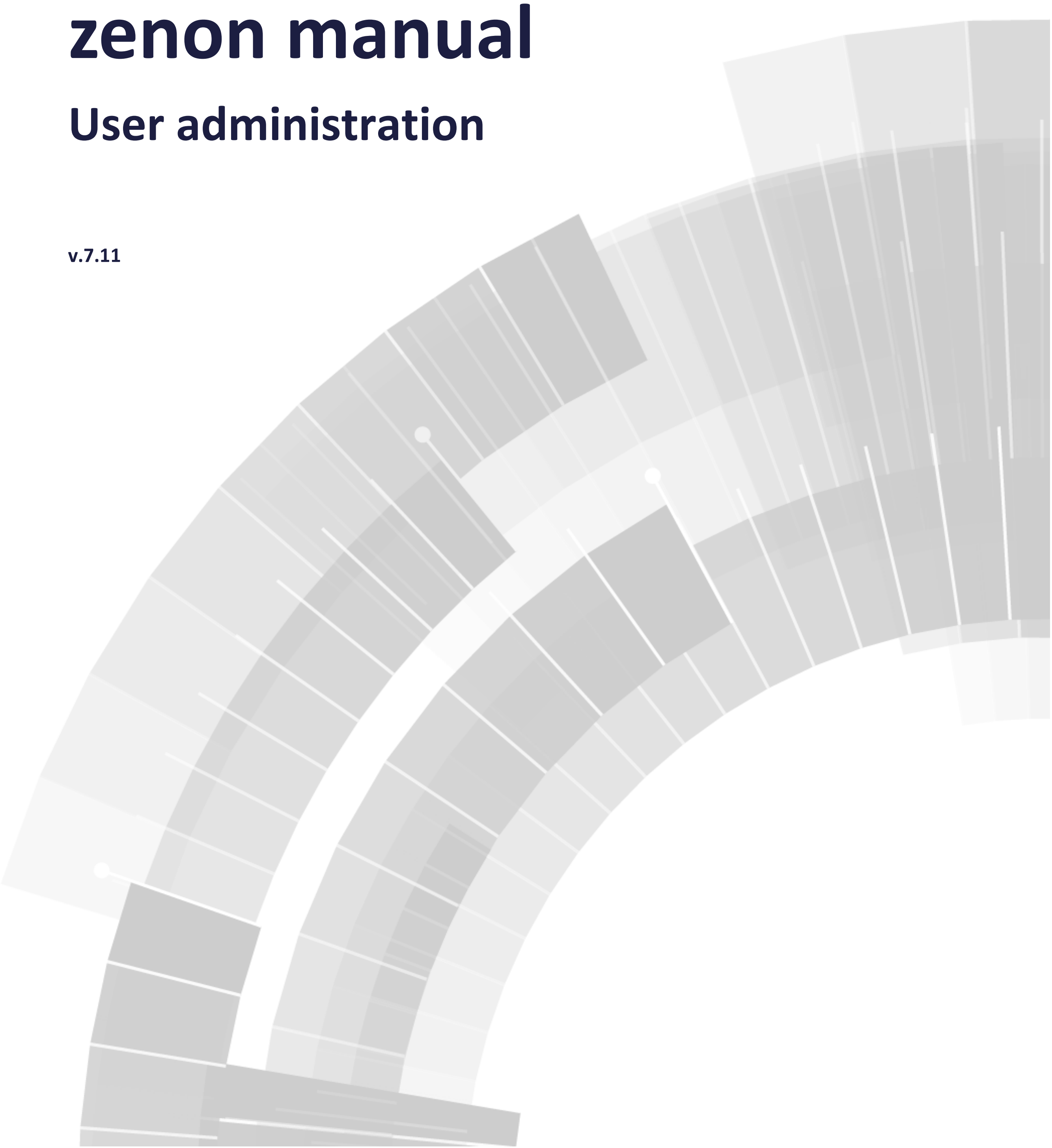
zenon manual

User administration

v.7.11



Contents

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 a user administration for the Editor and for the online operation (Runtime). The password system fulfills the guidelines of the FDA (Food and Drug Administration, 21 CFR Part 11). It is also possible to administer Active Directory users (on page 50) 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 46) 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 47) 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 43) 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 48) function. The user SYSTEM is thus logged in.

CREATING USERS AND ISSUING RIGHTS

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

1. 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 70):

Active Directory Lightweight Directory Services (on page 85) (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 71) (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 145), if user groups with the same name are created in zenon. A separate screen can be used to 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 39). Not all changes in the Editor are accepted after a simple reload (on page 44). 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 Context menu Project manager

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

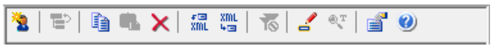
Menu item	Action
`New user`	Opens the dialog for creating a new user and adds the new user to the list of the detail view.
`Export XML all...`	Exports all entries as an XML file.
`Import XML`	Imports entries from an XML file.
`Editor profile`	Opens the drop-down list with predefined editor profiles.
`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 Detail view of toolbar and context menu



Menu item/symbol	Action
New user	Opens the dialog for creating a new user and adds the new user to the list of the detail view.
Jump back to starting element	If you entered the list via function **linked elements**, the symbol leads back to the start element. Only available in the context menu when all linked elements are opened.
Copy	Copies 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.
Copy	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

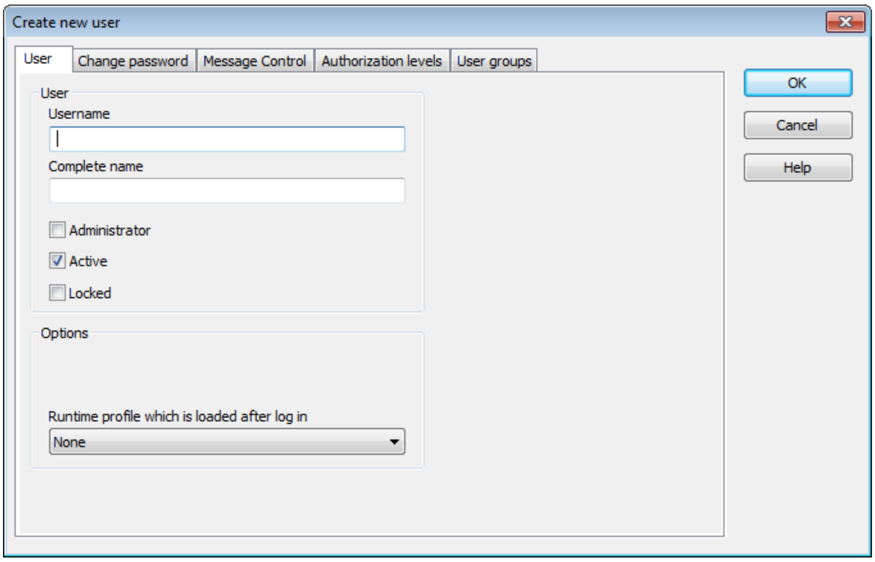
To create a new user:

1. navigate to node `User administration/User`
2. in the context menu of the project manager, the detail view or in the tool bar 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:



User

Username

Complete name

☐ Administrator

☑ Active

☐ Locked

Options

Runtime profile which is loaded after log in

None

Parameters	Description
Username	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 for the command in order to lock and unlock different areas.
Runtime profile which is called up at the log in.	Selection of the Runtime profiles from the drop-down list: ▸ None ▸ Default ▸ Last
OK	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.

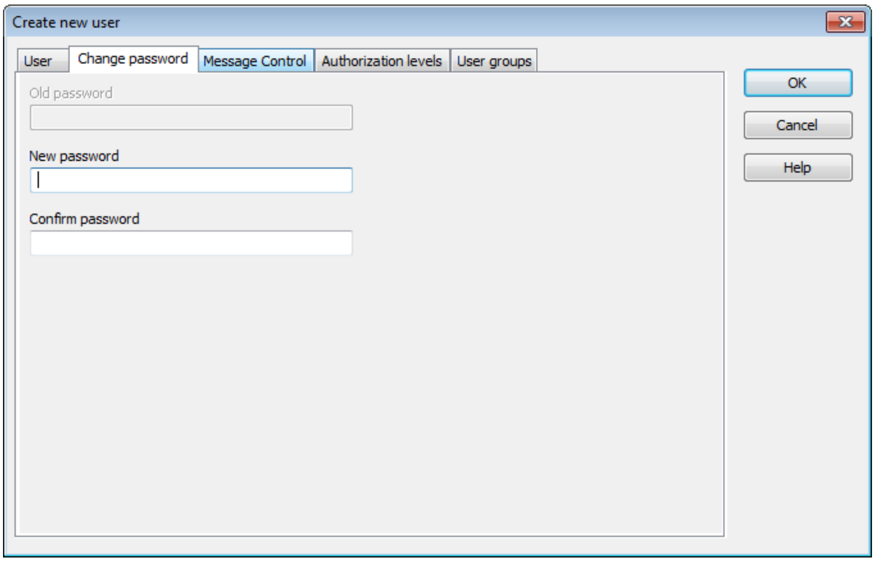
Information

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

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 `Min. password length` in group `User administration`. The default value is 6 characters.

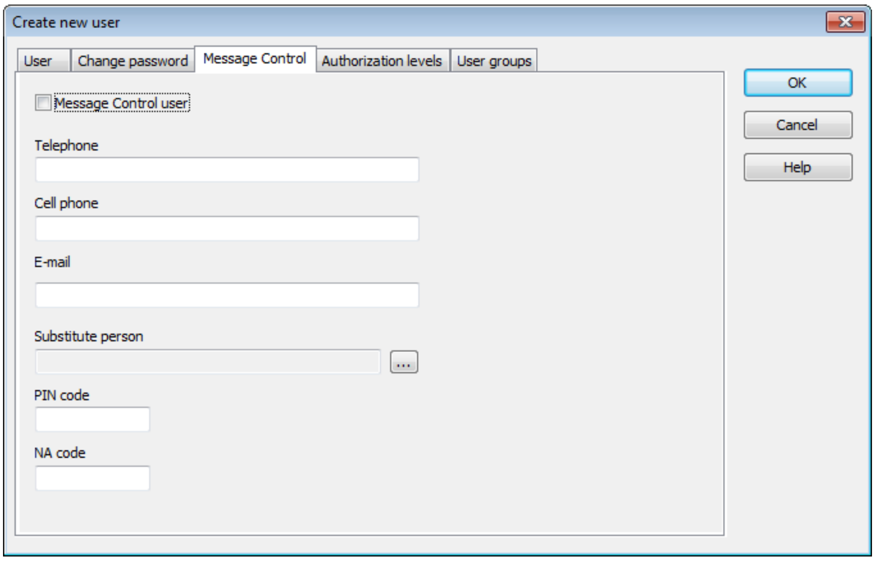


Parameters	Description
Old password	Current password.
New password	Enter new password. For language-spanning projects take care that it must be possible to enter the characters with the respective keyboard in the Runtime.
Confirm password	Repeat the password.
OK	Applies all changes in all tabs and closes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

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

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	Fixed network telephone number of the user. Used for text to speech. Enter numbers. The prefix + abbreviating 00 of the international area code is permitted.
Cell phone	Mobile phone number of the user. Used for messages via GSM and SMS (text messages). Enter numbers, the prefix + abbreviating 00 of the international area code is permitted.
Email	E-mail address of the user
Substitute person	Select a substitute person if the user cannot be reached or the receipt of the message is rejected. A click on button ... Opens the dialog to select a user.
PIN code	PIN code with which the user confirms the message.
NA code	PIN code with which the user rejects the receipt of the message (not available). Message is subsequently sent to the next user in the list.
OK	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.

⚠ **Attention**

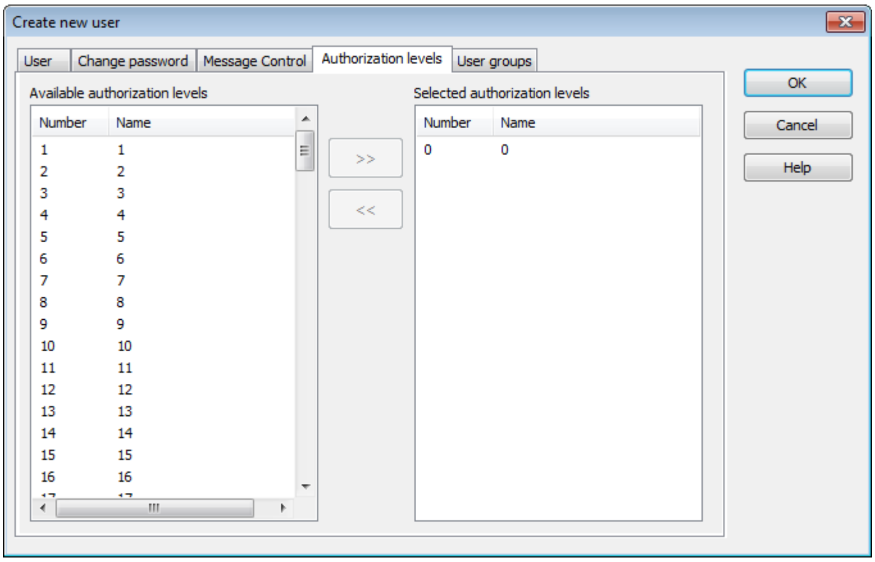
The acknowledgment codes for PIN (confirmation) and NA (rejection) must differ and should not be too similar.

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

If an unknown code is received, an 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.



Create new user

Available authorization levels

Number	Name
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	10
11	11
12	12
13	13
14	14
15	15
16	16

Selected authorization levels

Number	Name
0	0

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

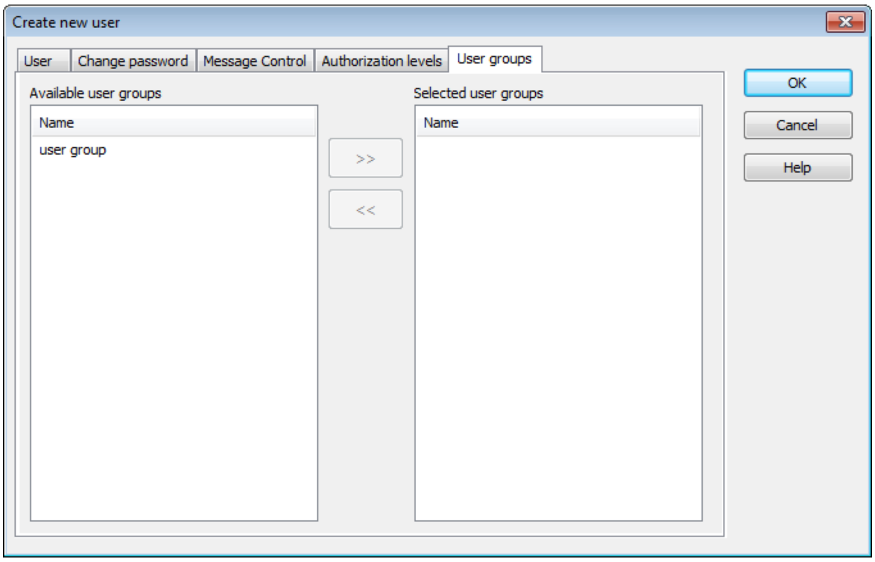
Info

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

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

3.3.5 User groups

Assignment of the user to user groups.



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

> **Info**
>
> *With the help of `Ctrl` and/or `Shift` you can select more than one entry at a time.*
>
> - By pressing and holding `Ctrl` you can select a number of entries.
> - By pressing and holding `Shift` and select two entriey, you select all entries which lie between the two selected entries.
> - By pressing and holding both `Ctrl` and `Shift` and selecting two entries, all entries which lie between the selected entries are selected. The entries which were selected beforehand remain selected.

3.4 Create a user group

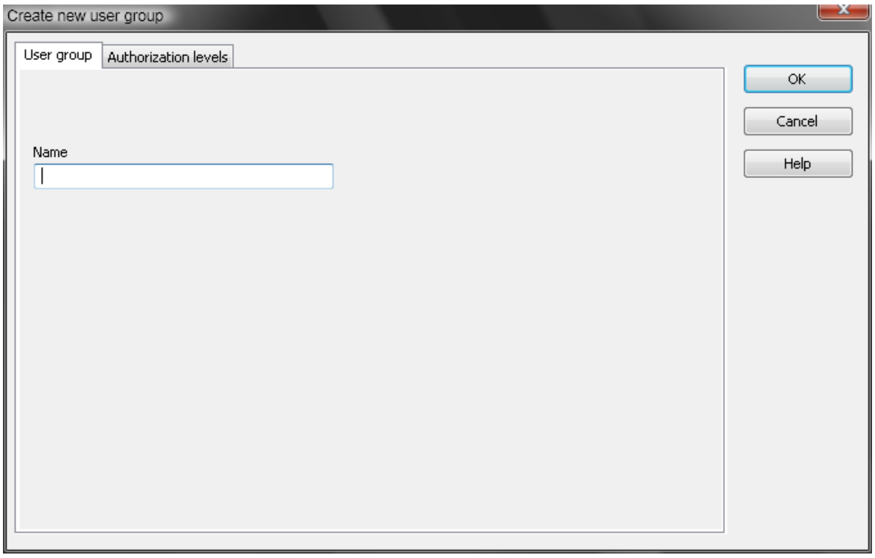
To create a user group:

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 21) and authorization levels (on page 22)

> ### 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 standard project are used in the event of a conflict. If the local group is deleted, the user again receives the rights from the group of the global project after the Runtime files are compiled in the Editor.*
>
> ***Example:***
>
> *A user group* **`A`** *is present in both the local project and in the global project. In the global project it is allocated the authorization levels `1`, `2`, `3`, `100` and `101`, and authorization levels `1` and `2` in the local project. In Runtime, the rules from the local project apply; only the authorization levels `1` and `2` are allocated. If user group A is not present in the local project, members of group* **`A`** *have authorization levels `1`, `2`, `3`, `100` and `101` from the global project.*

3.4.1 Naming a user group



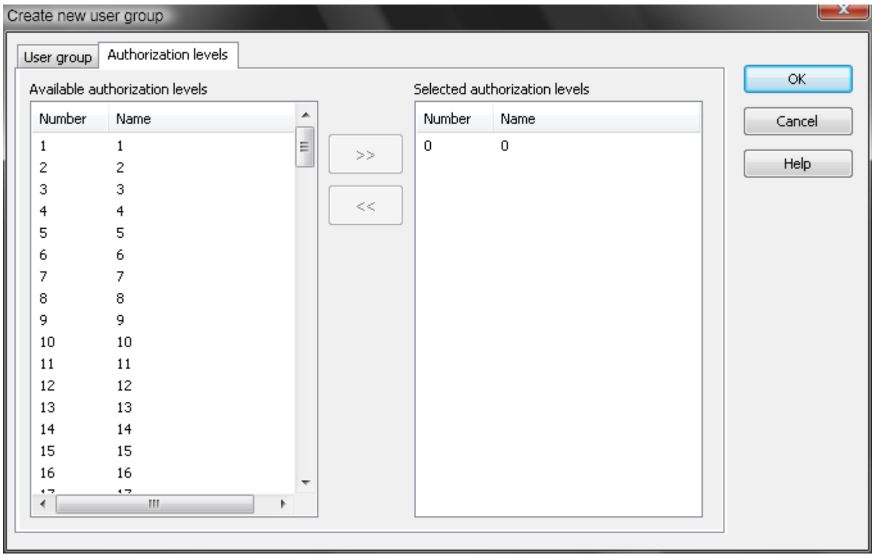
Enter the name of the user group you want to create.

Information

@ is not a valid character for a user group.

3.4.2 Authorization levels

Assignment of the authorization level to a user group.



Available authorization levels

Number	Name
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	10
11	11
12	12
13	13
14	14
15	15
16	16

Selected authorization levels

Number	Name
0	0

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

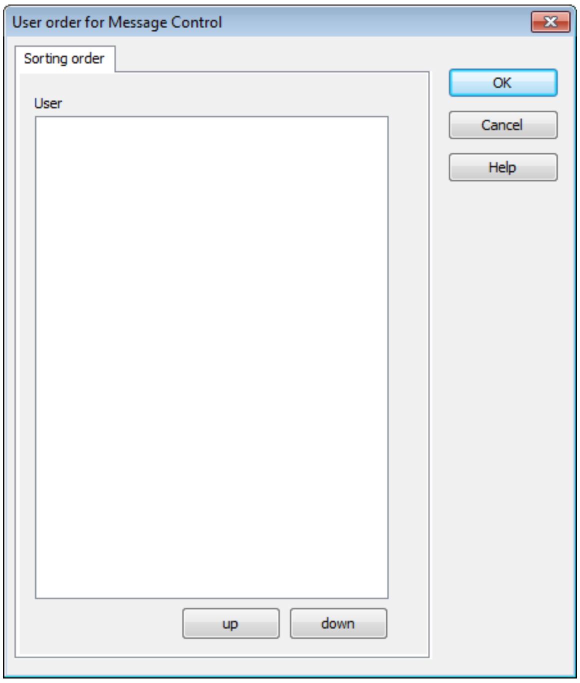
Info

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

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

3.4.3 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.
OK	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. The respective parameters are displayed in the properties window as a result of this. You can change the parameters User name, Full name, Password, authorization level and User groups.

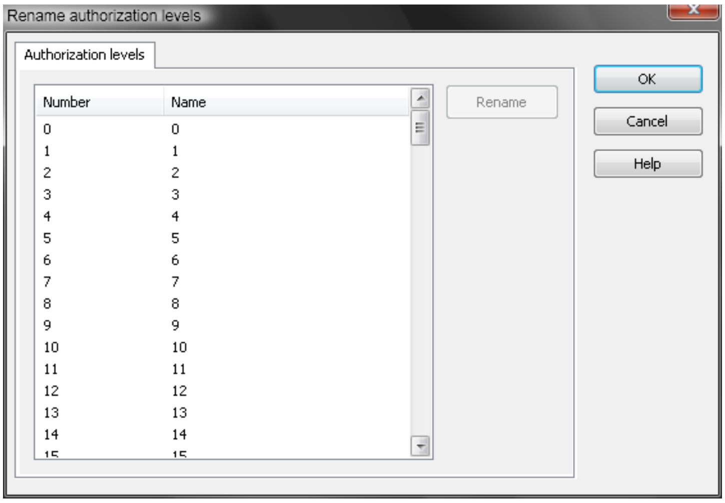
3.6 Changing a user group

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.



Number	Name
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	10
11	11
12	12
13	13
14	14
15	15

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: Tool bars 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 27).

ASSIGNING THE FUNCTION AUTHORIZATIONS

This assignment is effected by means of:

- Function authorizations Runtime (on page 28)
- 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 drag over and drag & drop take module rights into account.
- For module rights that are not granted:
  - The respective menu and tool bars are grayed out in the zenon Editor.
  - No 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

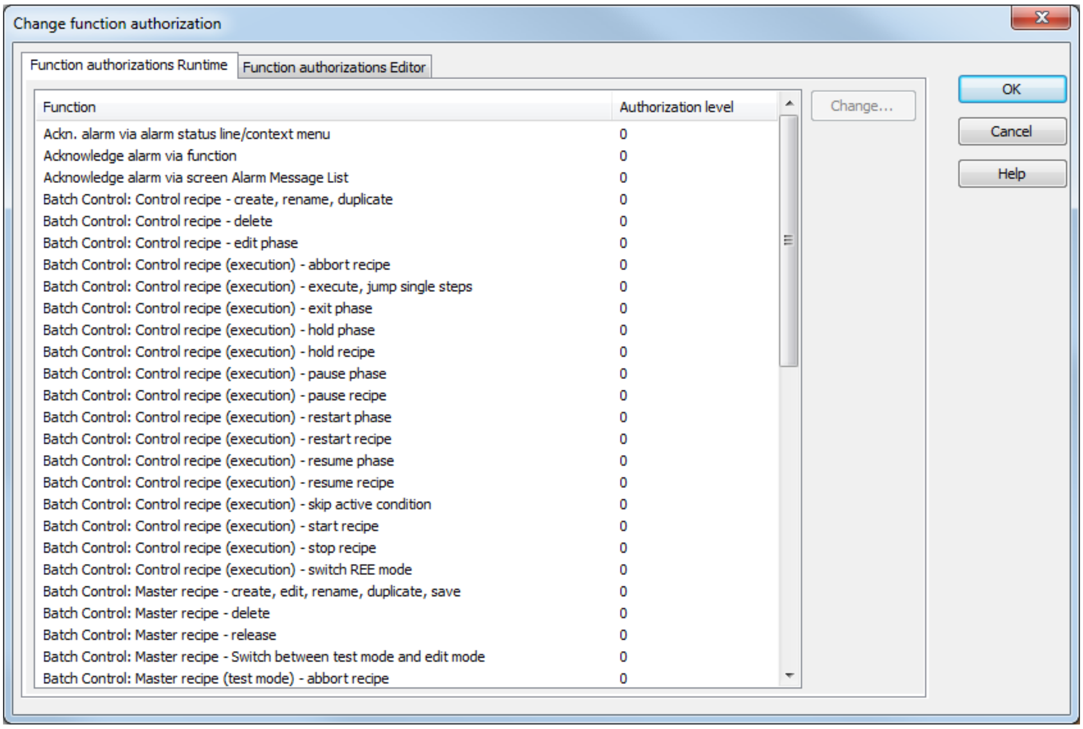
To issue a function authorization:

1. Select the user administration project properties in the project properties `User administration`
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 and/or for the respective module in the Editor.
5. Allocate the desired function authorization to an authorization level (on page 22).

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 and/or the project has been reloaded.

3.8.2 Function authorizations Runtime



Change function authorization
Function authorizations Runtime
Function authorizations Editor
Change...
OK
Cancel
Help

Function	Authorization level
Ackn. alarm via alarm status line/context menu	0
Acknowledge alarm via function	0
Acknowledge alarm via screen Alarm Message List	0
Batch Control: Control recipe - create, rename, duplicate	0
Batch Control: Control recipe - delete	0
Batch Control: Control recipe - edit phase	0
Batch Control: Control recipe (execution) - abbort recipe	0
Batch Control: Control recipe (execution) - execute, jump single steps	0
Batch Control: Control recipe (execution) - exit phase	0
Batch Control: Control recipe (execution) - hold phase	0
Batch Control: Control recipe (execution) - hold recipe	0
Batch Control: Control recipe (execution) - pause phase	0
Batch Control: Control recipe (execution) - pause recipe	0
Batch Control: Control recipe (execution) - restart phase	0
Batch Control: Control recipe (execution) - restart recipe	0
Batch Control: Control recipe (execution) - resume phase	0
Batch Control: Control recipe (execution) - resume recipe	0
Batch Control: Control recipe (execution) - skip active condition	0
Batch Control: Control recipe (execution) - start recipe	0
Batch Control: Control recipe (execution) - stop recipe	0
Batch Control: Control recipe (execution) - switch REE mode	0
Batch Control: Master recipe - create, edit, rename, duplicate, save	0
Batch Control: Master recipe - delete	0
Batch Control: Master recipe - release	0
Batch Control: Master recipe - Switch between test mode and edit mode	0
Batch Control: Master recipe (test mode) - abbort recipe	0

FUNCTION AUTHORIZATIONS FOR ALARMS

Parameters	Description
`Change alarm comment`	A Comment necessary for acknowledgement may be changed.
`Enter alarm comment`	A comment necessary for acknowledgement 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 an authorization in the I-project. **Comment:** System messages are messages that appear in the alarm status line when a certain (configurable) number of alarms has been reached.
`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: 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: 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) - switch REE mode`	When executing control recipes in the Batch Control module, the REE mode can only be switched 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`	Master recipes in the Batch Control module can only be

recipe - highlight as outdated	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) - switch REE mode	In test mode, with master recipes in the Batch Control module, the REE mode can only be switched 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	In test mode, with master recipes in the Batch Control

`recipe (test mode) - continue recipe`	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.

FUNCTION AUTHORIZATIONS, GENERAL

`Edit Extended Trend`	Curves in Extended Trend can be edited in Runtime. The following control elements are inactive if the user does not meet authorization requirements: ▸ Diagram ▸ Curves ▸ Frame ▸ activate ▸ axis
`Return to last screen (PgUp)`	Screen 'back' functions can be executed in Runtime.
`Screen catalogue`	The function screen switch (Screen - functions) with the set option show this dialog during Runtime can only be executed, if the user who is logged in fulfills authorization requirements.
`Notepad: Open file`	The function file `open` in screenNotepad can only be carried out if the logged in user has the appropriate authorization level.
`Notepad: Save file`	The function `save` in screenNotepad can only be carried out if the logged in user has the appropriate authorization level.

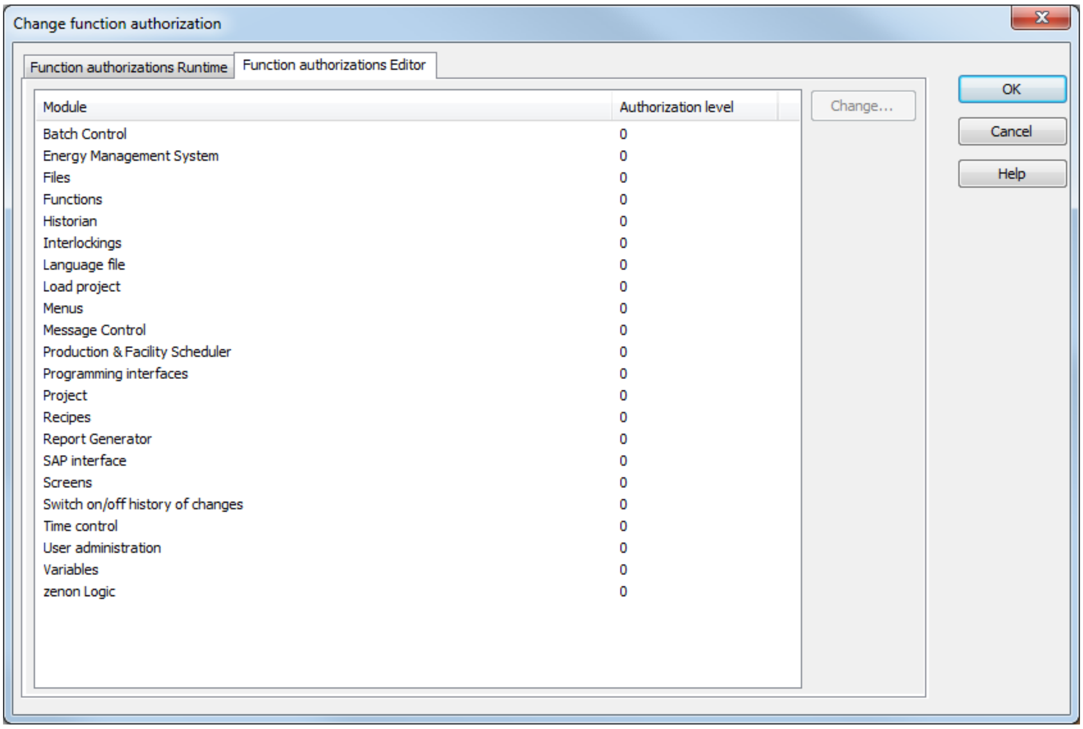
For all actions, the user must be logged in and have the corresponding authorization levels.

Information

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

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

3.8.3 Function authorizations Editor



Change function authorization
Function authorizations Runtime
Function authorizations Editor
Change...
OK
Cancel
Help

Module	Authorization level
Batch Control	0
Energy Management System	0
Files	0
Functions	0
Historian	0
Interlockings	0
Language file	0
Load project	0
Menus	0
Message Control	0
Production & Facility Scheduler	0
Programming interfaces	0
Project	0
Recipes	0
Report Generator	0
SAP interface	0
Screens	0
Switch on/off history of changes	0
Time control	0
User administration	0
Variables	0
zenon Logic	0

Parameters	Description
`Load project`	The project database 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.
`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.
`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.
`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.
`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.
`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.
`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.
`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.
`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.
`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.
`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.

Parameters	Description
zenon Logic	Only then can straton projects be edited or engineered in the Editor, 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.
Interlockings	Only then can interlockings be edited or engineered in the Editor, If the logged-in user is assigned to the corresponding user level.
Energy Management System	Only then is the Production and Facility Scheduler module available in the Editor for editing and engineering, 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 engineering, 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.
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.
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.
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.
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.
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.
Change	Opens the dialog to select the authorization levels.

Parameters	Description
OK	Accepts changes in all tabs and closes dialog.
Cancel	Discards changes in all tabs and closes dialog.
Help	Opens online help.

