be performed by use of enaio® administrator or scheduled using enaio® start.

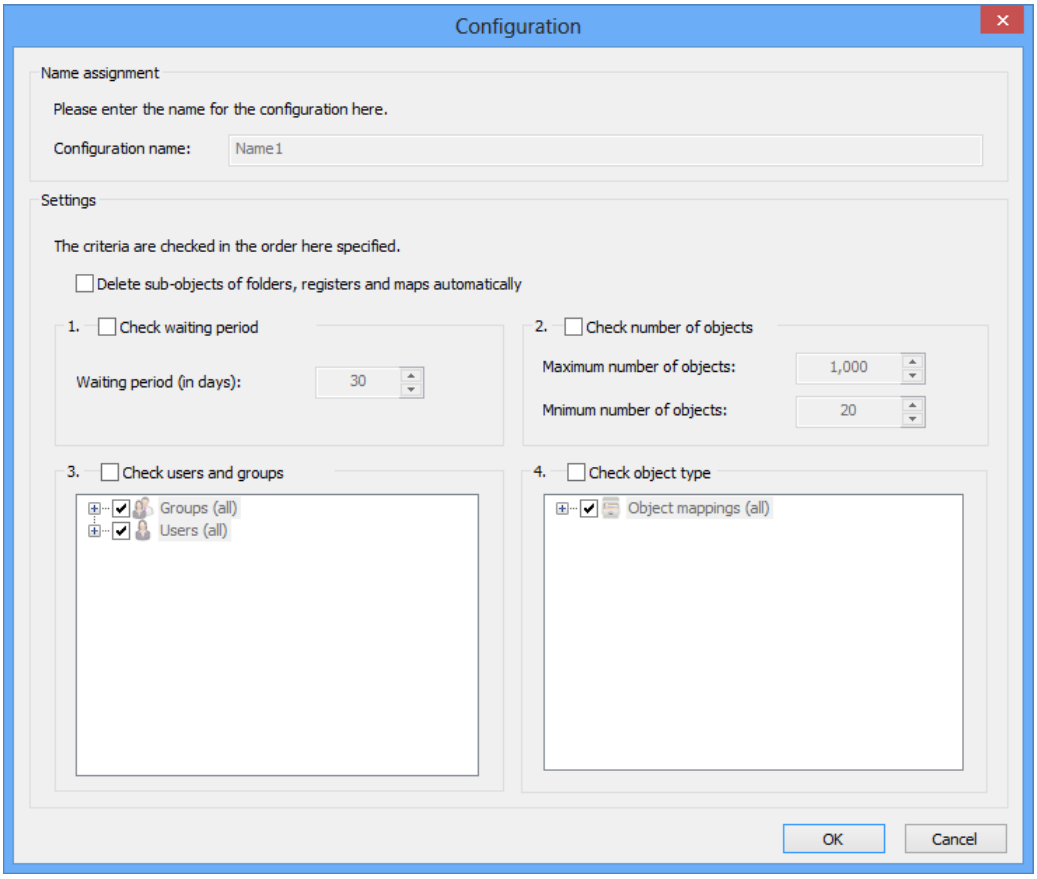
'Empty Trash Can' Action

If a user deletes an object, it is in the first place moved to the trash can from which it can be permanently deleted by users with the corresponding system role.

The 'Empty trash can' action permits you to permanently delete objects from the trash can according to specified rules.

To use this action, add the `axaccleantrash.dll` library (see ''Additions').

A configuration name is entered on the configuration dialog. The configuration name must not contain any space character. Decide whether the contents of folders, registers and portfolios are to be deleted if they meet the deletion criteria.



Name assignment

Please enter the name for the configuration here.

Configuration name: Name1

Settings

The criteria are checked in the order here specified.

☐ Delete sub-objects of folders, registers and maps automatically

1. ☐ Check waiting period

Waiting period (in days): 30

2. ☐ Check number of objects

Maximum number of objects: 1,000

Mnimum number of objects: 20

3. ☐ Check users and groups

☑ Groups (all)

☑ Users (all)

4. ☐ Check object type

☑ Object mappings (all)

You can specify the following criteria:

- **Waiting period**

  Enter a waiting period (in days) to delete only objects that have been in the trash can for at least this period of time.

- **Number of objects**

Activate this option to only delete objects once the maximum number of objects in the trash is exceeded. Deletion will always be stopped when the minimum number of objects is reached.

- **Users and groups**

  Only those objects will be deleted which have been moved to the trash can by the selected users/group members.

- **Object types**

  Only objects of the selected object types will be deleted.

The criteria are always checked in this order.

Confirm with **OK**. The configuration will be saved and the action can be performed by use of enaio® administrator or scheduled using enaio® start.

'Delete Objects' Action

The 'Delete objects' action is used to delete all objects that are specified in a query file from enaio® server. It can be used to delete folders, registers and documents.

When deleting folders or registers, the entire contents are deleted recursively.

Objects with more than one location will be deleted from all locations.

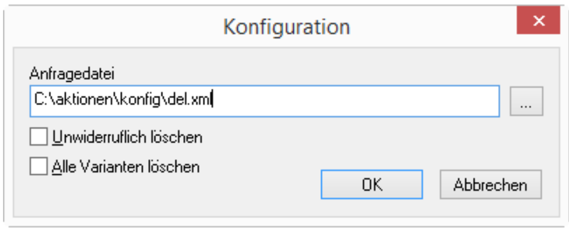
To use this action, add the `axacdel.dll` library (see ''Additions').

When setting up the automatic action (see 'Setting Up Automatic Actions'), specify a configuration name and choose a query file in the configuration dialog.

You can also establish whether the objects are permanently deleted or moved to the enaio® system trash can.

In the case of objects with variants, the active variant and all sub-variants are deleted. Use the corresponding option to delete all variants.

> Keep in mind that by activating the **Permanently delete** option, objects are removed completely and cannot be recovered.



Anfragedatei: C:\aktionen\konfig\del.xml

□ Unwiderruflich löschen

□ Alle Varianten löschen

In the query file specify the documents, registers and folders to be deleted.

You can create the query file with any arbitrary text editor. It has the following structure:

```
[ANFRAGE]
```

The file begins with the 'query' section.

```
SCHRANK=cabinet name
```

Enter the name of the cabinet to be deleted into the first line.

	Deleting registers and documents also requires to specify the cabinet of which the objects originate from.

`REGISTER=register type name`
`DOKUMENT=document type name`
	Insert the register type of the registers or the document type of the document to be deleted into the second line.

`KLAUSEL1=Objekt@Feld=Wert`
`...`
`KLAUSELn=Objekt@Feld=Wert`
	Optional logical expressions allow you to limit the selection to those objects that fulfill these conditions.
	Logical expressions must be numbered consecutively.

`Ausdruck1=Object@Field^Operator^Value`
`...`
`Ausdruckn=Object@Field^Operator^Value`
	Optional logic expressions allow you to limit the selection to those objects that correspond to these expressions.
	Logic expressions must be numbered consecutively.

Use internal names and enclose the name in percent signs.

The automatic action 'Delete objects' can be used to delete documents whose retention period has already expired.

Such objects are determined using an expression in the query file.

Example:

```
Ausdruck1=Object@1904^5^15.5.2011
```

'`1904`' is the database column containing the retention date, '`^5^`' is the comparison operator '<=' and '`15.5.2011`' is a date.'

All objects having a retention date that equals 15.5.2001 or lies before it will be deleted.

Details on expressions and operators can be found in the 'OS_Client-Programming-Reference' handbook.

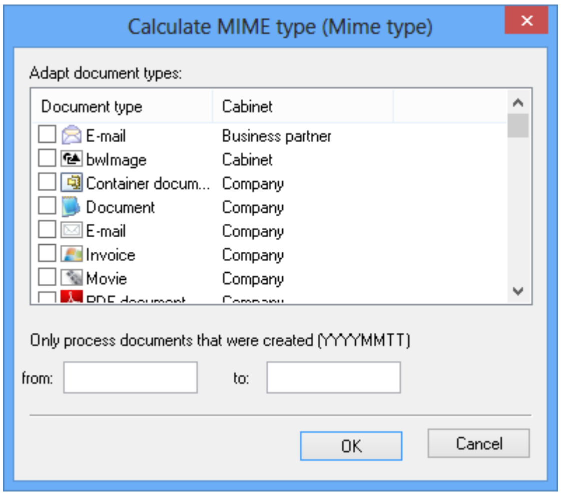
'Calculate MIME Type' Action

Since enaio® version 5.20, the MIME type and the file size of all document files are saved automatically. These data are accessible in the object information.

With the 'Calculate MIME type' action, you can have these data generated for older documents.

To use this action, add the `axacmtype.dll` library (see "Additions').

In the configuration dialog, enter a configuration name, the intended document types, and, optionally, the time-span in which the documents were created.



Calculate MIME type (Mime type)

Adapt document types:

Document type	Cabinet
☐ E-mail	Business partner
☐ bwImage	Cabinet
☐ Container docum...	Company
☐ Document	Company
☐ E-mail	Company
☐ Invoice	Company
☐ Movie	Company
☐ PDF document	Company

Only process documents that were created (YYYYMMTT)

from:

to:

'Pagination' Action

Pagination is a method for marking each page of a document with a label. The automatic action 'Pagination' allows you to paginate image documents from a particular folder before archiving.

Image documents which are administered in PDF format cannot be labeled.

The pagination can be positioned as you wish and has the format 'document xx, page yy or zz,' where 'xx' stands for the sequential number of the document in the relevant folder. This number is determined from the order of capture in the folder, i.e. the oldest document approved for archiving gets the lowest available number. 'yy' stands for the latest page number and 'zz' for the number of pages in the document.

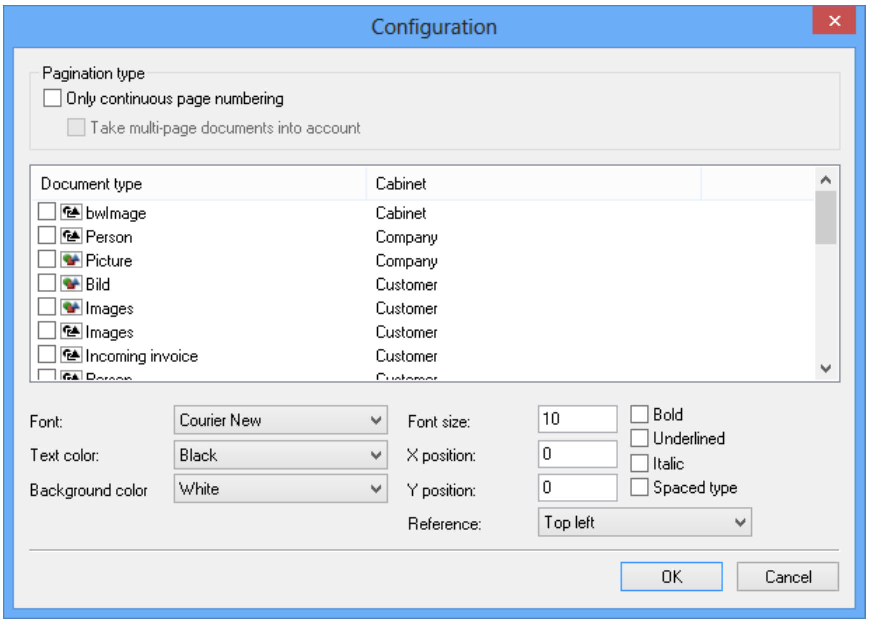
It is also possible to consecutively number all pages of all documents.

If a folder contains documents which have already been paginated and archived, the numbering is continued.

To use this action, add the `axacpage.dll` library (see ''Additions'). In addition, the license key 'PAG' is required.

When setting up the automatic action (see 'Setting Up Automatic Actions'), specify a configuration name.

The pagination is configured using the following dialog:



Pagination type

□ Only continuous page numbering

□ Take multi-page documents into account

Document type	Cabinet
□ bwImage	Cabinet
□ Person	Company
□ Picture	Company
□ Bild	Customer
□ Images	Customer
□ Images	Customer
□ Incoming invoice	Customer
□ Person	Customer

Font: Courier New

Text color: Black

Background color: White

Font size: 10

X position: 0

Y position: 0

Reference: Top left

□ Bold

□ Underlined

□ Italic

□ Spaced type

Select the pagination type, the document types, the position, and the formatting of the label.

Pagination has the format 'Document xx, Page yy of zz.' As an alternative, you can append continuous page numbering.

When using continuous page numbering, you can also decide whether or not to take account of multi-page documents. If a folder already contains paginated and archived documents in multi-page TIF format, the pagination action must access these archived, multi-page documents in order to determine the correct page number. The **Take multi-page documents into account** option is to be selected only for this case.

Select the document types to which you want append the pagination from the list. Use the fields **Font**, **Text color**, **Background color**, **Font size**, **Bold**, **Underlined**, **Italic**, and **Spaced type** to specify the attributes of the pagination. In the **Reference** field, you can define the reference point X and Y coordinates. Potential points are **Top left**, **Bottom left**, **Top right**, and **Bottom right**, which refer to the relevant corners of the printable area. Both the **X position** and the **Y position** fields are used to define the distance in millimeters between the pagination and the reference point. Positive integers must be entered only. The action 'Pagination' automatically determines the respective position within the printing area depending on the reference point.

The 'Pagination' action will also process reference documents. To avoid this, you can disable the creation of reference documents throughout the entire system. Moreover, it is possible to prevent documents or archived documents from being moved (see ''Documents'). After the 'Pagination' action was executed, the state 'approved for archiving' is kept by all paginated documents. Archive these documents before the 'Pagination' action is carried out again, otherwise they would be paginated anew. If you want to perform the 'Archiving' action immediately after the 'Pagination' action, you can let them be carried out as an action sequence.

'Database Query' Action

The automatic action 'Database query' allows you to send SQL queries to the enaio® database. The results can be saved to a file.

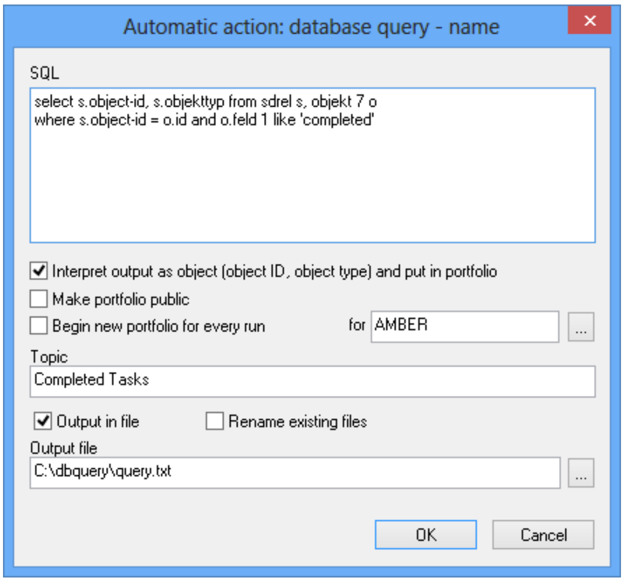
If the SQL result contains exactly two integer columns, these may be identified as object ID and object type and saved in the portfolio of a particular user. The combination of several queries and different users permits you to periodically query and distribute task packages.

By saving the results of the query to a file, it is possible to regularly create reports on the data pool which are then stored in the file system for further processing. The results of such a database query are saved in semicolon separated file format (CSV).

To use this action, add the `axacreq.dll` library (see ''Additions').

When setting up the automatic action (see 'Setting Up Automatic Actions'), specify a configuration name.

The database query is configured through the following dialog:



SQL

```
select s.object-id, s.objekttyp from sdrel s, objekt 7 o
where s.object-id = o.id and o.feld 1 like 'completed'
```

☑ Interpret output as object (object ID, object type) and put in portfolio

□ Make portfolio public

□ Begin new portfolio for every run — for: AMBER

Topic: Completed Tasks

☑ Output in file — □ Rename existing files

Output file: C:\dbquery\query.txt

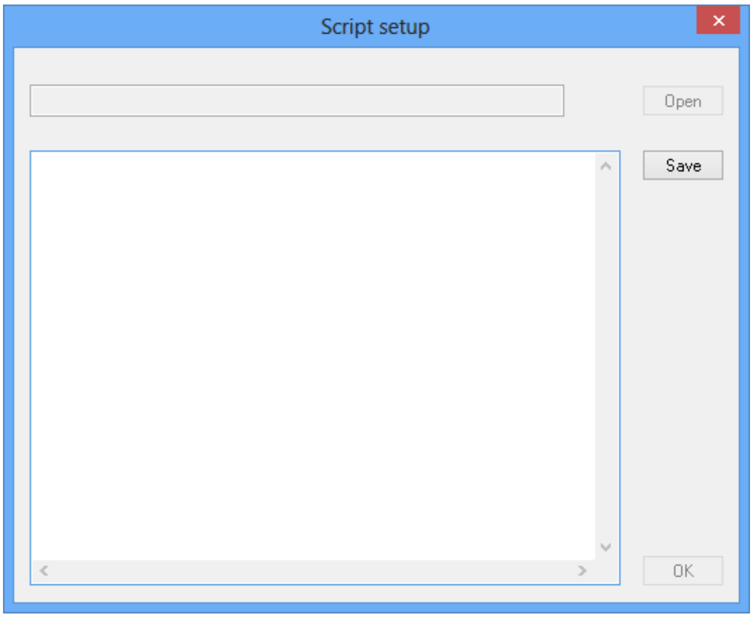
'Run Script' Action

The automatic 'Run script' action allows you to run VBScript code. Within the scripts it is possible to use objects that are provided by Windows, enaio® or other products. It is recommended to apply the action when enaio® start is used to periodically perform actions accessing enaio®. For example, the action allows for periodic report creation regarding enaio®. Alternatively, scripts can be executed by an external scheduler, but the enaio® objects will not be initialized. The initialization of enaio® objects will be guaranteed by the runtime environment of enaio® start or enaio® administrator.

To use this action, add the `axacscript.dll` library (see ''Additions').

When setting up the automatic action (see 'Setting Up Automatic Actions'), specify a configuration name.

The action is configured using the following dialog:



The script to be executed will be saved in the file system.

'Rendition' Action

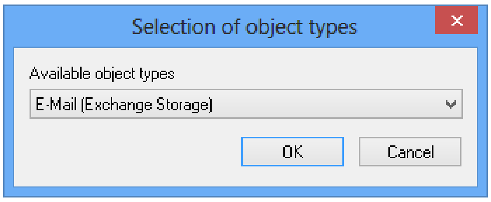
The 'Rendition' action creates copies in TIFF G4 or PDF file format of W-Documents and image documents and an additional variants of W-Documents.

Two check boxes are required on the data sheet of the document type, one as a selection check box and one as an error-indicator check box.

The action is only performed for documents that have their selection check box checked. After the action has been performed, the selection check box will be unchecked. If an error occurs, the error-indicator check box will be checked. Documents with active error-indicator check boxes will not be processed by this action.

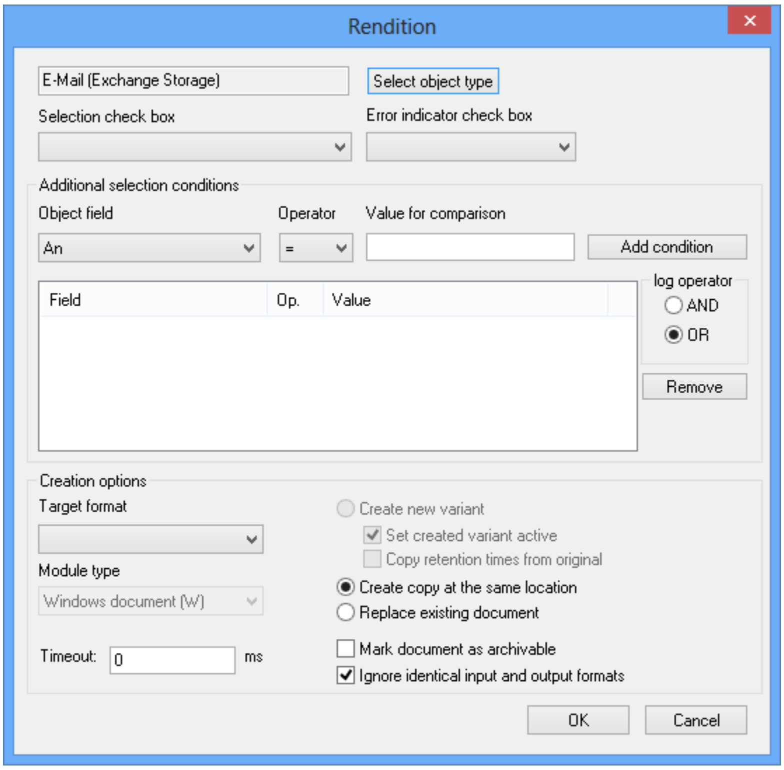
To use this action, add the `axacdok2tif.dll` library (see ''Additions').

When setting up the automatic action (see 'Setting Up Automatic Actions'), specify a configuration name and select the document type.



Available object types: E-Mail (Exchange Storage)

The configuration dialog will open.



E-Mail (Exchange Storage)

Selection check box

Error indicator check box

Additional selection conditions

Object field: An

Operator: =

Value for comparison

Field	Op.	Value

log operator

○ AND

● OR

Creation options

Target format

Module type: Windows document (W)

Timeout: 0 ms

○ Create new variant

☑ Set created variant active

□ Copy retention times from original

● Create copy at the same location

○ Replace existing document

□ Mark document as archivable

☑ Ignore identical input and output formats

Choose which check box serves as the selection and the error-indicator check box.

Selection conditions are optional. The fields **Object field**, **Operator**, and **Value for comparison** allow you to create conditions and to logically combine them. Variants in the selected target format will only be created if a document’s index data fulfill the conditions.

Decide whether you want a copy to be created or whether the document files of the existing document will be replaced by the converted document files. In terms of W-Documents, you can create a variant of the converted document file. The variant created that way can be flagged as the active variant. The scheduled retention period can be appended to variants as well.

Select the target format (TIFF G4 or PDF) into which the documents will be converted. You must specify the intended module type if you have chosen PDF as the target format of module-spanning W-Documents. If you choose the W-module, a PDF viewer is required at the workstation, e.g. Adobe Reader.

In case the source document is already available in the selected target format, a new file will only be created if you have activated the option **Ignore identical input and output formats**.

This option allows you to convert existing PDF documents into PDF/A documents if the integrated PDF conversion supports this standard.

Enter a timeout in milliseconds in case conversion is fully stretched and jobs cannot be processed instantly. A value of 0 milliseconds will not trigger a stop. If a set timeout is exceeded, the error indicator checkbox is activated.

The target format 'PDF' requires the configuration of PDF conversion (see 'Integrating a PDF Conversion').

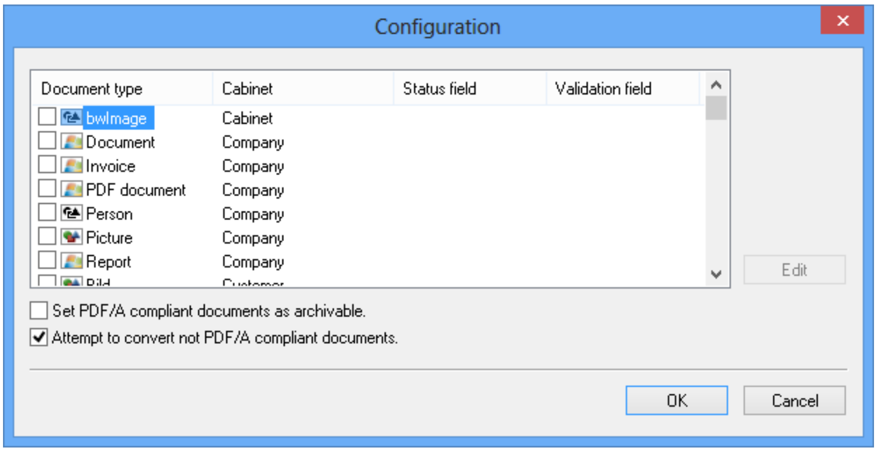
'PDF/A Validation' Action

The action 'PDF/A validation' checks whether PDF documents comply with the PDF/A standard and, if available, converts PDF documents into PDF/A documents.

To use this action, add the `axacpdfa.dll` library (see ''Additions').

When setting up the automatic action (see 'Setting Up Automatic Actions'), specify a configuration name.

Indicate all document types of which you want to convert documents in the configuration dialog.

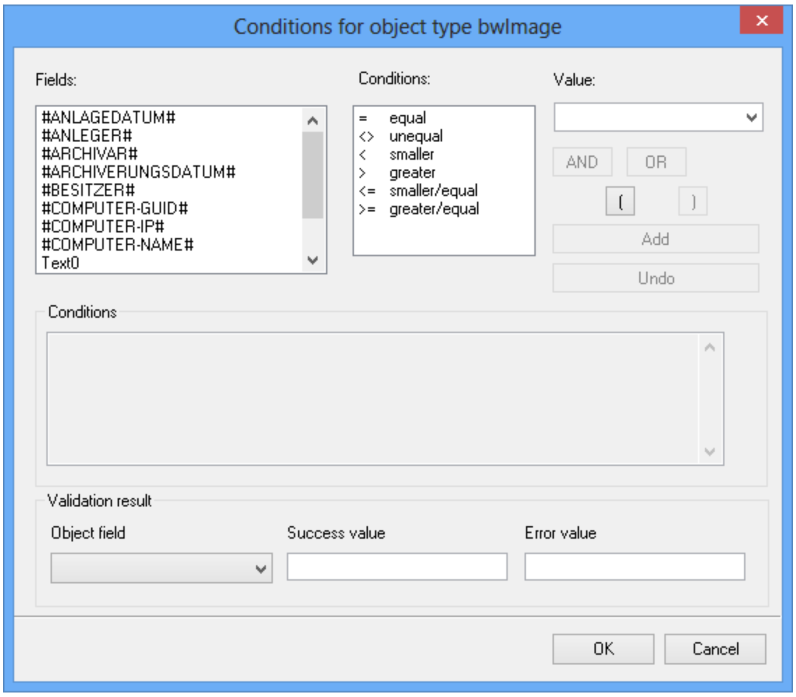


Document type	Cabinet	Status field	Validation field
□ bwImage	Cabinet		
□ Document	Company		
□ Invoice	Company		
□ PDF document	Company		
□ Person	Company		
□ Picture	Company		
□ Report	Company		
□ Bild	Customer		

□ Set PDF/A compliant documents as archivable.

☑ Attempt to convert not PDF/A compliant documents.

Using the **Edit** button you can specify conditions for documents of the selected document type, which have to be fulfilled in order to execute the action:



Fields:

#ANLAGEDATUM#
#ANLEGER#
#ARCHIVAR#
#ARCHIVERUNGSDATUM#
#BESITZER#
#COMPUTER-GUID#
#COMPUTER-IP#
#COMPUTER-NAME#
Text0

Conditions:

=	equal
<>	unequal
<	smaller
>	greater
<=	smaller/equal
>=	greater/equal

The **Fields** area lists the index data fields of the selected object type and basic parameter fields. Select the field for which you want to create a clause.

The **Links** area will list all available operators. Select an operator.

Enter a value for the selected field into the **Value** area. An asterisk ('*') can be used as a placeholder for any string of characters and a question point ('?') can be used as a wildcard for any single character. The field's list permits you to specify a value for a basic parameter.

Then click on the **Add** button.

By combining the field, the operator and the value, you have formed a condition. This condition can furthermore be logically combined with other conditions. The entire condition is shown in the **Conditions** field below. In this field, you cannot edit the entries. If you want to delete or correct entries, press the **Undo** button.

If you want to indicate successful conversion on the data sheet, specify an object field in the **Validation result** area that the **Success value** or, if conversion failed, the **Error value** is saved to.

Confirm the configuration with **OK**.

In addition to the option **Do not attempt to convert PDF/A compliant documents**, you can use this action to change the archivable property of documents of the selected document types. If you activate the option **Set PDF/A compliant documents as archivable**, documents which have been converted by this action, as well as documents which were already available as PDF/A-compliant files will receive the property 'approved for archiving.' All documents which are not PDF/A compliant will be at the same time set to 'not approved for archiving'.

Error Return Values for Actions

If you add the parameter '/X' to the generated start parameters for enaio® start, the value '0' is not returned every time in the event of an error; instead, a value is returned for the action during which the error occurred. This allows the relevant action to be identified in a series of actions.

Action	Internal error value	Hexadecimal error value	Decimal error value	Error level in command.exe
UNKNOWN	1019	0x800703FB	2147943419	-2147023877
AXACARCH	1020	0x800703FC	2147943420	-2147023876
AXACEXP	1021	0x800703FD	2147943421	-2147023875
AXACIMP	1022	0x800703FE	2147943422	-2147023874
AXACSYNC	1023	0x800703FF	2147943423	-2147023873
AXACABO	1024	0x80070400	2147943424	-2147023872
AXACHIST	1025	0x80070401	2147943425	-2147023871
AXACWDVL	1026	0x80070402	2147943426	-2147023870
AXACSCRIPT	1027	0x80070403	2147943427	-2147023869

AXACPAGE	1028	0x80070404	2147943428	-2147023868
AXACPREF	1029	0x80070405	2147943429	-2147023867
AXACREQ	1030	0x80070406	2147943430	-2147023866
AXACUNAC	1033	0x80070407	2147943431	-2147023865
AXACDOK2TIF	1032	0x80070408	2147943432	-2147023864
AXACMTIF	1033	0x80070409	2147943433	-2147023863
AXACLTRASH	1034	0x8007040A	2147943434	-2147023862
AXACHASH	1035	0x8007040B	2147943435	-2147023861
AXACSIGN	1036	0x8007040C	2147943436	-2147023860
AXACPDFA	1037	0x8007040D	2147943437	-2147023859
AXACDEL	1038	0x8007040E	2147943438	-2147023858
AXACCOM	1039	0x8007040F	2147943439	-2147023857
AXACEXEC	1040	0x80070410	2147943440	-2147023856
AXACCOLD	1041	0x80070411	2147943441	-2147023855
AXACUNME	1042	0x80070412	2147943442	-2147023854
AXACTARC	1043	0x80070413	2147943443	-2147023853
AXACADJR	1044	0x80070414	2147943444	-2147023852
AXACCRYPT	1045	0x80070415	2147943445	-2147023851
AXACIDX	1046	0x80070416	2147943446	-2147023850
AXACVCEXP	1047	0x80070417	2147943447	-2147023849
AXACSUMM	1048	0x80070418	2147943448	-2147023848
AXACCVGEN	1049	0x80070419	2147943449	-2147023847
AXACDBST	1050	0x8007041A	2147943450	-2147023846
AXACCL	1051	0x8007041B	2147943451	-2147023845
AXACWFHCLEAR	1052	0x8007041C	2147943452	-2147023844
AXACSYSC	1053	0x8007041D	2147943453	-2147023843
AXAOLFR	1054	0x8007041E	2147943454	-2147023842
AXACHASHD	1055	0x8007041F	2147943455	-2147023841
AXACMTYPE	1056	0x80070420	2147943456	-2147023840
AXACFAX	1058	0x80070421	2147943457	-2147023839
AXACDCM	1059	0x80070422	2147943458	-2147023838
AXACXMLE	1060	0x80070423	2147943459	-2147023837
AXACXMLC	1061	0x80070424	2147943460	-2147023836

Administrative Functions in enaio® administrator

Versions of Configuration Files

enaio® creates backup files of old configurations. You can use these backup copies in case of necessity to restore previous configurations if a manipulated configuration leads to inexplicable errors. You can compare the entries and also re-activate old configurations.

> Activating old configurations can cause inconsistencies and data loss. In case of doubt, please contact our support team.

Backup files are created of the following configuration files:

§ AS.cfg,

Allows you to configure the entire system, the archive system, the W-Module, and the archive print.

§ ASForm.cfg,

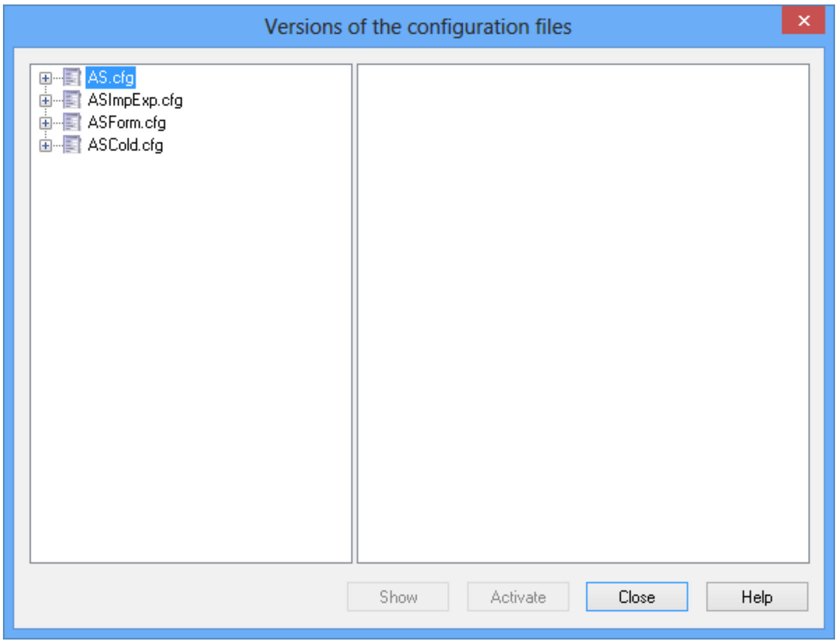
Allows you to configure enaio® capture.

§ ASCold.cfg,

Allows you to configure the automatic actions concerning COLD processes.

The configuration management window is opened by use of the **Versions of configuration files** item in the **Configuration** menu.

In the **Versions of the configuration files** window you will find a search tree which lists the configuration files.



Old configurations are each identified by the date, time and creator information.

Double click a configuration to display its details on the right.

You can activate a selected configuration through its context menu.

The automatic action **Cleanup of configuration and log files** supports you in managing configurations. This action deletes old configuration files. Only the last twenty configuration files of each type are retained.

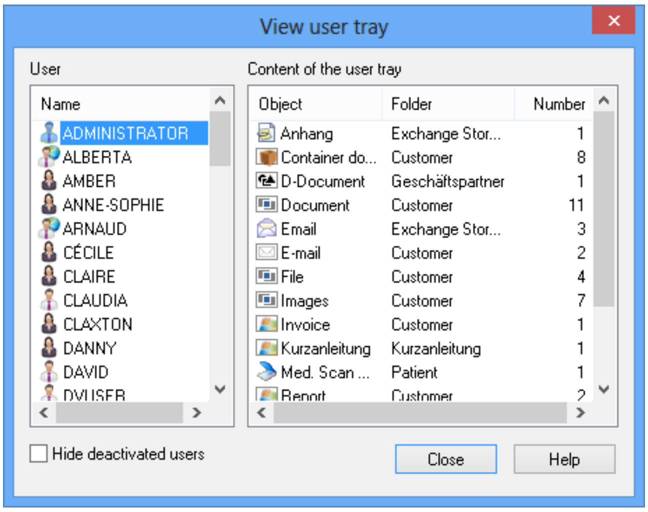
View User Trays

It is possible to view the filing trays of enaio® users. This may be useful if you want to check results after an import into the filing tray, or when the work area is quite full and you want to check how many documents are in the filing tray portfolios.

The **View user tray** dialog is opened with the **View user trays** item in the **Actions** menu.

The system role 'Administrator: View user trays' is required.

You will find a list of users there. Select a user in order to show the document types and the number of documents in the **Content of the user tray** area, which are in the user's filing tray.



Name
ADMINISTRATOR
ALBERTA
AMBER
ANNE-SOPHIE
ARNAUD
CÉCILE
CLAIRE
CLAUDIA
CLAXTON
DANNY
DAVID
DVUSER

Object	Folder	Number
Anhang	Exchange Stor...	1
Container do...	Customer	8
D-Document	Geschäftspartner	1
Document	Customer	11
Email	Exchange Stor...	3
E-mail	Customer	2
File	Customer	4
Images	Customer	7
Invoice	Customer	1
Kurzanleitung	Kurzanleitung	1
Med. Scan ...	Patient	1
Report	Customer	2

☐ Hide deactivated users

Close the window using the **Close** button.

Optimize Index Statistics

Extensive changes within the archive may reduce its working speed for the index tables of the database are no longer optimized.

In this case you can optimize the index statistics. You will find the **Optimize index statistics** function in the **Actions** menu.

You can also use the automatic action 'Database statistics update'.

If the index statistics optimization does not provide any result, it is possible to delete and recreate all index tables using enaio® editor.

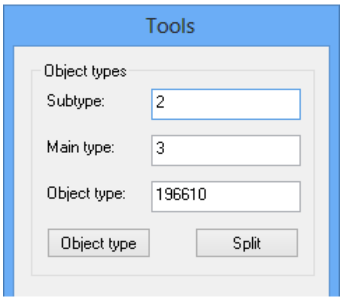
Before optimizing the index statistics, create a backup copy of the database. Index statistics optimization is only feasible if no user is currently accessing the database. enaio® server must be restarted afterwards. All users must restart enaio® client as well.

Tools

You may have to convert data for direct access for the database with your database-specific tools or for SQL queries.

Open the **Tools** dialog with the **Tools** item in the **Extra** menu.

The **Object types** area helps you to determine the object type from the main and subtype or to split the object type into main and subtype.

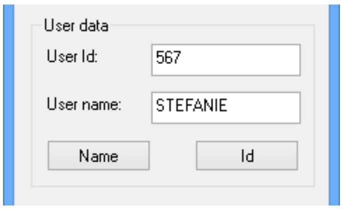


Subtype: 2

Main type: 3

Object type: 196610

The **User data** area allows you to determine the user name from the user ID or the user ID from the user name.

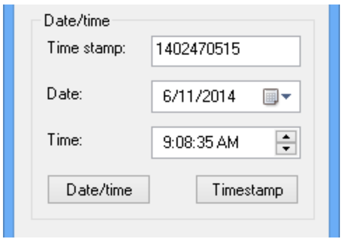


User data

User Id: 567

User name: STEFANIE

The **Date/time** area helps you to determine the date and time from the time stamp or the time stamp from the date and time.



Date/time

Time stamp: 1402470515

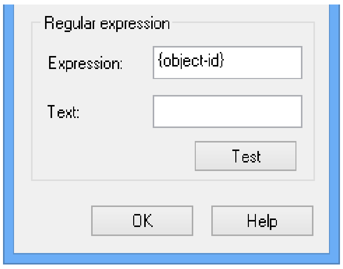
Date: 6/11/2014

Time: 9:08:35 AM

You can use regular expressions to make specifications for entries, e.g. passwords.

Here, you can enter a regular expression and check in the **Text** field whether or not the entry corresponds to the expression.

You will receive a respective notification.



Regular expression

Expression: {object-id}

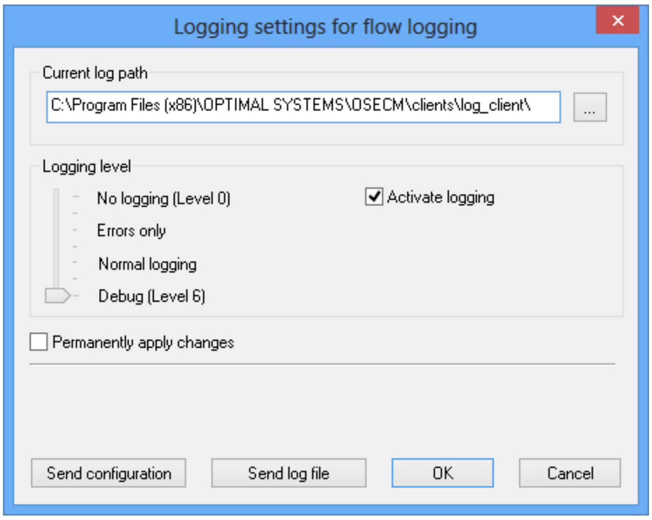
Text:

The enaio® administrator User Interface

The enaio® administrator Menu

Log Configuration

You can change the logging level for the period of a session. In case of error, it enables you to instantly send the relevant information to the administrator.



Logging settings for flow logging

Current log path

C:\Program Files (x86)\OPTIMAL SYSTEMS\OSECM\clients\log_client\

Logging level

- No logging (Level 0)
- Errors only
- Normal logging
- Debug (Level 6)

☑ Activate logging

☐ Permanently apply changes

The **Send configuration** button is used to send the currently set logging configuration by e-mail. In doing so, all log files of the current day and the configuration file will be send as a ZIP file.

Users with the system role 'Administrator: Configure entire system' can permanently adopt the logging level settings.

Exiting

This menu item is used to close enaio® administrator.

Configuration Menu

Entire System

You open the tabs on which you make settings for the entire system (see 'Entire System Settings').

Remote User Administration

You configure areas for the security system.

Security System

You open the **Security system** window. You configure the security system on the tabs (see 'Introduction to the Security System').

Set Up W-Module

In the **Set up W-module** window you can set up Windows applications for W-Documents (see 'Introduction to the W-Module').

Set up Archive Print

In the **Set up archive print** window you can set background images for enaio® printer and specify the archive print format (see 'Introduction to the Archive Print').

Electronic Signature

You set up signature types (see 'Introduction to the Electronic Signature').

Versions of Configuration Files

You open the **Versions of the configuration files** window. You can compare the entries of old configuration versions and also re-activate old configurations (see 'Versions of Configuration Files').

Actions Menu

Optimize Index Statistics

You can optimize the index statistics if extensive changes in the database have reduced the working speed (see 'Optimize Index Statistics').

View User Trays

You can view the filing trays of enaio® users (see 'View User Trays').

Automatic Actions

In the **Automatic actions** window you can set up automatic actions (see 'Introduction to Automatic Actions').

Convert/Reset Clauses

Version 8.50 now includes a new syntax for clauses to access rights. Existing clauses in versions prior to 8.50 can be converted. The conversion creates a log with which you can check the conversion before applying it.

If errors or warnings are shown, you should adjust or delete the corresponding clauses before conversion and recreate them after the conversion.

If you execute the conversion, a copy of the old clauses is automatically saved beforehand. The converted clauses are saved in the database.

If uncertainties occur despite checking, you can reset the clauses. The reset imports the copy of the old clauses.

Extras Menu

Changes to the Security System

You open the log of changes to the security system via the 'Security system' and 'Remote user administration' areas. You need the system role 'Security system configuration.'

This additional logging must be activated in enterprise-manager via **Server properties** > **General** > **Security**.

Delete History Entries

If the additional logging of the changes to the security system is activated, then clean up can be done by date via this log entries dialog.

The user needs supervisor rights for this. The entries of the last two months cannot be cleaned up.

Tools

You open the **Tools** dialog, which you can use for data conversion (see 'Tools').

Show System Role IDs

Activates or deactivates the display of system role IDs.

Help Menu

Help

Open the online help tool.

Info

You open the About window. It offers information on the installed version of enaio® administrator and, by clicking the **About** button, additional information on the configuration of the archive and the computer.

Toolbar

You open the tabs on which you make settings for the entire system (see 'Entire System Settings').

You open the **W-template administration** window. You configure the Windows document types on the tabs (see 'Introduction to the W-Module').

You open the **Security system** window. You configure users, groups, and access rights on the tabs (see 'Introduction to the Security System').

You open the remote user administration. Here you can configure areas for the security system (see 'Global and Local Administration').

You open the **Automatic actions** window. Here you set up the automatic actions (see 'Introduction to Automatic Actions').

You open the **Electronic signature configuration** window (see 'Introduction to the Electronic Signature').

You open the **About** window.

The enaio® enterprise-manager

Introduction to enaio® enterprise-manager

The main purpose of enaio® administrator is to manage the security system and the W-Module. Its configuration data are used for the entire server family.

enaio® enterprise-managerallows you to manage license keys, individual servers, and the archiving media for the respective server groups.

On top of that, enaio® enterprise-manager offers significant technical insight into system processes and can therefore be useful for system optimization and problem analysis.

enaio® enterprise-manager is a snap-in (32 bit) for the Microsoft Management Console.

To run enaio® enterprise-manager in the Microsoft Management Console on 64 bit operating systems, the command line parameter `-32` must be passed: `mmc -32`

> Users need the system role 'Administration of the Application Server.'

enaio® enterprise-manager and enaio® server-Monitor

enaio® server-monitor, like enaio® enterprise-manager, shows all data relevant for system configuration and all data related to the current system status.

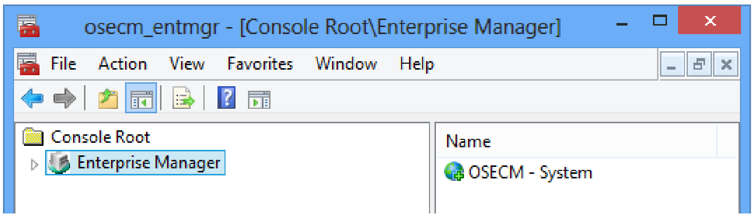
System data can be entirely exported with enaio® server-monitor. Export data may be helpful, in particular for system support as they allow the analysis and optimization of systems.

enaio® server-monitor, `axsvcmtr.exe`, is found in the installation directory `\server`. After start, the program reads all data concerning the system configuration and the current system state. These data can be exported into a file by using the menu or the toolbar.

> In contrast to enaio® enterprise-manager, enaio® server-monitor does not connect to enaio® server. Thus, an overview of the current system state is possible, even if enaio® server is not reacting.

Starting and Connecting

enaio® enterprise-manager can be started either by using the respective shortcut in the enaio® application group or the enaio® service manager or by opening the console file `osecm_entmgr.msc` located in the directory `\clients\admin`.

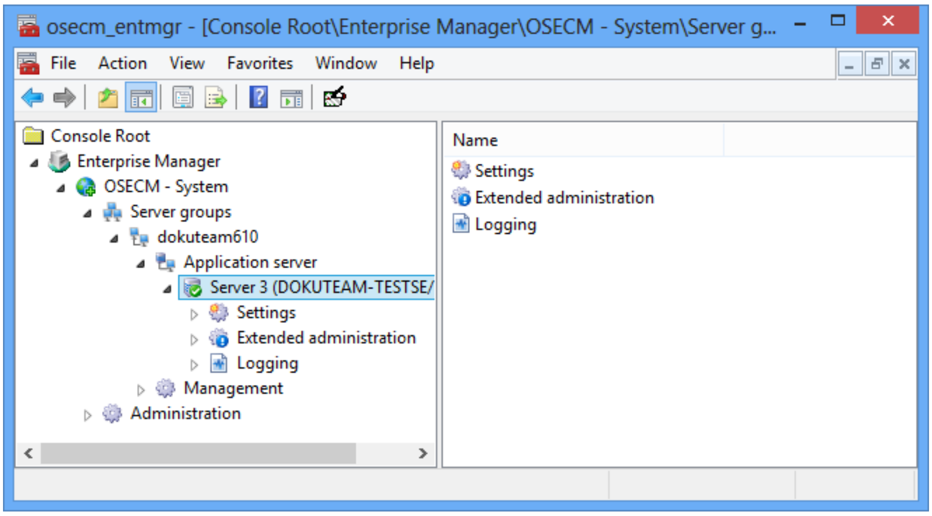


The context menu for the **Enterprise-Manager** > **New** item in the console tree allows you to add a server family. Enter the IP address and the port of a server in the server family. To connect to the server, you must log on to it.

This server acts as the family control server for enaio® enterprise-manager. All data of the server family is queried and modified by this server. Within the group, this server automatically becomes the group control server over which data for the media administration are queried and modified.

> If the server is not running, you must start and connect to it from within enaio® enterprise-manager.

In the console tree, enaio® enterprise-manager shows all set up server groups and assigned servers.



Each server family is composed of at least one server group with at least one assigned server. An administration area is assigned to each server group. It allows you to configure how the server group carries out archiving processes.

The server family itself is also assigned to an administration area which is used to manage license keys. If the 'Auto Login' mode is active, you will be logged in automatically.

You can integrate other server families.

When closing the Microsoft Management Console or enaio® enterprise-manager, you will be asked to save the console settings.

If you save the console settings, enaio® enterprise-manager will automatically connect to the family control server at the next start and display the current server groups and servers in the console tree.

Language Settings

The default language of enaio® enterprise-manager is German, but it allows being set to English:

- Open the `oxentmgr.cfg` file in the `clients\admin`folder.
- The following entries are required for 'English':

  ```
  [LOCALIZATION]
  LOCALE=1033
  LANGSTR="eng"
  ```

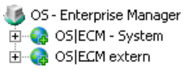
  The second entry specifies that the files `oxentmgr_pages-eng.xml` and `oxentmgr_sp-eng.xml` are loaded instead of the files `oxentmgr_pages-deu.xml` and `oxentmgr_sp-deu.xml`. The files contain configuration data.

Without these entries, German is set by default.

Overview of the Console Tree

enaio® enterprise-manager displays the server groups, servers, administration areas, and the setting area of each added server family in the console tree.

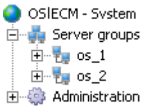
The following entries are found in the console tree:



All server families are listed under this entry.

You can add additional server families using this entry’s context menu. Although you have added multiple server families, they can be removed individually.

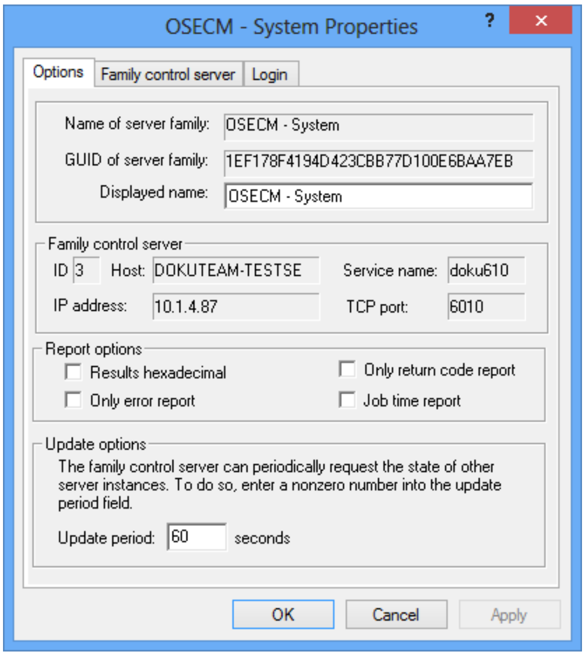
If a connection to a server family is not possible, the server family is marked.



