



©2016 Ing. Punzenberger COPA-DATA GmbH

All rights reserved.

Distribution and/or reproduction of this document or parts thereof in any form are permitted solely with the written permission of the company COPA-DATA. Technical data is only used for product description and are not guaranteed qualities in the legal sense. Subject to change, technical or otherwise.



Table of contents

1.	. Welcome to COPA-DATA help			6	
2.	User	Admini	istration	6	
3.	Engir	neering	in the zenon Editor	8	
	3.1	Project	t manager context menu	9	
	3.2	Toolba	ar and context menu detail view	9	
	3.3	Creatin	ng a user	11	
		3.3.1	Users	12	
		3.3.2	Change password	14	
		3.3.3	Message Control	15	
		3.3.4	Authorization levels	17	
		3.3.5	User groups	18	
	3.4	Create	e a user group	19	
		3.4.1	Name the user group	20	
		3.4.2	Authorization levels	21	
		3.4.3	Order in Message Control	22	
	3.5	Editing	g an user	23	
	3.6	Changi	ing a user group	23	
	3.7	7 Changing the names of the authorization levels			
3.8 Function authorizations		24			
		3.8.1	Configuration of function authorizations	25	
		3.8.2	Function authorizations Runtime	26	
		3.8.3	Function authorizations Editor	34	
	3.9	Screen	n types, dialogs and functions for login and user administration	37	
		3.9.1	Creating a screen of the type Login	38	
		3.9.2	Creating a user list screen	41	
		3.9.3	Creating a user group list screen	49	
		3.9.4	Create Edit user screen	53	
4.	zeno	n login	and user administration in Runtime	63	
	4.1	Login p	process and administration	64	
	4.2	User lo	ogin	67	



		4.2.1	Permanent login	67
		4.2.2	Temporary login	67
		4.2.3	Automatic login and logout for subprojects	70
		4.2.4	External authentication	71
	4.3	Adminis	ter users and user groups	71
	4.4	Screen t	types to administer users and user groups	72
		4.4.1	User list	73
		4.4.2	User Groups List	74
		4.4.3	Edit users and change password	74
	4.5	Function	ns for the user administration module	77
		4.5.1	Login with dialog	77
		4.5.2	Login without password	78
		4.5.3	Logout	79
		4.5.4	Change user	80
		4.5.5	Change password	. 101
	4.6	Passwoi	rd protection for dynamic elements	. 101
	4.7	Accept	changes in the Editor in Runtime	. 102
5.	Admi	nisterin	g Active Directory users from zenon Runtime	102
	5.1	Creating	g an Active Directory user administration screen	. 103
	5.2	Screen	switching to Active Directory user administration	. 105
	5.3	Adminis	ter Active Directory users in Runtime	. 109
		5.3.1	Manage organization unit	. 112
		5.3.2	Managing users	. 113
		5.3.3	Managing user groups	. 120
6.	Exter	nal user	administration with Microsoft Active Directory	123
	6.1	Active D	Pirectory (AD)	.124
		6.1.1	General	. 125
		6.1.2	Setting the zenon authorization levels in the description field of an Active Directory group	.125
		6.1.3	The same user groups in zenon and in Active Directory	. 127
		6.1.4	Active Directory extension scheme	. 127
		6.1.5	Schema extension – details	.132
				122
		6.1.6	Schema	. 132
		6.1.6 6.1.7	Configuration	



7.	abou	t AD/AD	LDS properties used in zenon	204
		6.3.3	Configure ADAM scheme snap-in	. 203
		6.3.2	Input AD scheme	. 202
		6.3.1	Create new instance of ADAM	. 200
	6.3	Active D	Directory Application Mode - ADAM (Windows XP only)	. 199
		6.2.5	Problem handling	. 197
		6.2.4	zenon administration with Active Directory	. 194
		6.2.3	AD LDS with Windows Server 2008	. 192
		6.2.2	AD LDS with Windows 7	. 172
		6.2.1	AD LDS with Windows 8 and Windows Server 2012	. 137
	6.2	Active D	Directory Lightweight Directory Services - AD LDS	. 137



1. Welcome to COPA-DATA help

GENERAL HELP

If you cannot find any information you require in this help chapter or can think of anything that you would like added, please send an email to documentation@copadata.com (mailto:documentation@copadata.com).

PROJECT SUPPORT

You can receive support for any real project you may have from our Support Team, who you can contact via email at support@copadata.com (mailto:support@copadata.com).

LICENSES AND MODULES

If you find that you need other modules or licenses, our staff will be happy to help you. Email sales@copadata.com (mailto:sales@copadata.com).

2. User Administration

zenon supports user administration for the Editor and for online operation Runtime. The password system fulfills the guidelines of the FDA (Food and Drug Administration, 21 CFR Part 11). It is also possible to administer Active Directory users (on page 102) in Runtime.





License information

Part of the standard license of the Editor and Runtime.

THE CONCEPT

The concept of zenon user administration assumes that different users have different operating rights (authorization levels and function authorizations). Administrators also have different rights, but have additional administrative rights, such as the administration of users. Users can be administered via zenon and the Windows Active Directory.

Each user can be assigned several different authorizations. A maximum of 128 (0 to 127) authorizations can be configured. Users can be assigned to the individual authorization levels and the attendant project-specific password design in relation to this can be created completely freely. Each user can have any level allocated. 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. Authorizations can only be issued if the administrator has those rights himself.

The user is logged in in Runtime using the login (on page 77) function and a login screen. If the user is to be logged in automatically based on an event (e.g. position of a key known to the system), the Login without password (on page 78) function is used. This function is projected with a limit value or a Rema of the variable in the variable management, respectively. With multi-project administration, users can automatically be logged in to subprojects with automatic (on page 70) login.

If during a defined period of time there is no operation, an automatic time-triggered logout can be engineered. Users can log off from the system at any time using the logout (on page 79) function. The user SYSTEM is thus logged in.

CREATING USERS AND ISSUING RIGHTS

In zenon, you can create and administer users in two ways:

- zenon Editor and Runtime:
 Users are created in the Editor and given rights. You can log in in Runtime. Administrators can also create users in Runtime and issue rights.
- 2. AD and AD LDS (on page 123):

Active Directory Lightweight Directory Services (on page 137) (AD LDS) is a simplified version of the Active Directory and is suitable for use on normal desktop operating systems; it is not necessary to use a server operating system. Active Directory (on page 124) (AD) and AD LDS can be used in zenon for the user administration in zenon Runtime. AD and AD LDS are not available for the zenon Editor.

User groups that are created in AD or AD LDS receive authorizations in zenon (on page 194), if user groups with the same name are created in zenon. A separate screen can be used to read AD and AD LDS from zenon Runtime and edit them. Users who are created here have user rights for all zenon projects, regardless of the project from which they were created.



3. Engineering in the zenon Editor

Users and user groups, passwords and authorizations are defined in the Editor. Settings can be modified in Runtime (on page 63). Not all changes in the Editor are accepted after a simple reload (on page 102). Changes in Runtime must be reloaded into the Editor in order to be able to be edited there and to guarantee the same status for Runtime and the Editor. 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 contents of the user administration are not replaced by default when transferred to Runtime.



3.1 Project manager context menu

CONTEXT MENU USER ADMINISTRATION

Menu item	Action
Editor profiles	Opens the drop-down list with predefined 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 with predefined 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 with predefined editor profiles.
Help	Opens online help.

Context menu detail view: see also User administration detail view toolbar and context menu (on page 9)

3.2 Toolbar and context menu detail view





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.
Сору	Copies the 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 after a confirmation from list.
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. Only cells that can be edited can be selected.
Replace text in selected column	Opens the dialog for searching and replacing texts.
Remove all filters	Removes all filter settings.
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.
Сору	Copies the 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 after a confirmation from list.
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. Only cells that can be edited can be selected.
Remove all filters	Removes all filter settings.
Replace text in selected column	Opens the dialog for searching and replacing texts.
Properties	Opens the Properties window for the selected entry.
Help	Opens online help.

3.3 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 toolbar select New user...
- 3. The dialog for configuration is opened
- 4. in the individual tabs define the settings for:
 - Users (on page 12)
 - Password (on page 14)
 - Message Control (on page 15)
 - Authorization levels (on page 17)
 - User groups (on page 18)



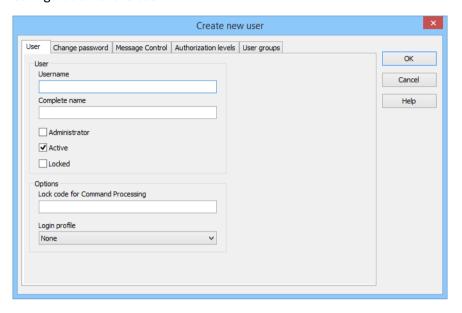
Information

Recommendation: As first user define an administrator. Only they can access all functions and therefore reactivate users who were locked because they have been blocked by the system.



3.3.1 Users

Configuration of the user:





Parameters	Description
User name	Enter the username. The user logs in to the system with his username.
	Maximum length: 20 characters.
	Note: This name must be unique.
Complete name	Enter the full name of the user. With this you can allocate a username 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 login in the Runtime.
	Note: According to FDA 21 PART 11 regulations, a user can never be deleted, so it is possible to trace who carried out which action at any time. Therefore for projects which adhere to these regulations, a user must not be deleted but only deactivated.
	To prevent the deletion of users, deactivate the User Administration property in the Deleting users group in the project properties.
Locked	Active: The user is locked in the Runtime and cannot login.
	This option is set automatically if a user enters an incorrect password more than is permitted.
Lock code	Four-digit PIN code.
	This code is used by the user in the command line to block areas or to unlock them. Only available if zenon Energy Edition has been licensed.
Login profile	Selection of the Runtime profile that is used for login from a drop-down list:
	▶ None
	▶ Default
	▶ Last

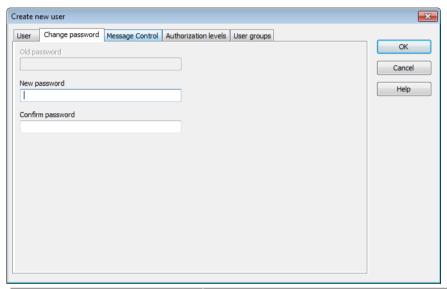
Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.
Help	Opens online help.



3.3.2 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 **Minimum password length** in group **User Administration**. The default value is 6 characters.



Parameters	Description
Old password	Current password.
New password	Enter new password. Input is automatically hidden.
	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 password. Input is automatically hidden.

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

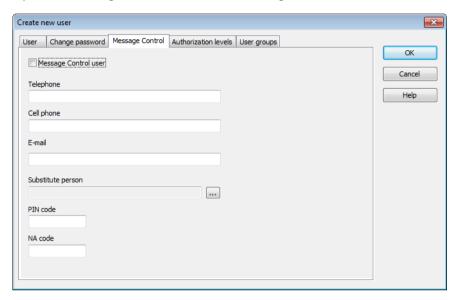
CLOSE DIALOG

Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.
Help	Opens online help.



3.3.3 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	Number of the voice-compatible telephone device of the user. Used for text to speech.	
	Enter numbers. In addition, the following are permitted:	
	► The prefix + as an abbreviation for 00 of the international area code is permitted.	
	 The following separators are also permitted in AD user administration: Minus (-), slash (/) and space Note: When communicating between AD and Message Control, separators are ignored as soon as the data from the is mapped to a zenon object. 	
Cell phone	Cellphone number of the user. Used for messages via GSM and SMS (text messages).	
	Enter numbers. In addition, the following are permitted:	
	► The prefix + as an abbreviation for 00 of the international area code is permitted.	
	 The following separators are also permitted in AD user administration: Minus (-), slash (/) and space Note: When communicating between AD and Message Control, separators are ignored as soon as the data from the is mapped to a zenon object. 	
Email	E-mail address of the user	
Substitute person	If a user has not been reached or they do not accept the message, a substitute person can be given. A click on button Opens the dialog to select a user. Only users who have been activated as Message Control users are offered for selection.	
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). The message is then sent to the next user in the list.	
	If there is no other user entered in the list, the message is entered as "not successfully acknowledged". The function assigned to this is executed. In addition, a "rejected by" CEL entry is created in each case.	
	Note: You can find further information on the assignment of functions in the Confirmation of receipt - confirmation of receipt settings chapter.	

Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.



Cancel	Discards all changes in all tabs and closes the dialog.
Help	Opens online help.

Δ

Attention

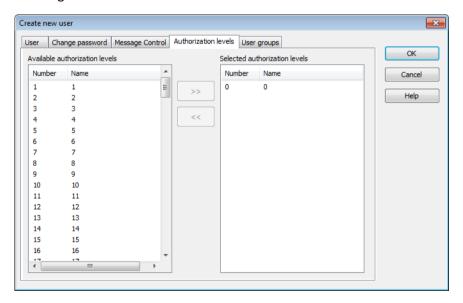
The acknowledgment codes for PIN (confirmation) and NA (rejection) must differ and should not be too similar.

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

If an unknown code is received, a SMS and e--mail is sent to the substitute person. The error message is played back for voice messages.

3.3.4 Authorization levels

Defining the authorization level for the user.



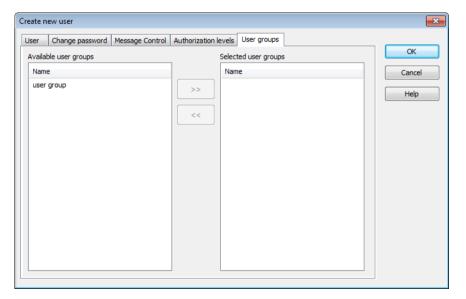


Parameters	Description
Available authorization levels	List of all available authorizations.
Selected authorization levels	List of assigned authorizations.
Button double arrow to the right	Entries selected in the list Available authorization levels are added to list Selected authorization levels .
Button double arrow to the left	Selected entries in list Selected authorization levels are removed from the list.

Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.
Help	Opens online help.

3.3.5 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.

Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.
Help	Opens online help.

3.4 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)



Q

Information

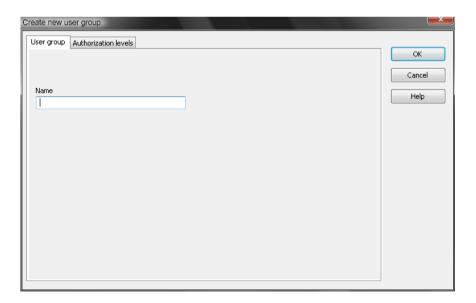
Each user group must have an unambiguous name in a project.

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 local project are used in the event of a conflict. If the local user 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 $\bf A$ 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 $\bf A$ is not present in the local project, members of group $\bf A$ have authorization levels 1, 2, 3, 100 and 101 from the global project.

3.4.1 Name the user group



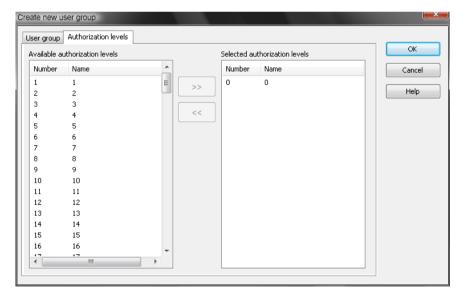


Parameters	Description
Name	Name of the new user group
	Attention: @ is not a valid character for a user group.

Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.
Help	Opens online help.

3.4.2 Authorization levels

Assignment of the authorization level to a user group.



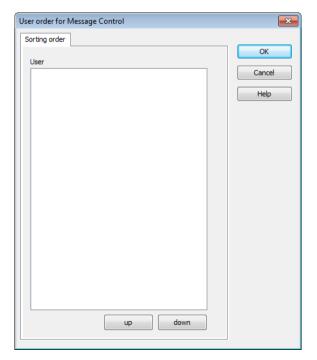


Parameters	Description
Available authorization levels	List of all available authorizations
Selected authorization levels	List of assigned authorizations
Button double arrow to the right	Entries selected in the list Available authorization levels are added to list Selected authorization levels.
Button double arrow to the left	Selected entries in list Selected authorization levels are removed from the list.

Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.
Help	Opens online help.

3.4.3 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.
ок	Applies settings and closes the dialog.
Cancel	Discards all changes and closes the dialog.
Help	Opens online help.

3.5 Editing an user

A user is changed by selecting the user from the list in the detail view. As a result of this, the corresponding properties are displayed in the properties window and can be changed here.

3.6 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.



Information

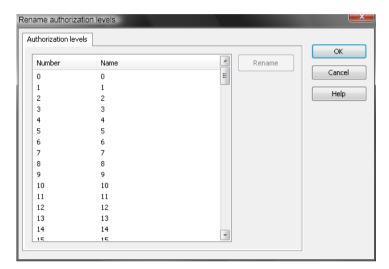
If you rename a user group, all users that are linked to this user group lose this link. The user group is displayed with (del).

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.



3.7 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.

3.8 Function authorizations

Function authorizations can be assigned in zenon. These function authorizations relate to functions in Runtime and the configuration of modules in the Editor. If a user does not have the function authorization, then

- ▶ In Runtime: the corresponding functions cannot be executed
- ▶ in the Editor: Toolbars and context menus of the corresponding module are grayed out

CONFIGURATION OF THE FUNCTION AUTHORIZATIONS

Function authorizations are configured in the zenon Editor (on page 25).

ASSIGNING THE FUNCTION AUTHORIZATIONS

This assignment is effected by means of:

► Function authorizations Runtime (on page 26)



► Function authorizations Editor (on page 34)

For global projects, the assignment is the same as for the Editor. In the process, the possibilities for selection are determined by the node points present in a global project.

As soon as one or more authorization levels greater than 0 are used, a login dialog appears when the project is loaded in the Editor. This dialog also appears if only one user was created in the project. This means that projects can be protected in the Editor. When entering the user name and password, a distinction is made between capital letter and small letters (case sensitivity).

IN GENERAL, THE FOLLOWING APPLIES:

- All project configurations for DragOver and drag&drop take module rights into account.
- For module rights that are not granted:
 - The respective menu and toolbars are grayed out in the zenon Editor.
 - No change to the project configuration is possible in the nodes and sub-nodes of the detail view.
 - The corresponding key combinations are not active.
 - The properties are grayed out in the properties window. As a result of this, further or "more in-depth" project configurations cannot be reached (for example combined elements, reaction matrix statuses, archive configuration etc.).
 - If there are no module rights for the function authorization screen, editing of screens with the mouse is also no longer possible.



Attention

Therefore please note, even at the engineering stage, that at least one user is assigned to the following three authorization levels:

- Load project
- ▶ Project
- User Administration

3.8.1 Configuration of function authorizations

To issue a function authorization:

- 1. Select the User Administration property group in the project properties.
- 2. In the Function authorizations properties field, click on the ... button
- 3. The dialog for configuration is opened.

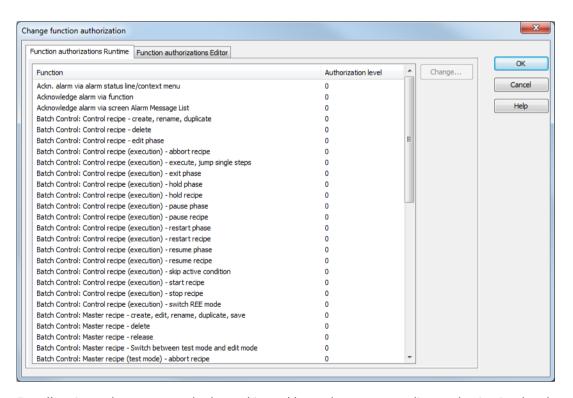


- 4. Issue the function authorization for the respective function in Runtime or for the respective module in the Editor.
- 5. Allocate the desired function authorization to an authorization level (on page 21).

To do this, it is necessary to have the respective licensing rights for the corresponding module. This is not taken in to account when engineering the individual authorization levels.

Note: Changes to the function authorizations are only effective once the Editor has been restarted or the project has been reloaded.

3.8.2 Function authorizations Runtime



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



FUNCTION AUTHORIZATIONS, GENERAL

Parameters	Description
Edit Extended Trend	Curves in Extended Trend can be edited in Runtime. The following control elements are not available if the user does not have authorization:
	▶ Diagram
	▶ Curves
	▶ Settings
	▶ Cursor on/off
	▶ X-Axis
Return to last screen (PgUp)	Screen 'back' functions can be executed in Runtime.
Screen switch: Enable "Show this dialog in Runtime"	The Screen switch function, with the Show this dialog in Runtime option active, can only be executed if the user who is logged in meets 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.

FUNCTION AUTHORIZATIONS FOR ALARMS

Parameters	Description
Change alarm comment	A comment necessary for acknowledgment can be changed.
Enter alarm comment	A comment necessary for acknowledgment can be entered.
Delete 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 authorization in the integration project.
	Comment: System messages are messages that appear in the alarm status line when a certain (configurable) number of alarms has been reached.
Acknowledge alarm via screen Alarm Message List	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.
Edit archive	Archive data (Archive server) can be amended in Runtime.

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.





Info

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

FUNCTION AUTHORIZATION BATCH CONTROL

Parameters	Description
Batch Control: Import recipe/operation	Recipes can only be imported as an XML file in the Batch Control module if the user has the corresponding rights.
Batch Control: Control recipe - create, rename, duplicate	Control recipes in the Batch Control module can only be created and administered if the user has the corresponding rights.
Batch Control: Control recipe - edit phase	Control recipes in the Batch Control module can only be edited if the user has the corresponding rights.
Batch Control: Control recipe - Delete	Control recipes in the Batch Control module can only be deleted if the user has the corresponding rights.
Batch Control: Control recipe (execution) - skip active condition	When executing control recipes in the Batch Control module, a phase can only be exited if the user has the corresponding rights.
Batch Control: Control recipe (execution) - exit phase	When executing control recipes in the Batch Control module, pending conditions can only be skipped if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - switch execution mode	In test mode, with master recipes in the Batch Control module, the execution mode can only be switched if the user has the corresponding rights.
Batch Control: Control recipe (execution) - switch execution mode	When executing control recipes in the Batch Control module, the execution mode can only be switched if the user has the corresponding rights.
Batch Control: Control recipe (execution) - execute, jump single steps	When executing control recipes in the Batch Control module, the execution of individual steps can only be skipped if the user has the corresponding rights.
Batch Control: Control recipe (execution) - hold phase	When executing control recipes in the Batch Control module, a phase can only be stopped if the user has the corresponding rights.
Batch Control: Control recipe (execution) - resume phase	When executing control recipes in the Batch Control module, a phase can only be continued if the user has the corresponding rights.
Batch Control: Control recipe (execution) - restart phase	When executing control recipes in the Batch Control module, a phase can only be restarted if the user has the corresponding rights.