Info

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

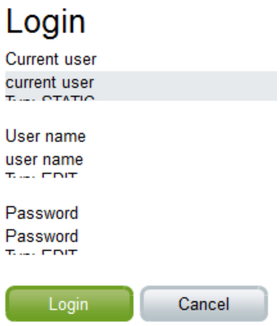
- By pressing and holding `Ctrl` you can select a number of entries.
- By pressing and holding `Shift` and select two entriey, you select all entries which lie between the two selected entries.
- By pressing and holding both `Ctrl` and `Shift` and selecting two entries, all entries which lie between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

3.9 Creating a screen of the type Login

Login in Runtime is generally carried out using a login (on page 37) screen. To create this screen:

1. Create a new screen in the Editor.
2. Select `login` as the screen type.
3. Select **Add template** in the control elements menu.
4. Adapt the screen to your requirements:
5. Create a function for screen switching to this screen and link it with a button.

SCREEN OF TYPE LOGIN



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 palced in the screen. Elements can be moved in the screen and placed individually.
`Current user (display)`	Display of the currently logged in user
`Username`	Input area for user idenfiication.
`Password`	Input field for password.
`OK`	Button to close the screen after login.
`Cancel`	Cancels the login process.
`Accept`	Button for logging in without closing the window.

RULES FOR LOGIN IN RUNTIME.

When logging in to the Runtime the following is true:

- After tree wrongly entered passwords, the user is locked for the system. Only the administrator can unlock the user.

- After entering a not existing username the system is locked. The system cannot be operated by any user and must be unlocked by an administrator.
- If a correct username is used at login but the password field remains empty no reaction happens. The system is not locked.

For details see **Operation in Runtime** (on page 39) chapter.

4. zenon login and user administration in Runtime

In order to log a user in actively in Runtime, there must be screen switching to a login (on page 37) screen.

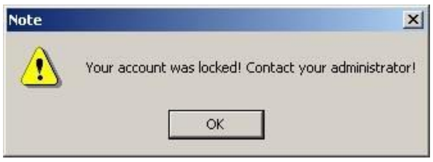
LOGIN

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 43) be logged into all subprojects.

Logging in in the Runtime has the following safety precautions:

- Password

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

  Note

  Your account was locked! Contact your administrator!

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

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

- Username

  When entering a non-existent username or no password, the error message '**Invalid username**' 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.

- 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.

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 ADAM/AD-LDS connection, ADAM/AD-LDS user identification and ADAM/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 85)
- Windows 7/Vista (on page 121)
- Windows Server 2008 (on page 144)

> **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 username 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 37), no password is entered for a valid user, you do not receive an error message. The user is not logged in. Even after three failed login tries with no password entered the system is not logged.*

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

4.1 Permanent and temporary login

Users can be logged in permanently or temporarily.

PERMANENT LOGIN

Permanent Login is carried out using the `Login with dialog` Function (on page 46) or the `Login without password` Function (on page 47). The user is thus 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.

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

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

TEMPORARY LOGIN

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

Login in Runtime:

- The dialog to log in is opened when a password-protected function is executed
- The user can log in and execute the operation according to their rights or they receive a message on missing rights
- The user is logged out immediately after the operation

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

4.2 Automatic login and logout in 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 and users from the AD/AD LDS 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.

4.3 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.

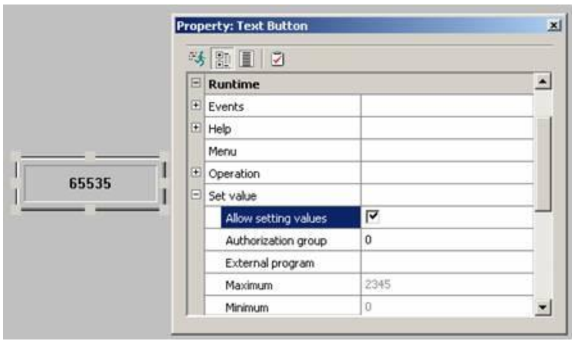
4.4 Password protection for dynamic elements

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.

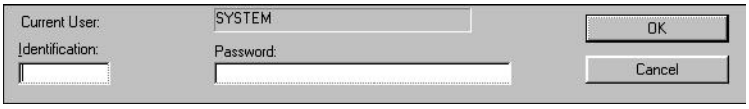


Runtime	
Events	
Help	
Menu	
Operation	
Set value	
Allow setting values	☑
Authorization group	0
External program	
Maximum	2345
Minimum	0

4.5 Password - Functions

4.5.1 Log in with dialog

This function opens the login dialog in the Runtime to log in to zenon again.



Current User: SYSTEM

Identification:

Password:

This attempt is logged in the Chronologic Event list.

A Login (on page 37) screen can also be used for login.

SIZE AND POSITION

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

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

```
[Command initiation]
```

3. Enter a value for

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

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

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

Information

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

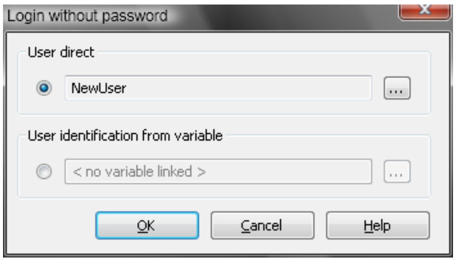
Windows Vista/7/8: `%ProgramData%\COPA-DATA\System\`

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 Chronologic Event List.

In order to create the function login without password:

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


Login without password
User direct
● NewUser ...
User identification from variable
○ < no variable linked > ...
OK
Cancel
Help

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

LOG IN VIA CHIP IDENT SYSTEM

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

- The user must exist in the 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

With this function during online operation (Runtime), the current user is logged out and the user "SYSTEM" with the authorization level 0 is logged in. The log in of an user is logged in the Chronologic Event List. If an Active Directory user is logged in, they are also logged out.

No transfer parameters are needed.

⚠ **Attention**

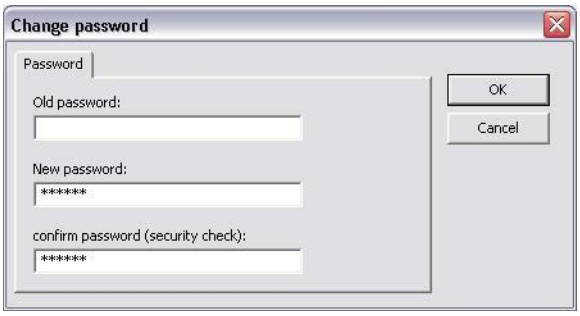
Automatic logout vs. automatic function:

- `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 password

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

An entry mask will open during online operation.



Change password

Password

Old password:

New password: ******

confirm password (security check): ******

Required inputs:

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

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

4.6 Deleting a user

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

> ⚠ **Attention**
>
> *Do not delete any users who are general module owners.*

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.*
>
> **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

To create an Active Directory user administration screen:

1. in the tool bar or in the context menu of node **Screens** select command **New screen**
2. an empty screen of type Standard is opened
3. Change the screen type in the detail view; to do this:
   a) click on **Standard** in the Screen type column
   b) Select Active Directory user administration in the drop-down list
4. Click in the screen.
5. select menu item **Control elements** from the menu bar
6. Click on **Add template** in the drop-down list.

7. The dialog for selecting a template is opened.

8. Select the desired template.

9. Standard elements are placed in pre-defined positions; these can be deleted or positioned elsewhere.

10. You can add further elements using the `Control elements` menu.

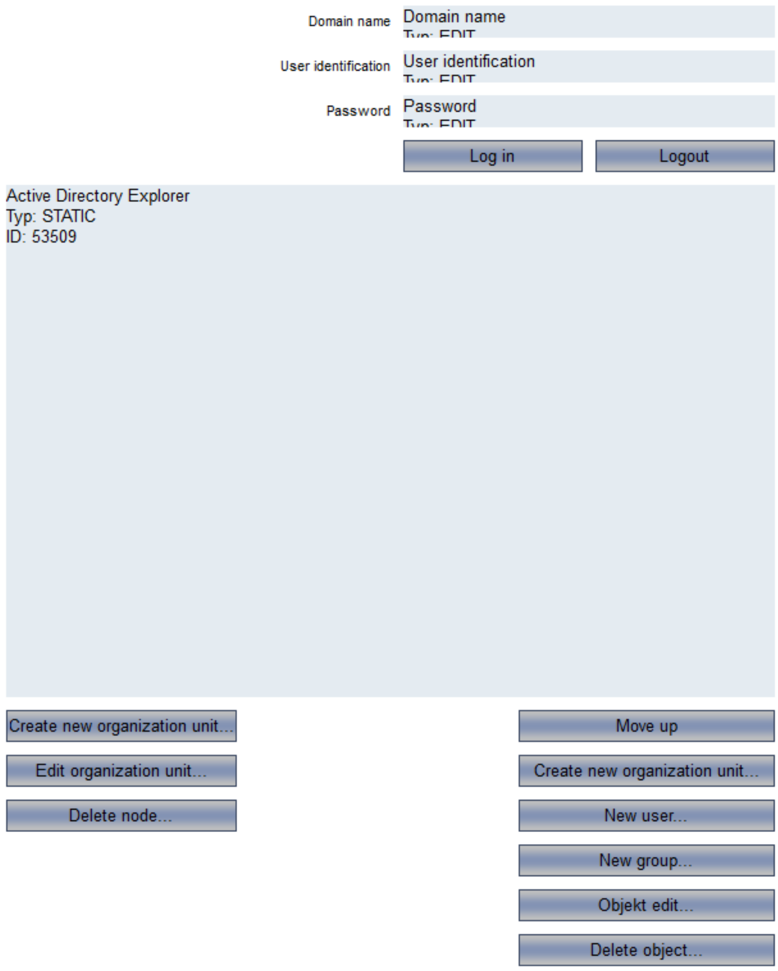
11. Name the screen. To do this:

    a) Click on the screen name in the detail view in the `name` column

    b) Give it its own name

12. Create a screen switch function in order to be able to call up the screen in Runtime

ACTIVE DIRECTORY USER ADMINISTRATION SCREEN



Domain name Typ: EDIT

User identification Typ: EDIT

Password Typ: EDIT

Active Directory Explorer
Typ: STATIC
ID: 53509

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 palced in the screen. Elements can be moved in the screen and placed individually.
`Active Directory window`	Control elements for the display and administration of the Active Directory.
`Active Directory window`	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.
`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.

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.

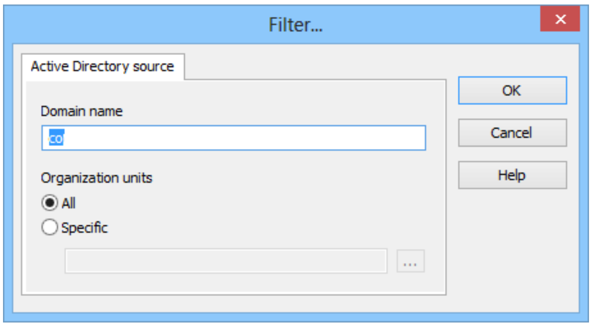
Configuring screen switching:

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



Filter...

Active Directory source

Domain name: co

Organization units

● All

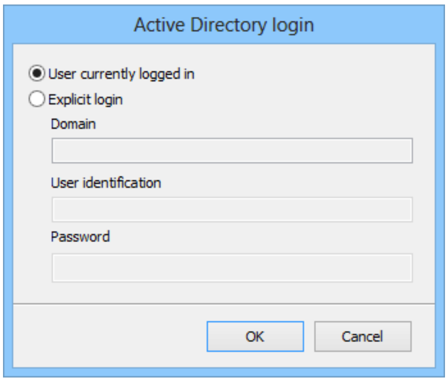
○ Specific

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

SELECT ORGANIZATION UNITS

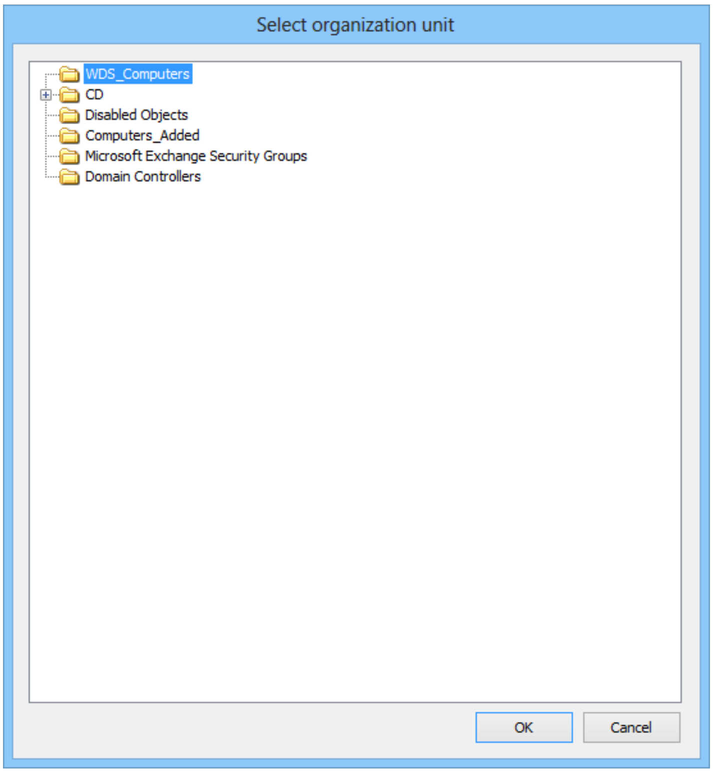
If you select **specific organization units** in the filter dialog, the dialog to enter the login files is opened first, then the dialog to select the organization units.

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:
OK	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.
OK	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

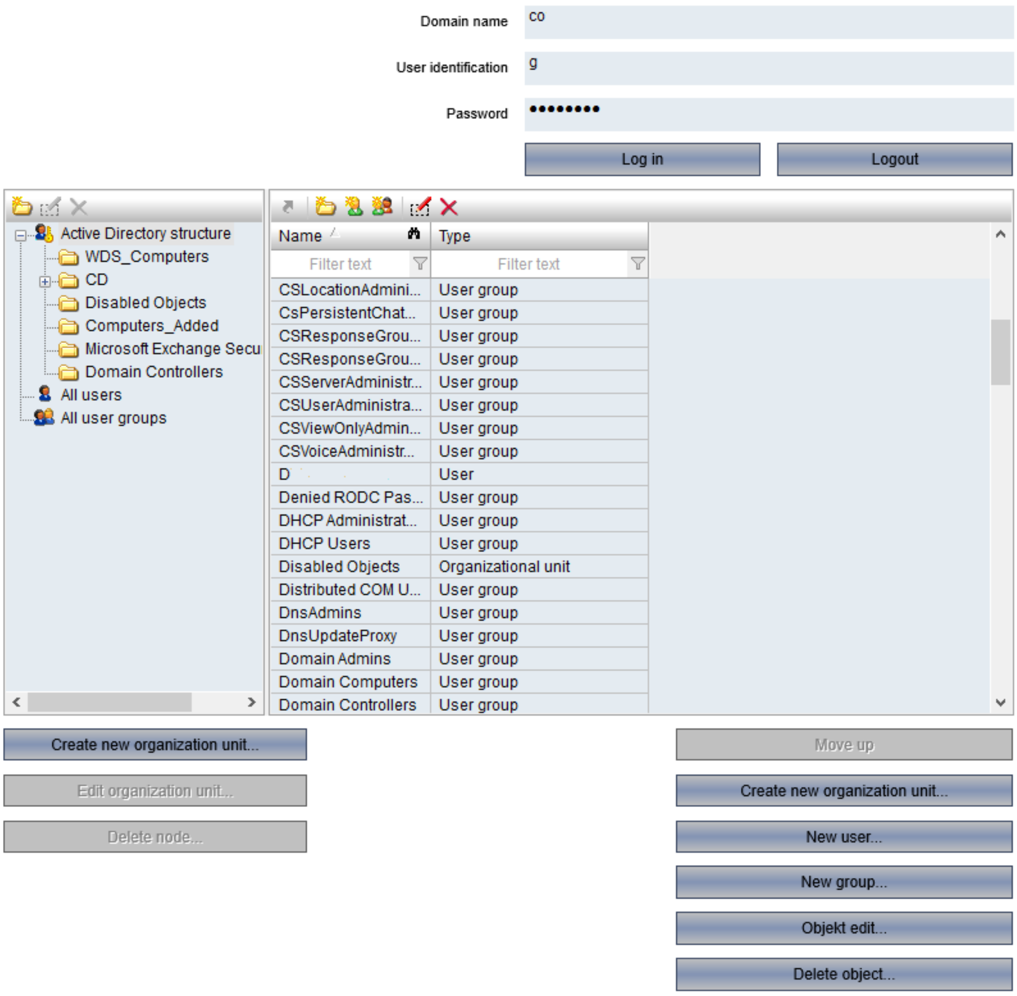
The screen is cleared when screen switching

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 149) occur, check the configuration in the Active Directory (on page 85) 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 59)
- Creating, editing and deleting users (on page 60)
- Creating, editing and deleting user groups (on page 66)

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



Domain name: co

User identification: g

Password: ••••••••

Name	Type
Filter text	Filter text
CSLocationAdmini...	User group
CsPersistentChat...	User group
CSResponseGrou...	User group
CSResponseGrou...	User group
CSServerAdministr...	User group
CSUserAdministra...	User group
CSViewOnlyAdmin...	User group
CSVoiceAdministr...	User group
D	User
Denied RODC Pas...	User group
DHCP Administrat...	User group
DHCP Users	User group
Disabled Objects	Organizational unit
Distributed COM U...	User group
DnsAdmins	User group
DnsUpdateProxy	User group
Domain Admins	User group
Domain Computers	User group
Domain Controllers	User group

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 palced in the screen. Elements can be moved in the screen and placed individually.
`Active Directory window`	Control elements for the display and administration of the Active Directory.
`Active Directory window`	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.
`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.

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.

DETAIL VIEW OF TOOLBAR AND CONTEXT MENU

Depending on the element selected, the context menu and the tool bar 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.

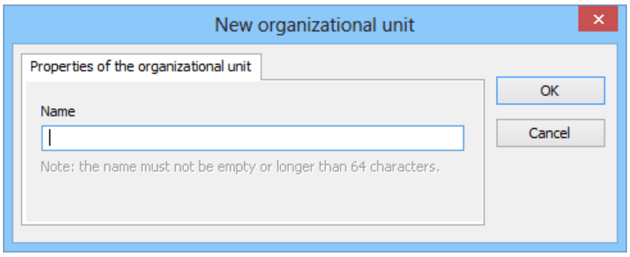
5.3.1 Manage organization unit

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



Note: the name must not be empty or longer than 64 characters.

3. Give it a name.

   Maximum length: 64 `characters`

4. Click on **OK**.

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.

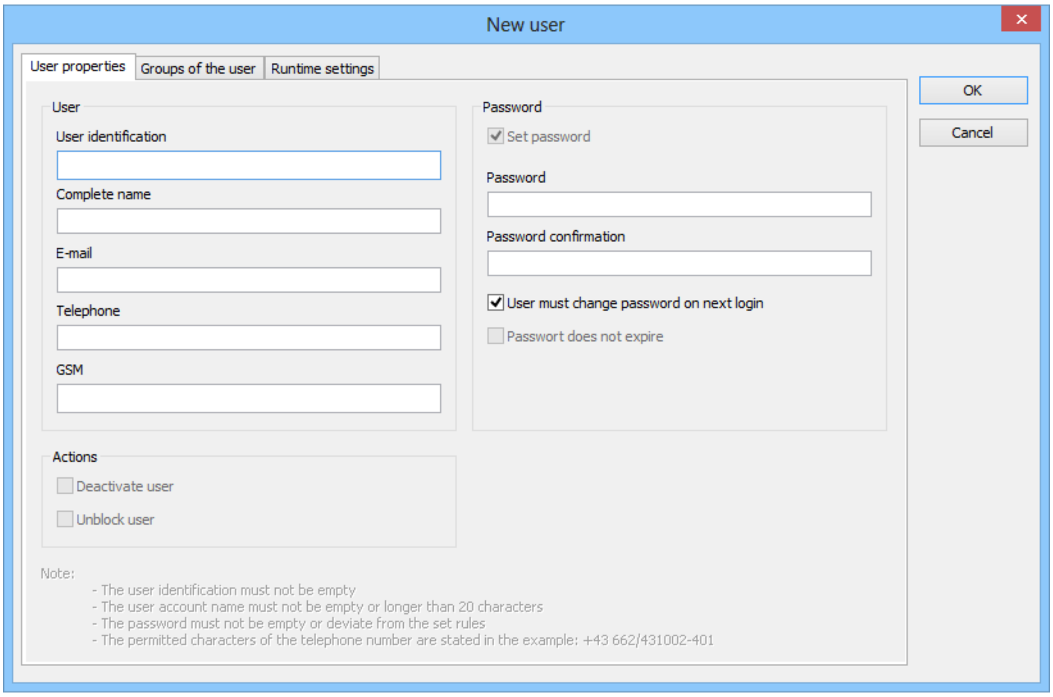
- Create new user: Click on the corresponding button, or the command in the tool bar or the context menu.
- Edit user: Double-click a user entry or click on the corresponding button or on the **`Edit selected object`** command in the context menu.
- Delete user: Highlight the desired user and press the **`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 7)/`Creation of a user` (on page 11) chapter.

USER PROPERTIES



☑ Set password

☑ User must change password on next login

□ Passwort does not expire

□ Deactivate user

□ Unblock user

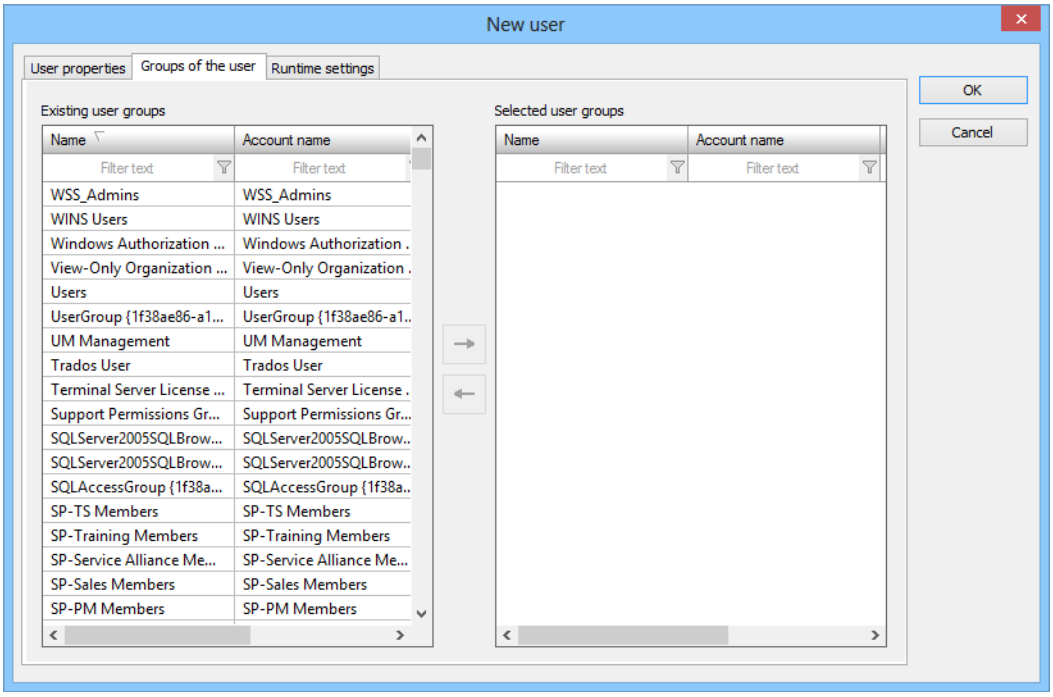
Note:

- The user identification must not be empty
- The user account name must not be empty or longer than 20 characters
- The password must not be empty or deviate from the set rules
- The permitted characters of the telephone number are stated in the example: +43 662/431002-401

Parameters	Description
Users	Settings for user data.
Username	Unique name of the user for the login.
Complete name	Displayed name of the user.
Email	E-mail address of the user
Telephone	Fixed network telephone number of the user. Used for text to speech. Enter numbers. The prefix + abbreviating 00 of the international area code is permitted.
GSM	Mobile phone number of the user. Used for messages via GSM and SMS (text messages). Enter numbers, the prefix + abbreviating 00 of the international area code is permitted.
Password	Settings for the password.
Set password	Active: The password is set again.
Password	Enter new password. For language-spanning projects take care that it must be possible to enter the characters with the respective keyboard in the Runtime.
Password confirmation	Repeat the password.
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	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.
OK	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 **<-**.

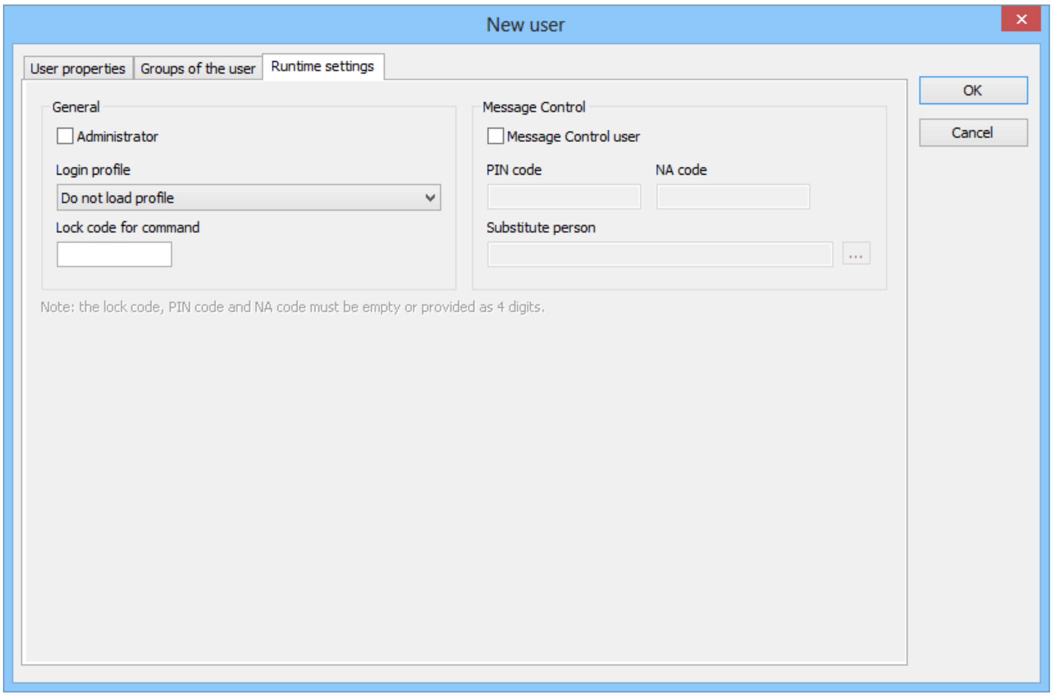


Name	Account name
WSS_Admins	WSS_Admins
WINS Users	WINS Users
Windows Authorization ...	Windows Authorization .
View-Only Organization ...	View-Only Organization .
Users	Users
UserGroup {1f38ae86-a1...	UserGroup {1f38ae86-a1..
UM Management	UM Management
Trados User	Trados User
Terminal Server License ...	Terminal Server License .
Support Permissions Gr...	Support Permissions Gr...
SQLServer2005SQLBrow...	SQLServer2005SQLBrow..
SQLServer2005SQLBrow...	SQLServer2005SQLBrow..
SQLAccessGroup {1f38a...	SQLAccessGroup {1f38a..
SP-TS Members	SP-TS Members
SP-Training Members	SP-Training Members
SP-Service Alliance Me...	SP-Service Alliance Me...
SP-Sales Members	SP-Sales Members
SP-PM Members	SP-PM Members

Name	Account name

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

RUNTIME SETTINGS

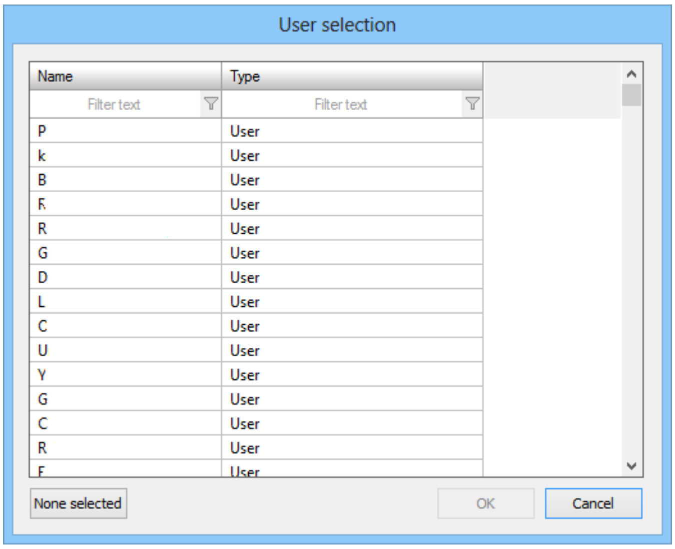


Note: the lock code, PIN code and NA code must be empty or provided as 4 digits.

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 profiles from the drop-down list: - None - Default - Last
Lock code for command	Four-digit PIN code. This code is used by the user for the command in order to lock and unlock different areas.
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). Message is subsequently sent to the next user in the list.
Substitute person	Select a substitute person if the user cannot be reached or the receipt of the message is rejected. A click on button ... Opens the dialog to select a user.
OK	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.



Name	Type
P	User
k	User
B	User
F	User
R	User
G	User
D	User
L	User
C	User
U	User
Y	User
G	User
C	User
R	User
F	User

Parameters	Description
List of persons	List of users available.
No selection	A user who is already defined in the dialog is
OK	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.

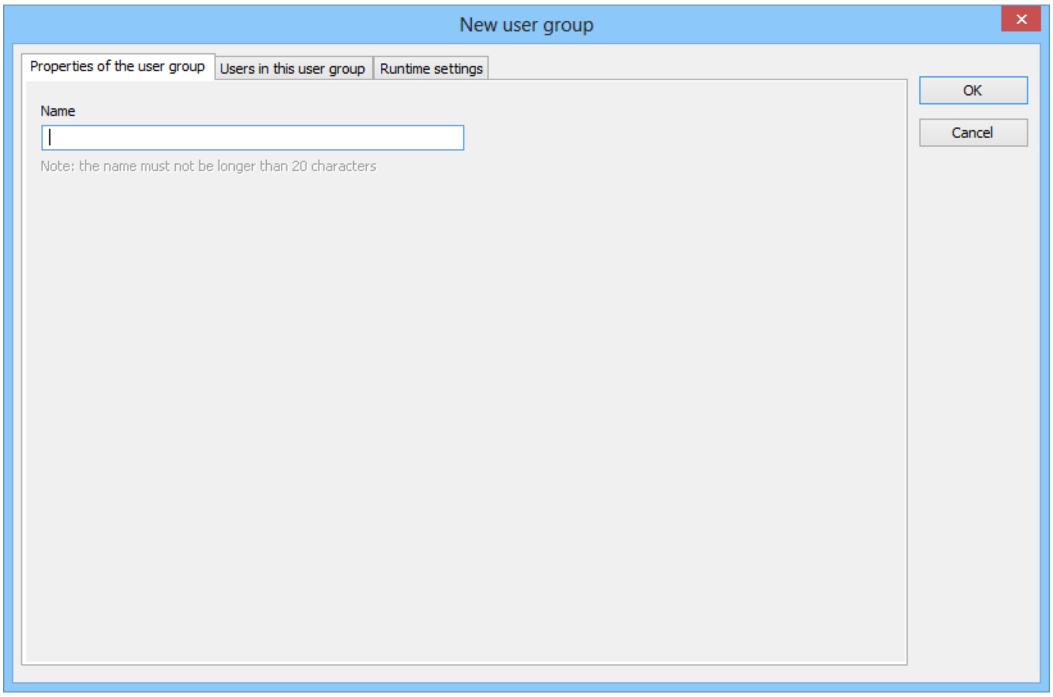
- Creating a new user group: Click on the corresponding button or the command in the tool bar or the context menu.
- Editing user groups: Double-click a user group entry or click on the corresponding button or on the **Edit selected object** command in the context menu.
- Deleting user groups: Highlight 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 7)/**Creation of a user** (on page 19) chapter.