The entry **Server groups** and **Administration** is assigned to each server family.

The server family's context menu permits you to rename the server family and to update its data.

Use the **Properties** entry to open the property dialog of a server family:



OSECM - System Properties

Name of server family: OSECM - System

GUID of server family: 1EF178F4194D423CBB77D100E6BAA7EB

Displayed name: OSECM - System

Family control server

ID 3 Host: DOKUTEAM-TESTSE Service name: doku610

IP address: 10.1.4.87 TCP port: 6010

Report options

□ Results hexadecimal □ Only return code report

□ Only error report □ Job time report

Update options

The family control server can periodically request the state of other server instances. To do so, enter a nonzero number into the update period field.

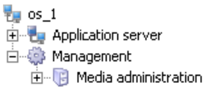
Update period: 60 seconds

The family control server is specified on the **Options** tab. You can specify **Reporting options**. enaio® enterprise-manager logs the server connections separately. The log can be viewed by clicking on the **Show report** button on the toolbar.

Insert an update period into the **Update options** area of the dialog after which the family control server queries the state of the other servers. The state icons of the servers are marked according to these query responses.

The family control server is also specified on the **Family control server** tab. You can decide whether to automatically establish a connection when starting enaio® enterprise-manager or to activate a respective notice in case an alternative connection address is used (see below).

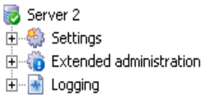
On the **Login** tab, the current user can choose to save his user name and password through the console settings. At the next start, enaio® enterprise-manager will use these user account data.



Each server group is provided with the entries **Application server** and **Administration**, which list all servers of the group and which offer entries for the media management. The **Media management** is used to configure how the server group performs archiving (see 'Media Management in enaio® enterprise-manager').

Due to the fact that media data are queried and modified over a group control server, one group control server is required within a server group. The family control server is by default defined as the group control server for its group. When further server groups are added, one server of each group must be designated as the group control server if, in that group, media data need to be configured.

This property is set by using the **All tasks > Set group control server** item from the context menu of a server.

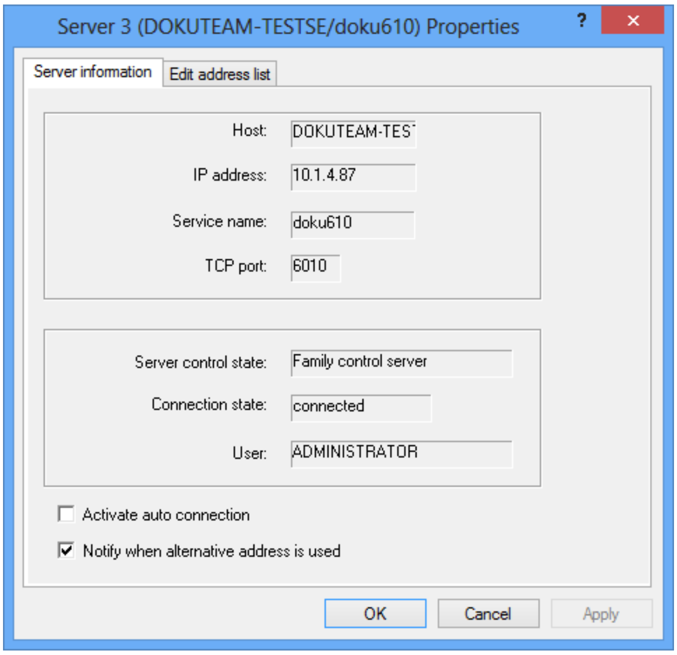


Server 2
Settings
Extended administration
Logging

Each server is provided with a settings area, an administration area and a logging area.

The state icon of each server indicates with a green tick that the connection to the server is established. If the state icon of a server shows a red cross, the connection to the server failed.

The context menu of each server enables you to connect to or disconnect the server as well as to open the properties dialog:



Server 3 (DOKUTEAM-TESTSE/doku610) Properties

Server information | Edit address list

Host: DOKUTEAM-TES
IP address: 10.1.4.87
Service name: doku610
TCP port: 6010

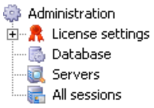
Server control state: Family control server
Connection state: connected
User: ADMINISTRATOR

☐ Activate auto connection
☑ Notify when alternative address is used

The **Server information** register shows a server's address and connection status. You can decide whether to automatically establish a connection when starting enaio® enterprise-manager or to activate a respective notice in case an alternative connection address is used.

Alternative connection addresses for enaio® enterprise-manager are added on the **Edit address list** tab.

Servers can be connected internally with their own addresses and can use other addresses for external communication. The family control server, which determines the addresses of other servers from the database, will in this case only show the internal connection. enaio® enterprise-manager can use the external connection.

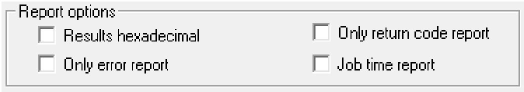


The license keys in particular are managed via the administration area of a server family (see 'Introduction to the License System').

It is also possible to access the database and server and session summaries.

Reports

enaio® enterprise-manager logs its connections to servers separately. Using the property dialog of a server family, you can define **Report options**.


Report options

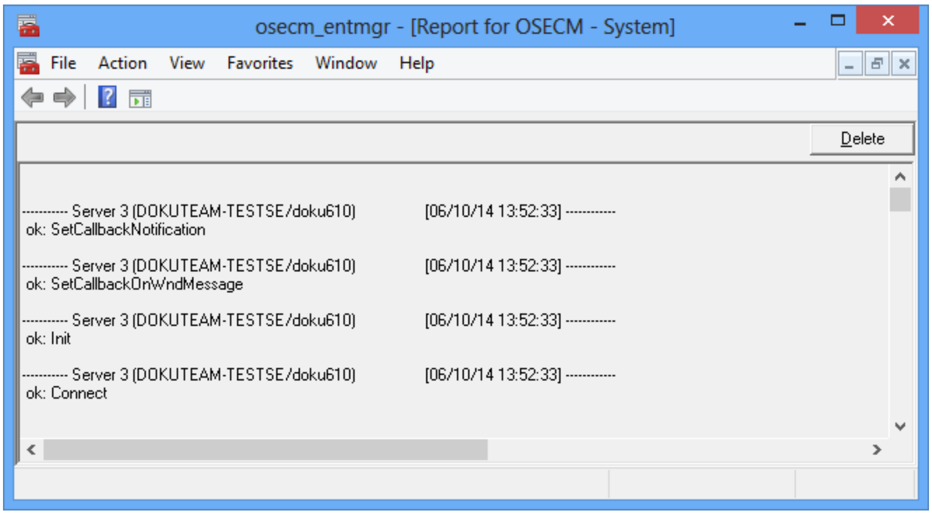
□ Results hexadecimal

□ Only error report

□ Only return code report

□ Job time report

This log can be viewed by clicking on the **Show report** button on the toolbar.



```
---------- Server 3 (DOKUTEAM-TESTSE/doku610)          [06/10/14 13:52:33] ----------
ok: SetCallbackNotification

---------- Server 3 (DOKUTEAM-TESTSE/doku610)          [06/10/14 13:52:33] ----------
ok: SetCallbackOnWndMessage

---------- Server 3 (DOKUTEAM-TESTSE/doku610)          [06/10/14 13:52:33] ----------
ok: Init

---------- Server 3 (DOKUTEAM-TESTSE/doku610)          [06/10/14 13:52:33] ----------
ok: Connect
```

The report display is updated automatically.

Like all enaio® components, enaio® enterprise-manager furthermore logs its activities according to the settings in the configuration file `oxrpt.cfg` which is located in the application directory `clients\admin`.

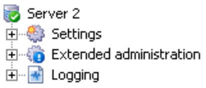
Server Configuration

Server families operate independently of each other. By exporting index data from the database or a server family and importing this data into the database of another server family, read access to documents of the first server family from the second can be made possible. This also requires the setup of a virtual archive (see 'Connections Between Server Families').

Within a server family, the servers in each server group can be configured differently if they are designated to perform different tasks. However, all servers access the common database and thus the same licenses, object definitions and user administration settings.

All servers of a server group perform the same tasks and must therefore be configured identically.

The server connection must be established in order to configure the server. Use the server's context menu to connect to it.



Servers are configured by using the areas **Settings**, **Extended administration**, and **Logging**.

Language Settings

The language defined through the operating system specifies which language is used by the server to communicate with a client.

In addition, the language can also be specified through registry entries. The following entries are required to set the language irrespective of the operating system settings:

`Key:`	`HKEY_LOCAL_MACHINE\SOFTWARE\Optimal Systems\<service name>`
`String:`	`Locale`
`Value for English:`	`1033`
`Value for German:`	`1033`

Server settings

The **Settings** area of a server offers the following configuration areas:

§ Server information

This page lists basic server data. The data cannot be modified.

§ Registry entries

All registry entries which are used by enaio® server are listed here. They can be customized in the respective area of the server properties.

§ Server properties

These pages can be used to modify the server properties. Each parameter is displayed together with a description and their available values if they are allowed to be modified.

§ Periodic jobs

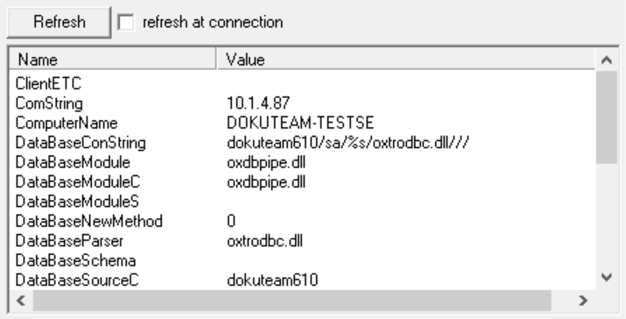
Periodic jobs run by the servers are set up here.

Each of the aforementioned pages must be refreshed individually after opening. You can alternatively activate the option **Update when connecting**.

Server Information

The **Server information** page summarizes basic server data.

The data cannot be modified.



Name	Value
ClientETC	
ComString	10.1.4.87
ComputerName	DOKUTEAM-TESTSE
DataBaseConString	dokuteam610/sa/%s/oxtrodbc.dll///
DataBaseModule	oxdbpipe.dll
DataBaseModuleC	oxdbpipe.dll
DataBaseModuleS	
DataBaseNewMethod	0
DataBaseParser	oxtrodbc.dll
DataBaseSchema	
DataBaseSourceC	dokuteam610

Database parameters can be modified via **Server properties > Category: Data**, other data can also be modified via server properties.

Registry entries

All registry entries which are used by enaio® server are listed here. The entries for the following key are shown:

```
HKEY_LOCAL_MACHINE\SOFTWARE\OPTIMAL SYSTEMS\<server name>\Schemata
```

> The registry may contain entries that are not shown here. Those entries may come from optional components or earlier versions of the system. You must not modify or delete them.

Each server checks the registry entries at start. If required entries are missing, they are created with default values.

The keys, strings and values are flagged with icons. For example, the icons indicate whether entries are required or optional. Use the **Key** button to open a window for an explanation of the icons.

It is recommended to not change values in the registry editor but in other areas, such as the **Server properties** area. These areas provide you with additional information on functions and available values. Changes will become effective in an instant for the corresponding engines are reloaded automatically.

If you have modified registry entries directly in the registry editor, you would have to manually restart the respective engines.

Server Properties

The **Server Properties** area is the main area for server configuration. It is divided into the following categories:

- General
- Data
- Engines
- Integrity
- Periodic Jobs
- Queues
- Services
- Full text

When opening, you have to refresh the display of each area. Or you can activate the **Refresh at connection** option.

Category: General

For the sake of clarity, data in the **General** category are divided into further areas. The following settings are available in this category:

General Parameters

Parameters	Default (registry entry)	Description
ComString	(ComString)	The IP address or host name of the computer on which the server is running or, if a cluster solution is used, the cluster IP address. This address is entered at installation and inserted into the registry. This entry must only be changed for cluster solutions. If used, enter the cluster IP address over which clients can reach the clustered server.
TCP port	(TCPPort)	The TCP port of the server instance. The port is entered at installation and inserted into the registry. If you change the port number, you must adjust this entry accordingly.
Crash timeout	300 seconds (CrashTimeout=300)	Defines after how many seconds a server blackout is suspected due to a missing alive signal. This entry is only taken into account when multiple servers are used. The alive signal is sent by the periodic job 'BeatPing/Serverping'. The timeout value must be greater than the period of the periodic job. Effected sessions will be taken over if the timeout expires and a server failure is suspected.

Max. count of TCP sockets	1500 (MaxConnections=1500)	The maximum number of TCP sockets that the server will open for TCP connect requests. If the computer's memory utilization is too high, you can reduce it by lowering this value. However, at least four TCP sockets are required for each client.
Timeout for the start of a job thread	10000 milliseconds (Threads\JobStartTimeout=10000)	The time provided for a job thread to start. After this timeout, it is attempted to start a new job thread. Increase the timeout value just temporarily in order that you can determine whether job threads, which could not start due to timeout, may be started then.
Wait before launching	0 seconds (WaitSec=0)	Number of seconds the server waits before it launches. A waiting period may be necessary in case the server has to wait for a database or full text server.
Free disk space	50 MB (Archive\MinDiskSpace=50)	The minimum free disk space in the WORK area, in the server installation directory and in the configured server log directory. If this minimum space is not available in one of these areas, the server will not start. It is recommended to increase this value. Large documents or extensive logging may occupy this space immediately. In operation, periodic jobs determine the remaining free disk space. When the value drops below the configurable amount of space, the administrator will be notified by e-mail. By default, these periodic jobs are activated and use the minimum disk space entered here as default value.
E-mail when	Not active	Defines whether or not to send

not found on main medium	(Archive\MailForMirrorDocument=0)	an e-mail to the administrator if a document was only found on the mirrored medium but not on the main medium. Such errors must always be investigated. The administrator's e-mail data must be available (see below).
Job execution without login	Allowed (LoginForJobs=1)	Defines whether or not to perform server jobs of clients which have not yet logged on.
Always close sessions	Close sessions (KillSessionOnDisconnect=1)	Turns on or off the reservation of sessions. Sessions should not be reserved.
Reservation time	0 seconds (SessionPreserve=0)	Defines how long a canceled session will remain reserved for later recovery (in seconds). Sessions should not be reserved. The reservation time is only relevant when sessions are reserved.
Computer name	- (ComputerName)	If specified, this name is used to identify the application server in the 'server' table. This entry must remain empty.
Memory size for compression and extraction	50 MB (Archive\MaxCabMemory=50)	Maximum size (in MB) of the file which is compressed/extracted in the memory; otherwise, the hard disk is used.
Path to access log	- (AccessProtocol)	The path to the access log. Without any entry the access log will not be created (see 'Introduction to Logging').
Use hard links	use (Switches\DoCopy=0)	Defines whether to copy document files or create hard links, especially in the work/cache area. If hard links cannot be created, the files will be copied. The server checks at start whether it is possible to create hard links. If not, an error message will be written to the start log.

		The creation of hard links can be generally deactivated through the following registry key: `Archive\DoNotUseHardLinks` Set the value to '1' in order to not check and to not create hard links.
Administrative e-mails	Allow e-mails (NoMails=0)	Disables or enables the sending of administrative e-mails for the transmission of system events. The log files 'startup.txt' and 'shutdown.txt' are enclosed to the e-mail.
E-mail address of the administrator	- (AdminMail)	E-mail address of an administrative recipient for the transmission of system events (server start/end) by the server. Use the semicolon to separate multiple e-mail addresses.
E-mail server	- (MailServer)	The IP address or host name of the e-mail server for administrative e-mails.
E-mail sender	- (MailSender)	The sender’s name or address to be given to the server when sending e-mails to an administrator. 'askrn' is used by default if this entry is left empty.
SMTP body	Yes (SMTPBody=1)	Defines whether or not to set the flag "BODY=8BITMIME" when sending e-mails. Some e-mail servers, for example the Exchange server 5.5 and earlier versions, cannot deal with this encoding and will report a syntax error. If so, set the value to 'No'.
SMTP NTLM domain	- (SMTPNtlmDomain)	Defines the NTLM domain for the authentication with NTLM.
SMTP authentication	None (SMTPAuthenticating=0)	Authentication method for SMTP
SMTP user name	- (SMTPUserName)	User name for SMTP login.

SMTP password	- (SMTPPassword)	Password for SMTP login. The password should be encrypted by calling the application `url-cipher-tool.jar` (cf. 'URL Encryption').
NetSend address	- (AdminNet)	The name of the computer to which administrative messages are sent with NetSend. If this entry is empty, NetSend messages will not be sent.
NetSend sender	- (AdminName)	The name of the sender for NetSend messages. A sender is optional.
Monitoring license utilization	90 (LicenseThreshold=90)	Enter a value defining the license utilization in percent – if this value is exceeded, an e-mail is sent to the administrator. Enter the value '0' to not monitor the license utilization. You can find details about monitoring in the section 'Determining Licenses.'
Email to license utilization	Send (LicenseThresholdMail=1)	Defines whether or not to send an e-mail to the administrator if the value defining the license utilization is exceeded. An exceeding of the utilization value will be written to the flow log if the log level is set to 3.
Maximum file size in GB	(MaxFileSize=1)	Maximum size for files. Files can be no more than 2 GB in size, and videos no more than 4 GB. For image modules, documents can consist of multiple files, and the total of all image files must not exceed 4 GB.

Login

To be able to log in, every user must enter his user name and password into the enaio® user administration system.

If you have chosen NTLM authentication and set up NTLM authentication in the operating system, users that have been handed over to the enaio® user administration system as NT users can log in with their Windows user name and password. The users and servers must always belong to the same domain. If NTLM authentication fails, standard authentication is automatically executed provided that respective data is available.

> If the activated NTLM authentication fails when enaio® enterprise-manager is started, no further authentication will be carried out.

Standard authentication is available and lets users log in with the enaio® user names and passwords. If the Windows user names correspond to the enaio® user names, you can active automatic login to the operating system.

If an LDAP server provides the user names (see 'LDAP Configuration), activate auto login and set the login mode to 'LDAP' in order to enable automatic login with the login data for the operating system. Users that have been signed out from the LDAP server will not be able to log in anymore, even if they are still registered as enaio® users. In LDAP mode, the login dialog asks for the LDAP user name and the enaio® password.

> Anonymous access to the LDAP directory service usually is not allowed; as a result, authentication at the LDAP system is required for identification of LDAP users and their rights. You must have an LDAP user with the appropriate rights. Name and password are entered on the 'LDAP Configuration in enaio® administrator.

You can also specify a login sequence for standard authentication.

Parameters	Default (registry entry)	Description
Auto login	Not active (Login\AutoLogin=0)	Allows auto login to enaio® in standard authentication mode, using the operating system's login data.
NTLM login	Not active (Login\NTLMLogin=0)	Allows NTLM authentication via Windows user name and password. The standard authentication is either carried out using the enaio® user name and passwords, or through LDAP or Active Directory (see below).
Login mode	Dialog (Login\LoginMode=0)	Defines whether in standard authentication mode the user is logged on via enaio® user administration, LDAP or Active Directory (Dialog/LDAP/Active

		Directory). If a login order has been defined, this value will be ignored.
Login order	- (Login\LoginPipe)	If multiple logon types are possible, list them here in the intended order. Use the following abbreviation: L=LDAP; A = Active Directory; I=User administration with password; U=User administration without password. Example: "LI," initial login is carried out with LDAP; if it fails, the user administration with password is used on the next attempt.
Check case-sensitivity of passwords	Do not check case-sensitivity (Login\PwdCaseSensitive=1)	Specifies whether or not to check the case sensitivity of passwords in standard authentication mode. In NTLM authentication mode, the operating system setting takes precedence.
Computer identification	Name (Station\Ident=name)	The modules can be assigned to the computers through names or the GUID. When installing terminal servers, the GUID must be used for identification because names may differ. This setting requires that the GUID has been used for licensing and that every computer that logs on has exactly one network card and can be identified.
Computer name adjust	Do not adjust (Station\ChangeName=0)	If computer identification is performed with the GUID, a changed computer name can be automatically

		updated for its display in the license management. This update is not obligatory.
Security level	No restriction (Login\SecurityLevel=0)	You can specify whether or not to close the application and to additionally lock the user account after three failed login attempts.
Domain	- (ValidDomains)	Specifies to which additional domains the user must belong in order to automatically log on to the server (auto login). Enter multiple servers separated by semicolon. Any user that belongs to the same domain as the server can always log in automatically.
Active Directory Domain	- (Login\LoginDomain)	Specifies which domain of the server will be used to authenticate the user in Active Directory authentication mode.
LDAP binding	- (Login\LDAP\Binding)	Enter the binding string that describes the particular position within the structure of the LDAP directory service, which forms the starting point for search requests. When specifying more than one LDAP server above, you can also enter multiple binding strings separated by semicolon.
LDAP host	- (Login\LDAP\Host)	Indicate the LDAP server and, separated by a colon, its port number. Enter multiple LDAP servers separated by semicolon. Data of the LDAP server that is reached at first will

		be used for the user administration.
LDAP user attribute	- (Login\LDAP\UserAttrib)	Enter the LDAP attribute that is used as unique user indication.
Regular expression for password syntax	- (Login\PwdComplexity)	Enter a regular expression in order to specify the password syntax which must be followed when distributing and changing passwords. If a password does not follow this syntax, it will not be accepted.
Description text for the password syntax	- (Login\PwdComplexityDescription)	A description of the syntax requirements which is displayed in the dialogs when distributing or changing passwords. Example: "Das Passwort muss mindestens 8 Zeichen lang sein.\r\n Your password must be at least 8 characters long.\r\n Votre mot de passe doit comporter au moins 8 caractères."
Validity period of passwords	0 (Login\PasswordExpirationInterval)	Enter a period in days for which a password is valid. The value '0' turns this function off.
Notification when the period of validity expires	5 (Login\PasswordExpirationWarning)	Enter a value in days after which the user is notified about password expiration.
Version check at server connection	Minor (Login\CheckVersion)	A version check can be carried out each time a client connects to enaio® server. If the versions do not match, enaio® server will forbid the connection. Major, minor release or service pack version can be validated. By default, the

		minor release version is checked. In order to make sure that no errors occur due to version differences, you can enable a validation of the service pack version.
User name for LoginPipe exceptions	- (Login\AlternativeUserNames)	Specify the users to be logged in using the alternative LoginPipe. Use the semicolon to separate multiple user names. The '*' entry allows all users to be logged in using the alternative LoginPipe. As well as specifying users, you must also specify the IP address of the computer on which the enaio® service is running using the 'IP addresses for LoginPipe exceptions' parameter. Furthermore, the system role 'Server: Switch job context' must be assigned to the users, otherwise the program cancels the operation with an error.
IP addresses for LoginPipe exceptions	- (Login\AlternativeIPAddresses)	Specify the IP addresses to be used for the alternative LoginPipe. Use the semicolon to separate multiple IP addresses. It is recommended to indicate only IP addresses of workstations on which enaio® services are executed. In addition to the IP address, you must use the parameter 'User names for LoginPipe exceptions' to specify also the user name under which the enaio® service is running.
Alternative LoginPipe	-	As with 'Login order' described above, you specify

	(Login\AlternativeLoginPipe)	an order for the login pipe exception. Only one entry is possible here as well. Use the following abbreviation: L=LDAP; A = Active Directory; I=User administration with password; U=User administration without password.

DMS Options

Parameters	Default (registry entry)	Description
Limit of query results	0 (DMSOptions\ RequestRowsetLimit=0)	Defines the maximum of data sets which may be returned by a server query. An error message is output if more data sets are determined. Enter the value '0' to specify 'no limit'. You must only limit the engine in agreement with the consulting team. Limitation may also restrict the execution of automatic actions, for example, the action 'Hash check'.
Use station name for checkout	No (DMSOptions\ CheckOutByComputerName=0)	Defines whether or not to identify the station based on its name for checkout. This may be required if stations cannot be clearly identified with the IP or the GUID which will thus lead to check-in errors.
Local date format	No (DMSOptions\ UseUserLocaleDate=0)	Follows the date and time format according to the settings of the local user at the workstation.
Local number format	No (DMSOptions\ UseUserLocaleNumber=0)	Follows the number format according to the settings of the local user at the workstation.

Security

Parameters	Default (registry entry)	Description
Encrypted Data section	Encryption not active (Archive\CryptoStorage=0)	Controls whether or not to encrypt the entire data area (work, cache, archive) with AES 256 (see 'Encryption of Document Files in enaio®')
Disable user rights at job calls	Only administrators (Security\ JobExecutionAccessLevel=1)	Defines which users are allowed to set the flag 'Do not check user rights' when executing jobs. 'Administrators' are users with system roles. Jobs can be carried out by use of scripts, deactivating the check of user rights for the sake of performance. Unfortunately, this creates a security hole. For that reason, it is recommended to only grant this function to administrators. To completely close this security hole, set the value to 'Nobody'.
Hashed communication	No (Security\ OnlyHashedJobs=0)	Controls whether enaio® server accepts only jobs with a hash value. The configuration file `oxmljsc.cfg` allows you to change the respective setting for clients. As default, jobs are transferred with hash values. The file is found in the respective application directories. Further information can be found in the system handbook DMS.
Compressed communication	No (Security\ OnlyZippedJobs=0)	Controls whether enaio® server only accepts jobs with compressed data. For clients located in the application directory, the following entries via the `oxmljsc.cfg` file are used to switch compression on: `packed=1`

		`packbound=0` The file is found in the respective application directories. You can switch on compressed communication for clients via the relevant `oxmljsc.cfg` file without switching on the exclusive compressed communication for the server. Further information can be found in the system handbook DMS.
Windows Version check	No (Security\ CheckWindowsVersion=0)	Specifies whether or not clients can only log in under Windows XP or greater Windows versions.
Signature check of modules when Loading	- (Security\ CheckSignatureModules)	Creates a list of modules which are checked for valid signatures as soon as they are started or loaded. The modules in the list are separated by semicolons. Example: `ax.exe;axbasics.dll;axavapps.dll`
Password encryption handling	Internal and AES algorithm (Security\ PwdDecryption=3)	Since version 6.0, enaio® is using the Advanced Encryption Standard (AES). Keep the default values if you have integrated an external application that does not yet encrypt according to this standard. If this is not the case, it is recommended for security reasons to select the value 'AES algorithm only' in order that enaio® server accepts only those passwords that are encrypted according to this standard.
Sharing active	Yes (Security\ EnableDocumentSharing=1)	Activate/deactivate sharing functions
Maximum sharing time	60 (Security\ DocumentSharingMaxDuration=60)	Maximum number of days during which documents are shared for joint processing.
Log changes to the	No (Security\	Additional logging of changes to the security system via the

security system	SecuritySystemHistory=0)	'Security system' and 'Remote user administration' areas.

workflow

Parameters	Default (registry entry)	Description
E-mail notification for work items	No (Workflow\ EmailOnWorkItem=0)	Specifies whether an additional e-mail will be sent when an activity is placed in a user’s inbox.
Support of deadlines	Yes (Workflow\SupportTimers=1)	Specifies whether dunning/retention periods will be processed by the workflow engine.
Processing sequence	2 Workflow\WorkerJobStrategy	Defines the order in which workflow steps are processed by the server: 1 = age of the steps, oldest first; 2 = age of the processes, oldest first; 3 = up-to-dateness of the steps, youngest first.

Conversion

Parameters	Default (registry entry)	Description
FOP path	- (Conversion\FOPPath)	Path to the batch file for the FOP (Formatting Object Processor). During server installation, the files are copied into the `\etc\fop` directory and the path is entered. The installation of JAVA is required, and the environment variable JAVA_HOME must be added to the Java installation path.
FOP timeout	30000 ms (Conversion\ FOPTimeout=30000)	Defines after how many milliseconds the FOP conversion process will be canceled. The conversion may require more time than specified here.
OpenOffice application	- (Conversion\SOfficePath)	This property may only be configured when authorized by the consulting team. Path to the OpenOffice

		application `soffice.exe` which is used for PDF conversion. This PDF conversion is currently only used for sending W-Documents in PDF format from the client to external recipients. If OpenOffice cannot convert the file format, users get an error message. OpenOffice is not installed automatically.
OpenOffice Timeout	10000 ms (Conversion\SofficeTimeout=10000)	This property may only be configured when authorized by the consulting team. Defines after how many milliseconds the PDF conversion process with OpenOffice will be canceled. The conversion may require more time than specified here.
Disable internal image conversion	No (Conversion\DisableInternalImageConversion)	Specifies whether images (e.g. to PDF) are converted internally or externally or by an external program. Note that OS_renditions can only convert single-sided PDF documents.
Fit quicklooks	No (Conversion\FitSlides)	Specifies whether the height and width of quicklooks or only their height will be adjusted to fit in the quicklook view. When selecting the second option, the quicklook may be truncated.
Use SLIDE cache	Yes (Archive\UseSlideCache)	Specifies whether renditions are saved in the SLIDE cache of the application server. Independent of this setting, renditions will always be saved in the rendition cache. Yes – Generated renditions will be saved in the SLIDE cache and read from there. No – Generated renditions will not be saved in the SLIDE cache. If a rendition is requested, it will

		be read from the rendition cache or generated, if not yet existing.
Call renditions using object ID	Yes (Archive\GetRenditionByID)	Yes – Existing renditions are called directly from the rendition cache using the object ID without transferring documents from enaio® server to enaio® renditionplus first. By using this option, network traffic is reduced. No – When requesting a rendition, the document is transferred from enaio® server to enaio® renditionplus. enaio® renditionplus reads the rendition from the cache. If the rendition cannot be found in the rendition cache, it will be generated by enaio® renditionplus as usual.

OCR

The settings are documented in the section 'OCR Using AXFROCR.'

Parameters	Default (registry entry)	Description
OCR program	NO_OCR (Archive\OcrExe)	Specify the path and name of an OCR program to have a full text index created of image documents. NO_OCR – No OCR from image documents. However, a full text index is added to text documents. axfrocr.exe – OCR with FineReader axrenocr.exe – OCR with enaio® renditionplus (FineReader)
Monitoring file	- (Archive\OcrAliveFile)	Only axfrocr.exe: Path and name of the file for checking whether the OCR program is still running.
Start OCR application	No (Archive\WatchOcr=0)	Only axfrocr.exe: Checks whether an OCR program is running and starts it if required.
OCR decryption	- (Archive\OcrDecryptPath)	Only axfrocr.exe: Directory into which files for OCR are

directory		stored in an unencrypted form.
OCR job directory	- (Archive\OcrJobPath)	Only axfrocr.exe: Directory into which OCR jobs will be filed. After changing the indicated directory the parameter in the file axfrocr.ini must also be changed (see 'The Configuration File').
Zonal OCR	OCR executor (Archive\Zonal=0)	Execute zonal OCR from within enaio® client through the OCR executor or the application.
Recognition speed	Standard recognition (Archive\OcrFastMode=0)	Faster recognition can negatively impact quality.

Subscription/Follow-up

Parameters	Default (registry entry)	Description
Send e-mail messages	Yes (Subscription\SendMails=1)	Defines whether e-mails will be sent when notifying a subscription/follow-up.
Send e-mails individually	Send e-mails individually (Subscription\SendSingleMail=1)	Defines whether e-mails will be sent individually or as collective e-mail when notifying a subscription/follow-up.
Attach index data	No (Subscription\ SendMailWithIndexData=0)	Defines whether index data will also be sent when notifying a subscription/follow-up. For data protection reasons, it can be necessary to send index data.

E-mail (inbox in enaio® client)

Parameters	Default (registry entry)	Description
E-mail integration	MAPI (Mail\Type=instell)	Specifies whether the inbox is integrated in the client via MAPI or IMAP. The respective client licenses must be available.
IMAP e-mail server	- (Mail\IMAPServer)	Specifies the full, qualified domain name of the IMAP e-mail server.
Port of the IMAP e-mail server	143 (Mail\IMAPPort)	Specifies the port of the IMAP e-mail server.
Name of the	-	Specifies the display name of the

IMAP e-mail server	(Mail\IMAPServerName)	IMAP e-mail server.
Proxy of the IMAP e-mail server	- (Mail\IMAPProxy)	Specifies the computer name of a firewall through which the IMAP server is to be accessed.
Proxy type of the IMAP e-mail server	No firewall (Mail\IMAPProxyType=0)	Specifies the type of the firewall.
Proxy login of the IMAP e-mail server	- (Mail\IMAPProxyUser)	Specifies the user name for authentication at the firewall.
Proxy password of the IMAP e-mail server	- (Mail\IMAPProxyPwd)	Specifies the password for authentication at the firewall.
Configure IMAP e-mail server	0 (Mail\ChangeIMAPServer)	Specifies whether the user can set the IMAP server by himself.
Setting e-mail display	Text-Area (Mail\IMAPShowHTMLMail)	The integrated e-mail application can display the text or html area of an e-mail message.

Client options

Parameters	Default (registry entry)	Description
PDF resolution	200 DPI (ClientOptions\PdfResolution)	Defines the resolution in PDF documents which are displayed in the internal viewer of enaio® client. The resolution value, which was selected when creating annotations on PDF documents, takes precedence over the value defined here.

Category: Data

Data in the **Data** category are divided into further areas. The following settings are available in this category:

Archiving

Archiving and archiving settings are described in detail above (see 'Archiving options').

Parameters	Default (registry entry)	Description
Server type	Main server (Archive\ServerType=0)	Main servers can archive documents of other servers; sub-

		servers can only archive their own documents.
Activate confirmed archiving	Not active (Archive\ConfirmedArch=0)	Controls confirmed archiving.
Free storage space	50 MB (Archive\FreeMediaSpace=50)	Indicates the storage space which will be kept free on archiving media.
Cluster size on the jukebox	1024 KB (Archive\JBClusterSize=1024)	Defines the default cluster size of the media in the jukebox for determining free space. This information is used if no information is made for the individual media.
Create backups	Not active (Archive\MakeBackups=0)	Specifies whether a backup of the media is stored in the backup directory during archiving.
Pegasus method for determining free media space	NTFS method (GetDiskFreeSpaceEx) (Archive\PegasusFreeSizeMethod=0)	Specifies the method which is used to determine the free space on the archiving media.
Pegasus method for determining the free space for the next document to be archived.	Initial calculation of total free space (Archive\PegasusFreeSpaceOnly=0)	The remaining free space for archiving on Pegasus media can be calculated based on the initially free space or determined anew each time.
Automatic prearchiving	Not active (Archive\AutoPreArch=0)	Defines whether documents of other server groups are handed over before archiving.
Sending e-mails during archiving	No e-mails (Archive\ArchAdminMail=0)	Specifies at which archiving events an e-mail is sent to the administrator.

Maximum number of archiving errors	1 (Archive\MaxErrorsCount=1)	Defines after how many errors archiving will be canceled. Insert '0' to not cancel the archiving process. Note that updating the enaio® server will reset this value to '1'.
Extended archiving logging	1 (Archive\ExtendedReport=1)	Specifies whether extended archive logging is activated. Thus, a detailed XML log file will be created.
Path and file name for extended archiving logging	archive%5%7%6%8%9%10.xml (Archive\ReportName)	Specifies the path and the file name of the log file for extended archive logging. The file will be written to the `\server\log` directory.
Delete archived documents	Do not delete (Archive\DeleteArchived=0)	Specifies whether files on media will be deleted if archived documents are deleted.
Hash value check during archiving/dearchiving	yes (Archive\ReadAfterWrite=1)	Defines whether to check hash values during archiving/dearchiving processes. This ensures correct handover but is detrimental to performance. This check is independent of the functions for document integrity.
Archive object definition	yes (Archive\ArchiveObjDef=1)	Specifies whether to additionally archive the corresponding

		object definition during each archiving process. If this option is deactivated, you have to ensure the equality of index data and the corresponding data model according to your procedural documentation.
Retention periods	Unix time range (Archive\RetentionBehavior2038=1)	Specifies the valid range for retention periods. 32 bit systems may require you to limit the valid retention date period. To do so, select the unix time range (1'). As a result it will be impossible to specify retention dates beyond Jan 19, 2038. If retention periods can be specified without constraint, select the continuous time range (2'). For example, for GRAU DATA. If you use NetApp archives, select the extended NetApp time range (3'). As a result, the valid time range for retention dates extends to Jan 19, 2071.

To guarantee simple configuration and secure operation, enaio® provides tools and means for different certified archive storage systems. Nevertheless, keep in mind to follow the configuration steps described in the respective interface manuals.

It is therefore recommended to coordinate, realize, document, and test the planning of retention periods, the selection of an archive storage system and its configuration, the configuration of retention periods as well as necessary archive storage system settings in enaio®, and the correct configuration and execution of archiving processes with our consulting department.

Database Parameters

Parameters	Default (registry entry)	Description
Data source	askrn (DataBase\Source=askrn))	Indicates the ODBC data source name for access to the database server. This entry is specified during installation, written to the registry and must not be modified.
Parser for database queries	ODBC parser (DataBase\Parser=oxtrodbc.dll)	The parser is predefined.
Database access	ODBC access (DataBase\Module=oxdbodbc.dll)	Defines whether the database is accessed using ODBC or DB piping. The type of access is given during installation. If you modify this entry, you must also change the following one.
Database access (extra)	ODBC access (DataBase\ModuleClient=oxdbodbc.dll)	Defines whether the database is accessed using ODBC or DB piping. The type of access is given during installation. If you modify this entry, you must also modify the previous one.
Database scheme	- (DataBase\Schema)	Specifies the name of the database scheme. The scheme will be used to determine table names, table indexes and column names. This entry is left blank if no custom scheme is explicitly specified for the database.
Maximum DB field length	2000 (DataBase\DBMaxChar=2000)	Indicates the maximum string length of a character field in the database. This value depends on the

		database in use and must be appropriately adjusted. This value can also be set using enaio® editor.
Pool size for job threads	5 (DataBase\PoolJobThreads=5)	Indicates the number of DB connections allowed in the pool of job threads. You can enter a value between '1' and '64'. It is recommended to not modify the value.
Pool size for read threads	5 (DataBase\PoolReadThreads=5)	Indicates the number of DB connections allowed in the pool of read threads. You can enter a value between '1' and '64'. The capacity can be viewed in the area **Extended administration** > **Database pool** > **Read threads**.
Replace CR character with CRLF	Replace (DataBase\ReplaceCR=1)	Defines whether CR characters in the database are replaced with CRLF characters for display reasons when reading strings.
Maximum hits	50000 (DBPipe\MaxHits=50000)	Maximum hit number of SQL Select statements. This setting also affects the automatic actions 'Sign' and 'Full text indexing' and limits the number of documents processed there.

ADO database access

Access to the database in the case of SQL queries (see 'SQL') is via ADO.

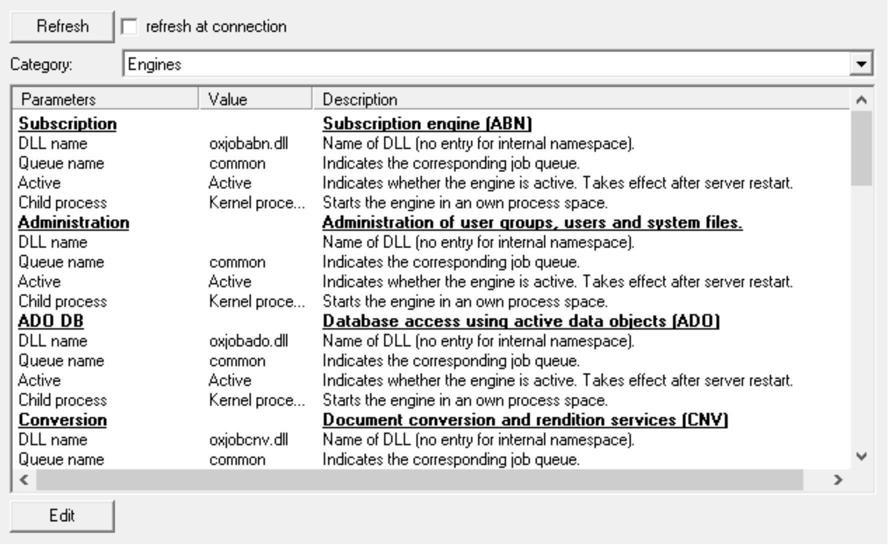
Parameters	Default (registry entry)	Description
Execution of SQL commands (write access)	Allow execution (ADO\ExecuteCommands=1)	Specifies whether to allow write access to the database when using the ADO database access with SQL queries. Set the value to 'Do not allow execution' in order to close this potential security hole.
Name of the	MSDASQL (ODBC)	Indicates the name of the OLE

OLE DB provider	(ADO\Provider=MSDASQL)	DB database provider.
Cursor type	Forward only (ADO\CursorTypeSelect=0)	Cursor type when opening an ADO query. Default up to 7.50: 'Dynamic.' This cursor type is not changed by updates. We recommend the cursor type 'ForwardOnly.' If necessary, check whether a change is possible.

> Please contact Consulting if you encounter problems with SQL queries.

Category: Engines

All engines are listed here. The engines for workflow are activated by the enaio® setup. If needed, the OCR and MED engines must be activated manually.



Category: Engines

Parameters	Value	Description
Subscription		**Subscription engine (ABN)**
DLL name	oxjobabn.dll	Name of DLL (no entry for internal namespace).
Queue name	common	Indicates the corresponding job queue.
Active	Active	Indicates whether the engine is active. Takes effect after server restart.
Child process	Kernel proce...	Starts the engine in an own process space.
Administration		**Administration of user groups, users and system files.**
DLL name		Name of DLL (no entry for internal namespace).
Queue name	common	Indicates the corresponding job queue.
Active	Active	Indicates whether the engine is active. Takes effect after server restart.
Child process	Kernel proce...	Starts the engine in an own process space.
ADO DB		**Database access using active data objects (ADO)**
DLL name	oxjobado.dll	Name of DLL (no entry for internal namespace).
Queue name	common	Indicates the corresponding job queue.
Active	Active	Indicates whether the engine is active. Takes effect after server restart.
Child process	Kernel proce...	Starts the engine in an own process space.
Conversion		**Document conversion and rendition services (CNV)**
DLL name	oxjobcnv.dll	Name of DLL (no entry for internal namespace).
Queue name	common	Indicates the corresponding job queue.

Engines that are not needed can be disabled. An active engine that is not needed only places extra load on the system when executing periodic jobs.

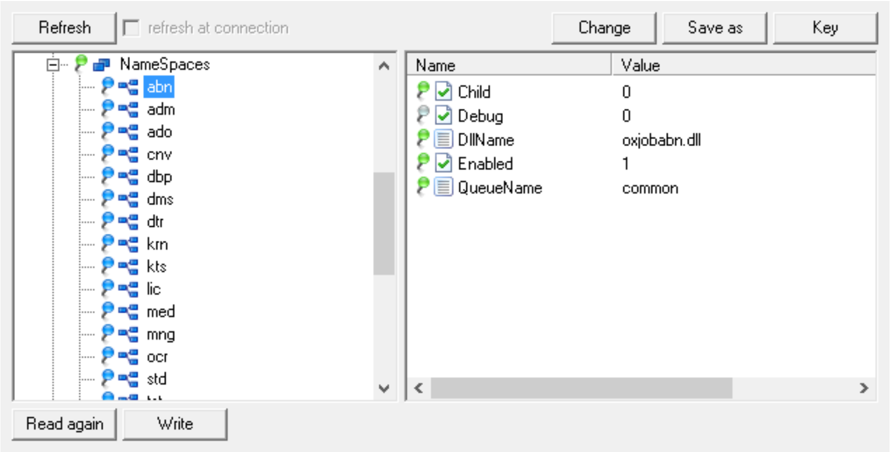
Periodic jobs, which are also activated by enaio®-setup, are assigned to the workflow engine.

Changes only take effect after server restart. It is possible to load or unload engines during runtime from the **Extended administration** > **Set up** > **Engines** area.

A queue name is specified for each engine. It is possible to set up new job queues for engines or to raise the number of threads. The job queues' capacity can be viewed in the area **Extended administration** > **Monitoring** > **Job queues** and the category **Queues** lists the parameters related to the queues for editing.

Engines are run in the kernel process space. They can be started in an individual process space for error analysis purposes. It is recommended to perform changes only after prior consultation with the support team.

This data is administered in the registry of the server. Under the registry key **NameSpaces**, a key with the required strings and values is created for each engine.



Name	Value
Child	0
Debug	0
DllName	oxjobabn.dll
Enabled	1
QueueName	common

Category: Integrity

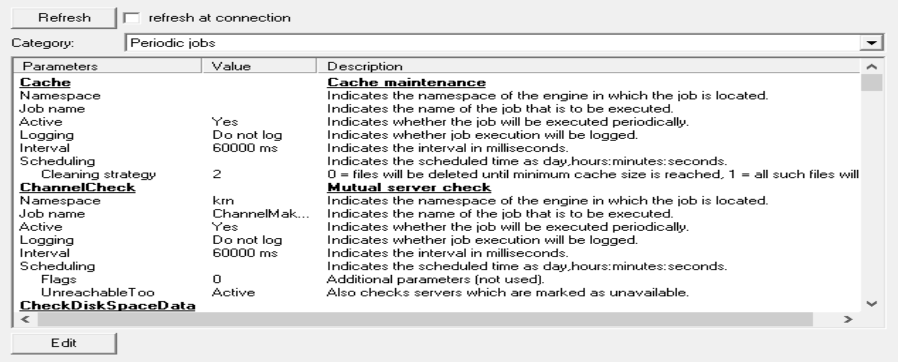
Settings available in the **Integrity** category allow you to activate mechanisms which support you in finding errors on storage media and detecting direct accesses to document files (see 'Validating Document Integrity').

Parameters	Default (registry entry)	Description
Hash value check before archiving	Do not check (integrity\HashNeeded=0)	The hash value can be checked prior to the archiving process.
Signature check before archiving	Do not check (integrity\SignatureNeeded=0)	Additionally, the signature of the hash value can be checked prior to the archiving process.
Hash-value check created before document call up	Do not check (integrity\CheckDocHashOnRequest=0)	The hash value can be checked whenever a document is requested. If the check is activated the hash value will also be checked after dearchiving.
Signature check before document request	Do not check (integrity\CheckDocSigOnRequest=0)	Additionally, the signature of the hash value can be checked whenever a document is requested.
Automatic signature creation	Do not create (integrity\Sign=0)	Every hash value which is generated at creation or modification of a document file is

		signed.
Signature errors treated as fatal	Do not cancel (integrity\ErrorAsFailure=0)	Errors which occur while creating or checking a signature will only cancel an action if you enter the value 'Cancel'.
Signature module	- (integrity\DllName=oxsignos.dll)	Only the module 'oxsignos.dll' can be used for signing. Do not change this value.
Signature module parameter	- (integrity\Parameters=algo=1)	Do not change this value.
Signature code	- (integrity\Code)	Subsequent signing of document files requires a signature code.
Period of validity of the signature code	- (integrity\CodeExpires)	The period of validity of the signature code for subsequent signing must be entered here.

Category: Periodic Jobs

Registry entries control the setup of jobs, which are periodically executed by the server, during installation.



Category: Periodic jobs

Parameters	Value	Description
Cache		**Cache maintenance**
Namespace		Indicates the namespace of the engine in which the job is located.
Job name		Indicates the name of the job that is to be executed.
Active	Yes	Indicates whether the job will be executed periodically.
Logging	Do not log	Indicates whether job execution will be logged.
Interval	60000 ms	Indicates the interval in milliseconds.
Scheduling		Indicates the scheduled time as day,hours:minutes:seconds.
Cleaning strategy	2	0 = files will be deleted until minimum cache size is reached, 1 = all such files will
ChannelCheck		**Mutual server check**
Namespace	krn	Indicates the namespace of the engine in which the job is located.
Job name	ChannelMak...	Indicates the name of the job that is to be executed.
Active	Yes	Indicates whether the job will be executed periodically.
Logging	Do not log	Indicates whether job execution will be logged.
Interval	60000 ms	Indicates the interval in milliseconds.
Scheduling		Indicates the scheduled time as day,hours:minutes:seconds.
Flags	0	Additional parameters (not used).
UnreachableToo	Active	Also checks servers which are marked as unavailable.
CheckDiskSpaceData		

This configuration area enables you to view all periodic jobs, allowing you to enable or disable them and to change their parameters.

Create new periodic jobs using the **Settings > Periodic jobs** area (see 'Periodic Jobs').

In most cases, these settings can be left as they are.

The following periodic jobs are set up:

- Server ping

  The server periodically writes a date to the database that other servers use to check whether or not the server is active. If not, the periodic job 'Server monitoring' enables other servers to release sessions of inactive servers.

  The period of job repetition is specified in milliseconds, default: 60000 ms.

- Server monitoring

  By use of the database entry, the server checks whether other servers are still active and, if necessary, releases sessions of inactive servers.

  The period of job repetition is specified in milliseconds, default: 60000 ms. The period must not be less than that of the server ping (see 'above').

- ChannelCheck

  The server periodically sends the information on whether other servers can be connected to through TCP. All those servers which are not available are marked and will not receive further jobs. Specify with the parameter 'UnreachableToo' whether or not to keep on trying to connect to these servers.

- ClientPing

  The server sends a ping to the clients.

  This general job can be extensively configured. You can specify which computers and applications a ping is sent to.

  It is recommended to set up a periodic job that consistently sends a ping to all computers.

  The following parameters can be specified:

Computer	The name of the computer where the message will be sent. If the entry is left empty, a ping will be sent to all computers.
GUIDs	This parameter is used internally and must be left empty.
Info	This parameter is used internally and must be left empty.
Instance	Indicates the enaio® application to which a ping is sent. Example: `ax` If the entry is left empty, a ping will be sent to all instances.
Message	`ping` – a ping is sent. Additional message types are available but not suited as periodic jobs.
Text	Leave this entry blank.
User	Leave this entry blank.