Batch Control: Control recipe (execution) - pause phase	When executing control recipes in the Batch Control module, a phase can only be paused if the user has the corresponding rights.
Batch Control: Control recipe (execution) - abort recipe	When executing control recipes in the Batch Control module, execution of the recipe can only be aborted if the user has the corresponding rights.
Batch Control: Control recipe (execution) - hold recipe	When executing control recipes in the Batch Control module, a recipe can only be stopped if the user has the corresponding rights.
Batch Control: Control recipe (execution) - resume recipe	When executing control recipes in the Batch Control module, a recipe can only be continued if the user has the corresponding rights.
Batch Control: Control recipe (execution) - restart recipe	When executing control recipes in the Batch Control module, a recipe can only be restarted if the user has the corresponding rights.
Batch Control: Control recipe (execution) - pause recipe	When executing control recipes in the Batch Control module, a recipe can only be paused if the user has the corresponding rights.
Batch Control: Control recipe (execution) - start recipe	When executing control recipes in the Batch Control module, a recipe can only be restarted if the user has the corresponding rights.
Batch Control: Control recipe (execution) - stop recipe	When executing control recipes in the Batch Control module, a recipe can only be stopped if the user has the corresponding rights.
Batch Control: Operation: create, edit, rename, duplicate, save	Operations in the Batch Control module can only be created, edited or administered if the user has the corresponding rights.
Batch Control: Operation: release	Operations in the Batch Control module can only be approved if the user has the corresponding rights.
Batch Control: Operation: delete	Operations in the Batch Control module can only be deleted if the user has the corresponding rights.
Batch Control: Master recipe - create, edit, rename, duplicate, save	Master recipes in the Batch Control module can only be created and administered if the user has the corresponding rights.
Batch Control: Master recipe - release	Master recipes in the Batch Control module can only be approved if the user has the corresponding rights.
Batch Control: Master recipe - Delete	Master recipes in the Batch Control module can only be deleted if the user has the corresponding rights.
Batch Control: Master recipe - Switch between test mode and edit mode	Switching between test mode and editing mode is only possible for master recipes in the Batch Control module if the user has the corresponding rights
Batch Control: Master recipe - highlight as outdated	Master recipes in the Batch Control module can only be



marked as obsolete if the user has the corresponding rights.



Batch Control: Master recipe (test mode) - skip active condition	In test mode, with master recipes in the Batch Control module, it is only possible to skip a pending condition if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - escape phase	In test mode, with master recipes in the Batch Control module, it is only possible to exit a phase if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - execute, jump single step	In test mode, with master recipes in the Batch Control module, it is only possible to skip the execution of individual steps if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - hold phase	In test mode, with master recipes in the Batch Control module, a phase can only be stopped if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - edit phase	In test mode, with master recipes in the Batch Control module, a phase can only be edited if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - resume phase	In test mode, with master recipes in the Batch Control module, a phase can only be continued if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - restart phase	In test mode, with master recipes in the Batch Control module, a phase can only be started if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - pause phase	In test mode, with master recipes in the Batch Control module, a phase can only be paused if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - abort recipe	In test mode, with master recipes in the Batch Control module, a recipe can only be aborted if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - hold recipe	In test mode, with master recipes in the Batch Control module, a recipe can only be held if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - continue recipe	In test mode, with master recipes in the Batch Control module, a recipe can only be continued if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - restart recipe	In test mode, with master recipes in the Batch Control module, a recipe can only be continued if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - pause recipe	In test mode, with master recipes in the Batch Control module, a recipe can only be paused if the user has the corresponding rights.
	



Batch Control: Master recipe (test mode) - start recipe	In test mode, with master recipes in the Batch Control module, a recipe can only be started if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - stop recipe	In test mode, with master recipes in the Batch Control module, a recipe can only be stopped if the user has the corresponding rights.

COMMAND SEQUENCER FUNCTION AUTHORIZATIONS:

Parameters	Description
Command Sequencer: Cancel execution	When executing command sequences in the Command Sequencer module, execution of the recipe can only be aborted if the user has the corresponding rights.
Command Sequencer: Continue execution	In the Command Sequencer module, a paused command sequence can only be continued if the user has the corresponding rights.
Command Sequencer: Pause execution	In the Command Sequencer module, a corresponding command sequence can only be paused if the user has the corresponding rights.
Command Sequencer: Start execution	Starting a command sequence in the Command Sequencer module is only possible if the user has the corresponding rights.
Command Sequencer: Switch execution mode	When executing command sequences in the Command Sequencer module, individual steps can only be executed or the execution of individual steps can only be skipped if the user has the corresponding rights.
Command Sequencer: Execute, jump single steps	When executing command sequences in the Command Sequencer module, individual steps can only be executed or the execution of individual steps can only be skipped if the user has the corresponding rights.
Command Sequencer: Create, edit, rename, duplicate, save	The administration of command sequences in the Command Sequencer module - for example creation, changing, editing, duplicating and saving - can only be configured if the user has the corresponding rights.
Command Sequencer: Delete	In the Command Sequencer module, configured command sequences can only be deleted if the user has the corresponding rights.
Command Sequencer: Import command sequences	Command sequences can only be imported as an XML file in the Command Sequencer module if the user has the corresponding rights.
Command Sequencer: Switching between execution and edit mode	Switching modes (edit mode and execution mode) is only possible in the Command Sequencer module if the user has the corresponding rights.



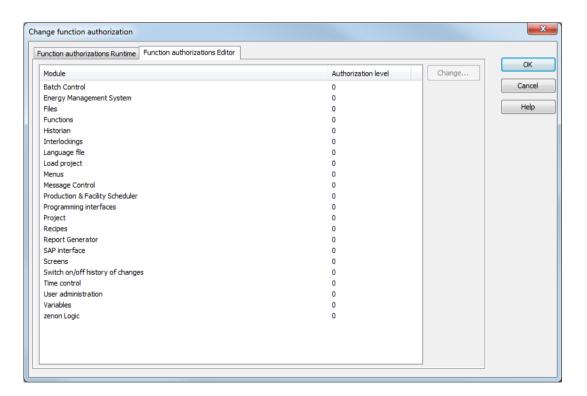
EDIT AUTHORIZATION LEVELS

Change	Opens the dialog (on page 21) to select the authorization levels. (The user group tab is hidden in the process)
	The selected authorization level is set for all selected functions.

CLOSE DIALOG

Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.
Help	Opens online help.

3.8.3 Function authorizations Editor





Parameters	Description
Switch on/off history of changes	The history of changes can only be switched on or off in the Editor, If the logged-in user is assigned to the corresponding user level.
Equipment Modeling	Only then is the Equipment modeling module available in the Editor for editing and engineering, If the logged-in user is assigned to the corresponding user level.
Historian	Only then is the Historian module available in the Editor for editing and engineering, If the logged-in user is assigned to the corresponding user level.
Batch Control	Only then is the Batch Control module available in the Editor for editing and engineering, If the logged-in user is assigned to the corresponding user level.
User Administration	Only then can users (on page 12) and user groups (on page 18) be edited or engineered in the Editor, If the logged-in user is assigned to the corresponding user level.
	Comment: In order to not be blocked out of a project, at least one user must be assigned to this function authorization.
Screens	Only then is the Screens node available in the Editor for editing and engineering, If the logged-in user is assigned to the corresponding user level.
Files	Only then is the Files node available in the Editor for editing and engineering, If the logged-in user is assigned to the corresponding user level.
Functions	Only then can functions and scripts be edited or engineered in the Editor, If the logged-in user is assigned to the corresponding user level.
Load Management	Only then is the Load management module available in the Editor for editing and project configuration, If the logged-in user is assigned to the corresponding user level.
Menus	Only then can menus be edited or engineered in the Editor, If the logged-in user is assigned to the corresponding user level.
Message Control	Only then is the Message Control module available in the Editor for editing and project configuration, If the logged-in user is assigned to the corresponding user level.
Production & Facility Scheduler	Only then is the Production& Facility Scheduler module available in the Editor for editing and engineering, If the logged-in user is assigned to the corresponding user level.
Programming Interfaces	Only then is the Programming interfaces node available in the Editor for editing and engineering, If the logged-in user is assigned to the corresponding user level.
Project	The project properties can only be amended in the Editor, If the



	logged-in user is assigned to the corresponding user level.
	Comment: In order to not be blocked out of a project, at least one user must be assigned to this function authorization.
Load project	The project can only be loaded in the Editor, If the logged-in user is assigned to the corresponding user level.
	Comment: In order to not be blocked out of a project, at least one user must be assigned to this function authorization.
Report Generator	Only then is the Report Generator available in the Editor for editing and engineering, If the logged-in user is assigned to the corresponding user level.
Recipes	Only then can Standard recipes and the Recipegroup Manager be edited or engineered in the Editor, If the logged-in user is assigned to the corresponding user level.
SAP Interface	Only then is the SAP interface module available in the Editor for editing and engineering, If the logged-in user is assigned to the corresponding user level.
Language File	Only then can Language switching be edited or engineered in the Editor, If the logged-in user is assigned to the corresponding user level.
Styles	Only then is the Styles module available in the Editor for editing and engineering, If the logged-in user is assigned to the corresponding user level.
	Note: Styles are only avialable in the Global Project.
Variables	Only then is the Variables node available in the Editor for editing and engineering, If the logged-in user is assigned to the corresponding user level.
Interlockings	Only then can Interlockings be edited or engineered in the Editor, If the logged-in user is assigned to the corresponding user level.
Time Control	Only then can Time Control be edited or engineered in the Editor, If the logged-in user is assigned to the corresponding user level.
zenon Logic	Only then can zenon Logic projects be edited or engineered in the Editor, If the logged-in user is assigned to the corresponding user level.

EDIT AUTHORIZATION LEVELS

Change	Opens the dialog (on page 21) to select the authorization levels. (The user group tab is hidden in the process)
	The selected authorization level is set for all selected functions.

CLOSE DIALOG



Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.
Help	Opens online help.

Info

You can select several entries at the same time with the keyboard shortcut Ctrl+mouse click or Shift+mouse click.

- You can select a number of entries by pressing and holding the Ctrl key.
- 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.

Screen types, dialogs and functions for login and user 3.9 administration

LOGIN

It is possible to log in to Runtime by means of:

- ▶ A Login (on page 38) screen: Permanent login, temporary login or entry of a signature via screen switching.
- Temporary login (on page 67) modal dialog: Is used for a temporary login if no login screen is linked.
- ▶ Login with dialog (on page 77) function: Login via a modal dialog or the login screen if this has been linked.
- Login without password (on page 78) function: Logging in a user without entering a password by means of direct linking or by chip identification system.

If a login screen is to be used for temporary login or the Login with dialog function is to be used, it must be linked in the Screen for Login project property.



USER ADMINISTRATION

The following types of user are available:

- ▶ User list (on page 41) screen: Lists all zenon users who have been created and makes it possible to create, edit or delete these via the Edit user screen and to configure authorization levels.
- ▶ User group list (on page 49) screen Lists all zenon user groups that have been created and makes it possible to create new ones and configure authorization levels.
- ▶ Edit user (on page 53) screen: Makes it possible to edit users and passwords in Runtime.
- ▶ Change user (on page 80) function: Opens a dialog to edit users and user groups.
- ► Change password (on page 101) function: Opens a dialog to edit your own password.

3.9.1 Creating a screen of the type Login

CREATING A SCREEN OF THE TYPE LOGIN

ENGINEERING

Steps to create the screen:

1. Create a new screen:

In the tool bar or the context menu of the **Screens**node, select the **New screen** command. An empty Standard screen is created.

- 2. Change the properties of the screen:
 - a) Name the screen in the Name property.
 - b) Select Login in the Screen type property.
 - c) Select the desired frame in the **Frame** property.
- 3. Configure the content of the screen:
 - a) select menu item Control elements from the menu bar
 - b) Select Insert template in the drop-down list. The dialog to select pre-defined layouts is opened. Certain control elements are inserted into the screen at predefined positions.
 - c) Remove elements that are not required from the screen.
 - d) If necessary, select additional elements in the **Elements** drop-down list. Place these at the desired position in the screen.
- 4. Create a screen switch function.



SCREEN OF TYPE LOGIN

Login User name User name Password Typ: EDIT Typ: EDIT Up: 40004 Signature Signature of privileged user Typ: EDIT Typ: EDIT Typ: EDIT Typ: EDIT Typ: EDIT Typ: EDIT



Control element	Description
Insert template	Opens the dialog for selecting a template for the screen type.
	Templates are shipped together with zenon and can also be created by the user.
	Templates add pre-defined control elements to pre-defined locations in the screen. Elements that are not necessary can also be removed individually once they have been created. Additional elements are selected from the drop-down list and placed in the screen. Elements can be moved on the screen and arranged individually.
Current user (display)	Display of the currently logged in user
	Note: Element of the type Dynamic text. Functionality is assigned using the Screen type specific action property.
User name	Input area for username.
	Note: Element of the type Dynamic text. Functionality is assigned using the Screen type specific action property.
Password	Input field for password.
	Note: Element of the type Dynamic text. Functionality is assigned using the Screen type specific action property.
Signature	Input field for signature.
	Note: Element of the type Dynamic text. Functionality is assigned using the Screen type specific action property.
Login	Button to close the screen after login.
Cancel	Cancels the login process.
Apply	Applies all changes and leaves the dialog open.
	Exception: The window is closed if the maximum number of invalid login attempts has been set to 0 using the Max. user error property.

COMPATIBLE ELEMENTS

Control element	Description
Compatible elements	Control elements that are replaced or removed by newer versions and continue to be available for compatibility reasons. These elements are not taken into account with automatic insertion of templates.
Users	Properties for users.
Current user (display)	Static Win32 control element. Was replaced by a dynamic text field in version 7.50. For the description, see new element.



User name	Static Win32 control element. Was replaced by a dynamic text field in version 7.50. For the description, see new element.
Password	Static Win32 control element. Was replaced by a dynamic text field in version 7.50. For the description, see new element.
Signature	Static Win32 control element. Was replaced by a dynamic text field in version 7.50. For the description, see new element.

Note: For dynamic text or switch control elements, the respective functionality is assigned using the **Screen type specific action** property.



Information

When logging in/out, the corresponding entries are created in the CEL all projects concerned.

Screen switch to login

With screen switching, you define which screen is opened in Runtime for user login.

To create a screen switch to a login screen:

- 1. Create a function.
- 2. Select screen switching.
- 3. select the login screen.
- 4. Link the function to a button.

3.9.2 Creating a user list screen

CREATING A USER LIST SCREEN

The user list screen lists all zenon users of the project who have been created and makes it possible to call up the Edit user screen and thus create, edit or delete users and configure authorization levels. Users from the global project are not displayed and cannot be administered.

ENGINEERING

Steps to create the screen:

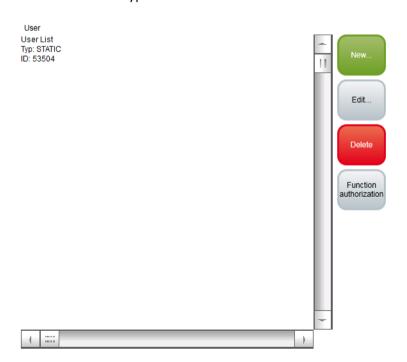


1. Create a new screen:

In the tool bar or the context menu of the **Screens**node, select the **New screen** command. An empty Standard screen is created.

- 2. Change the properties of the screen:
 - a) Name the screen in the Name property.
 - b) Select User List in the Screen type property.
 - c) Select the desired frame in the **Frame** property.
- 3. Configure the content of the screen:
 - a) select menu item Control elements from the menu bar
 - b) Select Insert template in the drop-down list. The dialog to select pre-defined layouts is opened. Certain control elements are inserted into the screen at predefined positions.
 - c) Remove elements that are not required from the screen.
 - d) If necessary, select additional elements in the **Elements** drop-down list. Place these at the desired position in the screen.
- 4. Create a screen switch function.

Note: This screen type is not available under Windows CE.





Control element	Description
Insert template	Opens the dialog for selecting a template for the screen type.
	Templates are shipped together with zenon and can also be created by the user.
	Templates add pre-defined control elements to pre-defined locations in the screen. Elements that are not necessary can also be removed individually once they have been created. Additional elements are selected from the drop-down list and placed in the screen. Elements can be moved on the screen and arranged individually.
User list	Displays the configured users.
New	Opens the screen defined in screen switching to create a new user.
Edit	Opens the screen defined in screen switching to edit a new user.
Delete	Deletes the selected user after requesting confirmation.
Function authorizations	Opens the dialog for issuing function authorizations.

Screen switching to the user list

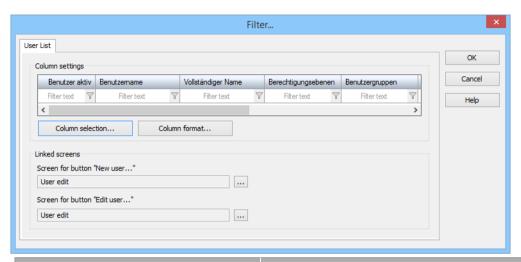
With screen switching, you define which screen is opened in Runtime for the creation or editing of users.

To create a screen switch to a user list screen:

- 1. Create a function.
- 2. Select screen switching.
- 3. Select user list screen.
- 4. The dialog for configuration is opened.
- 5. Configure the screen switching.
- 6. Confirm the configuration by clicking on **OK**.
- 7. Link the function to a button.



USER LIST DIALOG



Parameters	Description
Column settings	Display and configuration of the columns.
	Changing the order is carried out by moving the mouse or with the column selection button.
	The column width is set by moving the mouse or with the column format button.
Column selection	Opens the dialog for configuration (on page 45) of the columns.
Column Format	Opens the dialog to format (on page 47) the columns
Linked screens	Configuration of the screens that are opened in Runtime by clicking on the New and Edit buttons.
Screen for "New user" button	Opens the dialog to select a screen in order to select a screen to create a new user in Runtime. Only Edit user screens can be selected.
Screen for "Edit user" button	Opens the dialog to select a screen in order to select a screen to edit a user in Runtime. Only Edit user screens can be selected.

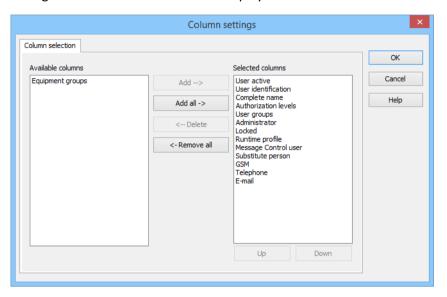
CLOSE DIALOG

Parameters	Description
ок	Applies settings and closes the dialog.
Cancel	Discards all changes and closes the dialog.
Help	Opens online help.



Column selection

Configuration of the columns to be displayed:





Button	Function
Available columns	List of columns that can be displayed in the table.
Selected columns	Columns that are displayed in the table.
Add ->	Moves the selected column from the available ones to the selected items. After you confirm the dialog with OK, they are shown in the detail view.
Add all ->	Moves all available columns to the selected columns.
<- Remove	Removes the marked columns from the selected items and shows them in the list of available columns. After you confirm the dialog with OK, they are removed from the detail view.
<- Remove all	All columns are removed from the list of the selected columns.
Up	Moves the selected entry upward. This function is only available for unique entries, multiple selection is not possible.
Down	Moves the selected entry downward. This function is only available for unique entries, multiple selection is not possible.

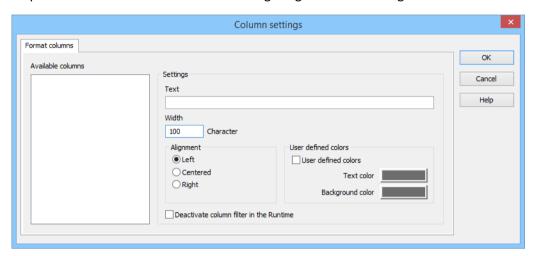
CLOSE DIALOG

Parameters	Description
ок	Applies settings and closes the dialog.
Cancel	Discards all changes and closes the dialog.
Help	Opens online help.



Column Format

Configuration of the properties of the columns for configurable lists. The settings have an effect on the respective list in the Editor or - when configuring screen switching - in Runtime.





AVAILABLE COLUMNS

Parameters	Description
Available columns	List of the available columns via Column selection . The highlighted column is configured via the options in the Settings area.

SETTINGS

Parameters	Description
Settings	Settings for selected column.
Text	Name for column title.
	The column title is online language switchable. To do this, the @ character must be entered in front of the name.
Width	Width of the column in characters. Calculation: Number time average character width of the selected font.
Alignment	Alignment. Selection by means of radio buttons.
	Possible settings:
	▶ Left-justified : Text is justified on the left edge of the column.
	Centered: Text is displayed centered in the column.
	Right-justified: Text is justified on the right edge of the column.
Deactivate column filter in	Active: The filter for this column cannot be changed in Runtime.
the Runtime	Note: Only available for:
	▶ Batch Control
	Extended Trend
	▶ Filter screens
	▶ Message Control
	Recipegroup Manager
User defined colors	Properties in order to define user-defined colors for text and background. The settings have an effect on the Editor and Runtime.
	Note:
	These settings are only available for configurable lists.
	In addition, the respective focus in the list can be signalized in Runtime by means of different text and background colors. These are configured using the project properties.
User defined colors	Active: User-defined colors are used.
Text color	Color for text display. Clicking on the color opens the color palette to select a color.