PROPERTIES OF THE USER GROUP


New user group
Properties of the user group
Users in this user group
Runtime settings
Name
Note: the name must not be longer than 20 characters
OK
Cancel

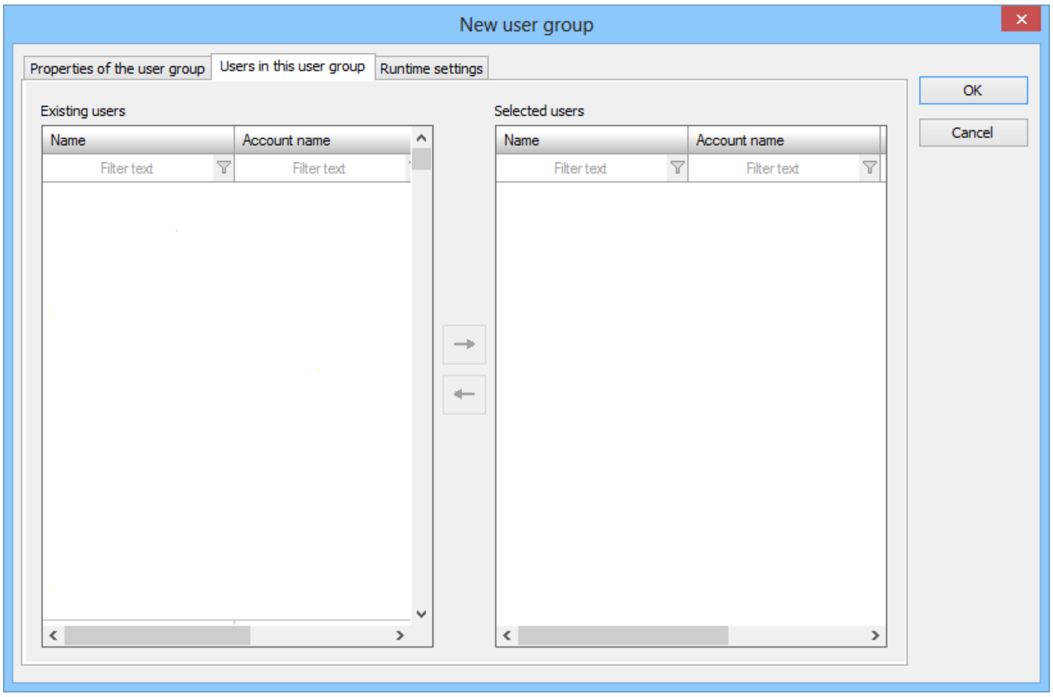
Parameters	Description
Name	Entry of a unique, valid name for the database backup.
OK	Applies all changes in all tabs and closes the dialog.
Cancel	Discards all changes in all tabs and closes the dialog.

USERS IN THIS USER GROUP

1. Select, in the **Existing users** window, the desired users from the existing users.

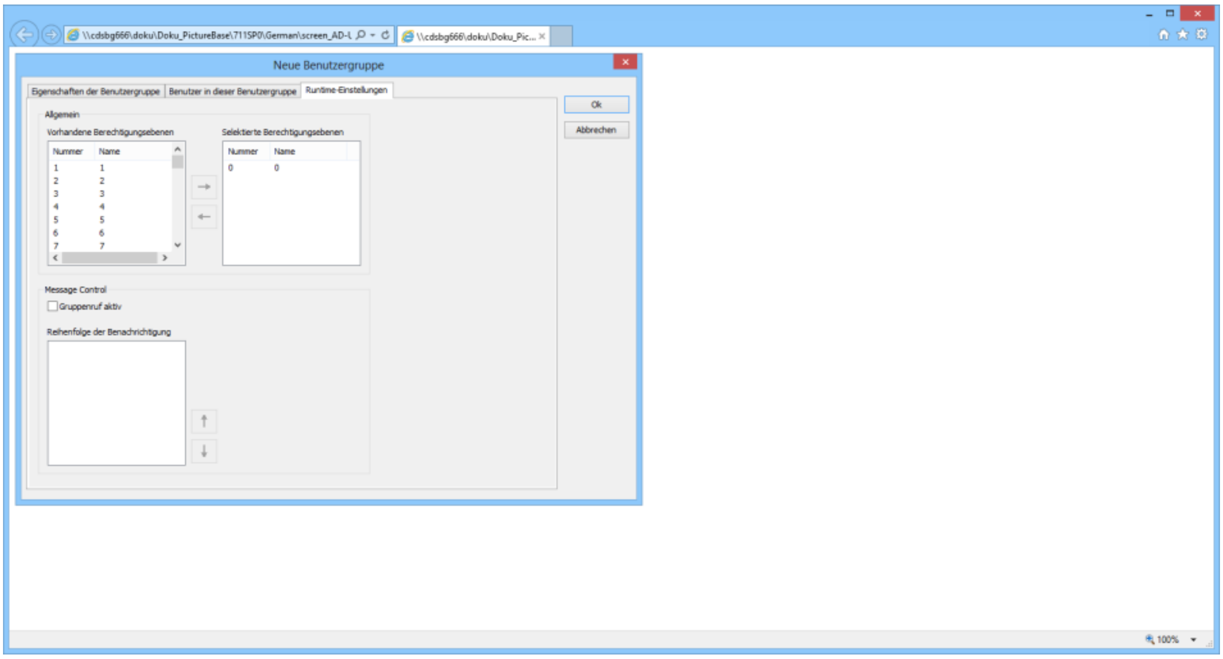
2. Add the selected users with the cursor key -> to the list of **selected users**.

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.
`OK`	Applies all changes in all tabs and closes the dialog.
`Cancel`	Discards all changes in all tabs and closes the dialog.

RUNTIME SETTINGS


\\cdsbg666\doku\Doku_PictureBase\711SP0\German\screen_AD-L
\\cdsbg666\doku\Doku_Pic...
Neue Benutzergruppe
Eigenschaften der Benutzergruppe
Benutzer in dieser Benutzergruppe
Runtime-Einstellungen
Ok
Abbrechen
Allgemein
Vorhandene Berechtigungsebenen
Selektierte Berechtigungsebenen
Message Control
Reihenfolge der Benachrichtigung
100%

Vorhandene Berechtigungsebenen

Nummer	Name
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Selektierte Berechtigungsebenen

Nummer	Name
0	0

☐ Gruppenruf aktiv

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	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.
OK	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 50) in Runtime

> ⚠ **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 `ADAM/AD-LDS connection`, `ADAM/AD-LDS user identification` and `ADAM/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:

1. The name of the authorization group in zenon user administration corresponds to the of the group names of a user group in Active Directory: Automatic assignment of the Active Directory user to zenon authorization group. All AD group users receive user rights that are defined in the zenon authorization group. See User groups in zenon and groups in Active Directory have the same name (on page 74)
2. In the description of the Active Directory group, the zenon authorization levels and the project are stored in a certain syntax. All users of the group receive the user rights stored in the AD group in zenon. See Assignment of an Active Directory user to zenon authorization levels (on page 73)
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 75).

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			
FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF
Authorization levels 1	Authorization levels 2	Authorization levels 3	Authorization levels 4

> **Example**
>
> *Group name: MASCHINE01##service staff*
>
> *Group description: free text##GRP=FFFFFFFF-FFFFFFFF-FFFFFFFF-FFFFFFFF##free text*
>
> *The users which are allocated to MACHINE01##service staff receive authorization level 0 - 127 in zenon.*

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

> **Example**
>
> *Group description: free text##GRP=7##free text*
>
> *The users which are allocated to a group with this description receive authorization level 0, 1 and 2 in zenon.*
>
> *7 hexadecimal equals 111 as binary number. For each 1 in the binary number, the corresponding authorization level is set. The right most bit stands for authorization level 0. The bit to the left of this, stands for authorization level 1 and so on.*

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

If a user is logged in 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 74) method or Allocation of an Active Directory user to zenon authorization levels (on page 73).

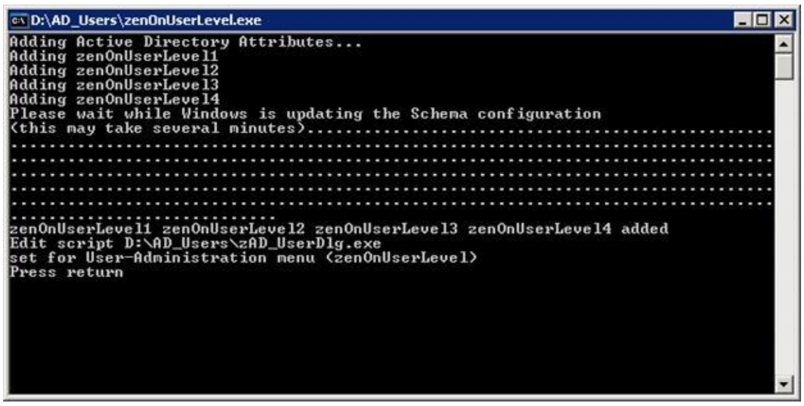
> **Information**
>
> *Active Directory, AD LDS and ADAM (for Windows XP) are not available with Windows CE.*

Installing the schema extension

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

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

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



D:\AD_Users\zenOnUserLevel.exe

```
Adding Active Directory Attributes...
Adding zenOnUserLevel1
Adding zenOnUserLevel2
Adding zenOnUserLevel3
Adding zenOnUserLevel4
Please wait while Windows is updating the Schema configuration
(this may take several minutes).................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
............................
zenOnUserLevel1 zenOnUserLevel2 zenOnUserLevel3 zenOnUserLevel4 added
Edit script D:\AD_Users\zAD_UserDlg.exe
set for User-Administration menu (zenOnUserLevel)
Press return
```

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

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

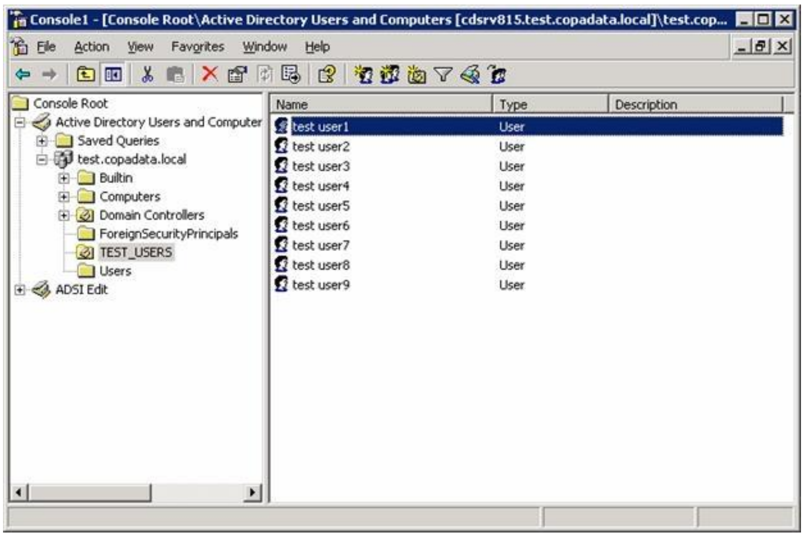
Information

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

Granting user rights

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

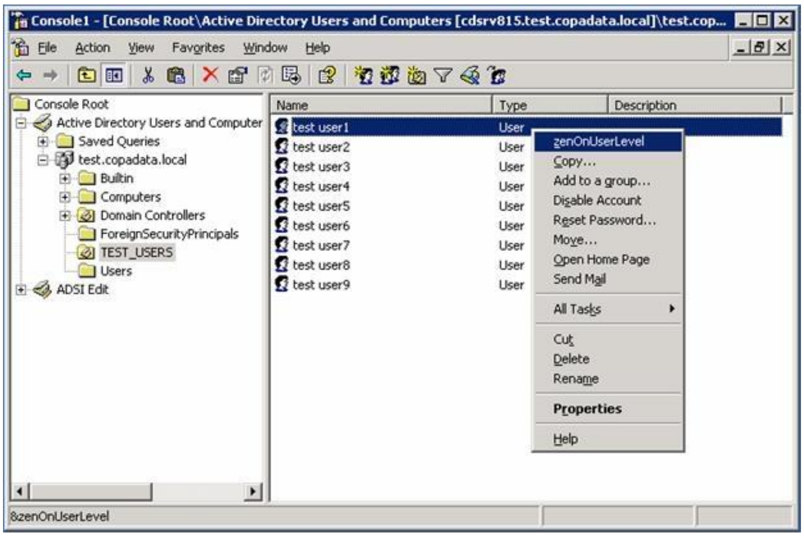
For this purpose, the Microsoft Management Console (MMC) with the **Active Directory Users and Computers** plug-in is opened.



Console1 - [Console Root\Active Directory Users and Computers [cdsrv815.test.copadata.local]\test.cop...

Name	Type	Description
test user1	User	
test user2	User	
test user3	User	
test user4	User	
test user5	User	
test user6	User	
test user7	User	
test user8	User	
test user9	User	

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**.



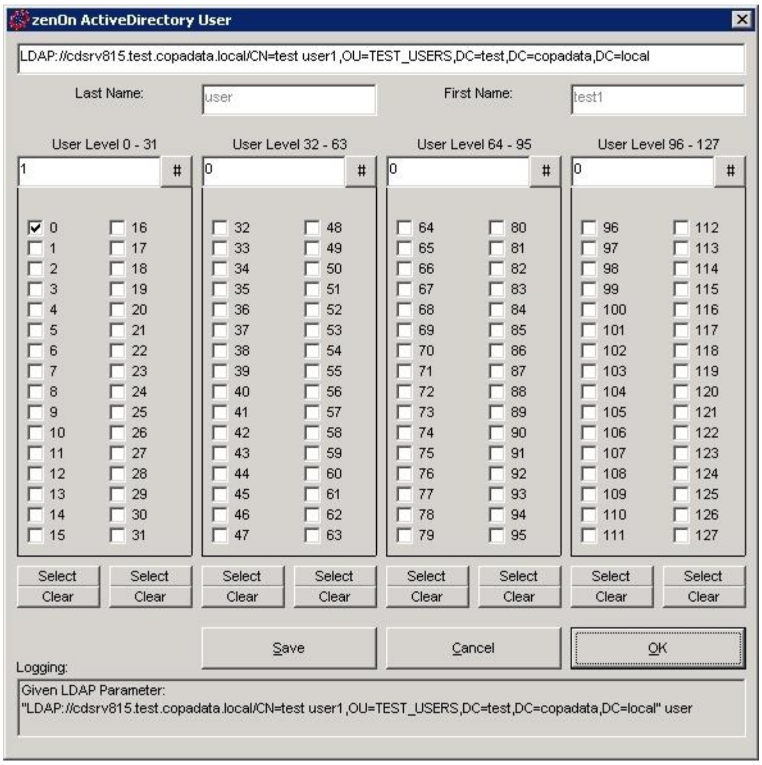
Console1 - [Console Root\Active Directory Users and Computers [cdsrv815.test.copadata.local]\test.cop...

Name	Type	Description
test user1	User	
test user2	User	
test user3	User	
test user4	User	
test user5	User	
test user6	User	
test user7	User	
test user8	User	
test user9	User	

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.



LDAP://cdsrv815.test.copadata.local/CN=test user1,OU=TEST_USERS,DC=test,DC=copadata,DC=local

Last Name: user

First Name: test1

User Level 0 - 31: 1

☑ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 22 ☐ 23 ☐ 24 ☐ 25 ☐ 26 ☐ 27 ☐ 28 ☐ 29 ☐ 30 ☐ 31

User Level 32 - 63: 0

☐ 32 ☐ 33 ☐ 34 ☐ 35 ☐ 36 ☐ 37 ☐ 38 ☐ 39 ☐ 40 ☐ 41 ☐ 42 ☐ 43 ☐ 44 ☐ 45 ☐ 46 ☐ 47 ☐ 48 ☐ 49 ☐ 50 ☐ 51 ☐ 52 ☐ 53 ☐ 54 ☐ 55 ☐ 56 ☐ 57 ☐ 58 ☐ 59 ☐ 60 ☐ 61 ☐ 62 ☐ 63

User Level 64 - 95: 0

☐ 64 ☐ 65 ☐ 66 ☐ 67 ☐ 68 ☐ 69 ☐ 70 ☐ 71 ☐ 72 ☐ 73 ☐ 74 ☐ 75 ☐ 76 ☐ 77 ☐ 78 ☐ 79 ☐ 80 ☐ 81 ☐ 82 ☐ 83 ☐ 84 ☐ 85 ☐ 86 ☐ 87 ☐ 88 ☐ 89 ☐ 90 ☐ 91 ☐ 92 ☐ 93 ☐ 94 ☐ 95

User Level 96 - 127: 0

☐ 96 ☐ 97 ☐ 98 ☐ 99 ☐ 100 ☐ 101 ☐ 102 ☐ 103 ☐ 104 ☐ 105 ☐ 106 ☐ 107 ☐ 108 ☐ 109 ☐ 110 ☐ 111 ☐ 112 ☐ 113 ☐ 114 ☐ 115 ☐ 116 ☐ 117 ☐ 118 ☐ 119 ☐ 120 ☐ 121 ☐ 122 ☐ 123 ☐ 124 ☐ 125 ☐ 126 ☐ 127

Logging:

```
Given LDAP Parameter:
"LDAP://cdsrv815.test.copadata.local/CN=test user1,OU=TEST_USERS,DC=test,DC=copadata,DC=local" user
```

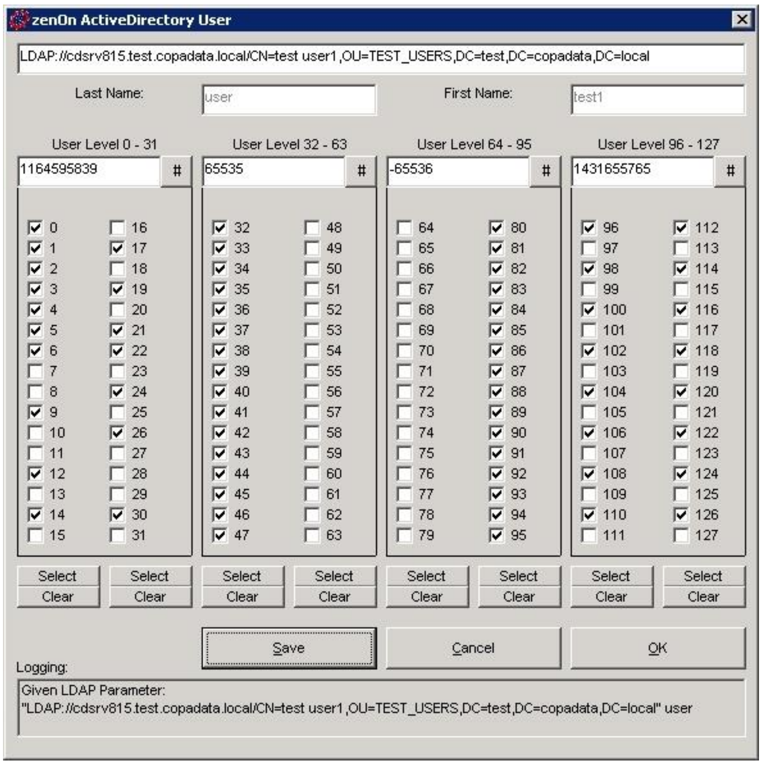
Up to 128 authorization levels per user can be defined with the help of the administration tool.

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



zenOn ActiveDirectory User

LDAP://cdsrv815.test.copadata.local/CN=test user1,OU=TEST_USERS,DC=test,DC=copadata,DC=local

Last Name: user

First Name: test1

User Level 0 - 31		User Level 32 - 63		User Level 64 - 95		User Level 96 - 127	
1164595839	#	65535	#	-65536	#	1431655765	#
☑ 0	□ 16	☑ 32	□ 48	□ 64	☑ 80	☑ 96	☑ 112
☑ 1	☑ 17	☑ 33	□ 49	□ 65	☑ 81	□ 97	□ 113
☑ 2	□ 18	☑ 34	□ 50	□ 66	☑ 82	☑ 98	☑ 114
☑ 3	☑ 19	☑ 35	□ 51	□ 67	☑ 83	□ 99	□ 115
☑ 4	□ 20	☑ 36	□ 52	□ 68	☑ 84	☑ 100	☑ 116
☑ 5	☑ 21	☑ 37	□ 53	□ 69	☑ 85	□ 101	□ 117
☑ 6	☑ 22	☑ 38	□ 54	□ 70	☑ 86	☑ 102	☑ 118
□ 7	□ 23	☑ 39	□ 55	□ 71	☑ 87	□ 103	□ 119
□ 8	☑ 24	☑ 40	□ 56	□ 72	☑ 88	☑ 104	☑ 120
☑ 9	□ 25	☑ 41	□ 57	□ 73	☑ 89	□ 105	□ 121
□ 10	☑ 26	☑ 42	□ 58	□ 74	☑ 90	☑ 106	☑ 122
□ 11	□ 27	☑ 43	□ 59	□ 75	☑ 91	□ 107	□ 123
☑ 12	□ 28	☑ 44	□ 60	□ 76	☑ 92	☑ 108	☑ 124
□ 13	□ 29	☑ 45	□ 61	□ 77	☑ 93	□ 109	□ 125
☑ 14	☑ 30	☑ 46	□ 62	□ 78	☑ 94	☑ 110	☑ 126
□ 15	□ 31	☑ 47	□ 63	□ 79	☑ 95	□ 111	□ 127
Select Clear	Select Clear	Select Clear	Select Clear	Select Clear	Select Clear	Select Clear	Select Clear

Logging:

```
Given LDAP Parameter:
"LDAP://cdsrv815.test.copadata.local/CN=test user1,OU=TEST_USERS,DC=test,DC=copadata,DC=local" user
```

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

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 from the Microsoft Server CD have been installed.

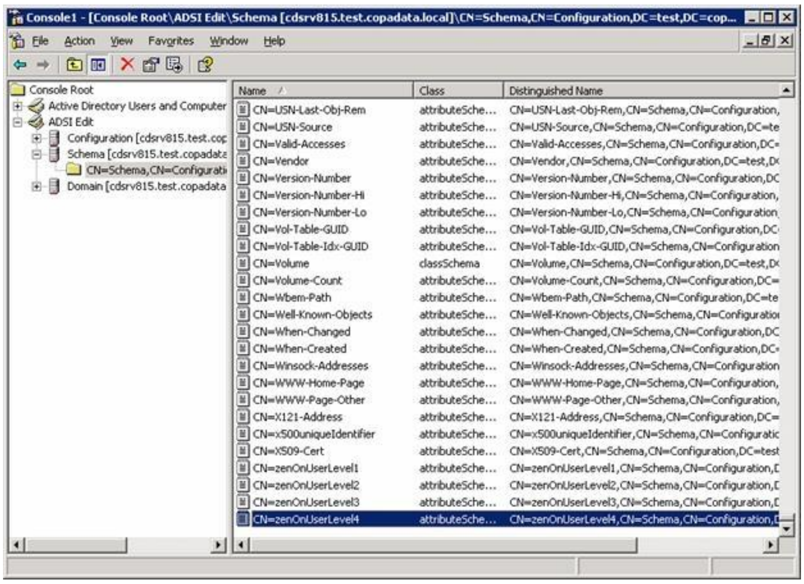
To be found on the CD under: `CD_ROOT/SUPPORT/TOOLS/SUPTOOLS.msi`

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

6.1.6 Schema

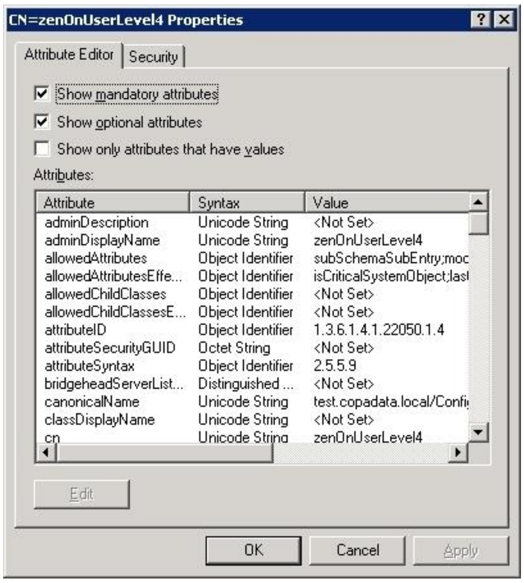
The additional attributes can be checked in the schema. These are normally listed at the bottom.

```
zenonUserLevel1 - zenonUserLevel4
```



Console1 - [Console Root\ADSI Edit\Schema [cdsrv815.test.copadata.local]\CN=Schema,CN=Configuration,DC=test,DC=cop...
File Action View Favorites Window Help
Console Root
Active Directory Users and Computer
ADSI Edit
Configuration [cdsrv815.test.cop
Schema [cdsrv815.test.copadata
CN=Schema,CN=Configurati
Domain [cdsrv815.test.copadata

Name	Class	Distinguished Name
CN=USN-Last-Obj-Rem	attributeSche...	CN=USN-Last-Obj-Rem,CN=Schema,CN=Configuration,
CN=USN-Source	attributeSche...	CN=USN-Source,CN=Schema,CN=Configuration,DC=te
CN=Valid-Accesses	attributeSche...	CN=Valid-Accesses,CN=Schema,CN=Configuration,DC=
CN=Vendor	attributeSche...	CN=Vendor,CN=Schema,CN=Configuration,DC=test,D
CN=Version-Number	attributeSche...	CN=Version-Number,CN=Schema,CN=Configuration,DC
CN=Version-Number-Hi	attributeSche...	CN=Version-Number-Hi,CN=Schema,CN=Configuration,
CN=Version-Number-Lo	attributeSche...	CN=Version-Number-Lo,CN=Schema,CN=Configuration
CN=Vol-Table-GUID	attributeSche...	CN=Vol-Table-GUID,CN=Schema,CN=Configuration,DC
CN=Vol-Table-Idx-GUID	attributeSche...	CN=Vol-Table-Idx-GUID,CN=Schema,CN=Configuration
CN=Volume	classSchema	CN=Volume,CN=Schema,CN=Configuration,DC=test,D
CN=Volume-Count	attributeSche...	CN=Volume-Count,CN=Schema,CN=Configuration,DC=
CN=Wbem-Path	attributeSche...	CN=Wbem-Path,CN=Schema,CN=Configuration,DC=te
CN=Well-Known-Objects	attributeSche...	CN=Well-Known-Objects,CN=Schema,CN=Configuratio
CN=When-Changed	attributeSche...	CN=When-Changed,CN=Schema,CN=Configuration,DC
CN=When-Created	attributeSche...	CN=When-Created,CN=Schema,CN=Configuration,DC=
CN=Winsock-Addresses	attributeSche...	CN=Winsock-Addresses,CN=Schema,CN=Configuration
CN=WWW-Home-Page	attributeSche...	CN=WWW-Home-Page,CN=Schema,CN=Configuration,
CN=WWW-Page-Other	attributeSche...	CN=WWW-Page-Other,CN=Schema,CN=Configuration,
CN=X121-Address	attributeSche...	CN=X121-Address,CN=Schema,CN=Configuration,DC=
CN=x500uniqueIdentifier	attributeSche...	CN=x500uniqueIdentifier,CN=Schema,CN=Configuratic
CN=X509-Cert	attributeSche...	CN=X509-Cert,CN=Schema,CN=Configuration,DC=test
CN=zenOnUserLevel1	attributeSche...	CN=zenOnUserLevel1,CN=Schema,CN=Configuration,D
CN=zenOnUserLevel2	attributeSche...	CN=zenOnUserLevel2,CN=Schema,CN=Configuration,D
CN=zenOnUserLevel3	attributeSche...	CN=zenOnUserLevel3,CN=Schema,CN=Configuration,D
CN=zenOnUserLevel4	attributeSche...	CN=zenOnUserLevel4,CN=Schema,CN=Configuration,D



☑ Show mandatory attributes

☑ Show optional attributes

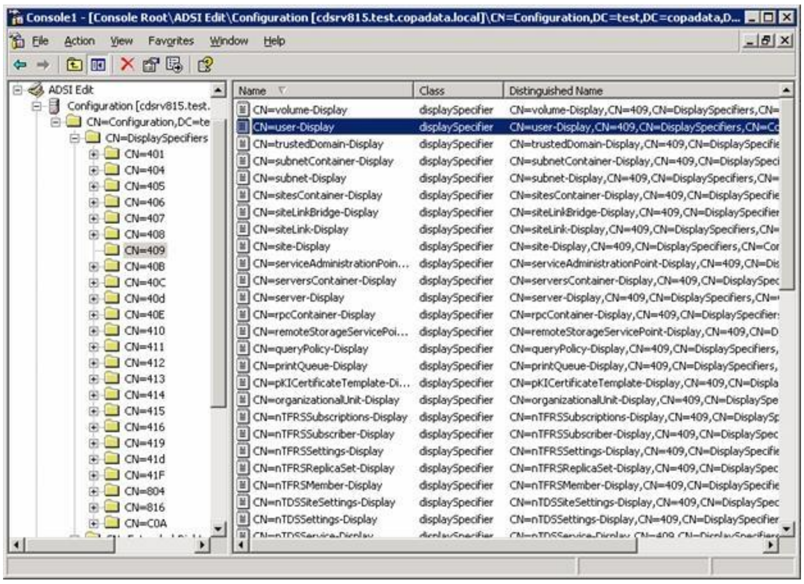
☐ Show only attributes that have values

Attributes:

Attribute	Syntax	Value
adminDescription	Unicode String	<Not Set>
adminDisplayName	Unicode String	zenOnUserLevel4
allowedAttributes	Object Identifier	subSchemaSubEntry;moc
allowedAttributesEffe...	Object Identifier	isCriticalSystemObject;las
allowedChildClasses	Object Identifier	<Not Set>
allowedChildClassesE...	Object Identifier	<Not Set>
attributeID	Object Identifier	1.3.6.1.4.1.22050.1.4
attributeSecurityGUID	Octet String	<Not Set>
attributeSyntax	Object Identifier	2.5.5.9
bridgeheadServerList...	Distinguished ...	<Not Set>
canonicalName	Unicode String	test.copadata.local/Confi
classDisplayName	Unicode String	<Not Set>
cn	Unicode String	zenOnUserLevel4

6.1.7 Configuration

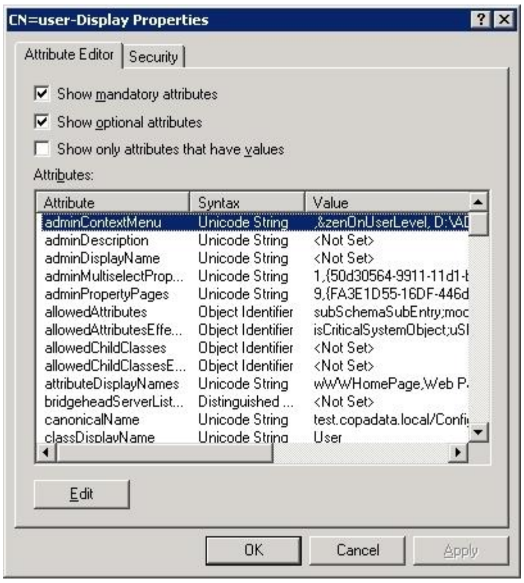
After the connection to configuration has been defined, the details of the single AD objects can be checked and edited. In this case, only the object user-display in the single 'DisplaySpecifiers' is of interest, because here the link between user object and AdministrationTool is established.



Console1 - [Console Root\ADSI Edit\Configuration [cdsrv815.test.copadata.local]\CN=Configuration,DC=test,DC=copadata,D...