  The parameters **Computer**, **Instance**, and **User** are combined with logical AND. Only one value can be entered for each. No entry means 'Send to all.'

  The **Extended administration > Monitoring > Connections > Active clients** area permits you to directly send messages to clients and close clients.

- SessionCheck

The server checks periodically or at a defined interval whether the tables for resource and session allocation contain entries which do not correspond to the sessions connected to the server anymore, and deletes all sessions which are inactive over an indicated period of time.

§ Cache

The server periodically clears the cache area.

Cache maintenance can also be set up as an automatic action (see ''Cache Maintenance' Action'). Job parameters are also discussed in this chapter.

§ Follow-up

The server periodically checks whether users have received follow ups and informs the clients.

In multi-server systems, a server can only inform the clients that are connected to the server.

§ Subscription

The server periodically checks whether users have subscribed to an object and informs the clients.

In multi-server systems, a server can only inform the clients that are connected to the server.

§ SessionDropNotActive

The server periodically checks whether there are sessions which are inactive for 72 hours. If so, those sessions will be deleted. The activity duration for sessions can be adjusted but must not be shorter than 8 hours, otherwise errors will occur.

§ Workflow check

The server periodically checks whether workflow processes are due to be modified because of dunning or retention periods. Activities affected by retention periods are activated after expiration, and those with expired deadlines are marked as late and have their defined action executed.

The period of job repetition is specified in milliseconds, default: 60000 ms. This period can generally be raised significantly.

If you neither use dunning nor retention periods, you can deactivate this job.

§ Workflow worker

The server executes workflow processes. Activities are started or ended by this job.

The period of job repetition is specified in milliseconds, default: 3000 ms. This period can be raised for a small number of processes.

§ Workflow notification

The server periodically checks whether workflow processes exist and informs all connected clients about changes in the inbox.

The period of job repetition is specified in milliseconds, default: 5000 ms. This period can generally be raised. It must not be decreased.

- WorkflowSpoolerJob

  The server periodically checks whether report tasks exist. The period of job repetition is specified in milliseconds, default: 6000 ms.

  If you do not use reports, you can deactivate this job.

- CheckExpires

  The server periodically checks when license keys expire and informs the administrator by e-mail.

  The default execution time of this job is scheduled every 4 hours. The **Days** parameter specifies the number of days prior to license key expiration that the e-mail is to be sent. By default, the e-mail will be sent 14 days before the license expires.

- CheckDiskSpaceData

  The server periodically checks the capacity of the drive containing the work directory.

  The period of job repetition is specified in milliseconds, default: 360000 ms. The parameter **Disk** indicates the logical drive; **InformAdmin – Yes** defines that if the remaining capacity drops below the value of the **MinSpace**, the administrator will be informed by e-mail.

  The preset value of '0' for **MinSpace** means that this value is equal to the setting for **Free hard disk space** in **Server properties > Category: General**.

- CheckDiskSpaceLog

  The server periodically checks the capacity of the drive containing the directory into which the server saves its logs.

  The period of job repetition is specified in milliseconds, default: 360000 ms. The parameter **Disk** indicates the logical drive; **InformAdmin – Yes** defines that if the remaining capacity drops below the value of the **MinSpace**, the administrator will be informed by e-mail (see 'above').

- CheckDiskSpaceRoot

  The server periodically checks the capacity of the drive containing the server directory.

  The period of job repetition is specified in milliseconds, default: 360000 ms. The parameter **Disk** indicates the logical drive; **InformAdmin – Yes** defines that if the remaining capacity drops below the value of the **MinSpace**, the administrator will be informed by e-mail (see 'above').

- GetProcessInfo

  System load is determined and logged periodically. A separate channel is required for logging (see 'Logging the System Load').

- ProcessSlideCPMessages

  The server checks regularly whether messages concerning the creation of renditions are available.

The period of job repetition is specified in milliseconds, default: 60000 ms. The parameter **QueueNames** indicates one or more names of the queues whose messages are processed by the job.

Furthermore, you can specify the following optional parameters in the area **Settings > Periodic jobs > Edit**:

ConcurrentJobCount `0` – no restriction. Even if the parameter is not specified, the number of parallel jobs is not limited.

`> 0` – number of jobs that can be executed in parallel. All further jobs are terminated immediately.

§ ProcessFulltextIdxCPMessages

> This job is automatically created by the server if MSSQL is specified as a full-text engine. The job must be disabled if there is a switch from MSSQL to Lucene.

The server checks regularly whether messages concerning the full text indexing of index data are available.

The period of job repetition is specified in milliseconds, default: 60000 ms. The parameter **QueueNames** indicates one or more names of the queues whose messages are processed by the job.

Furthermore, you can specify the following optional parameters in the area **Settings > Periodic jobs > Edit**:

ConcurrentJobCount `0` – no restriction. Even if the parameter is not specified, the number of parallel jobs is not limited.

`> 0` – number of jobs that can be executed in parallel. All further jobs are terminated immediately.

§ ProcessFulltextDocCPMessages

> This job is automatically created by the server if MSSQL is specified as a full-text engine. The job must be disabled if there is a switch from MSSQL to Lucene.

The server checks regularly whether messages concerning the full text indexing of documents are available.

The period of job repetition is specified in milliseconds, default: 60000 ms. The parameter **QueueNames** indicates one or more names of the queues whose messages are processed by the job.

Furthermore, you can specify the following optional parameters in the area **Settings > Periodic jobs > Edit**:

ConcurrentJobCount `0` – no restriction. Even if the parameter is not specified, the number of parallel jobs is not limited.

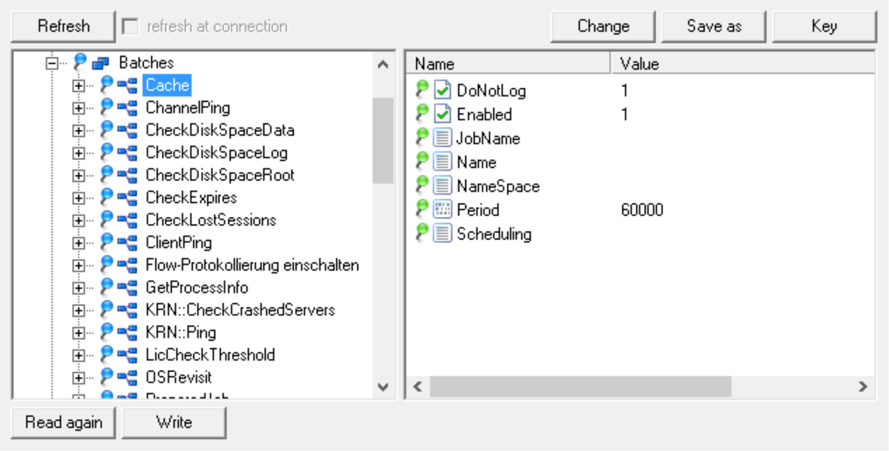
`> 0` – number of jobs that can be executed in parallel. All further jobs are terminated immediately.

The namespace of a job defined by the setup is used to automatically determine in which queue it is executed. Use the optional parameter `$$$QueueName$$$` that can be indicated for all jobs in the area **Settings** > **Periodic jobs** > **Edit** to specify a queue in which the job is executed. You can only specify queues that were created by the setup.

> Periodic jobs are only executed when the related engine is active. Changes take immediate effect; restarting the engine is not required.

By double-clicking an entry you can open its settings dialog. The parameters **JobName** and **Namespace** must not be edited.

This data is administered in the registry of the server. Under the **Batches** key, the keys for every periodic job are listed together with the required strings and values.

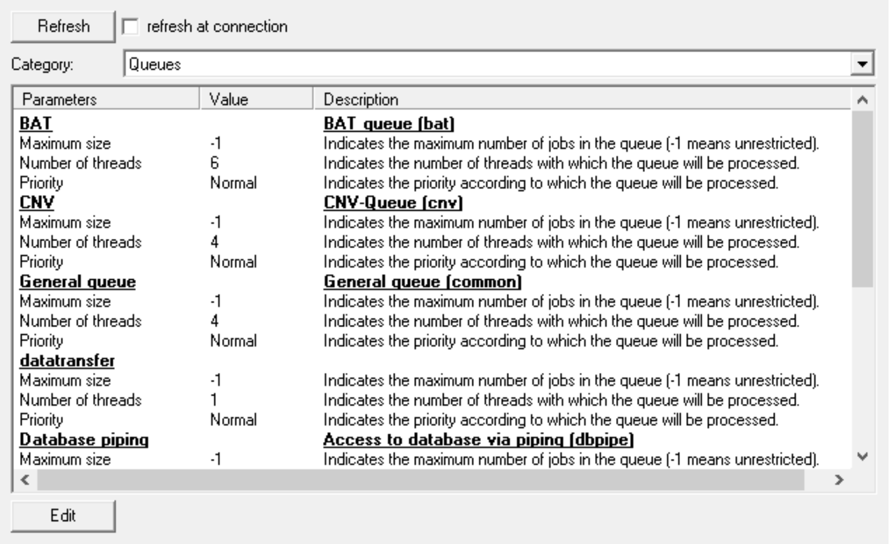


- Batches
  - Cache
  - ChannelPing
  - CheckDiskSpaceData
  - CheckDiskSpaceLog
  - CheckDiskSpaceRoot
  - CheckExpires
  - CheckLostSessions
  - ClientPing
  - Flow-Protokollierung einschalten
  - GetProcessInfo
  - KRN::CheckCrashedServers
  - KRN::Ping
  - LicCheckThreshold
  - OSRevisit

Name	Value
DoNotLog	1
Enabled	1
JobName	
Name	
NameSpace	
Period	60000
Scheduling	

Category: Queues

All queues are listed in this area.



Category: Queues

Parameters	Value	Description
BAT		**BAT queue [bat]**
Maximum size	-1	Indicates the maximum number of jobs in the queue (-1 means unrestricted).
Number of threads	6	Indicates the number of threads with which the queue will be processed.
Priority	Normal	Indicates the priority according to which the queue will be processed.
CNV		**CNV-Queue [cnv]**
Maximum size	-1	Indicates the maximum number of jobs in the queue (-1 means unrestricted).
Number of threads	4	Indicates the number of threads with which the queue will be processed.
Priority	Normal	Indicates the priority according to which the queue will be processed.
General queue		**General queue [common]**
Maximum size	-1	Indicates the maximum number of jobs in the queue (-1 means unrestricted).
Number of threads	4	Indicates the number of threads with which the queue will be processed.
Priority	Normal	Indicates the priority according to which the queue will be processed.
datatransfer		
Maximum size	-1	Indicates the maximum number of jobs in the queue (-1 means unrestricted).
Number of threads	1	Indicates the number of threads with which the queue will be processed.
Priority	Normal	Indicates the priority according to which the queue will be processed.
Database piping		**Access to database via piping [dbpipe]**
Maximum size	-1	Indicates the maximum number of jobs in the queue (-1 means unrestricted).

You can individually configure the maximum number of jobs in a queue, the number of threads and the priority for each queue.

The maximum number of jobs is by default set to '-1' (unrestricted). The priority of all queues is set to 'normal', and the number of threads varies.

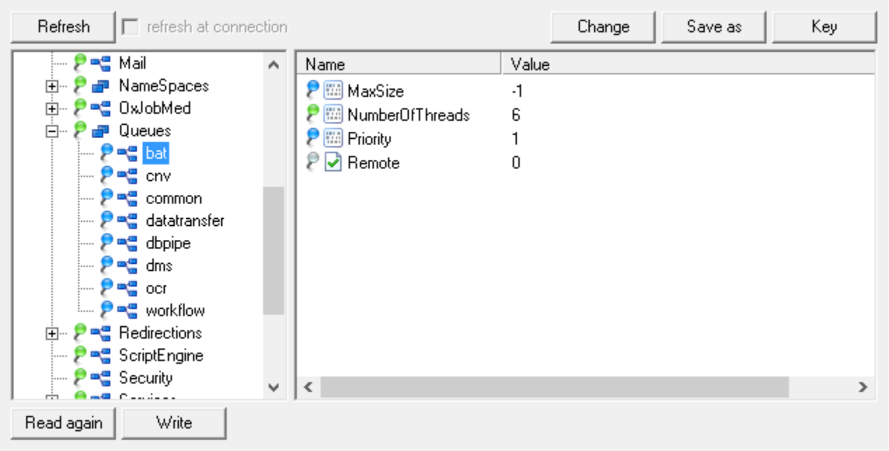
In most cases these settings can be left as they are. In the **Extended Administration > Monitoring > Queues** area you can see the capacity of the queues. For heavily loaded queues you can either increase the number of threads or create new queues for engines.

The BAT queue is the default queue for CPB batch processing. Processes running in the background or processes with long run times could slow down standard operations of the enaio® platform. It is recommended to outsource these processes to the BAT queue which is equipped with 6 threads by default in order to improve load balancing.

The priority according to which the operating system processes the threads of the OCR queue can be decreased in order to prevent the system performance to be reduced due to time-consuming OCR processes.

Given that you are using numerous and complex workflow processes and your computer is equipped with powerful hardware, you can increase the number of threads of the workflow queue to 6 or 8.

This data is administered in the registry of the server. Under the **Queues** key, a key and the required strings and values will be created for each queue.



Name	Value
MaxSize	-1
NumberOfThreads	6
Priority	1
Remote	0

Category: Services

Data in the **Services** category are divided into further areas.

The content processing bus and rendition cache, the core services enaio® contentviewer, enaio® documentviewer, enaio® appconnector (enaio® detailsviewer) and enaio® webservice as well as enaio® exchange and up to ten additional Web services, the latter appear as dashlets, are configured here.

The core services – enaio® contentviewer, enaio® documentviewer and enaio® detailsviewer – are used to display documents as well as document and index data and they can be integrated with enaio® client and enaio® web-client.

The service endpoints entered here are transferred automatically to the client registry at installation of enaio® client and can be read from other components. Changes to the service endpoints, however, are not automatically transferred to the client registry. To synchronize the client registry and the values of the server registry, perform an update of the client installation via the enaio® setup, or synchronize both registries with the tool `OS.UpdateLocalServiceRegistry.vbs` from the directory …`\clients\client32\samples`.

Content Processing Bus

Parameters	Default (Registry path/entry)	Description
Use content processing bus	Yes (CPB\RenditionExport)	Defines whether the content processing bus is used.
Rendition export queues	RENDITION (CPB\ RenditionExportQueueNames)	Specify the names for the rendition export queues. Use the semicolon to separate multiple names.
Index data export queues	FULLTEXTIDX (CPB\ FulltextIdxExportQueueNames)	Specify the names for the index data export queues. Use the semicolon to separate multiple names.
Document export queues	FULLTEXTDOC (CPB\ FulltextDocExportQueueNames)	Specify the names for the document export queues. Use the semicolon to separate multiple names.
Thumbnail export queues	SLIDE (CPB\ SlideExport QueueNames)	Specify the names for the thumbnail export queues. Use the semicolon to separate multiple names.
Queues for page count export	PAGECOUNT (CPB\ PageCountExportQueueNames)	Queue names for page count export. Use the semicolon to separate multiple names.

Rendition Cache

Parameters	Default (Registry path/entry)	Description
Service endpoint	- (Services\RenditionCache\API)	URL under which the service is accessible.
Service endpoint for direct access	- (Services\RenditionCache\ API_DIRECT)	The URL specifies the server that the rendition cache is running on. The setup automatically registers the URL on the enaio® server. The URL consists of the following elements: `http://<server> /osrenditioncache`

Contentviewer

Parameters	Default (Registry path/entry)	Description
Home URL	- (Conversion\ ContentViewerHome)	URL for parameterized service access Schema: `http://<server>/<service>/viewer/` Once the address is indicated, a link to the preview is embedded in each e-mail message when sending documents to internal recipients and the preview is activated in enaio® web-client.
Service endpoint for direct access	- (Conversion\API_DIRECT)	The URL specifies the server that the service is running on. The setup automatically registers the URL on the enaio® server.

Documentviewer

Parameters	Default (Registry path/entry)	Description
Home URL	- (Services\ DocumentViewer\URL)	URL for parameterized service access
Service endpoint	- (Services\DocumentViewer\API)	URL under which the service is accessible.
Service endpoint for direct access	- (Services\DocumentViewer\ API_DIRECT)	The URL specifies the server that the service is running on. The setup automatically registers the URL on the enaio® server. The URL consists of the following elements: `http://<server>/osdocumentviewer`
Home URL for thumbnails	- (Services\ DocumentViewer\ SendToURL)	URL for enaio® documentviewer document previews, e.g. when using the 'Send e-mail' feature in enaio® client. Thumbnails of the first page of documents which are attached to an e-mail will be inserted into the e-mail body whenever an e-mail is sent to an internal recipient.
Job directory	-	UNC path that enaio® documentviewer job files

	(Conversion\ ContentViewerJobFolder)	are filed to. The jobs are written to the `…\osdocumentviewer \data\jobs` directory if no other path was specified on the administration page `config.properties`. When the CPB is used, messages instead of jobs are used for communication, thus it is not necessary to specify the directory.

Appconnector

Parameters	Default (Registry path/entry)	Description
Home URL	- (Services\ AppConnector\URL)	Basic URL of enaio® appconnector
Service endpoint	- (Services\AppConnector\API)	URL under which the service is accessible.
Service endpoint for direct access	- (Services\AppConnector\ API_DIRECT)	The URL specifies the server that the service is running on. The setup automatically registers the URL on the enaio® server. The URL consists of the following elements: `http://<server>/osrest`

Web service

Parameters	Default (Registry path/entry)	Description
Service endpoint	- (Services\OSWS\API)	URL under which the service is accessible.
Service endpoint for direct access	- (Services\OSWS\API_DIRECT)	The URL specifies the server that the service is running on. The setup automatically registers the URL on the enaio® server. The URL consists of the following elements: `http://<server>/osws`

Exchange

Parameters	Default (Registry path/entry)	Description
Service endpoint	- (Services\OSExchange\API)	URL under which the service is accessible.
Service endpoint for direct access	- (Services\OSExchange\ API_ DIRECT)	The URL specifies the server that the application is running on. The URL is registered on the enaio® server as soon as it is started and the enaio® webservice settings are transferred to the server. The URL consists of the following elements: `http://<server>/ OsExchangeWS`

Imap

Parameters	Default (Registry path/entry)	Description
Service endpoint	- (Services\IMAP\API)	URL under which the service is accessible.
Service endpoint for direct access	- (Services\IMAP\API_DIRECT)	The URL specifies the server that the service is running on. The setup automatically registers the URL on the enaio® server.

Fulltext

Parameters	Default (Registry path/entry)	Description
Service endpoint	- (Services\Fulltext\API)	URL under which the service is accessible.
Service endpoint for direct access	- (Services\Fulltext\API_DIRECT)	The URL specifies the server that the service is running on. The setup automatically registers the URL on the enaio® server.

Gateway

Parameters	Default (Registry path/entry)	Description
Service endpoint	- (Services\Gateway\API)	URL under which the service is accessible.
Service endpoint	- (Services\Gateway\API_DIRECT)	The URL specifies the server that the service is running on. The

for direct access		setup automatically registers the URL on the enaio® server.

Detailsviewer

Parameters	Default (Registry path/entry)	Description
Home URL	- (Services\Detailsviewer\URL)	URL for parameterized service access
Service endpoint	- (Services\Detailsviewer\API)	URL under which the service is accessible.
Service endpoint for direct access	- (Services\Detailsviewer\API_DIRECT)	The URL specifies the server that the service is running on. The setup automatically registers the URL on the enaio® server.

Discovery

Parameters	Default (Registry path/entry)	Description
Service endpoint for direct access	- (Services\Discovery\API_DIRECT)	The URL specifies the server that the service is running on. The setup automatically registers the URL on the enaio® server.

Dashlet error

Parameters	Default (Registry path/entry)	Description
Home URL	http://www.optimal-systems.com (Services\Dashlet_ErrorURL)	This page is shown in the event of dashlet error or if a dashlet is not available.

Dashlet 1-10

Parameters	Default (Registry path/entry)	Description
Home URL	- (Services\Dashlet1_URL) (Services\Dashlet2_URL) …	Home URL for dashlet 1-10.
Title	Dashlet 1 (Services\Dashlet1_Title) Dashlet 2 (Services\Dashlet2_Title)	Window and tooltip title to be shown in the enaio® client workspace.

	…	
Icon ID	0 (Services\Dashlet1_IconID=0)	ID of an icon that is integrated using enaio® editor.
Load at start	No (Services\Dashlet1_LoadOnStartup) (Services\Dashlet2_LoadOnStartup) …	The dashlet will be displayed when the client starts and receives updates using method calls instead of URL parameters.

Dashlets do not need to be numbered sequentially. Therefore, single dashlets can be deactivated without any problem.

Category: Full text

Data in the **Full-text** category are divided into further areas.

Full-text general

Parameters	Default (registry entry)	Description
Full text engine	Lucene (VTX\Engine=lu)	Type of the used full text engine
Index documents	No (VTX\IndexDocument=0)	Defines whether to index the document files.
Index index data	No (VTX\IndexMetadata=0)	Defines whether index data of objects will be indexed.
Full text export directory	- (VTX\IndexExportPath)	The directory into which full text data will be filed.
Cache full-text files for OCR	No (VTX\CopyFiles=0)	Specifies whether full text files for OCR are temporarily saved in order to prevent conflicts caused by multiple file access.
Directory into which full text data are cached for OCR.	- (VTX\CopyFilesDir)	If full text files are temporarily saved (see above), the directory is specified here.

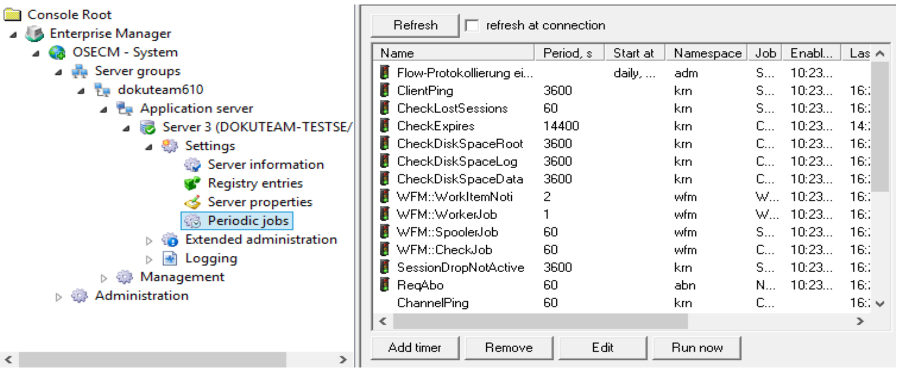
Lucene

Parameters	Default (registry entry)	Description
URL	- (VTX\LUC\IndexURL)	URL to the WEB service of the full-text engine.
Maximum number of results	1000 (VTX\LUC\IndexServerMaxHit=1000)	Maximum number of results a full text search in enaio® client can return. The default value is high and can be reduced.

OCR call	Yes (VTX\LUC\CallOCR=1)	Specifies whether OCR processing is carried out before image documents are transferred to the full text engine.
Full text auto-complete server	- (VTX\LUC\AutoCompleteServer)	Address or name of the server which runs the auto-complete feature for the full text service. In most cases the address or name are identical with the address of the full text server.
Full text auto-complete port	- (VTX\LUC\AutoCompletePort)	Server port.

Periodic Jobs

As in the **Settings > Server properties > Category: Periodic jobs** area, all periodic jobs executed by the server are listed here. An icon indicates whether or not the periodic job is active. You can use the **Edit** button to open the configuration dialog and modify the settings, or use the **Execute** button to execute a periodic job.

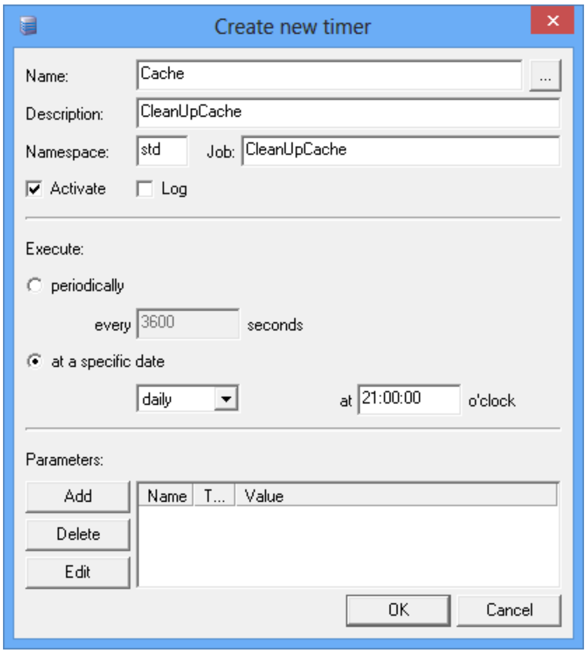


☐ refresh at connection

Name	Period, s	Start at	Namespace	Job	Enabl...	Las
Flow-Protokollierung ei...		daily, ...	adm	S...	10:23...	
ClientPing	3600		krn	S...	10:23...	16:
CheckLostSessions	60		krn	S...	10:23...	16:
CheckExpires	14400		krn	C...	10:23...	14:
CheckDiskSpaceRoot	3600		krn	C...	10:23...	16:
CheckDiskSpaceLog	3600		krn	C...	10:23...	16:
CheckDiskSpaceData	3600		krn	C...	10:23...	16:
WFM::WorkItemNoti	2		wfm	W...	10:23...	16:
WFM::WorkerJob	1		wfm	W...	10:23...	16:
WFM::SpoolerJob	60		wfm	S...	10:23...	16:
WFM::CheckJob	60		wfm	C...	10:23...	16:
SessionDropNotActive	3600		krn	S...	10:23...	16:
ReqAbo	60		abn	N...	10:23...	16:
ChannelPing	60		krn	C...		16:

This area can also be used to create new periodic jobs.

Click the **Add** button to open the configuration dialog. Either the data of the job which has been configured at last or data of the selected job are preset.



Create new timer

Name: Cache

Description: CleanUpCache

Namespace: std Job: CleanUpCache

☑ Activate □ Log

Execute:

○ periodically

every 3600 seconds

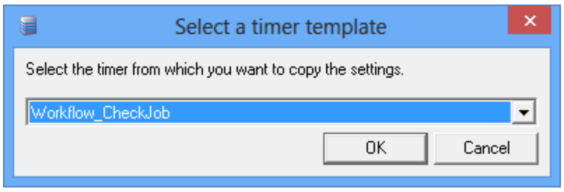
● at a specific date

daily at 21:00:00 o'clock

Parameters:

Configuration of periodic jobs requires detailed knowledge on server jobs and their parameters.

Open a template dialog using the button for the field **Name**:



Select a timer template

Select the timer from which you want to copy the settings.

Workflow_CheckJob

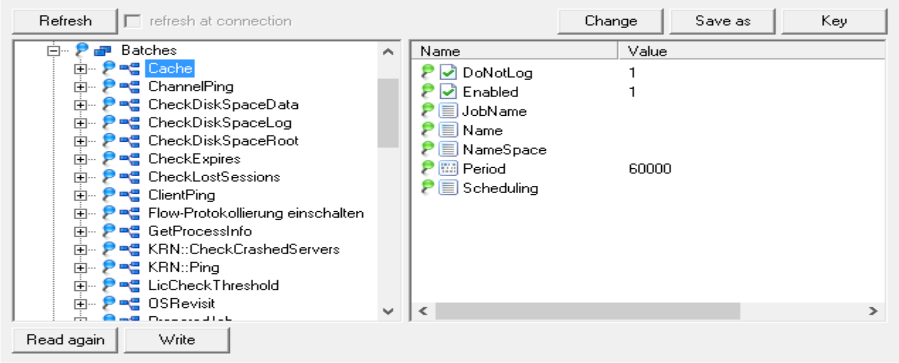
All periodic jobs which have been set up are available as templates.

However, templates are not required to set up a new periodic job.

The parameters and values assigned to a job are shown.

The namespace of a job is used to automatically determine in which queue it is executed. Use the optional parameter $$$QueueName$$$ to specify a queue in which the job is to be executed.

The data of periodic jobs is administered in the registry of the server. Under the **Batches** key, the keys for every periodic job are listed together with the required strings and values.



- Batches
  - Cache
  - ChannelPing
  - CheckDiskSpaceData
  - CheckDiskSpaceLog
  - CheckDiskSpaceRoot
  - CheckExpires
  - CheckLostSessions
  - ClientPing
  - Flow-Protokollierung einschalten
  - GetProcessInfo
  - KRN::CheckCrashedServers
  - KRN::Ping
  - LicCheckThreshold
  - OSRevisit

Name	Value
☑ DoNotLog	1
☑ Enabled	1
JobName	
Name	
NameSpace	
Period	60000
Scheduling	

Example for periodic jobs

The following example describes the configuration of a periodic job which turns on the flow logging of enaio® server in the evening and turns it off again in the morning.

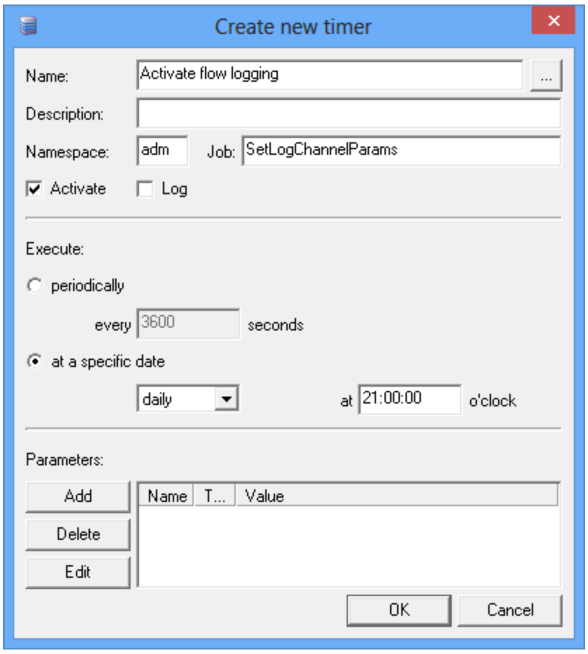
Description of the job:

adm.SetLogChannelParams		
Description:	This job turns the logging channels, which are configured for the server process, on or off at runtime and modifies the logging level.	
Parameter:	Flags (INT)	must be 0
	Params (STRING)	Describes what must be changed. This parameter has the following form: alias,channel,param=value; alias,channel,param=value; … Example: default,flow log,suspended=1; default,flow log,level=5;
Return:	(INT) : 0 = job successful, otherwise error code	

Multiple channels or multiple parameters can be thus addressed with a job. The intended settings must be separated by semicolons. A setting comprises the alias name, the channel name and the parameter name with value. The alias and channel names must be written exactly as in the file `orxpt.cfg` in the server directory. Parameter name is either 'level' or 'suspended'. The value of 'level' must be an integer from 0 to 6, the value of 'suspended' must be set to 1 (active) or 0 (inactive).

Configuration:

Open the configuration dialog using the **Add** button.



Create new timer

Name: Activate flow logging

Description:

Namespace: adm Job: SetLogChannelParams

☑ Activate □ Log

Execute:

○ periodically

every 3600 seconds

● at a specific date

daily at 21:00:00 o'clock

Parameters:

Name	T...	Value

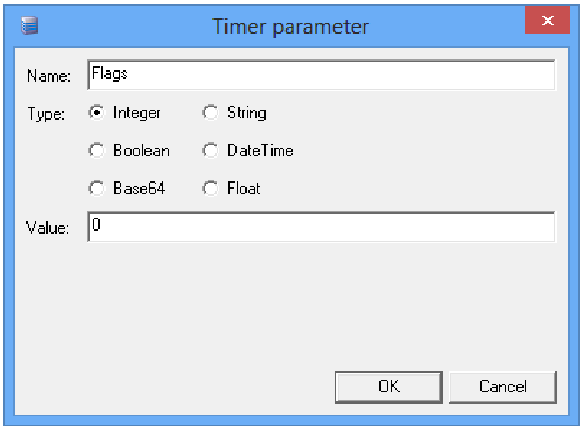
Enter a reasonable name, a description, the namespace, and the job; in this case, the namespace 'adm' and the job 'SetLogChannelParams'.

Multiple execution specifies where in the case of a job that is already running another job is started or not.

Decide whether to execute the job periodically or at a specific date that you can define, in the current example: every day at 9 p.m.

The job requires the two parameters **Flags** and **Params**. Specify these parameters in the **Parameters** area via the **Add** button.

The **Flags** parameter has the type **Integer** and the value '0.'



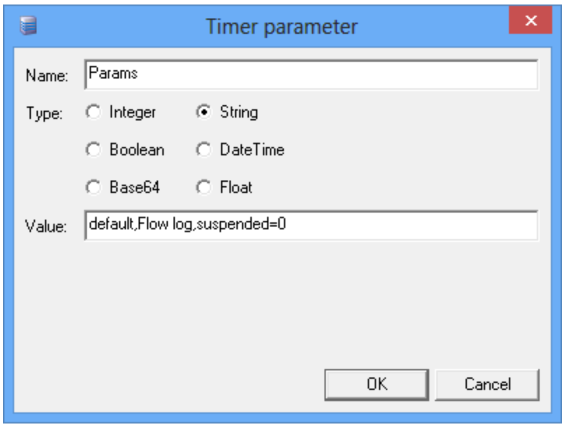
Timer parameter

Name: Flags

Type: ● Integer ○ String ○ Boolean ○ DateTime ○ Base64 ○ Float

Value: 0

The **Params** parameter has the type **String** and the value comprises the following three items: alias name, channel name, and activation of logging (suspended=0).



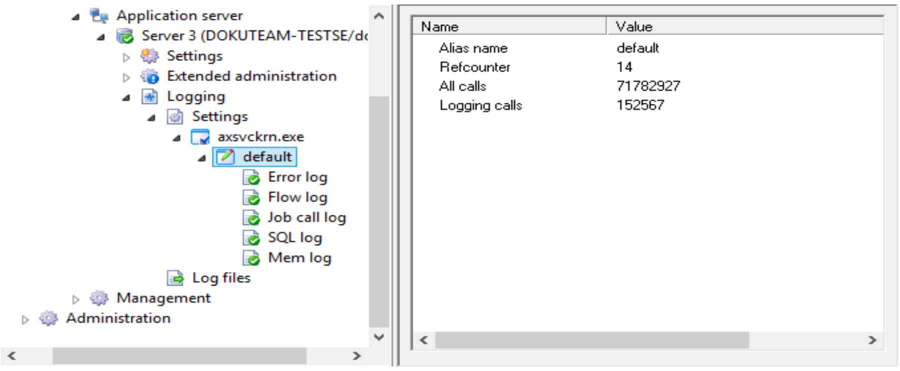
Timer parameter

Name: Params

Type: ○ Integer ● String ○ Boolean ○ DateTime ○ Base64 ○ Float

Value: default,Flow log,suspended=0

You can find the alias and channel names in the area **Server** > **Logging** > **Settings** > **axsvckrn.exe**. The alias name is indicated there. Log channels are assigned. The standard alias name is 'default,' while the standard log channels are 'Error,' 'Flow,' 'Log,' and 'SQL.'



```
Application server
  Server 3 (DOKUTEAM-TESTSE/dc
    Settings
    Extended administration
    Logging
      Settings
        axsvckrn.exe
          default
            Error log
            Flow log
            Job call log
            SQL log
            Mem log
      Log files
  Management
Administration
```

Name	Value
Alias name	default
Refcounter	14
All calls	71782927
Logging calls	152567

For the corresponding periodic job that disables logging, enter the intended time and assign the value 'suspended=1' to the **Params** parameter.

If you want to change the log level, indicate the intended level for the **Params** parameter, for example 'level=0.'

The data is saved in the registry.

Server – Extended Administration

The **Extended administration** area offers extensive insight into the system processes. This information can be useful for system optimization and error analysis.

The area is divided into the following sections:

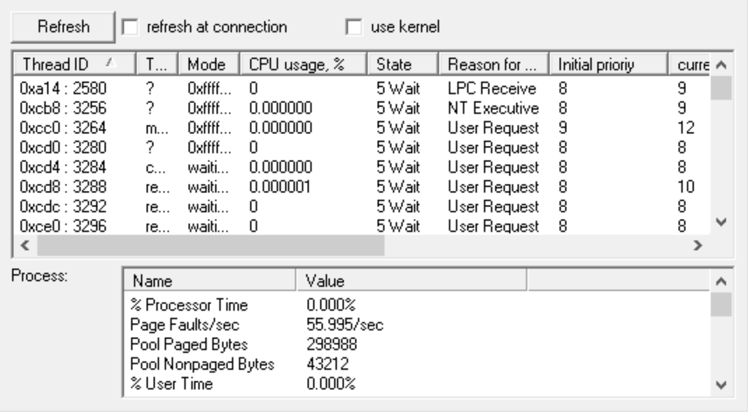
- Performance parameters
- Database pool
- Configuration
- Monitoring
- Miscellaneous

Performance Parameters

The **Performance parameters** area offers information on processes, job threads, and loaded modules.

Process information

This area displays detailed information on the process thread in which the server is running.



Refresh □ refresh at connection □ use kernel

Thread ID	T...	Mode	CPU usage, %	State	Reason for ...	Initial prioriy	curre
0xa14 : 2580	?	0xffff...	0	5 Wait	LPC Receive	8	9
0xcb8 : 3256	?	0xffff...	0.000000	5 Wait	NT Executive	8	9
0xcc0 : 3264	m...	0xffff...	0.000000	5 Wait	User Request	9	12
0xcd0 : 3280	?	0xffff...	0	5 Wait	User Request	8	8
0xcd4 : 3284	c...	waiti...	0.000000	5 Wait	User Request	8	8
0xcd8 : 3288	re...	waiti...	0.000001	5 Wait	User Request	8	10
0xcdc : 3292	re...	waiti...	0	5 Wait	User Request	8	8
0xce0 : 3296	re...	waiti...	0	5 Wait	User Request	8	8

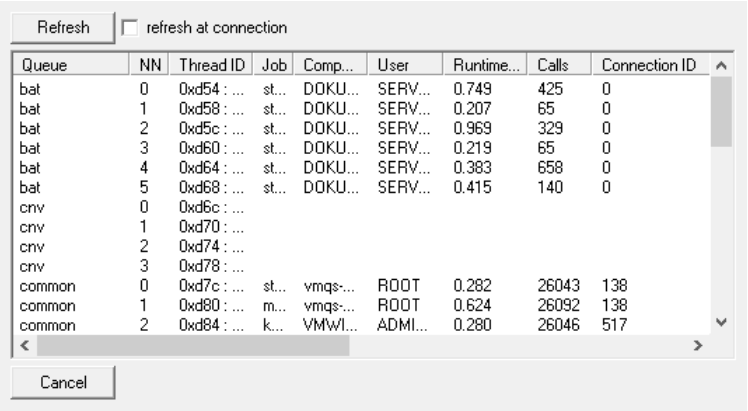
Process:

Name	Value
% Processor Time	0.000%
Page Faults/sec	55.995/sec
Pool Paged Bytes	298988
Pool Nonpaged Bytes	43212
% User Time	0.000%

Here, you can find out whether or not computer load is too high.

Job threads

All queues that are used by enaio® server are listed here.



Refresh □ refresh at connection

Queue	NN	Thread ID	Job	Comp...	User	Runtime...	Calls	Connection ID
bat	0	0xd54 : ...	st...	DOKU...	SERV...	0.749	425	0
bat	1	0xd58 : ...	st...	DOKU...	SERV...	0.207	65	0
bat	2	0xd5c : ...	st...	DOKU...	SERV...	0.969	329	0
bat	3	0xd60 : ...	st...	DOKU...	SERV...	0.219	65	0
bat	4	0xd64 : ...	st...	DOKU...	SERV...	0.383	658	0
bat	5	0xd68 : ...	st...	DOKU...	SERV...	0.415	140	0
cnv	0	0xd6c : ...						
cnv	1	0xd70 : ...						
cnv	2	0xd74 : ...						
cnv	3	0xd78 : ...						
common	0	0xd7c : ...	st...	vmqs-...	ROOT	0.282	26043	138
common	1	0xd80 : ...	m...	vmqs-...	ROOT	0.624	26092	138
common	2	0xd84 : ...	k...	VMWI...	ADMI...	0.280	26046	517

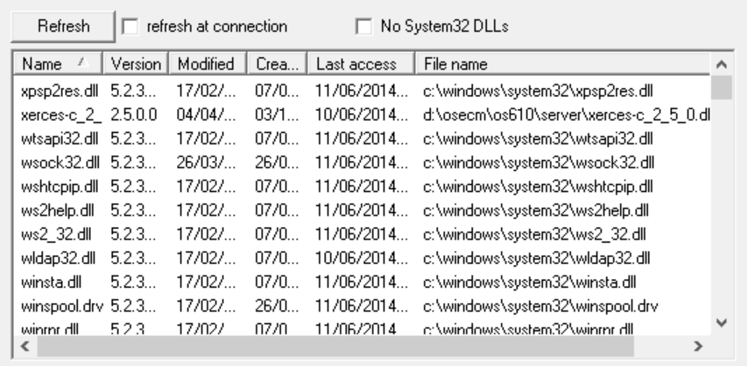
Cancel

You can determine which jobs are processed in which threads of the queues and the current state of each job.

If you select an entry, you can cancel the job execution.

Loaded modules

All libraries loaded by the server are listed here. Libraries from the System32 directory can be hidden.



Refresh ☐ refresh at connection ☐ No System32 DLLs

Name	Version	Modified	Crea...	Last access	File name
xpsp2res.dll	5.2.3...	17/02/...	07/0...	11/06/2014...	c:\windows\system32\xpsp2res.dll
xerces-c_2_	2.5.0.0	04/04/...	03/1...	10/06/2014...	d:\osecm\os610\server\xerces-c_2_5_0.dl
wtsapi32.dll	5.2.3...	17/02/...	07/0...	11/06/2014...	c:\windows\system32\wtsapi32.dll
wsock32.dll	5.2.3...	26/03/...	26/0...	11/06/2014...	c:\windows\system32\wsock32.dll
wshtcpip.dll	5.2.3...	17/02/...	07/0...	11/06/2014...	c:\windows\system32\wshtcpip.dll
ws2help.dll	5.2.3...	17/02/...	07/0...	11/06/2014...	c:\windows\system32\ws2help.dll
ws2_32.dll	5.2.3...	17/02/...	07/0...	11/06/2014...	c:\windows\system32\ws2_32.dll
wldap32.dll	5.2.3...	17/02/...	07/0...	10/06/2014...	c:\windows\system32\wldap32.dll
winsta.dll	5.2.3...	17/02/...	07/0...	11/06/2014...	c:\windows\system32\winsta.dll
winspool.drv	5.2.3...	17/02/...	26/0...	11/06/2014...	c:\windows\system32\winspool.drv
winrnr.dll	5.2.3	17/02/	07/0	11/06/2014	c:\windows\system32\winrnr.dll

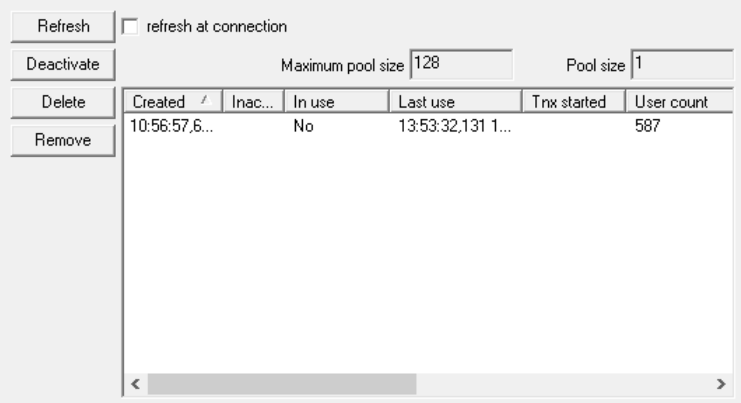
This view allows you to check the versions of libraries and the location from which they are loaded.

Database Pool

The **Database pool** area offers information on piping and the read threads.

Piping

The current status of the database connection is shown. The maximum pool size is preset to '128'. The current pool size is indicated and connections are listed.



☐ refresh at connection

Maximum pool size 128 Pool size 1

Created	Inac...	In use	Last use	Tnx started	User count
10:56:57,6...		No	13:53:32,131 1...		587

This view can be used to step-by-step eliminate hanging-up transactions of a connection.

In the first step, the transaction can be **disabled**. The server will not continue to process the transaction and wait whether the current job of the transaction can be terminated.

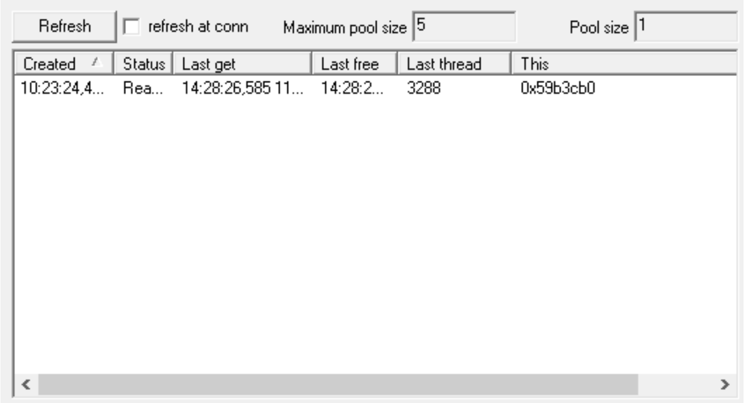
The second step is to **Delete** the transaction, i.e. the server will terminate it.

The connection can be **removed** in the third step, i.e. disconnected.

Read Threads

The current status of the database connection for the read threads is shown. The maximum pool size is preset to '5' and can be adjusted in the **Server properties > Category**: **Data** area, if the connection is heavily utilized.

The current and maximum pool size is shown and connections are listed.

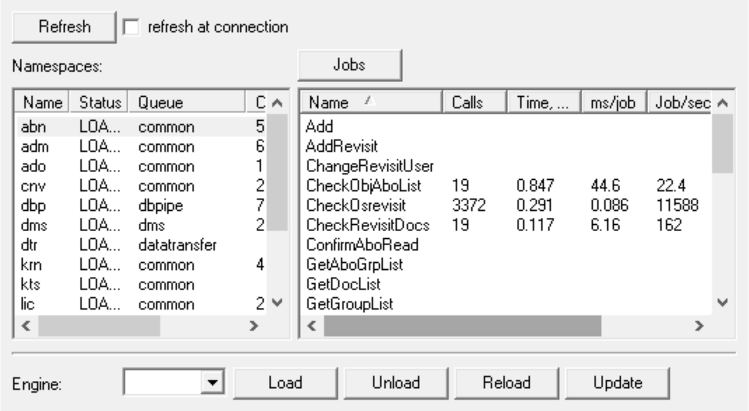


□ refresh at conn Maximum pool size 5 Pool size 1

Created	Status	Last get	Last free	Last thread	This
10:23:24,4...	Rea...	14:28:26,585 11...	14:28:2...	3288	0x59b3cb0

Setup/Engines

All loaded engines are listed here. An engine's number of job calls is listed along with other parameters related to the engines. If you select an engine and use the **Jobs** button, you can show all the engine jobs with the number and properties of calls.



□ refresh at connection

Namespaces:

Name	Status	Queue	C
abn	LOA...	common	5
adm	LOA...	common	6
ado	LOA...	common	1
cnv	LOA...	common	2
dbp	LOA...	dbpipe	7
dms	LOA...	dms	2
dtr	LOA...	datatransfer	
krn	LOA...	common	4
kts	LOA...	common	
lic	LOA...	common	2

Name	Calls	Time, ...	ms/job	Job/sec
Add				
AddRevisit				
ChangeRevisitUser				
CheckObjAboList	19	0.847	44.6	22.4
CheckOsrevisit	3372	0.291	0.086	11588
CheckRevisitDocs	19	0.117	6.16	162
ConfirmAboRead				
GetAboGrpList				
GetDocList				
GetGroupList				

Engine:

You can **load**, **unload**, and **reload** an engine, – i.e. unload and immediately reload.

You can load an updated version of an engine using the **Update** button. This version must be located in the `server\Update\new` directory. The server unloads the affected engine and replaces the current version with the updated version by loading it.

> If you work with more than one server, you must update the engines of all servers.

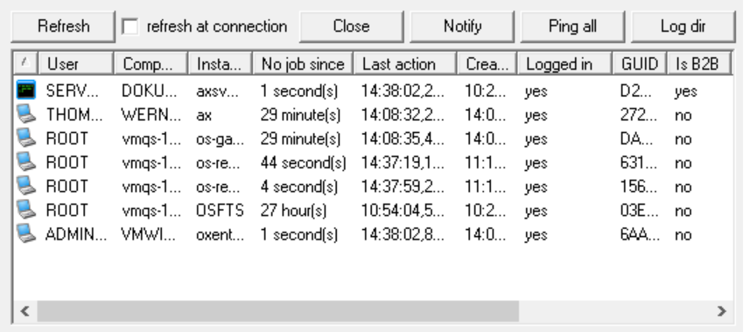
Monitoring

The **Monitoring** area offers information on connections to clients and servers, information on job queues and job calls, and also allows you to view and send notifications to clients.

Connections/Active clients

This area lists all current connections to clients.

The list includes the times at which a connection has been established and the last job has been executed.