Background color	Color for the display of the cell background. Clicking on the color opens the color palette to select a color.

CLOSE DIALOG

Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.
Help	Opens online help.

3.9.3 Creating a user group list screen

CREATING A USER GROUP LIST SCREEN

The User Groups list screen lists all zenon user groups created in the project and makes it possible to create new groups and assign authorization levels. User groups from the global project are not displayed and cannot be administered.

ENGINEERING

Steps to create the screen:

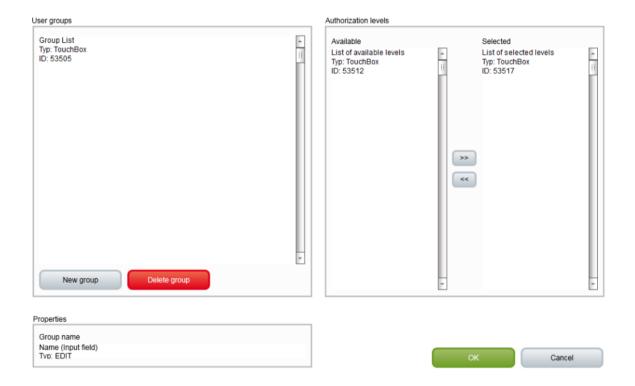
1. Create a new screen:

In the tool bar or the context menu of the **Screens**node, select the **New screen** command. An empty Standard screen is created.

- 2. Change the properties of the screen:
 - a) Name the screen in the Name property.
 - b) Select User Groups list in the Screen type property.
 - c) Select the desired frame in the Frame property.
- 3. Configure the content of the screen:
 - a) select menu item Control elements from the menu bar
 - b) Select Insert template in the drop-down list. The dialog to select pre-defined layouts is opened. Certain control elements are inserted into the screen at predefined positions.
 - c) Remove elements that are not required from the screen.



- d) If necessary, select additional elements in the **Elements** drop-down list. Place these at the desired position in the screen.
- 4. Create a screen switch function.



Control element	Description
Insert template	Opens the dialog for selecting a template for the screen type.
	Templates are shipped together with zenon and can also be created by the user.
	Templates add pre-defined control elements to pre-defined locations in the screen. Elements that are not necessary can also be removed individually once they have been created. Additional elements are selected from the drop-down list and placed in the screen. Elements can be moved on the screen and arranged individually.

GROUP LIST

Control elements for the display of the user groups.



Control element	Description
Previous group	Goes to the previous group.
Group list	List of available user groups.
Next group	Goes to the next group.
New group	Creates a new user group. The focus is set to the group name control element for input. Clicking on the OK button after input creates a new user group.
Delete group	Deletes selected group after a confirmation message.

PROPERTIES

Issue of group names and confirmation/rejection of changes.

Control element	Description
Group name	Display or entry of a group name.
	Note: Element of the type Dynamic text. Functionality is assigned using the Screen type specific action property.
ок	Applies changes.
Cancel	Discards all changes since the last acceptance with OK .

AUTHORIZATION LEVELS

Configuration of the authorization levels.



Control element	Description
Available authorization levels	Display of the authorization levels available.
Previous available authorization level	Goes to the previous level.
Listbox	Display of the authorization levels.
Next available level	Goes to the next level.
Apply level (>>)	Moves selected level from available authorization levels to selected authorization levels.
Remove level (<<)	Moves selected level from selected authorization levels to available authorization levels.
Selected authorization levels	Display of the authorization levels selected for the user group.
Previous selected level	Goes to the previous level.
Listbox	Display of the selected authorization levels.
Next selected level	Goes to the next level.

COMPATIBLE ELEMENTS

Control element	Description
Compatible elements	Control elements that are replaced or removed by newer versions and continue to be available for compatibility reasons. These elements are not taken into account with automatic insertion of templates.
Group name	Static Win32 control element. Was replaced by a dynamic text field in version 7.50. For the description, see new element.

Note: For dynamic text or switch control elements, the respective functionality is assigned using the **Screen type specific action** property.

Screen switching to user group list

With screen switching, you also define which screen is opened in Runtime for the creation or editing of user groups.

To create a screen switch to a user group list screen:

- 1. Create a function.
- 2. Select screen switching.
- 3. Select the user group list screen
- 4. Confirm the configuration by clicking on **OK**.



5. Link the function to a button.

3.9.4 Create Edit user screen

This screen type allows the editing of users in Runtime. Depending on the configuration of screen switching, users can be created or edited and passwords can be changed. Users and user groups from the global project cannot be administered.

Note: This screen type is not available under Windows CE.

CREATE EDIT USER SCREEN

ENGINEERING

Steps to create the screen:

1. Create a new screen:

In the tool bar or the context menu of the **Screens**node, select the **New screen** command. An empty Standard screen is created.

- 2. Change the properties of the screen:
 - a) Name the screen in the Name property.
 - b) Select Edit User in the Screen type property.
 - c) Select the desired frame in the **Frame** property.
- 3. Configure the content of the screen:
 - a) select menu item Control elements from the menu bar
 - b) Select Insert template in the drop-down list. The dialog to select pre-defined layouts is opened. Certain control elements are inserted into the screen at predefined positions.
 - c) Remove elements that are not required from the screen.
 - d) If necessary, select additional elements in the **Elements** drop-down list. Place these at the desired position in the screen.
- 4. Create a screen switch function.



CONTROL ELEMENTS



Control element	Description
Insert template	Opens the dialog for selecting a template for the screen type.
	Templates are shipped together with zenon and can also be created by the user.
	Templates add pre-defined control elements to pre-defined locations in the screen. Elements that are not necessary can also be removed individually once they have been created. Additional elements are selected from the drop-down list and placed in the screen. Elements can be moved on the screen and arranged individually.

USERS

Control element for user configuration.



Control element	Description
User name	Enter the username. The user logs in to the system with his username.
	Maximum length: 20 characters.
	Note: This name must be unique.
Complete name	Enter the full name of the user. With this you can allocate a username to a real person.
Administrator	Checkbox.
	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	Checkbox.
	Active: The user is active and can login in the Runtime.
	Note: According to FDA 21 PART 11 regulations, a user can never be deleted, so it is possible to trace who carried out which action at any time. Therefore for projects which adhere to these regulations, a user must not be deleted but only deactivated.
	To prevent the deletion of users, deactivate the User Administration property in the Deleting users group in the project properties.
Locked	Checkbox.
	Active: The user is locked in the Runtime and cannot login.
	This option is set automatically if a user enters an incorrect password more than is permitted.
Lock code for command processing	Four-digit PIN code.
	This code is used by the user in the command line to block areas or to unlock them. Only available if zenon Energy Edition has been licensed.
Login profile	Selection of the Runtime profile that is used for login from a drop-down list:
	▶ None
	▶ Default
	▶ Last

CHANGE PASSWORD



Control element for password configuration.

Control element	Description
Old password	Current password.
New password	Enter new password. Input is automatically hidden. 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 password. Input is automatically hidden.

MESSAGE CONTROL

Control element for configuration of Message Control.



Control element	Description
Message Control User	Checkbox.
	Active: The user is used by the module Message Control.
Telephone	Number of the voice-compatible telephone device of the user. Used for text to speech.
	Enter numbers. In addition, the following are permitted:
	The prefix + as an abbreviation for 00 of the international area code is permitted.
	The following separators are also permitted in AD user administration: Minus (-), slash (/) and space Note: When communicating between AD and Message Control, separators are ignored as soon as the data from the is mapped to a zenon object.
Cell phone	Cellphone number of the user. Used for messages via GSM and SMS (text messages).
	Enter numbers. In addition, the following are permitted:
	The prefix + as an abbreviation for 00 of the international area code is permitted.
	The following separators are also permitted in AD user administration: Minus (-), slash (/) and space Note: When communicating between AD and Message Control, separators are ignored as soon as the data from the is mapped to a zenon object.
Email	E-mail address of the user
Substitute person	If a user has not been reached or they do not accept the message, a substitute person can be given. A click on button Opens the dialog to select a user. Only users who have been activated as Message Control users are offered for selection.
Select substitute person	Click on the button to open the dialog to select a substitute person.
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). The message is then sent to the next user in the list.
	If there is no other user entered in the list, the message is entered as "not successfully acknowledged". The function assigned to this is executed. In addition, a "rejected by" CEL entry is created in each case.



	Note: You can find further information on the assignment of functions in the Confirmation of receipt - confirmation of receipt settings chapter.
--	--

AUTHORIZATION LEVELS

Control element to configure the authorization levels.

Control element	Description
Available authorization levels	List of all available authorizations.
Selected authorization levels	List of all available authorizations.
Apply authorization level (>>)	Entries selected in the list Available authorization levels are added to list Selected authorization levels.
Remove authorization level (<<)	Selected entries in list Selected authorization levels are removed from the list.

USER GROUPS

Control element to configure the user groups.

Control element	Description
Available user groups	List of all available user groups.
Selected user groups	List of assigned user groups.
Apply user group (>>)	Entries selected in the list Available user groups are added to list Selected user groups .
Remove user group (<<)	Selected entries in list Selected user groups are removed from the list.

TOUCH

Control element for navigation in list boxes, optimized for Touch operation.



Control element	Description
Available authorization level up	Navigates one authorization level up in the Available authorization levels list box.
Available authorization level down	Navigates one authorization level down in the Available authorization levels list box.
Selected authorization group up	Navigates one authorization level up in the Selected authorization levels list box.
Selected authorization group down	Navigates one authorization level down in the Selected authorization levels list box.
Available user groups up	Navigates one authorization level up in the Available user groups list box.
Available user groups down	Navigates one authorization level down in the Available user groups list box.
Selected user group up	Navigates one authorization level up in the Selected user groups list box.
Selected user group down	Navigates one authorization level down in the Selected user groups list box.

OK/CANCEL

Control element to confirm or discard changes.



Control element	Description
ок	Applies changes.
Cancel	Discards all changes since the last acceptance with OK .

COMPATIBLE ELEMENTS

Control element	Description
Compatible elements	Control elements that are replaced or removed by newer versions and continue to be available for compatibility reasons. These elements are not taken into account with automatic insertion of templates.
Users	Properties for users.
User name	Static Win32 control element. Was replaced by a dynamic text field in version 7.50. For the description, see new element.
Complete name	Static Win32 control element. Was replaced by a dynamic text field in version 7.50. For the description, see new element.
Administrator	Static Win32 control element. Was replaced by the switch element in version 7.50. For the description, see new element.
Active	Static Win32 control element. Was replaced by the switch element in version 7.50. For the description, see new element.
Locked	Static Win32 control element. Was replaced by the switch element in version 7.50. For the description, see new element.
Lock code for Command Processing	Static Win32 control element. Was replaced by a dynamic text field in version 7.50. For the description, see new element.
Change password	Properties for the password.
Old password	Static Win32 control element. Was replaced by a dynamic text field in version 7.50. For the description, see new element.
New password	Static Win32 control element. Was replaced by a dynamic text field in version 7.50. For the description, see new element.
Confirm password	Static Win32 control element. Was replaced by a dynamic text field in version 7.50. For the description, see new element.



Message Control	Properties for use in the Message Control module.
Message Control user	Static Win32 control element. Was replaced by the switch element in version 7.50. For the description, see new element.
Telephone	Static Win32 control element. Was replaced by a dynamic text field in version 7.50. For the description, see new element.
Cell phone	Static Win32 control element. Was replaced by a dynamic text field in version 7.50. For the description, see new element.
Email	Static Win32 control element. Was replaced by a dynamic text field in version 7.50. For the description, see new element.
Substitute person	Static Win32 control element. Was replaced by a dynamic text field in version 7.50. For the description, see new element.
PIN code	Static Win32 control element. Was replaced by a dynamic text field in version 7.50. For the description, see new element.
NA code	Static Win32 control element. Was replaced by a dynamic text field in version 7.50. For the description, see new element.

Note: For dynamic text or switch control elements, the respective functionality is assigned using the **Screen type specific action** property.

Screen switching for edit user

With the screen switching, you define how the edit user screen is called up. Depending on the configuration, you can:

- ► Create a new user
- ▶ Edit a user from the user list or from a string variable
- ► Change passwords

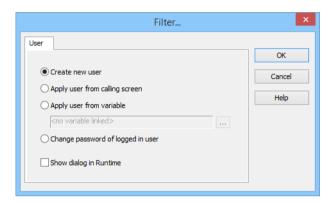
To create a screen switch to an edit user screen:

- 1. Create a function.
- 2. Select screen switching.
- 3. Select the edit user screen.
- 4. The dialog for configuration is opened.
- 5. Configure the screen switching.



- 6. Confirm the configuration by clicking on **OK**.
- 7. Link the function to a button.

USER LIST DIALOG





Parameters	Description
Create new user	The edit user screen is used to create a new user. The corresponding control elements are activated.
Apply user from calling screen	If the call is from the user list screen, the edit user screen that is selected in the user list is used to edit the user. The corresponding control elements are activated.
	Note: The editing user must have administrator rights in Runtime. At least one user must be selected in the list.
Apply user from variable	The edit user screen whose name is transferred form the defined string variable is used to edit the user. The corresponding control elements are activated.
	Click on the button to open the dialog for selecting a variable.
Change password of logged in user	The edit user screen is only used to change the password of the user who is currently logged on. The corresponding control elements are activated.
Show dialog in Runtime	Active: When calling up the function in Runtime, this dialog is opened and the user can adjust the configuration before execution.
	The dialog is displayed on the current computer in Runtime. During network operation when activating the client the dialog is also displayed on the client

CLOSE DIALOG

Parameters	Description
ок	Applies settings and closes the dialog.
Cancel	Discards all changes and closes the dialog.
Help	Opens online help.

4. zenon login and user administration in Runtime

Windows AD or AD LDS can also be used for user administration. Users can be logged in permanently or temporarily and administered in Runtime.



Particularly important values or functions can also be protected by means of a signature. To do this, the **Signature necessary** property must be activated for the corresponding property. In this case, the user must enter their password and signature again, even if they are logged in and have the appropriate rights. In doing so, an additional entry is created in the Chronological Event List.



Attention

Settings for users who are changed in the editor can only be applied if the **RT** changeable data project property (General group) allows overwriting of user properties when writing Runtime files.

Settings changed in Runtime can be applied using the *Import Runtime files* command (Runtime files toolbar) in the Editor. To do this, decompiling must be permitted in the *RT changeable data* property.

4.1 Login process and administration

The current user SYSTEM will be logged in with the approved user level LEVEL 0 after Runtime is started. In multi-project administration, users can also be automatically (on page 70) be logged into all subprojects.

RULES FOR LOGIN IN RUNTIME.

Logging in in the Runtime has the following safety precautions:

Password

A user is locked after having entered a wrong password several times and they are logged out automatically. Therefore no elements of the system can be operated if they require an authorization level higher than 0. They cannot carry out any operations linked to a user level any more. The number of login attempts that are permitted is configured in the project settings with the **Max. user error** property.

The user name that was used for the login attempt is logged in the Chronological Event List. The administrator has to unlock this user (deactivating the **Locked** property).

User name

If a non-existent user name is entered, 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 username 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.



If a correct user name is used for login but the password field remains empty, this is considered an invalid password. The user is blocked after a defined number of permitted unsuccessful attempts (default 2, block after a third failed attempt).

► 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.

Note: Changes to the password via functions, screens, dialogs and API are also checked and lead to the user being blocked if the current password is entered incorrectly several times. The number of characters in the field of the current password does not provide any indication of its the length of the password.

REQUIREMENTS FOR AD AND AD LDS USE

In order to be able to use AD and AD LDS for logging in to zenon Runtime, the zenon project property User Administration/Access to Active Directory must be configured.

- ▶ AD: Yes must be selected for the property and the computer must be in the domain.
- ► AD LDS: ADAM/AD-LDS must be selected for the property. The properties AD-LDS connection, AD-LDS user name and AD-LDS password correctly configured. Note: ADAM is no longer supported.
 - AD LDS must be prepared accordingly.

Administration is possible for:

- Windows 8, Windows 8.1 and Windows Server 2012 (on page 137)
- Windows 7 (on page 172)
- Windows Server 2008 (on page 192)



Attention

Rights that are issued in zenon are applicable for the respective project or the workspace. Rights that are issued in the Active Directory are applicable globally.

If rights have been issued to users or user groups of the Active Directory, then the rights for these users are applicable in all zenon projects!

MANAGEMENT IN 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 contents of the user administration are not replaced by default when transferred to Runtime.



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

- Create new users
- ▶ Amend existing users (except user name for login)
- 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 username 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.

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 38), 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 or a not existing user name, the system is locked after three tries as usual.



4.2 User login

Users can be logged in permanently or temporarily. Login is carried out by means of a modal dialog or a login screen.

4.2.1 Permanent login

After a permanent login, the user is permanently logged in and can carry out all operations that they are authorized (on page 17) to do. For actions that the user is not authorized to carry out, a message is shown accordingly.

Permanent login can be effected by means of:

- ► A screen switch to a login (on page 38) screen
- ▶ The function (on page 77) Login with dialog
- ► The Login without password function (on page 78)

Hint: Password-protected buttons can be made invisible for logged-in users. To do this, the **Locked** buttons property (**Project properties** -> **User Administration** -> **Login and signature**) must be configured accordingly.

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.

4.2.2 Temporary login

If an operation that requires authentication is necessary for a user who is not logged in, or entry of a signature is required, the user can be logged in temporarily. To do this, the **User Administration** property (-> **Login and signature** -> **Temp. login active**) must be activated.

Temporary login can be effected by means of:

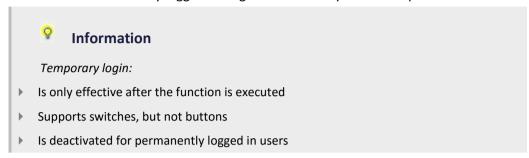
- ▶ Modal dialog, which is automatically called up by zenon.
- ▶ Login (on page 38) screen that is linked to the Screen for Login property.

Calling up login in Runtime:

- 1. The configured dialog to log in or enter a signature is opened when a password-protected function is executed.
 - If a Login (on page 38) screen is linked, this is opened. Otherwise a modal dialog is opened.
- 2. The user can log themselves in and execute operations in accordance with their rights. If the user does not have authorizations, they receive a corresponding message.



3. The user is automatically logged out again immediately after the operation



SCREEN OF TYPE LOGIN

This screen type allows temporary login or the entry of a signature.

Login Current user: SYSTEM User identification Password Signature Login Cancel Apply



Control element	Description
Current user (display)	Display of the currently logged in user
	Note: Element of the type Dynamic text. Functionality is assigned using the Screen type specific action property.
User name	Input area for username.
	Note: Element of the type Dynamic text. Functionality is assigned using the Screen type specific action property.
Password	Input field for password.
	Note: Element of the type Dynamic text. Functionality is assigned using the Screen type specific action property.
Signature	Input field for signature.
	Note: Element of the type Dynamic text. Functionality is assigned using the Screen type specific action property.
Login	Button to close the screen after login.
Cancel	Cancels the login process.
Apply	Applies all changes and leaves the dialog open.
	Exception: The window is closed if the maximum number of invalid login attempts has been set to 0 using the Max. user error property.

TEMPORARY LOGIN MODAL DIALOG

This dialog allows temporary login. If a signature is required, this must be entered in a second stage.



Control element	Description
Current user (display)	Display of the currently logged in user
User name	Input area for username.
Password	Input field for password.
ок	Button to close the screen after login.
Cancel	Cancels the login process.



4.2.3 Automatic login and logout for subprojects

In multi-project administration, users can be logged into subprojects and logged out from them automatically.

To allow a user to be able to log in and out automatically, the following must be the case in the Editor:

- ► The user must be created in the global project
- ► For each project that is to allow automatic login/logout, automatic login should be allowed

Attention: Users from the global project cannot be edited in Runtime.

CONFIGURATION IN THE EDITOR...

To configure automatic login/logout:

- 1. Open the project properties.
- 2. Navigate to node User Administration
- 3. Activate the Automatic login/logout in subprojects property.
- 4. Repeat this step for all projects that are to support automatic login/logout.

APPLICATION IN RUNTIME

Log into Runtime with a global user in a project.

The following applies in Runtime:

- ▶ When logging into a project, a global user is automatically logged in to all subprojects that support it. They are logged out of all subprojects when logging out.
- ► No corresponding dialogs are called up in the subprojects when logging in or out. Users who are already logged in are logged out.
- ▶ If the user logs out from a subproject, then:
 - They are logged out of this project and all its subprojects
 - They remain logged in to all superordinate projects in which they are logged in
- ▶ When logging in/out, the corresponding entries are created in the CEL all projects concerned.
- Automatic login/logout only works in the direction of projects to subprojects, never the other way round.

Note: This functionality is not suitable for temporary login.



PROCEDURE FOR WINDOWS USERS

A Windows user who is already logged into a subproject (AD/ADAM) is reused in a subproject with automatic login. To do this, the context (AD path or ADAM path) must be the same. If a Windows user is used for the first time in the login chain, the password is checked at this point. If a check at the start of the login chain returns invalidity, the complete login process is canceled. If a login attempt in a subproject is rejected, this login is canceled, but the process is continued for all other projects.

4.2.4 External authentication

User authentication can be carried out for external programs or applications using zenon API. If there is an incorrect external authentication, the system or the user can be blocked.

To do this:

Activate the System lock for wrong external authentication or User lock for wrong external authentication option under user administration.

Note: It is recommended that these options are activated in order to achieve the highest degree of security.

Furthermore, it is possible to state under the options **Max. user error** or **Max. password error** the amount of incorrect entries that are permitted to occur.

4.3 Administer users and user groups

Users and user groups can also be administered in Runtime.