ADSI Edit
Configuration [cdsrv815.test.
CN=Configuration,DC=te
CN=DisplaySpecifiers
CN=401
CN=404
CN=405
CN=406
CN=407
CN=408
CN=409
CN=40B
CN=40C
CN=40d
CN=40E
CN=410
CN=411
CN=412
CN=413
CN=414
CN=415
CN=416
CN=419
CN=41d
CN=41F
CN=804
CN=816
CN=C0A

Name	Class	Distinguished Name
CN=volume-Display	displaySpecifier	CN=volume-Display,CN=409,CN=DisplaySpecifiers,CN=
CN=user-Display	displaySpecifier	CN=user-Display,CN=409,CN=DisplaySpecifiers,CN=Co
CN=trustedDomain-Display	displaySpecifier	CN=trustedDomain-Display,CN=409,CN=DisplaySpecifie
CN=subnetContainer-Display	displaySpecifier	CN=subnetContainer-Display,CN=409,CN=DisplaySpeci
CN=subnet-Display	displaySpecifier	CN=subnet-Display,CN=409,CN=DisplaySpecifiers,CN=
CN=sitesContainer-Display	displaySpecifier	CN=sitesContainer-Display,CN=409,CN=DisplaySpecifie
CN=siteLinkBridge-Display	displaySpecifier	CN=siteLinkBridge-Display,CN=409,CN=DisplaySpecifier
CN=siteLink-Display	displaySpecifier	CN=siteLink-Display,CN=409,CN=DisplaySpecifiers,CN=
CN=site-Display	displaySpecifier	CN=site-Display,CN=409,CN=DisplaySpecifiers,CN=Cor
CN=serviceAdministrationPoin...	displaySpecifier	CN=serviceAdministrationPoint-Display,CN=409,CN=Dis
CN=serversContainer-Display	displaySpecifier	CN=serversContainer-Display,CN=409,CN=DisplaySpec
CN=server-Display	displaySpecifier	CN=server-Display,CN=409,CN=DisplaySpecifiers,CN=
CN=rpcContainer-Display	displaySpecifier	CN=rpcContainer-Display,CN=409,CN=DisplaySpecifier:
CN=remoteStorageServicePoi...	displaySpecifier	CN=remoteStorageServicePoint-Display,CN=409,CN=D
CN=queryPolicy-Display	displaySpecifier	CN=queryPolicy-Display,CN=409,CN=DisplaySpecifiers,
CN=printQueue-Display	displaySpecifier	CN=printQueue-Display,CN=409,CN=DisplaySpecifiers,
CN=pKICertificateTemplate-Di...	displaySpecifier	CN=pKICertificateTemplate-Display,CN=409,CN=Displa
CN=organizationalUnit-Display	displaySpecifier	CN=organizationalUnit-Display,CN=409,CN=DisplaySpe
CN=nTFRSSubscriptions-Display	displaySpecifier	CN=nTFRSSubscriptions-Display,CN=409,CN=DisplaySp
CN=nTFRSSubscriber-Display	displaySpecifier	CN=nTFRSSubscriber-Display,CN=409,CN=DisplaySpec
CN=nTFRSSettings-Display	displaySpecifier	CN=nTFRSSettings-Display,CN=409,CN=DisplaySpecifie
CN=nTFRSReplicaSet-Display	displaySpecifier	CN=nTFRSReplicaSet-Display,CN=409,CN=DisplaySpec
CN=nTFRSMember-Display	displaySpecifier	CN=nTFRSMember-Display,CN=409,CN=DisplaySpecifie
CN=nTDSSiteSettings-Display	displaySpecifier	CN=nTDSSiteSettings-Display,CN=409,CN=DisplaySpec
CN=nTDSSettings-Display	displaySpecifier	CN=nTDSSettings-Display,CN=409,CN=DisplaySpecifier
CN=nTDSService-Display	displaySpecifier	CN=nTDSService-Display,CN=409,CN=DisplaySpecifiers



CN=user-Display Properties

☑ Show mandatory attributes

☑ Show optional attributes

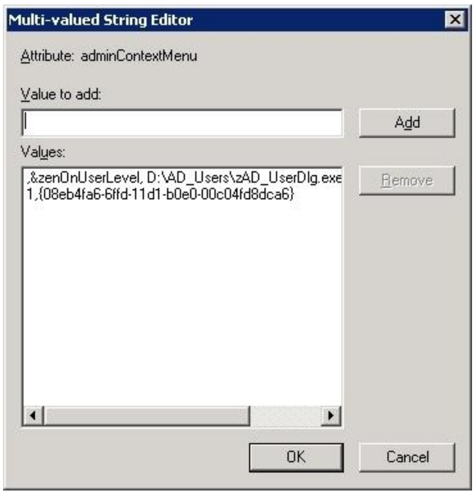
☐ Show only attributes that have values

Attributes:

Attribute	Syntax	Value
adminContextMenu	Unicode String	,&zenOnUserLevel, D:\AD
adminDescription	Unicode String	<Not Set>
adminDisplayName	Unicode String	<Not Set>
adminMultiselectProp...	Unicode String	1,{50d30564-9911-11d1-t
adminPropertyPages	Unicode String	9,{FA3E1D55-16DF-446d
allowedAttributes	Object Identifier	subSchemaSubEntry;moc
allowedAttributesEffe...	Object Identifier	isCriticalSystemObject;uSI
allowedChildClasses	Object Identifier	<Not Set>
allowedChildClassesE...	Object Identifier	<Not Set>
attributeDisplayNames	Unicode String	wWWHomePage,Web P.
bridgeheadServerList...	Distinguished ...	<Not Set>
canonicalName	Unicode String	test.copadata.local/Confi
classDisplayName	Unicode String	User

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

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



Multi-valued String Editor

Attribute: adminContextMenu

Value to add:

Values:

,&zenOnUserLevel, D:\AD_Users\zAD_UserDlg.exe
1,{08eb4fa6-6ffd-11d1-b0e0-00c04fd8dca6}

This entry can also be amended manually if necessary.

To do this:

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

The parameter has the following structure:

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

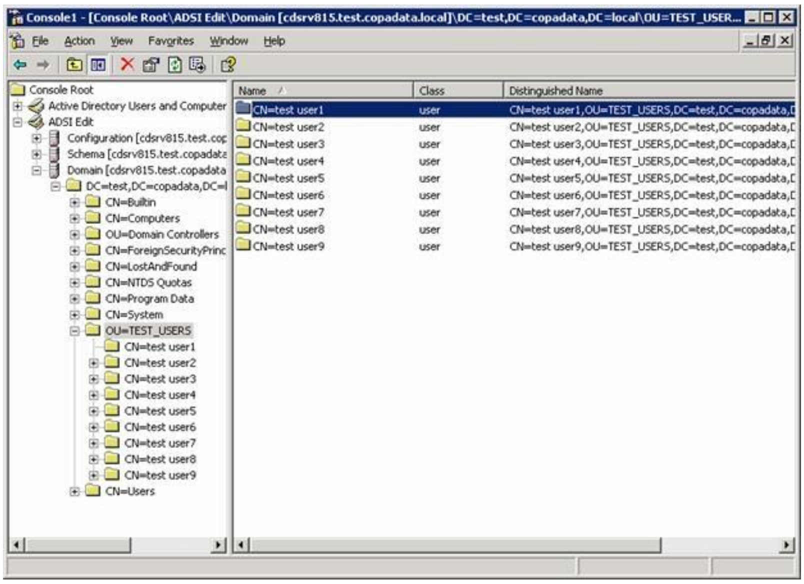
Example

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

`,&zenonUserLevel,D:/AD_Users/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.

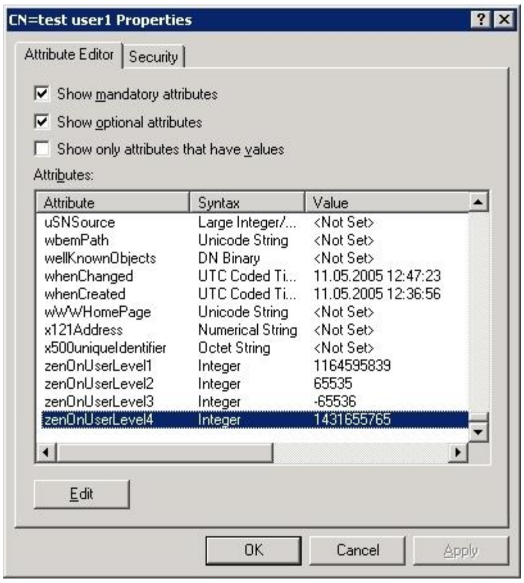


Console1 - [Console Root\ADSI Edit\Domain [cdsrv815.test.copadata.local]\DC=test,DC=copadata,DC=local\OU=TEST_USER...

```
Console Root
  Active Directory Users and Computer
  ADSI Edit
    Configuration [cdsrv815.test.cop
    Schema [cdsrv815.test.copadata
    Domain [cdsrv815.test.copadata
      DC=test,DC=copadata,DC=l
        CN=Builtin
        CN=Computers
        OU=Domain Controllers
        CN=ForeignSecurityPrinc
        CN=LostAndFound
        CN=NTDS Quotas
        CN=Program Data
        CN=System
        OU=TEST_USERS
          CN=test user1
          CN=test user2
          CN=test user3
          CN=test user4
          CN=test user5
          CN=test user6
          CN=test user7
          CN=test user8
          CN=test user9
        CN=Users
```

Name	Class	Distinguished Name
CN=test user1	user	CN=test user1,OU=TEST_USERS,DC=test,DC=copadata,D
CN=test user2	user	CN=test user2,OU=TEST_USERS,DC=test,DC=copadata,D
CN=test user3	user	CN=test user3,OU=TEST_USERS,DC=test,DC=copadata,D
CN=test user4	user	CN=test user4,OU=TEST_USERS,DC=test,DC=copadata,D
CN=test user5	user	CN=test user5,OU=TEST_USERS,DC=test,DC=copadata,D
CN=test user6	user	CN=test user6,OU=TEST_USERS,DC=test,DC=copadata,D
CN=test user7	user	CN=test user7,OU=TEST_USERS,DC=test,DC=copadata,D
CN=test user8	user	CN=test user8,OU=TEST_USERS,DC=test,DC=copadata,D
CN=test user9	user	CN=test user9,OU=TEST_USERS,DC=test,DC=copadata,D

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.



CN=test user1 Properties

☑ Show mandatory attributes

☑ Show optional attributes

□ Show only attributes that have values

Attributes:

Attribute	Syntax	Value
uSNSource	Large Integer/...	<Not Set>
wbemPath	Unicode String	<Not Set>
wellKnownObjects	DN Binary	<Not Set>
whenChanged	UTC Coded Ti...	11.05.2005 12:47:23
whenCreated	UTC Coded Ti...	11.05.2005 12:36:56
wWWHomePage	Unicode String	<Not Set>
x121Address	Numerical String	<Not Set>
x500uniqueIdentifier	Octet String	<Not Set>
zenOnUserLevel1	Integer	1164595839
zenOnUserLevel2	Integer	65535
zenOnUserLevel3	Integer	-65536
zenOnUserLevel4	Integer	1431655765

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 71) and is suitable for use on normal desktop operating systems; it is not necessary to use a server operating system. LikeAD (on page 71), AD LDS also supports:

1. The name of the authorization group in zenon user administration corresponds to the of the group names of a user group in Active Directory: Automatic assignment of the Active Directory user to zenon authorization group. All AD group users receive user rights that are defined in the zenon authorization group. See User groups in zenon and groups in Active Directory have the same name (on page 74)
2. In the description of the Active Directory group, the zenon authorization levels and the project are stored in a certain syntax. All users of the group receive the user rights stored in the AD group in zenon. See Assignment of an Active Directory user to zenon authorization levels (on page 73)

You can use AD LDS with:

- Windows Vista (on page 121)
- Windows 7 (on page 121)
- Windows 8 (on page 85)
- Windows Server 2008 (on page 144)
- Windows Server 2012 (on page 85)

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 86)
2. Create a new AD LDS instance (on page 89)
3. Import an AD LDS schema (on page 96)
4. Install Remote Administration for Windows Server (on page 97)
5. Configure the Active Directory snap-in (on page 98) in order to manage the AD LDS instances

6. Define the roles, organization units, users and user groups (on page 103)

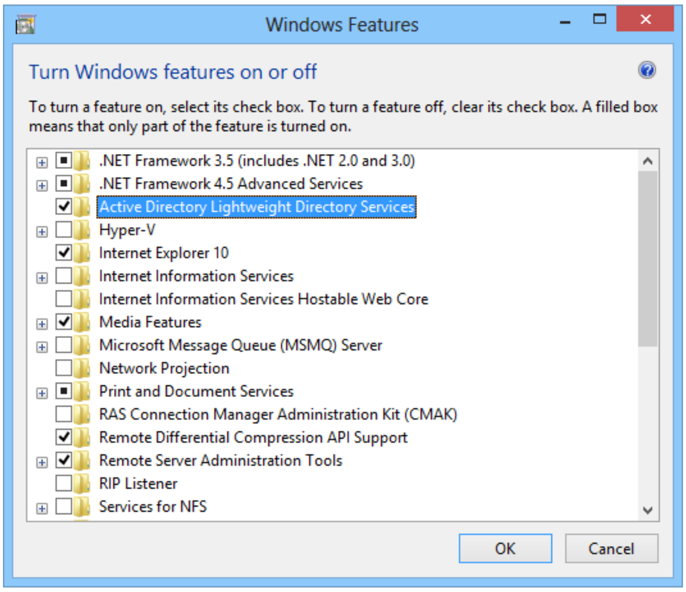
Note: The instructions on installation and use of AD LDS sometimes use screenshots with an English user interface.

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`**.



Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ■ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- ■ .NET Framework 4.5 Advanced Services
- ☑ Active Directory Lightweight Directory Services
- □ Hyper-V
- ☑ Internet Explorer 10
- □ Internet Information Services
- □ Internet Information Services Hostable Web Core
- ☑ Media Features
- □ Microsoft Message Queue (MSMQ) Server
- □ Network Projection
- ■ Print and Document Services
- □ RAS Connection Manager Administration Kit (CMAK)
- ☑ Remote Differential Compression API Support
- ☑ Remote Server Administration Tools
- □ RIP Listener
- □ Services for NFS

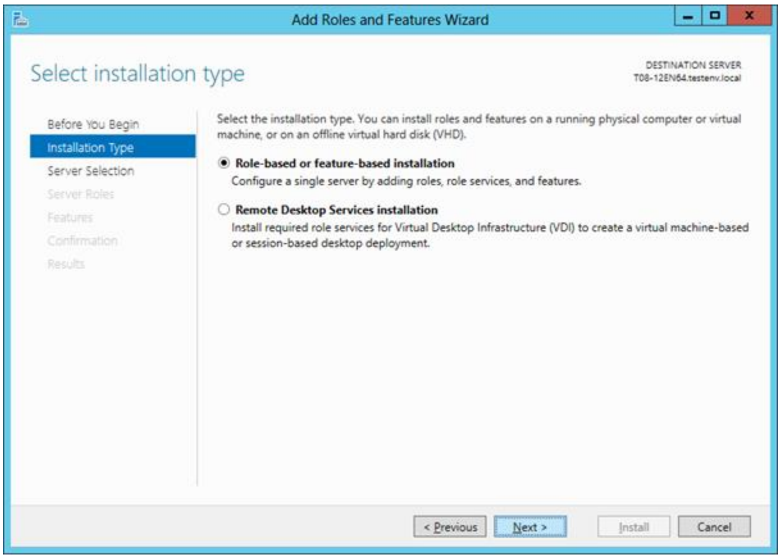
4. Activate the check box in front of `Active Directory Lightweight Directory Services`.
5. Click on **OK**.

WINDOWS SERVER 2012

To install AD LDS under Windows Server 2012:

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

2. The wizard is started.



Add Roles and Features Wizard

Select installation type

DESTINATION SERVER
T08-12EN64.testenv.local

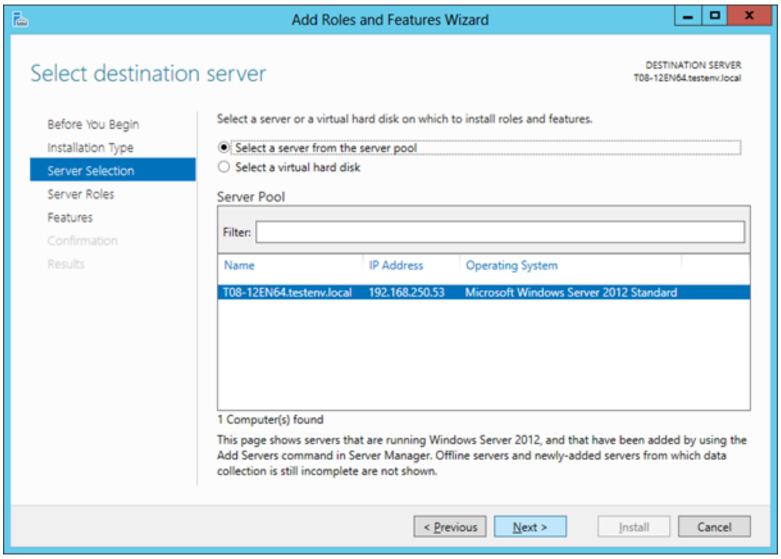
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

3. Select `Role-based or feature-based installation`.

4. Click on **`Next`**.



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
T08-12EN64.testenv.local

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

Filter:

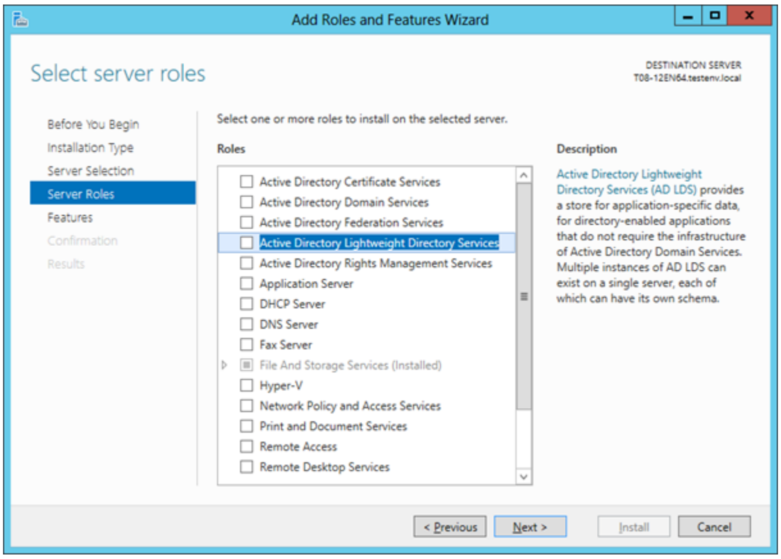
Name	IP Address	Operating System
T08-12EN64.testenv.local	192.168.250.53	Microsoft Windows Server 2012 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

5. Select a server from the server pool.

6. Click on **Next**.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
T08-12EN64.testenv.local

Select one or more roles to install on the selected server.

Roles

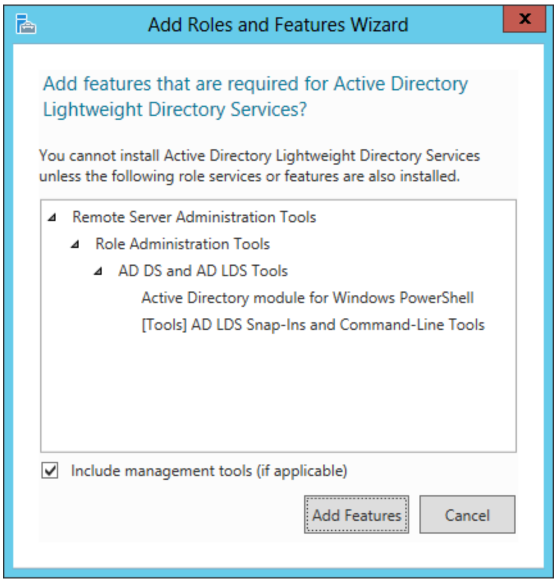
- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ▣ File And Storage Services (Installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services

Description

Active Directory Lightweight Directory Services (AD LDS) provides a store for application-specific data, for directory-enabled applications that do not require the infrastructure of Active Directory Domain Services. Multiple instances of AD LDS can exist on a single server, each of which can have its own schema.

7. Activate the check box in front of `Active Directory Lightweight Directory Services` for server roles.

8. Click on **Next**.



Add Roles and Features Wizard

Add features that are required for Active Directory Lightweight Directory Services?

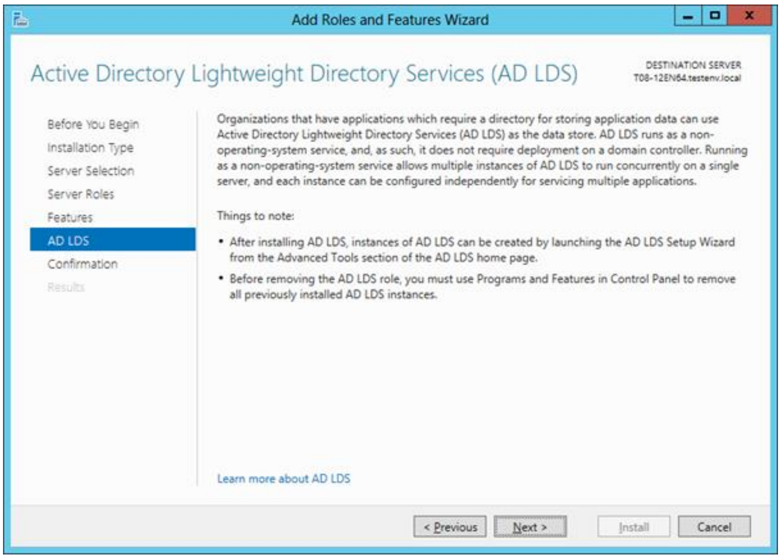
You cannot install Active Directory Lightweight Directory Services unless the following role services or features are also installed.

- Remote Server Administration Tools
  - Role Administration Tools
    - AD DS and AD LDS Tools
      - Active Directory module for Windows PowerShell
      - [Tools] AD LDS Snap-Ins and Command-Line Tools

☑ Include management tools (if applicable)

9. Activate the check box for `Include management tools`.

10. Click on **`Add Features`**.



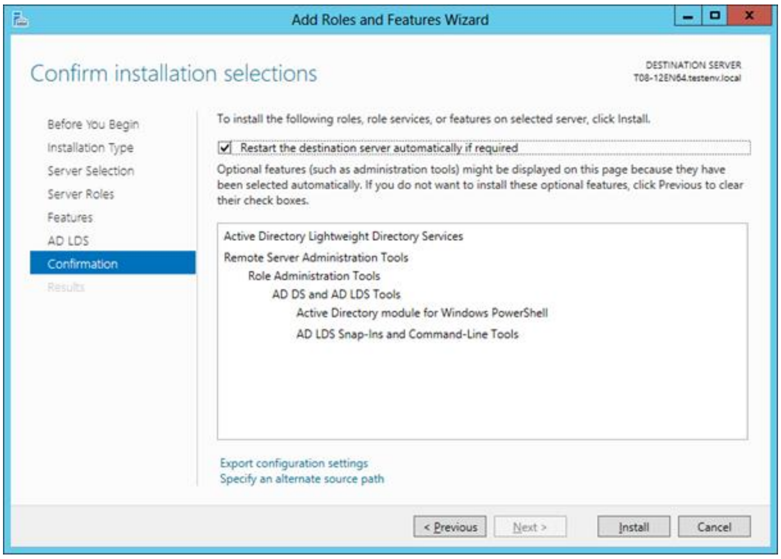
Active Directory Lightweight Directory Services (AD LDS)

Organizations that have applications which require a directory for storing application data can use Active Directory Lightweight Directory Services (AD LDS) as the data store. AD LDS runs as a non-operating-system service, and, as such, it does not require deployment on a domain controller. Running as a non-operating-system service allows multiple instances of AD LDS to run concurrently on a single server, and each instance can be configured independently for servicing multiple applications.

Things to note:

- After installing AD LDS, instances of AD LDS can be created by launching the AD LDS Setup Wizard from the Advanced Tools section of the AD LDS home page.
- Before removing the AD LDS role, you must use Programs and Features in Control Panel to remove all previously installed AD LDS instances.

11. Click on **`Next`**.



Confirm installation selections

To install the following roles, role services, or features on selected server, click Install.

☑ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Lightweight Directory Services
Remote Server Administration Tools
    Role Administration Tools
        AD DS and AD LDS Tools
            Active Directory module for Windows PowerShell
            AD LDS Snap-Ins and Command-Line Tools

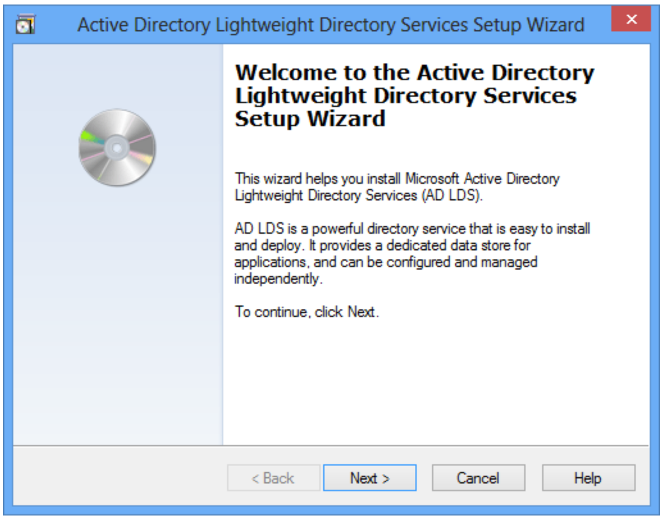
12. Confirm the automatic restart of the server.

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.



Active Directory Lightweight Directory Services Setup Wizard

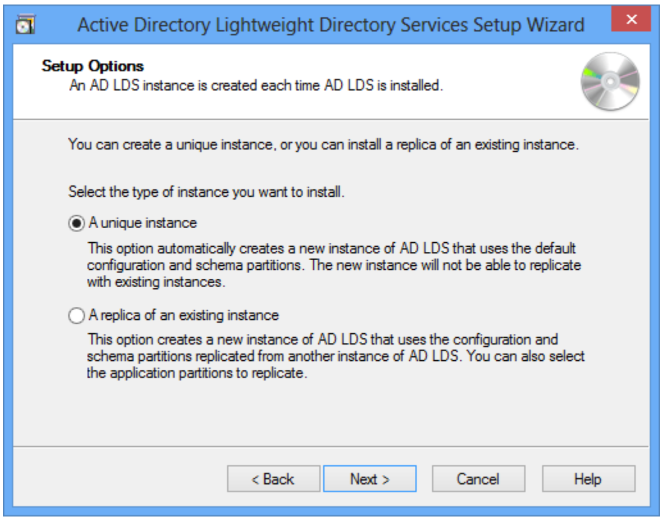
Welcome to the Active Directory Lightweight Directory Services Setup Wizard

This wizard helps you install Microsoft Active Directory Lightweight Directory Services (AD LDS).

AD LDS is a powerful directory service that is easy to install and deploy. It provides a dedicated data store for applications, and can be configured and managed independently.

To continue, click Next.

3. Click on **Next**.



Active Directory Lightweight Directory Services Setup Wizard

Setup Options

An AD LDS instance is created each time AD LDS is installed.

You can create a unique instance, or you can install a replica of an existing instance.

Select the type of instance you want to install.

● A unique instance

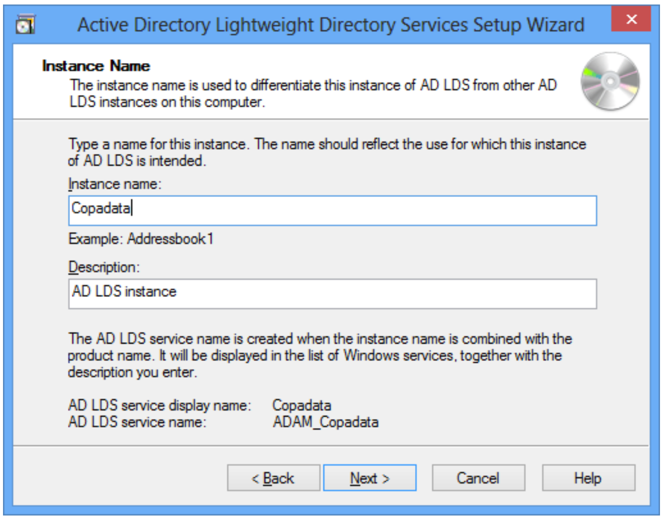
This option automatically creates a new instance of AD LDS that uses the default configuration and schema partitions. The new instance will not be able to replicate with existing instances.

○ A replica of an existing instance

This option creates a new instance of AD LDS that uses the configuration and schema partitions replicated from another instance of AD LDS. You can also select the application partitions to replicate.

4. Select `unique instance` as the installation type.

5. Click on **Next**.



Active Directory Lightweight Directory Services Setup Wizard

Instance Name

The instance name is used to differentiate this instance of AD LDS from other AD LDS instances on this computer.

Type a name for this instance. The name should reflect the use for which this instance of AD LDS is intended.

Instance name:
Copadata

Example: Addressbook1

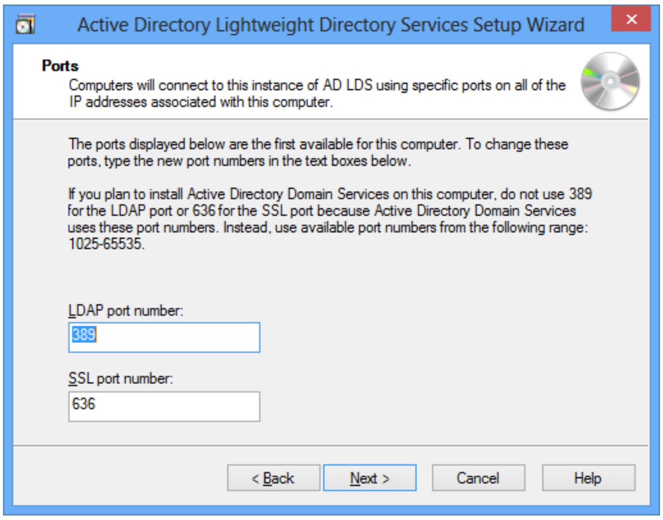
Description:
AD LDS instance

The AD LDS service name is created when the instance name is combined with the product name. It will be displayed in the list of Windows services, together with the description you enter.

AD LDS service display name: Copadata
AD LDS service name: ADAM_Copadata

6. Assign an **instance name**.

7. Click on **Next**.



Active Directory Lightweight Directory Services Setup Wizard

Ports

Computers will connect to this instance of AD LDS using specific ports on all of the IP addresses associated with this computer.

The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below.

If you plan to install Active Directory Domain Services on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory Domain Services uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.

LDAP port number:
389

SSL port number:
636

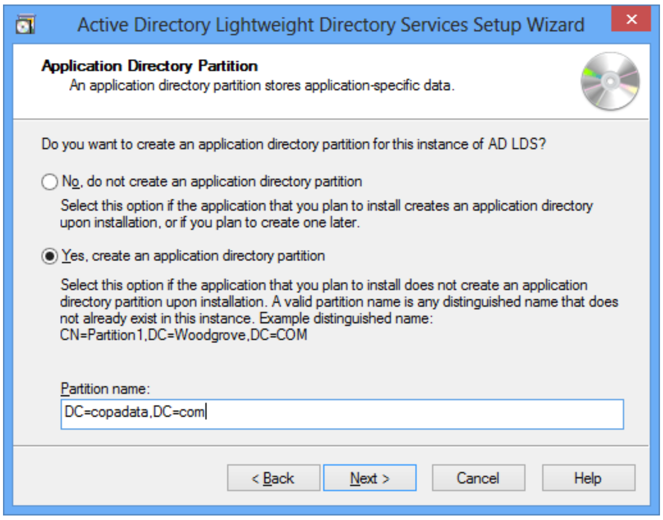
8. Enter the port number for LDAP and SSL.

   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**.



Active Directory Lightweight Directory Services Setup Wizard

Application Directory Partition

An application directory partition stores application-specific data.

Do you want to create an application directory partition for this instance of AD LDS?

○ No, do not create an application directory partition

Select this option if the application that you plan to install creates an application directory upon installation, or if you plan to create one later.