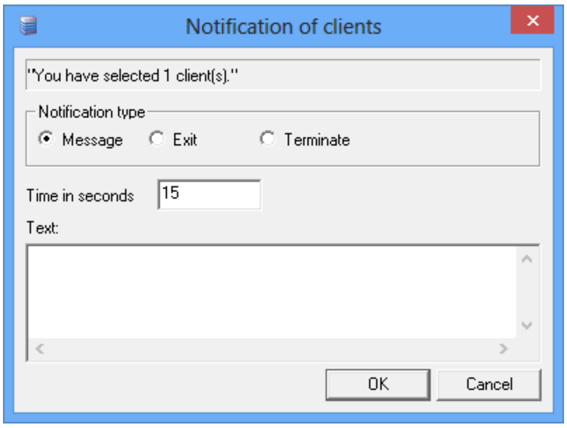
☐ refresh at connection

	User	Comp...	Insta...	No job since	Last action	Crea...	Logged in	GUID	Is B2B
	SERV...	DOKU...	axsv...	1 second(s)	14:38:02,2...	10:2...	yes	D2...	yes
	THOM...	WERN...	ax	29 minute(s)	14:08:32,2...	14:0...	yes	272...	no
	ROOT	vmqs-1...	os-ga...	29 minute(s)	14:08:35,4...	14:0...	yes	DA...	no
	ROOT	vmqs-1...	os-re...	44 second(s)	14:37:19,1...	11:1...	yes	631...	no
	ROOT	vmqs-1...	os-re...	4 second(s)	14:37:59,2...	11:1...	yes	156...	no
	ROOT	vmqs-1...	OSFTS	27 hour(s)	10:54:04,5...	10:2...	yes	03E...	no
	ADMIN...	VMWI...	oxent...	1 second(s)	14:38:02,8...	14:0...	yes	6AA...	no

You can close selected connection by using the **Close** button. Affected clients will create a new connection when the next job is to be performed.

Using the **Ping to all** button will send a ping to all clients. You will receive the results of the ping.

With the **Notify** button you can send a message to the selected clients or close them.



"You have selected 1 client(s)."

Notification type

● Message ○ Exit ○ Terminate

Time in seconds: 15

Text:

The following options available:

- Send **Message** to selected clients

  Type text and specify how long the message will be displayed in the client application.

- **Exit** selected clients

  Type text and specify the time until the client will exit.

  Once the specified time has expired, the selected clients will exit and all checked out documents checked in.

- **Terminate** selected clients

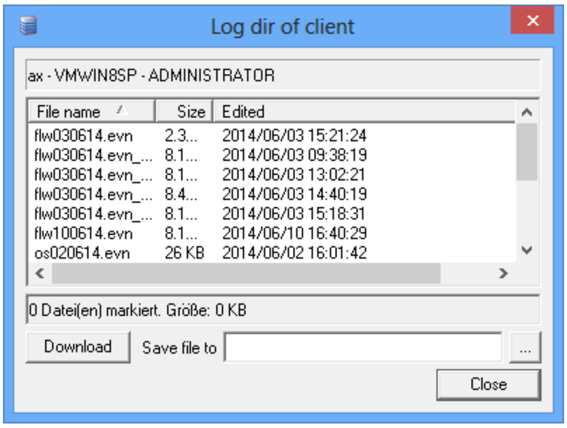
  Type text and specify the time until the client will exit.

  It may occur that client applications cannot exit. The feature **Terminate** can be used to shut down client applications. Checked out documents may not be checked in and temporary files may not be deleted either.

  Terminating client applications may cause data loss.

In multi-server systems, a server can only inform clients that are connected to the server.

Use the **Log dir** button to transfer the log of a selected client.



Log dir of client

ax - VMWIN8SP - ADMINISTRATOR

File name	Size	Edited
flw030614.evn	2.3...	2014/06/03 15:21:24
flw030614.evn_...	8.1...	2014/06/03 09:38:19
flw030614.evn_...	8.1...	2014/06/03 13:02:21
flw030614.evn_...	8.4...	2014/06/03 14:40:19
flw030614.evn_...	8.1...	2014/06/03 15:18:31
flw100614.evn	8.1...	2014/06/10 16:40:29
os020614.evn	26 KB	2014/06/02 16:01:42

0 Datei(en) markiert. Größe: 0 KB

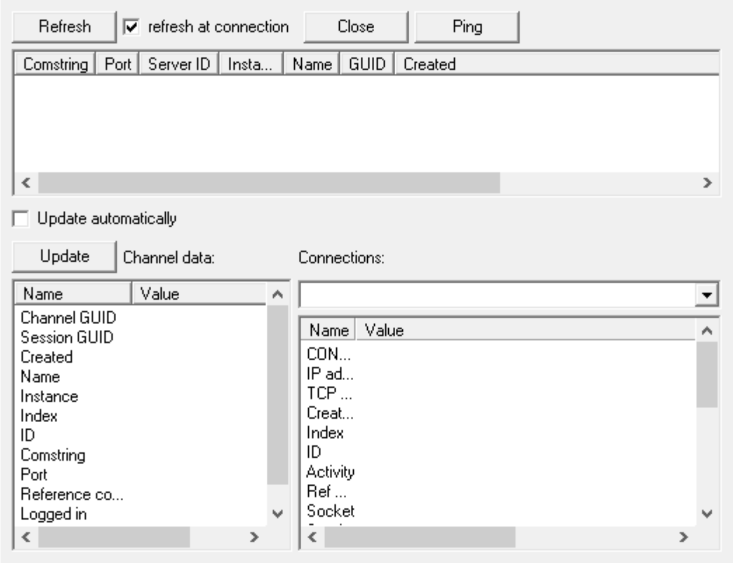
Save file to

Select the logs you want to transfer, specify a directory and click **Download**.

Connections to Other Servers

In this area, all of the server family's current connections to other servers are listed.

What is shown is when a server connection was created. You can close connections and send a pings.



☑ refresh at connection

Comstring	Port	Server ID	Insta...	Name	GUID	Created

□ Update automatically

Channel data:

Name	Value
Channel GUID	
Session GUID	
Created	
Name	
Instance	
Index	
ID	
Comstring	
Port	
Reference co...	
Logged in	

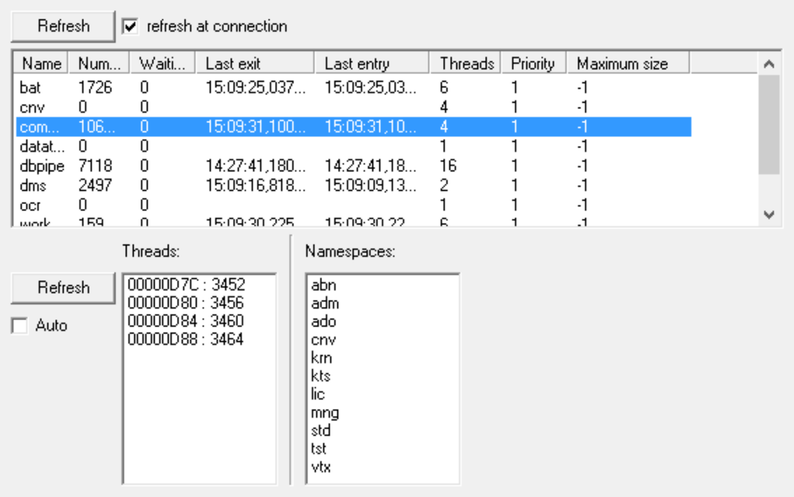
Connections:

Name	Value
CON...	
IP ad...	
TCP ...	
Creat...	
Index	
ID	
Activity	
Ref ...	
Socket	

To see all connection details in the lower area, select a server connection.

Job Queues

All job queues can be viewed here and you can estimate the current capacity using the parameters.



☑ refresh at connection

Name	Num...	Waiti...	Last exit	Last entry	Threads	Priority	Maximum size
bat	1726	0	15:09:25,037...	15:09:25,03...	6	1	-1
cnv	0	0			4	1	-1
com...	106...	0	15:09:31,100...	15:09:31,10...	4	1	-1
datat...	0	0			1	1	-1
dbpipe	7118	0	14:27:41,180...	14:27:41,18...	16	1	-1
dms	2497	0	15:09:16,818...	15:09:09,13...	2	1	-1
ocr	0	0			1	1	-1
work	159	0	15:09:30,225	15:09:30,22	6	1	-1

Threads:

00000D7C : 3452
00000D80 : 3456
00000D84 : 3460
00000D88 : 3464

Namespaces:

abn
adm
ado
cnv
krn
kts
lic
mng
std
tst
vtx

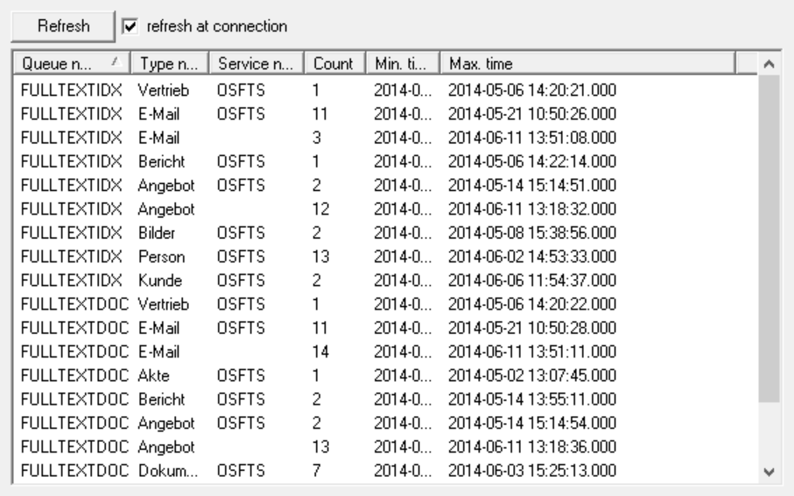
Select a queue, see the threads below. The engines assigned to the queue will also be listed.

CP Queues

In this area the jobs are shown which process the messages in the CPB queues.

Here you can see the service instances that have checked out one or more CPB messages for editing. The **Min. time** and **Max. time** indicate at what time the first and the last message was checked out by a service.

If no service name is assigned to a job, messages are available that are not yet processed by a service.



☑ refresh at connection

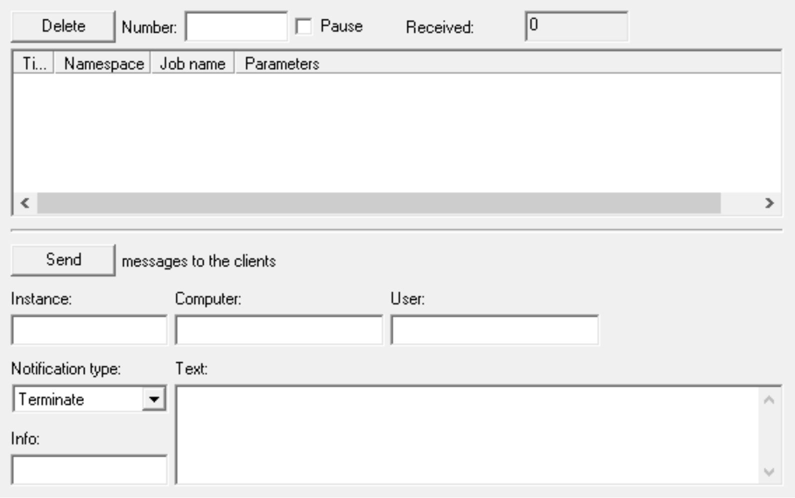
Queue n...	Type n...	Service n...	Count	Min. ti...	Max. time
FULLTEXTIDX	Vertrieb	OSFTS	1	2014-0...	2014-05-06 14:20:21.000
FULLTEXTIDX	E-Mail	OSFTS	11	2014-0...	2014-05-21 10:50:26.000
FULLTEXTIDX	E-Mail		3	2014-0...	2014-06-11 13:51:08.000
FULLTEXTIDX	Bericht	OSFTS	1	2014-0...	2014-05-06 14:22:14.000
FULLTEXTIDX	Angebot	OSFTS	2	2014-0...	2014-05-14 15:14:51.000
FULLTEXTIDX	Angebot		12	2014-0...	2014-06-11 13:18:32.000
FULLTEXTIDX	Bilder	OSFTS	2	2014-0...	2014-05-08 15:38:56.000
FULLTEXTIDX	Person	OSFTS	13	2014-0...	2014-06-02 14:53:33.000
FULLTEXTIDX	Kunde	OSFTS	2	2014-0...	2014-06-06 11:54:37.000
FULLTEXTDOC	Vertrieb	OSFTS	1	2014-0...	2014-05-06 14:20:22.000
FULLTEXTDOC	E-Mail	OSFTS	11	2014-0...	2014-05-21 10:50:28.000
FULLTEXTDOC	E-Mail		14	2014-0...	2014-06-11 13:51:11.000
FULLTEXTDOC	Akte	OSFTS	1	2014-0...	2014-05-02 13:07:45.000
FULLTEXTDOC	Bericht	OSFTS	2	2014-0...	2014-05-14 13:55:11.000
FULLTEXTDOC	Angebot	OSFTS	2	2014-0...	2014-05-14 15:14:54.000
FULLTEXTDOC	Angebot		13	2014-0...	2014-06-11 13:18:36.000
FULLTEXTDOC	Dokum...	OSFTS	7	2014-0...	2014-06-03 15:25:13.000

Notifications

This area displays the notifications received by the server.

The maximum number of notifications is to be entered into the **Number** field. If you select the option **Pause**, no messages will be received.

Use the **Delete** button to delete all messages.



Number:

□ Pause

Received: 0

Notification type: Terminate

You can also send and close messages to clients.

Parameter:

Instance The enaio® application to which the messages will be sent.

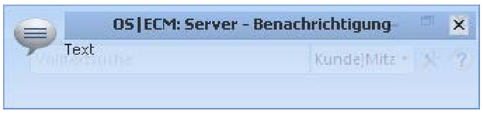
Example: `ax`

Computer The name of the computer to which the message will be sent.

User The enaio® user to whom the message is sent.

Message type Three types of messages can be sent:

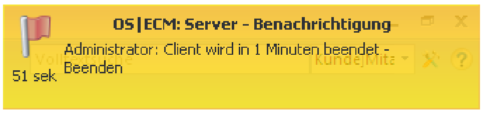
`Message` – A message with the value of the 'Text' parameter will be shown.



OS|ECM: Server - Benachrichtigung

Text

`Exit` – The application will be closed after the specified time has expired. A message with the contents of the 'Text' field will be displayed.



OS|ECM: Server - Benachrichtigung

Administrator: Client wird in 1 Minuten beendet - Beenden

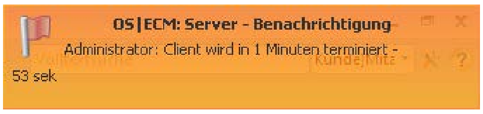
51 sek

The time remaining until the program is closed will be displayed.

The exit option corresponds to the user action 'Close' in enaio® client.

If a modal dialog is open in the application, the application can only be forced to close by sending a **Terminate** message.

`Terminate` –A message with the value of the 'Text' parameter will be shown. The application will be forced to close even if a modal dialog is open.



OS|ECM: Server - Benachrichtigung

Administrator: Client wird in 1 Minuten terminiert -

53 sek

Text This text will be displayed in the message.

If the user clicks on the text, a window will open and list all messages sent during the current session.

Info For exit and terminate messages, enter the number of minutes before program exit here. After counting down the indicated time, the message will close automatically.

The parameters **Computer**, **Instance**, and **User** are combined with logical AND. Only one value can be entered for each. No entry means 'Send to all.'

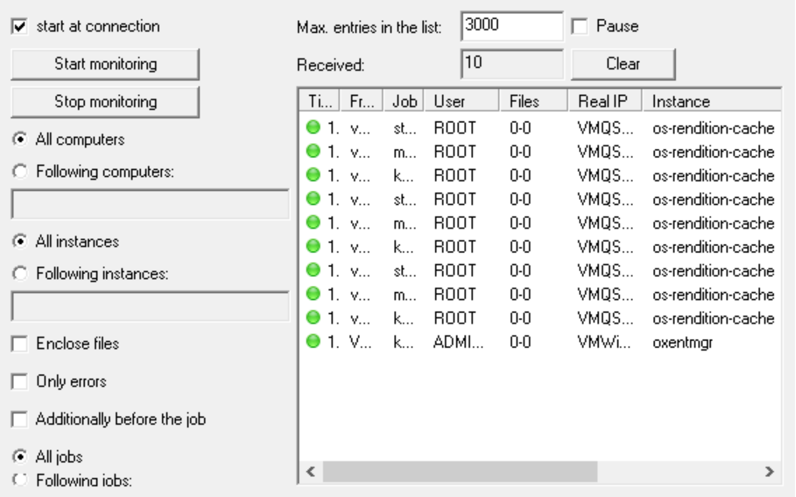
Use the **Send** button to carry out the corresponding action.

These functions can also be executed as periodic jobs using the **Monitoring > Connections > Active clients** area.

In multi-server systems, a server can only inform clients that are connected to the server.

Job calls

Here you can monitor the job calls of one or any other number of senders.



☑ start at connection

Start monitoring

Stop monitoring

● All computers

○ Following computers:

● All instances

○ Following instances:

□ Enclose files

□ Only errors

□ Additionally before the job

● All jobs

○ Following jobs:

Max. entries in the list: 3000 □ Pause

Received: 10 Clear

Ti...	Fr...	Job	User	Files	Real IP	Instance
● 1.	v...	st...	ROOT	0-0	VMQS...	os-rendition-cache
● 1.	v...	m...	ROOT	0-0	VMQS...	os-rendition-cache
● 1.	v...	k...	ROOT	0-0	VMQS...	os-rendition-cache
● 1.	v...	st...	ROOT	0-0	VMQS...	os-rendition-cache
● 1.	v...	m...	ROOT	0-0	VMQS...	os-rendition-cache
● 1.	v...	k...	ROOT	0-0	VMQS...	os-rendition-cache
● 1.	v...	st...	ROOT	0-0	VMQS...	os-rendition-cache
● 1.	v...	m...	ROOT	0-0	VMQS...	os-rendition-cache
● 1.	v...	k...	ROOT	0-0	VMQS...	os-rendition-cache
● 1.	V...	k...	ADMI...	0-0	VMWi...	oxentmgr

Specify one or several computers, separated by semicolons, or choose **All computers**.

Specify one or several instances to be monitored, i.e. enaio® components, separated by semicolons, or choose **All instances**. Instance names of individual enaio® components are transferred to enaio® server during startup and can be found in the **Instance** column.

Then decide whether to monitor all jobs or only selected ones. Select all jobs you want to monitor from the list. They are divided according to their engines.

For job monitoring, you can specify that only the 🟥 errors are listed. If you select the option **Additionally before the job**, all ▶ job calls that only have input parameters will be listed.

Activate the **Enclose files** option to copy all files which are sent through jobs to the temporary directory. The path is specified in the configuration dialog.

> This option can significantly increase network load.

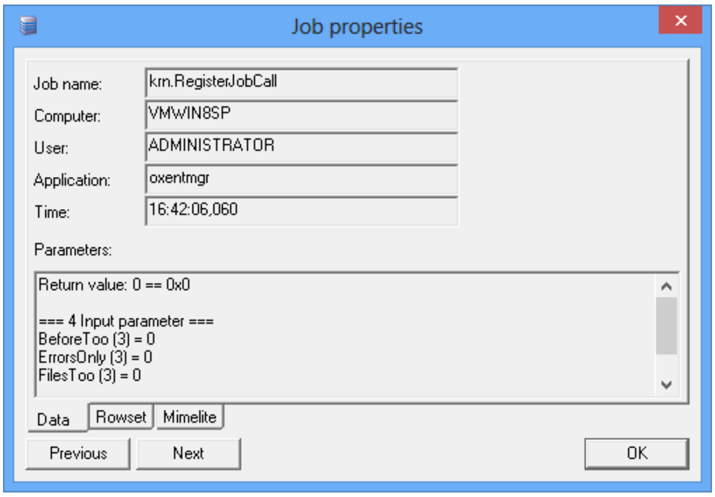
The jobs listed on the right are accordingly flagged with icons to indicate the type of entry.

Then click the **Start monitoring** button. Settings will be applied and the respective job calls listed.

If you activate the option **Start at connection**, job monitoring is started as soon as enaio® enterprise-manager is launched.

Enter the upper limit on the number of current job calls that will be shown in the **Max. entries in the list** field. The Pause option permits you to temporarily stop the recording.

Double clicking a list item will open the job's properties dialog:



Job properties

Job name: krn.RegisterJobCall
Computer: VMWIN8SP
User: ADMINISTRATOR
Application: oxentmgr
Time: 16:42:06,060

Parameters:

```
Return value: 0 == 0x0

=== 4 Input parameter ===
BeforeToo (3) = 0
ErrorsOnly (3) = 0
FilesToo (3) = 0
```

In the **Parameters** area on the **Data** tab, you will find a list of the input parameters as well as the return values of successful and failed jobs.

If the **Enclose files** option is activated, the path to the related file will be given here.

The **Rowset** tab shows SQL statements and results of the selected job.

On the **Mimelite** tab you can decode MIME encoded data.

Periodic job calls as well as their details are not displayed in this area for reasons of clarity. In order to facilitate analyses and debugging, e.g. during workflow development, periodic job calls can be sent to enaio® server-monitor. To do so, in the **Settings** > **Registry entries** area, change the value of the string `Schema\MonitorBatchCallsToo to '1.'` Sending of job calls to enaio® server-monitor is disabled by default.

Prepared Jobs

Jobs to be initialized by scripts or other customized contexts and performed by enaio® server can be parameterized in such a way that they are performed at a specific point of time.

Such jobs are listed here. You can intervene in the execution:

§ Run

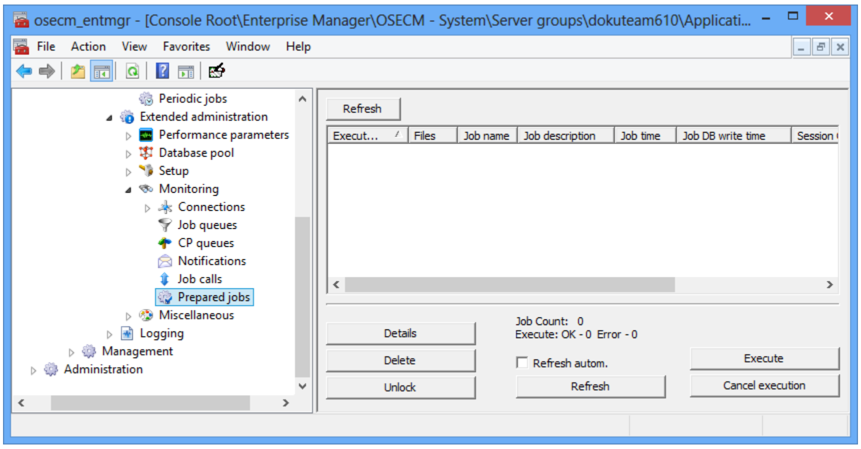
The prepared job will be performed instantly.

- Break the execution

  Execution of a prepared job is canceled
- Delete

  The prepared job will be deleted.
- Unlock

  Job data are locked in order to exclude multiple access issues. If a performance error occurs while the job is locked, you can unlock and perform the job.



Job Count: 0
Execute: OK - 0 Error - 0

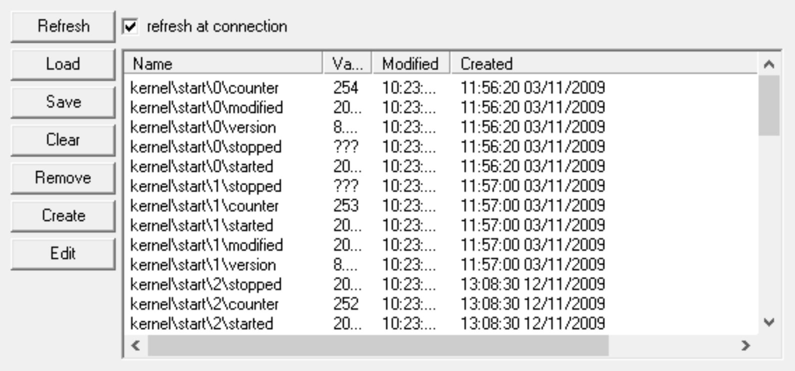
☐ Refresh autom.

Miscellaneous

Persistent Storage

The server’s last ten start and stop processes are entered into the database.

These data can be viewed here.



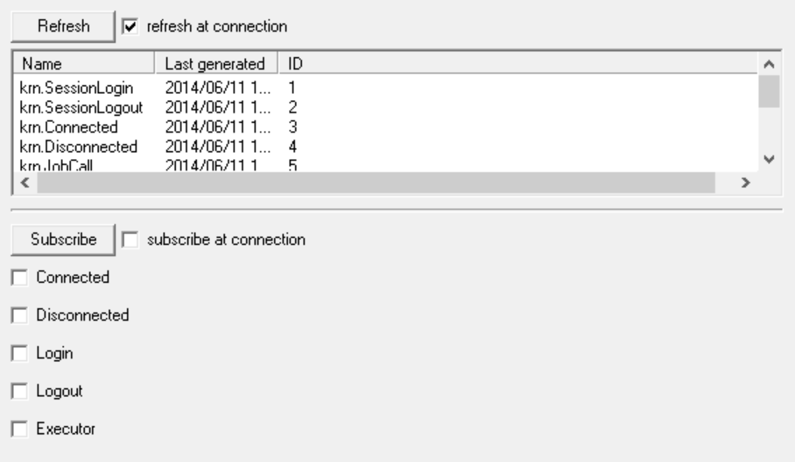
☑ refresh at connection

Name	Va...	Modified	Created
kernel\start\0\counter	254	10:23:...	11:56:20 03/11/2009
kernel\start\0\modified	20...	10:23:...	11:56:20 03/11/2009
kernel\start\0\version	8....	10:23:...	11:56:20 03/11/2009
kernel\start\0\stopped	???	10:23:...	11:56:20 03/11/2009
kernel\start\0\started	20...	10:23:...	11:56:20 03/11/2009
kernel\start\1\stopped	???	10:23:...	11:57:00 03/11/2009
kernel\start\1\counter	253	10:23:...	11:57:00 03/11/2009
kernel\start\1\started	20...	10:23:...	11:57:00 03/11/2009
kernel\start\1\modified	20...	10:23:...	11:57:00 03/11/2009
kernel\start\1\version	8....	10:23:...	11:57:00 03/11/2009
kernel\start\2\stopped	20...	10:23:...	13:08:30 12/11/2009
kernel\start\2\counter	252	10:23:...	13:08:30 12/11/2009
kernel\start\2\started	20...	10:23:...	13:08:30 12/11/2009

The entries of this area do not have any influence on the system's functions.

Kernel Events

Here you can subscribe to information on kernel events. The server will thus inform enaio® enterprise-manager about the events and enaio® enterprise-manager will then automatically update respective data in the affected settings areas.



Name	Last generated	ID
krn.SessionLogin	2014/06/11 1...	1
krn.SessionLogout	2014/06/11 1...	2
krn.Connected	2014/06/11 1...	3
krn.Disconnected	2014/06/11 1...	4
krn.JobCall	2014/06/11 1	5

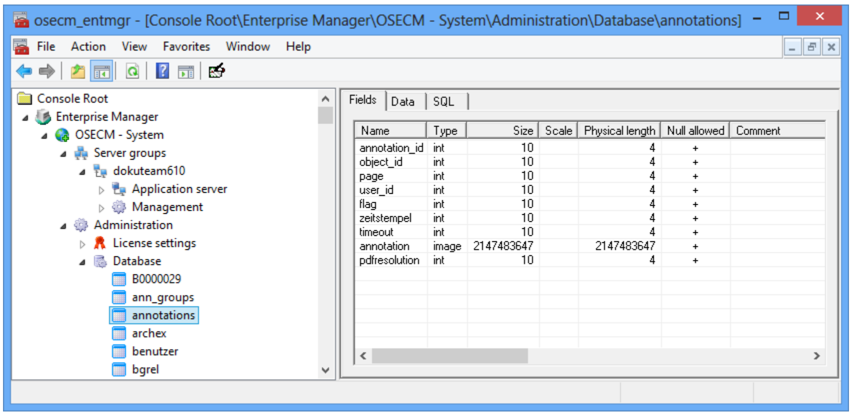
Other Administrative Functions

In the **enaio® server family** > **Administration** area you will find administrative functions for the entire server family. This area particularly allows you to manage the license system (see 'Introduction to the License System').

What is more, this area provides access to the database as well as an overview of a servers and sessions.

Database

To access the database, you must log in to it.


osecm_entmgr - [Console Root\Enterprise Manager\OSECM - System\Administration\Database\annotations]

Name	Type	Size	Scale	Physical length	Null allowed	Comment
annotation_id	int	10		4	+	
object_id	int	10		4	+	
page	int	10		4	+	
user_id	int	10		4	+	
flag	int	10		4	+	
zeitstempel	int	10		4	+	
timeout	int	10		4	+	
annotation	image	2147483647		2147483647	+	
pdfresolution	int	10		4	+	

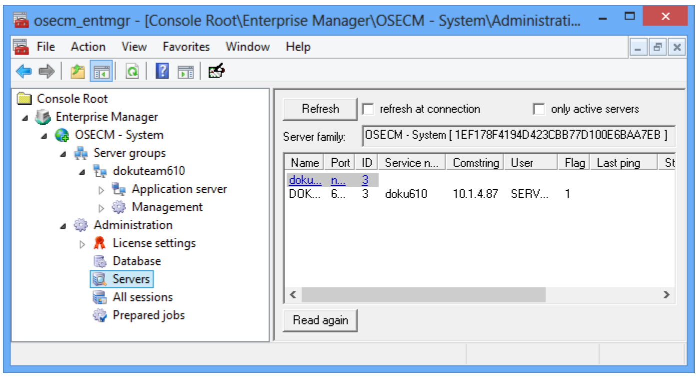
All tables which are contained in the database will be listed. The column definitions of each table are shown on the **Fields** tab, while table data are shown on the **Data** tab. Contents of BLOB fields can be viewed.

SQL statements can be executed via the **SQL** tab.

> Modification of data using SQL commands can lead to inconsistencies in the database and will cause data loss.

Servers

Under this node, all servers that are registered in the database are listed here together with the most important data.



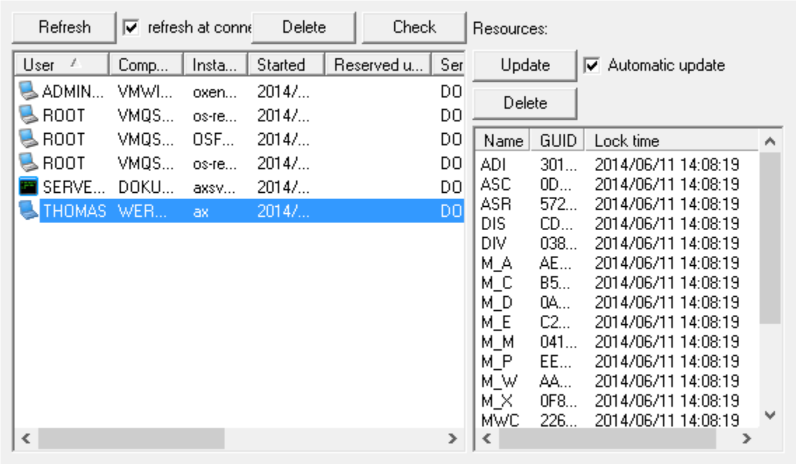
□ refresh at connection □ only active servers

Server family: OSECM - System [1EF178F4194D423CBB77D100E6BAA7EB]

Name	Port	ID	Service n...	Comstring	User	Flag	Last ping	St
doku...	n...	3						
DOK...	6...	3	doku610	10.1.4.87	SERV...	1		

All Sessions

This page lists all sessions of components which belong to the server family.



☑ refresh at conne

☑ Automatic update

User	Comp...	Insta...	Started	Reserved u...	Ser
ADMIN...	VMWI...	oxen...	2014/...		DO
ROOT	VMQS...	os-re...	2014/...		DO
ROOT	VMQS...	OSF...	2014/...		DO
ROOT	VMQS...	os-re...	2014/...		DO
SERVE...	DOKU...	axsv...	2014/...		DO
THOMAS	WER...	ax	2014/...		DO

Name	GUID	Lock time
ADI	301...	2014/06/11 14:08:19
ASC	0D...	2014/06/11 14:08:19
ASR	572...	2014/06/11 14:08:19
DIS	CD...	2014/06/11 14:08:19
DIV	038...	2014/06/11 14:08:19
M_A	AE...	2014/06/11 14:08:19
M_C	B5...	2014/06/11 14:08:19
M_D	0A...	2014/06/11 14:08:19
M_E	C2...	2014/06/11 14:08:19
M_M	041...	2014/06/11 14:08:19
M_P	EE...	2014/06/11 14:08:19
M_W	AA...	2014/06/11 14:08:19
M_X	0F8...	2014/06/11 14:08:19
MWC	226...	2014/06/11 14:08:19

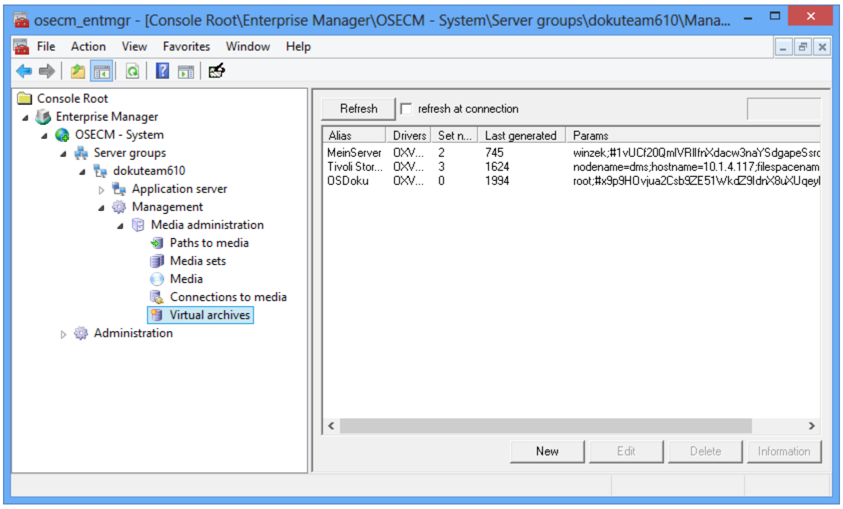
Select a session in order to display the license keys which are utilized by the session on the right side, where you also can delete them.

Connections Between Server Families

By exporting index data from the database or a server family and importing this data into the database of another server family, read access to documents of the first server family from the second can be made possible. To do so a virtual archive must be set up.

> You need a license key to integrate virtual archives.

Open the configuration area from the **Management** > **Media management** > **Virtual archives** item of a server group.



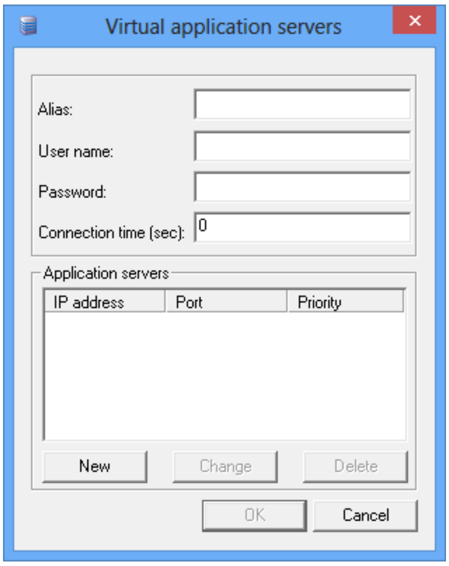
□ refresh at connection

Alias	Drivers	Set n...	Last generated	Params
MeinServer	OXV...	2	745	winzek;#1vUCf20QmlVRllfnXdacw3naYSdgapeSsrc
Tivoli Stor...	OXV...	3	1624	nodename=dms;hostname=10.1.4.117;filespacenam
OSDoku	OXV...	0	1994	root;#x9p9HOvjua2Csb9ZE51WkdZ9IdnX8uXUqeyl

Click **Refresh** to show the virtual archives, which have already been set up.

Set up a new path via the **New** button.

Firstly specify that you want to use an **Application server** as a virtual server. Then the following dialog will open.



Alias:

User name:

Password:

Connection time (sec): 0

Enter an alias, a user name and a password of a user who is registered as a user of the respective server family. This user furthermore requires access rights to the documents of which index data is exported from the source server family and imported to the destination server family.

The connection time (in seconds) is the period for which the connection will be kept open.

Click on the **New** button and specify the address and port of a server in the server family.

If you enter more than one server, divide the connection probability (priority) between them so that the sum is 100%. If you only define one server, enter '100' as its connection priority.

Confirm your entries with **OK**.

The new virtual archive will be displayed in the configuration area.

A system ID will be automatically assigned to every virtual archive. This system ID is required for the export of index data from the source server family.

You can find details about this in the enaio® import-export handbook.

Every time a user opens a document to which the system ID is assigned, the local server requests the document from the respective server.

These documents are labeled as reference documents in enaio® client. Reference documents can only be viewed not modified.

Virtual archives can be used for archiving.

Logging

Introduction to Logging

With enaio® logging you can set up a differentiated logging for each individual enaio® component.

At least one action ID is assigned to every message from a component. This ID allows log messages for flow, SQL, error, and general log messages to be directed to different output channels.

A channel accepts messages with the same action ID from one or more components and can store the messages in the internal log format or in OXMISC format.

The detailed channel properties settings allow configuring workstation and component-specific logging.

These settings are configured using enaio® manager-for-logfiles `axprotocolcfg.exe`. The configurations are saved in configuration files with the name `oxrpt.cfg`.

During installation of enaio®, you have indicated a path to the log directory. The setup program saves the configuration file `oxrpt.cfg`, which contains the log path for default log settings, to every directory containing enaio® components. Each component in the directory performs logging as defined in the configuration file `oxrpt.cfg` of the same directory.

Default logging creates flow, SQL, error, memory and job call log files with the following names:

`flwddmmyy.evn`

`sqlddmmyy.evn`

`errddmmyy.evn`

`memddmmyy.evn`

`logddmmyy.evn`

`dd` stands for the current day, `mm` is the current month, and `yy` is the current year.

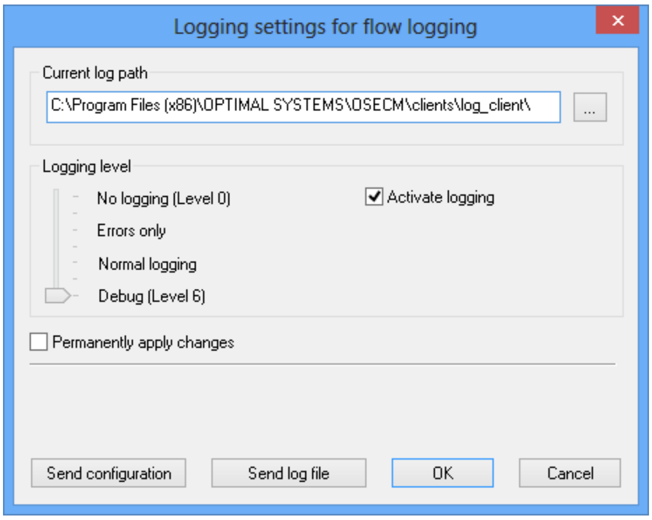
Using the configuration file oxrpt.cfg from the server directory, also flow and error logs for ABBYY FineReader text recognition are generated:

`frflddmmyy.evn`

`frerrddmmyy.evn`

These logs are saved in the internal log format. They can be opened with enaio® protocol-viewer `axrptview.exe`.

As a general rule, the flow logging can be changed at runtime from within every enaio® application. You can open the dialog **Log settings** via the **File** menu of the applications.



Logging settings for flow logging

Current log path

C:\Program Files (x86)\OPTIMAL SYSTEMS\OSECM\clients\log_client\

Logging level

No logging (Level 0)

Errors only

Normal logging

Debug (Level 6)

☑ Activate logging

□ Permanently apply changes

You can change the log settings for flow logging and activate/deactivate logging.

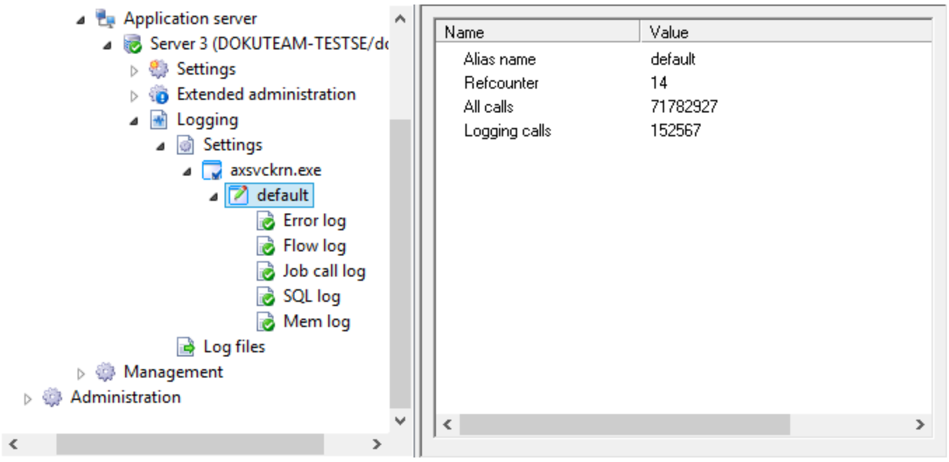
Users with the system role 'Administrator: Configure entire system' can permanently apply the changes. The modified settings are saved in the configuration file `oxrpt.cfg` of the application directory. They apply to all applications in this directory.

The settings for logging can be deployed to the client installation using the MSI package (see 'Installation Manual').

Logging and access to log settings can be disabled for all enaio® client installations using an entry in the `as.cfg` file located in the `etc` directory of the data directory:

```
[SYSTEM]
PreventLog=1
```

enaio® enterprise-manager can be used to manipulate the logging settings of enaio® server at runtime.



Name	Value
Alias name	default
Refcounter	14
All calls	71782927
Logging calls	152567

The following data for each standard log can be modified in the **Server > Logging** console root area:

§ Suspended

Logging can be enabled and disabled.

§ Level

The logging level can be modified.

§ Start new file every day

You can specify whether a new log file will be created every day.

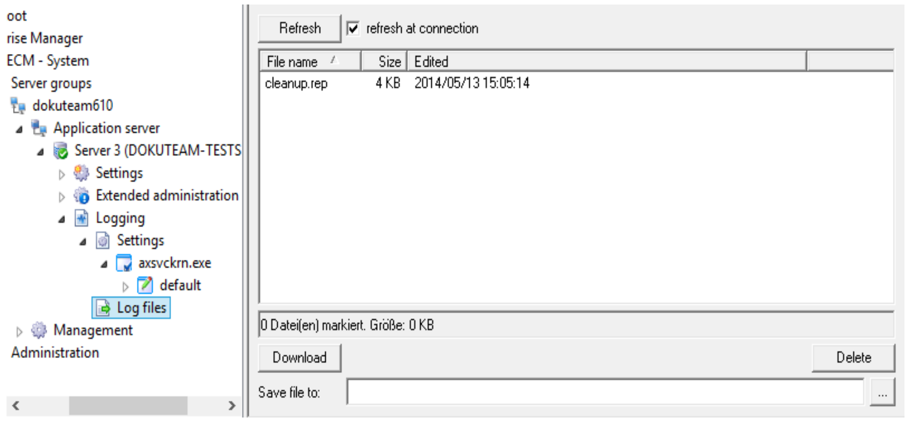
§ Maximum file size, KB

The maximum size of a log file in kilobyte

> The other data cannot be changed.

The chapter 'Periodic Jobs' provides an example of how to use periodic jobs to enable and disable server logging.

enaio® enterprise-manager also lets you pass logs from other servers.



File name	Size	Edited
cleanup.rep	4 KB	2014/05/13 15:05:14

0 Datei(en) markiert. Größe: 0 KB

All log files are listed under **Server** > **Logging** > **Log files** in the console root. To **Download** files, select them and specify a path. You can also delete files.

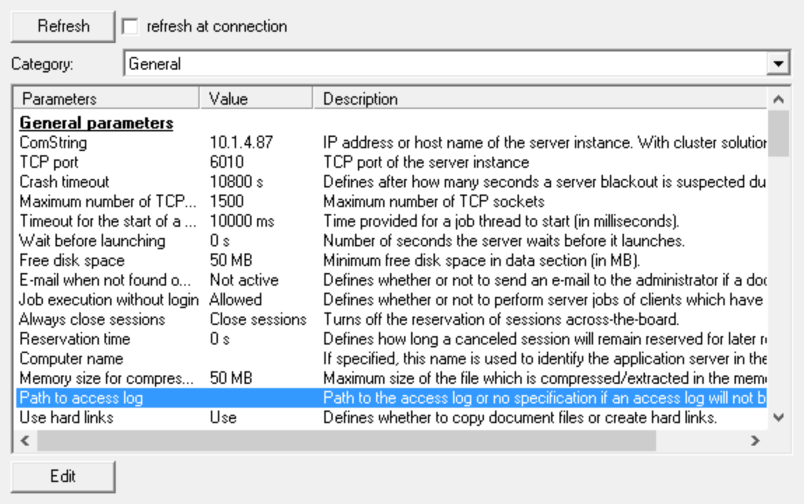
Irrespective of the logging configuration, log files are created automatically at every start and exit of enaio® server and saved to the directory `\server\ostemp`.

The log file for starting is called `startup.txt`, the log file for ending is called `shutdown.txt`. enaio® server enters the steps there that were executed and all the errors that occurred.

A message box will list all those errors which hindered a program or component to start.

Provided that enaio® server was started with the parameter 'v', a message box will list all errors that hindered enaio® server to start.

Access logging can also be activated irrespective of the general logging settings. It logs all data accesses and queries. Access logging is activated in enaio® enterprise-manager:



Category: General

Parameters	Value	Description
General parameters		
ComString	10.1.4.87	IP address or host name of the server instance. With cluster solutior
TCP port	6010	TCP port of the server instance
Crash timeout	10800 s	Defines after how many seconds a server blackout is suspected du
Maximum number of TCP...	1500	Maximum number of TCP sockets
Timeout for the start of a ...	10000 ms	Time provided for a job thread to start (in milliseconds).
Wait before launching	0 s	Number of seconds the server waits before it launches.
Free disk space	50 MB	Minimum free disk space in data section (in MB).
E-mail when not found o...	Not active	Defines whether or not to send an e-mail to the administrator if a doc
Job execution without login	Allowed	Defines whether or not to perform server jobs of clients which have
Always close sessions	Close sessions	Turns off the reservation of sessions across-the-board.
Reservation time	0 s	Defines how long a canceled session will remain reserved for later r
Computer name		If specified, this name is used to identify the application server in the
Memory size for compres...	50 MB	Maximum size of the file which is compressed/extracted in the mem
Path to access log		Path to the access log or no specification if an access log will not b
Use hard links	Use	Defines whether to copy document files or create hard links.

In the **Server Properties > Category: General** area and enter the log path as the value of the **Path to access log** parameter.

A log file with access data, named `sptyyyymmdd.txt`, will then be created there.

Database tables are generated and updated by the setup component `axmksys.dll`. Regardless of the setup, you can call up the `axmksys.exe` application from the service directory in order to adapt database tables. This component creates SQL and flow logs, the application in the directory `\log` in the application directory, the setup in the directory `\Programs\Common files\InstallShield\engine\6\Intel 32\LOG`. After successful installation, the setup logs are moved into the installation directory.

Warnings and Errors

Whether an event is to be treated as an error or only as a warning may not be clear in advance but only in connection with a specific installation. Therefore, it is possible to create a list of events for enaio® server which, instead of an error message, cause a warning and vice versa, instead of a warning, cause an error message.

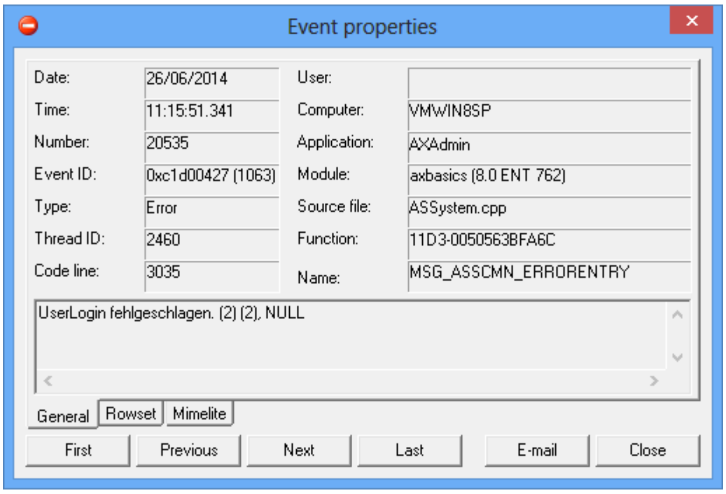
enaio® server checks whether the application directory contains a file named `axsvckrn.ert`, which contains such lists. If the file is found, its data is used to classify the events.

ERT files can be created with any editor.

Create the sections [eventstreatedasnonerror] and [eventstreatedaserror] for events which must only cause a warning and, instead of a warning, an error message, respectively.

In the intended section, enter the ID of the event and assign an application to it.

You can find these data in the enaio® protocol-viewer. You open the property dialog by double-clicking an event:



Event properties

Date:	26/06/2014	User:	
Time:	11:15:51.341	Computer:	VMWIN8SP
Number:	20535	Application:	AXAdmin
Event ID:	0xc1d00427 (1063)	Module:	axbasics (8.0 ENT 762)
Type:	Error	Source file:	ASSystem.cpp
Thread ID:	2460	Function:	11D3-0050563BFA6C
Code line:	3035	Name:	MSG_ASSCMN_ERRORENTRY

UserLogin fehlgeschlagen. (2) (2), NULL

It provides the ID and the application. You use the following syntax:

```
'Event ID' = 'switch',application
```

The event ID is entered in hexadecimal notation but without the leading flag '0x'.

The switch can either be '1' for 'on' or '0' for 'off'.

The application must be entered exactly as it appears in the properties dialog. Some applications are entered with, others without file extension.

