COPA-DATA
do it your way

zenon manual

User administration

v.7.00

Contents

1. Welcome to COPA-DATA help

GENERAL HELP

If you miss any information in this help chapter or have any suggestions for additions, please feel free to contact us via e-mail: documentation@copadata.com (mailto:documentation@copadata.com).

PROJECT SUPPORT

If you have concrete questions relating to your project, please feel free to contact the support team via e-mail: support@copadata.com (mailto:support@copadata.com)

LICENSES AND MODULES

If you realize that you need additional licenses or modules, please feel free to contact the sales team via e-mail: sales@copadata.com (mailto:sales@copadata.com)

2. User administration

zenon supports an user administration for the Editor and for the online operation (Runtime). The password system fulfills the guidelines of the FDA (Food and Drug Administration, 21 CFR Part 11).

License information

Part of the standard license of the Editor and Runtime.

THE CONCEPT

The password design assumes that different users have different operating rights (password levels). Even administrators have different operating rights but additionally have rights to administer users.

This password design gives the possibility of allocating several selective (separately defined) password levels (operating rights) to each user. A maximum of 128 (0-127, version 6.20 and higher) password levels is available. The assigning of the user to the individual password levels and the construction of the project-specific password design connected with this, can be done completely freely. Each user can have any levels released. Thus e.g. user 1 can have levels 0, 1, 5 and 6 assigned and user 2 can have levels 0, 1, 6, 8 and 10 assigned. The administrator can only assign rights which he himself has.

A user is logged in to Runtime in online operation by activating the Login (on page 81) function (Text button, Bitmap button, etc.). If the user should be logged in automatically based on an event (e.g. position of a key known to the system), the function Login without password (on page 82) is used. This function can e.g.be linked to a limit or a Rema.

The user can leave the system by using the function Logout (on page 83). The new user automatically logged in then has the name SYSTEM.

If during a defined period of time there is no operation, an automatic time triggered logout can be projected.

PROJECT MANAGER CONTEXT MENU

CONTEXT MENU USER ADMINISTRATION

Menu item	Action
Editor profiles	Opens the drop-down list that includes pre-defined editor profiles.
Help	Opens online-help

CONTEXT MENU USER

Menu item	Action
New user	Opens the dialog for creating a new user and adds the new user to the list of the detail view.
Export XML all ...	Exports all entries as an XML file.
Import XML	Imports entries from an XML file.
Editor profile	Opens the drop-down list that includes pre-defined editor profiles.
Help	Opens online help.

CONTEXT MENU USER GROUP

Menu item	Action
New user group	Opens the dialog for creating a new user group and adds the new user group to the list of the detail view.
Export XML all ...	Exports all entries as an XML file.
Import XML	Imports entries from an XML file.
Editor profiles	Opens the drop-down list that includes pre-defined editor profiles.
Help	Opens online help.

Context menu detail view: see also User administration detail view toolbar and context menu (on page 8)

3. Engineering in the Editor

> **Info**
>
> *If you change the default value for maximum password error under 'Project properties -> User administration -> Max. password error', keep in mind that this change is only active when you start the Runtime again. Function 'Reload' does not apply this change as otherwise an unlimited number of tries for entering the password would be possible.*

3.1 User administration detail view toolbar and context menu

Menu item/symbol	Action
New user	Opens the dialog for creating a new user and adds the new user to the list of the detail view.
Jump back to starting element	If you entered the list via function **linked elements**, the symbol leads back to the start element. Only available in the context menu when all linked elements are opened.
Copy	Copies selected entries to the clipboard.
Paste	Pastes the contents of the clipboard. If an entry with the same name already exists, the content is pasted as "Copy of".
Delete	Deletes selected entries.
Export selected XML..	Exports all selected entries as an XML file.
Import XML	Imports entries from an XML file.
Edit selected cell	Opens the selected cell for editing. The binocular symbol in the header shows which cell has been selected in a highlighted line.
Replace text in selected column	Opens the dialog for searching and replacing texts.
REMOVE ALL FILTERS	Removes all filter settings.
Import XML	Imports from an XML file.
Properties	Opens the **Properties** window for the selected entry.
Help	Opens online help.

CONTEXT MENU USER GROUP

Menu item	Action
New user group	Opens the dialog for creating a new user group and adds the new user group to the list of the detail view.
Copy	Copies selected entries to the clipboard.
Paste	Pastes the contents of the clipboard. If an entry with the same name already exists, the content is pasted as "Copy of".
Delete	Deletes selected entries.

Export XML all ...	Exports all entries as an XML file.
Import XML	Imports entries from an XML file.
Edit selected cell	Opens the selected cell for editing. The binocular symbol in the header shows which cell has been selected in a highlighted line.
Replace text in selected column	Opens the dialog for searching and replacing texts.
Properties	Opens the **Properties** window for the selected entry.
Export selected XML	Exports selected entries as an XML file.
Import XML	Imports from an XML file.
Remove all filters	Removes all filter settings.
Help	Opens online help.

3.2 Creating a user

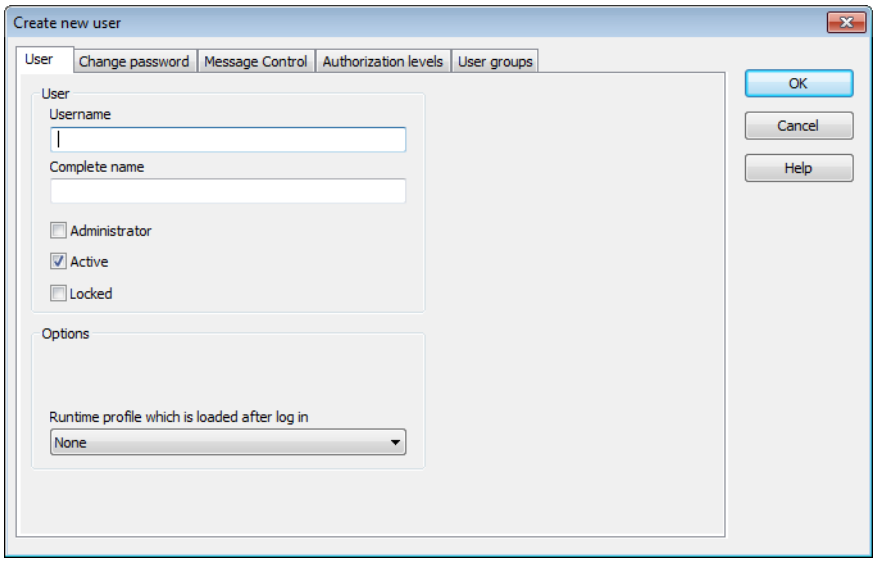
To create a new user:

1. navigate to node User administration/User
2. in the context menu of the project manager, the detail view or in the tool bar select New user...
3. The dialog for configuration is opened
4. in the individual tabs define the settings for:
   - Users (on page 11)
   - Password (on page 13)
   - Message Control (on page 14)
   - Authorization levels (on page 16)
   - User groups (on page 17)

> **Info**
>
> *Recommendation: As first user define an administrator. Only the administrator can access all functions and therefore reactivate users who were locked because they entered a wrong password three times.*

3.2.1 Users

Configuration of the user:



Parameters	Description
Username	Enter the user name. The user logs in to the system with his user name. Maximum length: 20 characters. Note: This number must be unique.
Complete name	Enter the full name of the user. With this you can allocate a user name to a real person.
Administrator	Active: The user gets the status of an administrator. Only an administrator can create new users, edit users, delete passwords, etc. in the Runtime.
Active	Active: The user is active and can log in in the Runtime. Note: According to FDA 21 PART 11 regulations an user nevers can be deleted so that at any time it is traceable, who executed which action. Therefore for projects which adhere to these regulations, a user must not be deleted but only deactivated. To prevent the deletion of users, in the project settings deactivate property Deleting users in group User administration.
Locked	Active: The user is locked in the Runtime and cannot log on. This option is set automatically if a user enters his password wrongly three times.
Lock code	Four-digit PIN code on. This code is used by the user for the command input in order to lock and unlock different areas.
Runtime profile which is called up at the log in.	Selection of the Runtime profiles from the drop-down list: ▸ None ▸ Default ▸ Last
OK	Accepts changes in all tabs and closes dialog.
Cancel	Discards changes in all tabs and closes dialog.
Help	Opens online help.

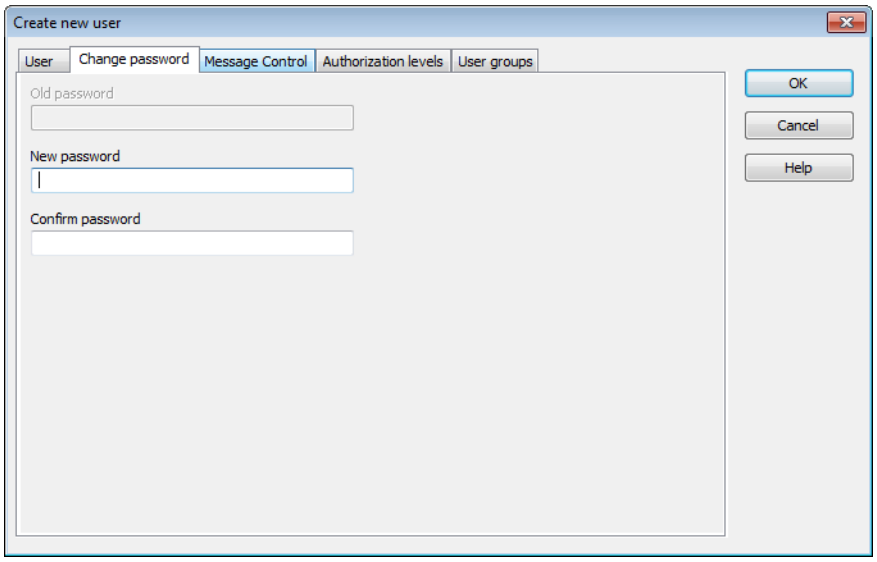
Info

An administrator can only enable users for groups for which he has the rights himself.

3.2.2 Change password

Defining or changing the password.

Passwords may have a maximum of 20 characters. The minimum length is defined in the project settings in property `Min. password length` in group `User administration`. The default value is 6 characters.

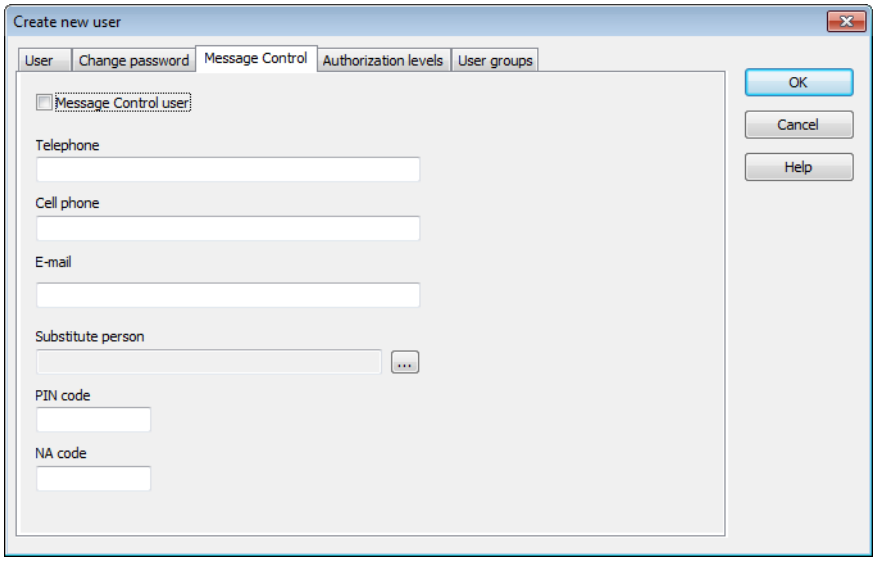


Parameters	Description
Old password	Current password.
New password	Enter new password. For language-spanning projects take care that it must be possible to enter the characters with the respective keyboard in the Runtime.
Confirm password	Repeat the new password.
OK	Accepts changes in all tabs and closes dialog.
Cancel	Discards changes in all tabs and closes dialog.
Help	Opens online help.

The function **Copy and paste** is not available for entering information in the password field.

3.2.3 Message Control

Options for using the users in module Message Control.



Parameters	Description
Message Control User	Active: The user is used by the module Message Control.
Telephone	Fixed network telephone number of the user. Used for text to speech. Enter numbers. The prefix + abbreviating 00 of the international area code is permitted.
Mobile phone	Mobile phone number of the user. Used for messages via GSM and SMS (text messages). Enter numbers, the prefix + abbreviating 00 of the international area code is permitted.
E-mail	E-mail address of the user
Substitute person	Select a substitute person if the user cannot be reached or the receipt of the message is rejected. A click on the ... button opens the selection dialog.
PIN code	PIN code with which the user confirms the message.
NA code	PIN code with which the user rejects the receipt of the message (not available). Message is subsequently sent to the next user in the list.
OK	Accepts changes in all tabs and closes dialog.
Cancel	Discards changes in all tabs and closes dialog.
Help	Opens online help.

Attention

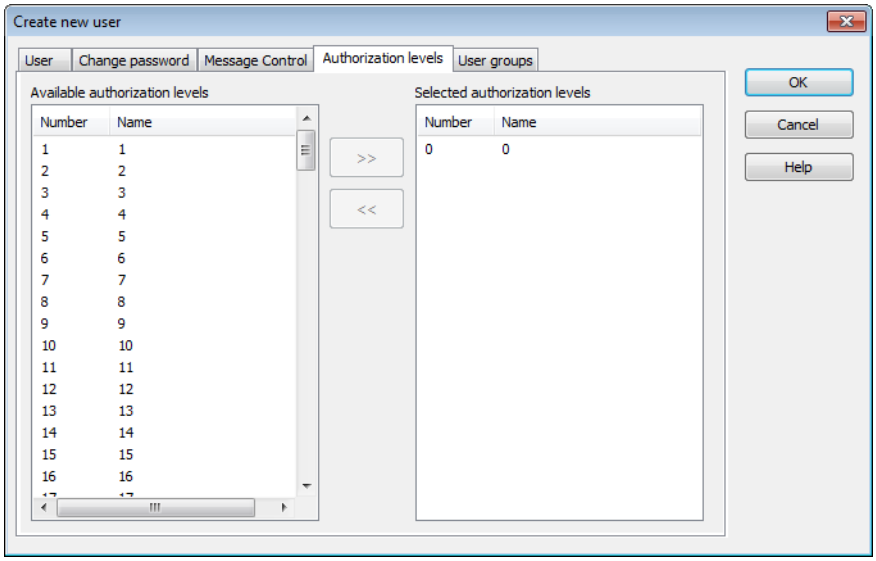
The acknowledgement codes for PIN (confirmation) and NA (rejection) must differ and should not be too similar.

If both codes are identical the code is interpreted as PIN and therefore as confirmation of the message.

If an unknown code is received, in case of SMS and e-mail the message is sent to the substitute person, in case of voice messages the error message is played.

3.2.4 Authorization levels

Defining the authorization level for the user.



Parameters	Description
Available authorization levels	List of all available authorizations
Selected authorization levels	List of assigned authorizations
Button double arrow to the right	Entries selected in the list **Available authorization levels** are added to list **Selected authorization levels**.
Button double arrow to the left	Selected entries in list **Selected authorization levels** are removed from the list.
OK	Accepts changes in all tabs and closes dialog.
Cancel	Discards changes in all tabs and closes dialog.
Help	Opens online help.