● Yes, create an application directory partition

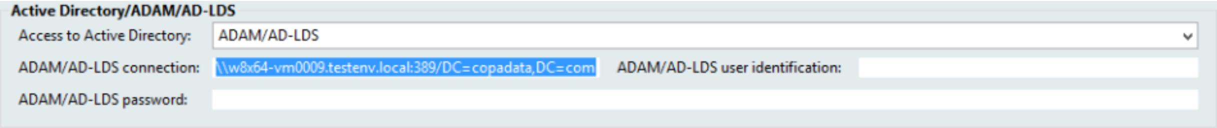
Select this option if the application that you plan to install does not create an application directory partition upon installation. A valid partition name is any distinguished name that does not already exist in this instance. Example distinguished name: CN=Partition1,DC=Woodgrove,DC=COM

Partition name: DC=copadata,DC=com

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 `ADAM/AD-LDS connection` property would be: `\\w8x64-vm0009.testenv.local:389/DC=copadata,DC=com`



Active Directory/ADAM/AD-LDS

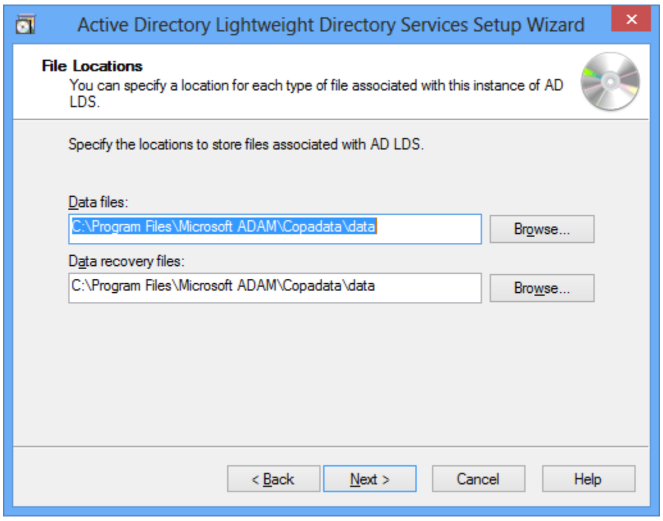
Access to Active Directory: ADAM/AD-LDS

ADAM/AD-LDS connection: \\w8x64-vm0009.testenv.local:389/DC=copadata,DC=com

ADAM/AD-LDS user identification:

ADAM/AD-LDS password:

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



Active Directory Lightweight Directory Services Setup Wizard

File Locations

You can specify a location for each type of file associated with this instance of AD LDS.

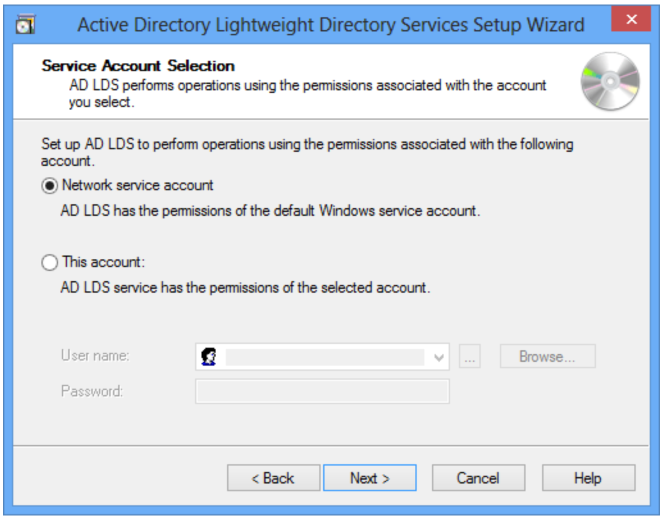
Specify the locations to store files associated with AD LDS.

Data files: C:\Program Files\Microsoft ADAM\Copadata\data

Data recovery files: C:\Program Files\Microsoft ADAM\Copadata\data

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

14. Click on **`Next`**.



Active Directory Lightweight Directory Services Setup Wizard

Service Account Selection

AD LDS performs operations using the permissions associated with the account you select.

Set up AD LDS to perform operations using the permissions associated with the following account.

● Network service account

AD LDS has the permissions of the default Windows service account.

○ This account:

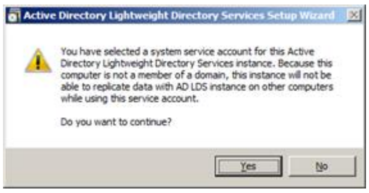
AD LDS service has the permissions of the selected account.

User name:

Password:

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:



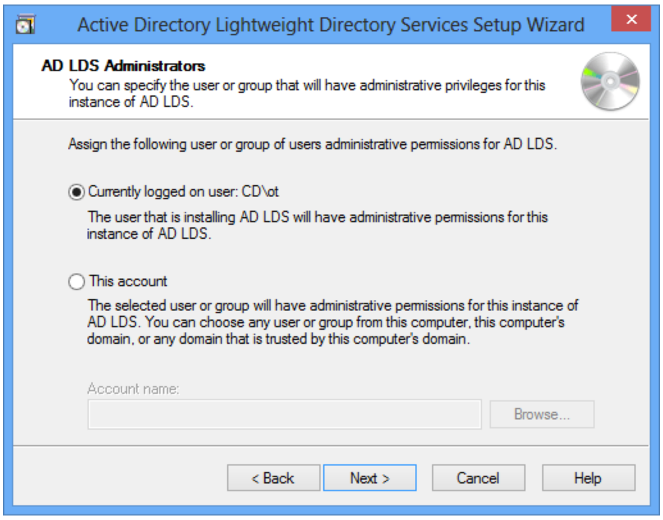
Active Directory Lightweight Directory Services Setup Wizard

You have selected a system service account for this Active Directory Lightweight Directory Services instance. Because this computer is not a member of a domain, this instance will not be able to replicate data with AD LDS instance on other computers while using this service account.

Do you want to continue?

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.



Active Directory Lightweight Directory Services Setup Wizard

AD LDS Administrators

You can specify the user or group that will have administrative privileges for this instance of AD LDS.

Assign the following user or group of users administrative permissions for AD LDS.

● Currently logged on user: CD\ot

The user that is installing AD LDS will have administrative permissions for this instance of AD LDS.

○ This account

The selected user or group will have administrative permissions for this instance of AD LDS. You can choose any user or group from this computer, this computer's domain, or any domain that is trusted by this computer's domain.

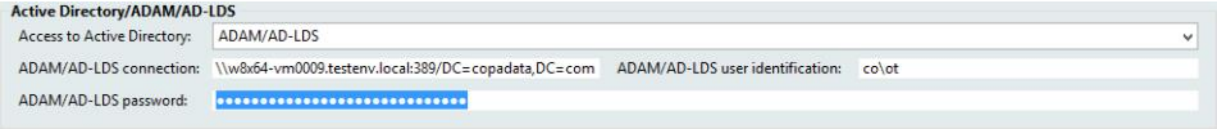
Account name:

17. Enter the user who is to administer AD LDS. In our example, the user will be the user who is currently logged on.

    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 `ADAM/AD-LDS user identification` and `ADAM/AD-LDS password` properties:



Active Directory/ADAM/AD-LDS

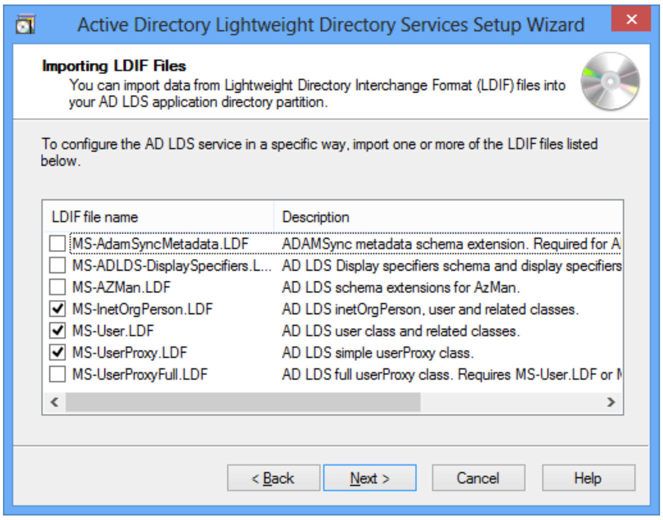
Access to Active Directory: ADAM/AD-LDS

ADAM/AD-LDS connection: \\w8x64-vm0009.testenv.local:389/DC=copadata,DC=com

ADAM/AD-LDS user identification: co\ot

ADAM/AD-LDS password: ••••••••••••••••••••••••••••••

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


Active Directory Lightweight Directory Services Setup Wizard
< Back
Next >
Cancel
Help

Importing LDIF Files

You can import data from Lightweight Directory Interchange Format (LDIF) files into your AD LDS application directory partition.

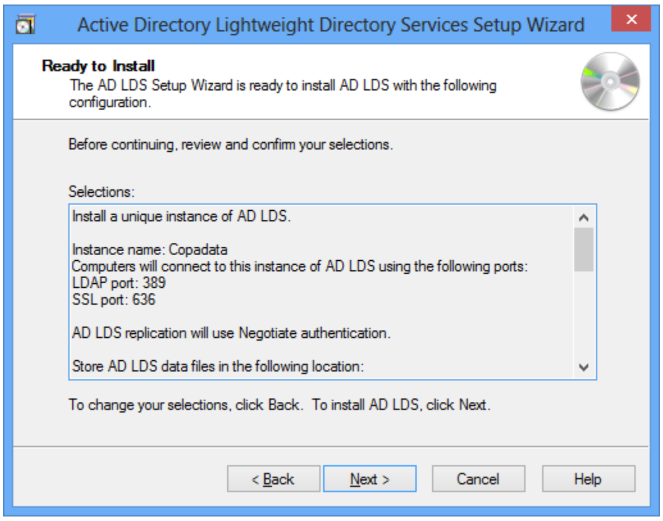
To configure the AD LDS service in a specific way, import one or more of the LDIF files listed below.

LDIF file name	Description
□ MS-AdamSyncMetadata.LDF	ADAMSync metadata schema extension. Required for A
□ MS-ADLDS-DisplaySpecifiers.L...	AD LDS Display specifiers schema and display specifiers
□ MS-AZMan.LDF	AD LDS schema extensions for AzMan.
☑ MS-InetOrgPerson.LDF	AD LDS inetOrgPerson, user and related classes.
☑ MS-User.LDF	AD LDS user class and related classes.
☑ MS-UserProxy.LDF	AD LDS simple userProxy class.
□ MS-UserProxyFull.LDF	AD LDS full userProxy class. Requires MS-User.LDF or M

19. Import the required LFIF files: You need:

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

20. Click on **Next**.


Active Directory Lightweight Directory Services Setup Wizard
< Back
Next >
Cancel
Help

Ready to Install

The AD LDS Setup Wizard is ready to install AD LDS with the following configuration.

Before continuing, review and confirm your selections.

Selections:

Install a unique instance of AD LDS.

Instance name: Copadata
Computers will connect to this instance of AD LDS using the following ports:
LDAP port: 389
SSL port: 636

AD LDS replication will use Negotiate authentication.

Store AD LDS data files in the following location:

To change your selections, click Back. To install AD LDS, click 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:

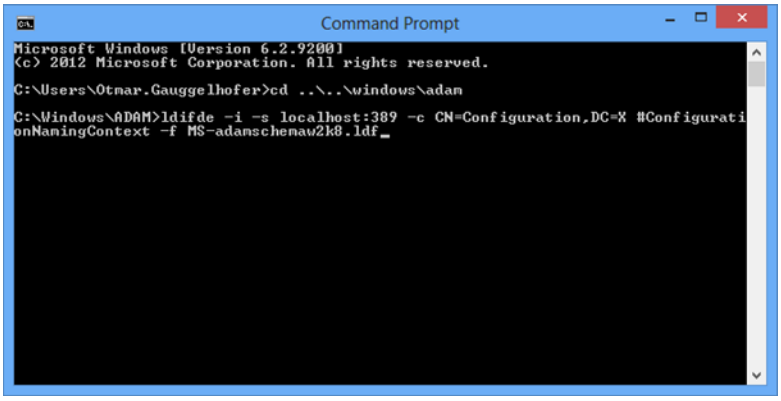
1. Open the command line.
2. Navigate to the AD LDS folder: `WINDIR%\ADAM`.
3. Enter the following command and press the `Enter` key:

```
ldifde -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:

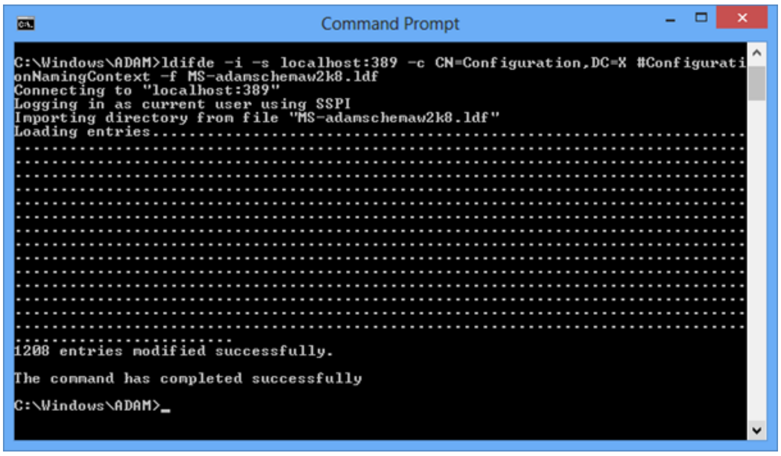
- Users
- Domain
- Passwort for ldifde

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



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Otmar.Gauggelhofer>cd ..\..\windows\adam

C:\Windows\ADAM>ldifde -i -s localhost:389 -c CN=Configuration,DC=X #Configurati
onNamingContext -f MS-adamschemaw2k8.ldf_
```

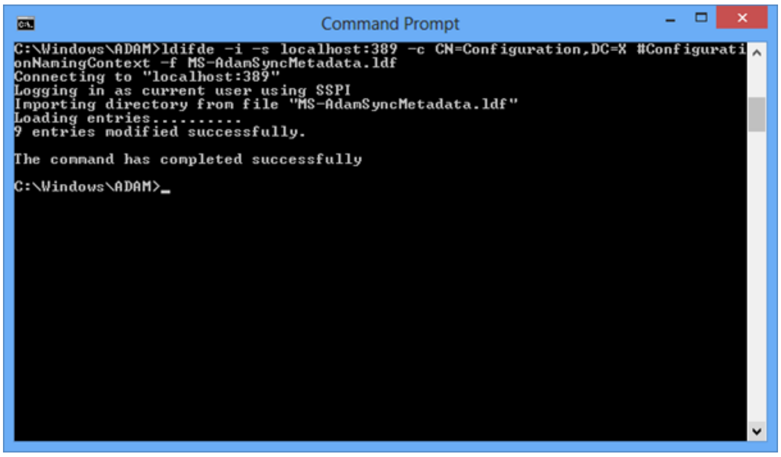
4. You receive a confirmation once the changes have been made.



```
C:\Windows\ADAM>ldifde -i -s localhost:389 -c CN=Configuration,DC=X #Configurati
onNamingContext -f MS-adamschemaw2k8.ldf
Connecting to "localhost:389"
Logging in as current user using SSPI
Importing directory from file "MS-adamschemaw2k8.ldf"
Loading entries.................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
........................
1208 entries modified successfully.

The command has completed successfully

C:\Windows\ADAM>_
```

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

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



```
C:\Windows\ADAM>ldifde -i -s localhost:389 -c CN=Configuration,DC=X #Configurati
onNamingContext -f MS-AdamSyncMetadata.ldf
Connecting to "localhost:389"
Logging in as current user using SSPI
Importing directory from file "MS-AdamSyncMetadata.ldf"
Loading entries..........
9 entries modified successfully.

The command has completed successfully

C:\Windows\ADAM>_
```

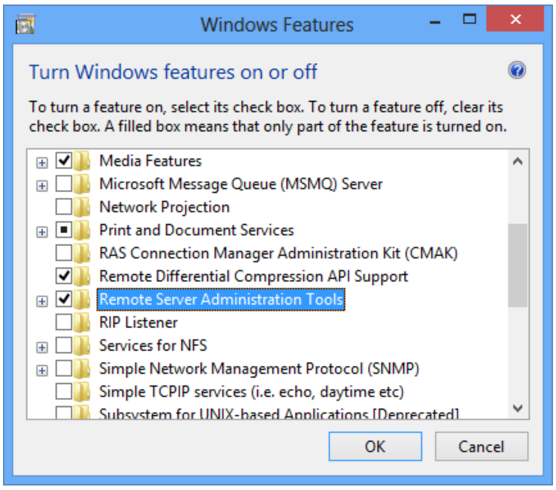
6. You receive a confirmation once it has been successfully carried out.

Installing Remote Server administration under Windows 8

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

1. Open the Control Panel
2. Open **`Programs and Features`**.

3. Select **`Turn Windows features on or off`**.



Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☑ Media Features
- ☐ Microsoft Message Queue (MSMQ) Server
- ☐ Network Projection
- ■ Print and Document Services
- ☐ RAS Connection Manager Administration Kit (CMAK)
- ☑ Remote Differential Compression API Support
- ☑ Remote Server Administration Tools
- ☐ RIP Listener
- ☐ Services for NFS
- ☐ Simple Network Management Protocol (SNMP)
- ☐ Simple TCPIP services (i.e. echo, daytime etc)
- ☐ Subsystem for UNIX-based Applications [Deprecated]

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

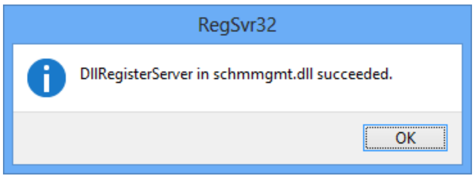
The following tools are helpful for the administration of AD LDS:

- 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.

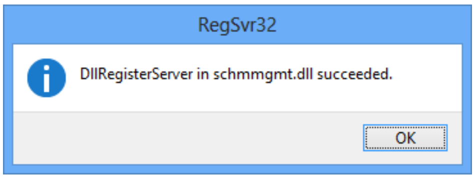


RegSvr32

DllRegisterServer in schmmgmt.dll succeeded.

2. Enter the following command and press the `Enter` key: **`regsvr32 schmmgmt.dll`**

3. You receive a confirmation after successful registration:

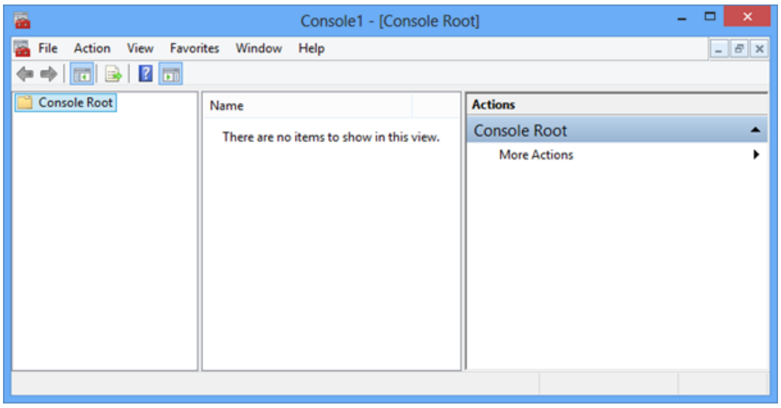


DllRegisterServer in schmmgmt.dll succeeded.

4. Open the version.

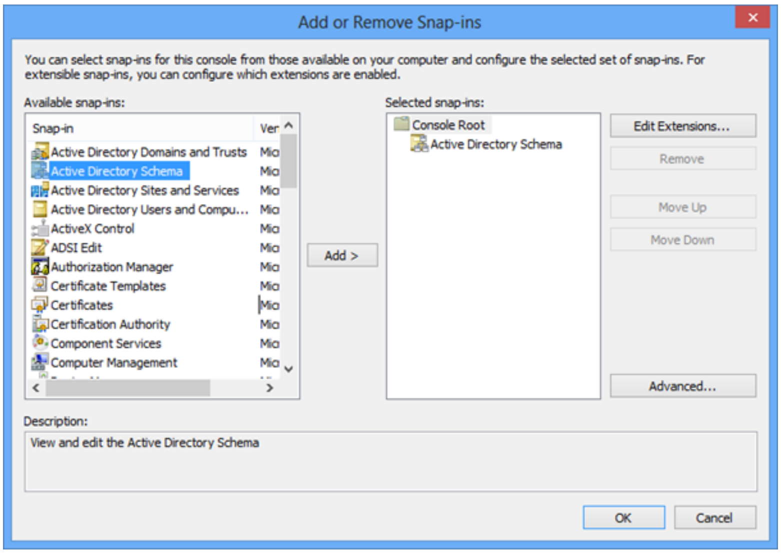
   Enter: **`mmc /a`**

5. The administration console is opened:



There are no items to show in this view.

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



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Ver
Active Directory Domains and Trusts	Mic
Active Directory Schema	Mic
Active Directory Sites and Services	Mic
Active Directory Users and Compu...	Mic
ActiveX Control	Mic
ADSI Edit	Mic
Authorization Manager	Mic
Certificate Templates	Mic
Certificates	Mic
Certification Authority	Mic
Component Services	Mic
Computer Management	Mic

Selected snap-ins:

- Console Root
  - Active Directory Schema

Description:

View and edit the Active Directory Schema

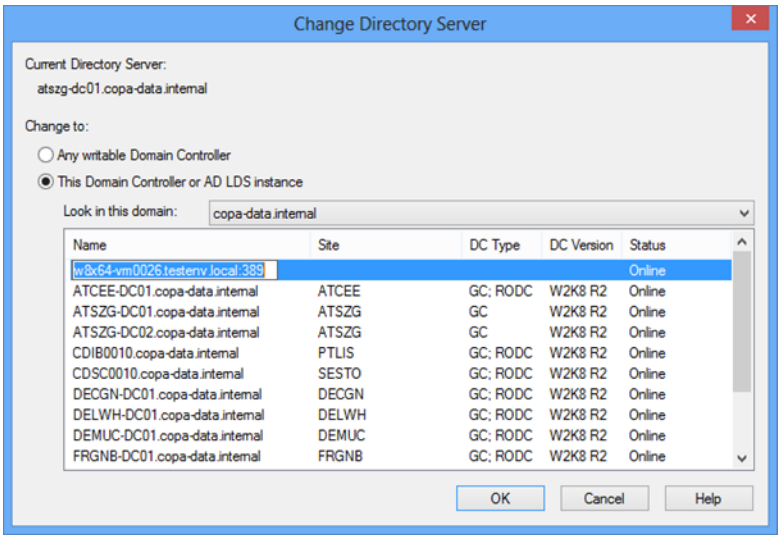
7. Select **`Active Directory Schema`**.

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



Change Directory Server

Current Directory Server:
atszg-dc01.copa-data.internal

Change to:

○ Any writable Domain Controller

● This Domain Controller or AD LDS instance

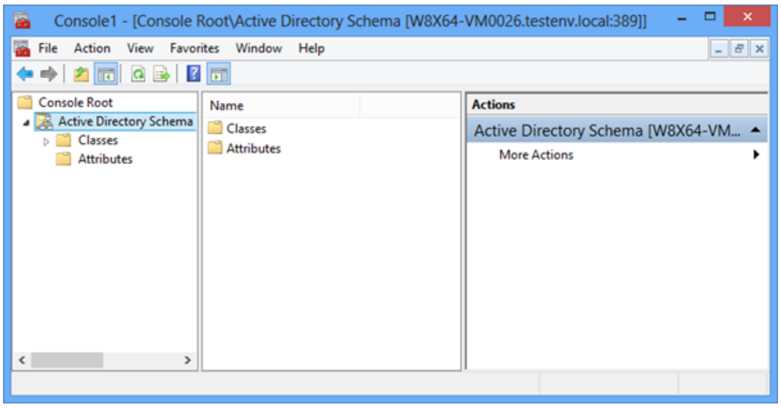
Look in this domain: copa-data.internal

Name	Site	DC Type	DC Version	Status
w8x64-vm0026.testenv.local:389				Online
ATCEE-DC01.copa-data.internal	ATCEE	GC; RODC	W2K8 R2	Online
ATSZG-DC01.copa-data.internal	ATSZG	GC	W2K8 R2	Online
ATSZG-DC02.copa-data.internal	ATSZG	GC	W2K8 R2	Online
CDIB0010.copa-data.internal	PTLIS	GC; RODC	W2K8 R2	Online
CDSC0010.copa-data.internal	SESTO	GC; RODC	W2K8 R2	Online
DECGN-DC01.copa-data.internal	DECGN	GC; RODC	W2K8 R2	Online
DELWH-DC01.copa-data.internal	DELWH	GC; RODC	W2K8 R2	Online
DEMUC-DC01.copa-data.internal	DEMUC	GC; RODC	W2K8 R2	Online
FRGNB-DC01.copa-data.internal	FRGNB	GC; RODC	W2K8 R2	Online

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:

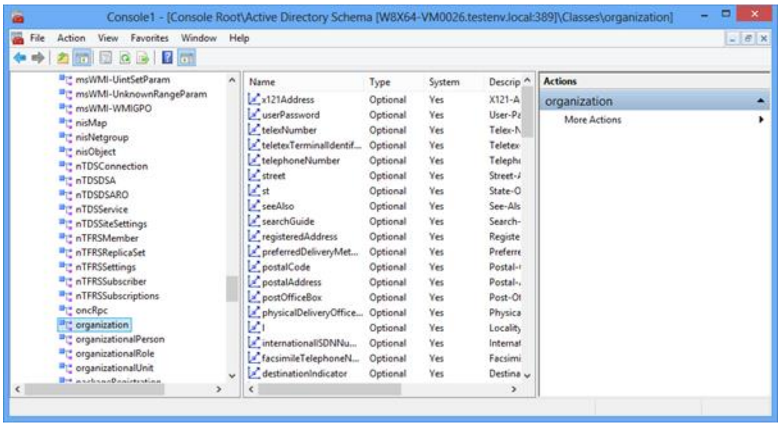


Console1 - [Console Root\Active Directory Schema [W8X64-VM0026.testenv.local:389]]

13. Save the snap-in via *File -> Save*.

14. Optional:

a) Open the **classes** folder and navigate to the **organization** entry.



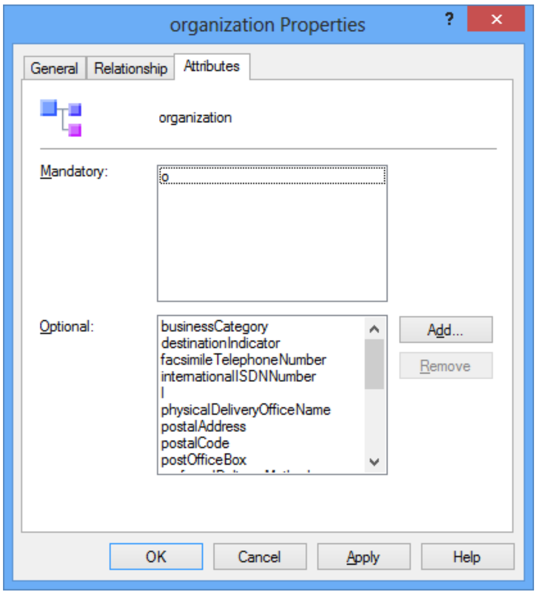
Console1 - [Console Root\Active Directory Schema [W8X64-VM0026.testenv.local:389]\Classes\organization]

msWMI-UintSetParam
msWMI-UnknownRangeParam
msWMI-WMIGPO
nisMap
nisNetgroup
nisObject
nTDSConnection
nTDSDSA
nTDSDSARO
nTDSService
nTDSSiteSettings
nTFRSMember
nTFRSReplicaSet
nTFRSSettings
nTFRSSubscriber
nTFRSSubscriptions
oncRpc
organization
organizationalPerson
organizationalRole
organizationalUnit

Name	Type	System	Descrip
x121Address	Optional	Yes	X121-A
userPassword	Optional	Yes	User-Pa
telexNumber	Optional	Yes	Telex-N
teletexTerminalIdentif...	Optional	Yes	Teletex
telephoneNumber	Optional	Yes	Teleph
street	Optional	Yes	Street-/
st	Optional	Yes	State-O
seeAlso	Optional	Yes	See-Als
searchGuide	Optional	Yes	Search-
registeredAddress	Optional	Yes	Registe
preferredDeliveryMet...	Optional	Yes	Preferre
postalCode	Optional	Yes	Postal-I
postalAddress	Optional	Yes	Postal-,
postOfficeBox	Optional	Yes	Post-Of
physicalDeliveryOffice...	Optional	Yes	Physica
l	Optional	Yes	Locality
internationalISDNNu...	Optional	Yes	Internat
facsimileTelephoneN...	Optional	Yes	Facsimi
destinationIndicator	Optional	Yes	Destina

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

c) Open the **Attributes** tab.



organization Properties

organization

Mandatory: o

Optional:
businessCategory
destinationIndicator
facsimileTelephoneNumber
internationalISDNNumber
l
physicalDeliveryOfficeName
postalAddress
postalCode
postOfficeBox

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`**.

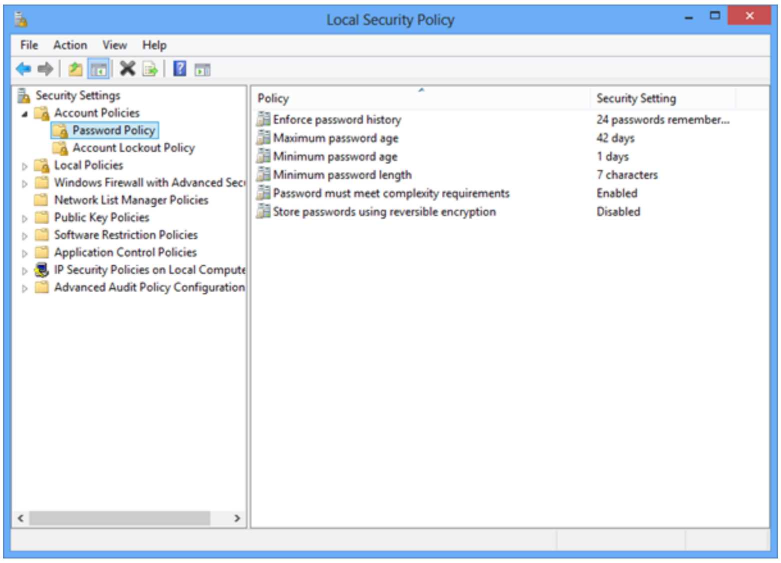
16. Close the console.

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.

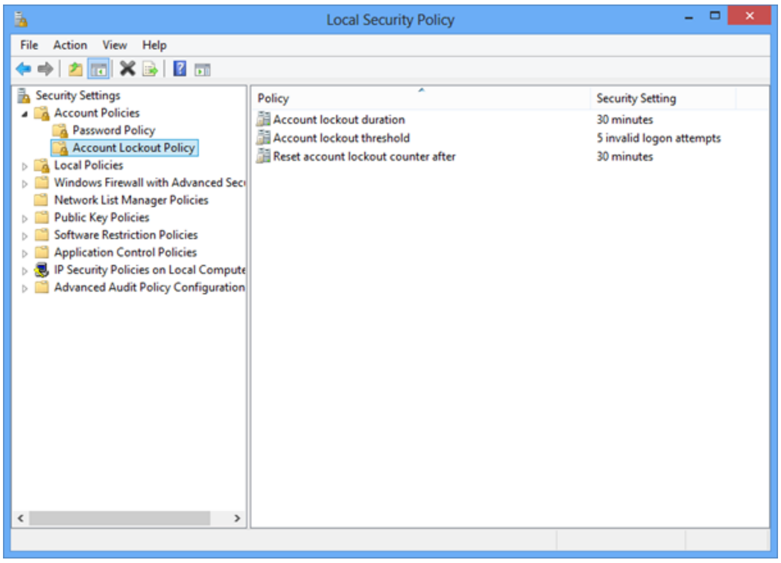
For local security guidelines:

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


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

4. Configure **`Account Lockout Policy`**


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

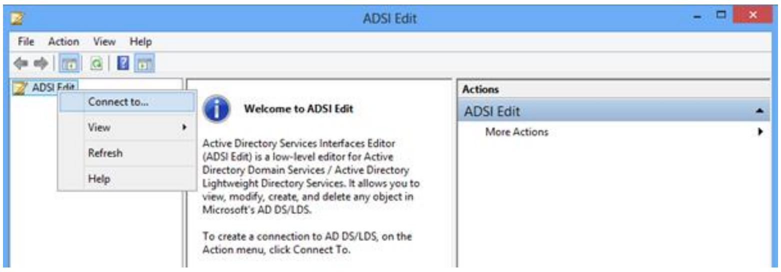
Configure roles, organization units and users

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.