For the example above, the entry must follow this form:

```
[eventstreatedasnonerror]
c1d00427=1,AXAdmin.exe
```

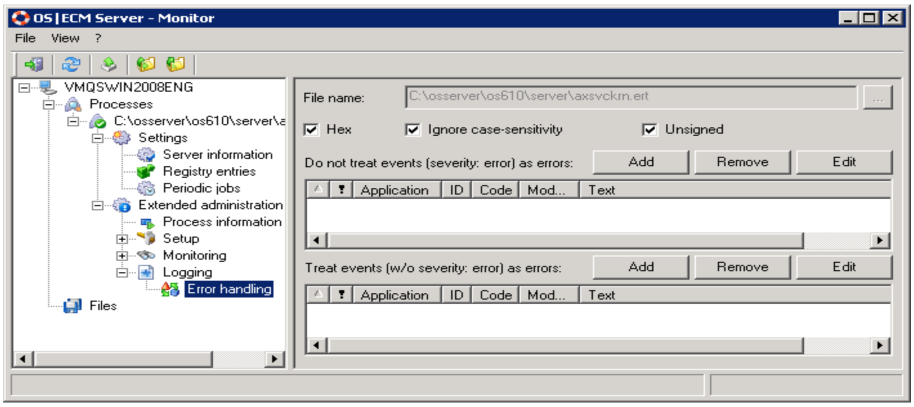
The text is not case-sensitive.

If you do not specify any application, the entry will apply to all applications.

Every event ID can only be entered once. If you want to assign more than one application, separate them by comma.

The file is saved as `axsvckrn.ert` in the `\server` directory. The data become effective after server restart.

enaio® server-monitor provides support in the **Error handling** section for creating the entries and the file.



File name: C:\osserver\os610\server\axsvckrn.ert

☑ Hex ☑ Ignore case-sensitivity ☑ Unsigned

Do not treat events (severity: error) as errors: Add Remove Edit

	!	Application	ID	Code	Mod...	Text

Treat events (w/o severity: error) as errors: Add Remove Edit

	!	Application	ID	Code	Mod...	Text

enaio® manager-for-logfiles

When enaio® is being installed, the log library `oxrpt.dll`, the configuration file `oxrpt.cfg`, and enaio® manager-for-logfiles `axprotocolcfg.exe` are installed in every directory with enaio® components.

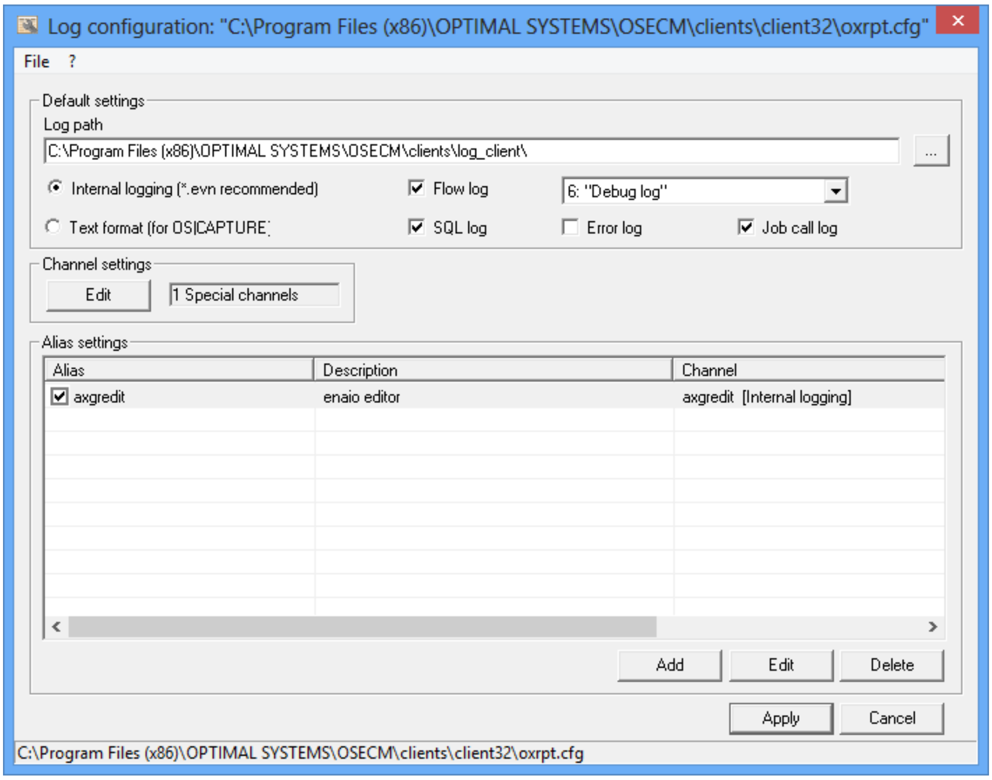
To change the default logging settings for components contained in this directory, use the configuration file `oxrpt.cfg` in the same directory or create new channels for components.

Every component reads its logging settings from the configuration file in its directory at program launched.

The enaio® manager-for-logfiles User Interface

> enaio® manager-for-logfiles is not incorporated in to the enaio® rights system. Make sure you have access to enaio® manager-for-logfiles via the operating system.

When the application starts, enaio® manager-for-logfiles opens the installed configuration file `oxrpt.cfg` from the application directory. The data from this configuration file are used for logging all components from the directory. The path and file name are shown in the title bar and the status bar.



Log configuration: "C:\Program Files (x86)\OPTIMAL SYSTEMS\OSECM\clients\client32\oxrpt.cfg"

Default settings

Log path: C:\Program Files (x86)\OPTIMAL SYSTEMS\OSECM\clients\log_client\

● Internal logging (*.evn recommended) ☑ Flow log 6: "Debug log"

○ Text format (for OS|CAPTURE) ☑ SQL log ☐ Error log ☑ Job call log

Channel settings: 1 Special channels

Alias settings

Alias	Description	Channel
☑ axgredit	enaio editor	axgredit [Internal logging]

C:\Program Files (x86)\OPTIMAL SYSTEMS\OSECM\clients\client32\oxrpt.cfg

You can change the logging directory, activate or deactivate flow, SQL, error, and job call logging, and change the logging level for flow logging.

> A higher level for flow logging can lead to slower response times or increased system load. Error messages are always included in a flow log.

Specify the path using any notation. Relative paths are also possible.

The choice between **Internal logging** and **Text format** exclusively refers to the logging of enaio® capture. We recommend that you choose internal logging. Customers who want to continue working with the text format can stay with this format. enaio® capture always creates batch-specific logs, which can be opened from within the application.

Changes apply to all components in the directory for which no individual channel has been set up.

Set up channels using the **Channel settings** area, assign channels to components and activate assignments using the **Alias settings**.

The editor is exited by clicking the **Cancel** button or by pressing **ESC** – changes will not be saved, though. Click the **Apply** button to save the changes and then exit the editor.

Channels

A channel accepts messages with the same action ID from one or more components and can store the messages in the internal log format or in OXMISC format.

Logs in the internal log format (`*.evn`) can be opened with enaio® protocol-viewer; logs in the OXMISC format can be opened with any editor.

We recommend the internal log format, as logs in enaio® protocol-viewer can be displayed in a very structured way.

Internal Log

Channels in the internal log format have the following properties:

Property	Default value	Range of values
Action	15	15 = Flow 11=Memory 9=SQL 8 = Error 7 = Job call
Level	1	0 = Only error log 1 = Application initialization 2 = Function entry points 3 = Function exit points 4 = Significant function points 5 = Detailed log 6 = Debug log
Stopped	NO	NO/YES 'YES' turns off the channel.

Optional	YES	NO/YES The setting 'NO' prevents the component to start when the channel is not available.
Share	YES	NO/YES When set to 'YES', multiple components can use the same channel to send messages.
LogRecreation	YES	NO/YES When set to 'YES', a new log file will be created once the current log file exceeds the maximum size.
LogStartupTimeout	5000	A timeout for logging in milliseconds after the start of the component.
LogStopTimeout	5000	A timeout for logging in milliseconds after the component is exited.
LogFileName	os%6%7%5.evn	Specify a path and a name for the log files. A relative path leads to the application directory. The file and folder name can contain the following parameters: %2 the name of the executed component %3 the name of the computer %5 the two digit year %6 the day %7 the month The extension 'evn' is the file extension to add.
LogMaxFileSize	65536	The maximum size of a log file, the value in kilobytes must be between 1024 and 524288. 524288 kilobytes correspond to 512 MB.
LogSizeControlOn	0	0 – disabled, 1 – enabled. The size of the log directory can be monitored.
LogExpirationDays	3	Once the high water mark which defines the size of the log directory is exceeded during log creation, logs that are older than specified here will be deleted until either the low water mark is reached or no more log files exist.
LogHighWater	192	Maximum number of files in the directory
LogLowWater	96	Minimum number for files in the directory

OXMISC Log

Channels in OXMISC format have the following properties:

Property	Default value	Range of values
Action	15	15 = Flow 11=Memory 9=SQL 8 = Error 7 = Job call
Level	1	0 = Only error log 1 = Application initialization 2 = Function entry points 3 = Function exit points 4 = Significant function points 5 = Detailed log 6 = Debug log
Stopped	NO	NO/YES 'YES' turns off the channel.
Optional	YES	NO/YES The setting 'NO' prevents the component to start when the channel is not available.
Share	YES	NO/YES When set to 'YES', multiple components can use the same channel to send messages.
MiscLogPath	Standard path	The log directory indicated in the standard settings is always used.
MiscLogFormat	TDUXMJP	T = Time; D = Date; U = User; X = Station; M = Module; J = Job; P = Procedure
MiscLogType	0	0, is ignored.

OXMISC logs are always saved to the log path specified in the standard settings. They are given the following names:

Flow logs	`osddmmjj.flw`
SQL logs	`osddmmjj.sql`
Error logs	`osddmmjj.err`
Job call logs	`osddmmjj.log`

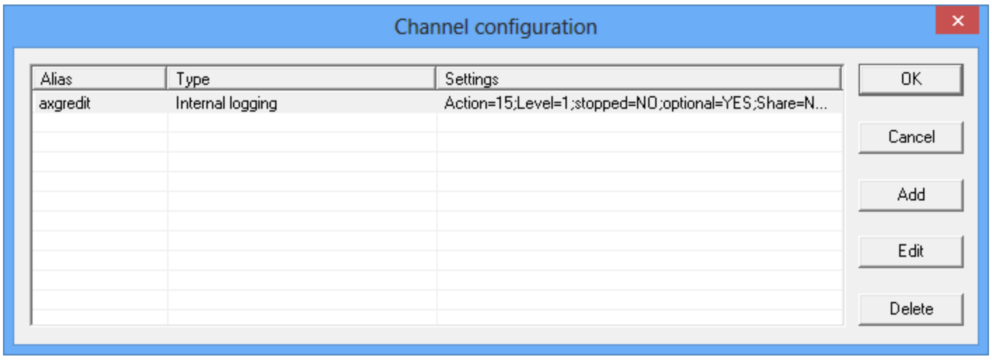
An example of an OXMISC log entry:

```
BEGIN
    TIME      : 12:55:50
```

```
     DATE      : 02/29/03
     USER      : THOMAS
     STATION   : 11D3-080009FEC5ED
     MODULE     : oxdbodbc
     JOB       : DisConnect
     STRING    : SQLFreeEnv(m_hEnv)
End
```

Setting Up Channels

The **Channel settings** area permits you to set up channels. Click the **Edit** button to open the **Channel configuration** dialog.

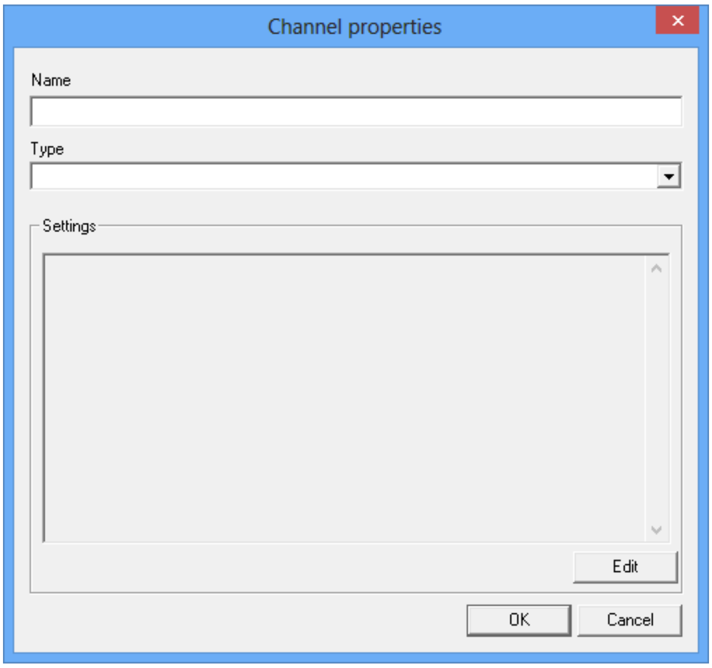


Alias	Type	Settings
axgredit	Internal logging	Action=15;Level=1;stopped=NO;optional=YES;Share=N...

It lists all already configured channels and allows you to edit and delete them.

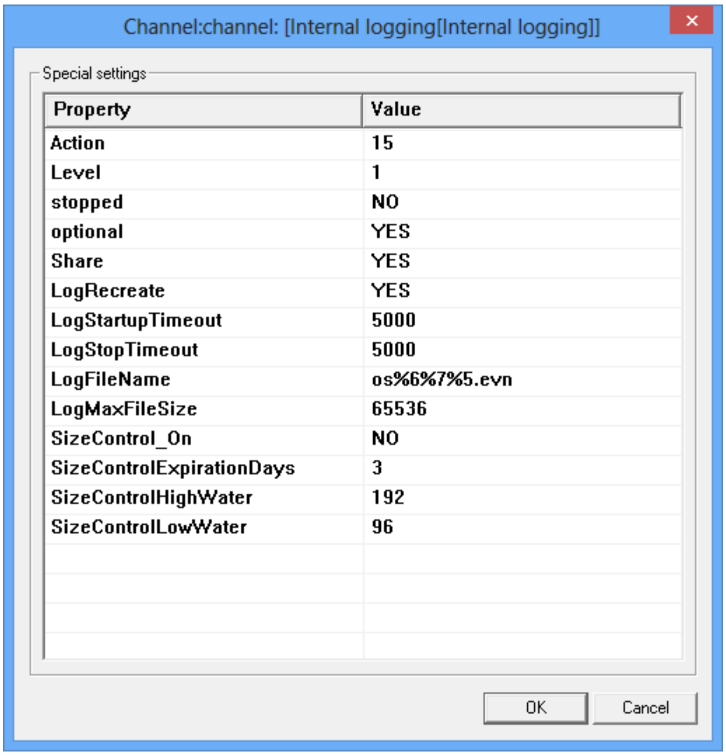
Use the **Add** button to set up a channel.

The **Channel properties** dialog will open.



Enter a channel name and select **Internal logging** or **Logging in OXMISC format** as the channel type. The default properties of the selected log type will be shown in the **Settings** area.

Click on **Edit** to change the properties:



Property	Value
Action	15
Level	1
stopped	NO
optional	YES
Share	YES
LogRecreate	YES
LogStartupTimeout	5000
LogStopTimeout	5000
LogFileName	os%6%7%5.evn
LogMaxFileSize	65536
SizeControl_On	NO
SizeControlExpirationDays	3
SizeControlHighWater	192
SizeControlLowWater	96

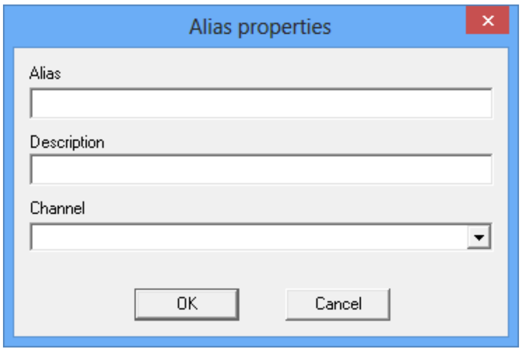
Confirm the changes by clicking the **OK** button in both the **Channel properties** and the **Channel configuration** dialog. As a result, the channel will be ready for assignment to components.

Components

The **Alias settings** area enables you to assign channels to components.

Existing channel assignments are listed in this area and can be edited or deleted. þ Selected assignments are active.

Open the **Alias properties** dialog using the **Add** button.

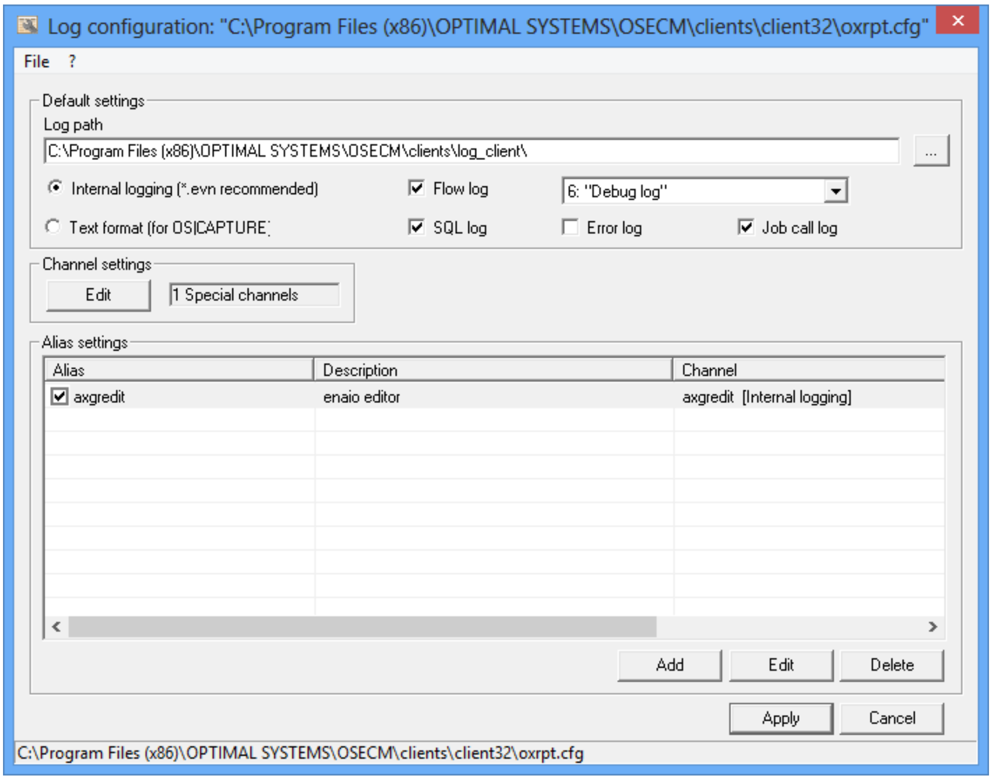


Enter the name of the component in the **Alias** field. To each executable file (*.exe) and each library (*.dll) you can assign a channel. Do not add the file extension when entering the name of the component into the **Alias** field.

Enter any text into the **Description** field.

Select the intended channel from the list of set up channels.

To assign the channel, click the **OK** button.



Log configuration: "C:\Program Files (x86)\OPTIMAL SYSTEMS\OSECM\clients\client32\oxrpt.cfg"

Default settings

Log path: C:\Program Files (x86)\OPTIMAL SYSTEMS\OSECM\clients\log_client\

● Internal logging (*.evn recommended) ☑ Flow log 6: "Debug log"

○ Text format (for OS|CAPTURE) ☑ SQL log ☐ Error log ☑ Job call log

Channel settings

Edit 1 Special channels

Alias settings

Alias	Description	Channel
☑ axgredit	enaio editor	axgredit [Internal logging]

C:\Program Files (x86)\OPTIMAL SYSTEMS\OSECM\clients\client32\oxrpt.cfg

> All assignments of configured channels are listed for each component, allowing you to only activate your own assignments.

Click the **Apply** button to save the configuration and to exit enaio® manager-for-logfiles.

Logging the System Load

A logging channel which records load data and writes them to a log file allows for the logging of the system load.

In enaio® enterprise-manager you can activate a preconfigured periodic job which is used to control this logging. This job periodically determines and logs load data.

Thus, system load can be monitored in great detail. This data which is periodically gathered follows this structure:

```
ProcessorTime=0.00%;
PageFaults=1.14/sec;
PoolPagedBytes=134952;
PoolNonpagedBytes=31272;
UserTime=0.000%;
PrivilegedTime=0.000%;
VirtualBytesPeek=499523584;
VirtualBytes=497057792;
WorkingSetPeek=212615168;
WorkingSet=212467712;
PageFileBytesPeek=311926784;
PageFileBytes=310927360;
PrivateBytes=310927360;
HandleCount=5741;
```

For new installations, this channel is automatically inserted into the log configuration file `oxrpt.cfg` in the server directory. In this case, you just need to activate the channel in enaio® enterprise-manager or edit the parameter **Suspended** in the configuration file.

The existing log configuration file will not be manipulated during system updates in order to prevent adjusted configurations from being overwritten.

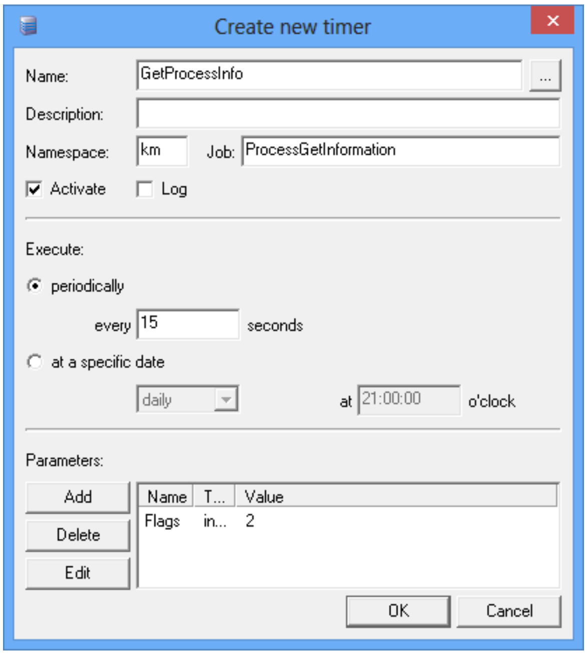
If you want to set up the channel, add the following entry to the log configuration file:

```
[oxrpt\channels\MEM-log]
LogFileName=mem%6%7%5.evn
Type=LOG
ChannelID=11
Level=3
Suspended=0
```

In addition, the log must be added to the list of standard logs:

```
[oxrpt\aliases\default]
1=Error-Protokoll
2=Flow-Protokoll
3=Log-Protokoll
4=SQL-Protokoll
5=MEM-Protokoll
```

What is more, you have to activate the periodic job 'GetProcessInfo' through enaio® enterprise-manager. A periodic execution interval of 15 seconds is preset by default. This setting allows for a quite detailed report on the system load but, if required, can be customized.



Create new timer

Name: GetProcessInfo

Description:

Namespace: km   Job: ProcessGetInformation

☑ Activate   ☐ Log

Execute:

● periodically

every 15 seconds

○ at a specific date

daily   at 21:00:00 o'clock

Parameters:

Name	T...	Value
Flags	in...	2

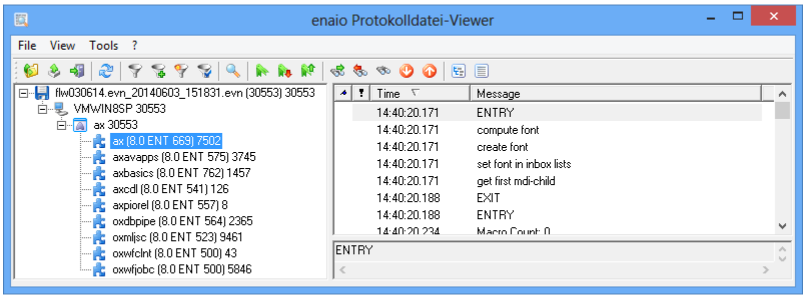
Active logging of the system load is quite resource-consuming. For that reason, it is recommended to activate the periodic job and channel only for a limited period to gain a system analysis.

enaio® protocol-viewer

Logs in the internal log format (*.evn) can be opened with enaio® protocol-viewer. You can find the `axrptview.exe` in every directory with components.

To open the logs, use the **File** menu or click the **Open file** button on the toolbar. Logs currently in use can be updated with the **View** menu, by pressing the **F5** key or the **Update** button on the toolbar.

enaio® protocol-viewer saves the settings (the most recently opened log, settings for the navigation and events area) in a configuration file and loads it on startup.



```
flw030614.evn_20140603_151831.evn (30553) 30553
  VMWIN8SP 30553
    ax 30553
      ax (8.0 ENT 669) 7502
      axavapps (8.0 ENT 575) 3745
      axbasics (8.0 ENT 762) 1457
      axcdl (8.0 ENT 541) 126
      axpiorel (8.0 ENT 557) 8
      oxdbpipe (8.0 ENT 564) 2365
      oxmljsc (8.0 ENT 523) 9461
      oxwfclnt (8.0 ENT 500) 43
      oxwfjobc (8.0 ENT 500) 5846
```

Time	Message
14:40:20.171	ENTRY
14:40:20.171	compute font
14:40:20.171	create font
14:40:20.171	set font in inbox lists
14:40:20.171	get first mdi-child
14:40:20.188	EXIT
14:40:20.188	ENTRY
14:40:20.234	Macro Count: 0

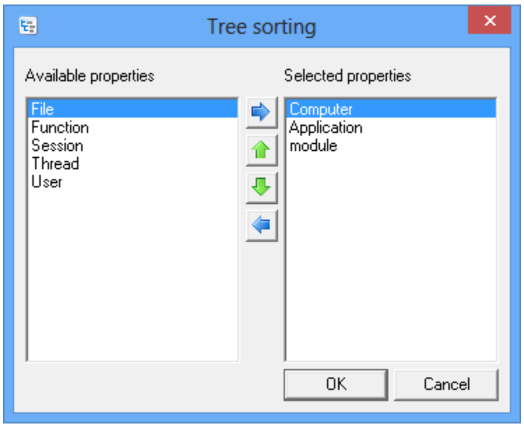
ENTRY

The viewer interface is divided into two areas: the navigation area on the left and the events area to the right.

Navigation pane

In the navigation area on the left, a navigation structure is shown, which you can set up using the **Tree sorting** button.

The **Tree sorting** button in the menu bar opens the **Tree sorting** dialog.



Available properties

- File
- Function
- Session
- Thread
- User

Selected properties

- Computer
- Application
- module

This dialog permits you to select the required level of the navigation structure and to specify the intended property sequence.

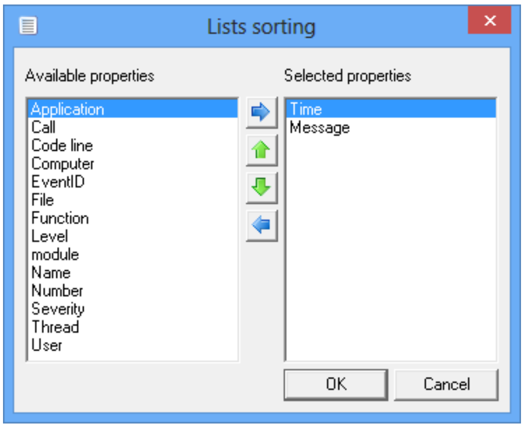
In addition to the entries in the navigation area, the number of assigned events is given. This information can be hidden by use of the **View** menu.

If you select an entry in the navigation area, you can export the assigned data. To do so, use the **File** menu to open the Export dialog and select the format and the file. If you choose the 'XML' format, only job calls are exported in XML form.

Events Area

In the events area on the right, you can find a list of the individual events belonging to the leaf level node currently selected in the navigation area. Beneath the list, the message related to the selected event is displayed.

- Click the **List sorting** button in the menu bar to specify the columns and their order.



Available properties

Application
Call
Code line
Computer
EventID
File
Function
Level
module
Name
Number
Severity
Thread
User

Selected properties

Time
Message

The list in the events area is sorted according to the selected columns and their defined order. In case the entries in the previous column are the same, the entries of the other columns in the event area can be sorted in ascending or descending order.

The columns **Bookmark** and **Event type** are automatically placed at the beginning, but cannot be used for sorting.

The event types are labeled as follows:

- Error
- Alert
- Information

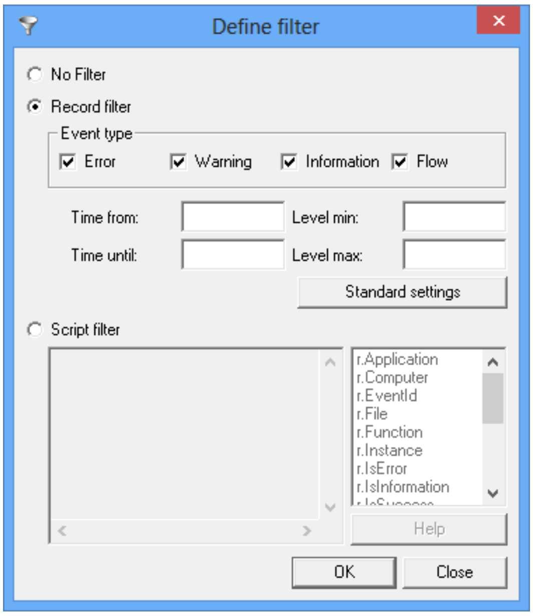
The toolbar provides filters which you can use to restrict the view to particular event types:

- Show errors, warnings and information.
- Show only errors
- Show all types.

You can restrict the list in the events area to particular event types, time frames and levels. In addition, you can search for event types.

Filter

- Use the **Define filter** button in the menu bar to set up filters.



Define filter

○ No Filter

● Record filter

Event type: ☑ Error ☑ Warning ☑ Information ☑ Flow

Time from: Level min:

Time until: Level max:

○ Script filter

r.Application
r.Computer
r.EventId
r.File
r.Function
r.Instance
r.IsError
r.IsInformation

Select one or more event types and specify an optional time frame (from/until) and a range of level (minimum/maximum).

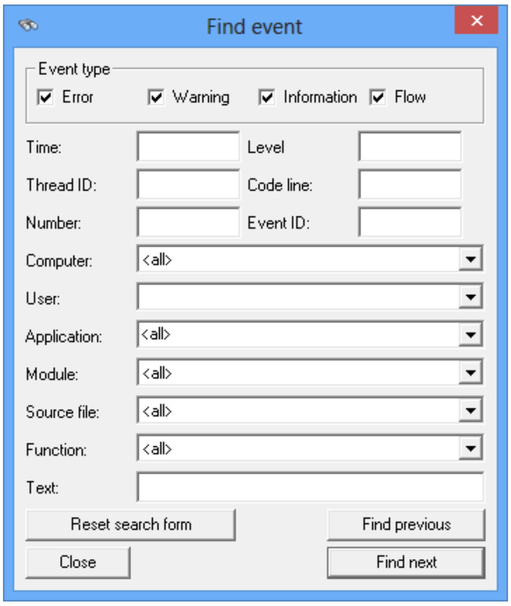
If you click **OK**, only the events that meet the criteria will be shown. In the navigation area, levels that contain no relevant data will be hidden. The number of events will be refreshed.

The filter criteria will be saved automatically.

You can also set up script filters. Click on the **Help** button to see further information.

Search

Use the **Find** button in the menu bar to specify search criteria.



Find event

Event type: ☑ Error ☑ Warning ☑ Information ☑ Flow

Time: Level

Thread ID: Code line:

Number: Event ID:

Computer: <all>

User:

Application: <all>

Module: <all>

Source file: <all>

Function: <all>

Text:

Select one or more event types and optionally enter additional properties as search criteria.

You can perform the search using the **Search backward / Search forward** buttons in the dialog or toolbar. All search criteria will be saved automatically once the dialog is closed.

Bookmarks

You can assign bookmarks to events in the event area. In total, there are 10 bookmarks available.

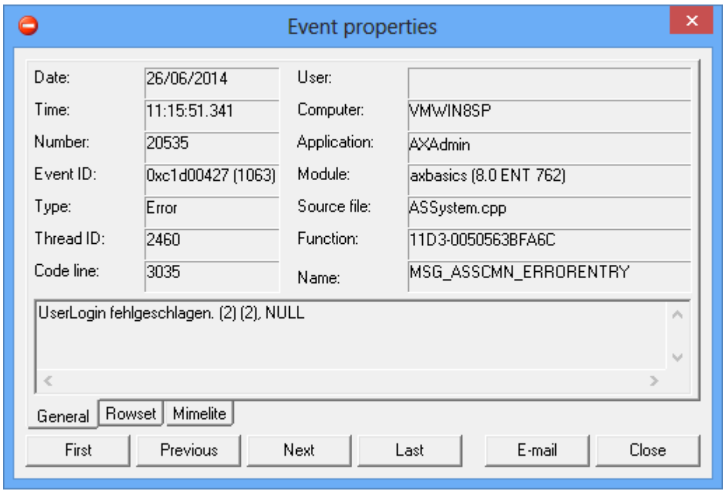
With the **Show/hide bookmarks** button you can either add a bookmark to a selected entry or delete the bookmark again.

You can go to the next or previous bookmark using the buttons on the toolbar; you can go to any bookmarks using the bookmark numbers in the **Tools > Go to bookmarks** menu.

Details

You can view the details (all properties) of each event.

Clicking the **Details** button will open the properties window of the selected event.



Event properties

Date:	26/06/2014	User:	
Time:	11:15:51.341	Computer:	VMWIN8SP
Number:	20535	Application:	AXAdmin
Event ID:	0xc1d00427 (1063)	Module:	axbasics (8.0 ENT 762)
Type:	Error	Source file:	ASSystem.cpp
Thread ID:	2460	Function:	11D3-0050563BFA6C
Code line:	3035	Name:	MSG_ASSCMN_ERRORENTRY

UserLogin fehlgeschlagen. (2) (2), NULL

Using buttons will enable you to switch between the detailed properties of the next or previous event or the first and last event.

You can use the **E-mail** button to transfer the data displayed to an e-mail form in your default e-mail application.

Encryption

Encryption of Document Files in enaio®

To secure the saving of document files on unsecured storage media and pass to unsecured networks, it is possible to encrypt documents.

The use of the Microsoft Crypto API, which is a component of the Windows operating system, and the encryption algorithm AES-256 ensures secure encryption of document files.

The 'RC2' encryption process was used up to Version 7.50. If document files are edited after this, they are encrypted with 'AES 256.' Document files can be subsequently encrypted with 'AES 256' using the 'Object encryption' action.

Both enaio® client and enaio® server provide the feature of document encryption. Define whether to use one or both enaio® components to encrypt document files since both use different symmetric keys which are part of the program code.

enaio® client encrypts all document files that are sent to enaio® server with the client key and decrypts all document files that are sent by the server. All document files are unencrypted before they are saved in the client cache.

Before saving them, enaio® server uses the server key to encrypt document files handed over by enaio® client. If a client requests a document, enaio® server decrypts the document file with the server key before passing it.

The automatic action 'Object Encryption' can be used to encrypt existing document files as well as decrypt documents.

Client Encryption

enaio® client uses the client key to encrypt all document files that have the property 'Encrypted filing' in their document type, before transferring them to enaio® server.

To enable encryption, the license key 'KRY' is additionally required at the workstation. If no license is available, enaio® client cannot decrypt document files and will not encrypt files before passing them to enaio® server.

Client encryption is administered using the **Encrypted filing** property in enaio® editor and licensing.

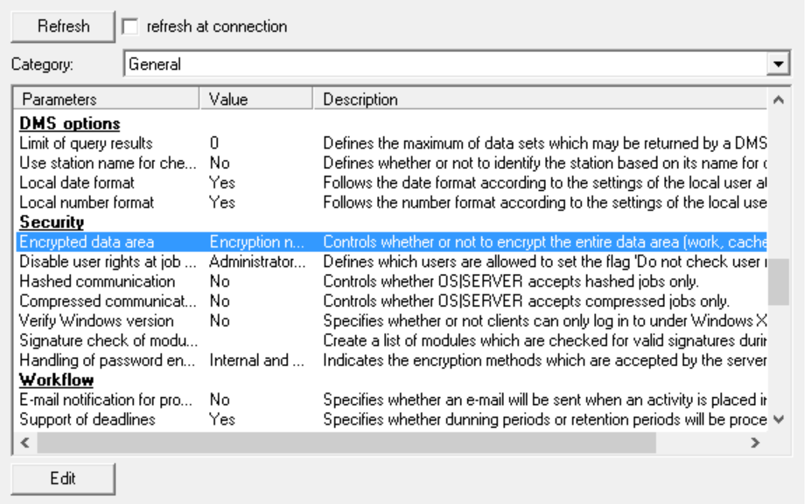
> Viewing document files encrypted by the client are shown only in enaio® documentviewer if the configuration is adjusted (see 'Content Preview of Client-Encrypted Documents').

Server Encryption

enaio® server encrypts all document files with the server key before saving them in the work area, regardless of whether they have the **Encrypted filing** property. Server encryption is independent of client encryption. Document files that have been encrypted by enaio® client will additionally be encrypted with the server key.

When document files are passed from enaio® server to enaio® client, the server at first decrypts them with the server key.

This encryption is defined in enaio® enterprise-manager via the **Server properties > Category: General** area.



Category: General

Parameters	Value	Description
DMS options		
Limit of query results	0	Defines the maximum of data sets which may be returned by a DMS
Use station name for che...	No	Defines whether or not to identify the station based on its name for (
Local date format	Yes	Follows the date format according to the settings of the local user al
Local number format	Yes	Follows the number format according to the settings of the local use
Security		
Encrypted data area	Encryption n...	Controls whether or not to encrypt the entire data area (work, cache
Disable user rights at job ...	Administrator...	Defines which users are allowed to set the flag 'Do not check user i
Hashed communication	No	Controls whether OS|SERVER accepts hashed jobs only.
Compressed communicat...	No	Controls whether OS|SERVER accepts compressed jobs only.
Verify Windows version	No	Specifies whether or not clients can only log in to under Windows X
Signature check of modu...		Create a list of modules which are checked for valid signatures durir
Handling of password en...	Internal and ...	Indicates the encryption methods which are accepted by the server
Workflow		
E-mail notification for pro...	No	Specifies whether an e-mail will be sent when an activity is placed ir
Support of deadlines	Yes	Specifies whether dunning periods or retention periods will be proce

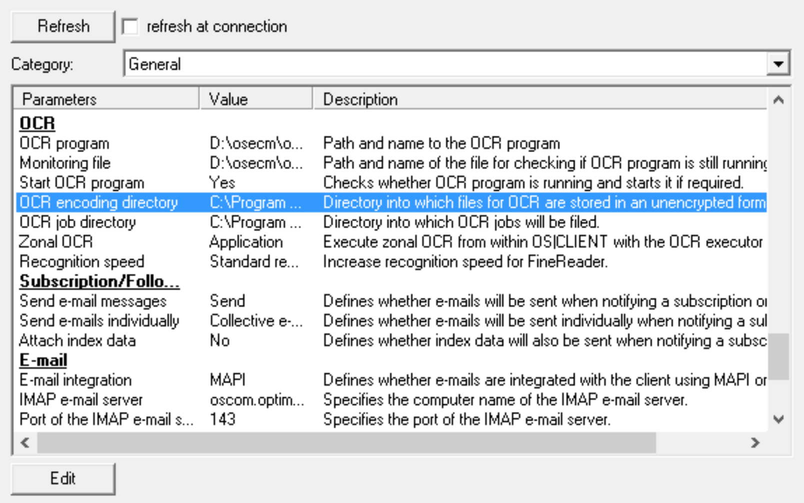
Double-click the parameter **Encrypted data area** to open a dialog which allows you to activate or deactivate encryption.

For server-side encryption the 'SKR' license key is required. If enaio® server was licensed with a test license, server encryption is not available.

enaio® server can create a full-text index for document files that have not been encrypted by enaio® client. Unencrypted files are then sent by enaio® server to the indexing component. After processing, the unencrypted file will be deleted immediately.

To index black and white as well as color images with the OCR component, you must enter a path that the unencrypted files are saved to. The path is specified as the value of the parameter **OCR decryption directory**.

> An OCR decryption directory must also be specified independently of an OCR for the 'Object encryption' action.



Category: General

Parameters	Value	Description
OCR		
OCR program	D:\osecm\o...	Path and name to the OCR program
Monitoring file	D:\osecm\o...	Path and name of the file for checking if OCR program is still runninç
Start OCR program	Yes	Checks whether OCR program is running and starts it if required.
OCR encoding directory	C:\Program ...	Directory into which files for OCR are stored in an unencrypted form
OCR job directory	C:\Program ...	Directory into which OCR jobs will be filed.
Zonal OCR	Application	Execute zonal OCR from within OS|CLIENT with the OCR executor
Recognition speed	Standard re...	Increase recognition speed for FineReader.
Subscription/Follo...		
Send e-mail messages	Send	Defines whether e-mails will be sent when notifying a subscription oı
Send e-mails individually	Collective e-...	Defines whether e-mails will be sent individually when notifying a sul
Attach index data	No	Defines whether index data will also be sent when notifying a subsc
E-mail		
E-mail integration	MAPI	Defines whether e-mails are integrated with the client using MAPI or
IMAP e-mail server	oscom.optim...	Specifies the computer name of the IMAP e-mail server.
Port of the IMAP e-mail s...	143	Specifies the port of the IMAP e-mail server.

For the subsequent encryption and decryption of document files, you can use the automatic action 'Object encryption.'

'Object Encryption' Action

The automatic action 'Object encryption' can be used to encrypt or decrypt documents of a particular type. The action uses the client key for encryption and decryption. If server encryption is activated, the server encrypts all documents determined by the action before saving them. If server encryption is deactivated, the server saves all called documents without server encryption.

To use this action, add the `axaccrypt.dll` library (see ''Additions').

When setting up the automatic action (see 'Setting Up Automatic Actions'), specify a configuration name and choose a query file in the configuration dialog.

The query file is used to specify which documents will be encrypted or decrypted with the client key.

The 'Encrypted filing' property of the document type is modified with enaio® editor to specify whether the documents are to be encrypted or decrypted, for the server encryption it is specified with the **Encrypted data area** property in enaio® enterprise-manager.

You can start the action manually or schedule a time for enaio® start to automatically start the action (see 'enaio® start').

With one configuration of the 'Object encryption' action, the documents of only one document type can be encrypted and decrypted. The action either requests all documents of the specified type or all documents that fulfill the logic expressions, regardless of whether they are encrypted.
An OCR decryption directory must also be specified for the 'Object encryption' action.

You can create the query file with any arbitrary text editor. It has the following structure:

`[ANFRAGE]` The file begins with the 'query' section.

`SCHRANK=cabinet name`

Enter the name of the cabinet that the documents originate from into the first line.

`DOKUMENT=document type name`

The document type of the documents comes in the second line.

```
KLAUSEL1=Objekt@Feld=Wert
...
KLAUSELn=Objekt@Feld=Wert
```

Optional logic expressions allow you to limit the selection to those documents that fulfill these conditions.

Logical expressions must be numbered consecutively.

Use internal names and enclose the name in percent signs.

> Also keep in mind that the **Maximum number of hits** setting in enaio® enterprise-manager limits the number of documents which can be processed. If more than 50000 documents are to be processed, this setting must be changed.

Logical Expressions

Optional logic expressions allow you to limit the selection to those documents that are indexed with the indicated value in the indicated field.

Example:

```
Klausel1=Kunde@Status=abgeschlossen
```

Documents of the indicated document type will be encrypted or decrypted accordingly only if the index data of the archive object type 'Customer', e.g. a folder, contain the value 'completed' in the field 'Status'.

Document integrity

Validating Document Integrity

As of Version 5.20, the hash value of the assigned document files will be automatically saved to each document.

To ensure document integrity, various functions which compare saved hash values to current hash values are at your disposal. This comparison may provide evidence of problems with storage media and additionally detect unauthorized access to files:

§ The automatic action 'Hash check' checks all document files in the WORK area of the connected server or on archive media.

§ The automatic action 'Hash check on object level' checks all those document files that are specified in a query file.

§ Hash values can be compared every time enaio® client requests a document.

§ Hash values can be compared before an audit-proof archiving process is started.

§ Users with the 'Open properties' system role for individual documents can run an integrity test of object information in enaio® client.

Moreover, the hash value can be signed by enaio® server. As a consequence it is ensured that unauthorized access to files cannot be concealed by tampering the hash values in the database.

The check results will be logged.

The user will be notified if a hash check, which is performed before enaio® client opens a document, has determined that the hash values differ. In such a case, only users with the system role 'DMS: Supervisor' are enabled to open such documents in read-only mode.

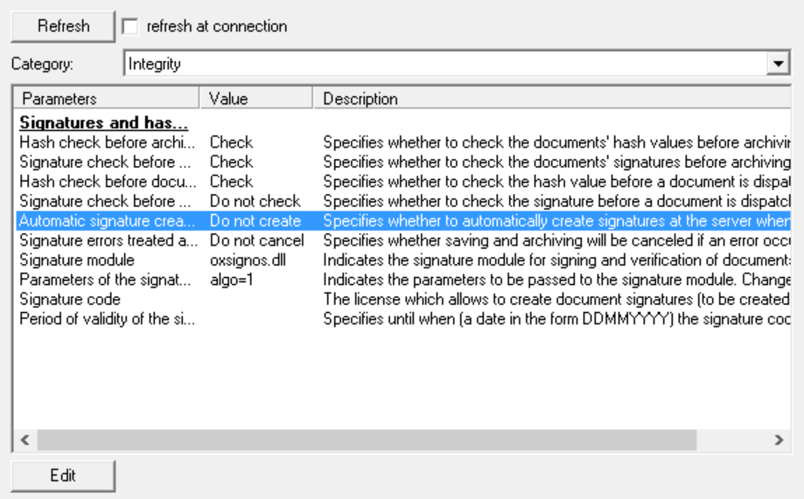
Documents will not be archived if a hash check, which is performed before archiving, has determined that the respective hash values differ.

Irrespective of the document integrity tests, hash values are determined before and after every document transfer, thereby excluding transmission errors.

Hash Value and Hash Value Signature

As of Version 5.20, the hash value will be automatically generated and saved in the database for every newly created or edited document with pages.

The feature which signs hash values is activated in enaio® enterprise-manager:



Category: Integrity

Parameters	Value	Description
Signatures and has...		
Hash check before archi...	Check	Specifies whether to check the documents' hash values before archivir
Signature check before ...	Check	Specifies whether to check the documents' signatures before archiving
Hash check before docu...	Check	Specifies whether to check the hash value before a document is dispat
Signature check before ...	Do not check	Specifies whether to check the signature before a document is dispatcl
Automatic signature crea...	Do not create	Specifies whether to automatically create signatures at the server wher
Signature errors treated a...	Do not cancel	Specifies whether saving and archiving will be canceled if an error occı
Signature module	oxsignos.dll	Indicates the signature module for signing and verification of document:
Parameters of the signat...	algo=1	Indicates the parameters to be passed to the signature module. Change
Signature code		The license which allows to create document signatures (to be created
Period of validity of the si...		Specifies until when (a date in the form DDMMYYYY) the signature coc

In the **Server Properties > Category: Integrity** area, enter the **Create** value to the **Automatic signature creation** parameter.

As a result, the hash values generated at archiving as well as at creation and modification of document files will be signed by enaio® server.

The parameters **Signature module** and **Signature module parameters** are set automatically. Change these entries only if explicitly instructed to do so by our consulting department.

The parameter **Signature errors treated as fatal** specifies whether or not to cancel the currently performed action in case of errors while signatures are checked or created.
Such errors are, for example, a failed communication with a signature module or a trust center and errors caused by expired certificates.
Do not cancel is preset.

Subsequent Creation of Hash Values

Hash checks can only be applied effectively if hash values exist of all document files. Hash values are also necessary in order to carry out checks for identical documents during document creation (see 'Checking for identical documents').

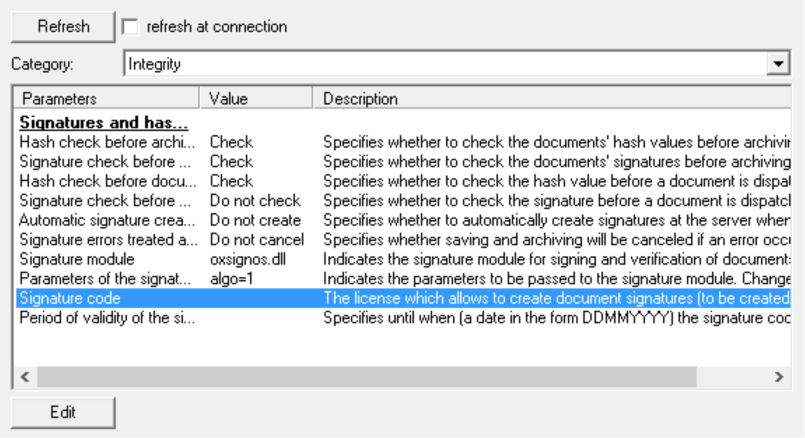
With the automatic action 'Sign' you can generate signed or unsigned hash values for document files that have been created with versions earlier than 5.20, and sign existing hash values.

Bear in mind that this action consumes significant time and resources if it is carried out on an extensive document inventory. This is why you must plan this action carefully. To test in advance the time required by the action, use a small number of representative documents. Also keep in mind that the **Maximum number of hits** setting in enaio® enterprise-manager limits the number of documents which can be processed. If more than 50000 documents are to be signed, this setting must be changed.

If you want to sign hash values, you will need a password and a signature code for this action. Both have a limited period of validity.

These data will be provided by our consulting department at your request. We require your current license file to create this data.