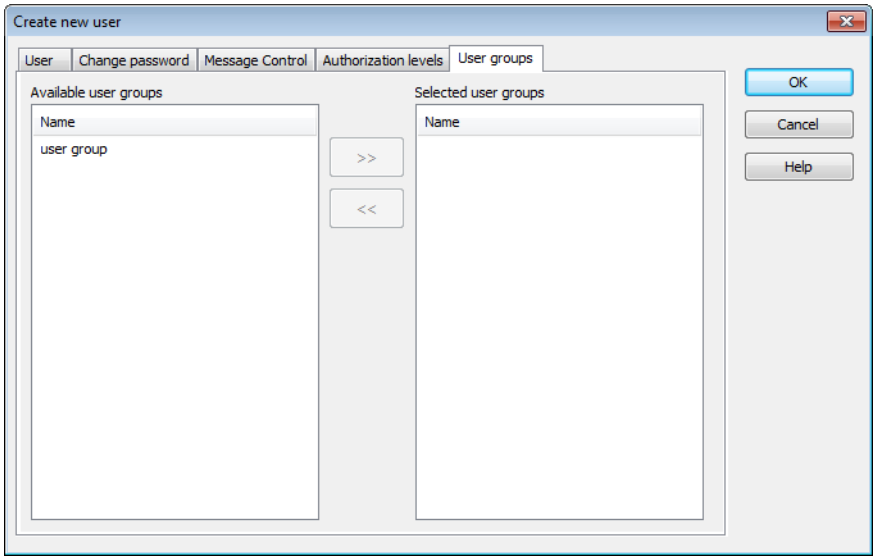
Info

With the help of `Ctrl` and/or `Shift` you can select more than one entry at a time.

- By pressing and holding `Ctrl` you can select a number of entries.
- By pressing and holding `Shift` and select two entriey, you select all entries which lie between the two selected entries.
- By pressing and holding both `Ctrl` and `Shift` and selecting two entries, all entries which lie between the selected entries are selected. The entries which were selected beforehand remain selected.

3.2.5 User groups

Assignment of the user to user groups.



Parameters	Description
Available user groups	List of all available user groups.
Selected user groups	List of assigned user groups.
Button double arrow to the right	Entries selected in the list **Available user groups** are added to list **Selected user groups**.
Button double arrow to the left	Selected entries in list **Selected user groups** are removed from the list.
OK	Accepts changes in all tabs and closes dialog.
Cancel	Discards changes in all tabs and closes dialog.
Help	Opens online help.

Info

With the help of `Ctrl` and/or `Shift` you can select more than one entry at a time.

- By pressing and holding `Ctrl` you can select a number of entries.
- By pressing and holding `Shift` and select two entriey, you select all entries which lie between the two selected entries.
- By pressing and holding both `Ctrl` and `Shift` and selecting two entries, all entries which lie between the selected entries are selected. The entries which were selected beforehand remain selected.

3.3 Create a user group

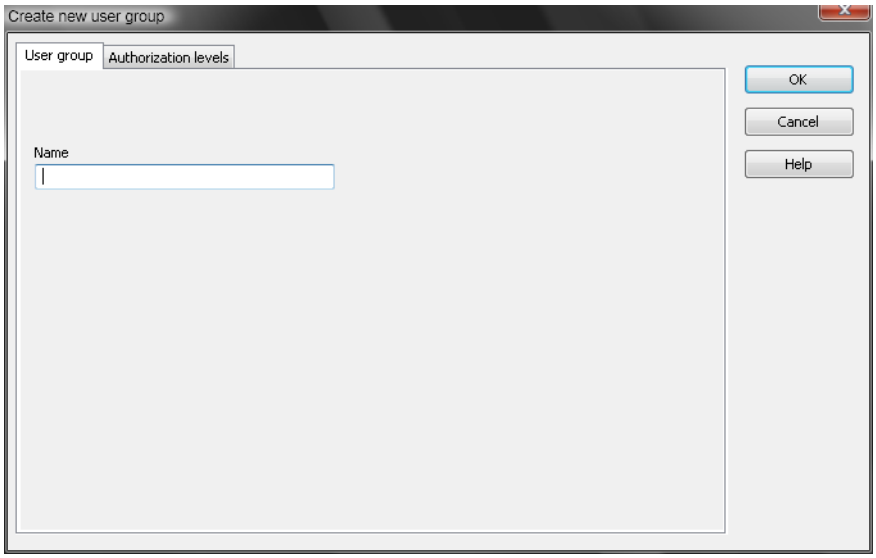
To create a user group:

1. Highlight the **User Groups** entry in the tree view of the Project Manager under the user administration entry

2. Right-click on the detailed view area (Project Manager Detail View) or directly on the **User Groups** entry
3. Select the **New user group** command in the context menu or alternatively click on the corresponding symbol in the toolbar
4. The **Create new user group** dialog is opened.
5. Define the name (on page 20) and authorization levels (on page 21)

> **Info**
>
> *Each user group must have an unambiguous name in a project.*
>
> *It is possible to create user groups with the same name in the global project and in the local project. If this is the case, the authorizations of the user group from the standard project are used in the event of a conflict. If the local group is deleted, the user again receives the rights from the group of the global project after the Runtime files are compiled in the Editor.*
>
> ***Example:***
>
> *A user group* **A** *is present in both the local project and in the global project. In the global project it is allocated the authorization levels 1, 2, 3, 100 and 101, and authorization levels 1 and 2 in the local project. In Runtime, the rules from the local project apply; only the authorization levels 1 and 2 are allocated. If user group A is not present in the local project, members of group* **A** *have authorization levels 1, 2, 3, 100 and 101 from the global project.*

3.3.1 Naming a user group



Enter the name of the user group you want to create.

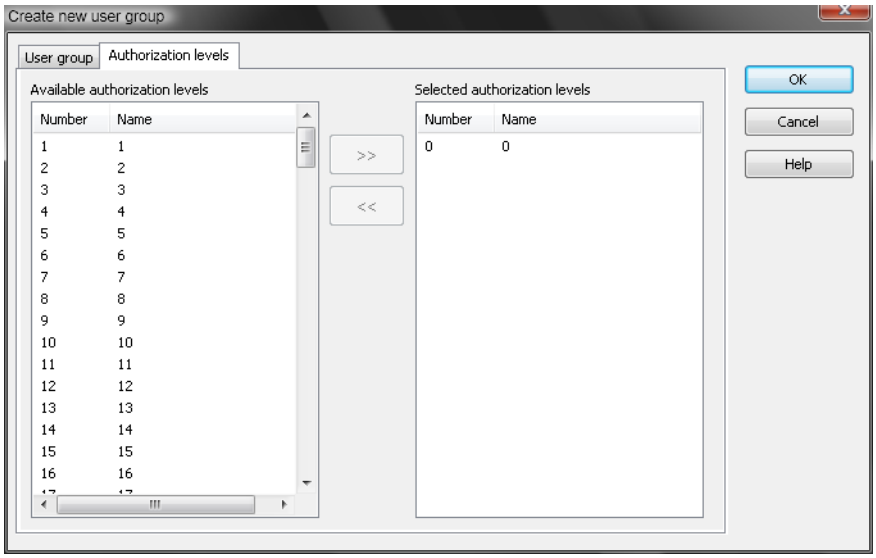
Info

The group name cannot be created with language switching, because it must be able to be checked in Active Directory.

@ is not a valid character for a user group.

3.3.2 Authorization levels

Assignment of the authorization level to a user group.



Parameters	Description
Available authorization levels	List of all available authorizations
Selected authorization levels	List of assigned authorizations
Button double arrow to the right	Entries selected in the list **Available authorization levels** are added to list **Selected authorization levels**.
Button double arrow to the left	Selected entries in list **Selected authorization levels** are removed from the list.
OK	Accepts changes in all tabs and closes dialog.
Cancel	Discards changes in all tabs and closes dialog.
Help	Opens online help.

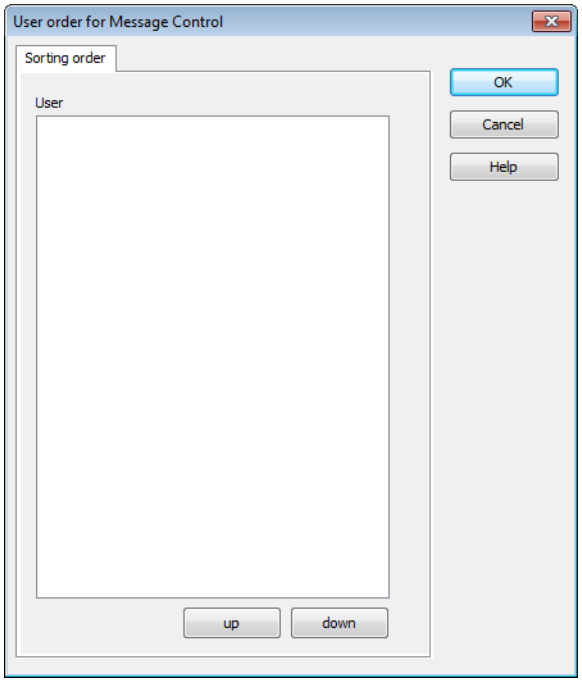
Info

With the help of `Ctrl` and/or `Shift` you can select more than one entry at a time.

- By pressing and holding `Ctrl` you can select a number of entries.
- By pressing and holding `Shift` and select two entriey, you select all entries which lie between the two selected entries.
- By pressing and holding both `Ctrl` and `Shift` and selecting two entries, all entries which lie between the selected entries are selected. The entries which were selected beforehand remain selected.

3.3.3 Order in Message Control

Defines the order of users within a group for the use of module Message Control.



Parameters	Description
Users	List of all available users
Up	Moves selected user up one place.
Down	Moves selected user down one place.
OK	Accepts changes in all tabs and closes dialog.
Cancel	Discards changes in all tabs and closes dialog.
Help	Opens online help.

3.4 Editing an user

A user is changed by selecting the user from the list in the detail view. The respective parameters are displayed in the properties window as a result of this. You can change the parameters `User name`, `Full name`, `Password`, `authorization level` and `User groups`.

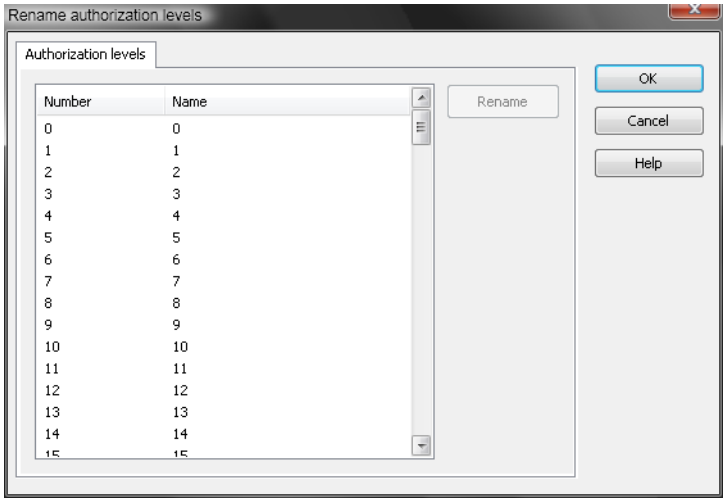
3.5 Changing a user group

A user group is changed by selecting the user group from the list in the detail view. The respective parameters are displayed in the properties window as a result of this. You can change the `Name` and `Authorization levels` parameters.

> **Info**
>
> *If you rename a user group, all users that are linked to this user group lose this link. The user group is displayed with (del).*
>
> *If there is already a user group with the same name in the global project however, all users previously linked to the group that has now been renamed assume all authorization levels of this user group.*

3.6 Changing the names of the authorization levels

You can change the names of the authorization groups globally for your project. To do this, go to the `User administration` group in project properties and click on the `Rename authorization levels` property there.



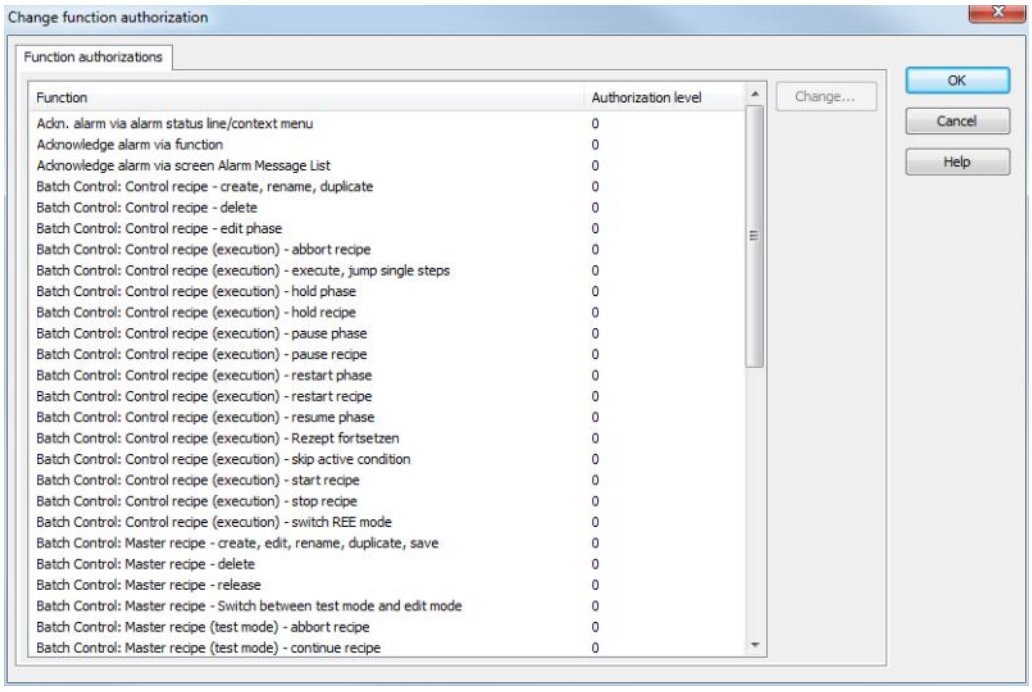
Open the editing field with a double click in the desired line of the **`Name`** column. Make the changes. The input is closed as soon as the focus is no longer in the field or it has been confirmed with `Enter`. The name is not changed if you press `Esc` or leave the edit field empty.

3.7 Function authorizations

Function authorizations ensure that certain actions in Runtime can only be carried out by those authorized to do them.

To issue a function authorization:

1. navigate to the `User administration` node in properties
2. Click on the `Function authorizations` property
3. The dialog for configuration is opened
4. Allocate the desired authorization to an authorization level
5. Allocate the authorized users to these authorization levels and remove them from all other users of this authorization level



Parameters	Description
Amending alarm comments	A Comment necessary for acknowledgement may be changed.
Entering alarm comments	A comment necessary for acknowledgement can be entered.
Acknowledge Alarm	Alarms can be deleted in Runtime.
Acknowledge alarm via alarm status line / context menu	Acknowledging an alarm via the alarm status line or the context menu is only possible if there is an authorization in the project of the alarm that is currently displayed. **For multi-project administration:** Acknowledging the system message in the alarm status line or via the context menu is only possible if there is an authorization in the I-project. **Comment:** System messages are messages that appear in the alarm status line when a certain (configurable) number of alarms has been reached.
Alarm acknowledgement via Alarm Message List screens	Acknowledging via Alarm message List screens is only possible with authorization in the project linked to the variable (multi-project administration). **Note:** If there is no authorization, the blinking is stopped but the alarm is not acknowledged.
Acknowledge alarm via function	Acknowledging via a function is only possible if there is an authorization for the selected alarms in the respective projects.
Switch on/off history of changes	In the Editor, the history of changes can only be switched on/off, if the user that is logged in is in the according authorization group.
Edit archive	Archive data (Archive server) can be amended in Runtime.
Edit Extended Trend	Curves in Extended Trend can be edited in Runtime. The following control elements are inactive if the user does not meet authorization requirements: ▸ Diagram ▸ Curves ▸ Frame ▸ activate ▸ axis

Return to last screen (PGUP)	Screen 'back' function can be executed in Runtime.
Screens catalogue	The function screen switch (Screen - functions) with the set option show this dialog during Runtime can only be executed, if the user who is logged in fulfills authorization requirements.
Notepad: Open file	The function file `open` in screenNotepad can only be carried out if the logged in user has the appropriate authorization level.
Notepad: Save file	The function `save` in screenNotepad can only be carried out if the logged in user has the appropriate authorization level.
Load project	In the Editor, the project data base can only be loaded, if the user that is logged in has the according authorization group.