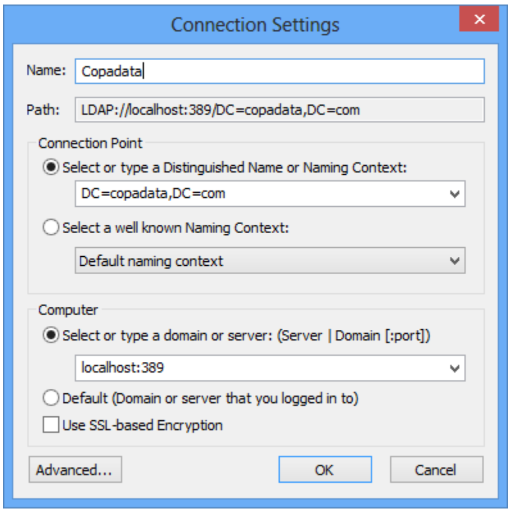
Welcome to ADSI Edit

Active Directory Services Interfaces Editor (ADSI Edit) is a low-level editor for Active Directory Domain Services / Active Directory Lightweight Directory Services. It allows you to view, modify, create, and delete any object in Microsoft's AD DS/LDS.

To create a connection to AD DS/LDS, on the Action menu, click Connect To.

2. Select **`Establish connection`** in the context menu.

3. The dialog for the connection settings is opened.



Name: Copadata

Path: LDAP://localhost:389/DC=copadata,DC=com

Connection Point

● Select or type a Distinguished Name or Naming Context:

DC=copadata,DC=com

○ Select a well known Naming Context:

Default naming context

Computer

● Select or type a domain or server: (Server | Domain [:port])

localhost:389

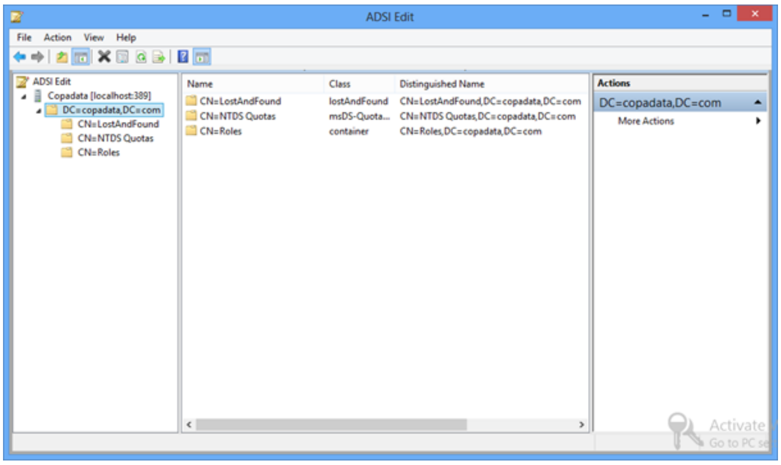
○ Default (Domain or server that you logged in to)

□ Use SSL-based Encryption

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):



ADSI Edit
- Copadata [localhost:389]
  - DC=copadata,DC=com
    - CN=LostAndFound
    - CN=NTDS Quotas
    - CN=Roles

Name	Class	Distinguished Name
CN=LostAndFound	lostAndFound	CN=LostAndFound,DC=copadata,DC=com
CN=NTDS Quotas	msDS-Quota...	CN=NTDS Quotas,DC=copadata,DC=com
CN=Roles	container	CN=Roles,DC=copadata,DC=com

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

- Configuring roles (on page 105)
- Configuring **maxPwdAge** (on page 107)
- Creating an organization unit (on page 108)

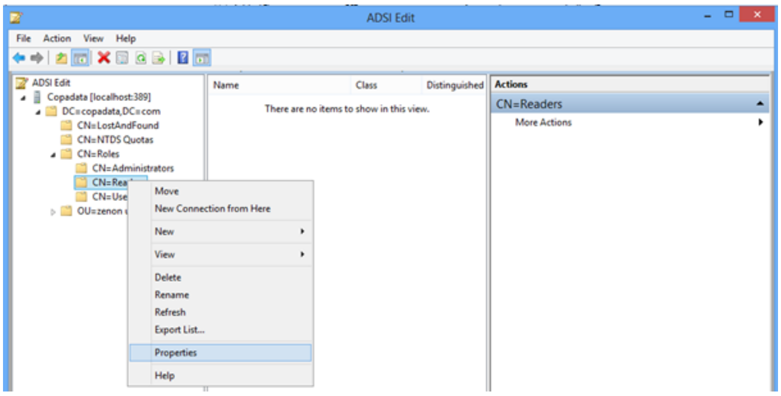
- Creating a group (on page 110)
- Creating a user (on page 114)
- Adding users to groups (on page 117)

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:

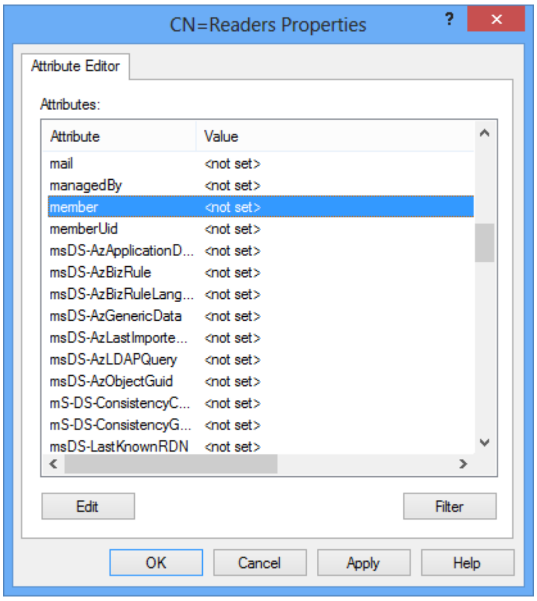
1. Expand the folder called **CN=Roles**.



There are no items to show in this view.

2. Highlight **CN=Readers**.
3. select **Properties** in the context menu

4. The properties dialog is opened



CN=Readers Properties

Attribute Editor

Attributes:

Attribute	Value
mail	<not set>
managedBy	<not set>
member	<not set>
memberUid	<not set>
msDS-AzApplicationD...	<not set>
msDS-AzBizRule	<not set>
msDS-AzBizRuleLang...	<not set>
msDS-AzGenericData	<not set>
msDS-AzLastImporte...	<not set>
msDS-AzLDAPQuery	<not set>
msDS-AzObjectGuid	<not set>
mS-DS-ConsistencyC...	<not set>
mS-DS-ConsistencyG...	<not set>
msDS-LastKnownRDN	<not set>

5. Navigate to the **member** entry.

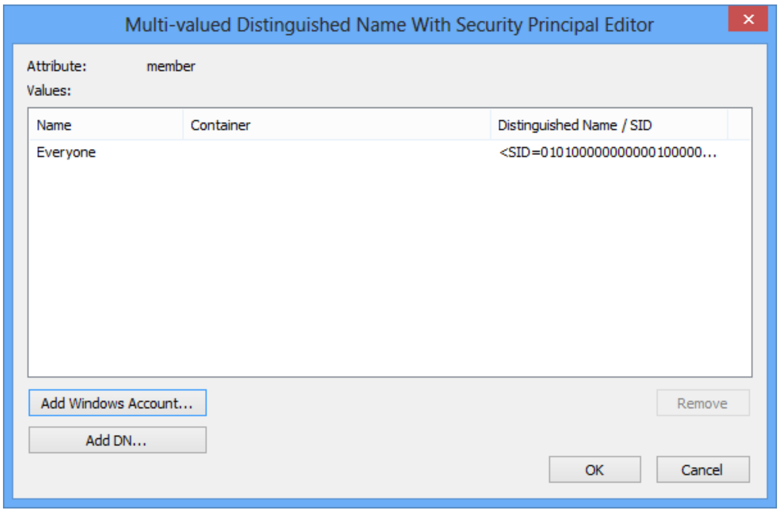
6. Click on **Edit**.

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



Multi-valued Distinguished Name With Security Principal Editor

Attribute: member

Values:

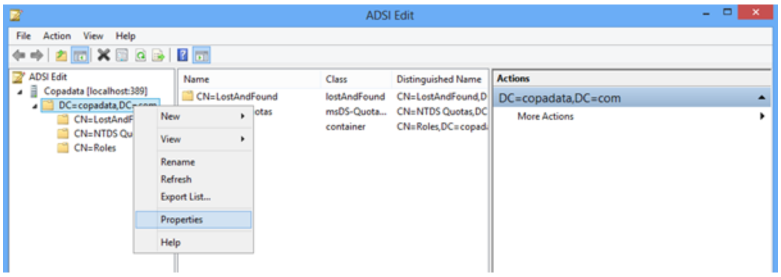
Name	Container	Distinguished Name / SID
Everyone		<SID=010100000000000100000...

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.

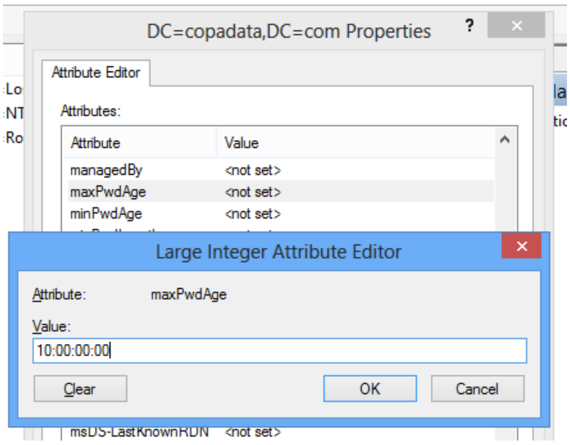
To configure rules:

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:



Name	Class	Distinguished Name
CN=LostAndFound	lostAndFound	CN=LostAndFound,D
otas	msDS-Quota...	CN=NTDS Quotas,DC
	container	CN=Roles,DC=copad

7. Navigate to the maxPwdAge entry.
8. Enter a valid value (format: `DD:HH:MM:SS`) and close the dialog.



Attribute	Value
managedBy	<not set>
maxPwdAge	<not set>
minPwdAge	<not set>
msDS-LastKnownRDN	<not set>

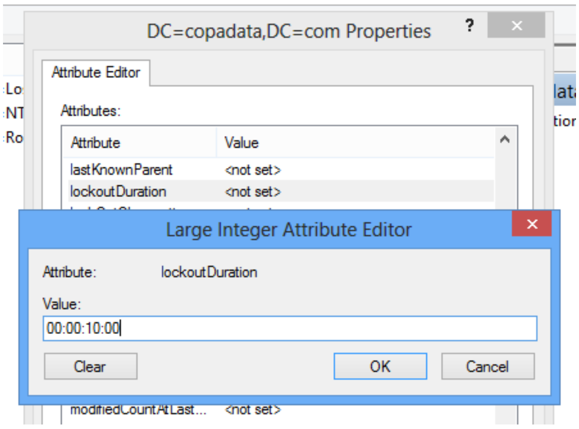
Attribute: maxPwdAge

Value: 10:00:00:00

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.

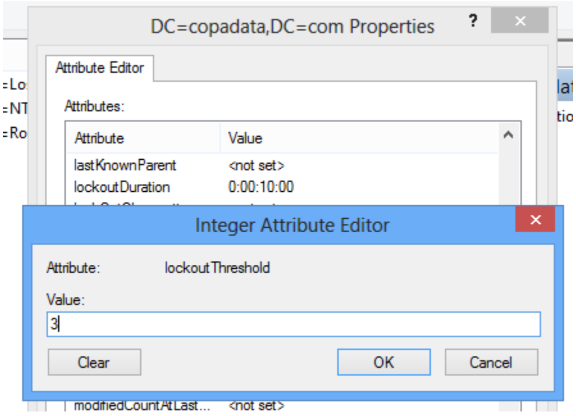


Attribute: lockoutDuration

Value: 00:00:10:00

11. Go to the `lockoutThreshold` entry.

12. Enter a valid value and close the dialog.



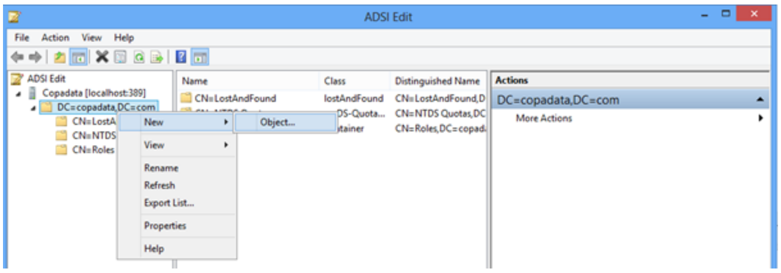
Attribute: lockoutThreshold

Value: 3

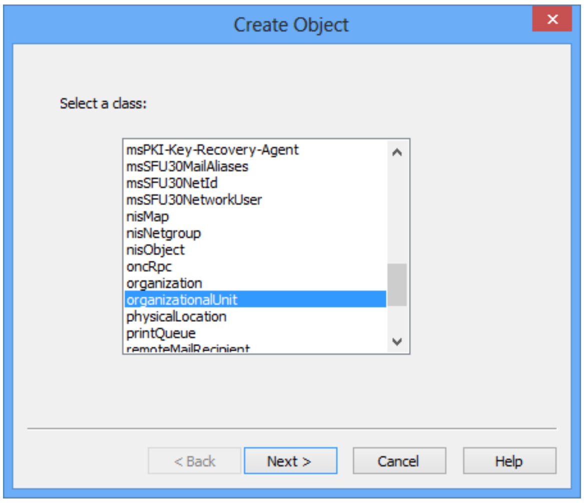
Creating an organization unit

To create an organization unit:

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

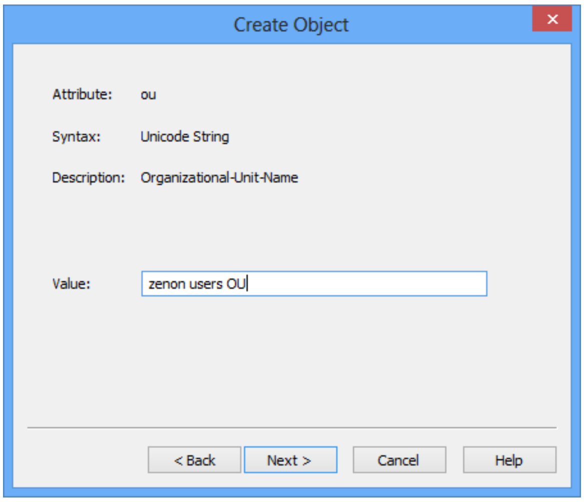


2. Select *New -> Object* in the context menu.



3. Select **`organizational unit`** as a class.

4. Click on **`Next`**.



Attribute: ou

Syntax: Unicode String

Description: Organizational-Unit-Name

Value: zenon users OU

5. Enter a name as a value.

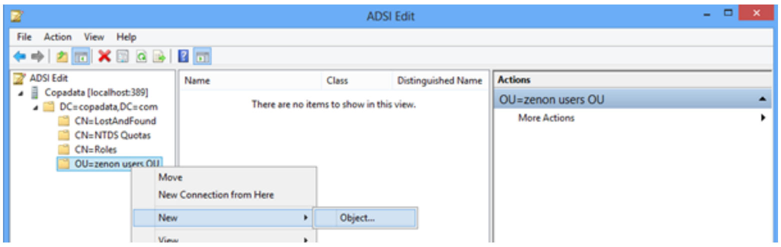
6. Click on **Next**.

7. Click on **Close**.

Creating a user group

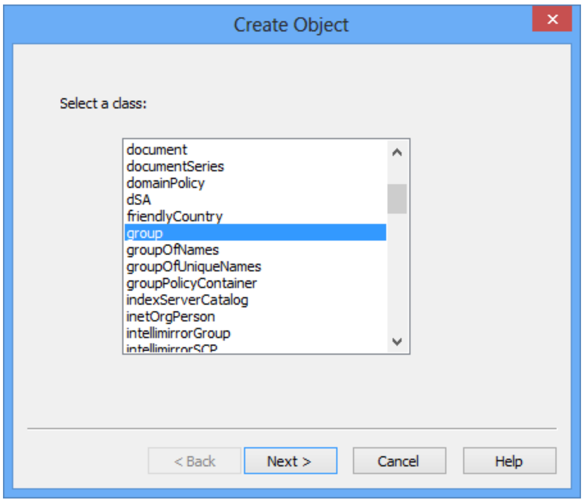
To create user groups:

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



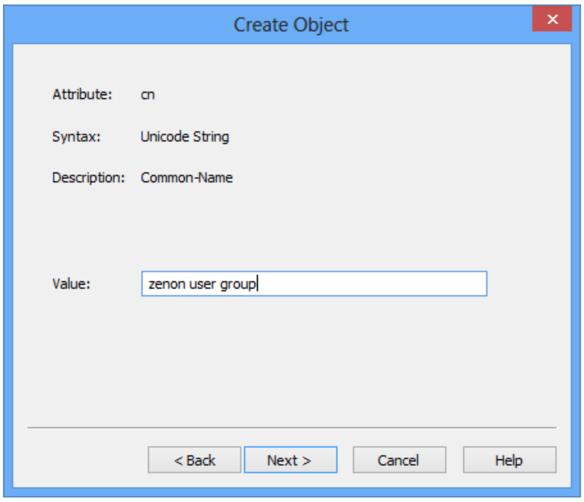
There are no items to show in this view.

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



3. Select the **Group** entry.

4. Click on **Next**.



Create Object

Attribute: cn

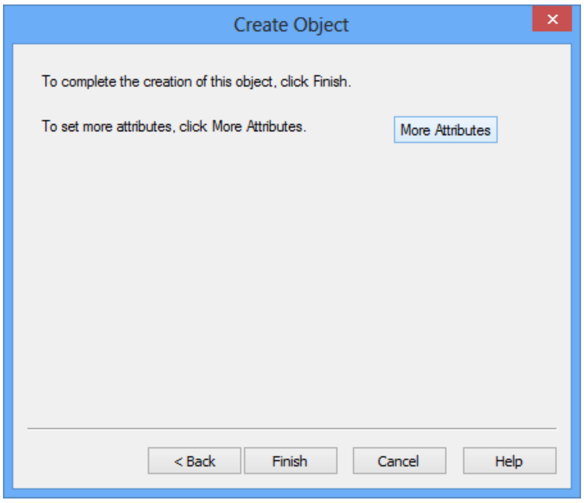
Syntax: Unicode String

Description: Common-Name

Value: zenon user group

5. Enter a name for `Value`.

6. Click on **Next**.



Create Object

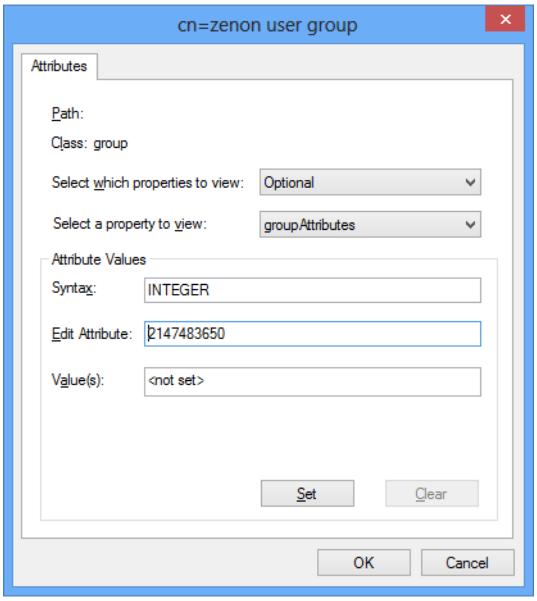
To complete the creation of this object, click Finish.

To set more attributes, click More Attributes.

7. Click on **Finish**.

8. Click on the **More attributes** button.

9. Select the entry **`groupAttributes`**.



cn=zenon user group

Attributes

Path:

Class: group

Select which properties to view: Optional

Select a property to view: groupAttributes

Attribute Values

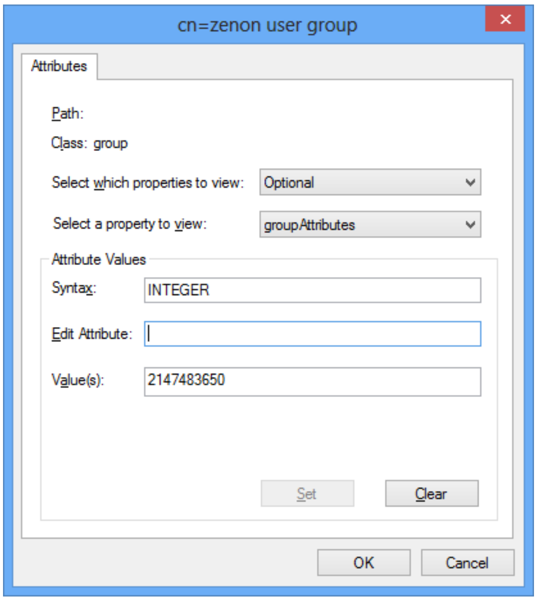
Syntax: INTEGER

Edit Attribute: 2147483650

Value(s): <not set>

10. Enter `2147483650` in `Edit attribute`.

11. Click on **`Define`**.



cn=zenon user group

Attributes

Path:

Class: group

Select which properties to view: Optional

Select a property to view: groupAttributes

Attribute Values

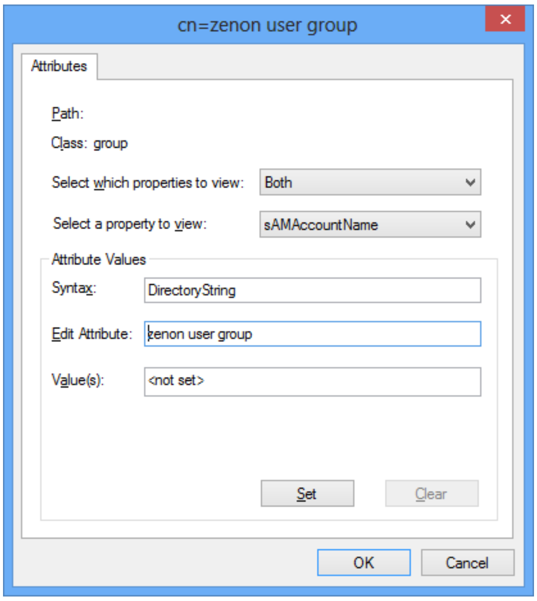
Syntax: INTEGER

Edit Attribute:

Value(s): 2147483650

12. Click on **OK**.

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



cn=zenon user group

Path:

Class: group

Select which properties to view: Both

Select a property to view: sAMAccountName

Attribute Values

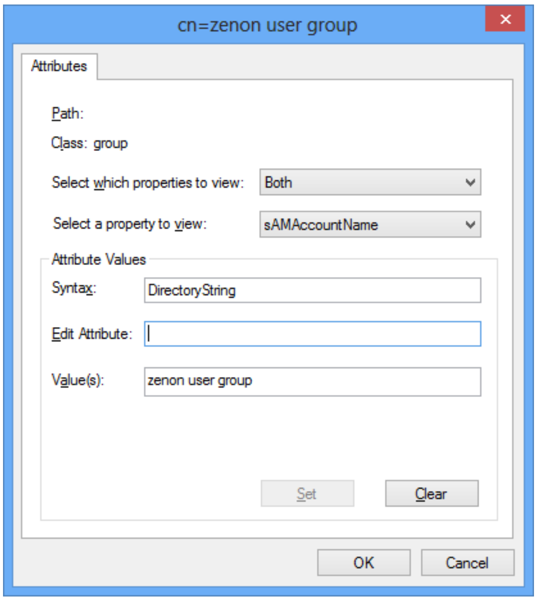
Syntax: DirectoryString

Edit Attribute: zenon user group

Value(s): <not set>

14. Enter the same value as for **group**.

15. Click on **Define**.



cn=zenon user group

Path:

Class: group

Select which properties to view: Both

Select a property to view: sAMAccountName

Attribute Values

Syntax: DirectoryString

Edit Attribute:

Value(s): zenon user group

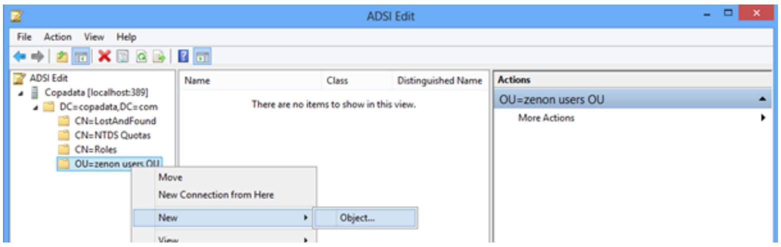
16. Click on **OK**.

17. Click on **Finish**.

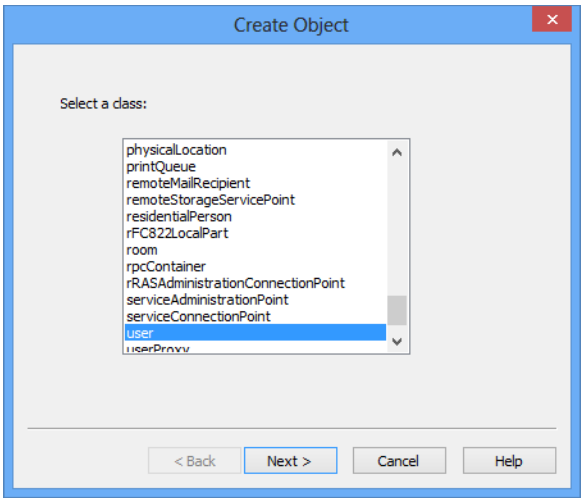
Creating a user

To create a user:

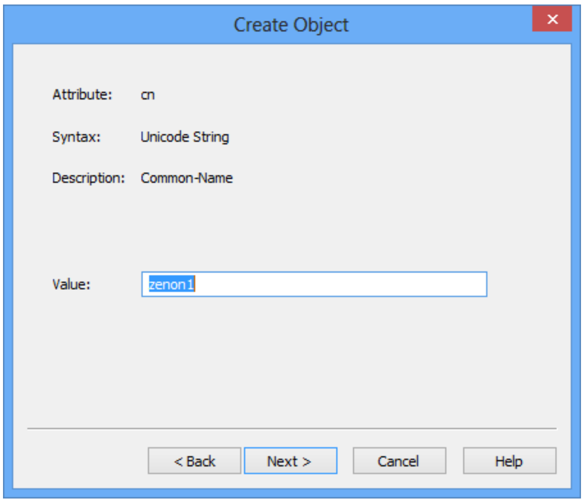
1. Highlight the organization unit.



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



3. Select the User object.



Attribute: cn

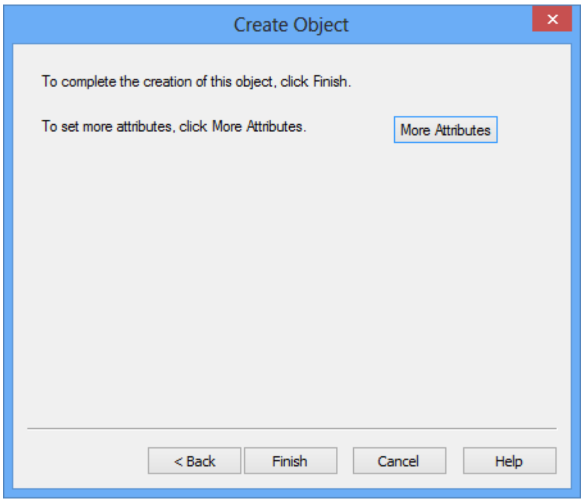
Syntax: Unicode String

Description: Common-Name

Value: zenon1

4. Enter a name as a `value`.

5. Click on **`Next`**.



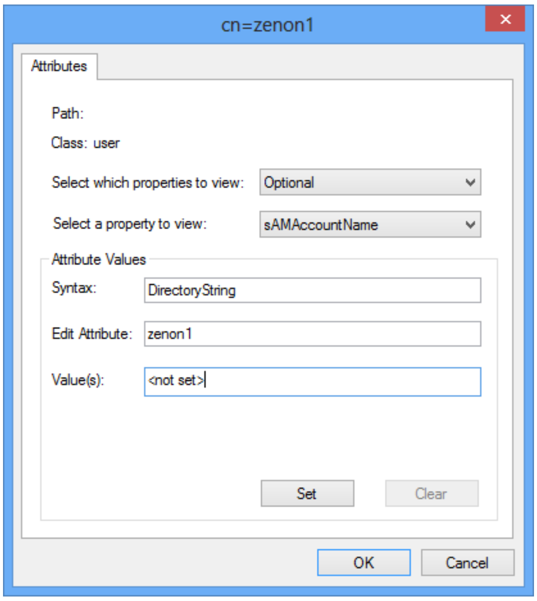
Create Object

To complete the creation of this object, click Finish.

To set more attributes, click More Attributes.

6. Click on **`More attributes`**.

7. Select `sAMAccountName`.



cn=zenon1

Path:

Class: user

Select which properties to view: Optional

Select a property to view: sAMAccountName

Attribute Values

Syntax: DirectoryString

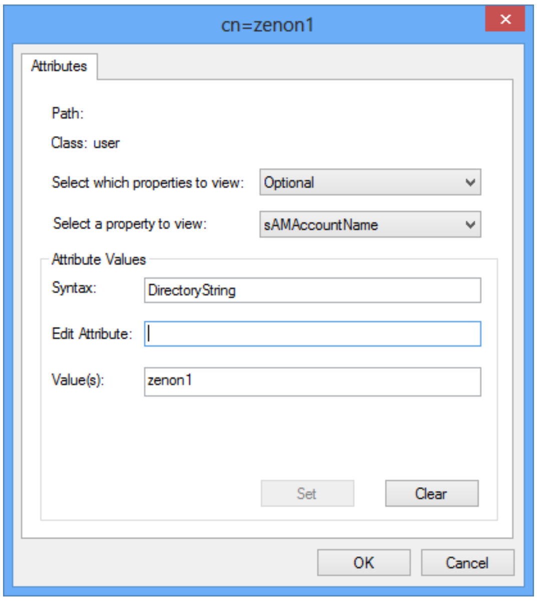
Edit Attribute: zenon1

Value(s): <not set>

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**.



cn=zenon1

Attributes

Path:

Class: user

Select which properties to view: Optional

Select a property to view: sAMAccountName

Attribute Values

Syntax: DirectoryString

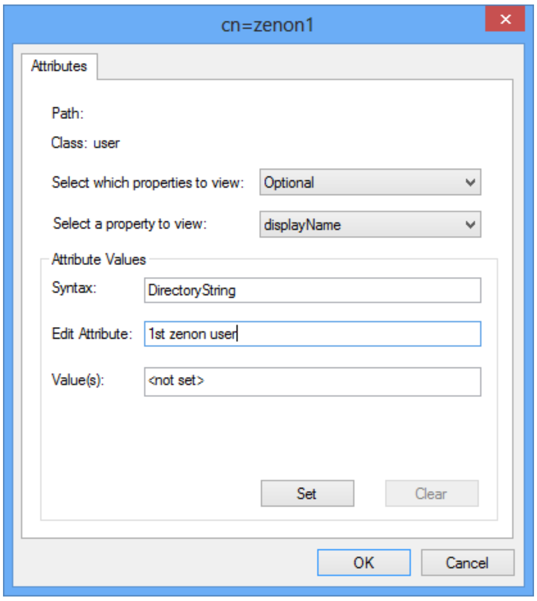
Edit Attribute:

Value(s): zenon1

10. Click on **OK**.

11. Click on **More attributes**.

12. Select `displayName`.



cn=zenon1

Attributes

Path:

Class: user

Select which properties to view: Optional

Select a property to view: displayName

Attribute Values

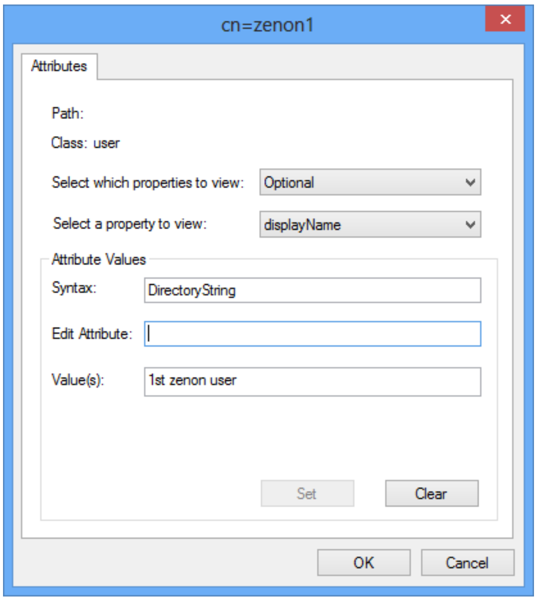
Syntax: DirectoryString

Edit Attribute: 1st zenon user

Value(s): <not set>

13. Enter a description for the display

14. Click on **Define**.


cn=zenon1

Attributes

Path:

Class: user

Select which properties to view: Optional

Select a property to view: displayName

Attribute Values

Syntax: DirectoryString

Edit Attribute:

Value(s): 1st zenon user

15. Click on **OK**.

16. Click on **Finish**.

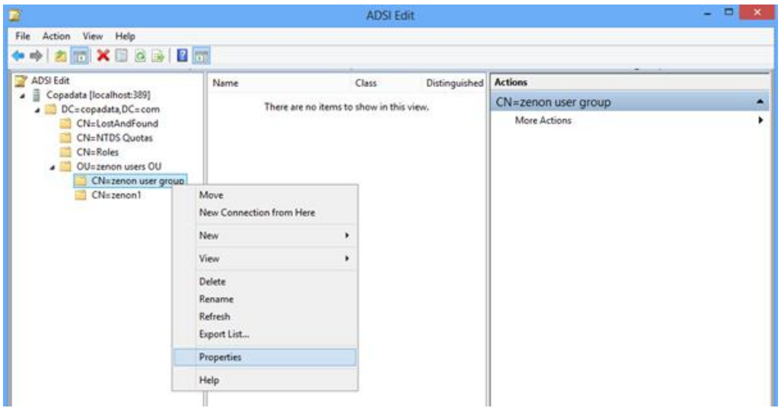
Adding users to groups and setting a password

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

ADDING A USER

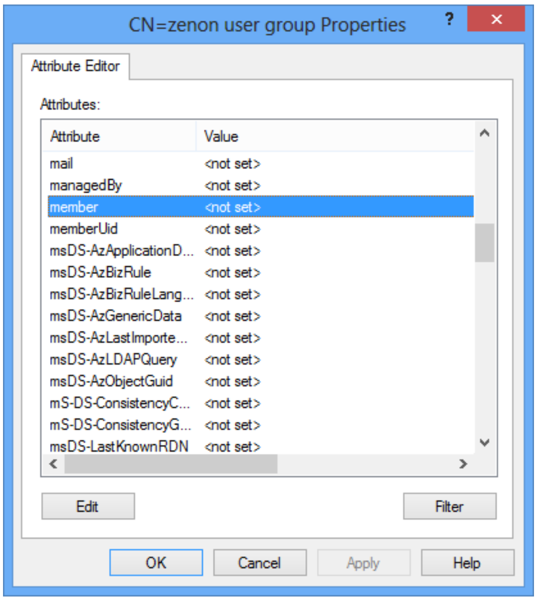
To add users to a group:

1. Highlight the group.



There are no items to show in this view.