Before configuring the automatic action 'Sign', switch to enaio® enterprise-manager and enter the signature code and the period of validity:



□ refresh at connection

Category: Integrity

Parameters	Value	Description
Signatures and has...		
Hash check before archi...	Check	Specifies whether to check the documents' hash values before archivir
Signature check before ...	Check	Specifies whether to check the documents' signatures before archiving
Hash check before docu...	Check	Specifies whether to check the hash value before a document is dispal
Signature check before ...	Do not check	Specifies whether to check the signature before a document is dispatcl
Automatic signature crea...	Do not create	Specifies whether to automatically create signatures at the server wher
Signature errors treated a...	Do not cancel	Specifies whether saving and archiving will be canceled if an error occi
Signature module	oxsignos.dll	Indicates the signature module for signing and verification of document:
Parameters of the signat...	algo=1	Indicates the parameters to be passed to the signature module. Change
Signature code		The license which allows to create document signatures (to be created
Period of validity of the si...		Specifies until when (a date in the form DDMMYYYY) the signature coc

In the **Server Properties > Category: Integrity** you will find the parameters **Signature code** and **Period of validity**. Enter the appropriate values there.

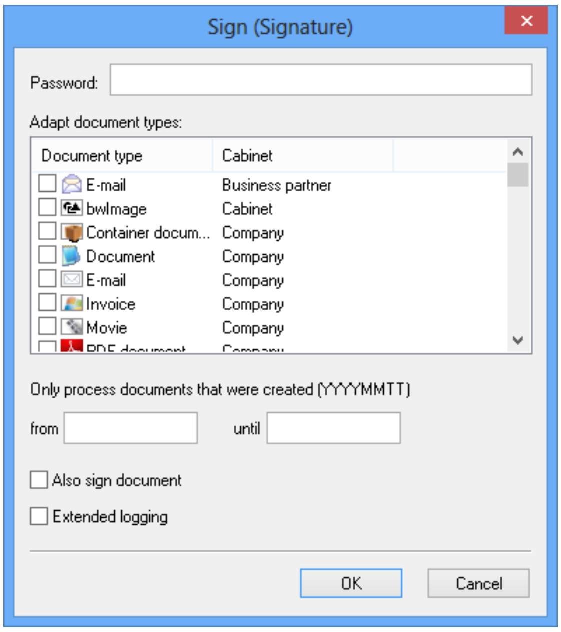
After the period of validity has expired, the 'Sign' action can no longer be carried out.

Add the automatic action 'Sign' `axacsign.dll`, in enaio® administrator using the **Entire system > Additions** tab (see ''Additions'). You can then create configurations for the actions and execute them using enaio® administrator or periodically using enaio® start (see 'Setting Up Automatic Actions').

Configuring the 'Sign' Action

Signature code and period of validity for the 'Sign' action are specified in enaio® enterprise-manager; the required password must be typed in a configuration dialog.

If you want only new hash values to be generated, no password and signature code is required.



Password:

Adapt document types:

Document type	Cabinet
□ E-mail	Business partner
□ bwImage	Cabinet
□ Container docum...	Company
□ Document	Company
□ E-mail	Company
□ Invoice	Company
□ Movie	Company
□ PDF document	Company

Only process documents that were created (YYYYMMTT)

from until

□ Also sign document

□ Extended logging

Hash values will be generated for all documents of the document types you have selected here. As an additional criterion, you can specify a timeframe of creation.

If you want to sign the hash values, select the option **Also sign documents**.

The action logs according to the settings in the configuration file `oxrpt.cfg` in the application directory. Additionally, a log file named `axacsign_date_time.xml` is created in the configured log directory. Therein, errors are logged. Activate the **Extended logging** option to have detailed information written to this file.

This action always creates new hash values, even if there are previously generated hash values. A comparison of these hash values does not take place. For security purposes, carry out a hash check when generating documents for which hash values already exist.

Automatic Actions 'Hash Check'

Two automatic actions for hash value and signature check are available:

§ the 'Hash check' action – `axachash.dll`

Select either archiving media or the WORK area for checking.

§ the 'Hash check at object level' action – `axachashd.dll`

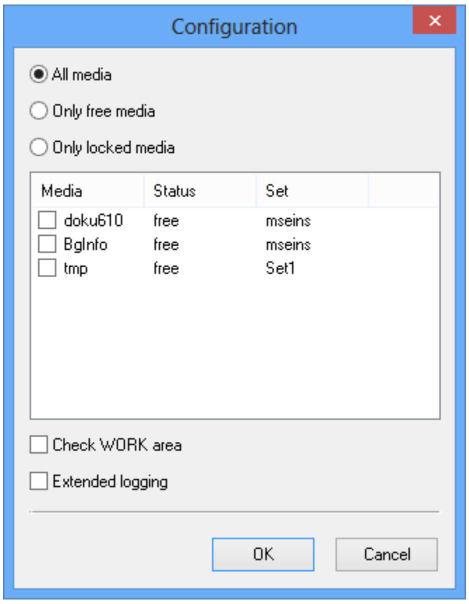
You must create a query file into which you can enter exact criteria for the hash check.

The automatic actions are integrated in enaio® administrator on the **Entire system > Additions** tab (see ''Additions'). You can then create configurations for the actions and execute them manually using enaio® administrator or periodically using enaio® start (see 'Setting Up Automatic Actions').

> Also keep in mind that the **Maximum number of hits** setting in enaio® enterprise-manager limits the number of documents which can be processed. If more than 50000 documents are to be checked, this setting must be changed.

Hash check

For the 'Hash check' action, specify the archive medium to be tested or the WORK area of the connected server. In the case of archive media, mirrored media for a main medium are also checked.



● All media

○ Only free media

○ Only locked media

Media	Status	Set
□ doku610	free	mseins
□ BgInfo	free	mseins
□ tmp	free	Set1

□ Check WORK area

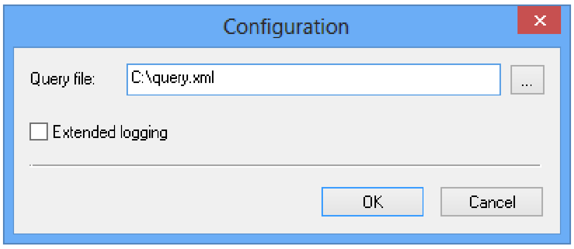
□ Extended logging

The action logs according to the settings in the configuration file `oxrpt.cfg` in the application directory. Additionally, a file named `axachash_date_time.xml` is created in the configured log directory. Therein, errors are logged. Activate the **Extended logging** option to have detailed information written to this file.

You can specify an e-mail address for a message to be sent to in the event of an error.

Hash check on object level

You must create a query file for the 'Hash check on object level' action. Specify this query file during configuration.



Query file: C:\query.xml

□ Extended logging

The action logs according to the settings in the configuration file `oxrpt.cfg` in the application directory. Additionally, a log file named `axachashd_date_time.xml` is created in the configured log directory. Therein, errors are logged. Activate the **Extended logging** option to have detailed information written to this file.

You can specify an e-mail address for a message to be sent to in the event of an error.

Query file

You can create the query file with any arbitrary text editor. It has the following structure:

`[ANFRAGE]`	The file begins with the 'query' section.
`SCHRANK=folder type name`	Enter the name of the folder type that the objects originate from into the first line.
`REGISTER=register name`	Optionally enter the name of the register that the objects come from.
`DOKUMENT=document type name`	Enter the document type that objects come from.

`KLAUSEL1=Objekt@Feld=Wert`
`...`
`KLAUSELn=Objekt@Feld=Wert`
	Optional logical expressions allow you to limit the selection to those objects that fulfill these conditions.
	Logical expressions must be numbered consecutively.

`Ausdruck1=Object@Field^Operator^Value`
`...`
`Ausdruckn=Object@Field^Operator^Value`
	Optional logic expressions allow you to limit the selection to those objects that correspond to these expressions.
	Logic expressions must be numbered consecutively.

If you use internal names, enclose the name between percent signs.

Clauses

Optional logic expressions allow you to limit the selection to those objects that are indexed with the indicated value in the indicated field.

Example:

```
Klausel1=Kunde@Status=abgeschlossen
```

Documents of the specified document type are checked using the document query only if the index data of the DMS object type 'Customer', e.g. a folder, contains the value 'completed' in the field 'Status'.

Expressions

Expressions allow you to limit the selection to objects by indicating technical parameters, e.g. basic parameters containing values.

Example:

```
Ausdruck1=Contract@1102^2^8
```

Only documents of the document type 'Contract' which do not contain value '8' in the field for the archiving status '1102' will be checked.

Documents without pages have archiving status '8'.

The 'Hash check at object level' action logs errors when checking documents without pages. Thus, using an expression to prevent checking of such documents is recommended.

Expressions offer extensive possibilities to specify the selection of objects. Information on expressions and logic expressions can be found in the 'OS_Client-Programming-Reference' handbook.

Continual Hash Check

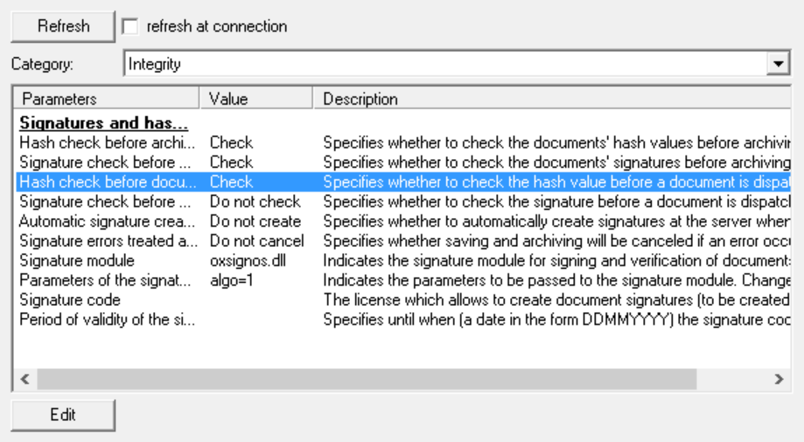
You may only turn on continual hash check if you have ensured that a hash value is present for every document file, whereas continual signature check additionally requires that all hash values have been signed and that automatic signing has been activated.

You can configure enaio® server to check the hash value every time a document is retrieved. If the newly-generated hash value fails to match the saved value, the user is notified in enaio® client and the document is not opened.

Only users with the system role 'DMS: Supervisor' are enabled to open such documents in read-only mode, provided that they are legible at all. The file can be saved externally, for example, but the document cannot be recovered.

You can determine whether hash values match or not, but if they do not match, you cannot determine the reason.

Continual hash check can be activated in enaio® enterprise-manager:



Category: Integrity

Parameters	Value	Description
Signatures and has...		
Hash check before archi...	Check	Specifies whether to check the documents' hash values before archivir
Signature check before ...	Check	Specifies whether to check the documents' signatures before archiving
Hash check before docu...	Check	Specifies whether to check the hash value before a document is dispat
Signature check before ...	Do not check	Specifies whether to check the signature before a document is dispatcl
Automatic signature crea...	Do not create	Specifies whether to automatically create signatures at the server wher
Signature errors treated a...	Do not cancel	Specifies whether saving and archiving will be canceled if an error occ
Signature module	oxsignos.dll	Indicates the signature module for signing and verification of document
Parameters of the signat...	algo=1	Indicates the parameters to be passed to the signature module. Change
Signature code		The license which allows to create document signatures (to be created
Period of validity of the si...		Specifies until when (a date in the form DDMMYYYY) the signature coc

In the **Server Properties > Category: Integrity** change the value of the parameter **Hash value check before document request** to **Check**.

If the hash values are signed, you can additionally activate the **Signature check before document request**.

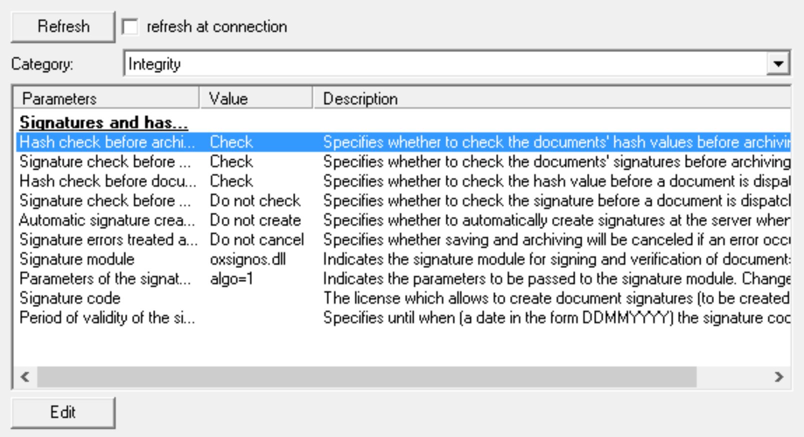
The parameter **Signature errors treated as fatal** specifies whether or not to cancel the currently performed action in case of errors while signatures are checked or created.
Such errors are, for example, a failed communication with a signature module or a trust center and errors caused by expired certificates.
Do not cancel is preset.

Hash value check before archiving

You may only turn on hash check before archiving if you have ensured that a hash value exists for every relevant document file, whereas continual signature check additionally requires all hash values to be signed.

enaio® server can execute a hash check before documents are archived. If the newly-generated hash value fails to match the saved value, the document will not be archived.

Hash check before archiving is activated in enaio® enterprise-manager:



Category: Integrity

Parameters	Value	Description
Signatures and has...		
Hash check before archi...	Check	Specifies whether to check the documents' hash values before archivi
Signature check before ...	Check	Specifies whether to check the documents' signatures before archiving
Hash check before docu...	Check	Specifies whether to check the hash value before a document is dispa
Signature check before ...	Do not check	Specifies whether to check the signature before a document is dispatc
Automatic signature crea...	Do not create	Specifies whether to automatically create signatures at the server whe
Signature errors treated a...	Do not cancel	Specifies whether saving and archiving will be canceled if an error occ
Signature module	oxsignos.dll	Indicates the signature module for signing and verification of document
Parameters of the signat...	algo=1	Indicates the parameters to be passed to the signature module. Change
Signature code		The license which allows to create document signatures (to be created
Period of validity of the si...		Specifies until when (a date in the form DDMMYYYY) the signature co

In the **Server Properties > Category: Integrity** change the value of the parameter **Hash value check before archiving** to **Check**.

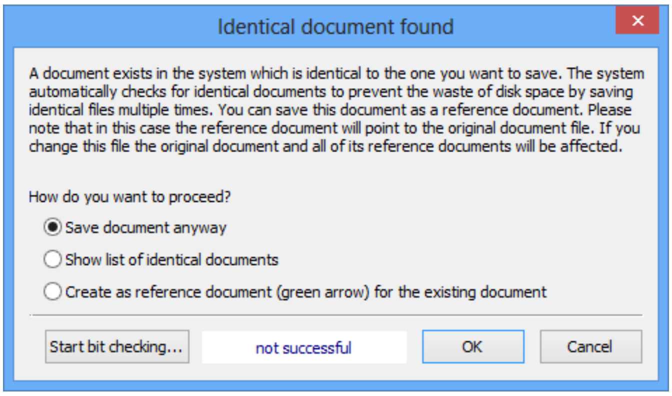
If the hash values are signed, you can additionally activate **Signature check before archiving**.

The parameter **Signature errors treated as fatal** specifies whether or not to cancel the currently performed action in case of errors while signatures are checked or created. Such errors are, for example, a failed communication with a signature module or a trust center and errors caused by expired certificates.
Do not cancel is preset.

Checking for identical documents

When creating documents, enaio® server can perform a check for identical documents.

The server checks whether any other document with the same hash value is stored. If so, enaio® client provides a respective notification.



Identical document found

A document exists in the system which is identical to the one you want to save. The system automatically checks for identical documents to prevent the waste of disk space by saving identical files multiple times. You can save this document as a reference document. Please note that in this case the reference document will point to the original document file. If you change this file the original document and all of its reference documents will be affected.

How do you want to proceed?

● Save document anyway

○ Show list of identical documents

○ Create as reference document (green arrow) for the existing document

The user can start a bit check to eliminate any doubts.

The user can choose to either file the current document, thereby merging the documents which are considered to be identical in a portfolio and open this portfolio, or to save the document as a reference document of the already existing document.

This check is activated by inserting the following entry into the `\etc\as.cfg` file of the data directory:

```
[SYSTEM]

CHECKFORIDENTDOCS=1
```

If more than one server is in use, this entry has to be added to the configuration file of each server.

Hash values must be saved for all documents (see 'Hash Value and Hash Value Signature').

Limitations

In some cases, it may be impossible to dependably determine whether an identical copy is present:

§ if client-side encryption for the document type is active,

§ if a handover involves document conversion, for example, when storing an image document which is converted into PDF format,

§ e-mail transfer.

SQL Queries

SQL Queries

SQL queries are queries that allow users to access data in the database by using enaio® client:

- regardless of the access rights defined for the archive objects and
- regardless of the system according to which the archive objects are organized.

You can, for example, query all registers where a specific document type is not yet present. You can query the number of pages scanned at a workstation within a certain time period in order to optimize the use of scanners. Access to precisely determined index data can be granted to users.

The results of a query can be passed to a VB script macro which is executed automatically or by the user.

The Consulting Team at OPTIMAL SYSTEMS will help you to set up SQL queries if you wish.

In the profile administration area, you can give users access to SQL queries or send them to users from the archive area. SQL queries are sent in an encrypted form.

> SQL queries can be used to modify and delete SQL statements and VB script data in the database. If you want to prevent this, change the write-permissions in enaio® enterprise-manager in the **Server properties > Category: Data > ADO database access**.

SQL queries can only be set up by users who have the system role 'Editor: Start' in the security system and the 'OSE' and 'OSM' module licenses installed at their workstation.

Users who have the 'OSE' module licensed at their workstation and who have the system role 'Client: execute SQL queries' can execute SQL queries. You can assign SQL queries to these users in the profile administration area.

The automatic action 'Execute SQL command' also allows you to execute SQL statements and to send the results as record sets to VB scripts. In contrast to SQL queries, this action can be used to modify data in the database (see 'Automatic Action 'Executing SQL Command').

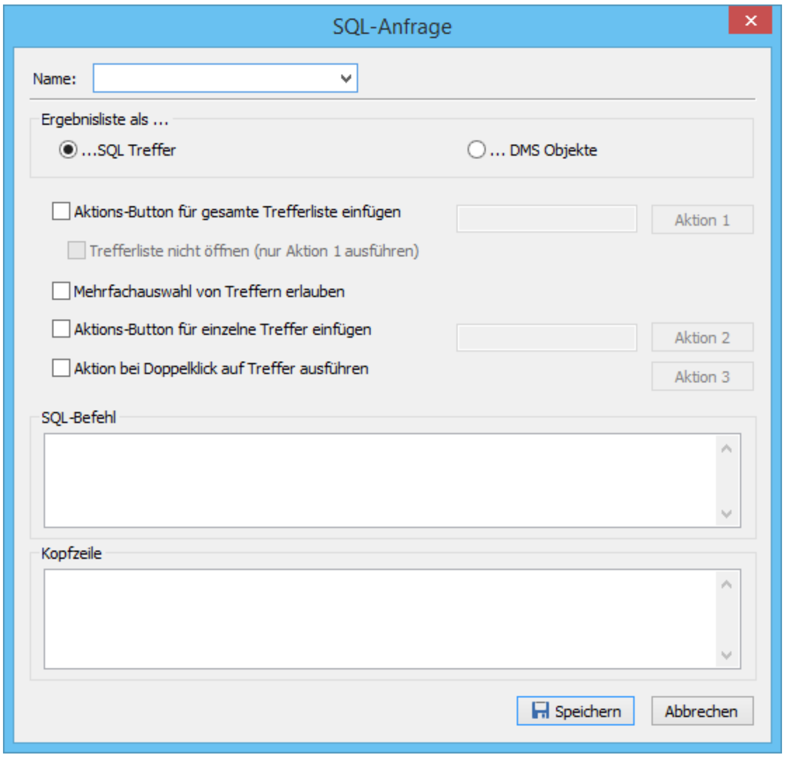
Setting up SQL Queries

SQL queries can only be set up by users who have the system role 'Editor: Start' and the 'OSE' and 'OSM' module licenses installed at their workstation.

enaio® client is used to set up extended queries.

In the **Object search** area, find the **Desktop** folder and the entry **SQL query** in the folder context menu.

Use this entry to open the **SQL query** window.



SQL-Anfrage

Name:

Ergebnisliste als ...

● ...SQL Treffer ○ ... DMS Objekte

□ Aktions-Button für gesamte Trefferliste einfügen

□ Trefferliste nicht öffnen (nur Aktion 1 ausführen)

□ Mehrfachauswahl von Treffern erlauben

□ Aktions-Button für einzelne Treffer einfügen

□ Aktion bei Doppelklick auf Treffer ausführen

SQL-Befehl

Kopfzeile

Enter a **Name** for the extended query.

You can choose whether the result of the query should be an SQL hit list or a list of DMS objects.

Result List as DMS Objects

Unlike the result list with SQL hits, a result list with DMS objects is a hit list that offers all standard functions for editing and organizing hits in enaio® client. Actions are not configured, nor are headers. The columns of the hit list depend on the settings for hit lists in enaio® client.

As an SQL command, only a statement in the format 'select id from object' is allowed. As with queries with result lists as SQL hits, the queries can contain variables, which are queried via a dialog. The variables can be set as defaults (cf. 'Variables').

Example:

The query determines all documents of a type, which are shared with a user who is specified via a preset variable with the user name.

```
select d.id from object28 d, osdoccollaboration c, user b where
d.id=c.doc_id and b.id=c.to_user and b.user like '$user,C30@#USER#$'
```

Result List as SQL Hit

Enter the SQL command in the **SQL command** area (see 'SQL Command').

In the **Header** area, you can optionally enter names to be used in the hit list instead of the database's internal names in the header of the table (see 'Header')

The checkboxes can be used to add VB scripts, which can be called up from the hit list (see 'VBScripts').

After clicking the **Save** button, the SQL query will be displayed with the given name in the **Desktop** folder.

SQL Command

SQL queries enable users to query data from the database by using SQL commands.

To do so, the SQL command must be inserted into the respective area of the **SQL query**.

Follow these rules:

§ The SQL command must begin with the SELECT clause.

Consequently, data cannot be deleted or modified.

§ Tables and columns must be referred to using their internal database names.

§ You can use variables.

The user is presented with a dialog to enter variable values to use for the query.

You can determine the table and column names by viewing the database area of enaio® editor.

In the title bar menu of a hit list in enaio® client, you will find the entry **SQL statement**. This entry opens a window with the SQL statement used to create the results list. This SQL statement also provides needed table and column names.

In expert mode, you can also view the SQL syntax of queries.

> Only users who can create SQL queries are allowed to access the SQL statements.

Variables

You can use variables within the SQL command. The user is presented with a dialog to assign values to the variables for the query.

The syntax of a variable looks as follows:

```
$Name,C30$
```

Variable declarations are surrounded by `$` signs. `Name` is the variable name you have chosen to use in the user dialog. A comma follows the name, and then a data type is specified.

The following types are available:

C String with '%' at the end, wildcards will be replaced

S	String, wildcards will be replaced
N	String without replacements
D	Date

An integer is added, specifying the length of the variable’s text field in the user dialog.

Subject to the data type and the database you are using, it may be necessary to parenthesize the variable with single quotes.

Variables may be preset. To this effect, the respective value must be previously inserted into the dialog. The user can either confirm or modify the value.

Syntax example of a variable with preset value:

```
$Name,C30@Hellmer$
```

The preset value is specified with a leading `@`. It is also possible to use the variable `#USER#` as the value for the current user or `#DATE#` for the current date. In addition, the variables `#COMPUTER-IP#`, `#COMPUTER-GUID#`, and `#COMPUTER-NAME#` are available.

If you do not want to preset a variable, do not use the '@' sign.

Conditions are created with '=' and '!='. Placeholders are not appended for execution. If the user leaves a string empty, an empty, thus not indexed, field will be searched for.

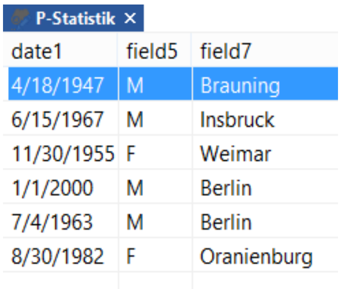
Example:

The SQL query creates a hit list with anonymized patient data for statistical evaluations. Instead of displaying all index data from the patient folder, only the content of three index data fields is shown: date of birth, gender and place of residence. The user can specify the gender with a preset variable. If the field is left empty, all patients will be listed.

```
select date1,field5,field7 from root6 where field5 LIKE
'$gender,C1$'
```

The internal database names of the table and the three required columns can be determined by viewing the properties in enaio® editor.

In enaio® client, a results list without gender restriction looks like this:



date1	field5	field7
4/18/1947	M	Brauning
6/15/1967	M	Insbruck
11/30/1955	F	Weimar
1/1/2000	M	Berlin
7/4/1963	M	Berlin
8/30/1982	F	Oranienburg

The header contains the internal database names of the columns if no alternative name has been entered in the **Header** area.

Header

The hit list of an extended query contains the internal database names of the columns in the header as column names. In the **SQL queries** window you can enter names for the columns in the **Header** area.

It is also possible to assign values for column formatting to the names.

The syntax is as follows:

```
name,value;
```

You can enter the following values:

-1 The column is as wide as the longest entry.

This is the default setting, which means that it can be ignored.

0 The column is not displayed.

VB scripts may require data that is to be queried but not displayed, for example, the ID of an archive object.

Width in pixel Enter a value for the width of the columns in pixels.

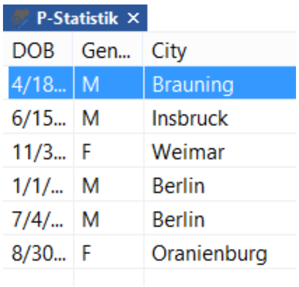
Example: `Place of residence,50;`

Example:

In the example above, three columns are requested. Names are assigned to these columns in the **Header** field.

```
DOB,50;Gender,50;City,-1;
```

In enaio® client the results list will appear as follows:



P-Statistik ✕

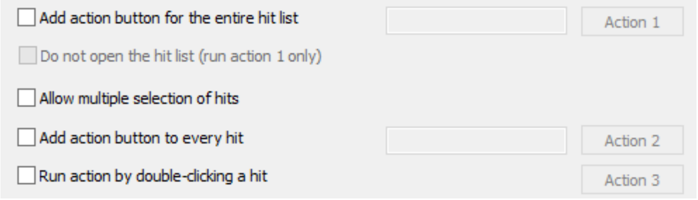
DOB	Gen...	City
4/18...	M	Brauning
6/15...	M	Insbruck
11/3...	F	Weimar
1/1/...	M	Berlin
7/4/...	M	Berlin
8/30...	F	Oranienburg

Instead of the internal database names, the header contains the entered names in the specified column format.

VBScripts

You can assign VB scripts to the data from the hit list of an extended query.

Select the required checkboxes in the **SQL query** window, click on the respective action button, and enter the VB script into the open script editor.



□ Add action button for the entire hit list

□ Do not open the hit list (run action 1 only)

□ Allow multiple selection of hits

□ Add action button to every hit

□ Run action by double-clicking a hit

Add action button for entire hit list

Activate this option if you want all data from the hit list to be sent to a VB script. Enter a name for the button in the following field through which the script will be executed. Click on the **Action 1** button to insert the VB script into the window.

Do not open hit list (run action1 only)

Activate this option to run the selected VB script instantly.

Allow multi-selection of hits

Activate this option if you want to send the data of all hits that were selected by the user to a VB script. The script of action 1 is assigned. It will be executed via the button named there.

Add action button for individual hits

Activate this option if all data of a selected hit to be handed over to a VB script. Enter a name for the button in the following field through which the script will be executed. Click on the **Action 2** button to insert the VB script into the window.

Run action by double-clicking a hit

Activate this option in order to send all data of a hit to a VB script by double-clicking the hit. Click on the **Action 3** button to insert the VB script into the window. If you do not enter any script there, the **Action 2** script will be run.

Examples:

The following script transfers all data from the hit list into an Excel table:

```
sub ExportToExcel()
dim excel                                             'Object variable for Excel
dim row, col                                          'Control variables

if recordset.recordcount = 0 then                     'Query whether the hit list is empty
   msgbox "Empty Recordset," vbCritical,"optimal_AS®"
else
  recordset.movefirst                                 'Cursor to the start of the record set
  set excel = CreateObject("excel.application")       'Create Excel object
  excel.workbooks.add                                 'Create new workbook
  for col = 0 to recordset.fields.count - 1           'Process all fields of the
```

	recordset
excel.activesheet.cells(1, col + 1').value = recordset.fields(col').Name	'and the field names in the first row
next	'next Field
excel.activesheet.cells(2,1').copyfromrecordset recordset	'Copy whole recordset from 2nd line
excel.visible = true	'Show Excel
set excel = nothing	'Make the object variable invalid
end If	
end sub	

```
ExportToExcel
```

To enable multiple selection, the variable `selrecords` provides the **Action 1** script with a list of comma separated indices for the selected entries in the record set. The transferred index for the first line of the hit list is '0.' If no hits are selected, `selrecords` is empty.

```
if recordset.recordcount > 0 then msgbox "Following entries were
selected: " & selrecords
```

The following script opens as **Action 2** or **Action 3** a single selected hit from the hit list via the 'ID.' Make sure that the cursor is at the respective position and must not be moved to the beginning by `recordset.movefirst`. The variable `selrecords` is not initialized before the **Action 2** or **Action 3** is run.

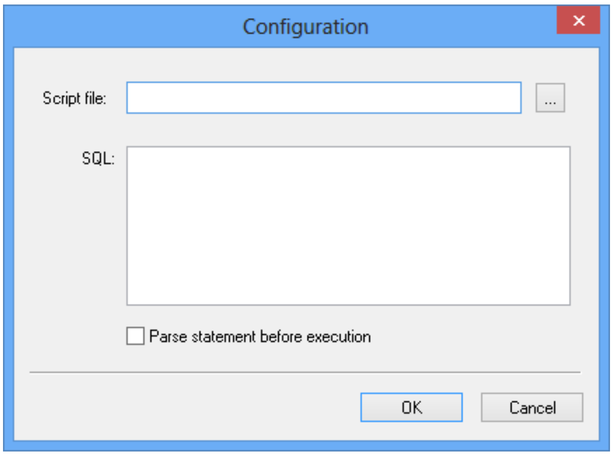
```
  set a = CreateObject( "optimal_AS.Application")

  objecttype = a.FindObjectType( RecordSet.Fields.Item("id"').Value)

  a.OpenObjectID RecordSet.Fields.Item("id"').Value, objecttype,0
```

Automatic Action 'Executing SQL Command'

The automatic action 'Execute SQL command' `axacolfr.dll` enables you to directly execute SQL commands and transfer the results to VB scripts in the form of recordsets.

Similar to the integration of other actions, use the **Additions** tab to add the automatic action 'Execute SQL command' and create a configuration.

In the configuration dialog you can specify an SQL statement and a script file.



You can then execute the action from either enaio® administrator or schedule it with enaio® start, in the same way as the other automatic actions.

enaio® mediamanagement

About enaio® mediamanagement

enaio® mediamanagement is an optional component of enaio® and incorporates media import, media export, and catalog printing.

Media Import enables importing image, audio and video files and applies contained metadata automatically at import. For this purpose the object type 'media content' can be used which contains fields for all common metadata of image, audio and video files.

With Media Export you can export image files and use configurations to define the format and resolution and make them available to all users.

Katalogdruck creates image files that are formatted for printing and also enables HTML output of pages. The output is formatted by use of XSL transformations. Configurations for catalog printing can be provided to all users.

enaio® mediamanagement data are part of the installation data and are installed with the 'mediamanagement' setup option. The components are integrated into enaio® client as an external application.

The following licenses are required:

- DPI for the media import

  One license must be permanently assigned to enaio® server as a seat license.
- DPE for Media Export
- DPK for Katalogdruck

The following system requirements must be met in order to install, configure, and use enaio® mediamanagement:

- Windows XP or higher
- .NET Framework 4.0 or higher
- Windows Media Player Version 11 or higher
- Installed feature: desktop display for Windows Server systems
- enaio® client with logged-in user account

enaio® mediamanagement-import

With enaio® mediamanagement-import, you import media files from a medium, e.g. a camera, or from a file system, into the enaio® system. The index data of the imported objects are automatically filled with the data from the media files.

enaio® mediamanagement-import supports the following file types:

Image	JPG, GIF, PNG, TIF, BMP, PSD, EPS, AI, CDR, PCT, TGA, PCX, WMF, SVG, CGM, DCM, PDF, ICO
Audio	WAV, MP3, WMA, MID, OGG, MOD, M4P, AAC, DTS, AC3, FLA
Video	AVI, MPG, WMV, MOV, MP4, RM, VOB, MPV, MKV, M2TS, TS, FLV, SWF, GIF

enaio® mediamanagement-import automatically detects connected devices. If enaio® mediamanagement-import is started and you connect a device, such as a digital camera, a notification appears in the notification area; click on the notification to start an import with the selected directory or device.

The user manual for enaio® mediamanagement-import can be found in the 'enaio® client' manual.

Installation and configuration

enaio® mediamanagement-import is automatically installed as part of enaio® mediamanagement by the setup if you select the 'mediamanagement' component from the setup options. The `axmediaimport.exe` application is then installed in the `client32` directory.

To configure enaio® mediamanagement-import, run the `axmediaimport.exe` application with the command line parameter '-config.' Once you have finished the configuration, the `axmedienimport.xml` configuration file is saved to the `etc` directory of the data directory. If users use enaio® mediamanagement-import, the application always accesses this global configuration file.

You need the 'Editor: Start' system role to configure enaio® mediamanagement-import. All users with this system role can then edit the enaio® mediamanagement-import. This always overwrites the existing configuration.

The program can only be started in the configuration or work mode, if enaio® client runs at the workstation.

Users who use enaio® mediamanagement-import require access rights to the object types and the 'DPI' license.

You can, for example, integrate enaio® mediamanagement-import into enaio® client as an external application for users (see the 'enaio® client' manual).

The 'Media Content' Object Type

On request, OPTIMAL SYSTEMS can provide you with the 'Media content' object type for use with enaio® mediamanagement. This already contains the established fields for the metadata of the individual media types.

How to adjust the object type according to your requirements and integrate it in the object definition can be found in the 'enaio® editor' handbook.

If you then select the 'Media content' object type for the configuration, enaio® mediamanagement-import recognizes it using the internal names and configures it automatically. The object type fields are automatically assigned to the corresponding import functions.

Import Functions

enaio® mediamanagement-import provides basic and dynamic functions for importing. The basic functions are the same for all media types. The dynamic functions always relate to a certain media type. The functions are assigned to object type fields. During an import, the data in the media files are read out by these functions and entered in the index data fields of the object types.

Basic functions:

- Current time
- Current user
- Current date
- Current format (image, audio or video)
- Modification date
- File size in byte/KB/MB
- File name with/without file extension
- Directory path
- Creation date:
- Fixed text
- Free text
- Complete file path with file name
- Only file extension
- Full user name

Dynamic functions for image files:

- Date taken (creation date)
- Alignment
- Authors
- Image format
- Bit depth
- Width in pixels/cm
- Latitude
- Copyright
- DPI horizontal/vertical
- Color mode
- Geo data
- Height in pixels/cm
- Camera maker/camera model
- Longitude

- Mime type
- Lens maker/lens model
- Aspect ratio

Dynamic functions for audio files:

- Sample size in Bits
- Sample rate in kHz
- Album
- Album artist
- Audio format
- Authors
- Bit rate
- Codec
- Copyright
- Genre
- Publisher
- Artists
- Year
- Channels
- Comments
- Composers
- Length
- Number
- Title

Dynamic functions for video files:

- Audio Bit rate
- Audio codec
- Authors
- Image width
- Images per second
- Image height
- Copyright
- Data rate
- Genre
- Total Bit rate
- Artists

- Year
- Length
- Aspect ratio
- Title
- Video codec
- Video format

Configure enaio® mediamanagement-import

You need the 'Editor: Start' system role to configure enaio® mediamanagement-import. All users with this system role can edit the configuration if they start enaio® mediamanagement in configuration mode. This always overwrites the existing configuration.

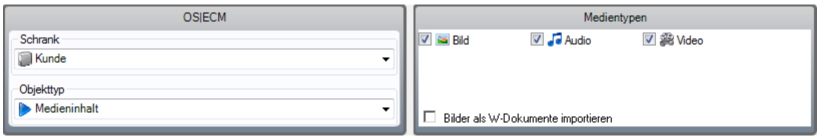
Once you have finished the configuration, the `axmedienimport.xml` configuration file is saved to the `etc` directory of the data directory. If users use enaio® mediamanagement-import, the application always accesses the configuration file in the global `etc` directory of the data directory.

Perform the following steps to configure enaio® mediamanagement-import:

1. Start enaio® client, because enaio® mediamanagement can only be started if enaio® client is running on the workstation.
2. Start enaio® mediamanagement, `axmediaimport.exe`, from the `client32` directory with the 'config' command line parameter.

   The enaio® mediamanagement wizard will open and guide you through the entire configuration.
3. In the **Object type – Assignments** dialog, select a cabinet and an object type from the selection lists in the **enaio®** area.

   The available media types which you can assign to the selected object types are shown in the **Media types** area. By default, all media types are selected.

   OS|ECM

   Schrank: Kunde

   Objekttyp: Medieninhalt

   Medientypen

   ☑ Bild ☑ Audio ☑ Video

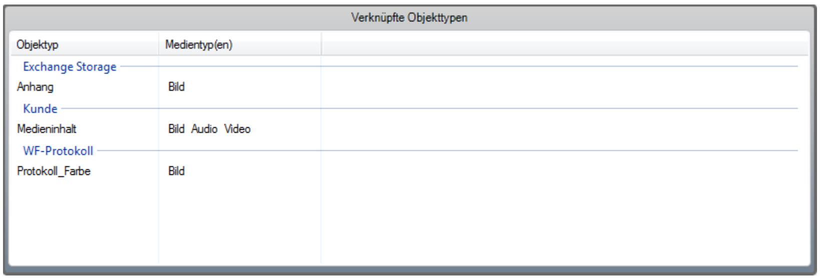
   □ Bilder als W-Dokumente importieren

   If you select the 'media content' object type, it will automatically be recognized on the basis of the internal names and automatically configured. The object type fields are then automatically assigned to the corresponding import functions.

   You can specify for every object type that images are imported as W-Documents so that these images can afterwards be edited in a Windows standard program. Enable the option **Import images as W-Documents**.

4. To create the assignment, click the **Link** button. You can assign every media type (image, audio and video) to only one object type per cabinet, however, you can assign more than one media type to an object type.

   In the **Assigned object types** area, all created links are listed for each cabinet.



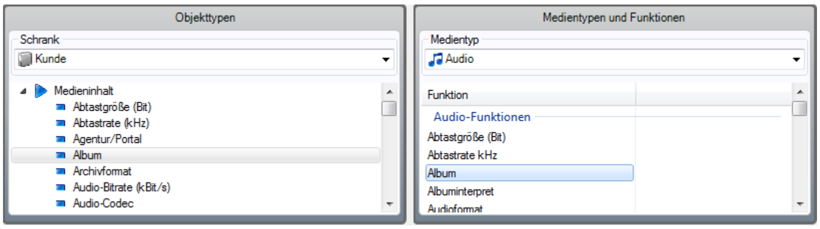
Verknüpfte Objekttypen

Objektyp	Medientyp(en)
Exchange Storage	
Anhang	Bild
Kunde	
Medieninhalt	Bild Audio Video
WF-Protokoll	
Protokoll_Farbe	Bild

The links cannot be subsequently edited. To change an assignment, you have to delete it and create it again. In order to delete an assignment, select it and click the **Remove assignment** button.

5. Click **Next**.
6. Then assign the desired import functions, free or fixed texts to the object type fields in the **Object type – function assignments** dialog. The functions read data from the media files and, during import, fill the index data fields with these media file data. Fixed texts are texts which are configured once, free texts are entered only when the user imports the files.

   There are two types of import functions that you can assign to the object types: basic functions and dynamic functions (see 'Import Functions'). Basic functions transfer data which do not refer to import files. With dynamic functions which depend on the selected media type, data are determined by the media files during import and are entered into the index data fields of the object type.



Objekttypen

Schrank: Kunde

- Medieninhalt
  - Abtastgröße (Bit)
  - Abtastrate (kHz)
  - Agentur/Portal
  - Album
  - Archivformat
  - Audio-Bitrate (kBit/s)
  - Audio-Codec

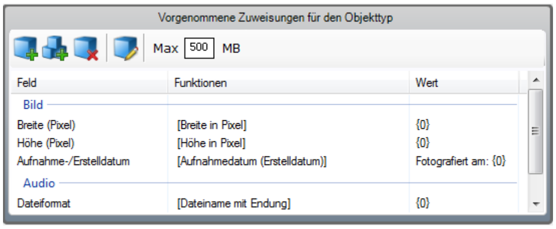
Medientypen und Funktionen

Medientyp: Audio

Funktion
Audio-Funktionen
Abtastgröße (Bit)
Abtastrate kHz
Album
Albuminterpret
Audioformat

7. Select the desired import function for every object type and click the **Assign function to the field** button. In order to assign several import functions to an object type field, press and hold CTRL or Shift when selecting the import function.

   All assignments for each cabinet and object type are listed in the **Assignments undertaken for the object type**.



Vorgenommene Zuweisungen für den Objekttyp

Max 500 MB

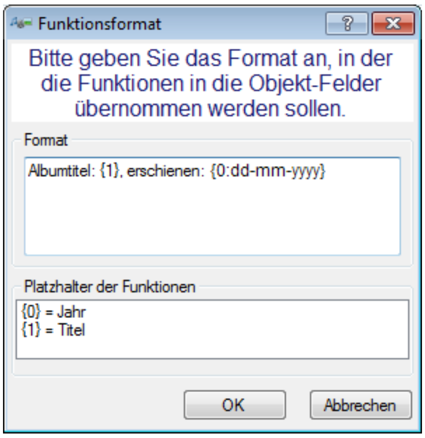
Feld	Funktionen	Wert
Bild		
Breite (Pixel)	[Breite in Pixel]	{0}
Höhe (Pixel)	[Höhe in Pixel]	{0}
Aufnahme-/Erstelldatum	[Aufnahmedatum (Erstelldatum)]	Fotografiert am: {0}
Audio		
Dateiformat	[Dateiname mit Endung]	{0}

You can also individually design the content of index data fields by creating an assignment with the **Assign formatted function to the field** button.

The **Function format** dialog is opened. In the **Format** dialog field, you can then enter any text which will additionally be written into the index data field. The maximum length and whether you can enter letters, numbers and/or special characters depends on the settings made for the corresponding object type field in enaio® editor. The placeholders, e.g. {0} and {1} specify where the text of the import value is entered. If the placeholder is used to insert a date, you can specify the date style. To do so, use the format specifiers: `y` (year), `M` (month), `d` (day), `h` (hour), `m` (minute), and `s` (second), e.g. {0:dd-MM-yyyy} for the date format '08-11-2010.'

Further format specifiers can be found on the following web page: http://www.csharp-examples.net/string-format-datetime/

The lower area of the dialog shows which placeholder is assigned to which import function. You must use all placeholders listed here in the **Format** area; otherwise you will get a message box.



Funktionsformat

Bitte geben Sie das Format an, in der die Funktionen in die Objekt-Felder übernommen werden sollen.

Format

Albumtitel: {1}, erschienen: {0:dd-mm-yyyy}

Platzhalter der Funktionen

{0} = Jahr
{1} = Titel

8. Confirm your entry with **OK**.

Media data are always imported with enaio® mediamanagement-import, regardless of whether key fields are unique, all mandatory fields are filled in, or catalog entries are included in the original catalog. Media data are not imported however, if a text is too long for a selected object type field.

Use the **Edit field functions** button to subsequently edit an assignment.

9. To delete an assignment, select it and click the **Remove assignment** button.

You can establish the maximum file size for each object type. Media files will not be imported if they are bigger than the specified file size. In the progress bar of the import and in the log you will see a message stating that the concerned files have not been imported due to their sizes.

10. Once you have created all the assignments, click **Next**.

All configuration settings will be summarized per cabinet in the next dialog. Click **Finish** to save the configuration.

As soon as the configuration is completed, the `axmedienimport.xml` configuration file is saved to the `etc` directory in the data directory.

To edit the existing configuration, restart enaio® mediamanagement in configuration mode and adjust the configuration as required.

enaio® mediamanagement-export

With enaio® mediamanagement, you export image files of the 'Media content' object type or any image file types. Configurations are created for the export in which the image format and resolution are specified.

The user manual for enaio® mediamanagement-export can be found in the 'enaio® client' manual.

Installation and configuration

enaio® mediamanagement-export is automatically installed as part of enaio® mediamanagement by the setup if you select the 'Media Management' component from the setup options. The `axmediamanagement.exe` application is then installed in the `client32` directory.

To configure enaio® mediamanagement-export, run the `axmediamanagement.exe` application with the command line parameter '-config.'

With this program you can configure the media export and catalog printing.

Configuration data are saved in the configuration file `axmediamanagement.xml`. Users having the system role 'Editor: Start' can save configurations as system-wide profiles. These profiles are saved in the `etc` directory of the data directory and can be accessed by any user. Every user can create configurations as local profiles. They are saved in the directory …`\etc\user\<username>` of the data directory.

Existing configuration files are overwritten.

The configuration file also contains the profiles for catalog printing.

Users who use enaio® mediamanagement-export require access rights to the object types and the 'DPE' license. The 'DPK' license is required for enaio® mediamanagement-catalog.

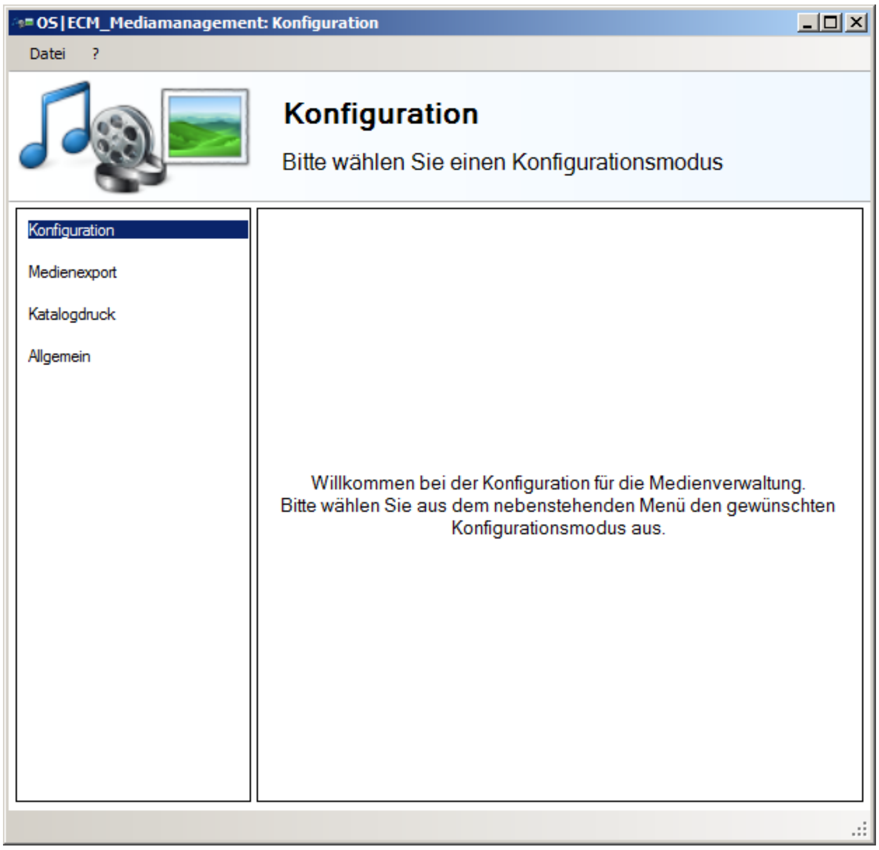
You can, for example, integrate enaio® mediamanagement-export into enaio® client as an external application for users (see the 'enaio® client' manual).

Configure enaio® mediamanagement-export

Only users having the system role 'Editor: Start' can create configurations for all users.

Perform the following steps to configure enaio® mediamanagement-export:

1. Start enaio® client.
2. Integrate `axmediamanagement.exe` from the `client32` directory as an external application with the `-config` parameter.
3. Start the external program.



OS|ECM_Mediamanagement: Konfiguration

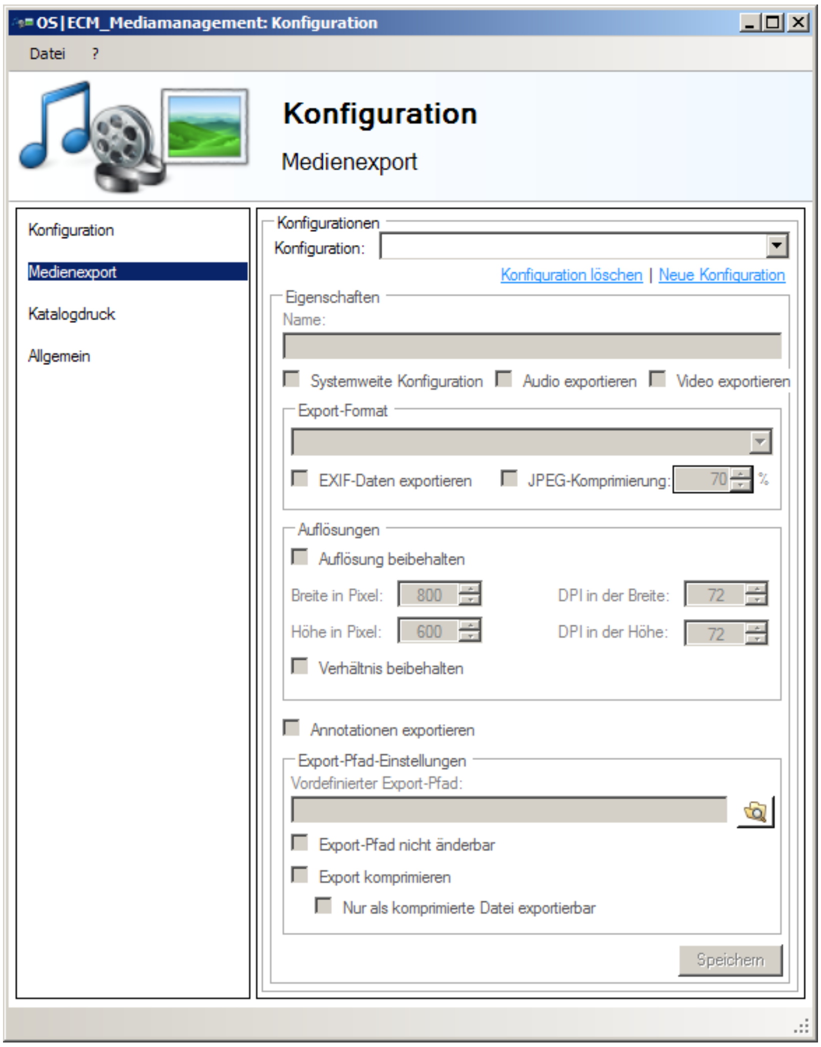
Konfiguration

Bitte wählen Sie einen Konfigurationsmodus

Willkommen bei der Konfiguration für die Medienverwaltung.
Bitte wählen Sie aus dem nebenstehenden Menü den gewünschten Konfigurationsmodus aus.