For all actions, the user must be logged in and have the corresponding authorization levels.

Info

Acknowledging an alarm is only possible if there is an authorization for the selected alarms in the according projects.

You can set different authorization groups for each of these acknowledging methods. This allows you, for example, to configure that a certain user group can only acknowledge via the alarm status line, not in any other way.

3.8 Creating a screen of the type Login

Operation by different users is possible in Runtime by means of the Login (on page 85) screen type. This screen must be created in the editor first.

You will find more information on the pre-defined screen types in the chapter 'Screens / Pre-defined screen types'.

After the screen is opened an empty screen is displayed. You can add the default control elements via menu Control elements ->Add template.

4. Active Directory (AD)

Active Directory can be used in zenon for the user administration in the zenon Runtime. For the zenon Editor AD is not available.

The active directory can be used for three types of zenon:

1. The name of the authorization group in zenon user administration corresponds to the of the group names of a user group in Active Directory: Automatic assignment of the Active Directory user to zenon authorization group. All AD group users receive user rights that are defined in the zenon authorization group. See User groups in zenon and groups in Active Directory have the same name (on page 29)
2. In the description of the Active Directory group, the zenon authorization levels and the project are stored in a certain syntax. All users of the group receive the user rights stored in the AD group in zenon. See Assignment of an Active Directory user to zenon authorization levels (on page 30)
3. The Active Directory schema is expanded by fields in which the zenon authorization levels are saved. This requires an Active Directory extension schema. However this is not suitable for use in an FDA 21 CFR Part 11 regulated environment. See: Active Directory extension schema (on page 31).

> **Info**
>
> *When checking the password in zenon, the `max. password age` is also checked from the Active Directory.*

> **Info**
>
> *Active Directory and ADAM/AD LDS are not available with Windows CE.*

4.1 General

In order to be able to use the users of the Active Directory (hereinafter called AD) in zenon, a domain based on a Windows server operating system is required. In order to be able to administer user in the Active Directory, the server has to be a DNS server.

So a domain controller with DNS and Active Directory has to be available to be able to use these user accounts as users of zenon on a PC in the domain.

Access to the users of the Active Directory has to be activated in the properties of the project.

Basic knowledge about the Active Directory and the Windows server technology is assumed.

Attention

If registration is via Active Directory, all computers without exception must have access to the Active Directory. This also applies to clients and web clients.

Background: *A client is logged in directly from the client to the Active Directory. The zenon Runtime server is not involved in this.*
An Active Directory user can therefore only be logged on if a client:

- Is a member of the domain
  and
- Has access to the domain

4.2 The same user groups in zenon and in Active Directory

The following applies for users in zenon and in Active Directory:

- If a user is in the AD, but not in zenon, then:
  - The user groups are checked in zenon
  - The group authorization levels to which the user belongs, are allocated to the AD user
- If a user exists in both AD and in zenon and the user logs into Runtime, then:
  - The local zenon user has priority over the AD user

- If no authorization levels are checked in AD, because the local user is logged in

4.3 Setting the zenon authorization levels in the description field of an Active Directory group

The Windows users from the Active Directory can be used in zenon.

Individual users can be allocated in the Active Directory groups. The names of the groups must be as described in the following syntax:

zenon project name##free text

The description contains the user authorization following this syntax:

free text ##GRP=HEX-number## free text

Info

Group name and group description are not case-sensitive.

In order to increase readability, the HEX-number is divided in four parts (one for each authorization group) which are separated by a dash.

Structure of the HEX number			
FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF
Authorization levels 1	Authorization levels 2	Authorization levels 3	Authorization levels 4

Example

Group name: MASCHINE01##service staff

Group description: free text##GRP=FFFFFFFF-FFFFFFFF-FFFFFFFF-FFFFFFFF##free text

The users which are allocated to MACHINE01##service staff receive authorization level 0 - 127 in zenon.

It is not necessary to enter all 32 digits. Missing digits are interpreted as 0.

Example

Group description: free text##GRP=7##free text

The users which are allocated to a group with this description receive authorization level 0, 1 and 2 in zenon.

7 hexadecimal equals 111 as binary number. For each 1 in the binary number the corresponding authorization level is set. The right-most bit stands for authorization level 0. The bit to the left of this, stands for authorization level 1 and so on.

A user can be allocated to multiple groups. In this case the user receives the sum of the authorization levels of each group.

If a user is logged in tozenon, first it is checked whether the user exist in zenon locally. If not, the Active Directory is search for the user. If the user also does not exist there, the user is not logged in an a corresponding entry in the CEL is created. If the user is present in AD, but authorization levels in zenon are not defined for these users, the following entry is created CEL: 'No user rights defined for the user in the AD.' The user is logged in with authorization level 0.

4.4 Active Directory extension scheme

Note: This expansion should not be used in an FDA 21 CFR Part 11 regulated environment. For FDA 21 CFR Part 11 compliant user administration, use either the User groups in zenon and groups in the Active Directory (on page 29) method or Allocation of an Active Directory user to zenon authorization levels (on page 30).

Info

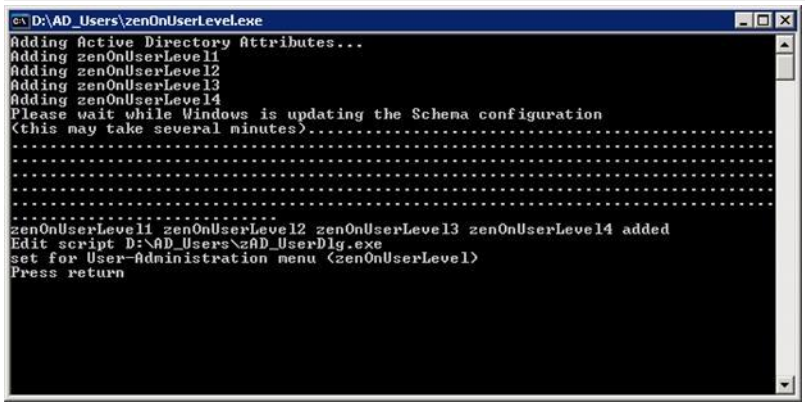
Active Directory and ADAM/AD LDS are not available with Windows CE.

4.4.1 Installing the schema extension

In order to be able to grant the 128 authorization levels of zenon to the users in the AD, these entries (4 integer values) have to be added to the AD schema.

For this purpose, two files (`zenonUserLevel.exe` and `zAD_UserDlg.exe`) are copied to the server (ideally to their own directory). As soon as the setup (`zenonUserLevel.exe`) has been started, this folder including the files contained in it must not be renamed or deleted.

> **Attention**
>
> *You can find the two files **zenonUserLevel.exe** and **zAD_UserDlg.exe** on the zenon DVD in the `/Software/zenonUserLevel/` folder*



Setup generates a reference to the file `zAD_UserDlg.exe` in the AD schema.

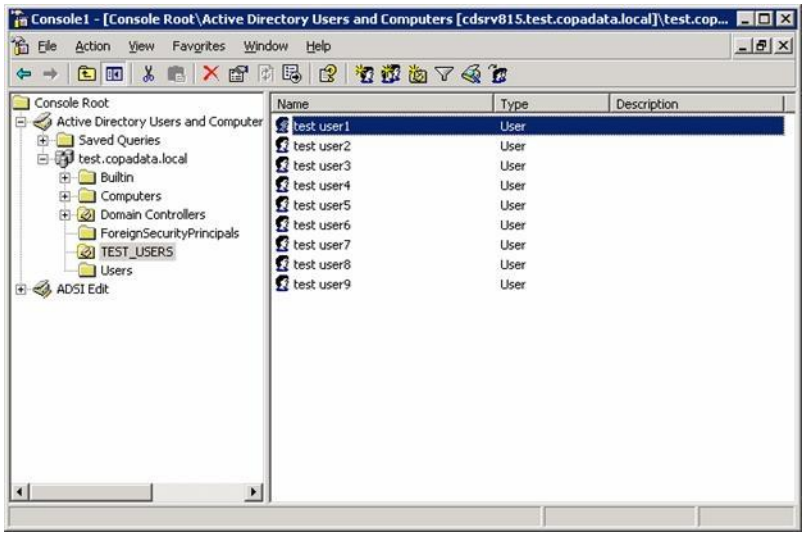
Additionally four integer values (zenonUserLevel1, zenonUserLevel2, zenonUserLevel3, zenonUserLevel4) are added to the AD schema.

> **Info**
>
> *Only a user of the group **Schema Administrators** is allowed to make these changes. Usually the domain administrator has these rights.*

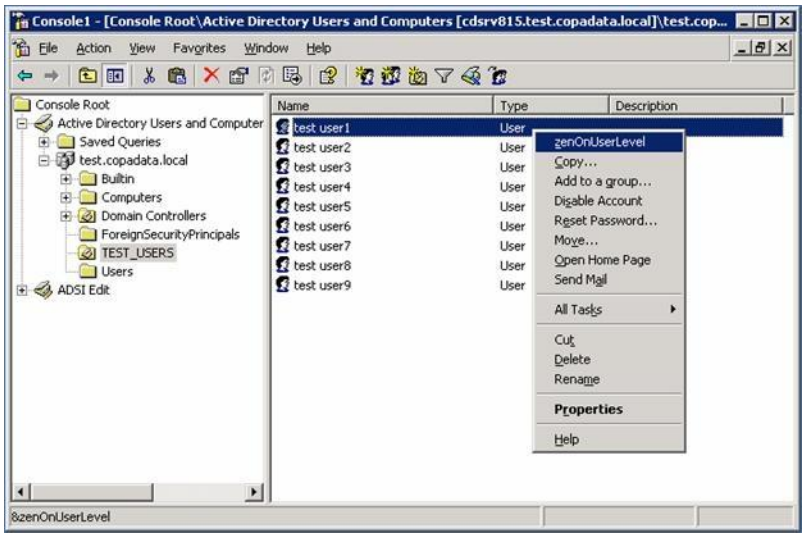
4.4.2 Granting user rights

After the successful extension of the schema the authorization levels can be granted to the single users.

For this purpose, the Microsoft Management Console (MMC) with the **`Active Directory Users and Computers`** plug-in is opened.



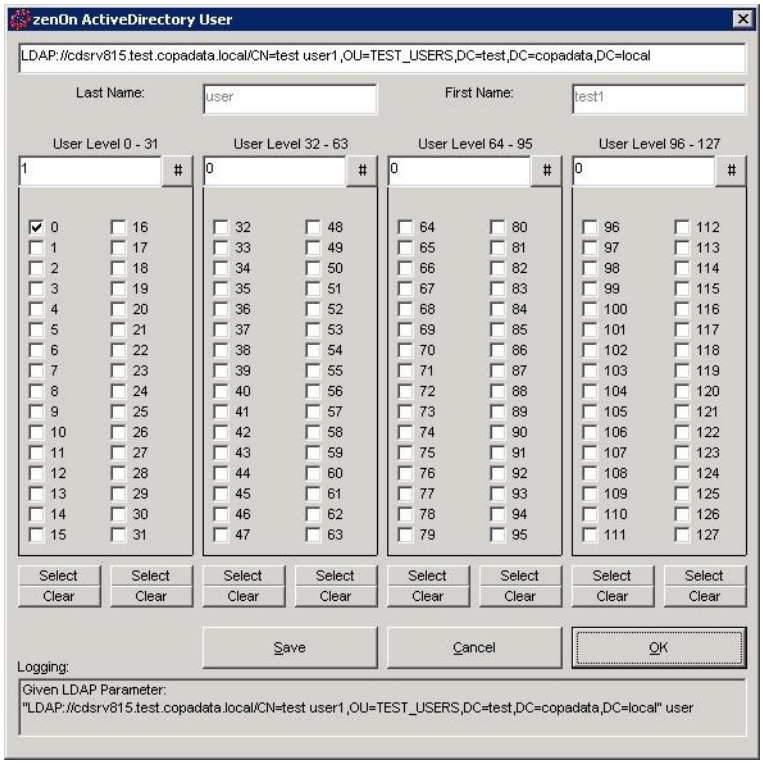
A context menu is opened by clicking on the desired user with the right mouse button. A new menu item is visible in the context menu: **`zenonUserLevel`**.



In this context menu, the **`zenonUserLevel`** entry has to be selected, so that the administration tool (zAD_UserDlg.exe) for the selected user is opened.

Info

The authorization levels for zenon can only be granted directly to the user, groups and organization units are not supported.



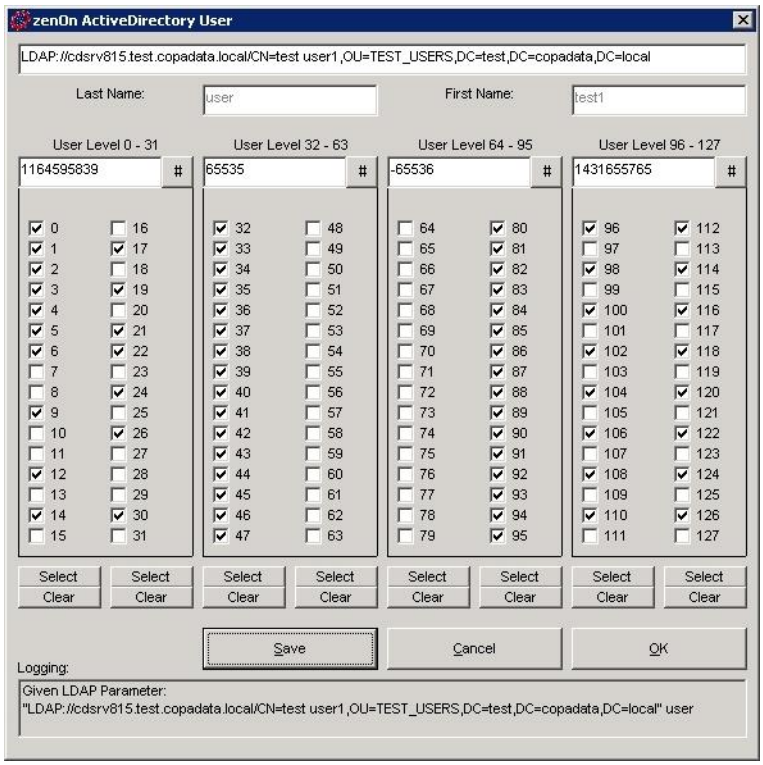
Up to 128 authorization levels per user can be defined with the help of the administration tool.

Info

As a default, the authorization level 0 is granted to each user; this cannot be deactivated in the administration tool.

*This level corresponds to the **SYSTEM** user of zenon.*

Description of the administration tool



Parameters	Description
[first line]	LDAP parameter that serves as connection string.
`Last name`	Last name of the selected user.
`First Name`	First name of the selected user.
`User Level`	Four integer values represent 32 authorization levels. They are inputted by activating or deactivating the checkboxes or directly inputting into the field.
#	Updates display of authorization levels.
Select	Activates all checkboxes in a column.
Clear	Deactivates all checkboxes in a column.
Save	Saves current settings.
Cancel	Rejects all changes made since the last save and closes the dialog.
OK	Saves all settings and closes dialog.
Logging	Displays logging information.

4.4.3 Schema extension – details

To clarify the whole background, the schema extensions are explained in detail here, so that they can be checked in the event of problems.

In order to be able to see the details of the AD schema, **ADSI Edit** has to be installed on the server. This tool is available as soon as the Support Tools from the Microsoft Server CD have been installed.