Information

Note the following with changes in Runtime:

- Write them back to the Editor of the project configuration computer
- Do not overwrite them with Editor settings

The following possibilities are available for user administration in Runtime:



Action	Average
Create user	▶ User list screen
	▶ Edit user screen
	▶ Change user function
Edit user	▶ User list screen
	▶ Edit user screen
	▶ Change user function
Delete user	▶ User list screen
	▶ Change user function
Change password	▶ Edit user screen
	▶ Change user function
	▶ Change password function
Assign function authorization	▶ Change user function
Creating a user group	▶ User group list screen
Edit user group	▶ User group list screen
Assign authorization level	▶ User group list screen

A

Attention

Do not delete a user who is a general module owner.

4.4 Screen types to administer users and user groups

Users cannot only be administered in Runtime with functions and modal dialogs; they can also be administered by means of special screen types:

- User list (on page 73): Lists all users and offers possibilities to create, edit and delete users as well as to assign function authorizations.
- User group list (on page 74): Lists all user groups and offers the possibility to create and administer user groups and to assign function authorizations.
- ▶ Edit user (on page 74): Allows the creation and administration of users.

You must be logged in as an administrator for all actions. Exception: Users without administrator rights can change their own password.



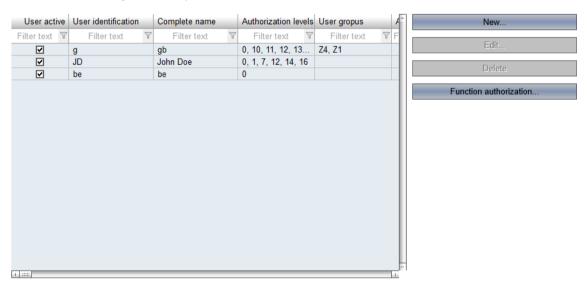
4.4.1 User list

You administer user lists with this screen. In doing so, the following applies:

- ▶ You must be logged in as an administrator.
- You can create new users.
- You can edit users.
- You can delete users.
- You can only issue function authorizations that you have yourself directly or as a member of a user group.

To administer users in lists:

- 1. Log in as an administrator.
- 2. Create a user list screen.
- 3. Configure the desired settings.
 - Clicking on New opens an edit user screen. This must be linked for screen switching.
 - Clicking on **Edit** opens an edit user screen. This must be linked for screen switching.



You can read details about the control elements in the Create user list screen (on page 41) chapter.



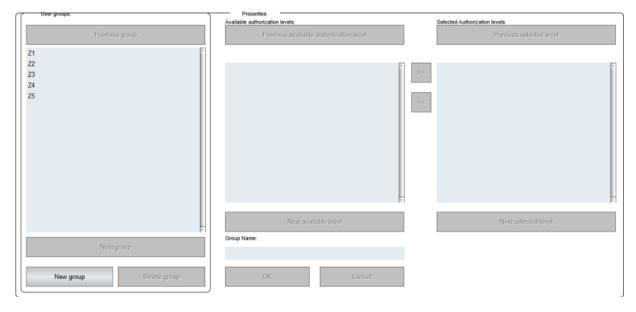
4.4.2 User Groups List

You administer user groups with this screen. In doing so, the following applies:

- ▶ You must be logged in as an administrator.
- ▶ You can only administer user groups to which you also belong.
- You can create new user groups.
 User groups that you create are assigned to you immediately. The group thus has at least one member and can be assigned further users.

To administer user groups:

- 1. Log in as an administrator.
- 2. Open a user group list screen.
- 3. Configure the desired settings. The possible settings correspond to those in the Editor.



You can read details about the control elements in the **Create user group list screen** (on page 49) chapter.

4.4.3 Edit users and change password

You can administer other users with this screen. All users can also change their own password. In doing so, the following applies:

1. You must be logged in as an administrator. Exception: Users without administrator rights can change their own password.



- ► You can only issue authorization levels that you have yourself directly or as a member of a user group.
- ► You can only assign user groups to which you also belong.
- ▶ You cannot change your own authorization levels or user groups in Runtime.

EDIT USER

To administer users:

- 1. Log in as an administrator.
- 2. Open an edit user screen or open a user list and click on New or Edit there.



3. Configure the desired settings. The possible settings correspond to those in the Editor or the Change user (on page 80) function.



You can read details about the control elements in the Create edit user screen (on page 53) chapter.

CHANGE PASSWORD

A modal dialog is called up in order for users to be able to change their own password. This dialog can also be replaced by an edit user screen. The dialog or screen can be called up modally if:

- ▶ The Change password function is executed
- ► The user who is logged in is to change their password (new user, expired password, password reset)

To allow users to edit their password by means of a screen:



- 1. Link, in the User Administration Login and signature project properties, the Screen for password change property to an edit user screen.
- 2. The screen is opened modally instead of the modal dialog.
- 3. Users can change their password.

4.5 Functions for the user administration module

The following functions are available for the user administration in Runtime:

- ► Login with dialog (on page 77): Opens a modal dialog or the login screen for permanent login in Runtime.
- Login without password (on page 78): Logs in the user defined in the Editor without password entry or allows login with a chip identification system.
- ► Logout (on page 79): Logs out the user who is currently logged in and logs in the System user with authorization level 0.
- ▶ Change user (on page 80): Opens a dialog to edit users and user groups.
- ▶ Change password (on page 101): Opens a dialog in Runtime to change the password.

4.5.1 Login with dialog

This function opens in Runtime, depending on the configuration:

- ▶ The modal login dialog
- ▶ The login (on page 38) screen

Modal dialog





Control element	Description
Current user (display)	Display of the currently logged in user
User name	Input area for username.
Password	Input field for password.
ок	Button to close the screen after login.
Cancel	Cancels the login process.

The login is logged in the Chronological Event list.

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 Processing]

3. Enter a values 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.



Information

You can find **zenon6.ini** in the following path:

Windows 7/8: %ProgramData%\COPA-DATA\System\

4.5.2 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 Chronological 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 login a user via a Chip Ident System.
	Click on button in order to open the dialog for selecting a String variable. For details see the "Log in via Chip Ident System" section.

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 zenon 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).

4.5.3 Logout

When this function is used in Runtime, the current user is logged out and the user SYSTEM is logged in with authorization level 0. The log in of an user is logged in the Chronological Event List. If an Active Directory user is logged in, they are also logged out.

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

4.5.4 Change user

The **Change user** function makes it possible to create and administer users and to assign them authorization levels in Runtime.

To create the function:

- 1. Create a new function.
- 2. Go to the User Administration section.
- 3. Select the Change user function.
- 4. Link the function to a button.

USE IN RUNTIME

This dialog is opened in Runtime when the function is called up. This allows the creation and editing of:

- ▶ Users (on page 81)
- ▶ User groups (on page 98)



Information

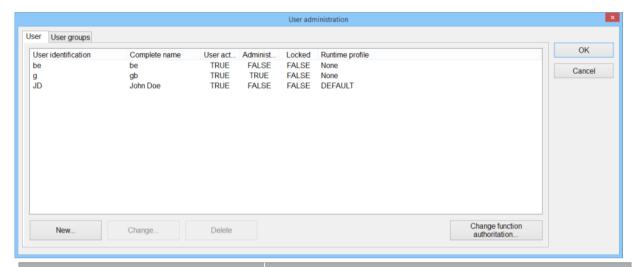
Rules:

- ▶ Administrators can administer all other users and their settings.
- Administrators cannot grant additional authorization levels themselves or add themselves to other user groups.
- Users without administrator rights can only change their password and their settings for Message Control.



Users

Users are configured in this tab.



Parameters	Description
List user	Lists all configured users.
New	Opens the dialog (on page 82) to create and amend new users.
Change	Opens the dialog (on page 82) to create and amend new users.
Delete	Deletes the selected user after requesting confirmation.
Change function authorization	Opens the dialog dialog (on page 89) to assign function authorizations to authorization levels for Runtime.

CLOSE DIALOG

Parameters	Description
ок	Applies settings and closes the dialog.
Cancel	Discards all changes and closes the dialog.

ADMINISTER USERS

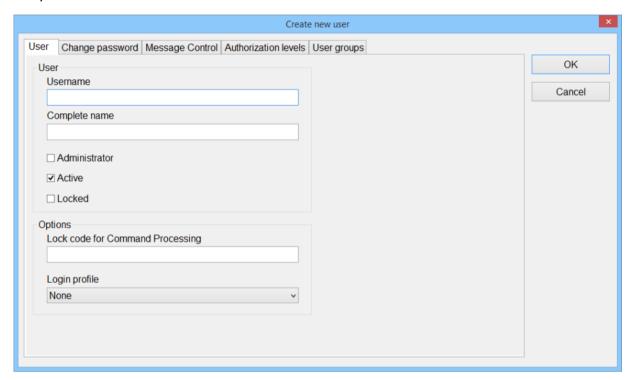
To administer a user:

- 1. Highlight the user in the list.
- 2. Select the desired action by clicking on one of the buttons.



Users

Entry of the user data.





Parameters	Description
User name	Enter the username. The user logs in to the system with his username.
	Maximum length: 20 characters.
	Note: This name must be unique.
Complete name	Enter the full name of the user. With this you can allocate a username 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 login in the Runtime.
	Note: According to FDA 21 PART 11 regulations, a user can never be deleted, so it is possible to trace who carried out which action at any time. Therefore for projects which adhere to these regulations, a user must not be deleted but only deactivated.
	To prevent the deletion of users, deactivate the User Administration property in the Deleting users group in the project properties.
Locked	Active: The user is locked in the Runtime and cannot login.
	This option is set automatically if a user enters an incorrect password more than is permitted.
Lock code	Four-digit PIN code.
	This code is used by the user in the command line to block areas or to unlock them. Only available if zenon Energy Edition has been licensed.
Login profile	Selection of the Runtime profile that is used for login from a drop-down list:
	None
	▶ Default
	▶ Last

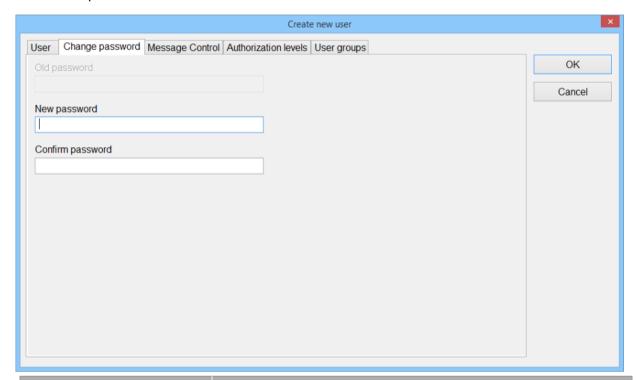
CLOSE DIALOG

Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.



Change password

Issue of the password for the user.



Parameters	Description
Old password	Current password.
New password	Enter new password. Input is automatically hidden.
	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 password. Input is automatically hidden.

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

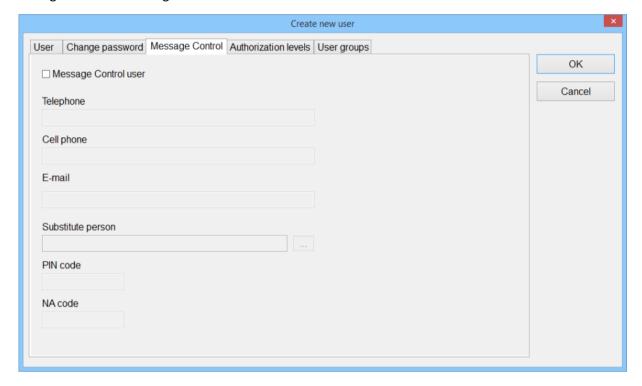
CLOSE DIALOG

Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.
© Information	
An administrator can only enable users for groups for which he has the rights himself.	



Message Control

Configuration for Message Control.





Parameters	Description	
Message Control User	Active: The user is used by the module Message Control.	
Telephone	Number of the voice-compatible telephone device of the user. Used for text to speech.	
	Enter numbers. In addition, the following are permitted:	
	► The prefix + as an abbreviation for 00 of the international area code is permitted.	
	The following separators are also permitted in AD user administration: Minus (-), slash (/) and space Note: When communicating between AD and Message Control, separators are ignored as soon as the data from the is mapped to a zenon object.	
Cell phone	Cellphone number of the user. Used for messages via GSM and SMS (text messages).	
	Enter numbers. In addition, the following are permitted:	
	► The prefix + as an abbreviation for 00 of the international area code is permitted.	
	The following separators are also permitted in AD user administration: Minus (-), slash (/) and space Note: When communicating between AD and Message Control, separators are ignored as soon as the data from the is mapped to a zenon object.	
Email	E-mail address of the user	
Substitute person	If a user has not been reached or they do not accept the message, a substitute person can be given. A click on button Opens the dialog to select a user. Only users who have been activated as Message Control users are offered for selection.	
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). The message is then sent to the next user in the list.	
	If there is no other user entered in the list, the message is entered as "not successfully acknowledged". The function assigned to this is executed. In addition, a "rejected by" CEL entry is created in each case.	
	Note: You can find further information on the assignment of functions in the Confirmation of receipt - confirmation of receipt settings chapter.	

CLOSE DIALOG

Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.



Cancel Discards all changes in all tabs and closes the dialog.

Δ

Attention

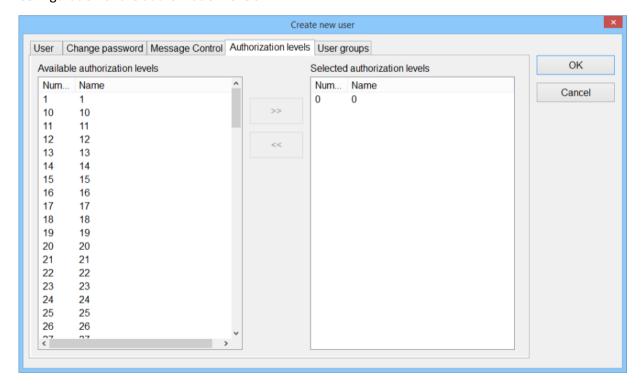
The acknowledgment codes for PIN (confirmation) and NA (rejection) must differ and should not be too similar.

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

If an unknown code is received, a SMS and e--mail is sent to the substitute person. The error message is played back for voice messages.

Authorization levels

Configuration of the authorization levels.





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.

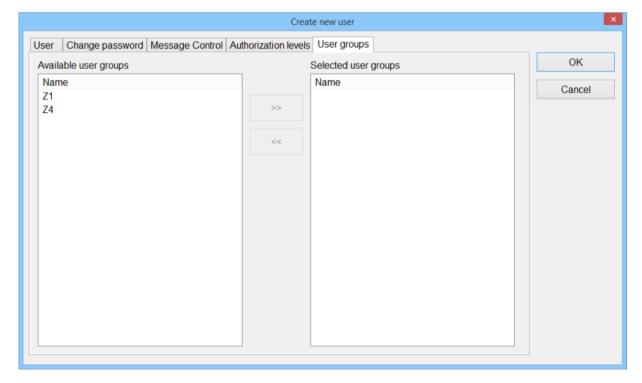
CLOSE DIALOG

Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.

User groups

Assignment of user groups.

Note: You can only assign user groups that you have yourself.





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.

CLOSE DIALOG

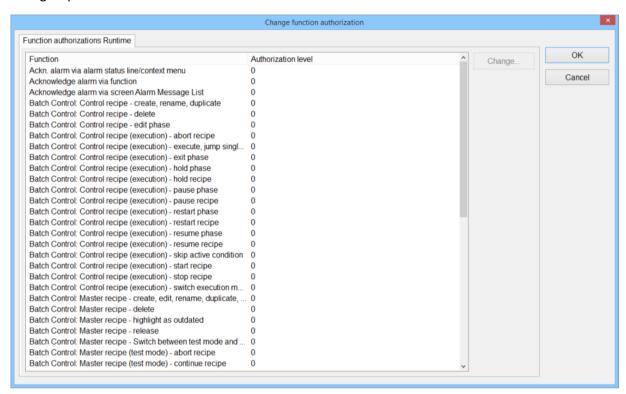
Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.

Issue function authorizations

Issue of function authorizations to authorization levels.



Note: You can only issue function authorizations that you have yourself directly or as a member of a user group.





Parameters	Description
List of functions	List of existing functions and the assigned authorization levels.
Change	Opens the dialog to assign a new authorization level.

CLOSE DIALOG

Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.

FUNCTION AUTHORIZATIONS, GENERAL

Parameters	Description
Edit Extended Trend	Curves in Extended Trend can be edited in Runtime. The following control elements are not available if the user does not have authorization:
	▶ Diagram
	▶ Curves
	▶ Settings
	▶ Cursor on/off
	▶ X-Axis
Return to last screen (PgUp)	Screen 'back' functions can be executed in Runtime.
Screen switch: Enable "Show this dialog in Runtime"	The Screen switch function, with the Show this dialog in Runtime option active, can only be executed if the user who is logged in meets 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.

FUNCTION AUTHORIZATIONS FOR ALARMS

Parameters	Description
Change alarm comment	A comment necessary for acknowledgment can be changed.
Enter alarm comment	A comment necessary for acknowledgment can be entered.
Delete 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 authorization in the integration project.
	Comment: System messages are messages that appear in the alarm status line when a certain (configurable) number of alarms has been reached.
Acknowledge alarm via screen Alarm Message List	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.
Edit archive	Archive data (Archive server) can be amended in Runtime.

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.





Info

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

FUNCTION AUTHORIZATION BATCH CONTROL

Parameters	Description
Batch Control: Import recipe/operation	Recipes can only be imported as an XML file in the Batch Control module if the user has the corresponding rights.
Batch Control: Control recipe - create, rename, duplicate	Control recipes in the Batch Control module can only be created and administered if the user has the corresponding rights.
Batch Control: Control recipe - edit phase	Control recipes in the Batch Control module can only be edited if the user has the corresponding rights.
Batch Control: Control recipe - Delete	Control recipes in the Batch Control module can only be deleted if the user has the corresponding rights.
Batch Control: Control recipe (execution) - skip active condition	When executing control recipes in the Batch Control module, a phase can only be exited if the user has the corresponding rights.
Batch Control: Control recipe (execution) - exit phase	When executing control recipes in the Batch Control module, pending conditions can only be skipped if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - switch execution mode	In test mode, with master recipes in the Batch Control module, the execution mode can only be switched if the user has the corresponding rights.
Batch Control: Control recipe (execution) - switch execution mode	When executing control recipes in the Batch Control module, the execution mode can only be switched if the user has the corresponding rights.
Batch Control: Control recipe (execution) - execute, jump single steps	When executing control recipes in the Batch Control module, the execution of individual steps can only be skipped if the user has the corresponding rights.
Batch Control: Control recipe (execution) - hold phase	When executing control recipes in the Batch Control module, a phase can only be stopped if the user has the corresponding rights.
Batch Control: Control recipe (execution) - resume phase	When executing control recipes in the Batch Control module, a phase can only be continued if the user has the corresponding rights.
Batch Control: Control recipe (execution) - restart phase	When executing control recipes in the Batch Control module, a phase can only be restarted if the user has the corresponding rights.



Batch Control: Control recipe (execution) - pause phase	When executing control recipes in the Batch Control module, a phase can only be paused if the user has the corresponding rights.
Batch Control: Control recipe (execution) - abort recipe	When executing control recipes in the Batch Control module, execution of the recipe can only be aborted if the user has the corresponding rights.
Batch Control: Control recipe (execution) - hold recipe	When executing control recipes in the Batch Control module, a recipe can only be stopped if the user has the corresponding rights.
Batch Control: Control recipe (execution) - resume recipe	When executing control recipes in the Batch Control module, a recipe can only be continued if the user has the corresponding rights.
Batch Control: Control recipe (execution) - restart recipe	When executing control recipes in the Batch Control module, a recipe can only be restarted if the user has the corresponding rights.
Batch Control: Control recipe (execution) - pause recipe	When executing control recipes in the Batch Control module, a recipe can only be paused if the user has the corresponding rights.
Batch Control: Control recipe (execution) - start recipe	When executing control recipes in the Batch Control module, a recipe can only be restarted if the user has the corresponding rights.
Batch Control: Control recipe (execution) - stop recipe	When executing control recipes in the Batch Control module, a recipe can only be stopped if the user has the corresponding rights.
Batch Control: Operation: create, edit, rename, duplicate, save	Operations in the Batch Control module can only be created, edited or administered if the user has the corresponding rights.
Batch Control: Operation: release	Operations in the Batch Control module can only be approved if the user has the corresponding rights.
Batch Control: Operation: delete	Operations in the Batch Control module can only be deleted if the user has the corresponding rights.
Batch Control: Master recipe - create, edit, rename, duplicate, save	Master recipes in the Batch Control module can only be created and administered if the user has the corresponding rights.
Batch Control: Master recipe - release	Master recipes in the Batch Control module can only be approved if the user has the corresponding rights.
Batch Control: Master recipe - Delete	Master recipes in the Batch Control module can only be deleted if the user has the corresponding rights.
Batch Control: Master recipe - Switch between test mode and edit mode	Switching between test mode and editing mode is only possible for master recipes in the Batch Control module if the user has the corresponding rights
Batch Control: Master recipe - highlight as outdated	Master recipes in the Batch Control module can only be



marked as obsolete if the user has the corresponding rights.



Batch Control: Master recipe (test mode) - skip active condition	In test mode, with master recipes in the Batch Control module, it is only possible to skip a pending condition if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - escape phase	In test mode, with master recipes in the Batch Control module, it is only possible to exit a phase if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - execute, jump single step	In test mode, with master recipes in the Batch Control module, it is only possible to skip the execution of individual steps if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - hold phase	In test mode, with master recipes in the Batch Control module, a phase can only be stopped if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - edit phase	In test mode, with master recipes in the Batch Control module, a phase can only be edited if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - resume phase	In test mode, with master recipes in the Batch Control module, a phase can only be continued if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - restart phase	In test mode, with master recipes in the Batch Control module, a phase can only be started if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - pause phase	In test mode, with master recipes in the Batch Control module, a phase can only be paused if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - abort recipe	In test mode, with master recipes in the Batch Control module, a recipe can only be aborted if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - hold recipe	In test mode, with master recipes in the Batch Control module, a recipe can only be held if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - continue recipe	In test mode, with master recipes in the Batch Control module, a recipe can only be continued if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - restart recipe	In test mode, with master recipes in the Batch Control module, a recipe can only be continued if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - pause recipe	In test mode, with master recipes in the Batch Control module, a recipe can only be paused if the user has the corresponding rights.