Export and catalog printing configurations are created with enaio® Media Management configuration.

4. Click **Media Export** in the navigation area.



JPEG-Komprimierung: 70 %

Breite in Pixel: 800

Höhe in Pixel: 600

DPI in der Breite: 72

DPI in der Höhe: 72

5. Click **New configuration** and enter the required properties.
6. Click **Save** to save the configuration.
7. Exit enaio® media management using the **File** menu, **Alt+F4**, or the close button.

Media Export Configuration Properties

Media export configurations have the following properties:

§ **Name**

Enter the name for a configuration. The name must be unique.

§ **System-wide configuration**

Users having the system role 'Editor: Start' can save configurations that can be applied to the entire system. These configurations are available to all users.

§ **Export audio / video**

Apart from image files, audio and video files can be exported as well. These are not changed during export.

§ **Export format**

Images can be converted to the formats 'PNG,' 'TIFF,' 'JPEG,' or 'GIF' or exported in the original format. If you select **Original**, the resolution cannot be modified; the images are exported in the way they are managed in enaio®. If you select **Edited**, the original format is retained, but the resolution can be changed.

For the 'JPEG' format, the compression can be specified.

- **Export EXIF data**

  Image files can be exported with or without contained EXIF data.

- **Resolution**

  You can maintain the resolution or enter other data.

  If you activate the **Maintain ratio** option, you only need to specify either the width or height and enter '1' as the other value.

- **Export annotations**

  Annotations on layers can be burnt into the exported file. If users don't have the right to edit annotations on the image files, they are burnt in by default.

- **Export path settings**

  The path for the export of all files is optional. If you specify a path, please consider the notation.

  A 'MediaExport' directory containing the export data is always created in the path. If this directory already exists, a counter is appended.

  If you activate **Export path not modifiable**, users cannot change the path. In this case, a path must be specified.

- **Compress export**

  If you activate this option, the export option **Export as compressed file** is preselected. All files can be saved in a ZIP archive.

  When **Only exportable as compressed file** is selected, the user cannot deactivate the export option **Export as compressed field**.

  Thus, the files are always saved in a ZIP archive.

Preinstalled Media Export Configurations

During installation, three system-wide configurations are created. System-wide configurations can be modified and deleted by users with the system role 'Editor: Start.'

With two configurations the 'JPEG' format is specified, the only difference is in the resolution. Path and compression are not predefined. The 'DTP/Print' configuration exports the image files in their original format.

- Internet

  250 pixels wide, 72 DPI

- Office tools

  1000 pixels wide, 150 DPI

§ DTP/Print

2000 pixels wide, 300 DPI

Edit Media Export Configurations

Every user can edit and delete own local configurations. System-wide configurations can only be modified and deleted by users having the system role 'Editor: Start'.

When enaio® Media Management is started, both the user's local configurations and the configurations for the entire system are loaded. System-wide profiles are identified by the additional text 'system-wide.'

The settings can be opened from the configuration list.

If you have modified the properties, click **Save** to save the configurations.

enaio® mediamanagement-catalog

With enaio® mediamanagement-catalog, image files of the 'Media content' object type or any other image file type can be printed in a structured manner or saved as an HTML page. The pages are formatted using an XSL transformation.

For catalog printing, configurations are created in which the number of files per page and further formatting options can be specified.

The user manual for enaio® mediamanagement-catalog can be found in the 'enaio® client' manual.

Installation and configuration

enaio® mediamanagement-catalog is automatically installed as part of enaio® mediamanagement by the setup if you select the 'Media Management' component from the setup options. The `axmediamanagement.exe` application is then installed in the `client32` directory.

To configure enaio® mediamanagement-catalog, run the `axmediamanagement.exe` application with the command line parameter '-config.'

With this program you can configure the catalog printing and media export.

Configuration data are saved in the configuration file `axmediamanagement.xml`. Users with the system role 'Editor: Start' can save system-wide configurations. These profiles are saved in the `etc` directory of the data directory and can be accessed by any user. Local configurations can be created by any user. They are saved in the directory …`\etc\user\<username>` of the data directory.

Existing configuration files are overwritten.

The configuration file also contains the configurations for media export.

Users who use enaio® mediamanagement-catalog require access rights to the object types and the 'DPK' license. The 'DPE' license is required for enaio® mediamanagement-export.

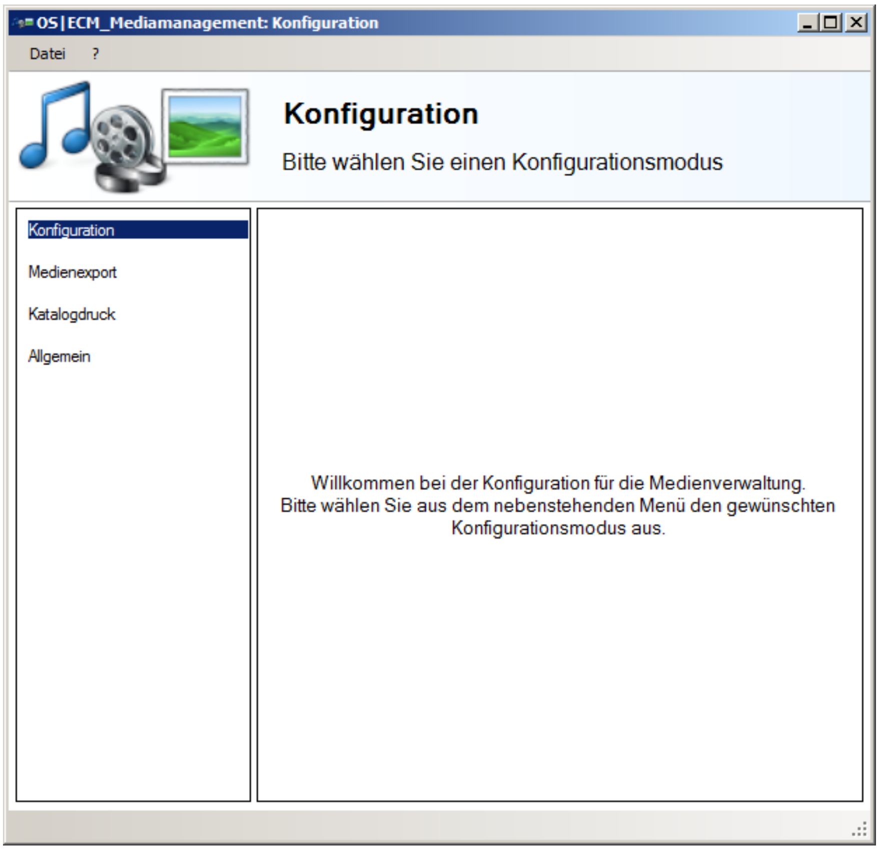
You can, for example, integrate enaio® mediamanagement-catalog into enaio® client as an external application for users (see the 'enaio® client' manual).

Configure enaio® mediamanagement-catalog

Only users having the system role 'Editor: Start' can create configurations for all users.

Perform the following steps to configure enaio® mediamanagement-catalog:

1. Start enaio® client.
2. Integrate `axmediamanagement.exe` from the `client32` directory as an external application with the `-config` parameter.
3. Start the external program.



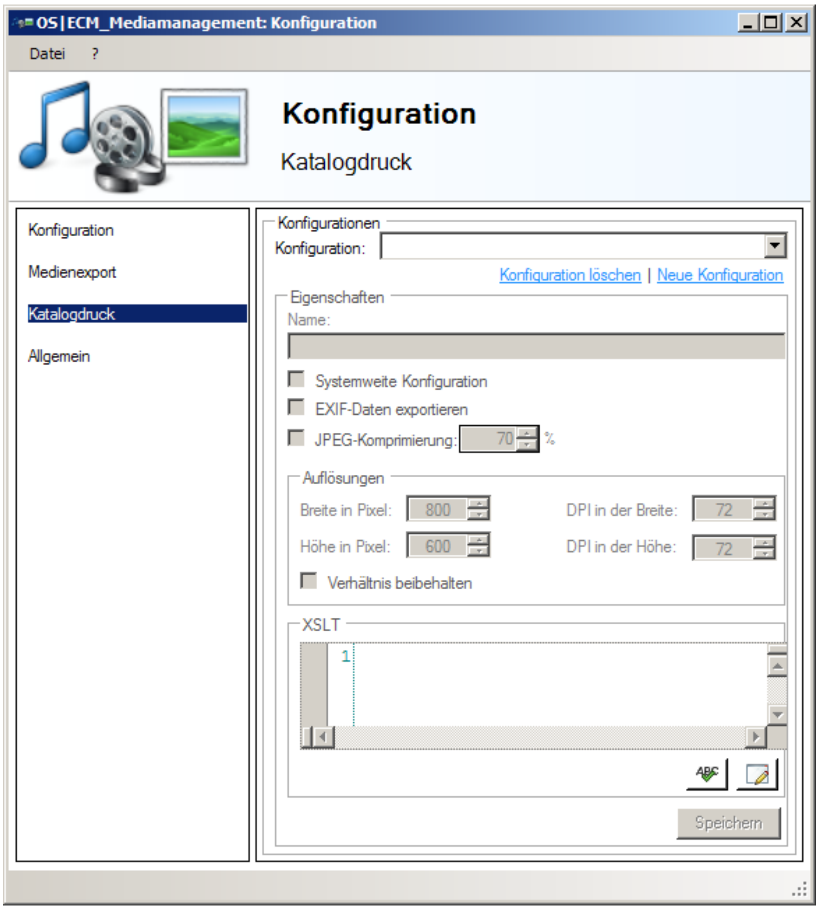
Konfiguration

Bitte wählen Sie einen Konfigurationsmodus

Willkommen bei der Konfiguration für die Medienverwaltung.
Bitte wählen Sie aus dem nebenstehenden Menü den gewünschten Konfigurationsmodus aus.

You can create catalog printing and export configurations with enaio® mediamanagement.

4. Click **Catalog printing** in the navigation area.



Konfiguration:

Name:

□ Systemweite Konfiguration

□ EXIF-Daten exportieren

□ JPEG-Komprimierung: 70 %

Breite in Pixel: 800

DPI in der Breite: 72

Höhe in Pixel: 600

DPI in der Höhe: 72

□ Verhältnis beibehalten

5. Click **New configuration** and enter the intended properties.
6. Click **Save** to save the configuration.
7. Exit enaio® mediamanagement using the **File menu**, **Alt+F4**, or the close button.

Katalogdruck Configuration Properties

Media export configurations have the following properties:

§ **Name**

Enter the name for a configuration. The name must be unique.

§ **System-wide configuration**

Users having the system role 'Editor: Start' can save configurations that can be applied to the entire system. These configurations are available to all users.

§ **Export EXIF data**

Image files can be exported with or without EXIF data.

§ **JPEG compression**

For catalog printing, image files are always created in the 'JPEG' format with the specified compression.

§ **Resolution**

You can maintain the resolution or enter other data.

If you activate the Maintain ratio option, you only need to specify either the width or height and enter '1' as the other value.

The specified width and height must match the XSLT formatting.

§ **XSLT**

Catalog printing contains four XSLT-based configurations. You can use them to create own configurations or customize the existing ones. The XSLT transformations are saved in the configuration file.

When customizing, in particular the resolution-print range ratio must be considered.

Preinstalled Media Export Configurations

During installation, four system-wide configurations are created. System-wide configurations can be modified and deleted by users with the system role 'Editor: Start.'

The only difference of the configurations is in the number of images that are output per page.

§ **2 images / page, index data**

Two pages are output on top of each other on one page.

§ **4 images / page, index data**

Four images are output on one page in two lines with two images each.

§ **16 images / page, index data**

16 images are output on one page in four lines with four images each.

§ **64 images / page, index data**

64 images are output on one page in eight lines with eight images each.

The entries in the XSLT area can be validated.

If you wish, the OPTIMAL SYSTEMS consulting team would be pleased to assist you in the XSLT creation.

Edit Katalogdruck Configurations

Every user can edit and delete own local configurations. System-wide configurations can only be modified and deleted by users having the system role 'Editor: Start'.

When enaio® Media Management is started, both the user's local configurations and the configurations for the entire system are loaded. System-wide configurations are identified by the additional 'system-wide' text.

The settings can be opened from the configuration list.

If you have modified the properties, click **Save** to save the configurations.

PDF administration

Integrating a PDF Conversion

The PDF file format is supported in numerous ways in enaio®; some functions require configuration of a PDF conversion.

- PDF can be selected as the output format when documents are exported by use of the automatic action 'Data/document export'.
- PDF conversion can be included into file import which is carried out by the automatic action 'Data/document import'.
- Documents can be converted to PDF for sending purposes to external recipients.

Image files are automatically converted into a PDF file. A PDF header is added to these files which can thus be viewed in a PDF viewer. Further configuration is not required.

Other file types must be opened with external applications which allow for saving files as PDF's. This process is controlled using a batch file.

> This solution was developed and tested to work with enaio® printer and Microsoft Office. Because there are differences between versions, all control possibilities for these and other applications must be tested individually.

Not only can you convert documents created with OpenOffice or LibreOffice, but also simply formatted Microsoft Office documents. To do this, you require the enaio® component enaio® documentviewer (see 'enaio® documentviewer'). This component provides extensive options for consistent conversion and OCR. If the appropriate configuration is used, the converted PDF documents comply with the PDF/A-1a standard.

enaio® documentviewer can be installed on a separate workstation. This will significantly ease the load on enaio® server.

Conversion of Microsoft Office Documents

Word, Excel and PowerPoint documents can be converted using the respective Office applications. The conversion is performed using a printer driver or a Microsoft add-in.

Printer Driver

The following printer drivers are used:

- the enaio® printer

enaio® printer creates image files to which a PDF header is added in order that they can be viewed in a PDF viewer. As a result, direct access to the text is not possible.

enaio® printer is installed on the workstation with the SETUP.

§ The printer driver 'Adobe PDF'

The Adobe PDF printer driver, which is subject to license, allows for the creation of PDF text files in which the text can still be accessed directly. This software's applicability must be tested for each individual case.

> In addition to the Adobe PDF printer, there are numerous PDF printer drivers available. However, the applicability of each printer driver must be tested for each individual case.

To enable conversion, you must create a batch file for each file type. Save these files to the `\server` directory. The name must correspond to the syntax `fileextension2pdf.bat`:

`doc2pdf.bat`	for Microsoft Word documents (.doc)
`docx2pdf.bat`	for Microsoft Word documents (.docx)
`xls2pdf.bat`	for Microsoft Excel documents (.xls)
`xlsx2pdf.bat`	for Microsoft Excel documents (.xlsx)
`ppt2pdf.bat`	for Microsoft PowerPoint documents (.ppt)
`pptx2pdf.bat`	for Microsoft PowerPoint documents (.pptx)

The batch files have the following content:

```
axprint2file.exe -in="%~1" -out="%~2" -app=application
-format=pdf -timeout="%~3" -printer="AS-printer"
```

Replace 'Anwendung' as follows:

`word`	for Microsoft Word
`Excel`	for Microsoft Excel
`Powerpoint`	for Microsoft PowerPoint

If you do not specify a printer driver, the system will first search for the 'Adobe PDF' printer driver and then for enaio® printer. If no driver is found, the user will be presented with an error message.

The registry provides the timeout parameter. To change the value, use enaio® enterprise-manager. You can also specify a value in milliseconds directly in the batch file.

> In order to prevent access conflicts, it may be useful to choose the **Print directly to the printer** option for enaio® printer under **Properties/Advanced**.

The 'Save as PDF' Add-In by Microsoft

The Microsoft add-in 'Save as PDF' for 2007 Microsoft Office adds the entry 'PDF' to the 'Save as' menu of Microsoft Office applications. This add-in is offered free of charge in the Microsoft Download Center.

You can use the add-in together with enaio® components for the conversion of documents into the formats 'doc', 'xls' and 'ppt'. Microsoft Word and PowerPoint documents are converted into the PDF/A format; whereas for Excel documents you must first activate the 'ISO 19005-1 compliant (PDF/A)' option to have them converted into PDF/A.

When installing enaio®, the application `office2pdfa.exe` will be copied to the `\server\` directory. Once a corresponding function in enaio® client is launched, the add-in enables the batch files `doc2pdf.bat, xls2pdf.bat`, and `ppt2pdf.bat` to start this application for conversion of these file types. `office2pdfa.exe` in turn starts Microsoft Office, which must be installed on enaio® server.

Please note the Microsoft license terms.

If Office 2007 formats are used, you must create the respective batch file. For example, to do so for the '.docx' format, copy and paste the `doc2pdf.bat` and rename it `docx2pdf.bat`.

In case you do not want to create PDF/A documents from Word or PowerPoint documents, the batch files can be supplemented with the `-nopdfa` parameter:

```
office2pdfa.exe %1;%2;-nopdfa
```

The `printhiddenslides` parameter is used to include hidden slides of PowerPoint presentations.

Concerning Excel documents, the entire workbook will always be printed.

If you have installed neither the add-in nor 2007 Microsoft Office, you must rename or remove these batch files.

Printing PDF Documents

Printing multiple W-Documents that are managed as PDFs at the same time may cause problems when using enaio® printer.

Documents may not be printed out in the correct order or may be incomplete.

If you are confronted with this problem, add the following line to the area [system] in the file `\etc\as.cfg` of the data directory: `PDFDDEPRINT=1`

Due to this entry, the OS_printer uses Adobe functions for printing.

Beforehand, the Adobe Reader or Adobe Acrobat must be installed at the workstation.

PDF/A

The following documents created by enaio® components conform to the 'PDF/A-1b' standard:

§ Image documents created with an image module.

Documents must not be edited. Once a page is added or deleted, the respective document no longer conforms to the 'PDF/A-1b' standard.

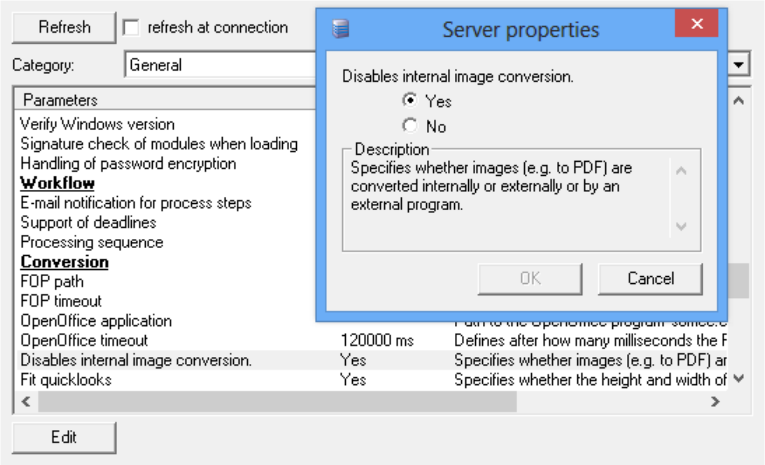
- PDF documents that are created by enaio® printer.
- Documents created with the enaio® office-utilities.

  If PDF printer drivers are installed at a workstation, enaio® office-utilities will offer them for selection under their corresponding names. Documents created this way may not conform to the 'PDF/A-1b' standard. For more information on this subject, contact the manufacturers of these printer drivers.
- Documents created with the 'Save as PDF' add-in by Microsoft for 2007 Microsoft Office, provided that the `-nopdfa` parameter has not been inserted into the batch file. For Excel documents, the user must activate the 'ISO 19005-1 compliant (PDF/A)' option.

> Check whether the converted PDF documents correspond to the 'PDF/A-1b' standard after installation.

If you use enaio® documentviewer for internal image conversion, the created PDF documents comply with the PDF/A-1a standard, provided the relevant configuration is used.

Use enaio® enterprise-manager to disable internal image conversion:



Server properties

Disables internal image conversion.
● Yes
○ No

Description
Specifies whether images (e.g. to PDF) are converted internally or externally or by an external program.

Parameters		
Verify Windows version		
Signature check of modules when loading		
Handling of password encryption		
Workflow		
E-mail notification for process steps		
Support of deadlines		
Processing sequence		
Conversion		
FOP path		
FOP timeout		
OpenOffice application		
OpenOffice timeout	120000 ms	Defines after how many milliseconds the F
Disables internal image conversion.	Yes	Specifies whether images (e.g. to PDF) ar
Fit quicklooks	Yes	Specifies whether the height and width of

Viewer Services

Introduction

Viewing services are core services of enaio® for the flexible display of documents, as well as document and index data. Other core services are the communication interface enaio® gateway, the REST interface enaio® appconnector, enaio® fulltext for full text indexing, enaio® service manager for collaboration with FineReader, and enaio® webservice for connecting external applications to enaio®. The core services are default components of enaio® and are required for operating the enaio® platform and the proper functioning of the individual enaio® components.

The following sections provide information about viewer services. The other core services are documented in the respective handbooks.

The viewing services can be integrated into enaio® webclient, enaio® dynamic-nav, enaio® mobile or external applications such as Microsoft Outlook.

Viewer services are:

§ enaio® documentviewer

§ enaio® detailsviewer

§ enaio® contentviewer

enaio® detailsviewer is implemented with enaio® appconnector, a REST interface that can be operated as enaio® detailsviewer when configured as described in the following sections. You can find more information about enaio® appconnector in the component handbook.

The core service enaio® gateway is important for operating the viewer services.

enaio® gateway

enaio® gateway is a proxy that is deployed as a communications interface between the core services.

enaio® gateway facilitates the display of content and the detail preview in enaio® client, the communication and authentication of core services, and the operation of enaio® webclient.

Installation

The following installation requirements must be met:

§ enaio® server is running and makes the IP port 80 available.

§ The core services and enaio® webclient if required have been installed.

enaio® gateway is automatically installed with the setup if you select the 'Gateway' component in the setup options.

In disparate environments, enaio® gateway must always be installed after all core services and enaio® webclient, so that enaio® gateway can read the URLs of the other core services from the server registry.

When installing enaio® gateway together with other core services on a computer, setup ensures that enaio® gateway is installed as the last core service.

The runtime environment (JDK and application server) is also automatically installed.

> The installed runtime environment should be used only for this core service, because when updating the core service the runtime environment is updated as well. If other enaio® or third-party components are run in the runtime environment, update errors may occur or the components may not be run after an update anymore.

Setup automatically registers the service on enaio® server with its URLs and service endpoints. You can view and modify these URLs in enaio® enterprise-manager under **Server properties > Category: Services > Gateway** (see 'Category: Services').

In multi-server systems, the core services should only be registered on a server; in other cases the URL end points of all core services should be unified manually.

Login takes place using the enaio® gateway and requires the following settings in enaio® enterprise-manager under **Settings -> Server properties -> General -> Login**:

§ User name for LoginPipe exceptions: *

§ IP addresses for LoginPipe exceptions: IP address of the Webclient installation

§ Alternative LoginPipe: IU

Configuration

enaio® gateway must be configured to set up the encrypted data transfer (HTTPS), the authentication method, or operation of enaio® webclient.

The authentication method of enaio® webclient is configured via enaio® gateway.

HTTPS

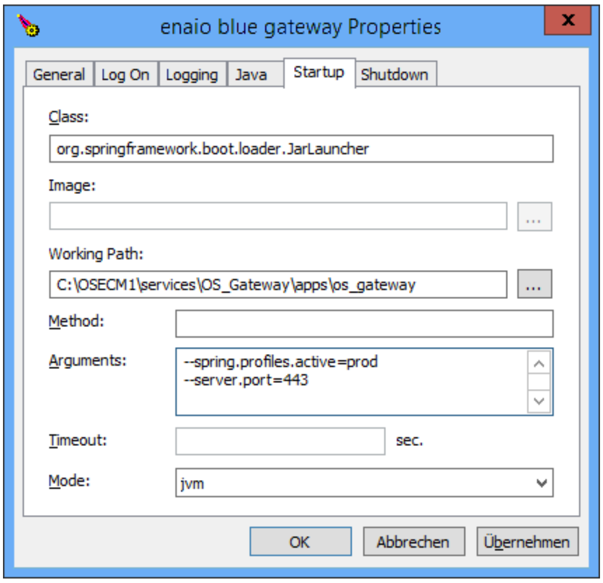
Set up the data transfer via HTTPS in the following way:

1. Create a key and a (self-signed) certificate in the keystore of the application server. You can find instructions under:

   `http://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html`

2. Set the standard port of the application server to the HTTPS standard port.

To do so, start the application manager `enaio blue gatewayw.exe` in the directory …`\services\OS_Gateway\bin` and set the `-server.port=443` on the **Startup** tab.



Class: org.springframework.boot.loader.JarLauncher

Image:

Working Path: C:\OSECM1\services\OS_Gateway\apps\os_gateway

Method:

Arguments:
--spring.profiles.active=prod
--server.port=443

Timeout: sec.

Mode: jvm

3. Enable data transfer by HTTPS in the configuration file `application-prod.yml`, which is located in the directory …`\services\OS_Gateway\apps\os_gateway\config`. It can be edited with any editor.
4. Add the following section to it:

```
https: {
enabled: true,
keyAlias: tomcat,
keystorePass: optimal,
keystoreFile: 'config/gw_keystore'
}
```

The parameters mean the following:

Parameters	Description
`enabled`	Enables data transfer by HTTPS.
`keyAlias:`	User name for the keystore
`keystorePass`	Password for the keystore user
`keystoreFile`	Directory which contains the keystore file.

Values with special characters require single quotation marks.

5. Save and close the file.

The data transfer by HTTPS is set up.

Authentication

It is possible to activate multiple login filters. If login fails with one filter, logging in with the next filter is tried. The following order applies:

§ Session GUID

- Simple
- Form-based
- NTLM
- Basic

  A login to enaio® webclient via a URL is only possible via the login filter 'Basic.' The parameter 'urlEncryption.urlAuthentication' and a CryptoProvider must also be enabled.

Aside from the 'simple' login filter, which should only be used for a purely technical application, all login fields are enabled by default.

Enable or disable the login filter in the configuration file `application-prod.yml`, which is in the directory …`\services\OS_Gateway\apps\os_gateway\config`. It can be edited with any editor.

> With NTLM as login filter, it is recommended to set up the technical user through login using the alternative LoginPipe. Depending on the login configuration, certain protective measures (tar pits) could otherwise delay or prevent the login of the technical user.

For NTLM authentication, the URL address to enaio® gateway must be recognized as a local intranet.

> For all clients that support NTLM, the following applies:
> If NTLM fails, Basic will not be executed, even if enabled.

Distributing Dashlets

A web application server or enaio® gateway can be used to distribute dashlets (see 'Dashlets in enaio® client').

To distribute with enaio® gateway, file the pages for dashlets in the directory …`\services\OS_Gateway\apps\os_gateway\public`. Make sure that you give the dashlets individual names so that no existing application with the same name is overwritten.

URL Encryption

Administratively, URLs can be provided for calling up core services and enaio® webclient. Sensitive data can be encrypted in URLs such as this.

> User name and password can only be encrypted in a URL if 'Basic' is enabled as a login filter.

So that enaio® gateway can process call ups with encrypted data sections, the configuration file `application-prod.yml` must be adapted.

The configuration file is in the following directory:

`\services\OS_Gateway\apps\os_gateway\config`

The file contains the following section:

```
urlEncryption.osCryptoProvider.enabled: false
urlEncryption.vigenereCryptoProvider.enabled: false
urlEncryption.vigenereCryptoProvider.key:
'~secret_~secret_~secret_~secret_'
urlEncryption.tokenPrefix: '(('
urlEncryption.tokenSuffix: '))'
urlEncryption.urlAuthentication: false
```

To enable, set the required values to 'true.'

- urlEncryption.urlAuthentication

  Enables encryption.

- urlEncryption.osCryptoProvider.enabled

  Encryption according to the Rijndael procedure. This procedure is also used in earlier versions of enaio®. A data section must contain more than 128 characters.

- urlEncryption.vigenereCryptoProvider.enabled

  Encryption according to the Vigenère procedure – not compatible with earlier versions of enaio®.

  A data section must contain more than 32 characters. The key must be specified (urlEncryption.vigenereCryptoProvider.key) and be precisely 32 characters long.

- urlEncryption.tokenPrefix/ urlEncryption.tokenSuffix

  Encrypted sections must be enclosed between a prefix and a suffix.

Data section can be encrypted by calling up the application `url-cipher-tool.jar` . It is located in the directory …`\components\` of the installation data.

The data section for encryption is transferred to the application via the following console call up. Example:

```
java -jar url-cipher-tool.jar -o -e -i data section
```

The encrypted data section is output through the console.

The Java Runtime Environment is needed for the operation.

Encrypted data sections must be enclosed in the URL according to the specified values for prefix and suffix.

Parameters for the `url-cipher-tool.jar` call

Parameters	Function
-d (--decrypt)	Mode for decryption
-e (--encrypt)	Mode for encryption
-o (--oscrypto)	Rijndael procedure with fixed key
-v (--vigenere)	Vigenère procedure
-k <arg> (--key<arg>)	Key to be applied (only with -v)

-i <arg> (--input <arg>)	Data section to be processed

Technical Users – Encrypted Passwords

If the passwords for the technical user in the configuration file `application-prod.yml` exceeds 20 characters, enaio® gateway automatically interprets this as an encrypted password.

The password can be specified in the configuration file as encrypted. It must be set in simple quotation marks.

The password can be encrypted via a call up of the application `url-cipher-tool.jar` (see above).

> The Rijndael procedure must be used as encryption.

CORS Access

Cross-Origin Resource Sharing (CORS) is a mechanism enabling cross origin requests for web browsers or other web clients. This kind of access is normally forbidden by the same origin policy. CORS is a compromise in favor of greater flexibility in the Internet while taking into account the highest possible security measures.

So that asynchronous JavaScript queries (Ajax) of a website, e.g. http://kunde.beispiel.de, can be successfully carried out on enaio® gateway with a different domain, e.g. http://<gateway_server>:80, the property `cors.enabled: true` must be added to the configuration file `application-prod-yml`. This will authorize all website hosts for CORS accesses.

The configuration file is in the following directory:

```
\services\OS_Gateway\apps\os_gateway\config
```

enaio® documentviewer

enaio® documentviewer integrates the preview of a selected enaio® document as a document preview in enaio® client. The content of a selected folder or register and the preview of a selected object can also be displayed in enaio® webclient. enaio® documentviewer offers simple functions for viewing, navigating, and searching.

Due to the integrated components enaio® renditionplus and Rendition Cache, enaio® documentviewer also enables the conversion of files into other file formats and text recognition in image files.

enaio® documentviewer consists of the following components:

- Web application

  With the Web application, displaying document previews in enaio® client is organized.

- Conversion component enaio® renditionplus enaio® renditionplus generates renditions from documents (images, PDFs, TIFF, text, thumbnails, etc.).

- Storage component Rendition Cache

  Rendition Cache is a cache for administering generated renditions centrally. Only one preview is generated per document. If one and the same document is sent multiple times or a reference document is created, enaio® documentviewer reuses the preview in the rendition cache.

When you send a document to an internal recipient, enaio® documentviewer allows you to include a reference to the preview file in the e-mail and activate the preview in enaio® webclient. In addition, a thumbnail of the first page of a document can be inserted into the e-mail body (see 'Documentviewer').

The user guide for enaio® documentviewer as a document preview can be found in the enaio® client handbook.

> enaio® documentviewer is installed with the login as a local system account, but must run on an account with administrative rights.

PDF preview

enaio® documentviewer can be converted to display previews in PDF format.

The PDF preview can be enabled via enaio® enterprise-manager.

To do so, enter the following home URL for enaio® documentviewer:

```
http://<gateway-IP address>
/dashlets/pdfview/viewer.html?osid={OBJECTIDENT}
&pagecount={pagecount}&sessionguid={sessionguid}
&servername={servername}&serverport={serverport}
&objecttype={objecttype}&q={searchterm}
```

The IP address of enaio® gateway is entered.

Installation Requirements

For better load balancing, it is recommended that enaio® documentviewer is operated separately from the enaio® server computer.

enaio® server must be installed and started, and provide an IP port.

enaio® gateway must be installed. The installation of enaio® gateway must be carried out after the installation of enaio® documentviewer.

The installation requires .Net Framework, which is installed through the enaio® setup, if it is not already on the computer.

Rapid distribution of data is only guaranteed if the computer on which enaio® documentviewer runs has fast I/O communication (hard disk, memory, etc.)

High-quality display of Office documents with enaio® documentviewer is only guaranteed if Microsoft Office 2010 (32 bit) is installed on the computer with enaio® renditionplus. When Microsoft Office 2010 is run for the first time, a dialog for setting automatic updates is displayed. Before installing enaio® documentviewer, you must start Microsoft Office once and set the update options. Otherwise the dialog when attempting to generate the previews will open and ultimately prevent generation.

In principle, enaio® documentviewer can also be used without Microsoft Office 2010. However, the quality of the Office documents displayed is lower.

Ghostscript Version 8.6 or higher (32 bit) must be installed to generate TIFF files from the PDF format. Due to license requirements, Ghostscript has to be installed separately.

Users can view previews only if they have the appropriate access rights. When calling up the document previews, an entry is created in the history both for the technical user and, for example, the user logged in to the enaio® client.

> Note that access rights are not automatically assigned to new document types and, if required, you must grant read rights for the technical user subsequently (see 'Introduction to the Security System').

It is recommended to publish the home URL and the URL for thumbnails under `intranet.kundendomain.de` in enaio® enterprise-manager in order to ensure long-time stability of the address and facilitate future server migrations of the viewing service.

Preview Generation

These options are available to generate document previews:

- On request: As soon as a user clicks on the desired document, the preview, if not automatically created already, is created and shown in the document preview.
- At creation: Previews will be generated automatically when a document is created.

This function can be specified for any object type in enaio® editor using the property 'Create preview automatically.'

The preview generation on request takes the most time.

Installation

enaio® documentviewer is an enaio® component that you install as a service with the enaio® setup.

Copy the enaio® installation data on the computer on which enaio® document viewer is to be installed, as running the enaio® setup from a network can lead to errors.

The runtime environment (JDK and application server) and the conversion components enaio® renditionplus and Rendition Cache are also automatically installed.

The installed runtime environment should be used only for this core service, because when updating the core service the runtime environment is updated as well. If other enaio® or third-party components are run in the runtime environment, update errors may occur or the components may not be run after an update anymore.

Setup automatically registers the service with the respective home URL and service endpoint on the enaio® server. You can view and modify these URLs in enaio® enterprise-manager under **Server properties > Category: Services > Documentviewer** (see 'Category: Services'). The registry keys are transferred to the client registry file during enaio® client installation and can be read by other components.

Changes to service endpoints are not automatically transferred to the client registry file. To synchronize the client registry file with the values of the server registry file, perform an update of the client installation either with the enaio® setup, or synchronize both registry files with the tool `OS.UpdateLocalServiceRegistry.vbs` from the directory `…\clients\client32\samples`. In systems with multiple servers the registry entries are transferred by the server with the highest probability of connection, or, if the probability of connection is less than 50% for all servers, they are transferred by the server in the last line of the `[SERVERS]` section in the `asinit.cfg` file of the client.

If several servers are in use and all need to access one enaio® documentviewer installation, you will need to manually adjust the URL addresses for all servers in enaio® enterprise-manager after the installation (see 'Documentviewer').

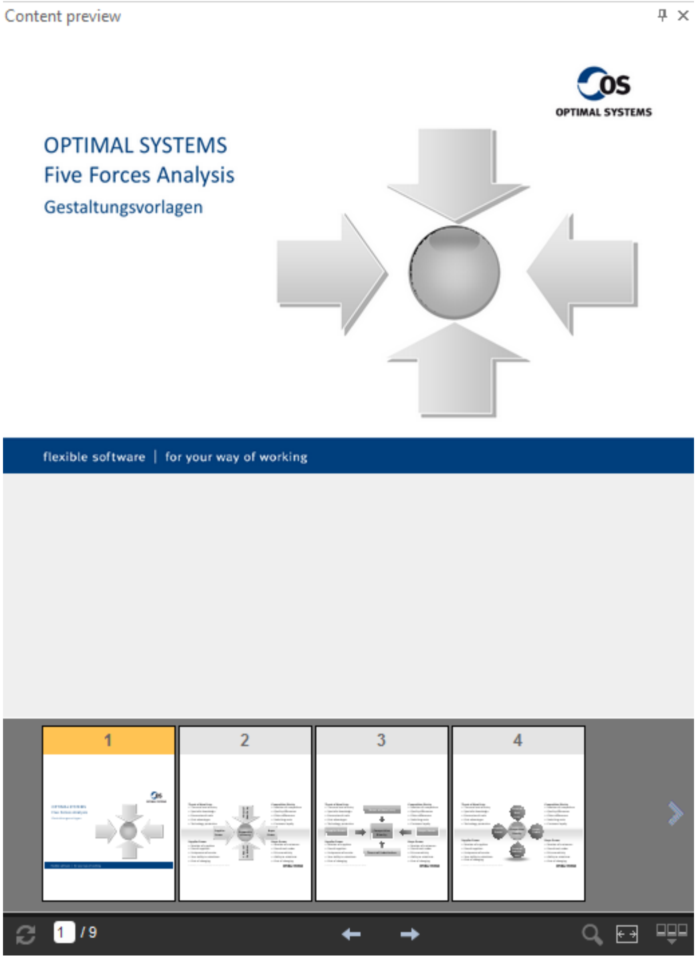
The process monitoring that is integrated in enaio® documentviewer and run automatically stops all processes that are not used for a certain amount of time. For that reason, the service must not be executed by the default system user. Open Windows services administration after the installation and configure the service so that it is executed in a local system administrator account.

After installation, access to the Rendition Cache must be limited to prevent unauthorized external access. To do this, open the administration page of enaio® documentviewer (see 'enaio® renditioncache') and navigate to the **enaio® renditioncache** area. Select **Server settings > IP filter** to specify the servers from which the Rendition Cache can be accessed, i.e. the IP address of the enaio® server on which the Rendition Cache (`…\server\___ren.bat`) is installed. This setting is specified as a regular expression. It is possible to specify more than one server.

Check whether there are hotfixes (`SP` directory) or patches for enaio® documentviewer available in the installation data. If yes, you must install them (see 'Installing a Hotfix or Patch').

The installation and configuration of enaio® documentviewer is then completed.

In enaio® client, users can show or hide the document preview in the ribbon using the **VIEW** tab.



If users receive a message that a document preview cannot be displayed due to missing rights although they have document access rights, it may be necessary to activate the session cookies in the default Internet browser used on the workstations.

The viewer service is uninstalled through the enaio® setup. Deinstallation via the control panel is not possible.

Configuration

Content Processing Bus

Core service coordination, particularly with regard to data and control flows when creating and modifying documents and index data, is controlled by a central content processing bus (CPB).

Saving messages about changes made to documents, links, variants, and index data in queues designed specifically for this purpose is the task of the CPB. Controlling and monitoring of the queues will be performed in enaio® enterprise-manager.

Batches integrated in the queues generate these messages and are also responsible for their deletion from the CPB when a core service requested the message and executed the corresponding job successfully. If a core service does not work properly anymore, it notifies the CPB to move the requested messages back to the queues, so that they can be requested again.

After the installation of enaio®, the CPB is set up for the use on an enaio® server. Queues and batches are provided with default values and a configuration is not required.

> The CPB may only be deactivated when authorized by the support or consulting team.

The following queues are set up for the CPB:

RENDITION	Queue for rendition generation. It is read out by enaio® documentviewer.
FULLTEXTIDX	Queue for full text indexing of index data. It is read out by the component set up for full text indexing, i.e. enaio® fulltext or MS SQL Server.
FULLTEXTDOC	Queue for full text indexing of documents. It is read out by the component set up for full text indexing, i.e. enaio® fulltext or MS SQL Server.
SLIDE	Queue for generating rendition in the SLIDE cache. It is read out by the SLIDE cache. Provided that the SLIDE cache has not been disabled in enaio® enterprise-manager, renditions generated by enaio® documentviewer will be saved here (see 'Conversion').
PAGECOUNT	Queues for determining the number of pages in documents. It is read out by the document preview and the object information.

Multiple instances of each queue can be configured, but it is not possible to create additional queue types for the CPB.

Queues and queue instances are configured in enaio® enterprise-manager in the **Server properties > Category: Services > Content processing bus** area (see 'Category: Services').

The following batches are set up by default for the queues:

ProcessSlideCPMessages	Processing of messages concerning rendition generation in the SLIDE cache
ProcessPageCountCPMessages	Processing of messages for generating page numbers

Batches can be configured in enaio® enterprise-manager in the **Server properties > Category: Periodic jobs** area (see 'Category: Periodic Jobs'). Optionally, you can define for all batches whether it is allowed to execute one or more batches in parallel and in which server queue they will be executed.

In systems with multiple enaio® servers, batches for CPB queues can be outsourced to one server for an increased performance.

Aside from the basic configuration, core services do not have to be configured specifically for the CPB.

Full text indexing of documents and index data as well as the generation of thumbnails can be activated for object types in enaio® editor.

The CPB offers extensive capabilities for the intelligent control of the data processing load. For example, batches can be distributed among several enaio® servers for performance optimization. Alternatively, multiple core services of the same type, e.g. multiple enaio® documentviewer instances, can be used for job processing. A prerequisite for this is that the components involved must be configured accordingly and each core service instance must have an individual instance name. Our consulting team would be pleased to assist you with the configuration of customized deployment scenarios.

To check the interaction between CPB and core services after the installation or an update, you can monitor jobs in the **Extended administration > Monitoring > CP queues** area of enaio® enterprise-manager (see 'CP Queues'). Here, you can verify whether messages could be processed or not.

Updating the Content Preview

enaio® documentviewer creates just one preview per document, which is saved in the Rendition Cache and reused. Once a document has been changed, a new preview is created, but the view is not automatically updated in the preview of enaio® client. The updated preview is only displayed when users click the **Update** button in the content preview footer.

Alternatively you can set up the automatic generation and display of a document preview when document content has been modified and checked in.

To do so, the area `[System]` in the …`\etc\as.cfg` file of the data directory must be extended with the following line: `RELOADAFTERDOCCHANGE=1`

This entry enables the automatic generation and display of a document preview as soon as document content has been modified and checked in.

Content Preview of Client-Encrypted Documents

Content previews of document files encrypted by enaio® client (see 'Client Encryption') can only be created if the document files to create the preview are decrypted by enaio® documentviewer.

The following configuration file must be adapted:

```
…\services\OS_DocumentViewer\webapps\osrenditioncache\WEB-INF\classes\config\config.properties
```

Change the value of the parameter `sec.decrypt.cc` from 'false' to 'true.'

If required, adjust the value of the parameter `sec.decrypt.cc.timespan`. The parameter specifies the timespan after which the decrypted document files and previews are deleted again. 7200000 seconds are preset, i.e. 2 hours.

Configuration on the Administration Page

enaio® documentviewer, enaio® renditionplus, Rendition Cache, and the use of an OCR engine can be configured centrally on the administration page:

```
http://localhost:8070/osdocumentviewer/admin
```

The administration page can be opened on any Internet browser (excluding Microsoft Internet Explorer).

The login to the administration page of enaio® documentviewer is done by Basic Authentication.

The default user name for the technical user is 'root' and the password 'optimal'; these must be changed during the initial configuration of enaio® documentviewer. The user name specified here is independent of the login name for the enaio® system.

A technical user must be set up for enaio® documentviewer. The technical user needs read access to document types from which renditions are to be generated. Without read rights, renditions will not be created from documents of that type. By assigning read rights, it is also possible to control the document types from which no previews will be generated, e.g. because it is not generally desirable or because an adequate rendition quality cannot be achieved for certain document types due to the format. Users can view previews only if they have the appropriate access rights. Note that access rights are not automatically assigned to new document types and, if required, you must grant read rights for the technical user subsequently (see 'Introduction to the Security System').

What is more, the 'Server: Switch job context' system role is required for the technical user. Without this system role, the user is not authorized to display content in the preview of enaio® client.

The administration page is divided into the areas enaio® documentviewer, enaio® renditionplus, and Rendition Cache. When you click in an area, the options related to the respective component are displayed.

The settings specified on the administration page will be saved in the files `config.properties` and `route.properties` in the directory `…\services\OS_DocumentViewer\webapps\osrenditioncache\WEB-INF\classes\config`.

If changes were made, you have to restart the core service.

The following settings can be changed on the administration page:

enaio® documentviewer

General Settings	
Timeout (ms)	Specify after how long (in ms) preview generation is canceled. Default: 300000
Temp-Verzeichnis (Temp directory)	Path to the conversion working directory. The temp directory contains temporary files for rendition generation and is automatically cleaned up by enaio® documentviewer on a regular basis. The directory should be on a local data carrier where rapid data access is possible. Default: Path that was specified at installation, e.g. `C:/enaio/services/OS_documentviewer/data/temp`

Administrator name	Login name for the administration page of enaio® documentviewer. Standard: root
Administrator password	Password for the administration page of enaio® documentviewer. A change of password applies to this administration page only and will not change the enaio® user's password. Default: optimal

enaio® renditionplus

Processing route configuration	
Use MS Office	If MS Office is used for document conversion, MS Office 2010 must be installed on the computer that enaio® renditionplus runs on. If enaio® renditionplus runs on Windows Server version 2008 or later, you must check if a desktop folder named `systemprofile` exists in `C:\Windows\SysWOW64\config` (64 bit) or in `C:\Windows\System32\config` (32 bit). If not, you need to create the folder. Please note that Microsoft Office must have been started once on the computer that enaio® renditionplus is used on, and ensure that the privacy options were set when configuring the processing routes. Otherwise the dialog with the privacy options will be opened when you attempt to generate the previews and will prevent generation. Default: Activated
Use Aspose	Aspose is an alternative that is used if neither MS Office nor OpenOffice exists on the computer. Aspose is installed automatically with enaio® documentviewer. Default: Activated
Use OpenOffice	OpenOffice is used for conversion of documents that were created with OpenOffice or LibreOffice and if other converters are deactivated or if conversion with other converters failed. Default: Activated
Create PDF/A files	Specify whether files are generated in PDF/A format via the enaio® client function **Send e-mail > Content (PDF)**. Default: disabled
Use CPE	Specify whether enaio® documentviewer should retrieve messages from the CPB. If the CPB has not been set up yet or is currently unavailable, it is advisable to deactivate this option. Otherwise enaio® documentviewer will generate an error message every time

	it tries to retrieve messages from the CPB, which may impair performance. Default: Activated
Cache options	
Maximum cache size	Specify the maximum size of the cache directory. Specify the unit using MB, GB or TB. Default: 500 GB Recommendation for the minimum size: 100 GB
Cache high-water mark (in percent)	Upper limit for automatic cache cleanup When the high-water mark is reached, renditions are deleted from the cache until the low-water mark is reached. The oldest unmodified renditions are deleted first. Text renditions, i.e. OCR results, are never deleted. Default: 80
Cache low-water mark (in percent)	Lower limit for automatic cache cleanup When the high-water mark is reached, renditions are deleted from the cache until the low-water mark is reached. The oldest unmodified renditions are deleted first. Text renditions, i.e. OCR results, are never deleted. Default: 60
Instead of a cache cleanup across cache size, upper and lower limit, you can set a single cleanup depending on age in the following file: `…\webapps\osrenditioncache\WEB-INF\classes\config\config.properties` Change the value of `cache.activeIndex` to '1.' Adjust the value of `cache.olderThanInSeconds`. 15811200 seconds are preset (183 days). Restart the service. Text renditions, i.e. OCR results, are not deleted here either.	
Additional options	
Update MS Office form fields	Establish whether form fields in MS Office documents are updated during conversion. Using the custom settings, you can define which form fields are updated. The selection comprises: date fields, fields with formulas and calculations, fields with page numbers, and fields with file names, and file paths. If you activate update with **Yes**, only those fields with page numbers and fields with formulas and calculations are updated. Default: No

enaio® renditioncache

Server settings	
Server connection	Name or IP address of the server and its port are followed by the addressing probability. Data must be separated by a colon. Default: server and port that were specified at installation, e.g. `localhost:4000:100` Multiple servers (separated by '#') can be specified.
Instance name	Name of the instance under which the documentviewer instance is executed. The instance name must be unique to avoid conflicts with other core services. Default: RenditionPlus
Name of the technical user	Server login name of the technical user. Preview generation is performed entirely with the technical user account. The technical user must therefore be granted read permissions for all document types for which a preview can be created. The technical user requires the 'Server: Switch job context' system role for the display in enaio® documentviewer. Standard: root
Password of the technical user	Server login password of the technical user. Preview generation is performed entirely with the technical user account. The technical user must therefore be granted read permissions for all document types for which a preview can be created. The technical user requires the 'Server: Switch job context' system role for the display in enaio® documentviewer. Default: optimal
Object history entry	When a preview is retrieved with enaio® documentviewer, a corresponding entry is written to the object history. Specify the text for this entry here. Default: document was not displayed for preview.
IP filter	Access to the Rendition Cache must be limited to avoid unauthorized external access. Specify the IP address(es) of the enaio® server(s) that are allowed to access the Rendition Cache, as a regular expression. This setting is specified as a regular expression. Default: .*
OCR engine	Establish whether text recognition is enabled with FineReader. OCR with enaio® documentviewer requires integration of the file `axrenocr.exe`with enaio® enterprise-manager in the **Server properties > Category: General > OCR** area (see'OCR').
Parallel OCR	Specify for how many documents text recognition is run simultaneously.
Working directories	
Cache	Path to the cache directory of the Rendition Cache.

directory	It contains already generated preview documents and should be on a data carrier which offers enough space. Detailed information on data carrier dimension can be found in the document 'System Requirements'. Default: path that was specified at installation, e.g. `C:/OSECM/Services/enaio documentviewer/data/cache`
Database directory	Path to database directory It contains databases for preview generation and should be on a local data carrier where fast data access is possible. Default: path that was specified at installation, e.g. `C:/OSECM/Services/enaio documentviewer/data/db`
Job directory	Path to the internal job directory. It contains jobs for preview generation and should be on a local data carrier where fast data access is possible. Default: path that was specified at installation, e.g. `C:/OSECM/Services/enaio documentviewer/data/jobs`
Session configuration	
User session timeout (ms)	Specify after how much time (in ms) an inactive user session is closed. Default: 1200000
Check user session activity	An extra job checks whether the current user session is still active. When the option is activated, enaio® documentviewer is better able to respond to network disruptions, however the volume of network traffic also increases due to the higher levels of communication. Default: Activated

LoginPipe exceptions are configured in enaio® enterprise-manager in the **Server properties > Category: General > Login** area (see'Login').