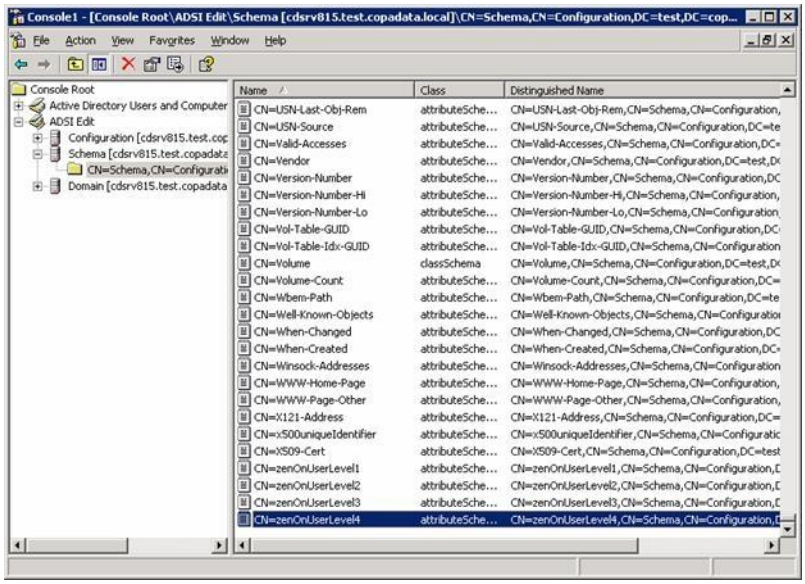
To be found on the CD under: `CD_ROOT/SUPPORT/TOOLS/SUPTOOLS.msi`

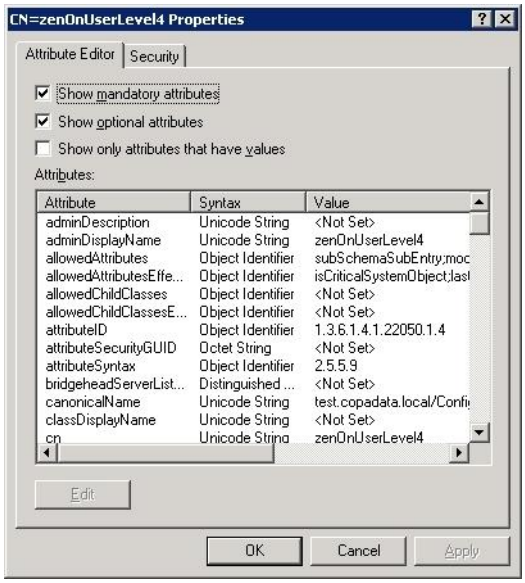
Then the **ADSI Edit** plug-in can be opened in the Microsoft Management Console (MMC). Now different connections can be established.

Schema

The additional attributes can be checked in the schema. These are normally listed at the bottom.

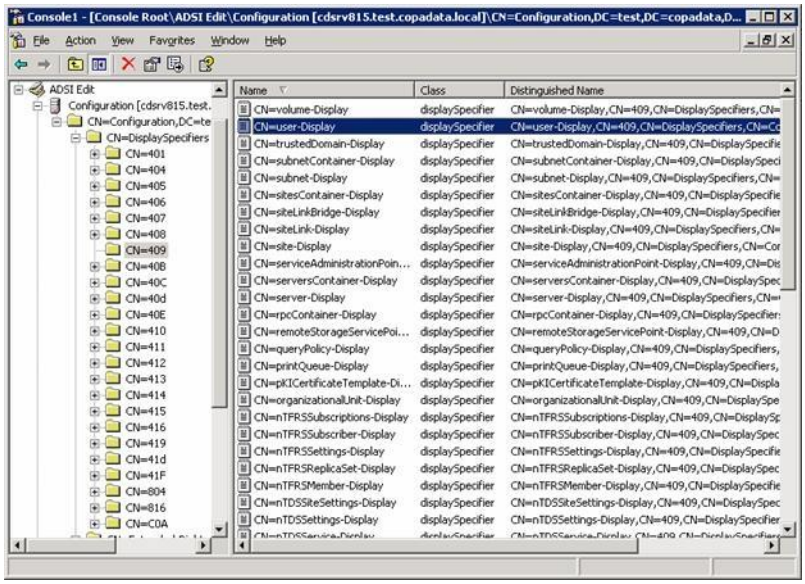
`zenonUserLevel1 - zenonUserLevel4`

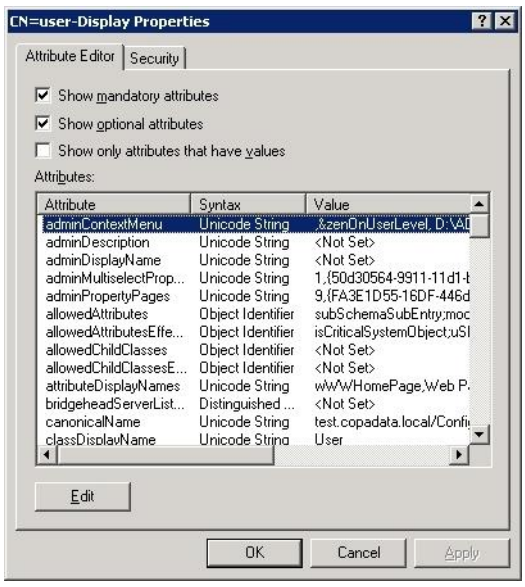




Configuration

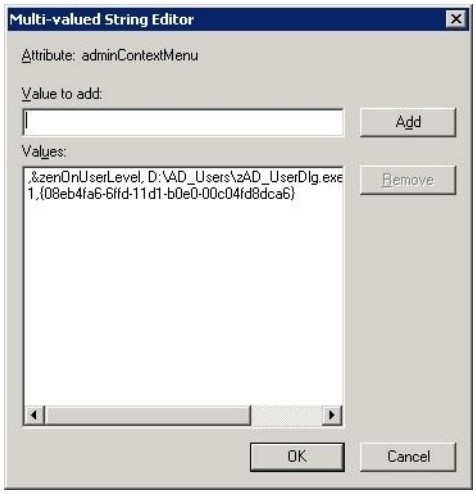
After the connection to configuration has been defined, the details of the single AD objects can be checked and edited. In this case, only the object user-display in the single 'DisplaySpecifiers' is of interest, because here the link between user object and AdministrationTool is established.





The properties of the **`user-Display`** object only contain attributes with the names `adminContextMenu`.

This attribute contains the link to the administration tool (**zAD_UserDlg.exe**).



This entry can also be amended manually if necessary.

To do this:

1. Select the entry
2. Press **Remove** button
3. Adapt the parameters
4. Use **Add** to add again

The parameter has the following structure:

```
,name of the menu entry, path of the file zAD_UserDlg.exe
```

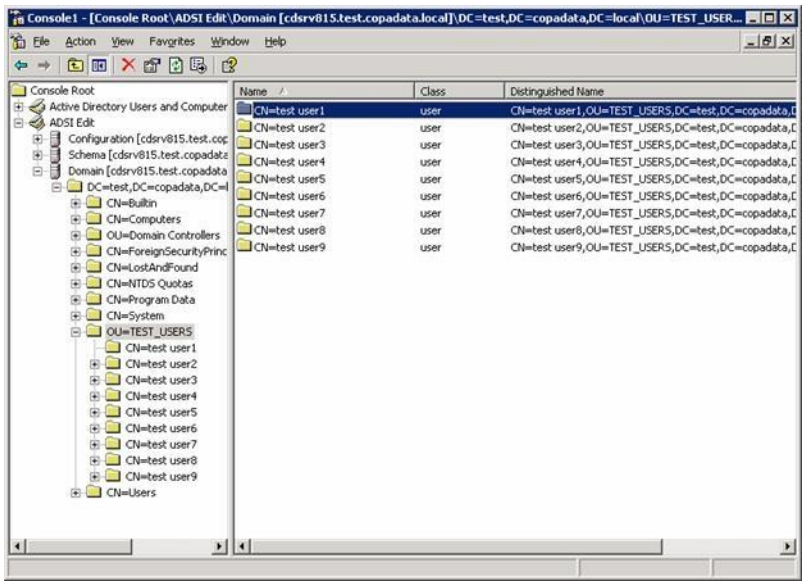
Example

Example, if the EXE file is in the directory `D:\\AD_Users`.

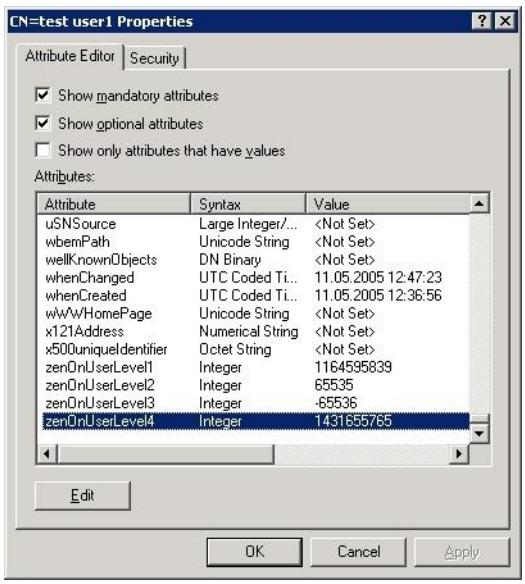
```
,&zenonUserLevel,D:/AD_Users/zAD_UserDlg.exe
```

Domain

If the **`Domain`** connection is opened, you immediately see parallels to the MMC with the **`Active Directory Users and Computers`** plug-in. This information can be found here again, but in more detail.



If you check the properties of a user object and scroll down to the bottom of the list, here you will also find 4 integer values for the authorization levels.



5. Active Directory Lightweight Directory Services - AD LDS (Windows Vista and subsequent versions)

Active Directory Lightweight Directory Services (abbreviation: AD LDS) is a simplified version of the Active Directory (on page 28) and is suitable for use on normal desktop operating systems; it is not necessary to use a server operating system. LikeAD (on page 28), AD LDS also supports:

1. The name of the authorization group in zenon user administration corresponds to the of the group names of a user group in Active Directory: Automatic assignment of the Active Directory user to zenon authorization group. All AD group users receive user rights that are defined in the zenon authorization group. See User groups in zenon and groups in Active Directory have the same name (on page 29)
2. In the description of the Active Directory group, the zenon authorization levels and the project are stored in a certain syntax. All users of the group receive the user rights stored in the AD group in zenon. See Assignment of an Active Directory user to zenon authorization levels (on page 30)

You can use AD LDS with:

- Windows Vista
- Windows 7
- Windows Server 2008

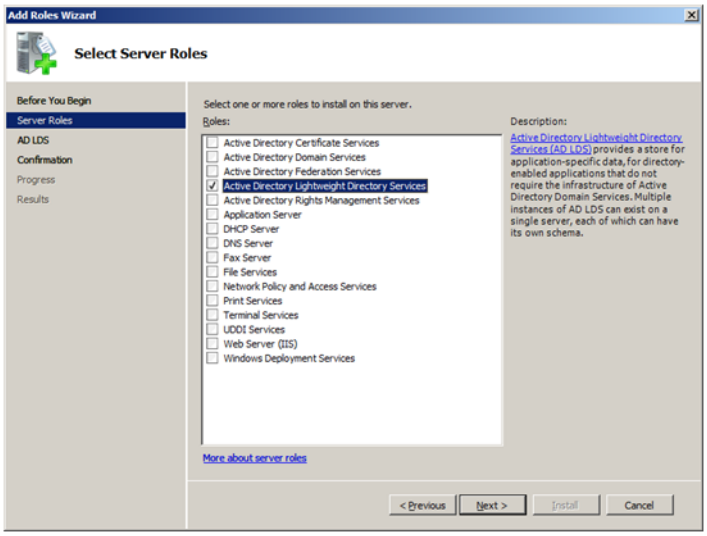
Use ADAM (on page 71) with Windows XP.

Installation and configuration with Windows Server 2008 is explained in these instructions. Usage with Windows Vista and Windows 7 is the same. For details of this, see the AD LDS with Windows 7 and Windows Vista (on page 69) chapter.

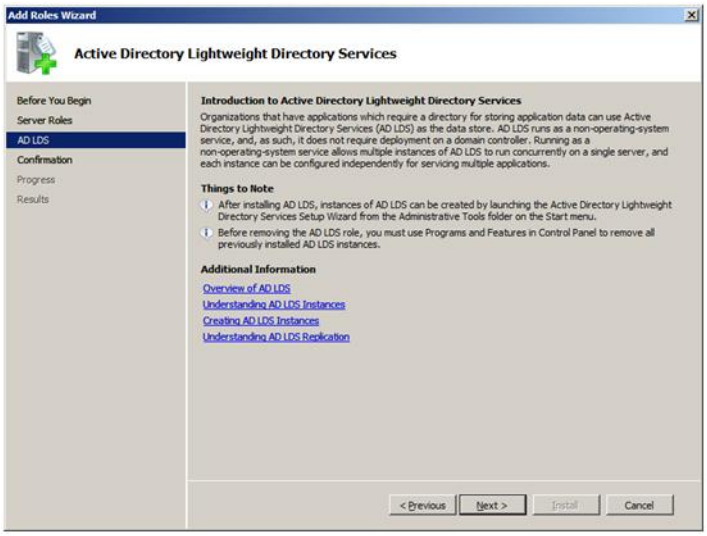
5.1 AD LDS with Windows 2008

To install the AD LDS server role:

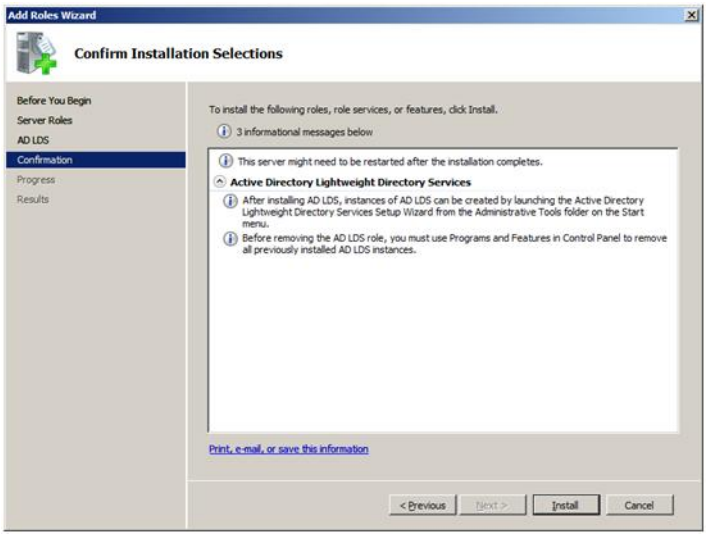
1. Select **`Server Manager`** in the administrative tools

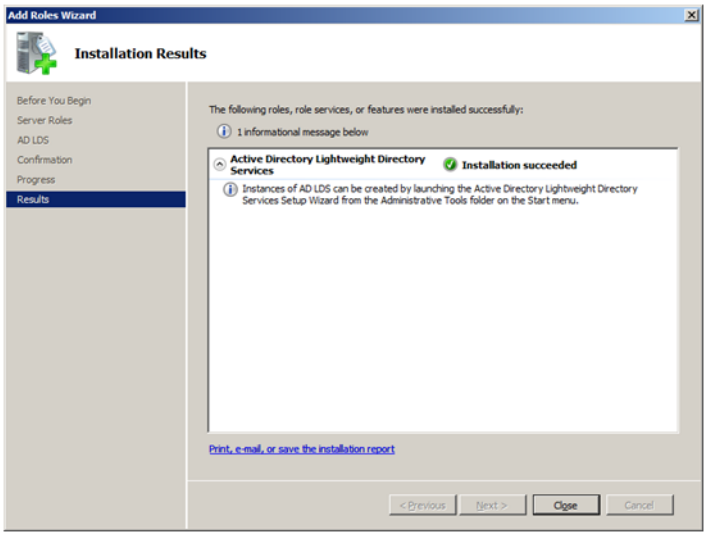


2. Click on **`Add Roles`**



3. Add the **AD LDS Role**





5.2 Create new AD LDS instance

To create a new AD LDS instance:

1. Call up, in the Active Directory Lightweight **Directory Services Control Panel**, the **AD LDS Setup Wizard**.

2. Start the wizard:

3. Select the `A unique instance` option.

4. Give the instance a name.

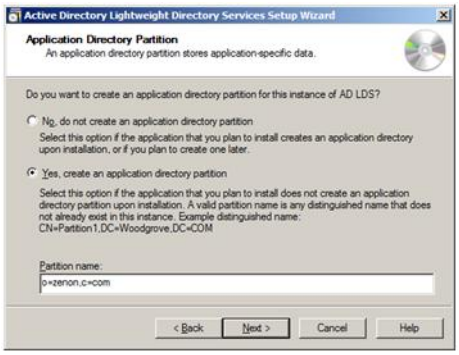
5. Configure the ports. Default:
   - LDAP: `389`

- SSL: `636`

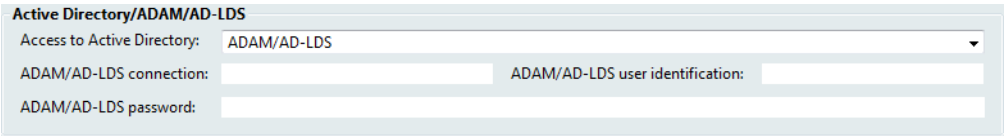
Note: If you change the pre-set port here, you must also amend the port in some of the following settings.