Batch Control: Master recipe (test mode) - start recipe	In test mode, with master recipes in the Batch Control module, a recipe can only be started if the user has the corresponding rights.
Batch Control: Master recipe (test mode) - stop recipe	In test mode, with master recipes in the Batch Control module, a recipe can only be stopped if the user has the corresponding rights.

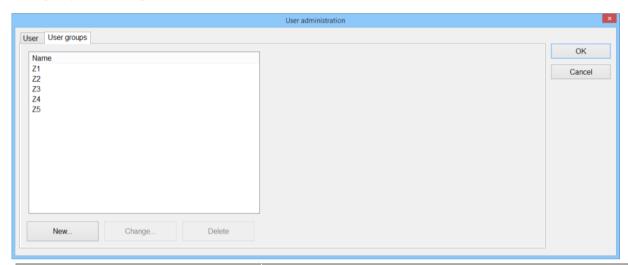
COMMAND SEQUENCER FUNCTION AUTHORIZATIONS:

Parameters	Description
Command Sequencer: Cancel execution	When executing command sequences in the Command Sequencer module, execution of the recipe can only be aborted if the user has the corresponding rights.
Command Sequencer: Continue execution	In the Command Sequencer module, a paused command sequence can only be continued if the user has the corresponding rights.
Command Sequencer: Pause execution	In the Command Sequencer module, a corresponding command sequence can only be paused if the user has the corresponding rights.
Command Sequencer: Start execution	Starting a command sequence in the Command Sequencer module is only possible if the user has the corresponding rights.
Command Sequencer: Switch execution mode	When executing command sequences in the Command Sequencer module, individual steps can only be executed or the execution of individual steps can only be skipped if the user has the corresponding rights.
Command Sequencer: Execute, jump single steps	When executing command sequences in the Command Sequencer module, individual steps can only be executed or the execution of individual steps can only be skipped if the user has the corresponding rights.
Command Sequencer: Create, edit, rename, duplicate, save	The administration of command sequences in the Command Sequencer module - for example creation, changing, editing, duplicating and saving - can only be configured if the user has the corresponding rights.
Command Sequencer: Delete	In the Command Sequencer module, configured command sequences can only be deleted if the user has the corresponding rights.
Command Sequencer: Import command sequences	Command sequences can only be imported as an XML file in the Command Sequencer module if the user has the corresponding rights.
Command Sequencer: Switching between execution and edit mode	Switching modes (edit mode and execution mode) is only possible in the Command Sequencer module if the user has the corresponding rights.



User group

User groups are configured in this tab.



Parameters	Description
List of user groups	Lists all configured user groups.
New	Opens the dialog (on page 82) to create and amend new user groups.
Change	Opens the dialog (on page 82) to create and amend new user groups.
Delete	Deletes the selected user group after confirmation.

CLOSE DIALOG

Parameters	Description
ок	Applies settings and closes the dialog.
Cancel	Discards all changes and closes the dialog.

ADMINISTER USER GROUPS

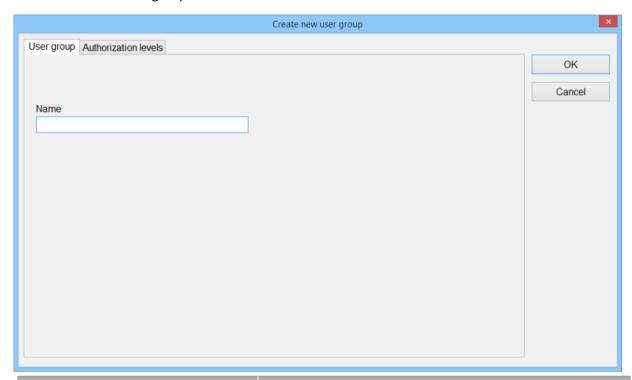
To administer a user group:

- 1. Highlight the user group in the list.
- 2. Select the desired action by clicking on one of the buttons.



User group

Creation of a new user group.



Parameters	Description
Name	Name of the new user group
	Attention: @ is not a valid character for a user group.

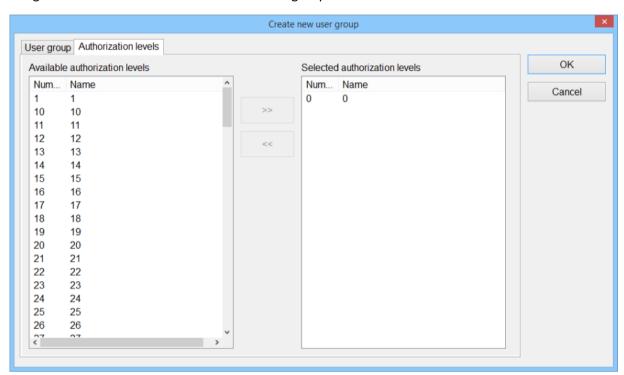
CLOSE DIALOG

Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.



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.

CLOSE DIALOG

Parameters	Description
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.



4.5.5 Change password

When this function is used, the user who is logged in can change their current password in Runtime. For system-internal users no changes are possible.

A dialog to change the password is called up in Runtime.



Required inputs:

Parameters	Description
Old password	Enter current password.
New password	Enter new password.
Confirm password	Enter new password again.
ОК	Accepts the new password and closes the dialog.
Cancel	Cancels the process.

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

4.6 Password protection for dynamic elements

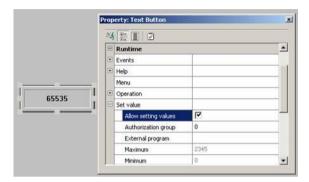
All dynamic elements that either execute a function or allow the setting of values can be linked to an authorization group for the Runtime.

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.



4.7 Accept changes in the Editor in Runtime

Not all changes to the user administration are accepted in Runtime after a reload. Note most of all:

THE MAXIMUM NUMBER OF INCORRECT PASSWORD INPUTS

If you change the standard value for the maximum number of erroneous attempts for entering a password in the Editor, this change is only effective once Runtime is restarted. Reloading alone is not sufficient, because otherwise as many attempts at entering a password as desired would be possible. You change the value at: Project properties -> User Administration -> Max. user error

CHANGES TO USER GROUPS AND AUTHORIZATIONS

If user groups are added or removed or authorizations are changed in the Editor, these changes are not accepted in Runtime for users that are logged in on reloading. In order for these changes to be effective, users who are logged in must log out of the system and log in again. This also applies to use by Active Directory users.

5. Administering Active Directory users from zenon Runtime

You can access the Windows Active Directory in Runtime with an Active Directory user administration screen. You can create, delete and edit organization units, users and user groups and assign them rights in zenon.





Information

Active Directory, AD LDS and ADAM (for Windows XP) are not available with Windows CE.

DOMAINS IN RUNTIME

In Runtime, the domain of the user who started Runtime for the Active Directory login is used. Only the users who belong to this domain can log in.

USER AUTHORIZATION



Attention

Rights that are issued in zenon are applicable for the respective project or the workspace. Rights that are issued in the Active Directory are applicable globally.

If rights have been issued to users or user groups of the Active Directory, then the rights for these users are applicable in all zenon projects!

5.1 Creating an Active Directory user administration screen

ENGINEERING

Steps to create the screen:

1. Create a new screen:

In the tool bar or the context menu of the **Screens**node, select the **New screen** command. An empty Standard screen is created.

- 2. Change the properties of the screen:
 - a) Name the screen in the Name property.
 - b) Select Active Directory user administration in the Screen type property.
 - c) Select the desired frame in the **Frame** property.
- 3. Configure the content of the screen:
 - a) select menu item Control elements from the menu bar



- b) Select Insert template in the drop-down list. The dialog to select pre-defined layouts is opened. Certain control elements are inserted into the screen at predefined positions.
- c) Remove elements that are not required from the screen.
- d) If necessary, select additional elements in the **Elements** drop-down list. Place these at the desired position in the screen.
- 4. Create a screen switch function.

ACTIVE DIRECTORY USER ADMINISTRATION SCREEN





Parameters	Description
Insert template	Opens the dialog for selecting a template for the screen type.
	Templates are shipped together with zenon and can also be created by the user.
	Templates add pre-defined control elements to pre-defined locations in the screen. Elements that are not necessary can also be removed individually once they have been created. Additional elements are selected from the drop-down list and placed in the screen. Elements can be moved on the screen and arranged individually.
Login	Control elements for logging into the Active Directory.
Domain name	Entry and display of the domain name.
User name	Entry and display of the AD user name.
Password	Entry of the password.
Login	Clicking logs the user into the AD.
Logout	Clicking logs the user out.
Active Directory Explorer	Control elements for the display and administration of the Active Directory.
	Contains the Active Directory detail view: Window in which the structure of the Active Directory is displayed.
Create new organization unit (tree)	Opens the dialog to create a new organization unit in the tree.
Delete organization unit (Tree)	Deletes the organization unit selected in the tree after requesting confirmation.
One level up	Navigates to one level higher in the structure.
Create new organization unit	Creates a new organization unit below the element selected in the tree. The corresponding dialog is opened:
Create new user	Opens the dialog to crate a new user.
Create new user group	Opens the dialog to create a new user group.
Edit object	Opens the dialog to edit the selected object.
Delete object	Deletes the selected object.

5.2 Screen switching to Active Directory user administration

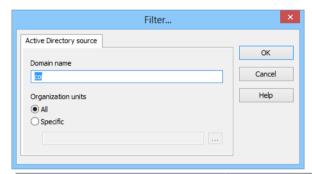
To use the Active Directory user administration screen in Runtime, configure screen switching. In doing so, you can set pre-settings for the organization units to be displayed. This is how you can control the organization units that respective users can select.



Configuring screen switching:

- 1. Create a screen switch to an Active Directory user administration screen function.
- 2. Issue a **domain name**, in order to open the AD of a certain domain in Runtime. You can also leave the name empty. Then the **domain name** must be entered in Runtime when logging in.
- 3. Configure the **organization units** to be displayed. You can have them all displayed, or select specific ones.
- 4. Close the dialog by clicking on **OK** and link the function with a button in the screen.

FILTER DIALOG



Parameters	Description
Domain name	Entry of the domain for which the Active Directory is to be loaded when screen switching.
Organization units	Selection of the organization units to be displayed. Selection by means of radio buttons:
	 All: All nodes of the AD structure organization of the domains are displayed in Runtime.
	▶ Specific : Allows the selection of certain organization units. Clicking on the button in the input field opens the dialog to select the organization units.
ок	Applies settings and closes the dialog.
Cancel	Discards all changes and closes the dialog.
Help	Opens online help.

SELECT ORGANIZATION UNITS

If you select **specific organization units** in the filter dialog, the dialog to enter the login files is opened first, then the dialog to select the organization units.



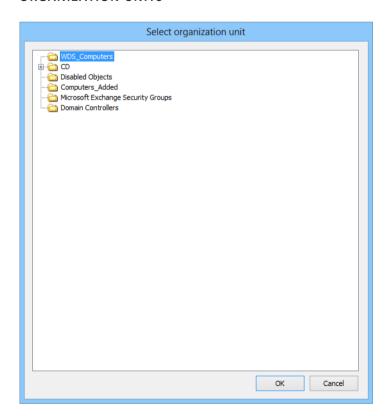
LOGIN





Parameters	Description
User currently logged in	Active: The user who is currently logged into the computer is logged in to the AD to select the organization units.
Explicit login	Active: A certain user who is logged in to the AD to select the organization units.
	Domain: Entry of the domains whose structure is to be displayed.
	Username: User. Can remain empty if reading of the data only is sufficient.
	> Password:
ок	Applies settings and opens the Select organization units dialog.
Cancel	Discards all changes and closes the dialog.

ORGANIZATION UNITS





Parameters	Description	
List of organization units	Display of all organization units of the selected domain. Selection from the folder tree.	
ок	Applies settings and closes the dialog.	
Cancel	Discards all changes and closes the dialog.	

5.3 Administer Active Directory users in Runtime.

Organization units, user groups and users of the active directory can be administered from zenon Runtime with an Active Directory user administration screen.



Attention

Rights that are issued in zenon are applicable for the respective project or the workspace. Rights that are issued in the Active Directory are applicable globally.

If rights have been issued to users or user groups of the Active Directory, then the rights for these users are applicable in all zenon projects!

ACTIVE DIRECTORY USER ADMINISTRATION SCREEN

The screen is cleared when screen switching

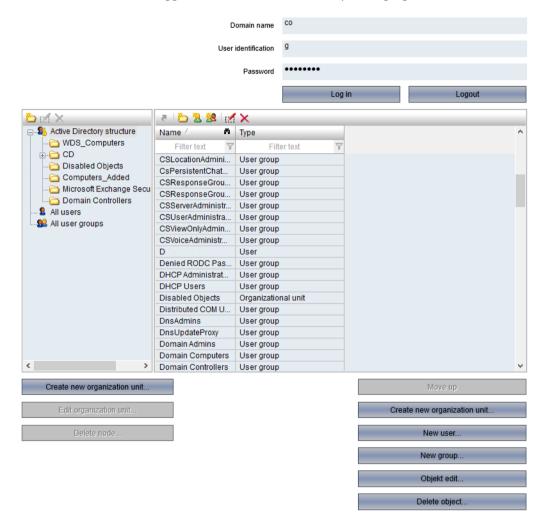
To administer users in the AD:

- 1. Enter the domain name (can already be defined in the screen switching), user name and password
- 2. Click on Login
- 3. The connection is created.

 If errors (on page 197) occur, check the configuration in the Active Directory (on page 137) and in zenon.
- 4. The domain data is read and displayed in the window.
- 5. Edit the desired elements. Available actions:
 - Creating and deleting organization units (on page 112)
 - Creating, editing and deleting users (on page 113)
 - Creating, editing and deleting user groups (on page 120)



Note: The user who is logged on must have the corresponding rights in the domain.





Parameters	Description
Login	Control elements for logging into the Active Directory.
Domain name	Entry and display of the domain name.
User name	Entry and display of the AD user name.
Password	Entry of the password.
Login	Clicking logs the user into the AD.
Logout	Clicking logs the user out.
Active Directory Explorer	Control elements for the display and administration of the Active Directory.
	Contains the Active Directory detail view: Window in which the structure of the Active Directory is displayed.
Create new organization unit (tree)	Opens the dialog to create a new organization unit in the tree.
Delete organization unit (Tree)	Deletes the organization unit selected in the tree after requesting confirmation.
One level up	Navigates to one level higher in the structure.
Create new organization unit	Creates a new organization unit below the element selected in the tree. The corresponding dialog is opened:
Create new user	Opens the dialog to crate a new user.
Create new user group	Opens the dialog to create a new user group.
Edit object	Opens the dialog to edit the selected object.
Delete object	Deletes the selected object.

TREE CONTEXT MENU

Depending on the element selected, the context menu in the tree (left window) provides the following commands:

Command	Description
Create new organization unit	Creates a new organization unit below the element selected in the tree. The corresponding dialog is opened:
Create new user	Deletes the organization unit selected in the tree after requesting confirmation.

TOOLBAR AND CONTEXT MENU DETAIL VIEW

Depending on the element selected, the context menu and the toolbar in the detail view (right window) provide the following commands:





Command	Description
One level up	Navigates to one level higher in the structure.
Create new organization unit	Creates a new organization unit below the element selected in the tree. The corresponding dialog is opened:
Create new user	Opens the dialog to crate a new user.
Create new user group	Opens the dialog to create a new user group.
Edit selected object	Opens the dialog to edit the selected object.
Delete selected object	Deletes the selected object.

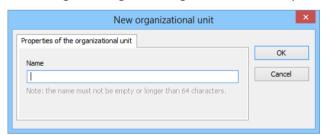
5.3.1 Manage organization unit

You can create and delete AD organization units in the tree and in the detail view.

CREATING AN ORGANIZATION UNIT

To create a new organization unit:

- 1. Click in the screen on the button or select **Create new organization unit** in the context menu of a highlighted element.
- 2. The dialog to configure an organization unit is opened



3. Give it a name.

Maximum length: 64 characters

4. Click on **OK**.

EDIT ORGANIZATION UNIT

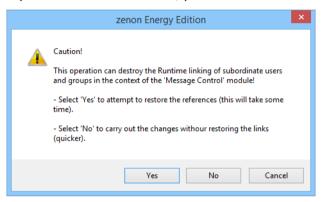
The name of the organization unit can be changed.

Attention: When changing the name, links to users and user groups that are used in the **Message Control** module are destroyed.



To edit an organization unit in the tree:

- Select the desired organization unit and click on the corresponding button or command in the context menu. In the detail view, click on the **Edit object** or the **Edit selected object** command in the context menu.
- 2. The dialog editing is opened.
- 3. Edit the object.
- 4. If you click on the OK button, you are asked how linking should be handled:



- 5. Select the desired option:
 - Yes: The renaming is carried out.

An attempt is made to restore linking to users and user groups that are used in the Message Control module.

This process can take some time.

- No: The change is made immediately.
 Attention: Linking to users and user groups that are used in the Message Control module can be destroyed!
- Cancel: The renaming is not applied and the dialog is closed.

DELETE ORGANIZATION UNIT

To delete an organization unit in the tree, select the desired organization unit and click on the corresponding button or command in the context menu. In the detail view, click on the **Delete object** button or the **Delete selected object** command in the context menu.

Note: An organization unit can only be deleted if it no longer contains any objects.

5.3.2 Managing users

New users can be created and existing users can be edited and deleted. Users with the same visual name in the list can be distinguished by the information in the tool tip.



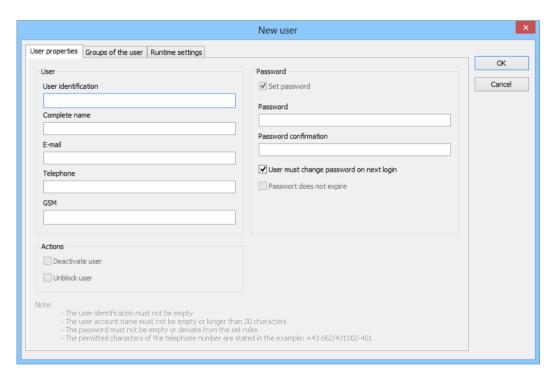
- Create new user: Click on the corresponding button, or the command in the toolbar or the context menu.
- ► Edit user: Double-click a user entry or click on the corresponding button or on the **Edit selected object** command in the context menu.
- ▶ Delete user: Highlight the desired user and press the **Del** button, click on the corresponding button or on the **Delete selected object** command in the context menu.

When creating and editing, a dialog is opened, in which you can configure the user.

CREATING OR EDITING A USER DIALOG

The dialog consists of three tabs. You can also find notes on the options in the **Project configuration in the Editor** (on page 8)/**Creation of a user** (on page 11) chapter.

USER PROPERTIES





USERS

Parameters	Description	
Users	Settings for user data.	
User name	Unique name of the user for the login.	
Complete name	Displayed name of the user.	
Email	E-mail address of the user	
Telephone	Number of the voice-compatible telephone device of the user. Used for text to speech.	
	Enter numbers. In addition, the following are permitted:	
	The prefix + as an abbreviation for 00 of the international area code is permitted.	
	The following separators are also permitted in AD user administration: Minus (-), slash (/) and space Note: When communicating between AD and Message Control, separators are ignored as soon as the data from the is mapped to a zenon object.	
GSM	Cellphone number of the user. Used for messages via GSM and SMS (text messages).	
	Enter numbers. In addition, the following are permitted:	
	The prefix + as an abbreviation for 00 of the international area code is permitted.	
	The following separators are also permitted in AD user administration: Minus (-), slash (/) and space Note: When communicating between AD and Message Control, separators are ignored as soon as the data from the is mapped to a zenon object.	

PASSWORD

Parameters	Description
Password	Settings for the password.
Set password	Active: The password is set again.
Password	Enter new password. Input is automatically hidden. For language-spanning projects take care that it must be possible to enter the characters with the respective keyboard in
	the Runtime.
Password confirmation	Repeat the password. Input is automatically hidden.
User must change password on next login	Active: The user must, as soon as they log in to the system, change their password.



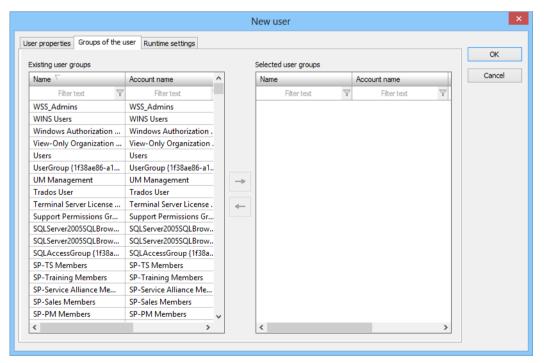
Password does not expire	Active: Password never needs to be changed
--------------------------	--

ACTIONS

Parameters	Description
Actions	Configuration of actions for the account.
Deactivate user	Active: The user is deactivated and can no longer log in.
Unblock user	Active: The blocked user is unblocked and can log in in Runtime again.
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.