You must specify the user name and the IP address of the computer on which enaio® documentviewer is run. The user must also be assigned the 'Server: Switch job context' system role.

enaio® renditionplus and Rendition Cache

With enaio® renditionplus, a rendition service is provided for converting files into different file formats and text recognition in image files. The conversion process for numerous source and target formats can be controlled in great detail and customized to individual requirements.

The Rendition Cache is the storage component of enaio® documentviewer; it centrally manages the generated renditions and contains the conversion logic.

The batch file ___`ren.bat` is copied to the server directory when enaio® documentviewer is installed.

This file controls communication with the Rendition Cache through the REST client `curl.exe`, which is also installed, and ensures that all conversions to the PDF or TIF format that have not been configured yet using a batch file are forwarded to the Rendition Cache for processing.

If you manage exclusively single-sided image documents in PDF format in the image modules, you can use enaio® renditionplus to convert them by disabling the internal image conversion in enaio® enterprise-manager via **Server properties > Category: General > Conversion** .

For multiple-page image documents that are managed in PDF format, enaio® renditionplus would only convert the first page of each document. All other pages would be lost. enaio® renditionplus is generally unsuitable for these conversions.

enaio® renditionplus enables W-Documents in enaio® client to be converted to a PDF format via the **Send email > Content (PDF)** and then sent. If the administration page of enaio® documentviewer has been configured accordingly, the converted files comply with the PDF/A-1a standard.

enaio® renditionplus provides renditions automatically with the object ID of the document belonging to the rendition. In this way, a rendition can be read directly from the Rendition Cache using the object ID when it is sent using the enaio® client function **Send email > Content (PDF)** without the document first having to be transferred from enaio® server to enaio® renditionplus. This speeds up conversion and reduces the data quantity to be transmitted across the network.

You configure the setting in enaio® enterprise-manager in the **Server settings > Category: General > Conversion > Call renditions using object ID** area. Calling renditions using the object ID is activated by default.

Which source formats are converted to which target formats by enaio® renditionplus is provided in the following table.

Source formats:	Extension	Target formats:	PDF	TIFF	PDF/A
		Preview image			
Bitmap Graphic	bmp	x	x	x	x
Comma-separated values	csv	x	x	x	x
Device-Independent Bitmap Graphic	dib	x	x	x	x
Word document	doc	x	x	x	x
MS Word document with macros	docm	x	x	x	x
MS Word XML document	docx	x	x	x	x
MS Word document template	dot	x	x	x	x
MS Word XML document template with macros	dotm	x	x	x	x

MS Word XML document template	dotx	x	x	x	x
AutoCAD drawing	dwg	x[1]	x[4]	x[1]	x[4]
Drawing Interchange File Format	dxf	x[1]	x[1]	x[1]	x[1]
Extended (Enhanced) Windows Metafile Format	emf	x[2]	x[2]	x[2]	x[2]
Outlook E-mail	eml	x[2]	x[2]	x[2]	x[2]
Encapsulated Portable Document Format	epdf	x[2]	x[2]	x[2]	x[2]
EclipsePackager Invoice	epi	x	x	x	x
Encapsulated PostScript	eps[5]	x	x	x	x
Encapsulated PostScript	epsf[5]	x	x	x	x
Encapsulated PostScript	epsi[5]	x	x	x	x
OpenEXR Bitmap	exr	x	x	x	x
Graphics Interchange Format	gif	x	x	x	x
Windows Icons	ico	x	x	x	x
Joint Photographic Experts Group	jpg	x	x	x	x
MS Project	mpp	x[1]	x[1]	x[1]	x[1]
Multipage TIFF Bitmap	mpt	x[1]	x[1]	x[1]	x[1]
Microsoft Exchange mail document	msg[3]	x	x	x	x
OpenDocument (Ver 2) Graphics Document	odg	x	x	x	x
OpenDocument (Ver 2) Presentation	odp	x	x	x	x
OpenDocument (Ver 2) Spreadsheet	ods	x	x	x	x
OpenDocument (Ver 2) Text Document	odt	x	x	x	x
Portable Bitmap Graphic	pbm	x	x	x	x
Picture Exchange	pcx	x	x	x	x
Portable Document Format	pdf	x	x	x	x
Portable Network Graphics	png	x	x	x	x
Portable Anymap	pnm	x	x	x	x
PowerPoint Templates	pot	x	x	x	x
MS Presentation template with macros	potm	x	x	x	x
MS Presentation template	potx	x	x	x	x
MS PowerPoint slideshow	pps	x	x	x	x
MS PowerPoint slideshow with macros	ppsm	x	x	x	x

MS PowerPoint XML slideshow	ppsx	x	x	x	x
MS PowerPoint presentation	ppt	x	x	x	x
MS PowerPoint presentation with macros	pptm	x	x	x	x
MS PowerPoint XML presentation	pptx	x	x	x	x
Post Script	ps[5]	x	x	x	x
Post Script Level 2	ps2[5]	x	x	x	x
Post Script Level 3	ps3[5]	x	x	x	x
Photoshop Document	psd	x	x	x	x
Pyramid Encoded TIFF	ptif	x	x	x	x
Rich Text Format	rtf	x	x	x	x
Scalable Vector Graphics	svg	x[1]	x[1]	x[1]	x
Compressed Scalable Vector Graphics	svgz	x[1]	x[1]	x[1]	x
OpenOffice Spreadsheet	sxc	x	x	x	x
OpenOffice Presentation	sxi	x	x	x	x
OpenOffice Text	sxw	x	x	x	x
MS Visio Drawing	vsd	x	x	x	x
MS Visio Smartshape	vss	x	x	x	x
MS Visio Template	vst	x	x	x	x
Wireless Bitmap File Format	wbmp	x	x	x	x
Windows Metafile	wmf	x	x	x	x
MS Works Word Processor	wps	x	x	x	x
X Bitmap Graphic	xbm	x	x	x	x
Gimp eXperimental Computing Facility	xcf	x	x	x	x
MS Excel Binary File Format	xls	x	x	x	x
MS Excel Binary Workbook with macros	xlsb	x	x	x	x
MS Excel template with macros	xlsm	x	x	x	x
MS Excel Workbook	xlsx	x	x	x	x
MS Excel Template	xlt	x	x	x	x
MS Excel workbook with macros	xltm	x	x	x	x
MS Excel Template	xltx	x	x	x	x
Extensible Markup Language	xml	x	x	x	x

[1] Requires Microsoft Office 2010 to be installed on the enaio® renditionplus computer. For vsd files, Microsoft Visio must be installed and already have been started once from the enaio® renditionplus user account.

[2] Only the body is converted for these file formats.

[3] E-mails in MSG format can also be converted to EML.

[4] MS Visio can only convert a few DWG files to PDF. If a DWG file can be opened with MS Visio, it can be converted.

[5] These documents can only be displayed with limited quality. Additional converters are required to generate better quality renditions.

The list of supported formats contains the formats that can usually be rendered using the converters included in the scope of supply. Because Microsoft Office documents may contain all kinds of embedded objects, rendering may not produce 100% accurate results.

In addition to the listed formats, other formats can be rendered for specific projects with support from the Professional Services Team at OPTIMAL SYSTEMS, as well as additional converters. If other converters are used, these must be able to be invoked from the command line and generate a PDF as the output format. Converters must not open dialogs that require input.

OCR Using AXFROCR

Together with the text recognition software ABBYY FineReader, the OCR component AXFROCR converts image documents into text documents for full text indexing. AXFROCR, `axfrocr.exe` is installed by enaio®-setup into the …`\server` directory. enaio® server starts AXFROCR if a document is created for which full-text indexing is enabled in the object definition and is assigned to neither a W nor an e-mail document type. The same applies to the automatic action 'Full text indexing' and neither W- nor E-mail document types have been selected.

AXFROCR checks the directory to which enaio® server writes the job files required by AXFROCR to process documents together with FineReader.

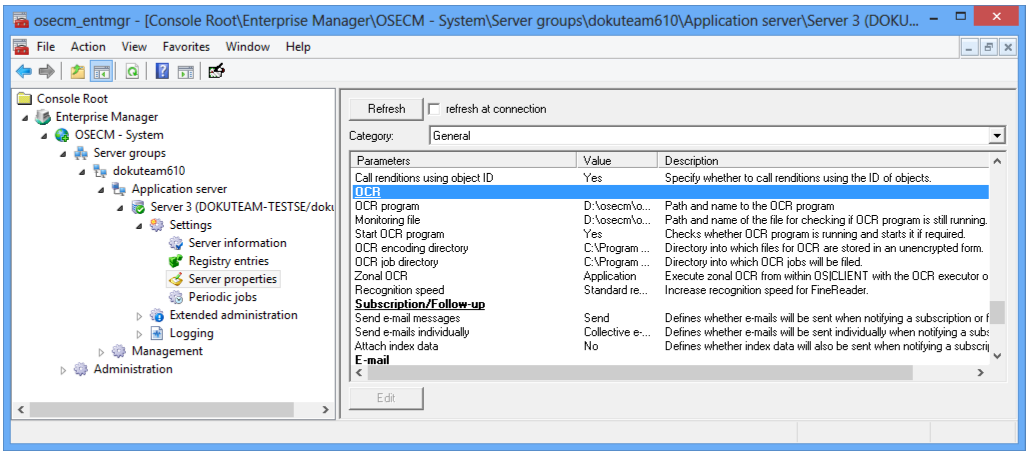
The connection between AXFROCR and FineReader must be configured in enaio® enterprise-manager; configurations must be synchronized with the configuration file `axfrocr.ini`.

Use a single OCR job directory to coordinate multiple enaio® servers with individual text recognitions. Indicate the job directory for each enaio® server in enaio® enterprise-manager as well as in the OCR configuration files using identical directory names in UNC notation. The 'ErrorPath' must also be specified identically in the OCR configuration files using UNC notation.

enaio® supports FineReader Version 11 which is installed with the setup via enaio® service manager and for which you receive a license key. Other FineReader versions are not supported. OPTIMAL SYSTEMS cannot therefore guarantee the function of these versions.

OCR configuration in enaio® enterprise-manager

Perform the settings for full-text indexing of image documents with ABBYY FineReader in enaio® enterprise-manager in the **Server properties > Category: General** area:



□ refresh at connection

Category: General

Parameters	Value	Description
Call renditions using object ID	Yes	Specify whether to call renditions using the ID of objects.
OCR		
OCR program	D:\osecm\o...	Path and name to the OCR program
Monitoring file	D:\osecm\o...	Path and name of the file for checking if OCR program is still running.
Start OCR program	Yes	Checks whether OCR program is running and starts it if required.
OCR encoding directory	C:\Program ...	Directory into which files for OCR are stored in an unencrypted form.
OCR job directory	C:\Program ...	Directory into which OCR jobs will be filed.
Zonal OCR	Application	Execute zonal OCR from within OS|CLIENT with the OCR executor o
Recognition speed	Standard re...	Increase recognition speed for FineReader.
Subscription/Follow-up		
Send e-mail messages	Send	Defines whether e-mails will be sent when notifying a subscription or f
Send e-mails individually	Collective e-...	Defines whether e-mails will be sent individually when notifying a subs
Attach index data	No	Defines whether index data will also be sent when notifying a subscri
E-mail		

- OCR program

  Enter the path to the application `axfrocr.exe` to enable enaio® server to start the OCR application AXFROCR. Enter `NO_OCR` if you do not use OCR but full-text indexing for text documents.

- Monitoring file

  A file created and frequently updated by the program checks whether or not the OCR program is running. Enter name and path of the file.

- Start OCR application

  When entering `Yes`, the monitoring file is used to check whether or not the OCR application is running. If the OCR program is not running, it will be started. Enter `No` to write job files without check to the job directory.

- OCR decryption directory

  Image documents encrypted by the server must be decrypted to enable text recognition. Specify the directory in which image files are filed in an unencrypted manner. Image documents are instantly deleted after processing.

  The entry is only required with enabled server encryption. Full-text indexing is not available with enabled client encryption.

- OCR job directory

  The directory to which enaio® server writes job files. The OCR application monitors this directory. Please check access rights to this directory.

- Zonal OCR

  The entry is used to specify how zonal OCR is performed in enaio® client. When being performed by the executor, an additional FineReader license is required. When being performed by the application, full text indexing uses the application's license.

  The entry is exclusively required with zonal OCR being performed by the executor in enaio® client. When being performed by the application, parameters and entries must be written to the file `axfrocr.ini` as known from full-text indexing.

- Recognition speed

Set the recognition speed to `Fast recognition` for high quality documents. Increased recognition speed for documents of less quality will cause errors.

The Configuration File

The OCR component AXFROCR reads set configurations from the file `axfrocr.ini` on start. If the file is not located together with AXFROCR in one directory, the program will create the file `axfrocr.ini` with default values.

You can edit the entries within the file with any editor.

Parameters	Function	Values	Default value
JobPath	Path to the directory to be monitored. It must correspond to the parameter **OCR job directory** in enaio® enterprise-manager. If the path was changed in enaio® enterprise-manager, it must be manually adapted here, too.		Directory in which AXFROCR has been started.
ErrorPath	Path to the directory to which job files are written in case they cannot be processed.		Directory in which AXFROCR has been started.
Alive	AXFROCR can create and frequently update an alive file. The file's editing date allows applications to determine whether AXFROCR is currently in operation and if not, to start AXFROCR. It must correspond to the parameter **Start OCR application** in enaio® enterprise-manager.	0 = do not create alive file 1 = create alive file	1
AliveFile	Path to and name of the alive file. It must correspond to the parameter **Monitoring file** in enaio® enterprise-manager.		'Directory in which AXFROCR has been started' \axfrocr.run
Alivetime	Interval in ms during which AXFROCR updates the alive file.		2000
StartOnce	Specifies whether AXFROCR can be started multiple	0 = multiple times	1

	times.	1 = once	
PollTime	Interval in ms after which AXFROCR checks the monitored directory for new job files.		2000
JobDelete	Specifies whether to delete job files or to add the extension 'bak'.	1 = delete 0 = rename	0
TextFormat	Text format for text file output.	All text formats supported by FineReader can be selected.	ASCII Standard for Windows
Zonal	Settings for zonal OCR in enaio® client. When being performed by the executor, an additional FineReader license is required. When being performed by the application, full text indexing uses the application's license. It must correspond to the parameter **Zonal OCR** in enaio® enterprise-manager.	1 = zonal OCR by the application 0 = zonal OCR by the executor	0
TextLanguage	Language settings of text recognition	all languages supported by FineReader	German
MinImageXY	OCR processing threshold value. Specifies the minimum image size that starts OCR processing.	x = images that vertically and horizontally are smaller than x pixels are not processed. -1 = disables the behavior	20

Since access rights to the AXFROCR directory are usually limited at the server, it is recommended to modify the default values of 'JobPath,' 'ErrorPath,' and 'AliveFile.'

If multiple source files are passed with an OCR job, it is filed in the directory containing jobs that cannot be processed (ErrorPath) as soon as an OCR error occurs caused by one of the source files.

enaio® renditionplus and Quicklooks

If the property **Document type without slide creation** is disabled for document types in enaio® editor, enaio® renditionplus automatically creates quicklooks. If the property is enabled, no quicklooks are created.

E-Mails in enaio® documentviewer

The e-mail display in enaio® documentviewer is formatted using the `header.properties` configuration file in the …`\OS_DocumentViewer\renditionplus\bin\apps\OsMail` directory.

The file can be adapted.

`Subject=`	The subject is displayed
`Subject.ValueFontFace=Calibri`	Font for the subject
`Subject.ValueFontColor=#000000`	Color for the subject
`Subject.ValueFontSize=5pt`	Font size for the subject
`From=`	The sender is displayed
`From.ValueFontFace=Calibri`	Font for the sender
`From.ValueFontColor=#000000`	Color for the sender
`From.ValueFontSize=3pt`	Font size for the sender
`To=To:`	Recipients are displayed. Preset 'To:'
`To.KeyFontFace=Calibri`	Font for the prefix
`To.KeyFontColor=#8888ff`	Color for the prefix
`To.KeyFontSize=2pt`	Font size for the prefix
`To.ValueFontFace=Calibri`	Font for the recipients
`To.ValueFontColor=#000000`	Color for the recipients
`To.ValueFontSize=2pt`	Font size for the recipients
`Date=Date:`	The date is displayed. 'Date:' is preset
`Date.KeyFontFace=Calibri`	Font for the prefix
`Date.KeyFontColor=#8888ff`	Color for the prefix
`Date.KeyFontSize=2pt`	Font size for the prefix
`Date.ValueFontFace=Calibri`	Font for the date
`Date.ValueFontColor=#000000`	Color for the date
`Date.ValueFontSize=2pt`	Font size for the date

```
fixHeader=true
```

The file can be expanded according to this model. For example, a formatting section for carbon-copied recipients can be added:

```
Cc=Cc:

Cc.KeyFontFace=Calibri

Cc.KeyFontColor=#8888ff

Cc.KeyFontSize=2pt

Cc.ValueFontFace=Calibri

Cc.ValueFontColor=#000000

Cc.ValueFontSize=2pt
```

Configurations in enaio® enterprise-manager

Enter the URL address for enaio® documentviewer in the **Server properties > Category: Services > Documentviewer** area in enaio® enterprise-manager (see 'Documentviewer').

Integrating enaio® documentviewer into a dashlet allows you to add the following additional information for the URL address:

URL parameter	Description
{objectident}	Object ID
{objecttype}	Object type
UserID	User ID
{userguid}	User GUID
{sessionguid}	Session-GUID
{servername}	Server name
{serverport}	Server port
{pagecount}	Number of the page which you want to display.
q={searchterm}	Transfer a search term. The references are highlighted in color in enaio® documentviewer.
annotations=0	Disables the annotation function in enaio® documentviewer.

The parameters are propended by a question mark and separated by the & character.

Example:

```
http://localhost:8070/documentviewer/app/viewer/{objectident}/?servername={servername}&serverport={serverport}&sessionGuid={sessionguid}
```

becomes

```
http://localhost:8070/documentviewer/app/viewer/213/?servername=localhost&serverport=40000&sessionGuid=AB617AF75F464568B502F7700F1C10F4
```

The parameters `sessionguid`, `servername,`, and `serverport` are required for session GUID authentication. If one of these parameters is missing, the subsequent authentication method will be tried (NTLM, Basic Authentication).

enaio® detailsviewer

enaio® detailsviewer provides flexible HTTP access to index and document data. enaio® detailsviewer will show, for example, index data of selected enaio® objects in the detail preview of enaio® client.

The enaio® detailsviewer service is implemented using both enaio® components, enaio® gateway and enaio® appconnector.

enaio® gateway is a proxy that is used as a communications interface between the core services.

enaio® appconnector is a REST interface that can be operated as enaio® detailsviewer with the configuration described in the following sections. Alternatively, enaio® appconnector can serve as an interface with mobile applications and provide structured access to enaio® server as a communication component. In the latter scenario, enaio® appconnector must be purchased.

You can find more information about enaio® appconnector in the component handbook.

The user guide for the details preview can be found in the enaio® client handbook.

Installation Requirements

For better load balancing, it is strongly recommended that enaio® gateway and enaio® appconnector are operated separately from the enaio® server computer.

enaio® server is installed, started, and provides an IP port.

The installation requires .NET 4.0 framework which is installed through the enaio® setup, if it is not on the computer.

It is recommended to publish the viewing service address under `intranet.kundendomain.de` in enaio® enterprise-manager in order to ensure long-time stability of the address and facilitate future server migrations of the viewer service.

Installation

enaio® detailsviewer is an enaio® component that you install as a service using the enaio® setup.

Save the enaio® setup locally on the computer on which enaio® detailsviewer is to be installed, as running the enaio® setup from a network can result in errors.

Select the enaio® appconnector component in the setup.

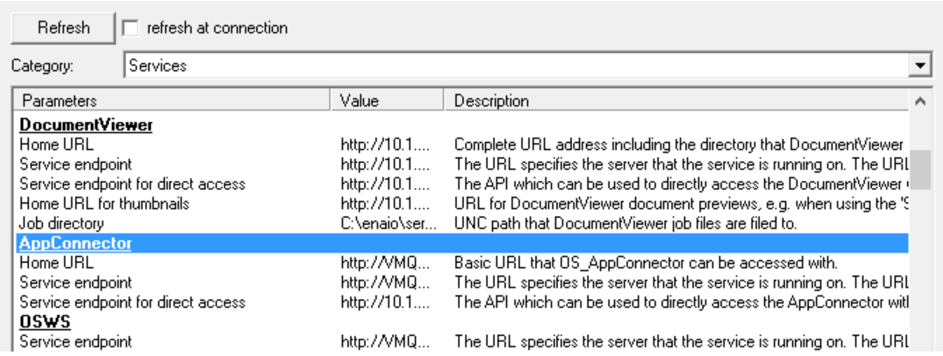
The runtime environment (JDK and application server) is also automatically installed.

The installed runtime environment should be used only for this core service, because when updating the core service the runtime environment is updated as well. If other enaio® or third-party components are run in the runtime environment, update errors may occur or the components may not be run after an update anymore.

Setup automatically registers the service with the respective home URL and service endpoint on the enaio® server. You can view and modify these URLs in enaio® enterprise-manager under **Server properties > Category: Services > Appconnector** (see 'Category: Services'). The registry keys are transferred to the client registry file during enaio® client installation and can be read by other components.

Changes to service endpoints are not automatically transferred to the client registry file. To synchronize the client registry file with the values of the server registry file, perform an update of the client installation either with the enaio® setup, or synchronize both registry files with the tool `OS.UpdateLocalServiceRegistry.vbs` from the directory …`\clients\client32\samples`. In systems with multiple servers the registry entries are transferred by the server with the highest probability of connection, or, if the probability of connection is less than 50% for all servers, they are transferred by the server in the last line of the `[SERVERS]` section in the `asinit.cfg` file of the client.

If several servers are used and all need to access one enaio® detailsviewer installation, you must manually adjust the addresses for all servers in enaio® enterprise-manager after the installation (see Appconnector').



Category: Services

Parameters	Value	Description
DocumentViewer		
Home URL	http://10.1....	Complete URL address including the directory that DocumentViewer
Service endpoint	http://10.1....	The URL specifies the server that the service is running on. The URL
Service endpoint for direct access	http://10.1....	The API which can be used to directly access the DocumentViewer
Home URL for thumbnails	http://10.1....	URL for DocumentViewer document previews, e.g. when using the '
Job directory	C:\enaio\ser...	UNC path that DocumentViewer job files are filed to.
AppConnector		
Home URL	http://VMQ...	Basic URL that OS_AppConnector can be accessed with.
Service endpoint	http://VMQ...	The URL specifies the server that the service is running on. The URL
Service endpoint for direct access	http://10.1....	The API which can be used to directly access the AppConnector wit
OSWS		
Service endpoint	http://VMQ...	The URL specifies the server that the service is running on. The URL

Check whether hotfixes (`SP` directory) or patches for enaio® appconnector are available in the installation data. If yes, you must install them (see 'Installing a Hotfix or Patch').

The installation and configuration of enaio® detailsviewer is then completed and you need to install the core service enaio® gateway. Otherwise enaio® detailsviewer cannot be used.

The viewer service is uninstalled through the enaio® setup. Deinstallation via the control panel is not possible.

enaio® contentviewer

enaio® contentviewer is a framework application that combines enaio® documentviewer and enaio® detailsviewer, enabling a combined view of the two services in enaio® client or enaio® webclient, for example.

For interface projects, enaio® contentviewer can also be integrated differently. Please contact the OPTIMAL SYSTEMS consulting team for information about this.

Installation

enaio® contentviewer is a service that is available once the core services enaio® documentviewer, enaio® detailsviewer, and enaio® gateway are available.

The setup automatically registers the service at enaio® server and enters its home URL into the **Server properties** > **Services** area in enaio® enterprise-manager.

You can view and modify these URLs in enaio® enterprise-manager under **Server properties** > **Category: Services** > **Contentviewer** > **Home URL** (see 'Category: Services').

If several servers are used and all need to access one enaio® contentviewer installation, you must manually adjust the URL address of enaio® contentviewer for all servers in enaio® enterprise-manager after the installation (see 'Contentviewer').

It is recommended to publish the viewing service address under `intranet.kundendomain.de` in enaio® enterprise-manager in order to ensure long-time stability of the address and facilitate future server migrations of the viewer service.

Configuration

By default, enaio® contentviewer displays the index data and basic parameters from enaio® detailsviewer first upon opening. To see the content preview from enaio® documentviewer in the display, add the parameter `?pagecount=1` to the URL for enaio® contentviewer.

Example:
`http://localhost/oscontentviewer/viewer/{objectident}/?pagecount=1`

The URL address for enaio® contentviewer is specified in the **Server properties** > **Category: Services** > **Contentviewer** area in enaio® enterprise-manager (see 'Contentviewer').

Integration in Microsoft Outlook

In MS Outlook, preview files can be shown in e-mails with enaio® contentviewer. The components required are copied to the directory `\clients\client32\` during the enaio® installation:

§ `axoutlookpreview.bat`

Run this component to register `axoutlookpreview.exe` which is located in the same directory of the workstation.

Alternatively, this component can be entered in the `asinit.cfg` file as a module in the 'Registration' section.

In order to register under Microsoft Windows Vista, the logged in user needs administrative rights. In addition, the User Account Control must be disabled.

- `AxOutlookPreview.reg` or `AxOutlookPreview64.reg`

  Enter the URL address of enaio® documentviewer in this file and register this data by running the file on the workstation. This information can also be deployed using administrative tools.

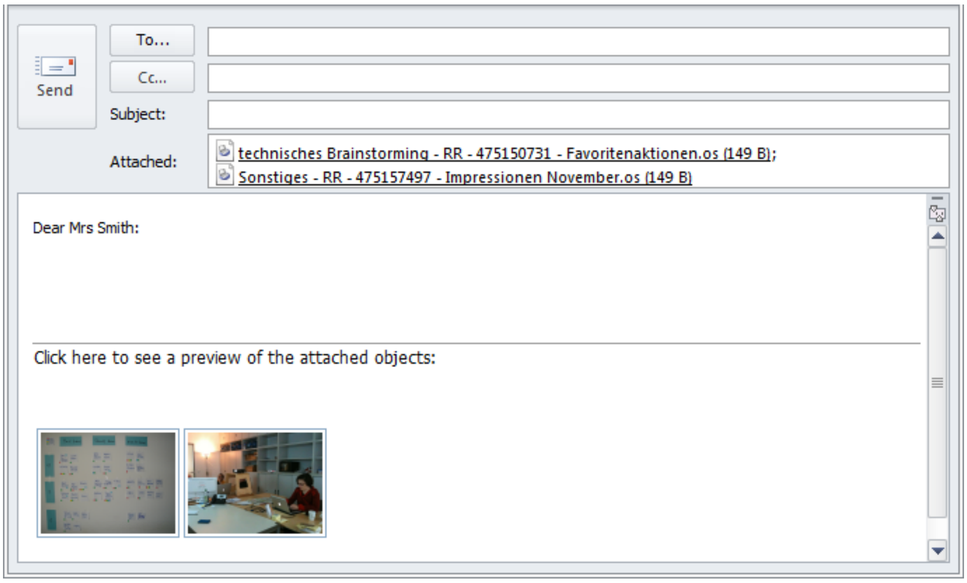
Afterward, the preview function is also available in Microsoft Outlook.

> Note that the user has to log in every time an e-mail is opened if the NTLM authentication filter is not enabled.

The component `AxOutlookPreview.exe` also serves as a display module enabling you to specify which applications are used to show documents managed in enaio® (see 'Display of OS Files').

Thumbnails in E-Mails

When sending e-mails with Microsoft Outlook to internal recipients, a thumbnail of the first page of an attached enaio® object can be inserted into the e-mail body.



technisches Brainstorming - RR - 475150731 - Favoritenaktionen.os (149 B);
Sonstiges - RR - 475157497 - Impressionen November.os (149 B)

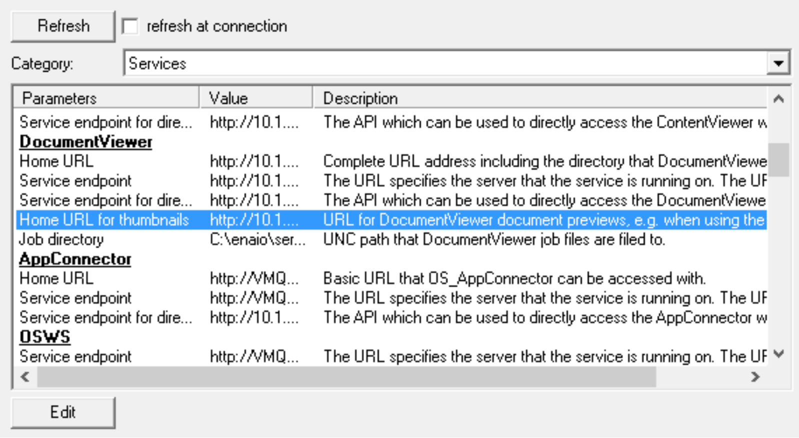
Dear Mrs Smith:

Click here to see a preview of the attached objects:

To do so, add the URL address for thumbnail previews in enaio® enterprise-manager.

The URL address for thumbnail views is:

```
http://<server>/osrenditioncache/app/api/document/{objectident}
/rendition/thumbnail
```



Category: Services

Parameters	Value	Description
Service endpoint for dire...	http://10.1....	The API which can be used to directly access the ContentViewer w
DocumentViewer		
Home URL	http://10.1....	Complete URL address including the directory that DocumentViewe
Service endpoint	http://10.1....	The URL specifies the server that the service is running on. The UF
Service endpoint for dire...	http://10.1....	The API which can be used to directly access the DocumentViewe
Home URL for thumbnails	http://10.1....	URL for DocumentViewer document previews, e.g. when using the
Job directory	C:\enaio\ser...	UNC path that DocumentViewer job files are filed to.
AppConnector		
Home URL	http://VMQ...	Basic URL that OS_AppConnector can be accessed with.
Service endpoint	http://VMQ...	The URL specifies the server that the service is running on. The UF
Service endpoint for dire...	http://10.1....	The API which can be used to directly access the AppConnector w
OSWS		
Service endpoint	http://VMQ...	The URL specifies the server that the service is running on. The UF

The 'target formats' section provides an overview of all document formats that can be converted to thumbnails.

Installing a Hotfix or Patch

When installing a hotfix or patch, only those files that differ from the current version are replaced. Updating your installation to a newer version is not possible using a hotfix or a patch.

Installing a hotfix or patch replaces only a few system files so the core service installation may not need to be configured again.

A hotfix does not back up the existing core service installation.

Before replacing files, it is checked whether adequate file versions are available at hotfix or patch installation. If this is not the case or a newer hotfix or patch was already installed, no files will be replaced. The hotfix and patch installations will be canceled reporting a message that the version of the installed service is wrong.

Hotfixes are located in the `SP` directory of the installation data.

Patches can be downloaded from the OPTIMAL SYSTEMS partner portal, the service portal for partners and customers of the OPTIMAL SYSTEMS group.

Updating Viewing Services

A viewer services update can be done from the enaio® setup.

A backup of the current configuration file versions is performed automatically. After an update, the backed up configuration files can be found in the application subdirectory `backup-(timestamp)` of the viewing service and are automatically imported into the updated version.

Dashlets in enaio® client

Dashlets are customizable, context-sensitive areas which can be integrated with enaio® client.

Dashlets allow you to integrate information sources, e.g. Internet pages like Wikipedia or Google Maps, and Web applications like enaio® detailsviewer (see 'enaio® detailsviewer') using what are known as dashlet services.

Dashlet services must be created. Respective information will be supplied by the OPTIMAL SYSTEMS professional services team upon request.

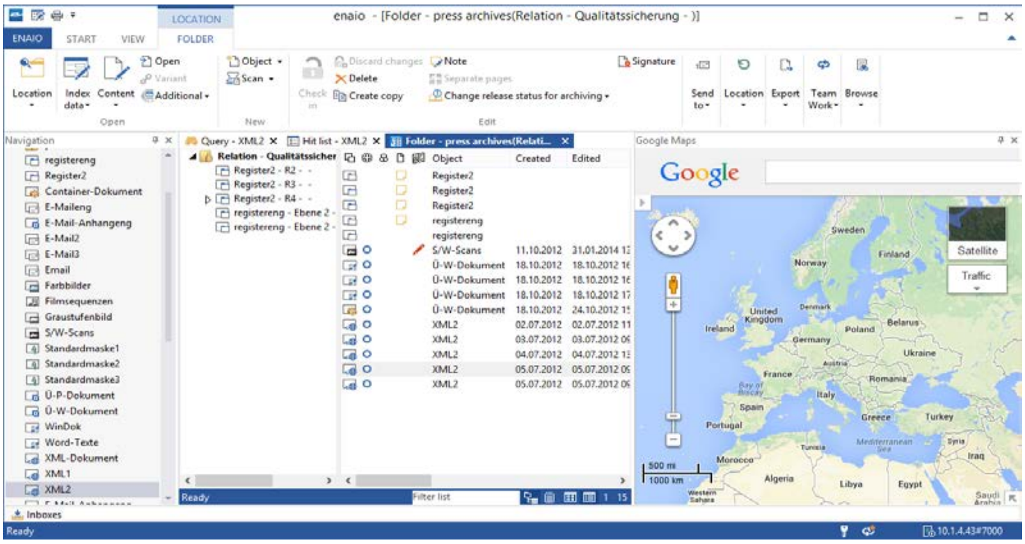
Dashlets do not require an installation to run, their display in enaio® client just need to be configured.

The content of dashlets is predefined by the administrator and cannot be changed by users.

A web application server or the core service enaio® gateway can be used for distributing dashlets (see 'enaio® gateway'). To distribute with enaio® gateway, file the pages for dashlets in the directory …`\services\OS_Gateway\apps\os_gateway\public`. Make sure that you give the dashlets individual names so that no existing application with the same name is overwritten.

Up to ten additional context-sensitive areas can be integrated with enaio® client. Several dashlets can be stacked.

For every integrated dashlet, an additional button will be added in the ribbon on the **VIEW** tab in enaio® client.



Object	Created	Edited
Register2		
Register2		
Register2		
registereng		
registereng		
S/W-Scans	11.10.2012	31.01.2014 1
Ü-W-Dokument	18.10.2012	18.10.2012 1
Ü-W-Dokument	18.10.2012	18.10.2012 1
Ü-W-Dokument	18.10.2012	18.10.2012 1
Ü-W-Dokument	18.10.2012	24.10.2012 1
XML2	02.07.2012	02.07.2012 11
XML2	03.07.2012	03.07.2012 0
XML2	04.07.2012	04.07.2012 1
XML2	05.07.2012	05.07.2012 0
XML2	05.07.2012	05.07.2012 0

They are controlled through a scheme where information of the currently selected object is passed and an URL address is called. If required, simple Web applications can be used to extend, change or forward the URL address.

Dashlet content can be loaded and displayed when starting a client, and can therefore be used to present a unique welcome page, for example. In addition, these dashlets are not informed of changed contexts by URL parameters, but instead receive these via a JScript callback, without reloading the page. So that dashlets are shown when a client is started up, set the parameter **Load at start** to **Yes** in enaio® enterprise manager under **Service properties** > **Services** > **Dashlet**. The parameter can be individually adapted for each dashlet.

Before users are able to show/hide a set up dashlet by clicking the respective button, they have to reset the window layout of enaio® client (**View** > **Settings** > **Workspace**).

Configuration

In the **Server Properties > Category: Services** area in enaio® enterprise-manager, enter the URL address for the dashlets and the title, which will be shown in enaio® client (see 'Dashlet 1-10') and optionally an icon. All icons which were integrated by use of enaio® editor can be indicated using the icon ID.

When integrating viewer services in a dashlet you can add further information to the URL address:

URL parameter	Description
{objectident}	Object ID
{objecttype}	Object type
UserID	User ID
{userguid}	User GUID
{sessionguid}	Session-GUID
{servername}	Server name
{serverport}	Server port
{pagecount}	Number of the page which you want to display.

The parameters are propended by a question mark and separated by the & character.

Example:

```
http://localhost:8070/documentviewer/app/viewer/{objectident}/?servername={servername}&serverport={serverport}&sessionGuid={sessionguid}
```

becomes

```
http://localhost:8070/documentviewer/app/viewer/213/?servername=localhost&serverport=40000&sessionGuid=AB617AF75F464568B502F7700F1C10F4
```

The parameters `sessionguid`, `servername,`, and `serverport` are required for session GUID authentication. If one of these parameters is missing, the subsequent authentication method will be tried (NTLM, Basic Authentication).

Using the parameter `?q={searchterm}`, a search term can also be passed. The references are then highlighted in color in enaio® documentviewer:

With the following URL, for example, the index data and basic parameters of documents selected in hit lists, folder or register lists will be displayed in a dashlet:

```
http://localhost:8060/osrest/api/documents/raw/{OBJECTIDENT}/?format=html&sessionguid={sessionguid}&servername={servername}&serverport={serverport}
```

enaio® feedreader and contentfeeder

Introduction to Feeds

enaio® contentfeeder allows you to access RSS feeds with user-specific subscription, follow-up, and workflow data from enaio® using an RSS reader.

If enaio® webclient is integrated into enaio®, the user can open an object directly or start the workflow step using the RSS feed.

enaio® feedreader can regularly query the RSS feeds of any channel, save them as electronic mail files, and generate an XML file that is used to transfer these electronic mail files into enaio® as e-mail objects with an automatic import action.

Both feed components are installed from the Web archive `os_feed.war` and configured using the collective configuration file `config.properties`.

In addition, the license key 'FRD' is needed for both feed components.

Feeds – Installation

enaio® contentfeeder and enaio® feedreader are components of a Web application. The Web application requires the installation of the Apache Tomcat Web server since version 5.5.x in the Windows server environment. The installation program for the Web server is available free of charge and, if required, we would be happy to provide it to you.

To install the feed components, load the `os_feed.war` Web archive as a local WAR file using the Tomcat Web Application Manager. After installation, the Web application will start automatically.

The Web archive `os_feed.war` is located on the installation media under directory `\components\OS_feed`.

The installation file `MhtActiveX.msi` is also found in this directory. Run this file to install on the Web server the components that enaio® feedreader needs to convert RSS feeds in HTML format into EML files.

Configuration – enaio® contentfeeder

enaio® contentfeeder is configured using the `config.properties` configuration file from the `os_feed/web-inf/ directory` of the Web server. Here, you specify how the enaio® server can be addressed.

Provided that enaio® web-client is integrated, you can also configure the connection to enaio® web-client in this file.

To use enaio® contentfeeder, first enable the following function in the configuration file:

`contentfeeder-using=true`	on/off

enaio® server

For the connection to the enaio® server, enter the IP and port in the following format:

`osecm.server = 127.0.0.1`	IP address of enaio® server
`osecm.port = 4550`	port of enaio® server

Update Interval

RSS feed data are cached. If a user updates the RSS reader data, they will be again queried from enaio® server only after the expiration of a specified period. The data are submitted from the cache until the period expires.

`cache-intervall=60`	interval in seconds

enaio® webclient

For the connection to enaio® webclient, enter the address and the port of the Web server, as well as the root directory:

`osweb.server = localhost`	address/IP
`osweb.port = 80`	Port
`osweb.root = osweb`	root directory

If you are not using enaio® webclient, the following entry is necessary:

`Osweb.using = no`	switch 'yes/no'

This entry prevents the data concerning subscriptions, follow-ups and workflow from being supplemented with a link to the respective page in enaio® web-client.

The other entries in the configuration file `config.properties` must not be modified.

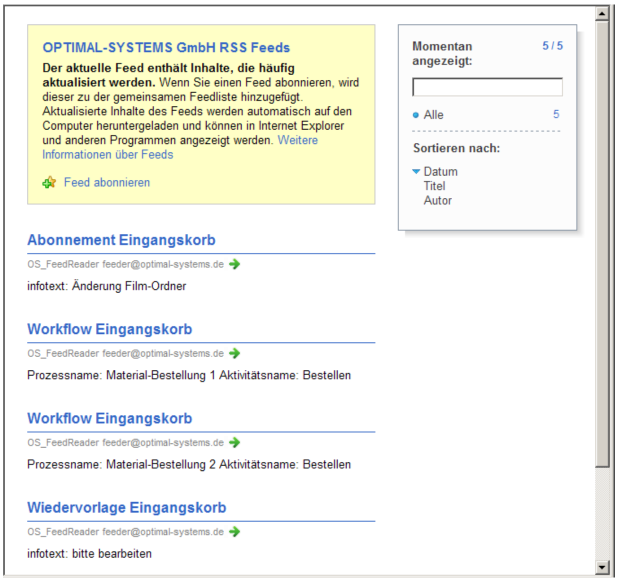
RSS Reader

You can integrate any arbitrary RSS reader. For access to the subscription and workflow data from enaio®, specify the root folder of the Web application of the Web server.

Example:

```
http://localhost:8080/feedreader/
```

Depending on the selected RSS reader and the configured authentication (see below) you either have to enter the user name and the password right away or these data are entered when the program is called or login is performed automatically.



OPTIMAL-SYSTEMS GmbH RSS Feeds

Der aktuelle Feed enthält Inhalte, die häufig aktualisiert werden. Wenn Sie einen Feed abonnieren, wird dieser zu der gemeinsamen Feedliste hinzugefügt. Aktualisierte Inhalte des Feeds werden automatisch auf den Computer heruntergeladen und können in Internet Explorer und anderen Programmen angezeigt werden. Weitere Informationen über Feeds

Feed abonnieren

Abonnement Eingangskorb

OS_FeedReader feeder@optimal-systems.de

infotext: Änderung Film-Ordner

Workflow Eingangskorb

OS_FeedReader feeder@optimal-systems.de

Prozessname: Material-Bestellung 1 Aktivitätsname: Bestellen

Workflow Eingangskorb

OS_FeedReader feeder@optimal-systems.de

Prozessname: Material-Bestellung 2 Aktivitätsname: Bestellen

Wiedervorlage Eingangskorb

OS_FeedReader feeder@optimal-systems.de

infotext: bitte bearbeiten

Authentication

Authentication is necessary for access to the data. The type of authentication is set in the configuration file …`os_feed/web-inf/web.xml`.

By default, simple HTTP authentication (HTTP Basic Authentication) is used. The browser opens a login dialog into which the user enters the enaio® user name and the enaio® password.

The following entry sets this type of authentication:

```
<filter>

<filter-name>AuthenticationFilter</filter-name>

<filter-class>com.os.http.BasicHttpFilter</filter-class>

</filter>
```

Alternatively, an NTLM authentication can be set. Thus, the user is automatically logged on provided that the current Windows user name is also an enaio® user name.

The following entry sets this type of authentication:

```
<filter>

<filter-name>AuthenticationFilter</filter-name>

<filter-class>com.os.http.NTLMHttpFilter</filter-class>

</filter>
```

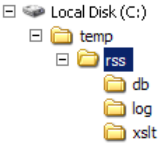
Other authentication types are possible. You can find information about this in the above section on enaio® documentviewer and in the documentation on configuring enaio® webclient.

Configuration of enaio® feedreader

If you want to save RSS feeds of any providers as electronic mail files (EML) and import them, install the components which convert RSS feeds in HTML format into EML files.

During the installation of the Web archive, the application `oxvbcreateHtml_EML.exe` is copied into the directory …`os_feed/web-inf/`. This application requires components which can be installed to the Web server using the installation file `MhtActiveX.msi` from the directory `\components\OS_feed\` of your installation media. Internet access is also required.

The installation of the Web archive creates the following directory structure for electronic mail files:



The EML files are saved to the `RSS` directory. The `DB` directory contains a database with information on the feed entries which have already been handed over. Error logs are written to the `LOG` directory. The `XSLT` directory contains necessary templates which are used to format the data files for the import.

If you need a different directory structure, change the respective entries in the configuration file `config.properties`.

To use the feed import, enable the following function in the configuration file at first:

`feedreader-using=true`	on/off

Proxy Server

If you are using a proxy server, enter the respective data into the configuration file:

`proxy-using=true`	on/off
`http-proxy-host=proxy.optimal-systems.de`	Address
`http-proxy-port=4118`	Port

RSS Feed List

In the configuration file, list the RSS feeds that you want to apply:

`feedimporter.list=Feed1,Feed2,Feed3`	The entries are separated by comma.

Enter the data of each entry in the following format:

`Feed1`	Label
`feedimporter.Feed1.url=http://www.os.de/os.rdf`	Address
`feedimporter.Feed1.generate.eml=true`	conversion on/off

If you turn the conversion off, only the files with the title, link and description data of the entries will be created.

Update

Specify in the configuration file how often updated data must be searched for:

`import-timer-interval=3600` update interval in seconds

The database in the directory `\temp\rss\db` checks whether the feed entries are new or already present.

Templates

In addition to the EML files, a data file is required for the import with an automatic action. For each entry, this data file contains the assignment of title, link, description, and EML file. When configuring the import with the import wizard, assign this data to the data fields of the import object. The data file is created according to a template. Create a template called `Feed.xslt` for every entry in the RSS feed list.

In the directory …`\temp\rss\xslt`, you will find the template `template.xslt`. This template can be used as a model. For every entry in the RSS feed list, save the template under the respective name to the directory `XSLT`.

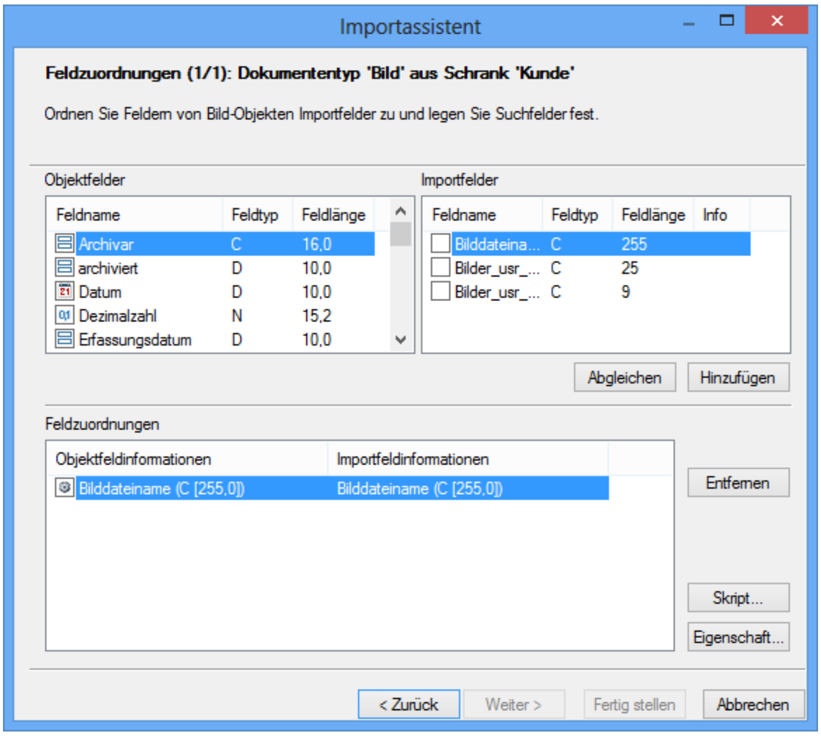
You can supplement the templates with fixed fields which must be assigned to every data set of the feed:

```
<item>
    <xsl:copy-of select="node()"/>
          <fixedfield1>content1</fixedfield1>
          <fixedfield2>content2</fixedfield2>
</item>
```

EML Import

Due to the templates, data files which are used as import files for XML imports are created in the …`\temp\rss` directory.

When configuring the import, assign the data to the fields of an e-mail object. For transferring electronic mail files, assign the import field **eml-file** to the object field **Image file name**.



Feldzuordnungen (1/1): Dokumententyp 'Bild' aus Schrank 'Kunde'

Ordnen Sie Feldern von Bild-Objekten Importfelder zu und legen Sie Suchfelder fest.

Objektfelder

Feldname	Feldtyp	Feldlänge
Archivar	C	16,0
archiviert	D	10,0
Datum	D	10,0
Dezimalzahl	N	15,2
Erfassungsdatum	D	10,0

Importfelder

Feldname	Feldtyp	Feldlänge	Info
☐ Bilddateina...	C	255	
☐ Bilder_usr_...	C	25	
☐ Bilder_usr_...	C	9	

Feldzuordnungen

Objektfeldinformationen	Importfeldinformationen
Bilddateiname (C [255,0])	Bilddateiname (C [255,0])

Details on configuring import actions can be found in the 'enaio® import-export' handbook.

Index