6. Specify the **`Partition Name`**.

In our example: `o=zenon,c=com`



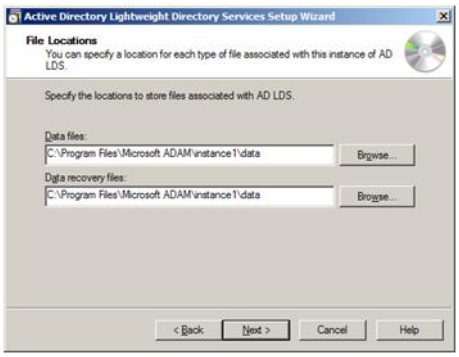
The **`Partition Name`** is used together with the port and the server name later in zenon.



This configuration can also be set up later in zenon. Continue with configuration in the wizard.

7. Define the save location.

   The setting can be left as the default setting.



8. Define the service account for AD LDS.

In our example: **`Network service account`**

If the computer on which AD LDS is installed is not a member of a domain, you receive a warning message:

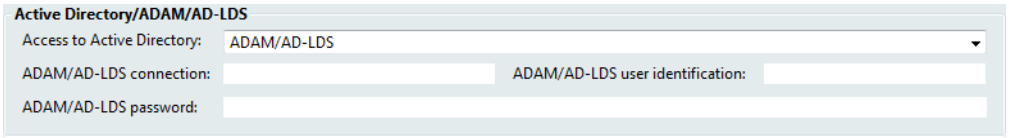
This does not impair the functionality of AD LDS. Exception: You use the Replication function.

Confirm the warning by clicking on the **`Yes`** button.

9. Define the user who receives administrator rights.

In our example, we use `Currently logged on user`. In our case, a local user with administrator rights.

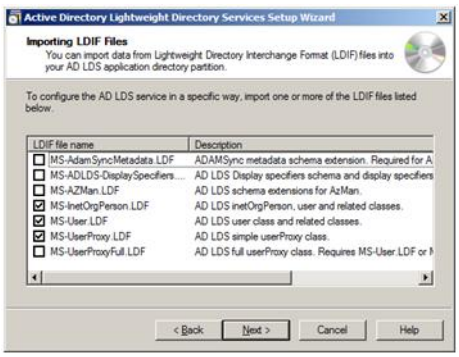
The user and their password are used later in zenon.



This configuration can be set up later. Continue with configuration in the wizard.

10. Import the required LDIF files:

    - **`MS-InetOrgPerson.LDF`**
    - **`MS-User.LDF`**
    - **`MS-UserProxy.LDF`**



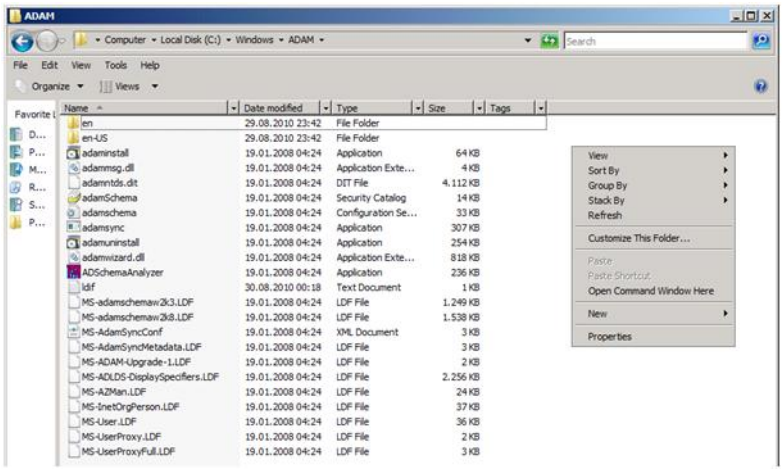
11. Finish the installation

5.3 Importing an AD LDS schema

To import the AD LDS schema:

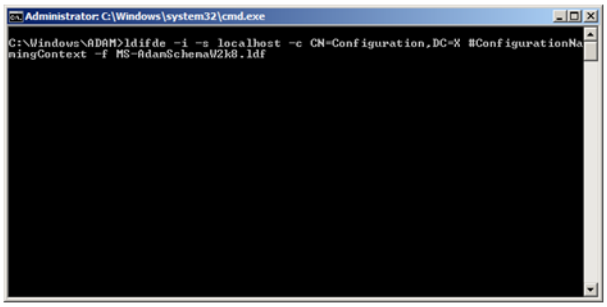
1. In Windows Explorer, navigate to the `%WINDIR%\ADAM` folder.

2. Select [`Shift key + right mouse click`] in the context menu: **`Open input request here.`**

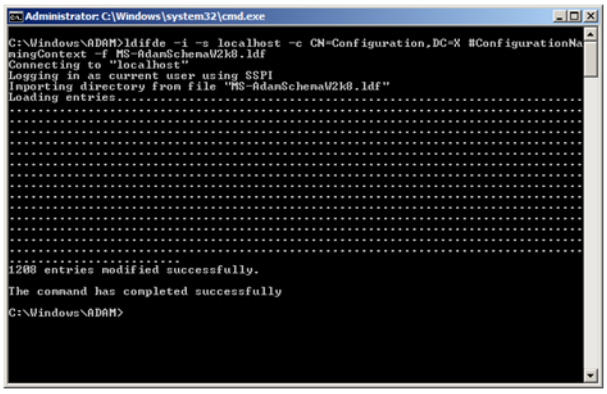


3. Enter the following character string:

`ldifde -i -s localhost -c CN=Configuration,DC=X #ConfigurationNamingContext -f MS-AdamSchemaW2k8.ldf`



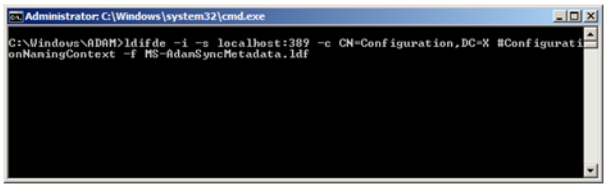
4. Press the Return key:



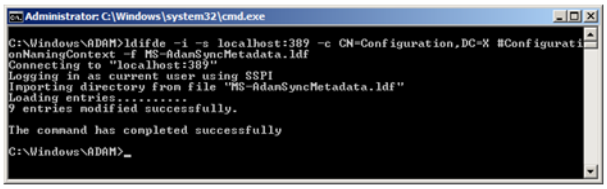
5. Enter the following character string:

ldifde -i -s localhost:389 -c CN=Configuration,DC=X #ConfigurationNamingContext -f MS-AdamSyncMetadata.ldf

Note: If you have changed a port, it must be amended here accordingly.



6. Press the Return key:



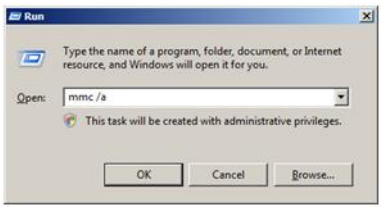
5.4 Configuring the AD Snap-in schema

To configure the Snap-in schema, first register using the command prompt (administrator rights are required):

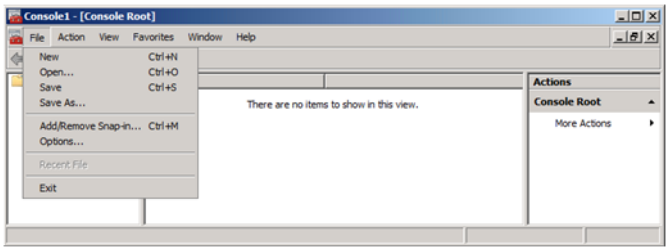
1. Click on the **Start** button
2. Navigate to **Command prompt**
3. Select `Run as administrator` in the context menu
4. At the command prompt, enter: **regsvr32 schmmgmt.dll**
5. Confirm by pressing the **Return** key

CONFIGURATION

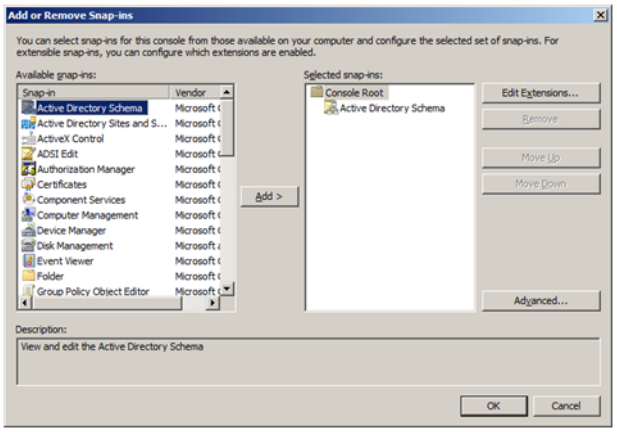
1. Click on the **Start** button
2. Open **Run**
3. Enter: **mmc /a**



4. Click on *File -> Add/Remove Snap-in...*

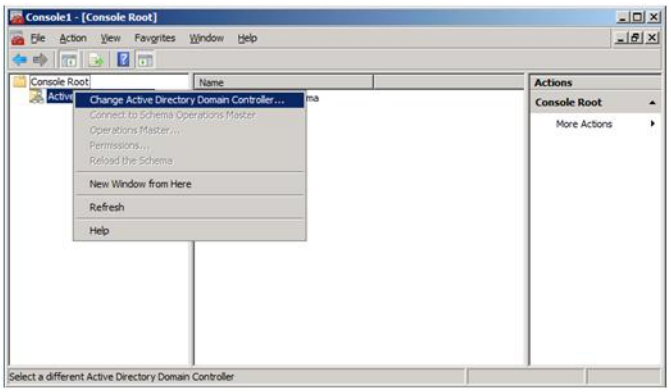


5. Select **Active Directory Schema**
6. Click on **Add**
7. click on **OK**

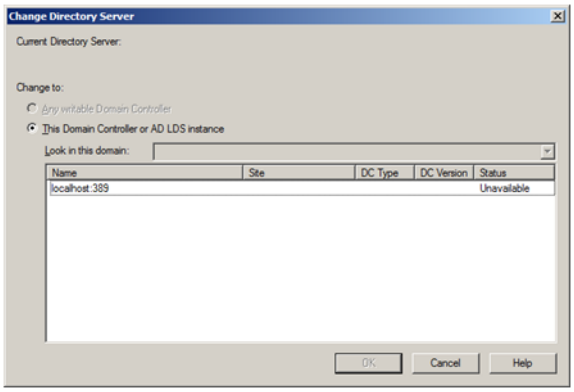


8. Navigate to **Active Directory Schema**

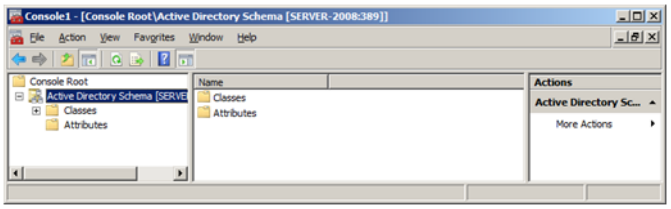
9. Select `Change Active Directory Domain Controller...` in the context menu



10. Enter the server and port (`localhost:389` in this example)

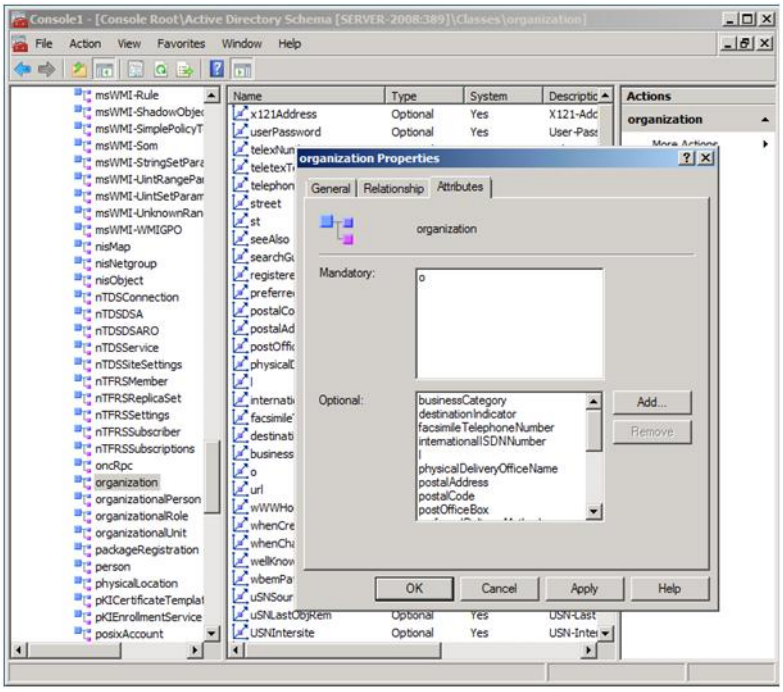


11. You should now see this window:



12. Navigate to *Classes -> organization*

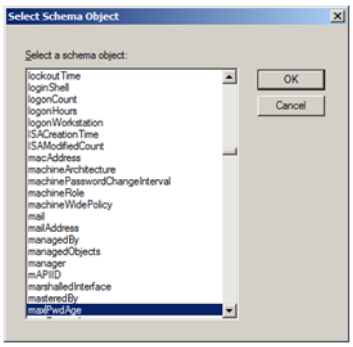
13. Open **Properties**



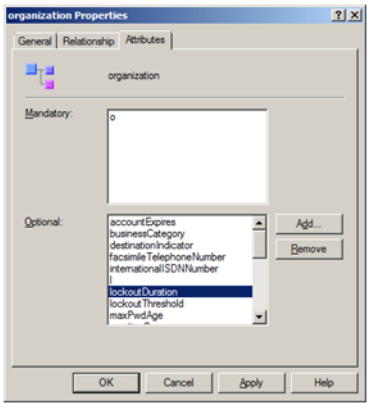
14. Click on **Add**

    a) Search for `maxPwdAge`

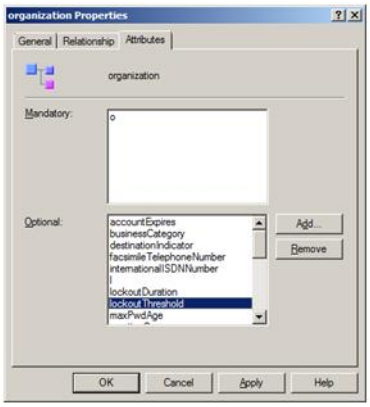
    b) click on **OK**



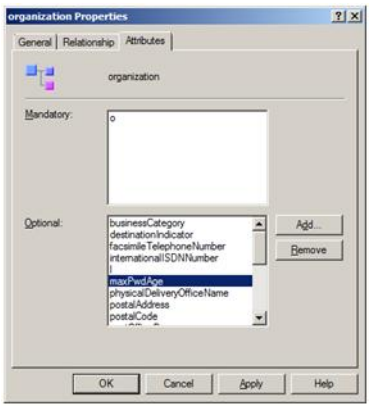
c) Repeat this step for `lockoutDuration`



d) and for `lockoutThreshold`



15. click on OK

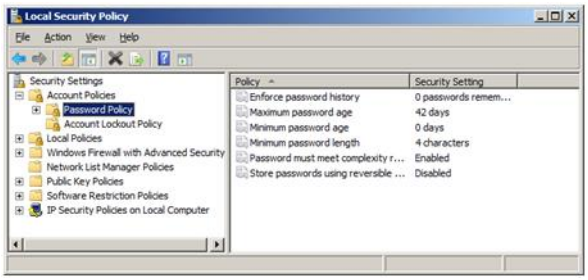


These steps are absolutely necessary to have `maxPwdAge` available in the organization unit (on page 58), which is configured next.