USER GROUPS OF THE USER

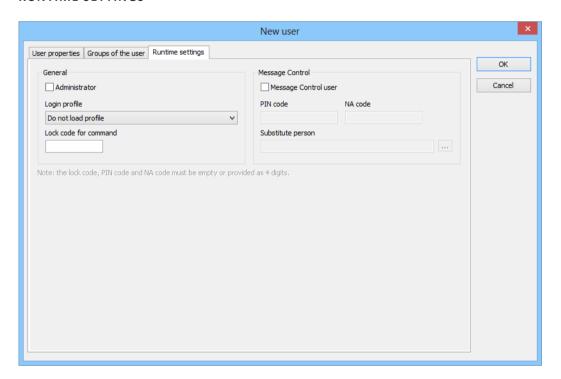
- 1. Select, in the **Existing user groups** window, the desired user groups from the existing ones.
- 2. Add the selected groups to the list of **selected user groups** with the cursor key ->.
- 3. You can also select user groups that have already been allocated and remove them again with the cursor key <-.





Parameters	Description
Existing user groups	List of configured user groups.
Selected user groups	List of the user groups selected for the user.
Cursor keys	Clicking moves the highlighted groups to the corresponding list.
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.

RUNTIME SETTINGS





GENERAL

Parameters	Description
General	General settings.
Administrator	Active: The user takes on the role of a zenon administrator. Only an administrator can unblock zenon user accounts that have been blocked.
	Note: If a user is stipulated as an administrator, then this role is also applicable for all zenon projects!
Login profile	Selection of the Runtime profile that is used for login from a drop-down list:
	None
	▶ Default
	▶ Last
Lock code for Command Processing	Four-digit PIN code.
	This code is used by the user in the command line to block areas or to unlock them. Only available if zenon Energy Edition has been licensed.

MESSAGE CONTROL

Parameters	Description
Message Control	Settings for Message Control.
Message Control user	Active: The user is used by the module Message Control.
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). The message is then sent to the next user in the list.
	If there is no other user entered in the list, the message is entered as "not successfully acknowledged". The function assigned to this is executed. In addition, a "rejected by" CEL entry is created in each case.
	Note: You can find further information on the assignment



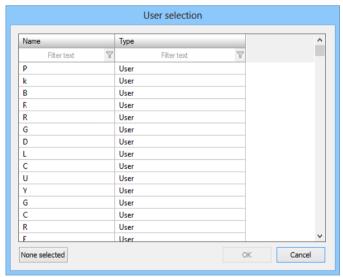
of functions in the Confirmation of receipt - confirmation
of receipt settings chapter.

SUBSTITUTE PERSON

Parameters	Description
Substitute person	If a user has not been reached or they do not accept the message, a substitute person can be given. A click on button Opens the dialog to select a user. Only users who have been activated as Message Control users are offered for selection.
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.

SUBSTITUTE PERSON DIALOG

If a substitute person is to be selected for the Message Control module, a click on the button opens a dialog with previously-configured users.



Parameters	Description
List of persons	List of users available.
None selected	A user who is already defined in the dialog is
ок	Applies settings and closes the dialog.
Cancel	Discards all changes and closes the dialog.



Select the desired user and click on **OK**.

To remove a substitute person who has already been configured, click on None and then on OK.

5.3.3 Managing user groups

New user groups can be created and existing user groups can be edited and deleted.

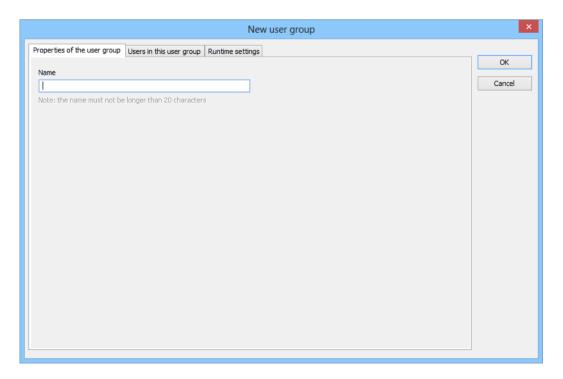
- ► Creating a new user group: Click on the corresponding button, or the command in the toolbar or the context menu.
- ▶ Editing user groups: Double-click a user group entry or click on the corresponding button or on the **Edit selected object** command in the context menu.
- ▶ Deleting user groups: Highlight the desired user group and press the **Del** button, click on the corresponding button or on the **Delete selected object** command in the context menu.

When creating and editing, a dialog is opened, in which you can configure the user.

CREATING OR EDITING A USER DIALOG

The dialog consists of three tabs. You can also find notes on configuration in the **Project configuration** in the **Editor** (on page 8)/**Creation of a user** (on page 19) chapter.

PROPERTIES OF THE USER GROUP

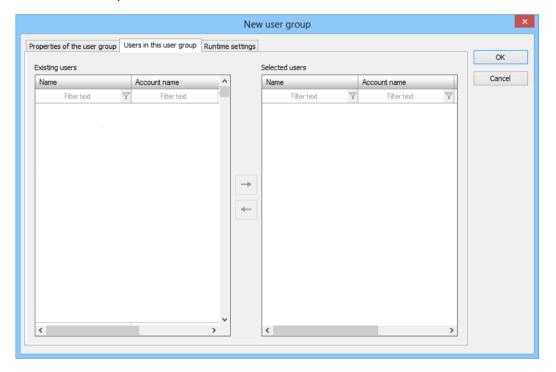




Parameters	Description
Name	Entry of a unique, valid name for the database backup.
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.

USERS IN THIS USER GROUP

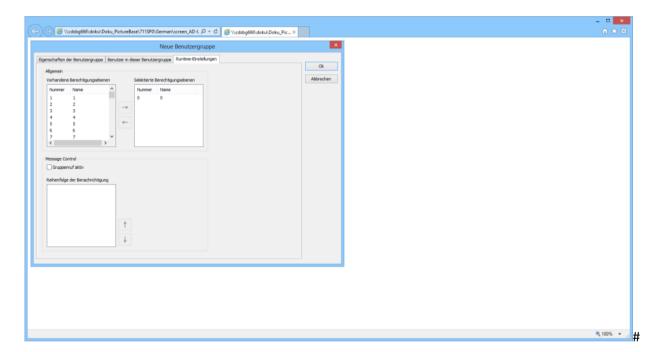
- 1. Select, in the **Existing users** window, the desired users from the existing users.
- 2. Add the selected users with the cursor key -> to the list of **selected users**.
- 3. You can also select users who have already been allocated and remove them again with the cursor key <-.





Parameters	Description	
List of existing users	List of configured users.	
List of selected users	List of the users selected for this group.	
Cursor keys	Clicking on a cursor key moves the selected user to the corresponding group.	
ок	Applies all changes in all tabs and closes the dialog.	
Cancel	Discards all changes in all tabs and closes the dialog.	

RUNTIME SETTINGS





GENERAL

Parameters	Description
General	General settings. Configuration of the authorization levels.
List of existing authorization levels	List of the authorization levels configured in zenon.
List of selected authorization levels	List of authorization levels that are allocated to this group.
Cursor keys	Clicking on a cursor key moves the authorization levels to the corresponding group.

MESSAGE CONTROL

Parameters	Description
Message Control	Configuration for zenon Message Control.
Group call active	Active: All members of the user group are messaged when messaging via Message Control.
Sequence of messaging	List of all available users. Sequencing is carried out using the cursor keys.
ок	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.

6. External user administration with Microsoft Active Directory

With zenon, you can also use Microsoft Active Directory for user administration:

- ► User groups in Active Directory that have the same name as zenon user groups receive the same rights as in zenon
- ► Can be managed with zenon users in the Active Directory (on page 102) in Runtime



1

Attention

Rights that are issued in zenon are applicable for the respective project or the workspace. Rights that are issued in the Active Directory are applicable globally.

If rights have been issued to users or user groups of the Active Directory, then the rights for these users are applicable in all zenon projects!

In order to be able to use AD and AD LDS for logging in to zenon Runtime, the zenon project property **User Administration/Access to Active Directory** must be configured.

- ▶ **AD**: Yes must be selected for the property and the computer must be in the domain.
- ► AD LDS: ADAM/AD-LDS must be selected for the property. The properties AD-LDS connection, AD-LDS user name and AD-LDS password correctly configured.

 Note: ADAM is no longer supported.
- ▶ AD LDS must be prepared accordingly.

6.1 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:

- The name of the authorization group in the zenon user administration corresponds to the group names of a user group in the Active Directory: Automatic assignment of the Active Directory user to the zenon authorization group. all users of the AD group get the user rights that are defined in the zenon authorization group. See User groups in zenon and groups in the Active Directory have the same name (on page 127)
- 2. In the description of the Active Directory group, the zenon authorization levels and the project are saved with a certain syntax. All users of the group get the user rights saved in the AD group in zenon. See Assignment of an Active Directory user to zenon authorization levels (on page 125)
- 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 127).



Information

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





Information

Active Directory, AD LDS and ADAM (for Windows XP) are not available with Windows CE.

6.1.1 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 login 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

6.1.2 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



Information

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			
FFFFFFF	FFFFFFF	FFFFFFF	FFFFFFF
Authorization levels 1	Authorization levels 2	Authorization levels 3	Authorization levels 4



Example

Group name: MASCHINE01##service staff

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 to zenon, 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.



6.1.3 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

6.1.4 Active Directory extension scheme

Note: This expansion should not be used in an FDA 21 CFR Part11 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 127) method or Allocation of an Active Directory user to zenon authorization levels (on page 125).



Information

Active Directory, AD LDS and ADAM (for Windows XP) are not available with Windows CE.

Installation of the schema extension

In order for the users in AD to also be able to be assigned the 128 authorization levels of zenon, the AD schema must be supplemented with these entries (4 integer values).

For this purpose, two files (**zenonUserLevel.exe** and **zAD_UserDig.exe**) are copied to the server (ideally to their own folder). As soon as the setup (**zenonUserLevel.exe**) has been started, this folder and the files contained therein must no longer be renamed or deleted.



Δ

Attention

You can find the two files **zenonUserLevel.exe** and **zAD_UserDlg.exe** on the zenon installation medium in the /Software/zenonUserLevel/folder

```
© D:\AD_Users\zenOnUserLevel.exe

Adding Active Directory Attributes...
Adding zenOnUserLeve11
Adding zenOnUserLeve12
Adding zenOnUserLeve13
Adding zenOnUserLeve14
Please vait while Windows is updating the Schema configuration
(this may take several minutes)...

ZenOnUserLeve11 zenOnUserLeve12 zenOnUserLeve13 zenOnUserLeve14 added
Edit script D:\AD_Users\zenOnUserDuserDig.exe
set for User-Administration menu (zenOnUserLeve1)
Press return
```

A reference to the ${\tt zAD_UserDlg.exe}$ file is stored in the AD schema.

Furthermore, 4 integer values (zenonUserLevel1, zenonUserLevel2, zenonUserLevel3, zenonUserLevel4) are added to the AD schema.



Information

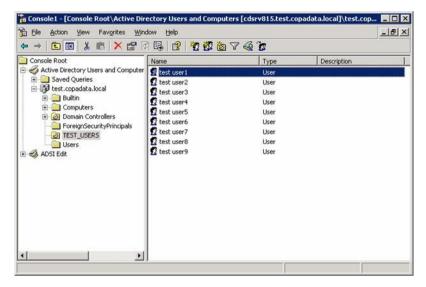
Only a user from the **Schema administrators** group can make these changes! The domain administrator normally has these rights.

Granting user rights

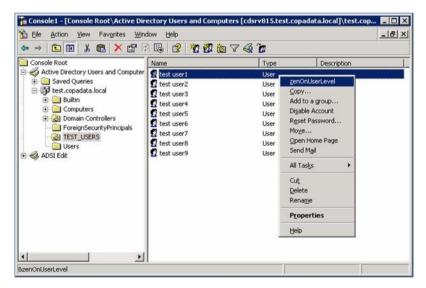
After the successful extension of the schema the authorization levels can be granted to the single users.



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**.



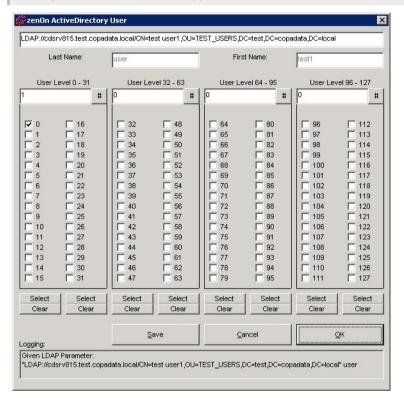
In this context menu, the **zenonUserLevel** entry has to be selected, so that the administration tool (zAD_UserDlg.exe) for the selected user is opened.





Information

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.



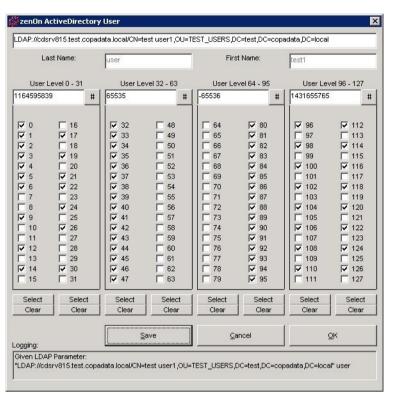
Information

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.
ок	Saves all settings and closes dialog.
Logging	Displays logging information.



6.1.5 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.

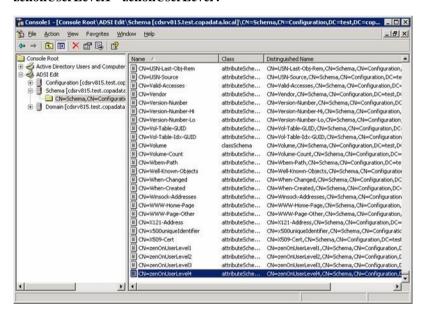
In order to be able to see the details of the AD schema, **ADSI Edit** has to be installed on the server. This tool is available as soon as the support tools for the Microsoft Server have been installed.

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

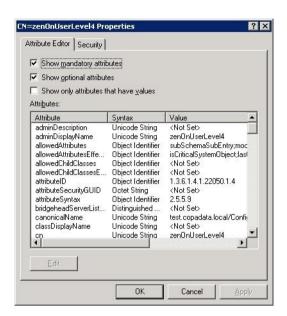
6.1.6 Schema

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

zenonUserLevel1 - zenonUserLevel4



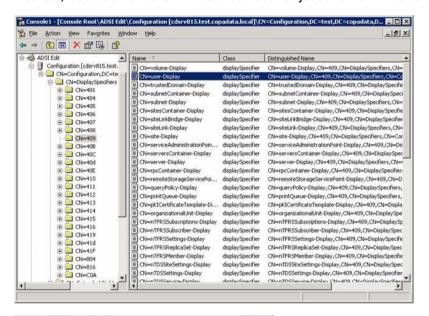


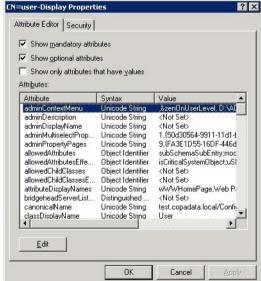




6.1.7 Configuration

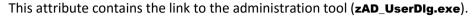
After the connection to configuration has been defined, the details of the single AD objects can be checked and edited. In this case, only the object user-display in the single 'DisplaySpecifiers' is of interest, because here the link between user object and AdministrationTool is established.





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







This 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:

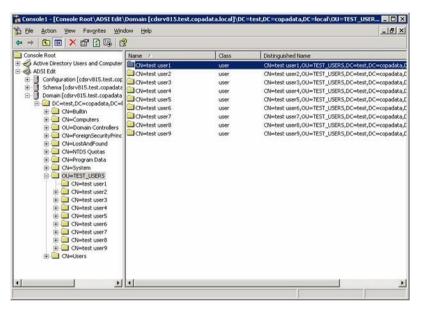
, name of the menu entry, path of the file zAD_UserDlg.exe



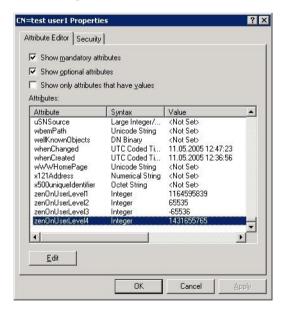


6.1.8 Domain

If the connection **domain** is openen, it looks similar to the MMC with the PlugIn **Active Directory Users and Computers**. Exactly this information can also be found here, but with more details.



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.





6.2 Active Directory Lightweight Directory Services - AD LDS

Active Directory Lightweight Directory Services (abbreviation: AD LDS) is a simplified version of the Active Directory (on page 124) and is suitable for use on normal desktop operating systems; it is not necessary to use a server operating system. LikeAD (on page 124), AD LDS also supports:

- 1. The name of the authorization group in the zenon user administration corresponds to the group names of a user group in the Active Directory: Automatic assignment of the Active Directory user to the zenon authorization group. all users of the AD group get the user rights that are defined in the zenon authorization group. See User groups in zenon and groups in the Active Directory have the same name (on page 127)
- 2. In the description of the Active Directory group, the zenon authorization levels and the project are saved with a certain syntax. All users of the group get the user rights saved in the AD group in zenon. See Assignment of an Active Directory user to zenon authorization levels (on page 125)

You can use AD LDS with:

- ▶ Windows 7 (on page 172)
- ▶ Windows 8 (on page 137)
- ▶ Windows Server 2008 (on page 192)
- Windows Server 2012 (on page 137)

6.2.1 AD LDS with Windows 8 and Windows Server 2012

To use AD LDS with Windows 8, Windows 8.1 or Windows Server 2012 and zenon:

- 1. Install AD LDS (on page 138)
- 2. Create a new AD LDS instance (on page 141)
- 3. Import an AD LDS schema (on page 147)
- 4. Install Remote Administration for Windows Server (on page 149)
- 5. Configure the Active Directory snap-in (on page 149) in order to manage the AD LDS instances
- 6. Define the roles, organization units, users and user groups (on page 154)

Note: The instructions on installation and use of AD LDS sometimes use screenshots with an English user interface.

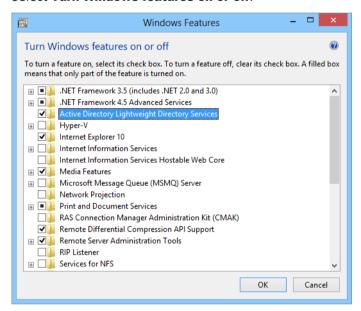


Installing AD LDS

WINDOWS 8

To install AD LDS under Windows 8:

- 1. Open Control Panel.
- 2. Open Programs and Features.
- 3. Select Turn Windows features on or off.



- 4. Activate the check box in front of Active Directory Lightweight Directory Services.
- 5. Click on **ok**.

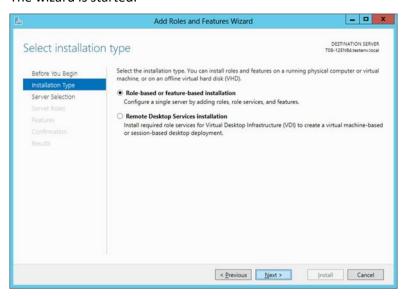
WINDOWS SERVER 2012

To install AD LDS under Windows Server 2012:

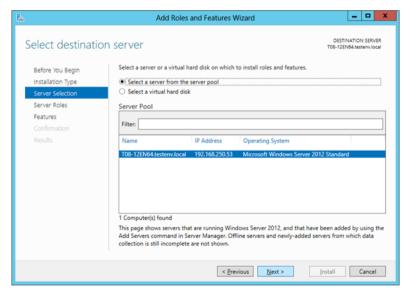
1. Go to Manage -> Add Roles and Features.



2. The wizard is started.



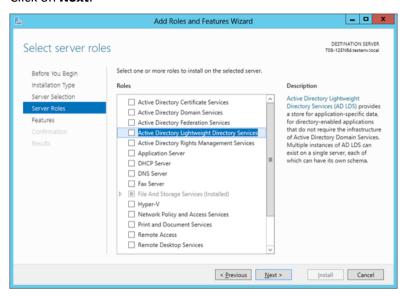
- 3. Select Role-based or feature-based installation.
- 4. Click on Next.



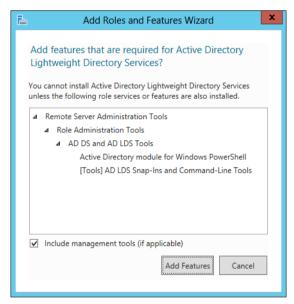
5. Select a server from the server pool.



6. Click on Next.



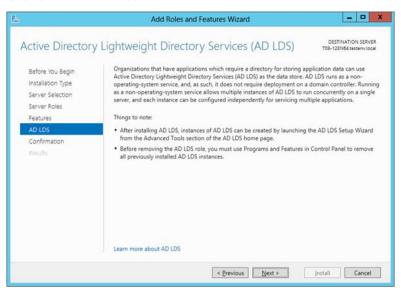
- 7. Activate the check box in front of Active Directory Lightweight Directory Services for server roles.
- 8. Click on Next.



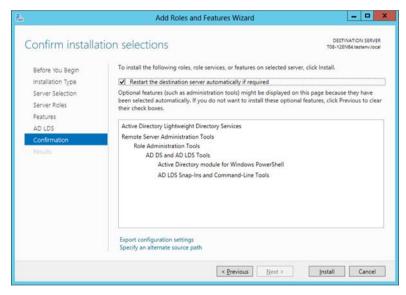
9. Activate the check box for Include management tools.



10. Click on Add Features.



11. Click on Next.



12. Confirm the automatic restart of the server.

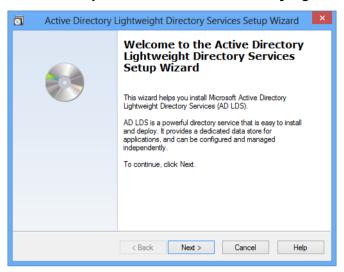
Create new AD LDS instance

To create a new AD LDS instance:

1. In Windows, go to the %ProgramData%\Microsoft\Windows\Start Menu\Programs\Administrative Tools folder.



2. Start the Setup Assistant for Active Directory Lightweight Directory Services file.



3. Click on Next.



4. Select unique instance as the installation type.

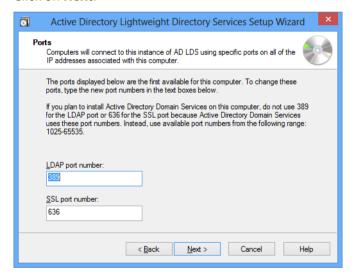


5. Click on Next.



6. Assign an instance name.

7. Click on Next.



8. Enter the port number for LDAP and SSL.

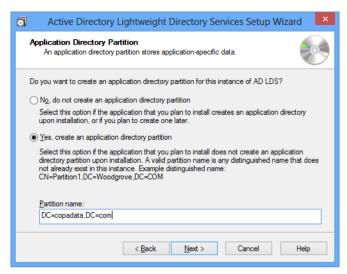
Default LDAP: 389 Default SSL: 636

Note: If you change one of the port numbers, this must also be amended in one of the following

steps.