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

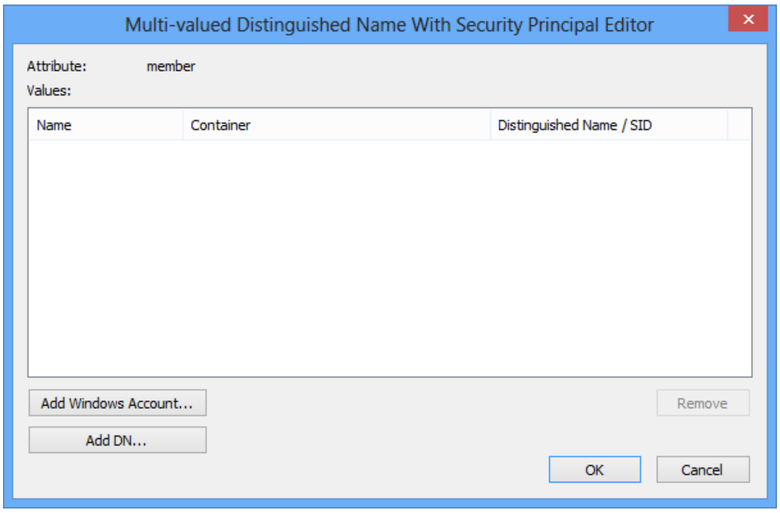


Attributes:

Attribute	Value
mail	<not set>
managedBy	<not set>
member	<not set>
memberUid	<not set>
msDS-AzApplicationD...	<not set>
msDS-AzBizRule	<not set>
msDS-AzBizRuleLang...	<not set>
msDS-AzGenericData	<not set>
msDS-AzLastImporte...	<not set>
msDS-AzLDAPQuery	<not set>
msDS-AzObjectGuid	<not set>
mS-DS-ConsistencyC...	<not set>
mS-DS-ConsistencyG...	<not set>
msDS-LastKnownRDN	<not set>

3. Highlight `member`

4. Click on **`Edit`**.


Multi-valued Distinguished Name With Security Principal Editor
Add Windows Account...
Add DN...
Remove
OK
Cancel

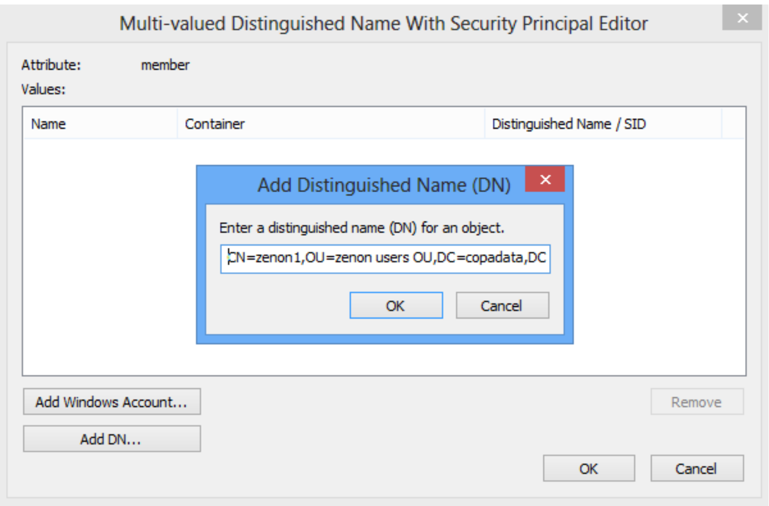
Attribute: member

Values:

Name	Container	Distinguished Name / SID

5. Click on **Add DN**.

   The dialog to add a previously-configured user is opened



Attribute: member

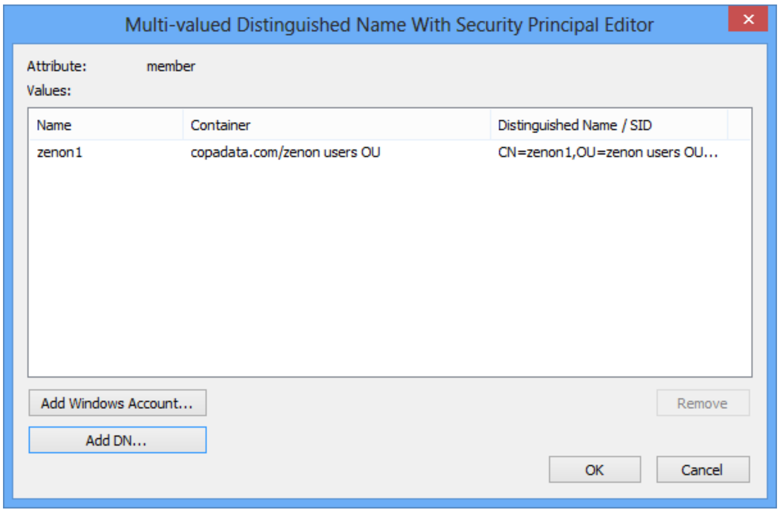
Values:

Enter a distinguished name (DN) for an object.

CN=zenon1,OU=zenon users OU,DC=copadata,DC

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.



Multi-valued Distinguished Name With Security Principal Editor
Add Windows Account...
Add DN...
Remove
OK
Cancel

Attribute: member

Values:

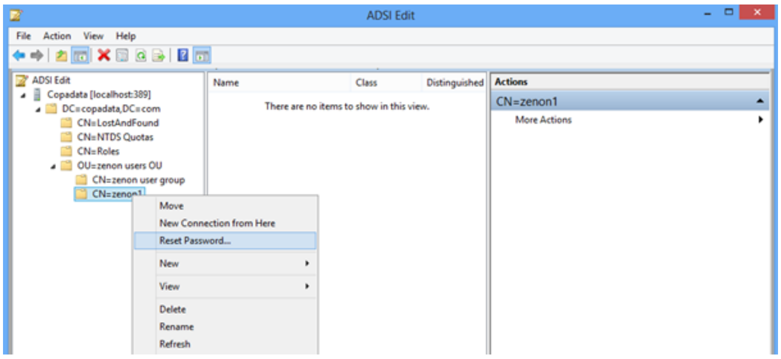
Name	Container	Distinguished Name / SID
zenon1	copadata.com/zenon users OU	CN=zenon1,OU=zenon users OU...

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.



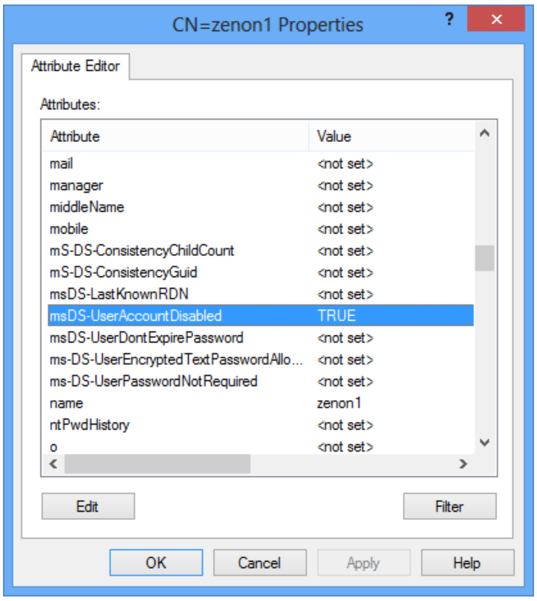
2. Select **Reset password** in the context menu.

3. Issue a password.

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

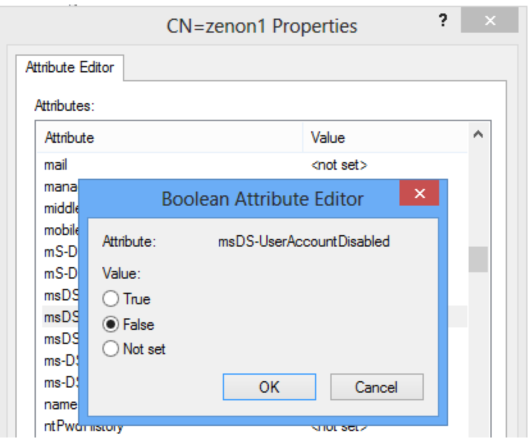
4. Close the dialog.

5. Select **Properties** in the context menu of the user



Attribute	Value
mail	<not set>
manager	<not set>
middleName	<not set>
mobile	<not set>
mS-DS-ConsistencyChildCount	<not set>
mS-DS-ConsistencyGuid	<not set>
msDS-LastKnownRDN	<not set>
msDS-UserAccountDisabled	TRUE
msDS-UserDontExpirePassword	<not set>
ms-DS-UserEncryptedTextPasswordAllo...	<not set>
ms-DS-UserPasswordNotRequired	<not set>
name	zenon1
ntPwdHistory	<not set>
o	<not set>

6. Select `msDS-UserAccountDisabled` in the properties.



Attribute	Value
mail	<not set>

Attribute: msDS-UserAccountDisabled

Value:

○ True
● False
○ Not set

7. Set the value to `incorrect`.

The user can now be used in zenon.

6.2.2 AD LDS with Windows 7 and Windows Vista

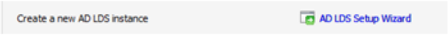
AD LDS can also be used with Windows Vista and Windows 7. You can find the setups for these on the Microsoft website (http://www.microsoft.com/downloads/en/default.aspx).

After installation, configuration is carried out via *System control-> Administration* in the same way as the description for Windows Server 2008 (on page 144).

Create new AD LDS instance

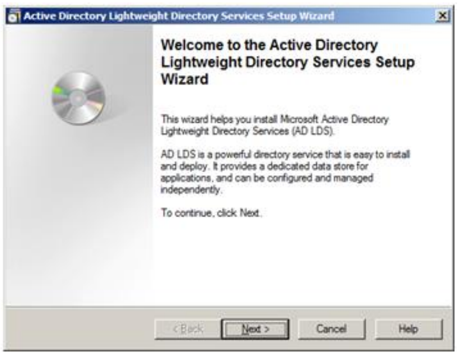
To create a new AD LDS instance:

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



Create a new AD LDS instance

2. Start the wizard:


Active Directory Lightweight Directory Services Setup Wizard
< Back
Next >
Cancel
Help

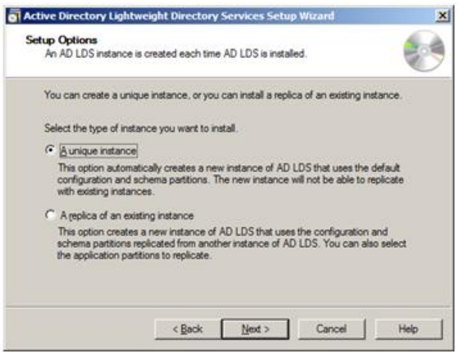
Welcome to the Active Directory Lightweight Directory Services Setup Wizard

This wizard helps you install Microsoft Active Directory Lightweight Directory Services (AD LDS).

AD LDS is a powerful directory service that is easy to install and deploy. It provides a dedicated data store for applications, and can be configured and managed independently.

To continue, click Next.

3. Select the `A unique instance` option.


Active Directory Lightweight Directory Services Setup Wizard
< Back
Next >
Cancel
Help

Setup Options

An AD LDS instance is created each time AD LDS is installed.

You can create a unique instance, or you can install a replica of an existing instance.

Select the type of instance you want to install.

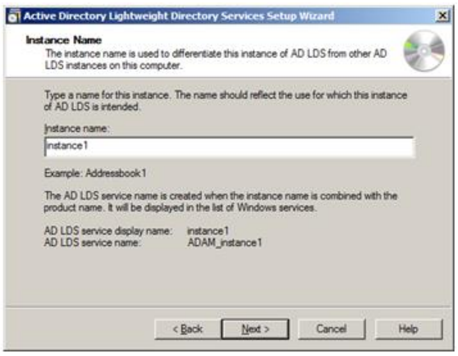
● A unique instance

This option automatically creates a new instance of AD LDS that uses the default configuration and schema partitions. The new instance will not be able to replicate with existing instances.

○ A replica of an existing instance

This option creates a new instance of AD LDS that uses the configuration and schema partitions replicated from another instance of AD LDS. You can also select the application partitions to replicate.

4. Give the instance a name.


Active Directory Lightweight Directory Services Setup Wizard
< Back
Next >
Cancel
Help

Instance Name

The instance name is used to differentiate this instance of AD LDS from other AD LDS instances on this computer.

Type a name for this instance. The name should reflect the use for which this instance of AD LDS is intended.

Instance name: instance1

Example: Addressbook1

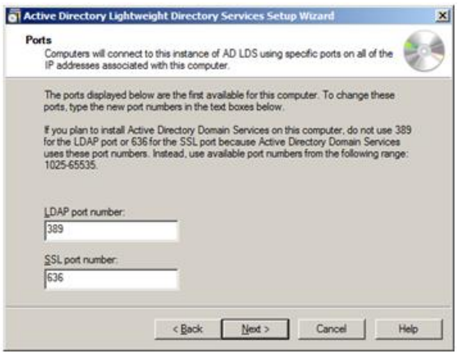
The AD LDS service name is created when the instance name is combined with the product name. It will be displayed in the list of Windows services.

AD LDS service display name: instance1
AD LDS service name: ADAM_instance1

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.


Active Directory Lightweight Directory Services Setup Wizard

Ports

Computers will connect to this instance of AD LDS using specific ports on all of the IP addresses associated with this computer.

The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below.

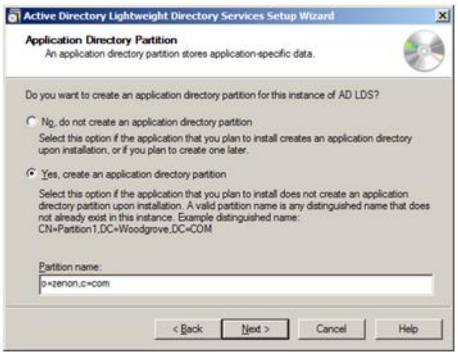
If you plan to install Active Directory Domain Services on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory Domain Services uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.

LDAP port number: 389

SSL port number: 636

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

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


Active Directory Lightweight Directory Services Setup Wizard

Application Directory Partition

An application directory partition stores application-specific data.

Do you want to create an application directory partition for this instance of AD LDS?

○ No, do not create an application directory partition

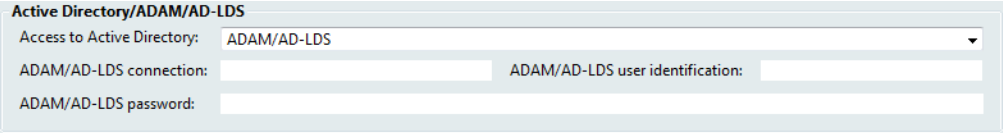
Select this option if the application that you plan to install creates an application directory upon installation, or if you plan to create one later.

● Yes, create an application directory partition

Select this option if the application that you plan to install does not create an application directory partition upon installation. A valid partition name is any distinguished name that does not already exist in this instance. Example distinguished name: CN=Partition1,DC=Woodgrove,DC=COM

Partition name: o=zenon,c=com

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


Active Directory/ADAM/AD-LDS

Access to Active Directory: ADAM/AD-LDS

ADAM/AD-LDS connection:

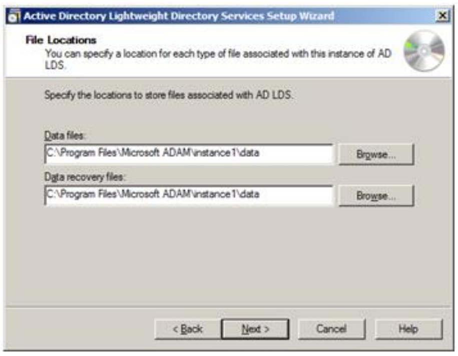
ADAM/AD-LDS user identification:

ADAM/AD-LDS password:

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.



Active Directory Lightweight Directory Services Setup Wizard

File Locations

You can specify a location for each type of file associated with this instance of AD LDS.

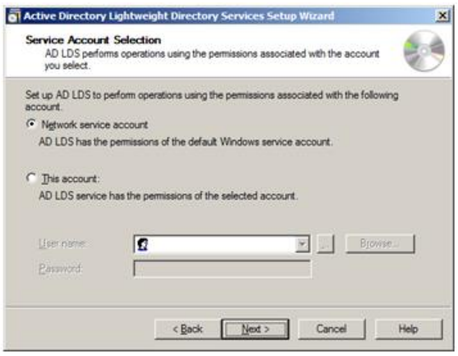
Specify the locations to store files associated with AD LDS.

Data files:
C:\Program Files\Microsoft ADAM\instance1\data

Data recovery files:
C:\Program Files\Microsoft ADAM\instance1\data

8. Define the service account for AD LDS.

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



Active Directory Lightweight Directory Services Setup Wizard

Service Account Selection

AD LDS performs operations using the permissions associated with the account you select.

Set up AD LDS to perform operations using the permissions associated with the following account.

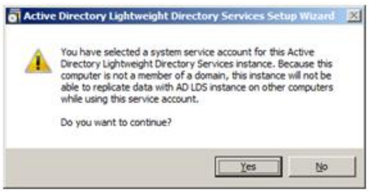
● Network service account
AD LDS has the permissions of the default Windows service account.

○ This account:
AD LDS service has the permissions of the selected account.

User name:

Password:

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



Active Directory Lightweight Directory Services Setup Wizard

You have selected a system service account for this Active Directory Lightweight Directory Services instance. Because this computer is not a member of a domain, this instance will not be able to replicate data with AD LDS instance on other computers while using this service account.

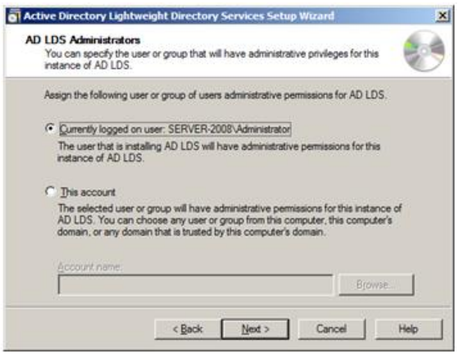
Do you want to continue?

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

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

9. Define the user who receives administrator rights.

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



Active Directory Lightweight Directory Services Setup Wizard

AD LDS Administrators

You can specify the user or group that will have administrative privileges for this instance of AD LDS.

Assign the following user or group of users administrative permissions for AD LDS.

● Currently logged on user: SERVER-2008\Administrator

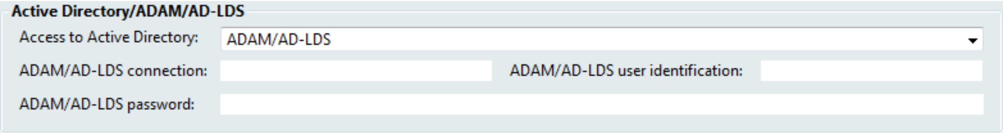
The user that is installing AD LDS will have administrative permissions for this instance of AD LDS.

○ This account

The selected user or group will have administrative permissions for this instance of AD LDS. You can choose any user or group from this computer, this computer's domain, or any domain that is trusted by this computer's domain.

Account name:

The user and their password are used later in zenon.



Active Directory/ADAM/AD-LDS

Access to Active Directory: ADAM/AD-LDS

ADAM/AD-LDS connection:

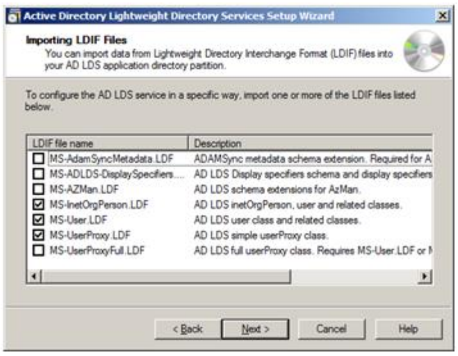
ADAM/AD-LDS user identification:

ADAM/AD-LDS password:

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`**



Active Directory Lightweight Directory Services Setup Wizard

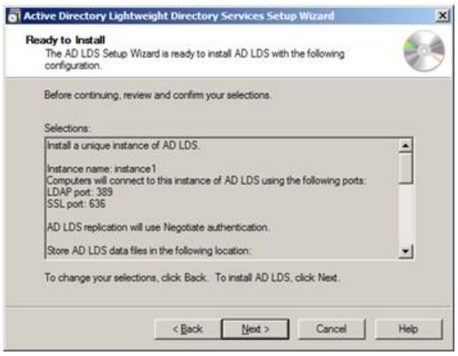
Importing LDIF Files

You can import data from Lightweight Directory Interchange Format (LDIF) files into your AD LDS application directory partition.

To configure the AD LDS service in a specific way, import one or more of the LDIF files listed below.

LDIF file name	Description
□ MS-AdamSyncMetadata.LDF	ADAMSync metadata schema extension. Required for A
□ MS-ADLDS-DisplaySpecifiers....	AD LDS Display specifiers schema and display specifiers
□ MS-AZMan.LDF	AD LDS schema extensions for AzMan.
☑ MS-InetOrgPerson.LDF	AD LDS inetOrgPerson, user and related classes.
☑ MS-User.LDF	AD LDS user class and related classes.
☑ MS-UserProxy.LDF	AD LDS simple userProxy class.
□ MS-UserProxyFull.LDF	AD LDS full userProxy class. Requires MS-User.LDF or M

11. Finish the installation



Active Directory Lightweight Directory Services Setup Wizard

Ready to Install

The AD LDS Setup Wizard is ready to install AD LDS with the following configuration.

Before continuing, review and confirm your selections.

Selections:

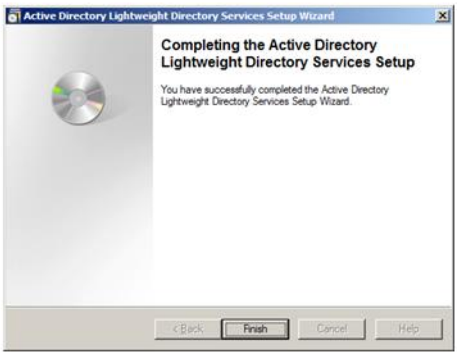
Install a unique instance of AD LDS.

Instance name: instance1
Computers will connect to this instance of AD LDS using the following ports:
LDAP port: 389
SSL port: 636

AD LDS replication will use Negotiate authentication.

Store AD LDS data files in the following location:

To change your selections, click Back. To install AD LDS, click Next.



Active Directory Lightweight Directory Services Setup Wizard

Completing the Active Directory Lightweight Directory Services Setup

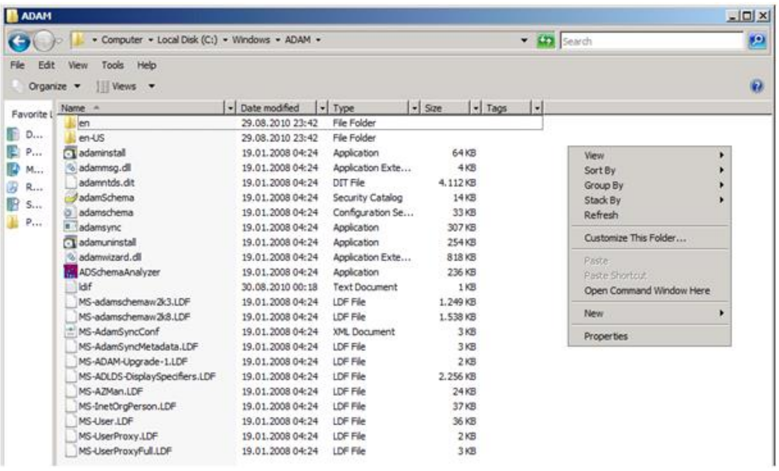
You have successfully completed the Active Directory Lightweight Directory Services Setup Wizard.

Importing an AD LDS schema

To import the AD LDS schema:

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

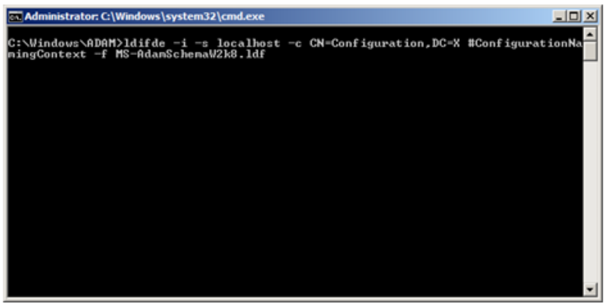
2. Select [`Shift key + right mouse click`] in the context menu: **`Open input request here`**.



Name	Date modified	Type	Size	Tags
en	29.08.2010 23:42	File Folder		
en-US	29.08.2010 23:42	File Folder		
adaminstall	19.01.2008 04:24	Application	64 KB	
adammsg.dll	19.01.2008 04:24	Application Exte...	4 KB	
adamntds.dit	19.01.2008 04:24	DIT File	4.112 KB	
adamSchema	19.01.2008 04:24	Security Catalog	14 KB	
adamschema	19.01.2008 04:24	Configuration Se...	33 KB	
adamsync	19.01.2008 04:24	Application	307 KB	
adamuninstall	19.01.2008 04:24	Application	254 KB	
adamwizard.dll	19.01.2008 04:24	Application Exte...	818 KB	
ADSchemaAnalyzer	19.01.2008 04:24	Application	236 KB	
ldif	30.08.2010 00:18	Text Document	1 KB	
MS-adamschemaw2k3.LDF	19.01.2008 04:24	LDF File	1.249 KB	
MS-adamschemaw2k8.LDF	19.01.2008 04:24	LDF File	1.538 KB	
MS-AdamSyncConf	19.01.2008 04:24	XML Document	3 KB	
MS-AdamSyncMetadata.LDF	19.01.2008 04:24	LDF File	3 KB	
MS-ADAM-Upgrade-1.LDF	19.01.2008 04:24	LDF File	2 KB	
MS-ADLDS-DisplaySpecifiers.LDF	19.01.2008 04:24	LDF File	2.256 KB	
MS-AZMan.LDF	19.01.2008 04:24	LDF File	24 KB	
MS-InetOrgPerson.LDF	19.01.2008 04:24	LDF File	37 KB	
MS-User.LDF	19.01.2008 04:24	LDF File	36 KB	
MS-UserProxy.LDF	19.01.2008 04:24	LDF File	2 KB	
MS-UserProxyFull.LDF	19.01.2008 04:24	LDF File	3 KB	

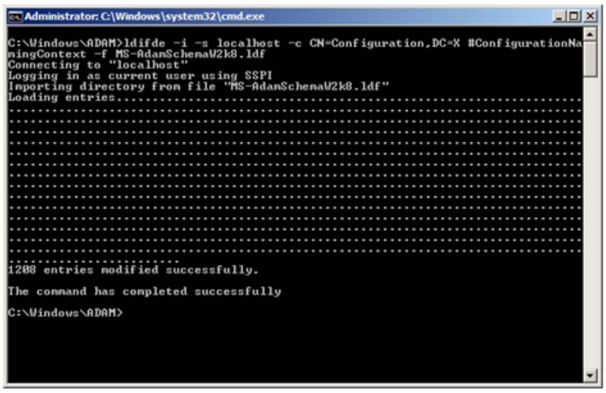
3. Enter the following character string:

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



```
C:\Windows\ADAM>ldifde -i -s localhost -c CN=Configuration,DC=X #ConfigurationNa
mingContext -f MS-AdamSchemaW2k8.ldf
```

4. Press the Return key:

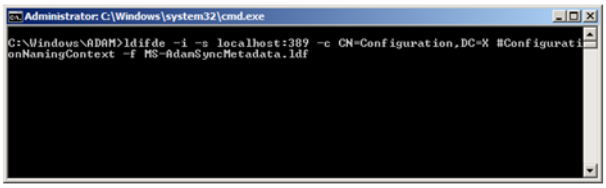


```
C:\Windows\ADAM>ldifde -i -s localhost -c CN=Configuration,DC=X #ConfigurationNa
mingContext -f MS-AdamSchemaW2k8.ldf
Connecting to "localhost"
Logging in as current user using SSPI
Importing directory from file "MS-AdamSchemaW2k8.ldf"
Loading entries.................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
........................
1208 entries modified successfully.

The command has completed successfully

C:\Windows\ADAM>
```

5. Enter the following character string:

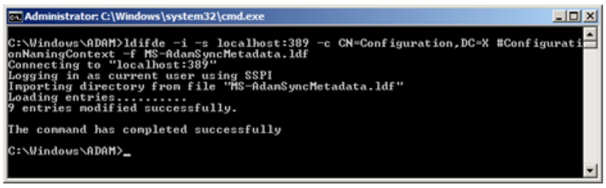
```
ldifde -i -s localhost:389 -c CN=Configuration,DC=X #ConfigurationNamingContext -f
MS-AdamSyncMetadata.ldf
```

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



```
C:\Windows\ADAM>ldifde -i -s localhost:389 -c CN=Configuration,DC=X #Configurati
onNamingContext -f MS-AdamSyncMetadata.ldf
```

6. Press the Return key:

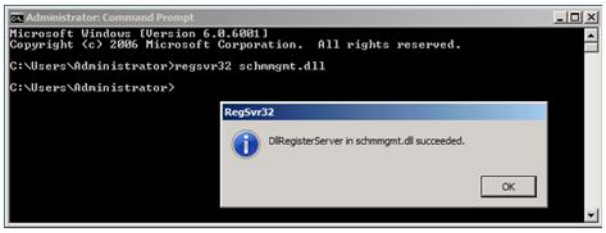


```
C:\Windows\ADAM>ldifde -i -s localhost:389 -c CN=Configuration,DC=X #Configurati
onNamingContext -f MS-AdamSyncMetadata.ldf
Connecting to "localhost:389"
Logging in as current user using SSPI
Importing directory from file "MS-AdamSyncMetadata.ldf"
Loading entries..........
9 entries modified successfully.

The command has completed successfully

C:\Windows\ADAM>_
```

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

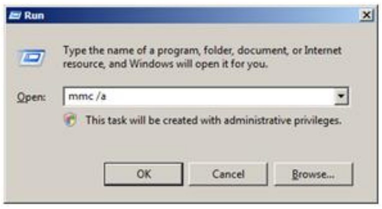


```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>regsvr32 schmmgmt.dll

C:\Users\Administrator>
```

DllRegisterServer in schmmgmt.dll succeeded.