- `maxPwdAge` defines the maximum password age; the password must be changed after this time.
- `lockoutDuration` defines how long a user is locked out for after they have repeatedly entered their password incorrectly.
- `lockoutThreshold` defines the number of possible failed attempts before a user is locked out for a certain period.

In the local security guidelines, you define the regulations for:

- `Password complexity`
- `Minimum password length`
- `Age`



5.5 Configure organization units, groups and users

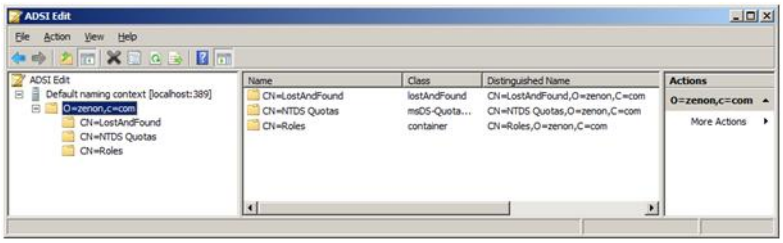
To configure organization units, groups and users:

1. Open *Start -> Administrative Tools -> ADSI Edit*

2. Select `Connect to...` in the context menu

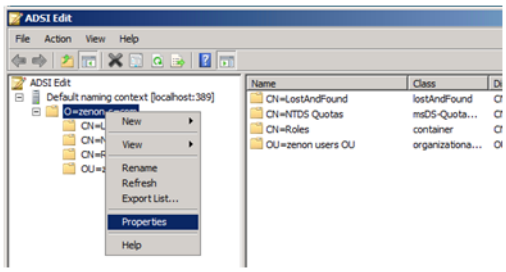
3. Use the following settings (change other settings if they have been set up previously):
   a) `Connection Point: o=zenon,c=com`
   b) `Computer: localhost:389`

You should now see the following configuration:



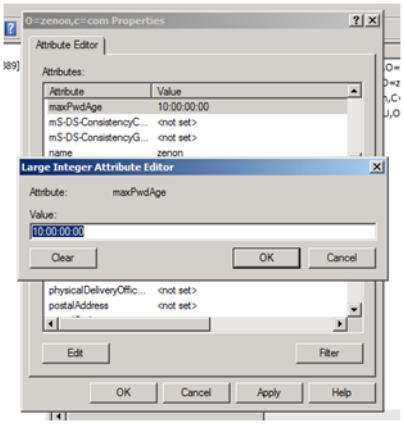
CONFIGURING MAXPWDAGE

1. Highlight **`O=zenon,c=com`**
2. Click on **`Refresh`**
3. Close **`ADSI Edit`**
4. Open **`ADSI Edit`** again
5. Highlight **`O=zenon,c=com`**
6. Select **`Properties`** in the context menu.



7. navigate to `maxPwdAge`
   a) Enter a valid value

b) Format: `DD:HH:MM:SS` (in our example `10:00:00:00`)

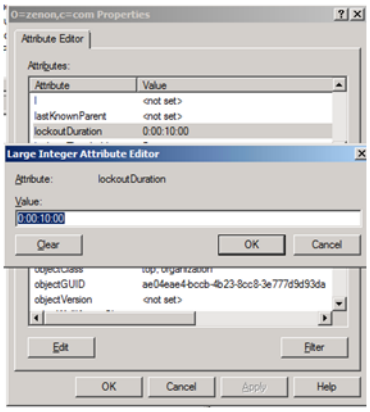


Note: If the `maxPwdAge` property is not visible, check to see that it has been correctly added (on page 50). A refresh, or closing and opening **`ADSI Edit`** or reloading the schemas may rectify the problem.

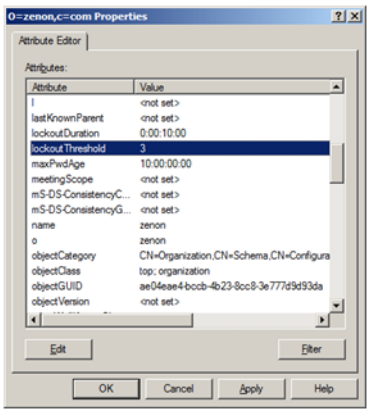
8. Navigate to `lockoutDuration`

   a) Enter a valid value

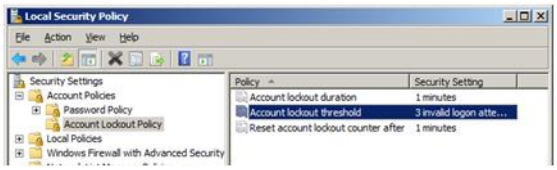
   b) Format: `DD:HH:MM:SS` (in our example `00:00:10:00,` -> 10 minutes)



9. Navigate to `lockoutThreshold`



10. Enter the same value as in the local security guidelines (`3` for example)



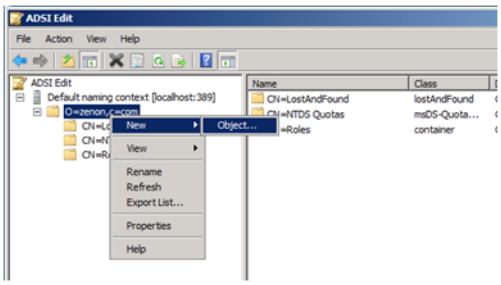
Note: The settings for the duration of the account block are ignored in AD LDS. The `lockoutDuration` property (`O=zenon,c=com`) is used.

5.5.1 Organization units

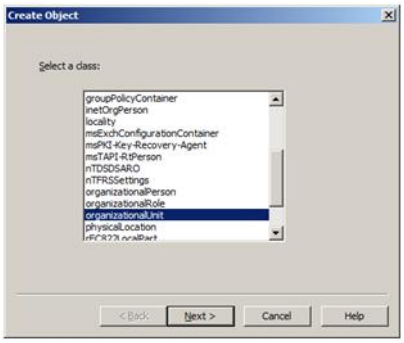
To create an organization unit:

1. Highlight **`O=zenon,c=com`**

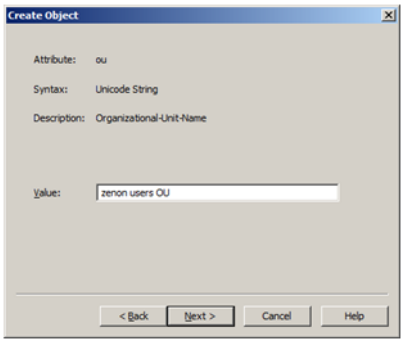
2. Select *New -> Object* in the context menu



3. Select **organizationalUnit**



4. Enter a name (in our example: `zenon users OU`)



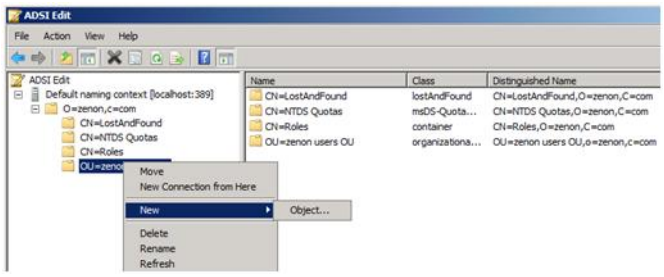
5. Click on **Next** and then in **Finish**

5.5.2 groups

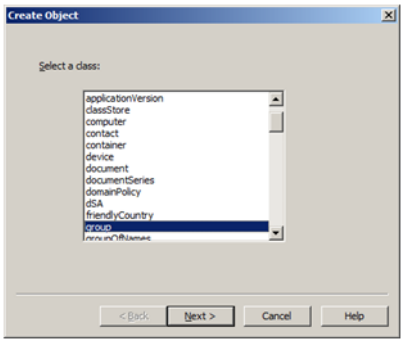
To create a group:

1. Highlight the organization unit (on page 58)

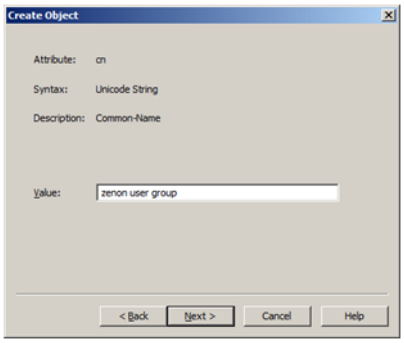
2. Select *New -> Object* in the context menu



3. Select **`group`**



4. Enter a name (in our example: **`zenon user group`**)



5. Click on **`Next`**

6. Switch to the **`Attributes`** tab

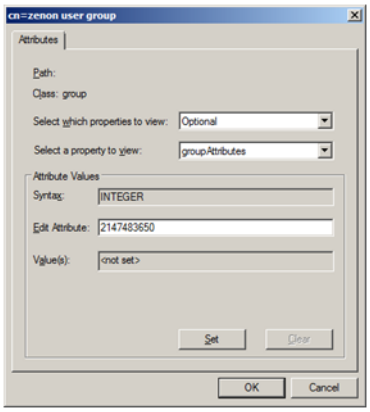
7. Click on **`More attributes`**

   a) Navigate to `Select a property to view`

   b) Select `groupAttributes` in the drop-down list

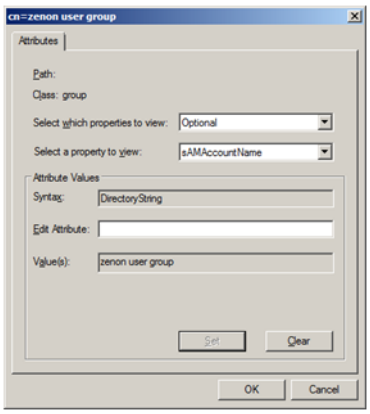
   c) Navigate to `Edit Attribute`

d) Enter the value `2147483650` (represents an **`account group`**)



8. Click on **`Set`**
9. Now select `sAMAccountName` in `Select a property to view`
10. Enter the same value as for the group (**`zenon user group`**)

Note: This setting is necessary in order for the user groups in zenon to be configured



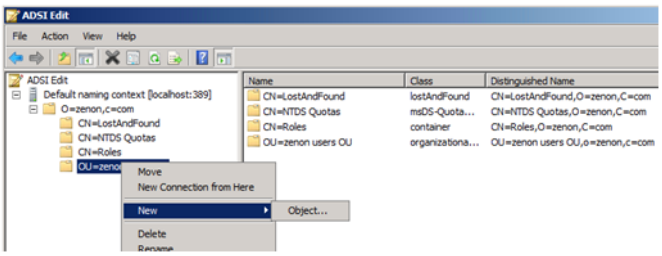
11. Click on **`OK`** and then in **`Finish`**

5.5.3 Users

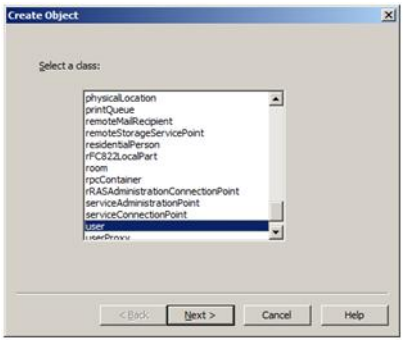
To create a user:

1. Highlight the organization unit (on page 58)

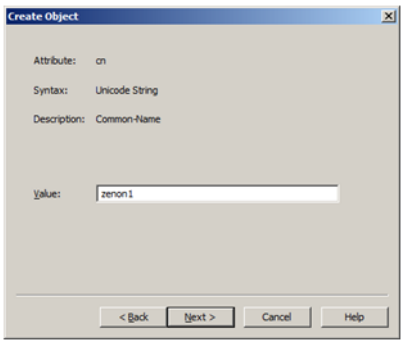
2. Select *New -> Object* in the context menu



3. Select the **`User`** class



4. Enter a name (in our example: **`zenon1`**)



5. Click on **`Next`**

6. Switch to the **`Attributes`** tab

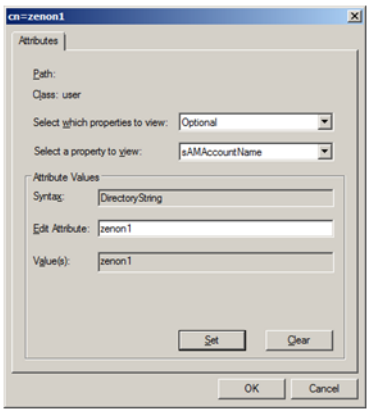
7. Click on **`More attributes`**

   a) Navigate to `Select a property to view`

   b) Select `sAMAccountName` in the drop-down list

   c) Navigate to `Edit Attribute`

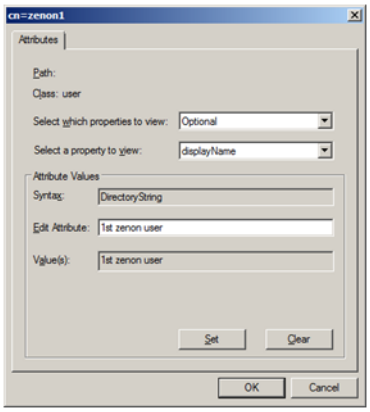
d) Enter the same value as for the user (`zenon1`)
(this configuration is necessary in order for the user to be able to be used in zenon.)



8. Click on **`Set`**

9. Now select `displayName` in `Select a property to view`

10. Enter a value for the display of a name, such as **`1st zenon user`**



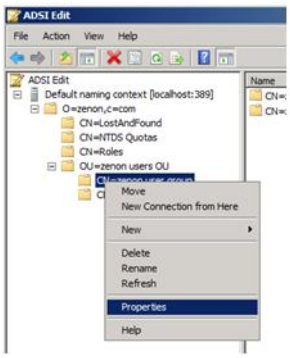
11. Click on **`Set`**, then on **`OK`** and on **`Finish`**

ADDING A USER TO THE GROUP

To add users to a group:

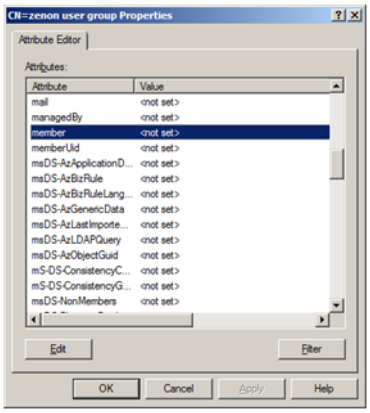
1. Select **`zenon user group`**

2. Select **Properties** in the context menu.



3. Highlight **member**

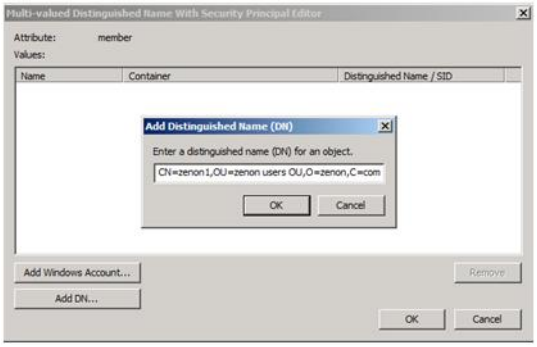
4. Click on **Edit**.