9. Click on Next.



- 10. Activate the option for an application directory partition.
- 11. Enter Partition name.

Note: The **partition name** is used together with the port number and server name in zenon. In this example, the entry in the corresponding zenon **AD-LDS connection** property would be:

\\w8x64-vm0009.testenv.local:389/DC=copadata,DC=com



12. Click on Next in the assistant.



13. Enter the save location for data files and restores. (you can leave it at the default setting.)



14. Click on Next.



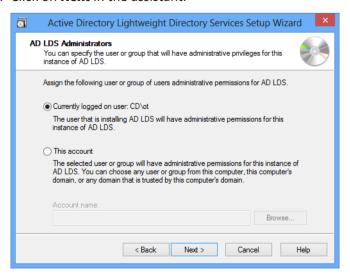
15. Select the authorization levels with which authorization processes are to be carried out. (Network service account in this example)

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



This will not impair the functionality as long as you do not carry out any replications. Confirm the notice by clicking **Yes**

16. Click on **Next** in the assistant.





17. Enter the user who is to administer AD LDS. The user who is currently logged on is used in this example.

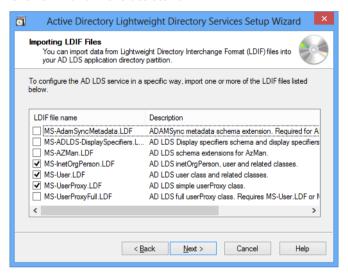
The user does not need to be a local administrator or domain administrator. A group can also be given.

However: An individual user must be given in zenon. This can be a member of a group.

The user configured here is used in zenon in the **AD-LDS user name** and **AD-LDS password** properties:



18. Click on Next in the assistant.



- 19. Import the required LFIF files: You need:
 - MS-InetOrgPerson.LDF
 - MS-User.LDF
 - MS-UserProxy.LDF



20. Click on Next.



21. Confirm the configuration by **clicking on Next**The installation is carried out.

22. Close the assistant by clicking on the Finish button

Importing an AD LDS schema

To import LD ADS schemas:

- 1. Open the command line.
- 2. Navigate to the AD LDS folder: WINDIR%\ADAM.
- 3. Enter the following command and press the Enter key:

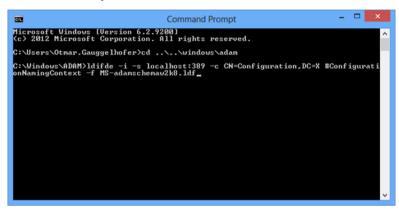
Idifde -i -s localhost:389 -c CN=Configuration,DC=X #ConfigurationNamingContext -f MS-adamschemaw2k8.ldf

Note: If you have configured a dedicated user for the AD LDS partition, you must also enter:

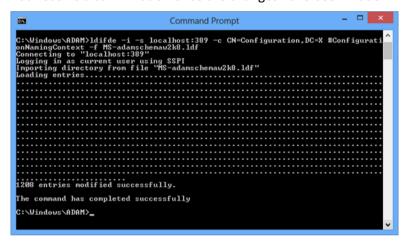
- Users
- Domain
- Passwort for Idifde



Syntax: (user: ADLDS, domain: T08-12en64, password: password): Idifde -i -s localhost:389 -c CN=Configuration,DC=X #ConfigurationNamingContext -f MS-adamschemaw2k8.ldf -b ADLDS T08-12en64 Copadata1

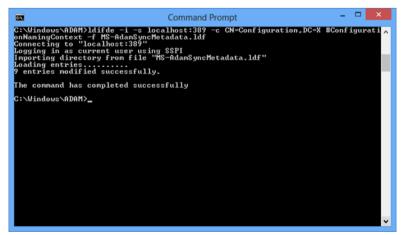


4. You receive a confirmation once the changes have been made.



5. Enter the following command and press the Enter key (the rules for dedicated users also apply here too, as with the previous step):

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



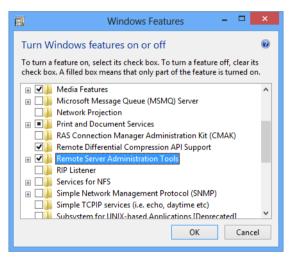


6. You receive a confirmation once it has been successfully carried out.

Installing Remote Server administration under Windows 8

Under Windows 8, you must still install the Remote Server administration. To do this:

- 1. Open Control Panel.
- 2. Open Programs and Features.
- 3. Select Turn Windows features on or off.



- 4. Activate the check box in front of Remote server administration tools.
- 5. Click on OK.

Note: If the **remote server administration tools** are not displayed, download these from the Microsoft website and install them.

Tools

The following tools are helpful for the administration of AD LDS:

- ▶ Microsoft **mmc** with the Active Directory schema snap-in: **mmc -a**
- ▶ ADSI Edit
- ► ADExplorer (can be downloaded from Microsoft Sysinternals)

Configuring Active Directory schema snap-in

To configure the Active Directory schema snap-in:



1. Open the command line with administrator rights.



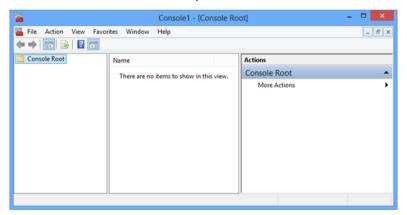
- 2. Enter the following command and press the Enter key: regsvr32 schmmgmt.dll
- 3. You receive a confirmation after successful registration:



4. Open the version.

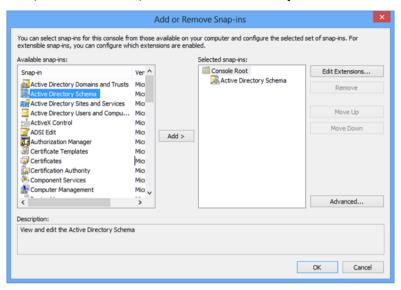
Enter: mmc /a

5. The administration console is opened:

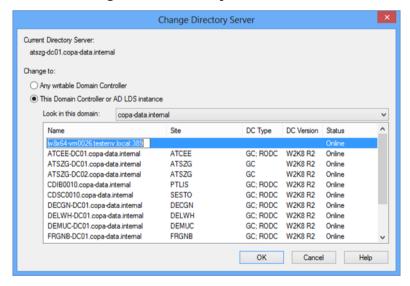




6. Click, in the File menu, on the Add/remove snap-in command.



- 7. Select Active Directory Schema.
- 8. Click on Add.
- 9. Click on OK.
- 10. Highlight the Active Directory Schema entry.
- 11. Select the Change Active Directory Domain Controller command in the context menu

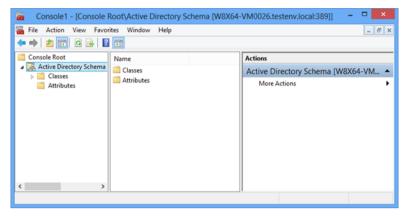




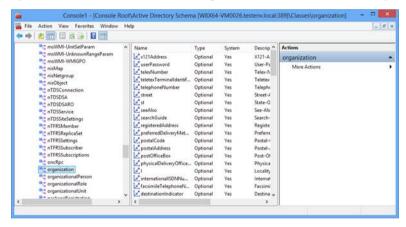
12. Enter the server name and the port in the empty field. In our example: w8x64-vm0026.testenv.local:389.

Select your server and port here.

You now see this view:



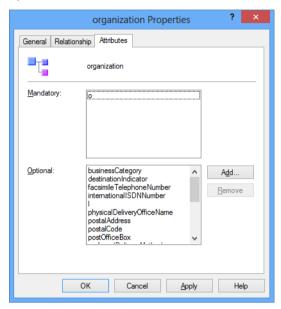
- 13. Save the snap-in via File -> Save.
- 14. Optional:
 - a) Open the **Classes** folder and navigate to the **organization** entry.



b) Click on **Properties** in the context menu.



c) Open the Attributes tab.



d) Click on Add and search for maxPwdAge. Click on OK.

Add lockoutDuration and lockoutThreshold too.

Close the dialog by clicking on **OK**.

These steps are optional and require the corresponding rights. **maxPwdAge** defines the time period in which the password is valid before it must be replaced. **lockoutDuration** defines how long a user is blocked after their password has repeatedly been entered incorrectly. The permitted number of incorrect password entries is defined with **lockoutThreshold**.

- 15. Open the **Classes** folder and navigate to the **user** entry.
 - a) Click on **Properties** in the context menu.
 - b) Open the Attributes tab.
 - c) Click on **Add** and search for **sAMAccountName**. Click on OK. Add groupMembershipSAM and userAccountControl too.

Close the dialog by clicking on **OK**.

16. Close the console.

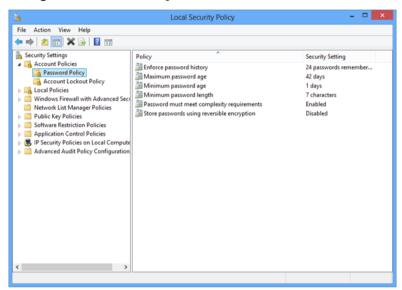
PASSWORD GUIDELINES

The guidelines for password complexity, minimum password length and minimum password age are configured in the local security guidelines of the computer. If the computer on which AD LDS is running is in a workgroup, you see the local security guidelines. If the computer is in a domain, you see the domain security policies. Depending on your installation, you must configure the password guidelines.

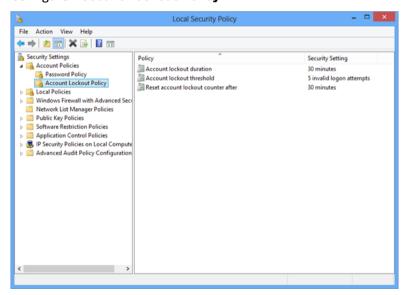
For local security guidelines:



- 1. Go to %ProgramData%\Microsoft\Windows\Start Menu\Programs\Administrative Tools\Tools\
- 2. Start Local Security Policy
- 3. Configure Password Policy



4. Configure Account Lockout Policy



Configure roles, organization units and users

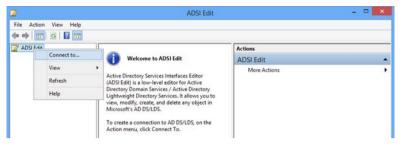
Use the ADSI Editor to configure the roles, organization units and users. You can find it in the path

%ProgramData%\Microsoft\Windows\Start Menu\Programs\Administrative Tools\.

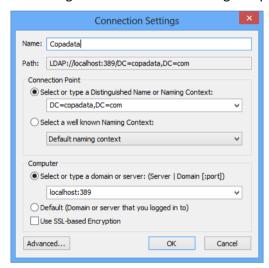


To set up configurations with the ADSI editor:

1. Start the ADSI editor.



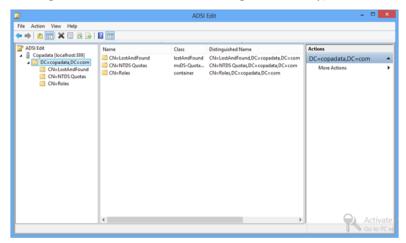
- 2. Select **Establish connection** in the context menu.
- 3. The dialog for the connection settings is opened.



- 4. Configure the following options according to your selected settings:
 - Connection point: DC=copadata, DC=com
 - Computer: localhost: 389
 - Close the dialog by clicking on OK.



5. You should now have the following view of the editor (open the tree in the left window by clicking on the cursor or double clicking on the entry):



This is the starting point for all other configurations. In our example:

- ► Configuring roles (on page 156)
- ► Configuring maxPwdAge (on page 158)
- ► Creating an organization unit (on page 160)
- Creating a group (on page 161)
- ► Creating a user (on page 164)
- ▶ Adding users to groups (on page 168)

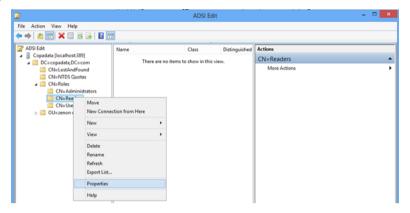
Configuring roles

In this chapter, you find out how you can issue zenon read rights for the structure of the AD LDS tree.

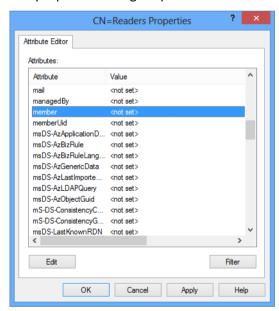
To do this:



1. Expand the folder called CN=Roles.



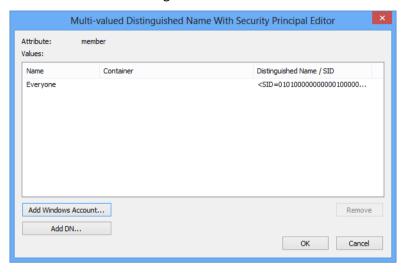
- 2. Highlight CN=Readers.
- 3. select **Properties** in the context menu
- 4. The properties dialog is opened



- 5. Navigate to the **member** entry.
- 6. Click on Edit.
- 7. Click on Add Windows account.
- 8. Add the user **Everyone** (everyone) for the local host.
- 9. Close the dialog.



10. You will have the following view

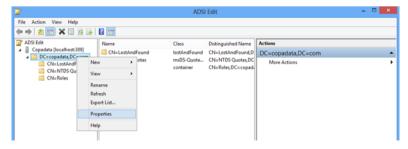


Configuring the password duration

This area is important if you want dedicated password rules for the zenon organization unit. If you do not configure these rules, the local security guidelines of the computer on which AD LDS was installed are applied.

To configure rules:

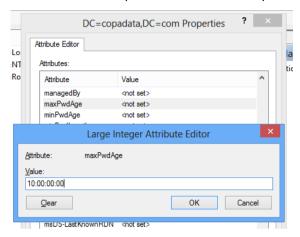
- 1. Highlight the folder called DC=copdata,DC=com.
- 2. Click on Refresh.
- 3. Close the ADSI editor.
- 4. Open the editor again.
- 5. Highlight the entry **DC=copdata,DC=com**.
- 6. Open the properties using the context menu:



7. Navigate to the maxPwdAge entry.

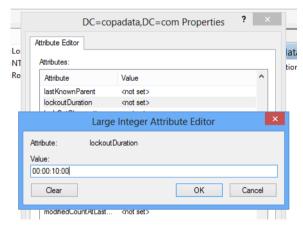


8. Enter a valid value (format: **DD:HH:MM:SS**) and close the dialog.

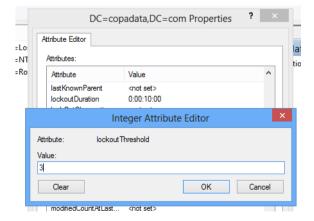


Note: If the entry **maxPwdAge** is not available, check to see if the property has been added correctly. The updating or closing and reopening of the editor can also rectify the problem.

- 9. Navigate to the lockoutDuration entry
- 10. Enter a valid value (format: **DD:HH:MM:SS**) and close the dialog.



- 11. Go to the lockoutThreshold entry.
- 12. Enter a valid value and close the dialog.

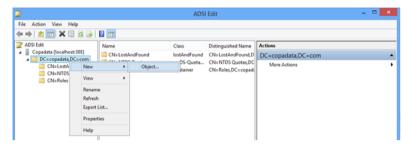




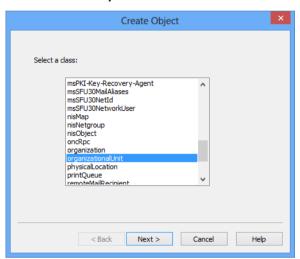
Creating an organization unit

To create a organization unit:

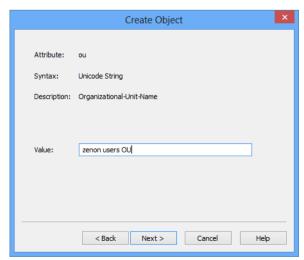
1. Highlight the folder called **DC=copdata,DC=com**.



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



- 3. Select organizational unit as a class.
- 4. Click on Next.



5. Enter a name as a value.

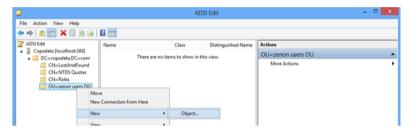


- 6. Click on Next.
- 7. Click on Close.

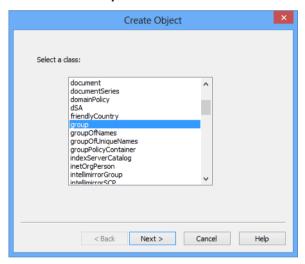
Creating a user group

To create user groups:

1. Highlight the folder with the organization unit that has been created.



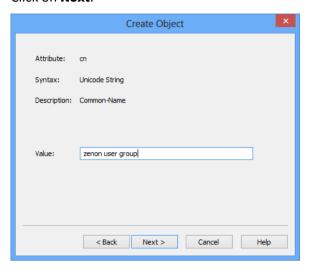
2. Select New -> Object in the context menu.



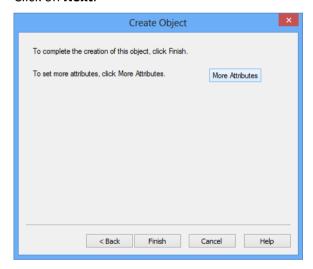
3. Select the **Group** entry.



4. Click on Next.



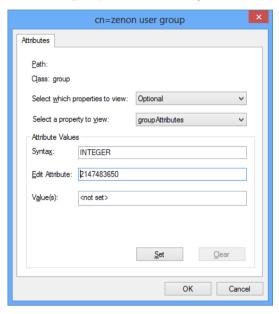
- 5. Enter a name for Value.
- 6. Click on Next.



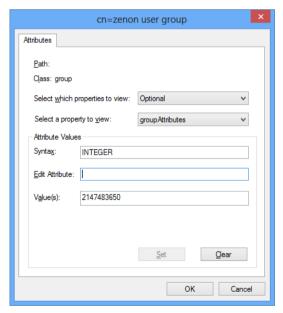
- 7. Click on Finish.
- 8. Click on the More attributes button.



9. Select the **groupAttributes** entry



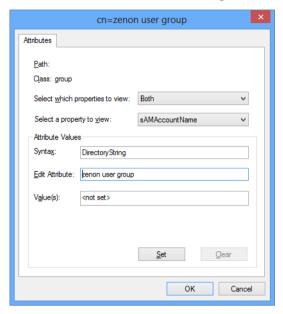
- **10**. Enter 2147483650 in Edit attribute.
- 11. Click on Define.



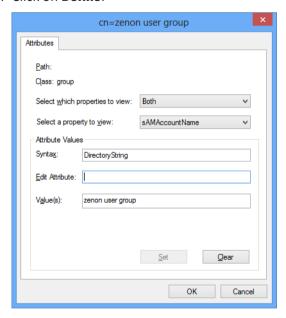
12. Click on **oK**.



13. Select, in the More attributes dialog, the sAMAccountName property.



- 14. Enter the same value as for **group**.
- 15. Click on Define.



- 16. Click on OK.
- 17. Click on Finish.

Creating a user

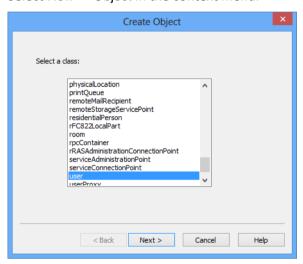
To create a user:



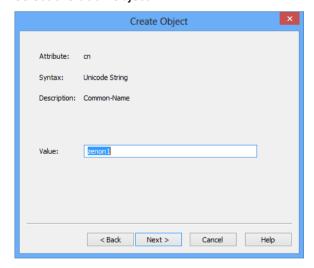
1. Highlight the organization unit.



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



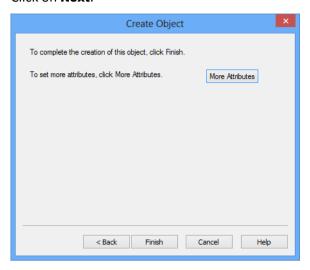
3. Select the User object.



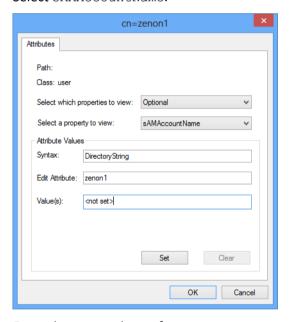
4. Enter a name as a value.



5. Click on Next.



- 6. Click on More attributes.
- 7. Select sAMAccountName.

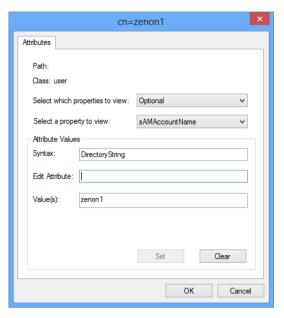


8. Enter the same value as for User.

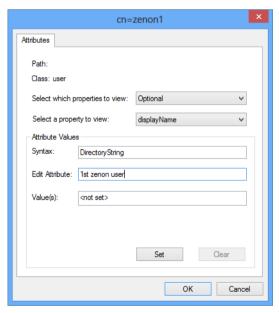
Note: This is important in order for the user to be used in zenon.



9. Click on **Define**.



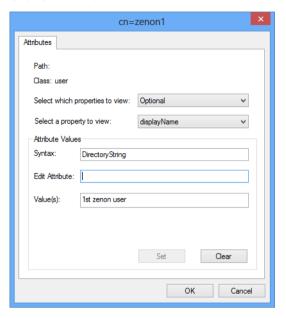
- 10. Click on OK.
- 11. Click on More attributes.
- 12. Select displayName.



13. Enter a description for the display



14. Click on Define.



- 15. Click on OK.
- 16. Click on Finish.

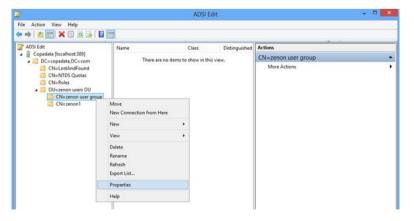
Adding users to groups and setting a password

In this section, you add a user to a group and issue a password.

ADDING A USER

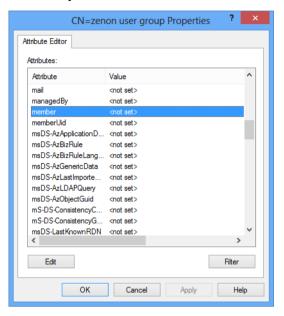
To add users to a group:

1. Highlight the group.

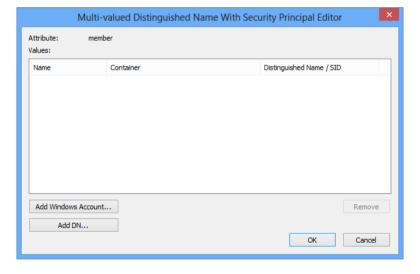




2. select **Properties** in the context menu



- 3. Highlight member
- 4. Click on Edit.



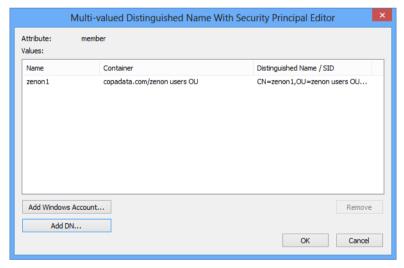


5. Click on Add DN.

The dialog to add a previously-configured user is opened



- 6. Enter, for the user from our example: CN=zenon1,OU=zenon users OU,DC=copadata,DC=com
- 7. Click on **OK** to close the dialog.



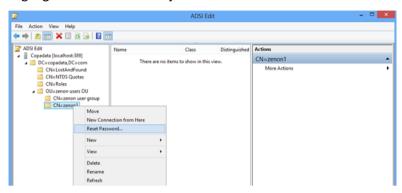
8. Click on OK.

SET PASSWORD

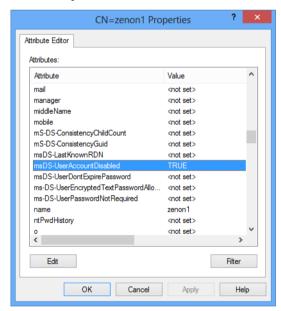
Now define a password for the user. To do this:



1. Highlight the user that has just been created.

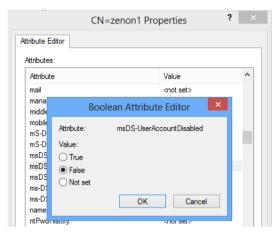


- 2. Select **Reset password** in the context menu.
- Issue a password.
 Note: the password must meet the requirements of the local security guidelines.
- 4. Close the dialog.
- 5. Select **Properties** in the context menu of the user





6. Select msDS-UserAccountDisabled in the properties.



7. Set the value to incorrect.

The user can now be used in zenon.

6.2.2 AD LDS with Windows 7

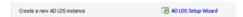
AD LDS can also be used with Windows 7. You can find the setups for these on the Microsoft website (http://www.microsoft.com/downloads/en/default.aspx).

After installation, configuration is carried out via System control-> Administration in the same way as the description for Windows Server 2008 (on page 192).

Create new AD LDS instance

To create a new AD LDS instance:

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

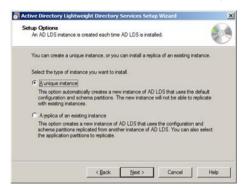




2. Start the wizard:



3. Select the A unique instance option.



4. Give the instance a name.



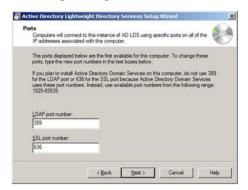
5. Configure the ports. Default:

• **LDAP**: 389

• SSL: 636

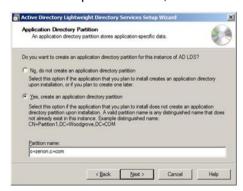


Note: If you change the pre-set port here, you must also amend the port in some of the following settings.



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 <code>Currently logged on user</code>. In our case, a local user with administrator rights.



The user and their password are used later in zenon.

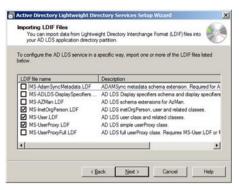


This configuration can be set up later. Continue with configuration in the wizard.

- 10. Import the required LDIF files:
 - MS-InetOrgPerson.LDF



- MS-User.LDF
- MS-UserProxy.LDF



11. Finish the installation





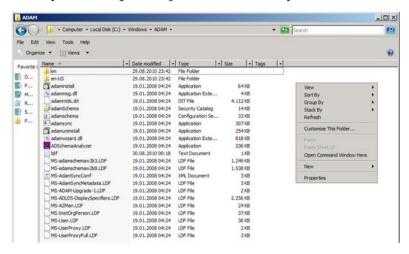
Importing an AD LDS schema

To import the AD LDS schema:

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

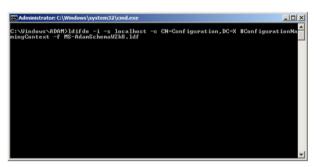


2. Select [Shift key + right mouse click] in the context menu: Open input request here.

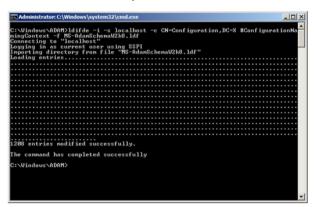


3. Enter the following character string:

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



4. Press the Return key:



5. Enter the following character string:

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



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

```
    □ Administrator: C\Windows\system32\cmd.exe
    □ X
    C:\Windows\ADAH>\Idifde -i -z localhost:389 -c CN=Configuration, DC=X #ConfigurationNaningContext -f HS=fidanSyncHetadata.ldf
```

6. Press the Return key:

Configuring the AD Snap-in schema

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

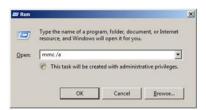
- 1. Click on the Start button.
- 2. Navigate to Command prompt.
- 3. Select Run as administrator in the context menu.
- 4. At the command prompt, enter: regsvr32 schmmgmt.dll.
- 5. Confirm by pressing the **Return** key.



CONFIGURATION

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

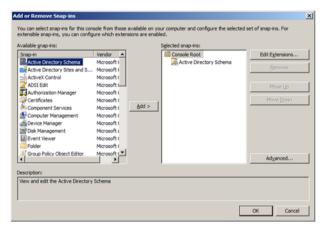




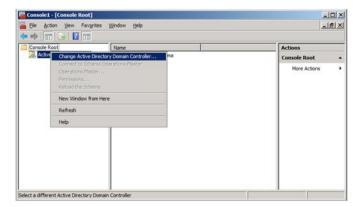
4. Click on File -> Add/Remove Snap-in....



- 5. Select Active Directory Schema.
- 6. Click Add.
- 7. Click OK.

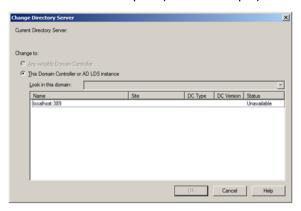


- 8. Go to Active Directory Schema.
- 9. Select Change Active Directory Domain Controller... in the context menu





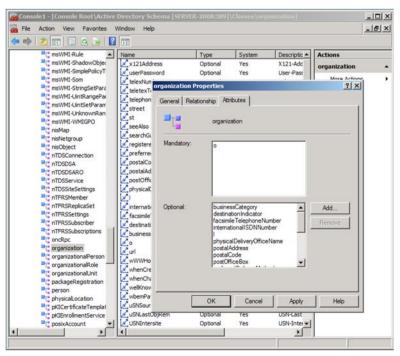
10. Enter the server and port (in this example) localhost: 389).



11. You should now see this window:



- 12. Go to Classes -> organization.
- 13. Open Properties:



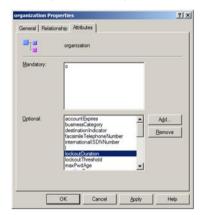
- 14. click Add.
 - a) Search for maxPwdAge.



b) Click **oK**.



c) Repeat this step for lockoutDuration



d) and for lockoutThreshold.





15. Click **OK**.



- 16. Open the **Classes** folder and navigate to the **user** entry.
 - a) Select the **Properties** entry in the context menu.
 - b) Open the Attributes tab.
 - c) Click on Add and look for sAMAccountName.
 - d) Click OK.
 - e) Also add groupMembershipSAM and userAccountControl.
 - f) Close the dialog by clicking on **OK**.
- 17. Close the console.

Note:

- ► These steps are absolutely necessary to have maxPwdAge available in the organization unit, 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



Configure organization units, groups and users

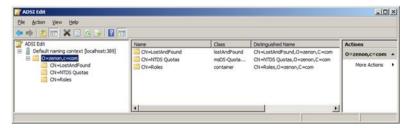
To configure organization units, groups and users:

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

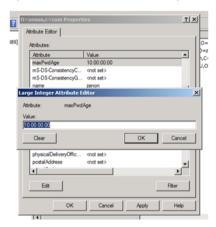
- 1. Highlight O=zenon,c=com
- 2. Click on Refresh
- 3. Close ADSI Edit
- 4. Open ADSI Edit again
- 5. Highlight O=zenon,c=com



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

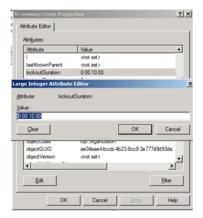


- 7. navigate to maxPwdAge
 - a) Enter a valid value
 - b) Format: DD: HH: MM: SS (in our example 10:00:00:00)



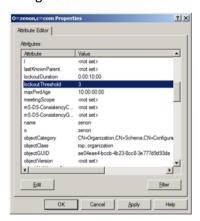
Note: If the maxPwdAge property is not visible, check to see that it has been correctly added. A refresh, or closing and opening **ADSI Edit** or reloading the schemas may rectify the problem.

- 8. Navigate to lockoutDuration
 - a) Enter a valid value
 - b) Format: DD:HH:MM:SS (in our example 00:00:10:00, -> 10 minutes)

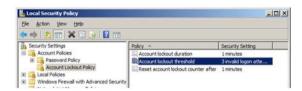




9. Navigate to lockoutThreshold



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

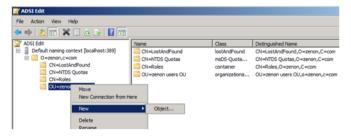


Note: The settings for the duration of the account block are ignored in AD LDS. The **lockoutDuration** property (O=zenon, c=com) is used.

Users

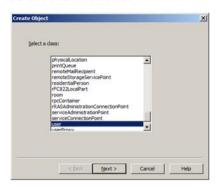
To create a user:

- 1. Highlight the organization unit
- 2. Select New -> Object in the context menu





3. Select the **User** class



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



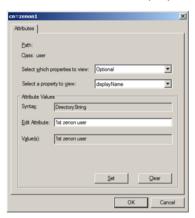
- 5. Click on Next
- 6. Switch to the Attributes tab
- 7. Click on More attributes
 - a) Navigate to Select a property to view
 - b) Select sAMAccountName in the drop-down list
 - c) Navigate to Edit Attribute
 - d) Enter the same value as for the user (zenon1)(this configuration is necessary in order 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:

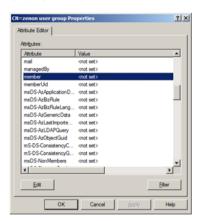
- 1. Select zenon user group
- 2. Select **Properties** in the context menu.



3. Highlight member



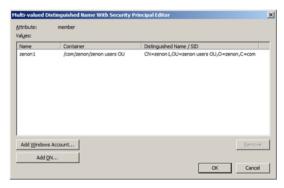
4. Click on Edit.



- 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:



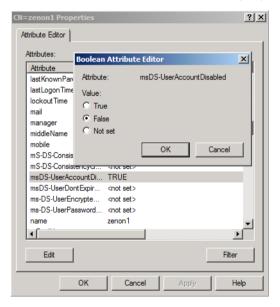


6. Define a password for the user zenon1



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

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



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

Organization units

To create a organization unit:

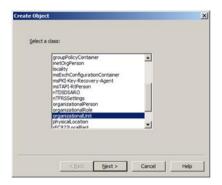
1. Highlight O=zenon,c=com



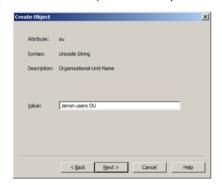
2. Select New -> Object in the context menu



3. Select organizationalUnit



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



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

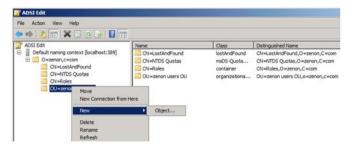
Groups

To create a group:

1. Highlight the organization unit



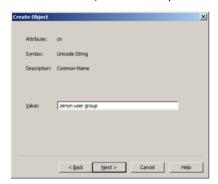
2. Select New -> Object in the context menu



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

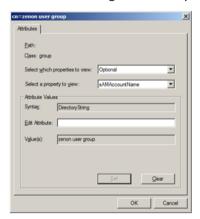


d) Enter the value 2147483650 (represents an account group)



- 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



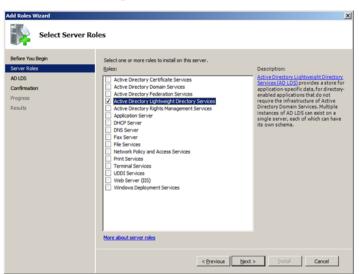
11. Click on **OK** and then in **Finish**

6.2.3 AD LDS with Windows Server 2008

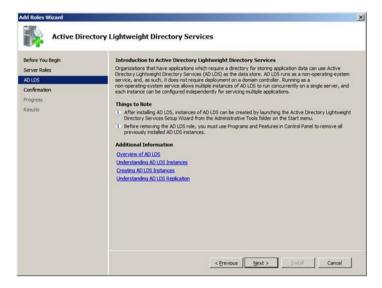
To install the AD LDS server role:



1. Select Server Manager in the administrative tools

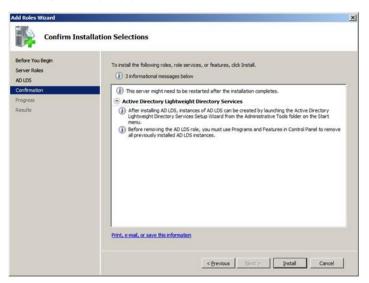


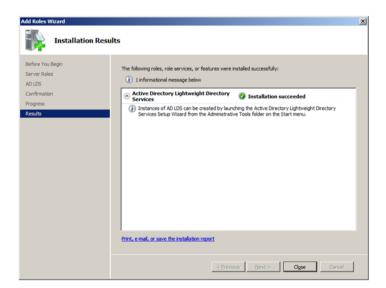
2. Click on Add Roles





3. Add the AD LDS Role





6.2.4 zenon administration with Active Directory

For use in zenon, first configure the settings in the Editor (on page 195) and set the user identification to AD LDS level in Runtime (on page 195).



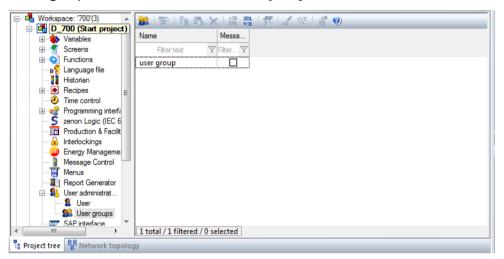


Editor

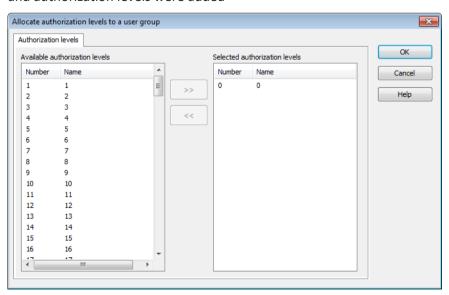
Configuration is carried out in the project properties in User Administration:



▶ A user group with the name zenon user group was created



and authorization levels were added



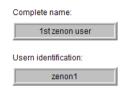
Runtime - system driver variables

► The user **zenon1** can log in to zenon:

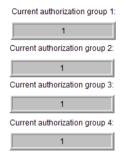
The Complete name property in zenon corresponds to the AD LDS attribute displayName.



The User name property corresponds to the AD LDS attribute samaccountName.



▶ 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):



ERROR TREATMENT

If errors in Runtime occur, check if:

- ► The settings have been set up correctly:
 - User name
 - 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:

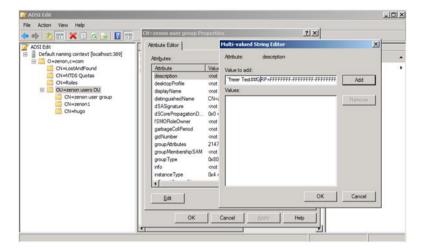
- The names correspond to each other
- ▶ sAMAccountName of the group in **AD LDS** was set
- ► The user in AD **LDS** was added to the group



ΑD

If operating authorizations from the user group in **AD** 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 125) section.

6.2.5 Problem handling

CHECK THE CONNECTION TO THE AD LDS DIRECTORY

- 1. Start the Microsoft ADExplorer on the computer on which the zenon Editor or zenon Runtime is used.
- 2. Attempt to establish a connection to the AD LDS directory with the settings used in zenon.
- 3. The causes of the error can be:
 - Incorrect host name
 - Incorrect port
 - Firewall rules in the network

USER CANNOT LOG IN

Check to see if all attributes are set correctly in AD LDS:

▶ sAMAccountName



- ▶ groupMembershipSAM
- ▶ userAccountControl

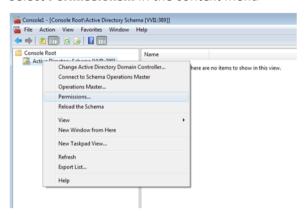
THE USER DOES NOT RECEIVE ALL AUTHORIZATION LEVELS THAT WERE ASSIGNED TO THEM.

- Please check:
- ▶ Is the Name of the zenonUser Group configured the same that in AD LDS?
- ▶ Is the AD LDS user assigned to the corresponding AD LDS group?
- ▶ Is the attribute sAMAccountName set in the AD LDS group?

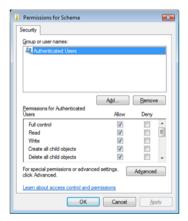
NO CONTENT IN THE SNAP-IN

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

1. Select Permissions... in the context menu



2. Assign the necessary users the corresponding rights (you add new users by clicking on **Add**)

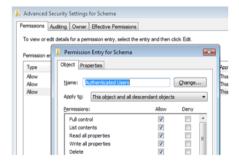




3. Click on the Advanced button



- 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

6.3 Active Directory Application Mode - ADAM (Windows XP only)

Active Directory Application Mode (ADAM) is designed for use with Windows XP. Windows XP is no longer supported by zenon, because Microsoft has discontinued the product and no longer supports it. This documentation only relates to systems that still run under Windows XP.

For current operating systems, use Active Directory Lightweight Directory Services (on page 137):

- Windows 7
- ▶ Windows 8/8.1
- ▶ Windows Server 2008
- Windows Server 2012

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 200)



- 2. Bring in an AD schema (on page 202)
- 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 203) 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 124).
 - You can create the zenon authorization levels as described in Using the Active Directory (on page 124) under attributedescription.



Information

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

6.3.1 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.



Information

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.



Information

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(x86)%\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.



Information

When installing ADAM on a Windows XP XP, you must install these files on the same logical volume. When installing ADAM under Windows Serve 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.



Q

Information

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.



Information

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.

6.3.2 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:

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

Press the Return key.

6.3.3 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. about AD/AD LDS properties used in zenon

ENCRYPTION

NTLM/Kerberos encryption is used to log in a zenon AD/ADAM user. No explicit encryption is envisaged for ADSI (MS APIs for AD) for the exchange of data other than passwords in the session that is already logged on.



LIST OF THE PROPERTIES IN AD/ AD LDS USED BY ZENON

DOMAIN

General form	Remark
defaultNamingContext	
distinguishedName	From containers.
name	From containers.
objectClass	From containers.
maxPwdAge	
lockoutDuration	

USER GROUP

General form	Remark
distinguishedName	
name	
sAMAccountName	
member	Possible amendment of the value necessary in AD/AD LDS.
description	
groupMembershipSAM	Is set when editing in zenon in the Active Directory user administration screen.
groupType	
objectClass	

USERS

General form	Remark
distinguishedName	
sAMAccountName	
displayName	
memberOf	Possible amendment of the value necessary in AD/AD LDS.
mail	
telephoneNumber	
Mobile	



pwdLastSet	
userAccountControl	
groupMembershipSAM	Is set when editing in zenon in the Active Directory user administration screen.
userPrincipalName	Possible amendment of the value necessary in AD/AD LDS.
objectClass	
objectCategory	
ZenOnUserLevel1	Not a default property of AD/AD LDS. Is not normally needed. Only present for compatibility reasons.
ZenOnUserLevel2	Not a default property of AD/AD LDS. Is not normally needed. Only present for compatibility reasons.
ZenOnUserLevel3	Not a default property of AD/AD LDS. Is not normally needed. Only present for compatibility reasons.