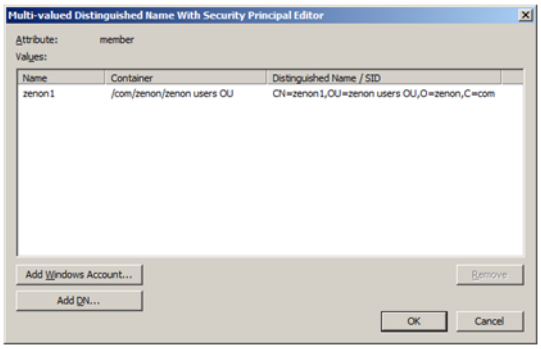
5. To add (**user**) to the AD LDS account that was created beforehand:

   a) Click on **Add DN...**

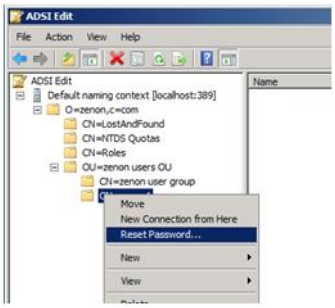
   b) At the input field, enter: `CN=zenon1,OU=zenon users OU,O=zenon,C=com`



c) You receive the result:

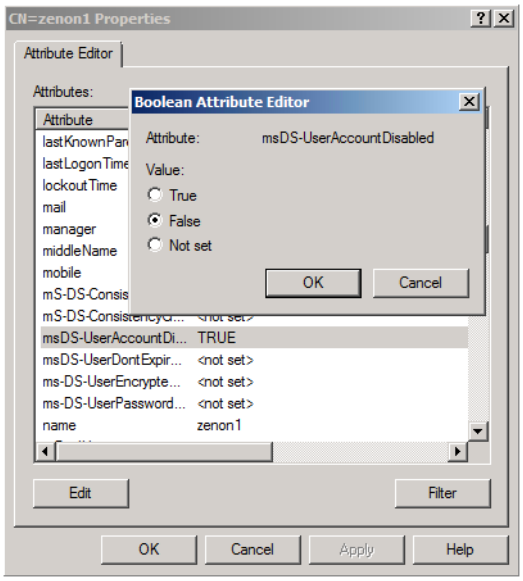


6. Define a password for the user **zenon1**



Note: the password must meet the requirements of the local security guidelines

7. Set the the `set msDS-UserAccountDisabled` property to `False` for user zenon1



The user has now been created and can be used in zenon.

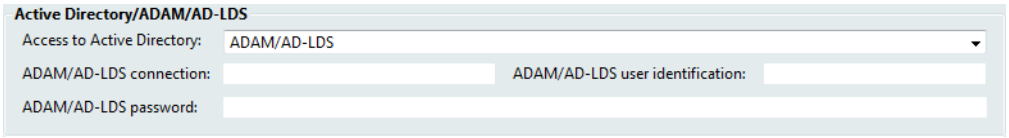
5.6 Use in zenon

For use in zenon, first configure the settings in the Editor (on page 66) and then set the user identification at AD LDS level to Runtime (on page 67).

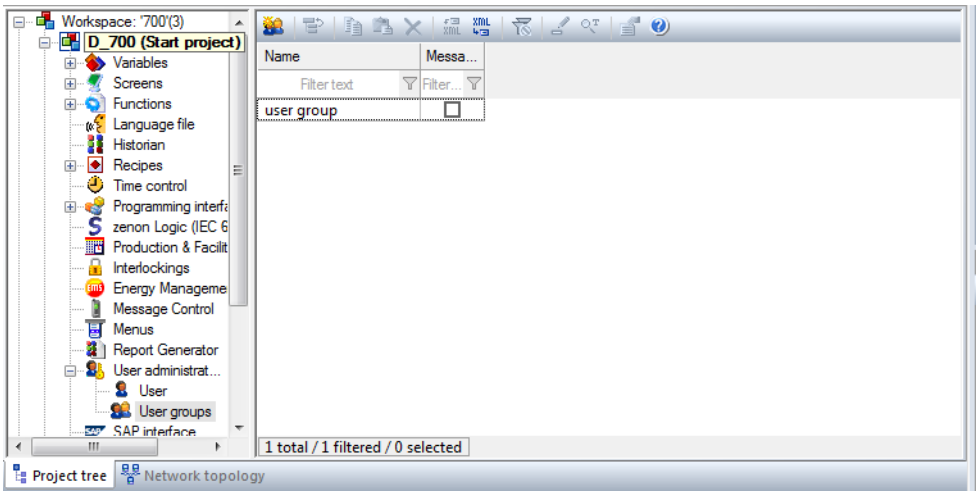
> **Info**
>
> *Active Directory and ADAM/AD LDS are not available with Windows CE.*

5.6.1 Editor

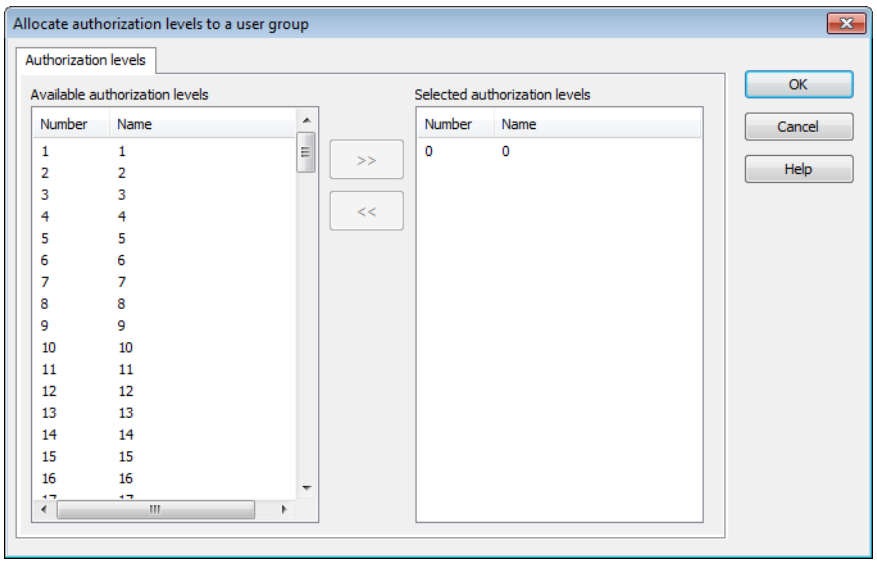
Configuration is carried out in the project properties in `User administration`:



- A user group with the name `zenon user group` was created

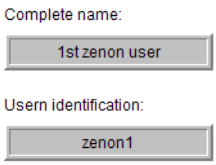


- and authorization levels were added

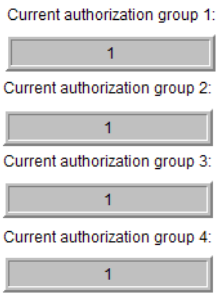


5.6.2 Runtime - system driver variables

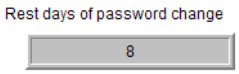
- The user zenon1 can log in to zenon:



- The user receives their authorization levels from the zenon group:



- The remaining days until the password must be changed are displayed (with a day's difference):



TROUBLESHOOTING

If errors in Runtime occur, check if:

- The settings have been set up correctly:
  - Username
  - sAMAccountName
- The firewall settings have been set up correctly:
- The Editor configuration is correct for:
  - Connection
  - Password

If the user does not receive any authorization levels from the zenon group, check if:

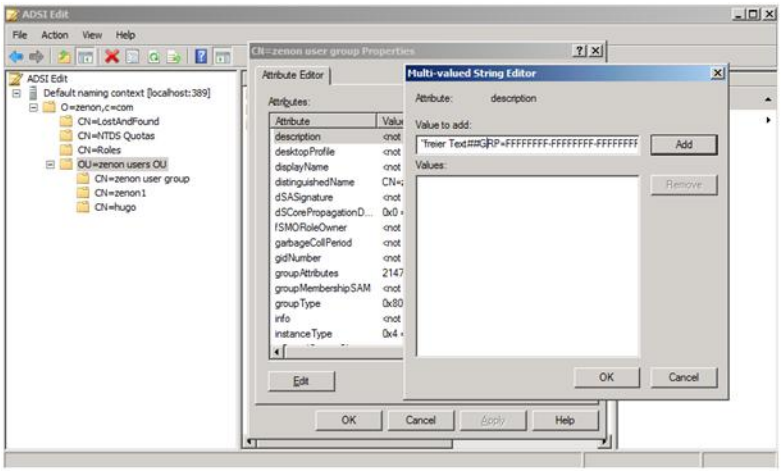
- The names correspond to each other
- sAMAccountName of the group in **AD LDS** was set
- The user in AD **LDS** was added to the group

AD/ADAM

If operating authorizations from the user group in **AD/ADAM** are to come, the following must be the case in **AD LDS**:

- The `description` property must be amended for the group

- The group must have the exact same name as the project



For further information, see the Setting the zenon authorization levels in the description field of an Active Directory group (on page 30) section.

5.7 AD LDS with Windows 7 and Windows Vista

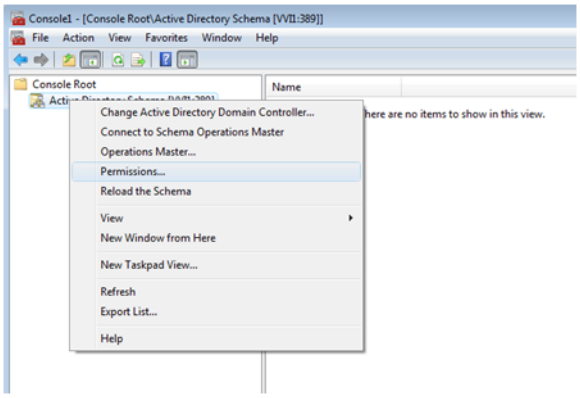
AD LDS can also be used with Windows Vista and Windows 7. You can find the setups for these on the Microsoft website http://www.microsoft.com/downloads/en/default.aspx.

After installation, configuration is carried out via *System control-> Administration* in the same way as the description for Windows Server 2008 (on page 41).

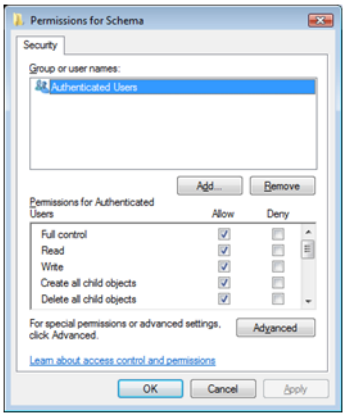
5.7.1 Problem handling under Windows Vista/Windows 7

If no content is displayed after the Active Directory schema is opened, the access rights must be amended. To do this:

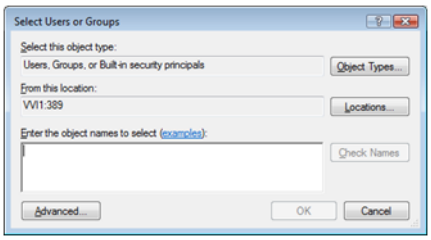
1. Select **Permissions...** in the context menu.



2. Allocate the required users with the necessary rights (add new users by clicking on **Add**)



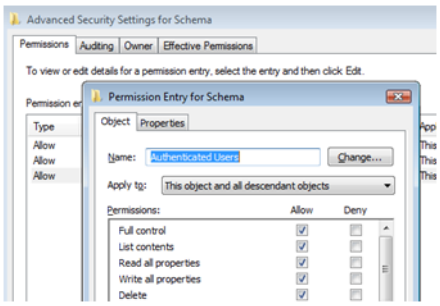
3. Click on the **Advanced** button



4. Click on the **Advanced** button

5. Open the **Permissions** tab

6. Activate the `Apply to this object and all descendant objects` option for the respective user



7. Close the console and open it again (**`mmc /a`**) for further configuration

6. Active Directory Application Mode - ADAM (for Windows XP)

Active Directory Application Mode (ADAM) is designed for use with Windows XP.

For

- Windows Vista
- Windows 7
- Windows Server 2008

Use Active Directory Lightweight Directory Services (on page 41)

REQUIREMENTS

In order to be able to use Active Directory Application Mode for zenon, you must pay attention to the following points when configuring ADAM.

1. Create a new ADAM instance (on page 72)
2. Bring in an AD schema (on page 75)

3. In order to make access possible for the ADAM user, click *Program -> Administration -> Local security guidelines*. In the following dialog click *Security settings -> Account guidelines*. Define the desired settings for password guidelines and account blocking guidelines.
4. Configure the ADAM Snap-in (on page 76) schema.
5. In Snap-In make a right-click under Classes -> Organization and select properties. On tab **Attribute** enter `maxPxdAge` as optional attribute. With this you make sure that the password validation and the password change work analog to the Active Directory.

Note: You must enter the validity period of the password in nanoseconds.

6. Create user and user groups in ADAM. Pay attention to the following:
   - At the user and at the user group you must enter the name again manually under Property -> Attribute-Editor at the Attribute `sAMAccountName`.
   - At the user group you must enter the name as described in Using the Active Directory (on page 28).
   - You can create the zenon authorization levels as described in Using the Active Directory (on page 28) under attribute`description`.

> **Info**
>
> *In order to display the user name with the help of the system driver variable, you must set the user name manually in ADAM at the user under Properties -> Attribute-Editor at the Attribute `displayName`.*

6.1 Create new instance of ADAM

THIS IS HOW YOU INSTALL AN INSTANCE OF ADAM USING THE ACTIVE DIRECTORY APPLICATION MODE SETUP ASSISTANT

- Click on start to launch the Active Directory Application Mode setup assistant, show all programs and then on ADAM, and then click on Create ADAM instance.
- On the welcome page, click on Next.

- On the set up options page, you can choose if you wish to install a separate ADAM instance or would like to assign an existing configuration to a new instance. Because you are installing the first ADAM instance, click on install separate instance Click on "Next" after this.
- On the Instance name page, enter a name for the ADAM instance to be installed. The name is used to clearly identify the ADAM instance on the local computer. Then click on Next.
- On the Ports page, enter the communication ports that are to be used by the ADAM instance. ADAM can communicate using LDAP (Lightweight Directory Access Protocol) or SSL (Secure Sockets Layer). You must therefore give a value for both ports. Then click on Next.

> **Info**
>
> *If one of the standard ports is already used on the computer on which you install ADAM, the Active Directory Application Setup Assistant automatically looks for the next available port, starting with 50000. For example, ports 389 and 636, as well as ports 3268 and 3269 are used on global catalog servers. Therefore, when installing ADAM on a domain controller, the standard values 50000 for the LDAP port and 50001 are assigned to the SSL port.*

- On the Application directory partition page, you can create an application partition or a name context) by clicking on Yes, create application directory partition. If, you click on No, do not create application directory partition you must create an application partition manually after installation. If you create an application partition, you must enter a defined name for the new partition. Then click on Next.

> **Info**
>
> *ADAM supports defined names in X.500 and in DNS style (Domain Name System) for upper level directory partitions.*

- On the File path page, you can display and amend the installation directories for ADAM files and recovery files (protocol files). ADAM files and recovery files are saved under %ProgramFiles%\Microsoft ADAM\Instanzname\data by default. In doing so, Instance name displays the ADAM instance name that you enter on the Instance name page. Click on Next, to import the standard paths.

> **Info**
>
> *When installing ADAM on a computer under Windows XP, you must install these files on the same logical volume. When installing ADAM under Windows Server 2003 and Windows Server 2003 R2 in a production environment, it is recommended that you install the files on separate physical data carriers.*
>
> *Program files and administration programs are installed by ADAM in %windir%\ADAM.*

- On the Select service account page, select an account that is used as a service account for ADAM. The selected account determines the security context in which the ADAM instance is executed. If you do not install ADAM on a domain controller, the network service account of Active Directory Application Mode Setup Assistant is used by default. Click on Next, to import the Network service account standard setting. When installing ADAM on a domain controller, click on This account instead and then select a domain user account as an ADAM service account.

> **Info**
>
> *You can change the ADAM service account after installing ADAM with the command line program dsmgmt. When installing ADAM on a domain controller, you must select a domain user account as an ADAM service account.*

- On the ADAM administrators page, select a user or a group as a standard administrator for the ADAM instance. The selected user or selected group has full administrator functionality for the ADAM instance. As standard, the current registered user is given by the Active Directory Application Mode Setup Assistant. You can change this selection in each local account or domain account or in each group in the network. Click on the standard value Current registered user, and then click on Next.
- You can import two LDF files with user class object definitions into the ADAM scheme on the Import LDIF file page. Importing user class object definitions is optional.
  - Click on Import selected LDIF file for this ADAM instance.
  - Click on MS-InetOrgPerson.LDF and then on Add.
  - Click on MS-User.LDF and then on Add.
  - Click on MS-UserProxy.LDF,on Add and then on Next.

- On the Ready for installation page, you can verify the selected installation options. If you click on Next, the Active Directory Application Mode Setup Assistant starts by copying the files and installing ADAM on the computer.
- If the Active Directory Application Setup Assistant has successfully finished installing ADAM, the following message is shown: "The Active Directory Application Setup Assistant mode was concluded successfully." If the Finish assistant page is displayed, click on Finish to close the assistant.

> **Info**
>
> *If the Active Directory Application Setup Assistant is not successfully concluded, the reason for the error is displayed on the Summary page.*

- If an error occurs in the Active Directory Application Assistant, before the Summary is opened, you can verify the error message displayed. Furthermore, you can click on Start and then on Execute and enter one of the following filenames:
  %windir%\Debug\Adamsetup.log
  %windir%\Debug\Adamsetup_loader.log
  . The files %windir%\Debug\Adamsetup.log and %windir%\Debug\Adamsetup_loader.log contain useful information for dealing with problems in relation to ADAM setup errors.

6.2 Input AD scheme

This is how you use the Active Directory/ADAM synchronization program for the first time

- click on **Start**,
- Open **All Programs**,
- Click on **ADAM** and
- then on **ADAM administration programs**:

A command window in the ADAM directory opens.

To extend the ADAM schema to the standard schema objects of Windows Server in Active Directory:

- Enter the following command on one line of the command prompt:

```
ldifde -i -s localhost -c CN=Configuration,DC=X #ConfigurationNamingContext -f MS-AdamSchemaW2k8.ldf
```

- Press the Return key.

6.3 Configure ADAM scheme snap-in

CONFIGURING THE ADAM SCHEME SNAP-IN ADMINISTRATION PROGRAM.

You can administer the ADAM scheme with another ADAM administration program, the ADAM scheme snap-in. If you have already used the Active Directory scheme snap-in, you should be familiar with the ADAM scheme. Before you can use the ADAM scheme snap-in, you must create an MMC file for it, as described in this process.

- Click on start, then on Execute, enter mmc /a and then click on OK.
- In the file menu, click on Add/remove snap-in and then click on Add.
- Click on the independent snap-ins available in the ADAM scheme, on Add, on Close and then click on OK.
- To save this console, click on Save in the File menu.
- Enter the following filename and then click on Save:
  %windir%\system32\adamschmmgmt.msc
- Create a connection to the ADAM instance using the ADAM scheme snap-in. To do this, right click on ADAM scheme in the console structure and click on change ADAM server. Enter `localhost` at ADAM server and `389` at Port.
- Click on OK. The ADAM scheme snap-in now looks as follows. You can search through and display the classes and attributes of the ADAM scheme.
- To create a link for the ADAM scheme snap-in start menu, carry out the following actions:
  - Right click on Start, click on Open – all users, double-click on the folder programs, and double-click on the ADAM folder.
  - Move to New in the file menu, and then click on link.
  - In the assistant to create links, enter adamschmmgmt.msc as the save location for the element and then click on Next.
  - On the select program description page, enter the name for the link and the name of the ADAM scheme, and then click on Finish.

7. Operating during Runtime

Each user has the possibility to change his own password. But he cannot edit another user. Only an administrator can do that. Changes in Runtime must be read back in the Editor, in order to be available there. Note the `RT changeable data` property when transferring Runtime files. Here, it is specified whether the configuration of the user administration is transferred to Runtime and overwrites the configuration in Runtime.

The administrator can use the **`Change User`** function to:

- Create new users
- Amend existing users (except user name for log-in)
- Create, amend or delete user groups

  If an administrator creates a new user group in Runtime, they are automatically a member of this group.
- Issuing authorization levels

  The administrator can only give users authorization levels that they have. This avoids, that an administrator opens the entire system to himself.

Note: User and user groups from the Editor global project are combined with the users and user groups of the project. They can neither be edited in Runtime, nor read back in the Editor.

> **Attention**
>
> *Compliance with FDA 21 CFR Part 11:*
>
> - Neither user nor administrator can change the user name in the Runtime.
> - Deleting users can be prohibited in the project settings with the help of the `Deleting users` property in the `User administration` group.

LOGIN

The current user `SYSTEM` will be logged in with the approved user level `LEVEL 0` after Runtime is started.

Logging in in the Runtime has the following safety precautions:

- Password

A user is locked after having entered a wrong password three times and he is logged out automatically. Therefore no elements of the system can be operated if they require an authorization level higher than `0`. They also cannot carry out any operations linked to a user level.
The following message is displayed:

The administrator then has to unlock this user (deactivating the property **`Locked`**).

The user name of a user trying to log in incorrectly is logged in the Chronological Event List.

- Username

When entering a non-existent user name or no password, the error message '**`Invalid user name`**' is displayed. After three unsuccessful attempts, the system is blocked for all elements that require a higher authorization level than `0`. No user is therefore in a position to carry out protected operations with a user level. Only the administrator can unlock the system.

The user name of a user trying to log in incorrectly is logged in the Chronological Event List as an event for the user that is currently logged in.

- Logging in after deactivation

If an user is deactivated and he tries to log in, this is not possible. This attempt is logged in the Chronologic Event list.

PASSWORD

The user himself is the only one knowing his password. And he is the only one able to change his password. Once the user has been given a password by the Administrator, they must change it when they first log in. This makes sure, that no administrator knows user passwords und thus could effect wrong signatures. (Important for FDA 21 PART 11).

If an user forgets his password, the administrator can delete his password und enter a new initial password. To do this the administrator does not have to know the password. The user must change their password the next time they log in.

For more information on changed Runtime files see also chapter: Project and workspace / RT changeable data

Attention

Login via screen of type ***Login****: If, when logging in via a* ***Login*** *screen (on page 85), no password is entered for a valid user, you do not receive an error message. The user is not logged in. Even after three failed login tries with no password entered the system is not logged.*

If entering a wrong password and/or a not existing user name, the system is locked after three tries as usual.

7.1 Permanent and temporary login

Users can be logged in permanently or temporarily.

PERMANENT LOGIN

Permanent Login is carried out using the `Log in with dialog` Function (on page 81) or the `Login without password` Function (on page 82). The user is thus permanently logged in and can carry out all operations that they are authorized (on page 16) to do. For actions that the user is not authorized to carry out, a message is shown accordingly.

Hint: Password-protected buttons can be made invisible for logged-in users. To do this, the `Locked buttons` property (`Project properties` -> `User administration` -> `Temporary log in`) must be activated.

Note: Temporary login is not possible for logged-in users. Logged-in users therefore do not receive a dialog to log in temporarily for functions for which they do not have sufficient authorization.

TEMPORARY LOGIN

If an operation that requires authentication is necessary for a user who is not logged in, they can be logged in temporarily. To do this, the `Temp. login active` property (-> `User administration` -> `Temporary log in`) must be switched to active.

Login in Runtime:

- The dialog to log in is opened when a password-protected function is executed

- The user can log in and execute the operation according to their rights or they receive a message on missing rights
- The user is logged out immediately after the operation

> **Info**
>
> *Temporary login:*
>
> - Is only effective after the function is executed
> - Supports switches, but not buttons
> - Is deactivated for permanently logged in users

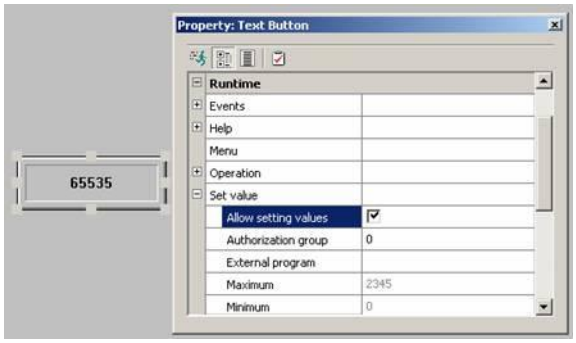
7.2 Password protection for dynamic elements

All dynamic elements that either execute a function or allow the setting of values can be linked to an authorization group for the Runtime.

Create a dynamic element. E.g. a text button. In the properties window the properties of the element are displayed.

In the group 'User' select the property '`Authorization group`'. Here the authorization group necessary to execute the function can be defined.

In dynamic elements where the setting of values should be secured, a variable has to be linked and the property "Allow setting values" has to be activated in the properties window, before the authorization group can be defined.



7.3 Password - Functions

7.3.1 Login with dialog

This function opens the log-in field to log-in to zenon again.

This attempt is logged in the Chronologic Event list.

A Login (on page 85) screen can also be used for login.

SIZE AND POSITION

The size and position of the login window in Runtime can be defined in **zenon6.ini**:

1. Open zenon 6.ini
2. Create or modify the area:

```
[Command initiation]
```

3. Enter a value for

```
POSITION= left, right, top, bottom
```

Default: **POSITION= 0.001, 0.999, 0.835, 0.964**

Attention: The size relates to the screen size and not the size of the main window.

Info

You can find zenon6.ini in the following path:

Windows Vista/7: `C:\ProgramData\COPA-DATA\System\`

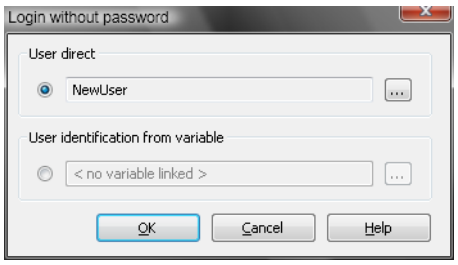
Windows XP: `C:\Dokumente und Einstellungen\All users\Anwendungsdaten\COPA-DATA\System`

7.3.2 Login without password

The function makes it possible to log in a user to zenon without a password in the Runtime. For this the user is directly named or logged in via Chip Ident System. This function can be executed by an event (status of a key) or by time control. The login is logged in the Chronologic Event List.

In order to create the function login without password:

- create a new function
- navigate to node User administration
- select Login without password
- the dialog for the selection of user opens
- select the type of log in



Parameters	Description
`User direct`	Logs in the selected user.
`User from variable`	Logs in the user with the user name from the transferred variable. Makes it possible to log in a user via a Chip Ident System. Click on button ... in order to open the dialog for selecting a String variable. For details see paragraph "Log in via Chip Ident System".

LOG IN VIA CHIP IDENT SYSTEM

The log in `User from variable` makes it possible to use Chip ident Systems such as Eucher or Keba Identsystem. In order to use the log in with a variable, pay attention to the following:

- The user must exist in the <CD_PRODUCTNAME< user administration or in the Active Directory with the same user name as in the chip.

for example: User name in the chip is J. Smith. Then there must exist a J. Smith with respective rights in the user administration or in the Active Directory.

- If the user holds his chip in front of the chip reader, the String variable (e.g. `username`) is filled with the data of the chip (e.g. J. Smith) and the user is logged in.
- In order for this to work, a **`reaction matrix`** of the type `String` must exist which reacts to each value change and executes the function.
  - This reaction matrix must be linked with the variable (e.g. username).

7.3.3 Logout

With this function the current user is logged out and the user SYSTEM with the authorization level 0 is logged in. The logout of an user is logged in the Chronologic Event List.

No transfer parameters are needed.

Attention

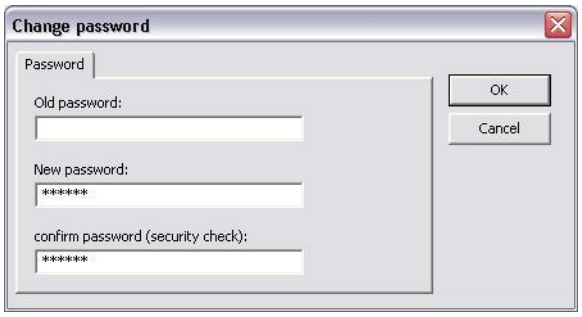
Automatic Logout vs. Automatic Function:

- `Automatic Logout`: Happens `permanently` after a certain time period has passed after the last user action
- `Automatic function`: Happens `only once` after a certain time period has passed after the last user action

7.3.4 Change password

With this function a logged in user can change his password in the Runtime. For system-internal users no changes are possible. The function then is not executed.

An entry mask will open during online operation.



Required inputs:

Parameters	Description
Old password	enter current password
New password	enter new password
Safety query	confirmation of new password

If no password has been assigned to the user, he can define it, the first time he executes the function in the Runtime. In the dialog no old password is demanded then.

7.4 Deleting an user

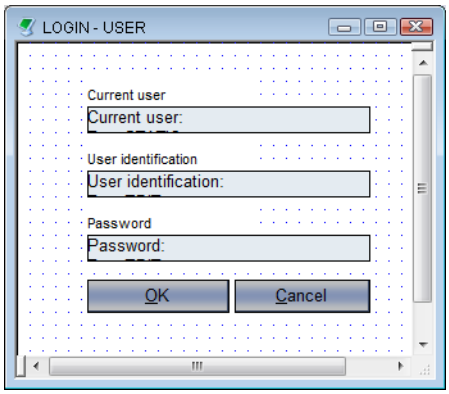
Select the user to delete in the detailview and open the context menu with a right mouse click. Execute the command **Delete** and confirm the additional confirmation dialog.

7.5 Screen of type Login

By using the screen type “Login”, it is possible to create individual login screens. (You will find more information on the pre-defined screen types in the chapter 'Screens / Pre-defined screen types'.)

The creation of the login screen is done by the definition of a new screen of the screen type **Login**.

On opening the screen an empty screen is opened and the Drop-down list **Control elements** in the menu line is filled.



Control elements:

Control element	Description
Current user	Label current user
Display - current user	Display of the currently logged in user
Identification	Label user name
Edit Identification	Input area for user name
Password	Text “Password”
Edit Password	Input field for password
OK	Button to close the screen after login
Cancel	Button for cancelation
Login	Button for logging in without closing the window

LOGIN

When logging in to the Runtime the following is true:

- After tree wrongly entered passwords, the user is locked for the system. Only the administrator can unlock the user.
- After entering a not existing user name the system is locked. The system cannot be operated by any user and must be unlocked by an administrator.
- If a correct user name is used at login but the password field remains empty no reaction happens. The system is not locked.

For details see **Operation in Runtime** (on page 77) chapter.