CONFIGURATION

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

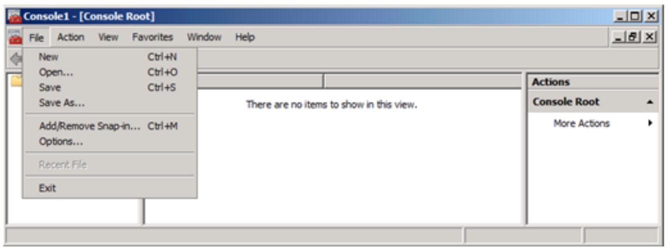


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc /a

This task will be created with administrative privileges.

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

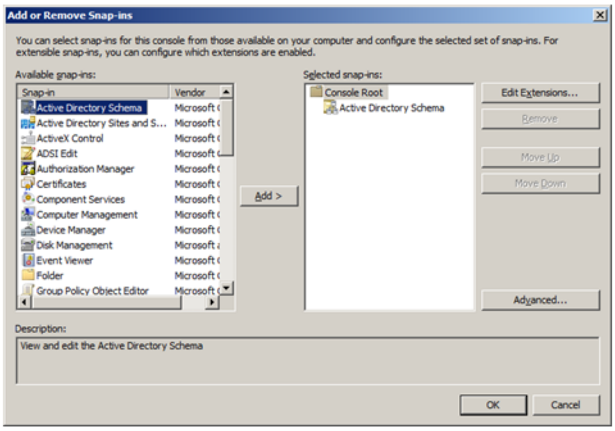


There are no items to show in this view.

5. Select **Active Directory Schema**

6. Click on **Add**

7. click on **OK**



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Schema	Microsoft
Active Directory Sites and S...	Microsoft
ActiveX Control	Microsoft
ADSI Edit	Microsoft
Authorization Manager	Microsoft
Certificates	Microsoft
Component Services	Microsoft
Computer Management	Microsoft
Device Manager	Microsoft
Disk Management	Microsoft
Event Viewer	Microsoft
Folder	Microsoft
Group Policy Object Editor	Microsoft

Selected snap-ins:

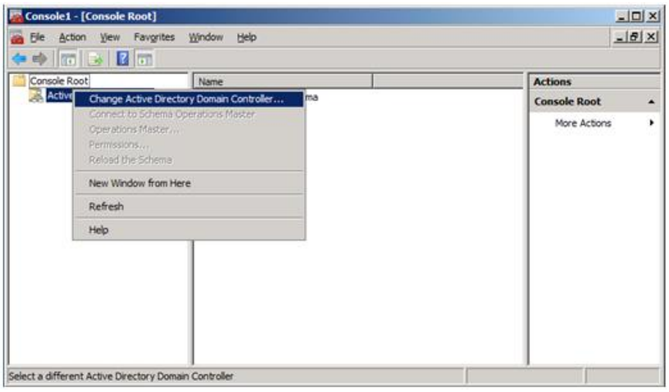
Console Root
Active Directory Schema

Description:

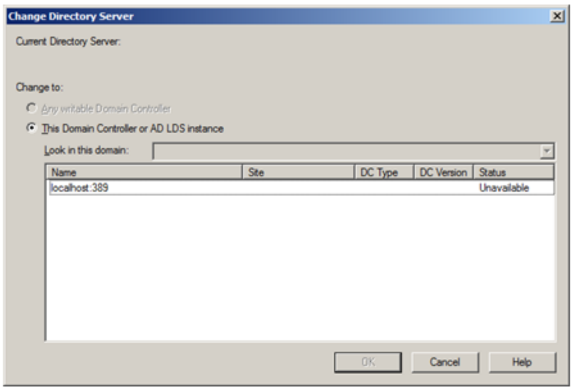
View and edit the Active Directory Schema

8. Navigate to **Active Directory Schema**

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


Console1 - [Console Root]
File Action View Favorites Window Help
Console Root
Active
Name
Change Active Directory Domain Controller...
Connect to Schema Operations Master
Operations Master...
Permissions...
Reload the Schema
New Window from Here
Refresh
Help
Actions
Console Root
More Actions
Select a different Active Directory Domain Controller

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



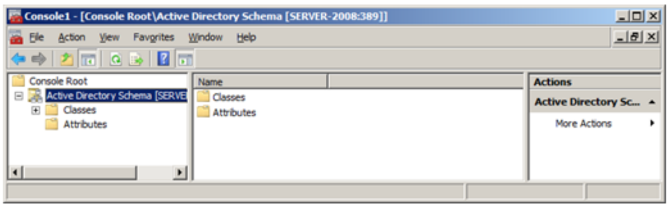
○ Any writable Domain Controller

● This Domain Controller or AD LDS instance

Look in this domain:

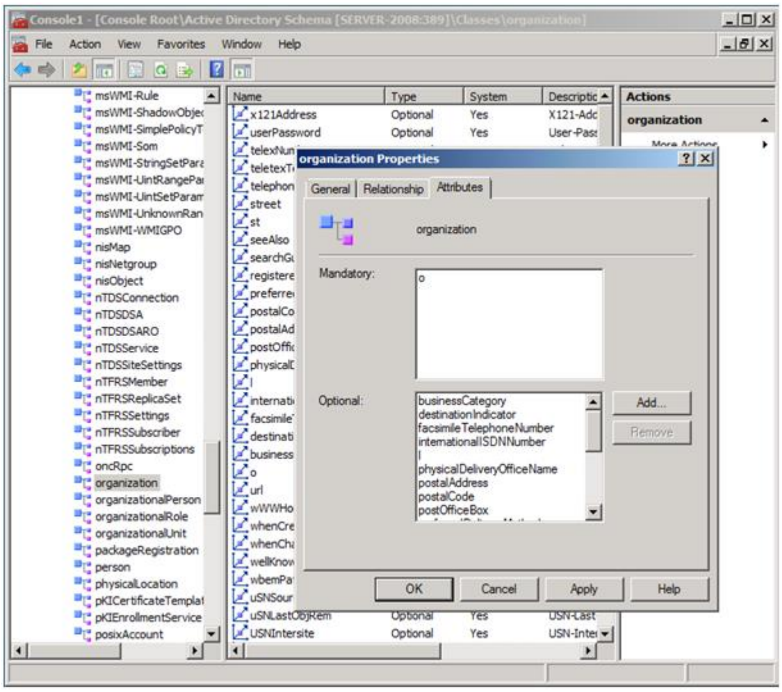
Name	Site	DC Type	DC Version	Status
localhost:389				Unavailable

11. You should now see this window:


Console1 - [Console Root\Active Directory Schema [SERVER-2008:389]]
File Action View Favorites Window Help
Console Root
Active Directory Schema [SERVE
Classes
Attributes
Name
Classes
Attributes
Actions
Active Directory Sc...
More Actions

12. Navigate to *Classes -> organization*

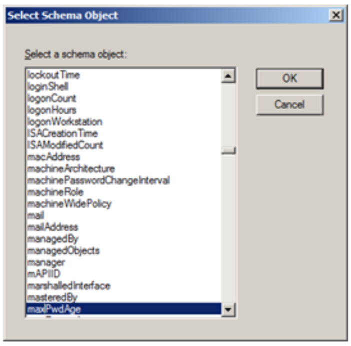
13. Open **`Properties`**



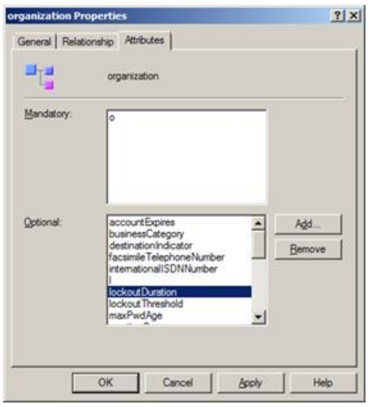
14. Click on **`Add`**

a) Search for `maxPwdAge`

b) click on **`OK`**



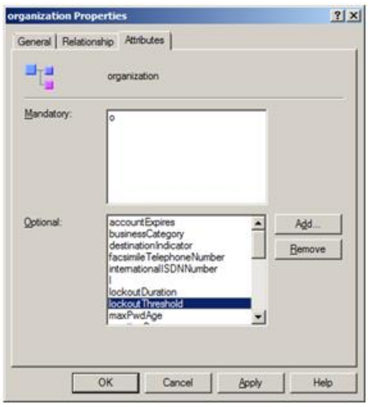
c) Repeat this step for `lockoutDuration`



Mandatory: o

Optional:
accountExpires
businessCategory
destinationIndicator
facsimileTelephoneNumber
internationalISDNNumber
l
lockoutDuration
lockoutThreshold
maxPwdAge

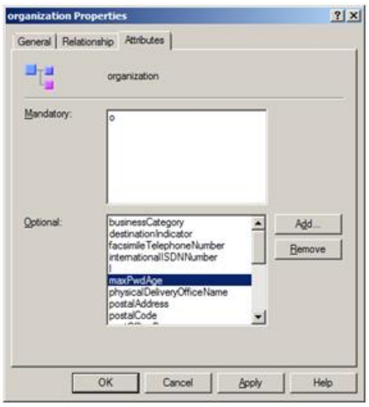
d) and for `lockoutThreshold`



Mandatory: o

Optional:
accountExpires
businessCategory
destinationIndicator
facsimileTelephoneNumber
internationalISDNNumber
l
lockoutDuration
lockoutThreshold
maxPwdAge

15. click on **OK**



Mandatory: o

Optional:
businessCategory
destinationIndicator
facsimileTelephoneNumber
internationalISDNNumber
l
maxPwdAge
physicalDeliveryOfficeName
postalAddress
postalCode

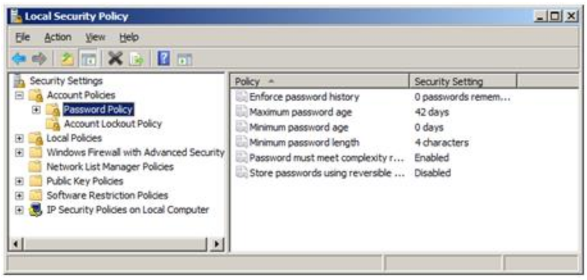
These steps are absolutely necessary to have `maxPwdAge` available in the organization unit, which is configured next.

- `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`

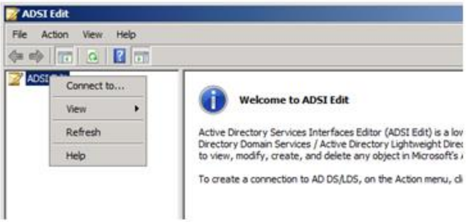


Policy	Security Setting
Enforce password history	0 passwords remem...
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	4 characters
Password must meet complexity r...	Enabled
Store passwords using reversible ...	Disabled

Configure organization units, groups and users

To configure organization units, groups and users:

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



Welcome to ADSI Edit

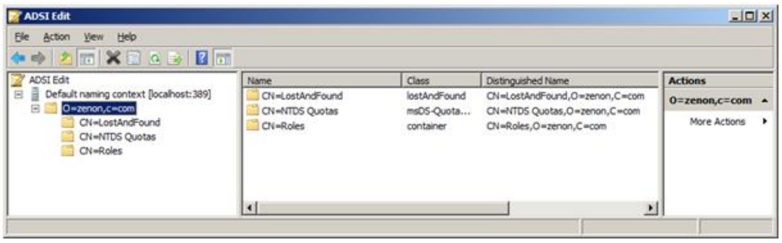
Active Directory Services Interfaces Editor (ADSI Edit) is a low
Directory Domain Services / Active Directory Lightweight Direc
to view, modify, create, and delete any object in Microsoft's
To create a connection to AD DS/LDS, on the Action menu, cl

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`

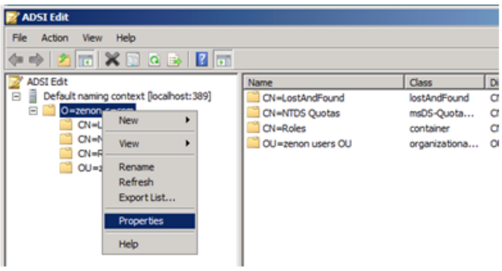
You should now see the following configuration:



Name	Class	Distinguished Name
CN=LostAndFound	lostAndFound	CN=LostAndFound,O=zenon,C=com
CN=NTDS Quotas	msDS-Quota...	CN=NTDS Quotas,O=zenon,C=com
CN=Roles	container	CN=Roles,O=zenon,C=com

CONFIGURING MAXPWDAGE

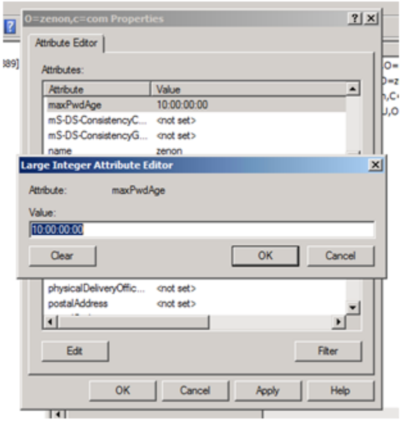
1. Highlight `O=zenon,c=com`
2. Click on **`Refresh`**
3. Close **`ADSI Edit`**
4. Open **`ADSI Edit`** again
5. Highlight `O=zenon,c=com`
6. Select **`Properties`** in the context menu.



Name	Class	Di
CN=LostAndFound	lostAndFound	CI
CN=NTDS Quotas	msDS-Quota...	CI
CN=Roles	container	CI
OU=zenon users OU	organizationa...	OI

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

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



O=zenon,c=com Properties

Attribute Editor

Attributes:

Attribute	Value
maxPwdAge	10:00:00:00
mS-DS-ConsistencyC...	<not set>
mS-DS-ConsistencyG...	<not set>
name	zenon
physicalDeliveryOffic...	<not set>
postalAddress	<not set>

Large Integer Attribute Editor

Attribute: maxPwdAge

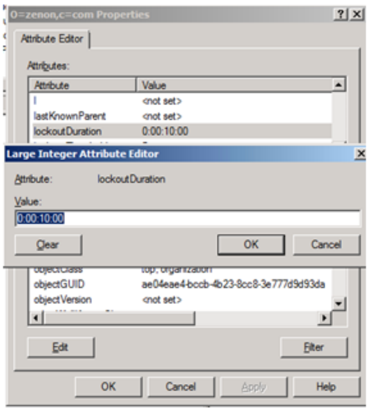
Value: 10:00:00:00

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)



O=zenon,c=com Properties

Attribute Editor

Attributes:

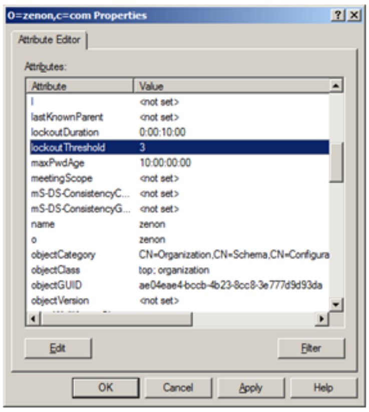
Attribute	Value
l	<not set>
lastKnownParent	<not set>
lockoutDuration	0:00:10:00
objectClass	top; organization
objectGUID	ae04eae4-bccb-4b23-8cc8-3e777d9d93da
objectVersion	<not set>

Large Integer Attribute Editor

Attribute: lockoutDuration

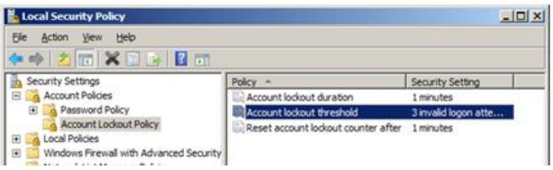
Value: 0:00:10:00

9. Navigate to `lockoutThreshold`



Attribute	Value
l	<not set>
lastKnownParent	<not set>
lockoutDuration	0:00:10:00
lockoutThreshold	3
maxPwdAge	10:00:00:00
meetingScope	<not set>
mS-DS-ConsistencyC...	<not set>
mS-DS-ConsistencyG...	<not set>
name	zenon
o	zenon
objectCategory	CN=Organization,CN=Schema,CN=Configura
objectClass	top; organization
objectGUID	ae04eae4-bccb-4b23-8cc8-3e777d9d93da
objectVersion	<not set>

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



Policy	Security Setting
Account lockout duration	1 minutes
Account lockout threshold	3 invalid logon atte...
Reset account lockout counter after	1 minutes

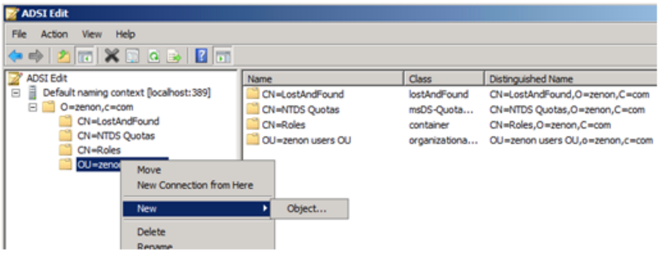
Note: The settings for the duration of the account block are ignored in AD LDS. The `lockoutDuration` property (`O=zenon,c=com`) is used.

Users

To create a user:

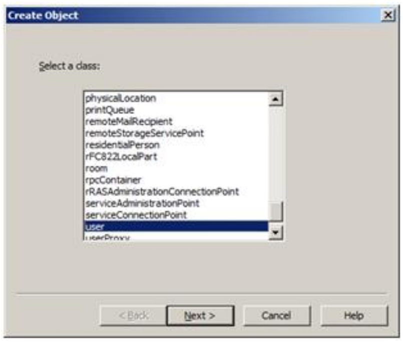
1. Highlight the organization unit

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

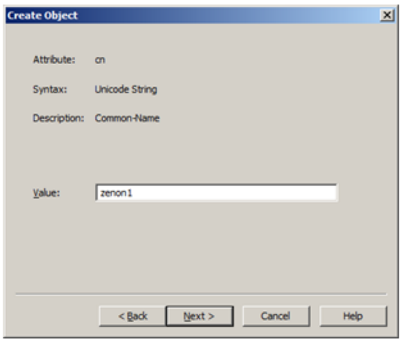


Name	Class	Distinguished Name
CN=LostAndFound	lostAndFound	CN=LostAndFound,O=zenon,C=com
CN=NTDS Quotas	msDS-Quota...	CN=NTDS Quotas,O=zenon,C=com
CN=Roles	container	CN=Roles,O=zenon,C=com
OU=zenon users OU	organizationa...	OU=zenon users OU,o=zenon,c=com

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



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



Attribute: cn

Syntax: Unicode String

Description: Common-Name

Value: zenon1

5. Click on **`Next`**

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

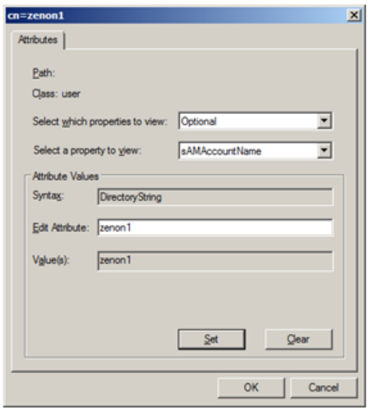
7. Click on **`More attributes`**

   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.)


cn=zenon1

Attributes

Path:

Class: user

Select which properties to view: Optional

Select a property to view: sAMAccountName

Attribute Values

Syntax: DirectoryString

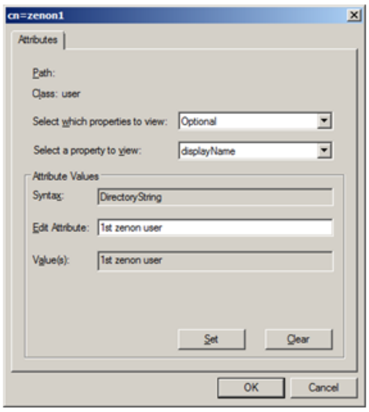
Edit Attribute: zenon1

Value(s): zenon1

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`**


cn=zenon1

Attributes

Path:

Class: user

Select which properties to view: Optional

Select a property to view: displayName

Attribute Values

Syntax: DirectoryString

Edit Attribute: 1st zenon user

Value(s): 1st zenon user

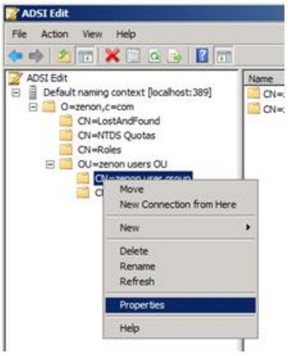
11. Click on **`Set`**, then on **`OK`** and on **`Finish`**

ADDING A USER TO THE GROUP

To add users to a group:

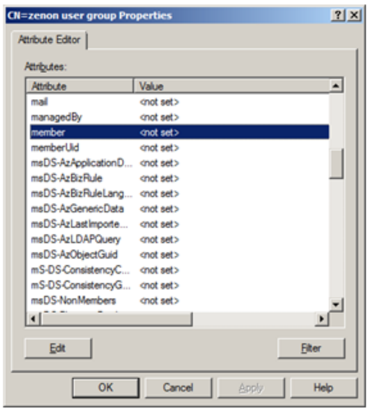
1. Select **`zenon user group`**

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



3. Highlight **member**

4. Click on **Edit**


CN=zenon user group Properties

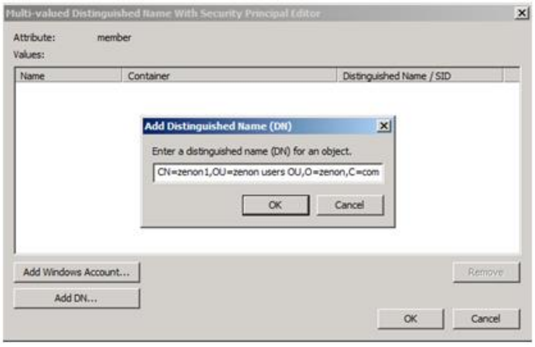
Attributes:

Attribute	Value
mail	<not set>
managedBy	<not set>
member	<not set>
memberUid	<not set>
msDS-AzApplicationD...	<not set>
msDS-AzBizRule	<not set>
msDS-AzBizRuleLang...	<not set>
msDS-AzGenericData	<not set>
msDS-AzLastImporte...	<not set>
msDS-AzLDAPQuery	<not set>
msDS-AzObjectGuid	<not set>
mS-DS-ConsistencyC...	<not set>
mS-DS-ConsistencyG...	<not set>
msDS-NonMembers	<not set>

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`


Multi-valued Distinguished Name With Security Principal Editor

Attribute: member

Values:

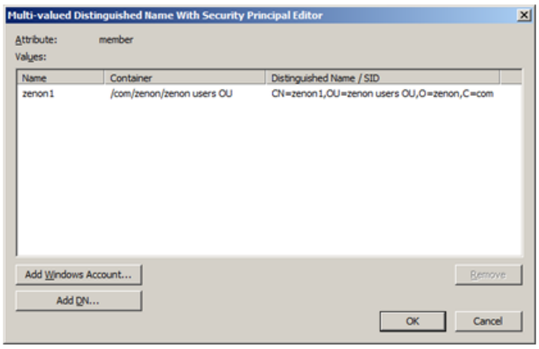
Name	Container	Distinguished Name / SID

Add Distinguished Name (DN)

Enter a distinguished name (DN) for an object.

CN=zenon1,OU=zenon users OU,O=zenon,C=com

c) You receive the result:



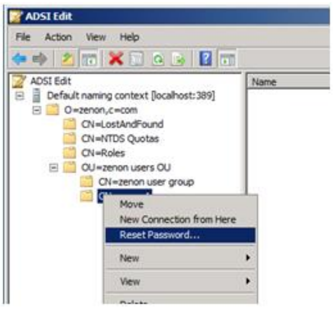
Multi-valued Distinguished Name With Security Principal Editor

Attribute: member

Values:

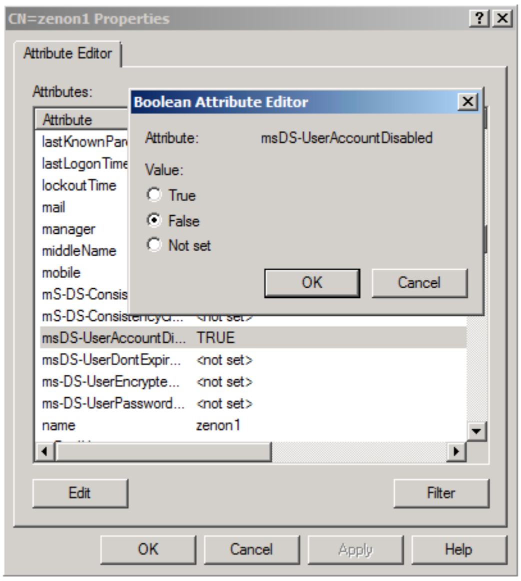
Name	Container	Distinguished Name / SID
zenon1	/com/zenon/zenon users OU	CN=zenon1,OU=zenon users OU,O=zenon,C=com

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



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

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



CN=zenon1 Properties

Attribute Editor

Attributes:

Attribute	
lastKnownPar	
lastLogonTime	
lockoutTime	
mail	
manager	
middleName	
mobile	
mS-DS-Consis	
mS-DS-ConsistencyG...	<not set>
msDS-UserAccountDi...	TRUE
msDS-UserDontExpir...	<not set>
ms-DS-UserEncrypte...	<not set>
ms-DS-UserPassword...	<not set>
name	zenon1

Boolean Attribute Editor

Attribute: msDS-UserAccountDisabled

Value:

○ True

● False

○ Not set

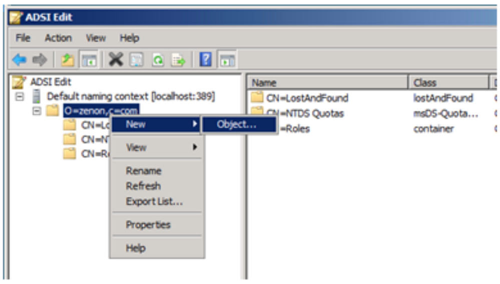
The user has now been created and can be used in zenon.

Organization units

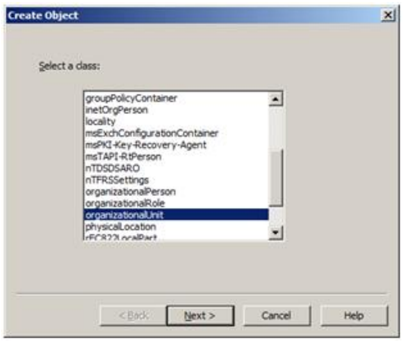
To create a organization unit:

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

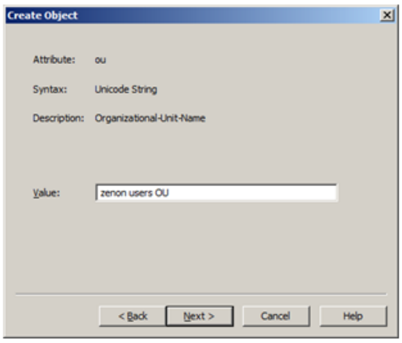
2. Select *New -> Object* in the context menu



3. Select **organizationalUnit**



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


Attribute: ou

Syntax: Unicode String

Description: Organizational-Unit-Name

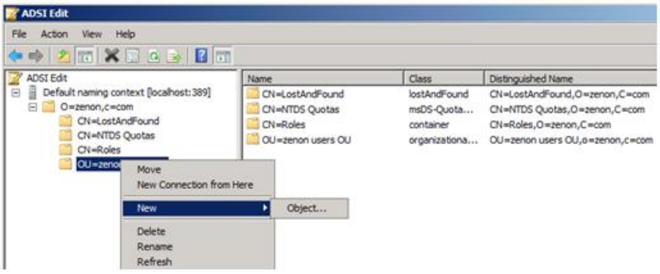
Value: zenon users OU

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

Groups

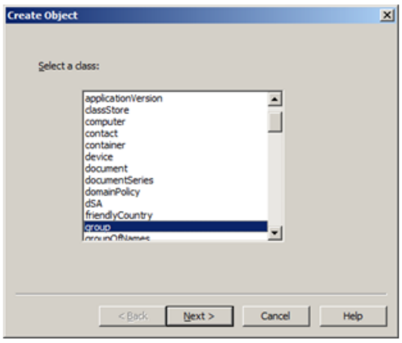
To create a group:

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

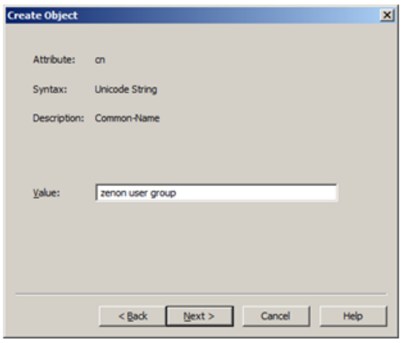


Name	Class	Distinguished Name
CN=LostAndFound	lostAndFound	CN=LostAndFound,O=zenon,C=com
CN=NTDS Quotas	msDS-Quota...	CN=NTDS Quotas,O=zenon,C=com
CN=Roles	container	CN=Roles,O=zenon,C=com
OU=zenon users OU	organizationa...	OU=zenon users OU,o=zenon,c=com

3. Select **`group`**



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



Attribute: cn

Syntax: Unicode String

Description: Common-Name

Value: zenon user group

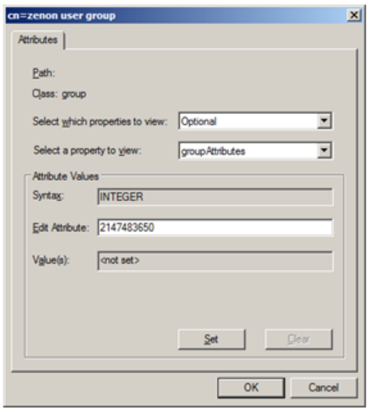
5. Click on **`Next`**
6. Switch to the **`Attributes`** tab
7. Click on **`More attributes`**

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`**)



Path:

Class: group

Select which properties to view: Optional

Select a property to view: groupAttributes

Attribute Values

Syntax: INTEGER

Edit Attribute: 2147483650

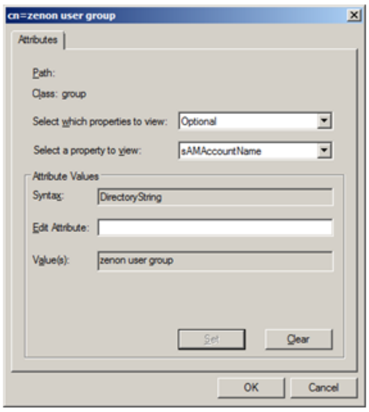
Value(s): <not set>

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



Path:

Class: group

Select which properties to view: Optional

Select a property to view: sAMAccountName

Attribute Values

Syntax: DirectoryString

Edit Attribute:

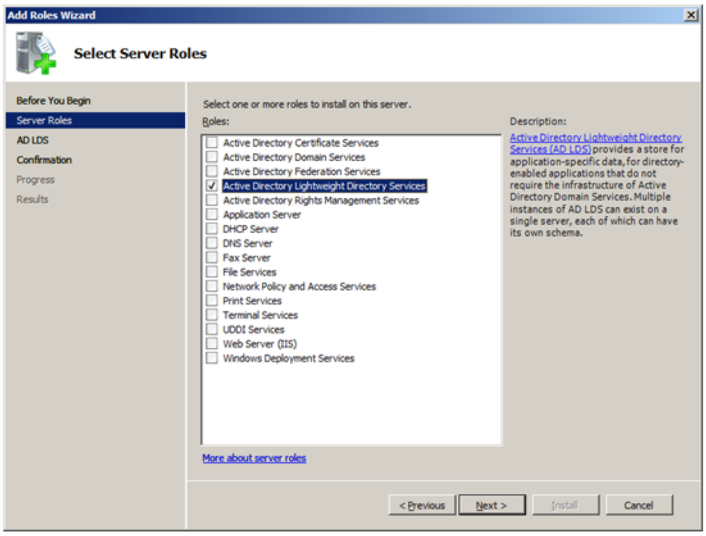
Value(s): zenon user group

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



Select Server Roles

Select one or more roles to install on this server.

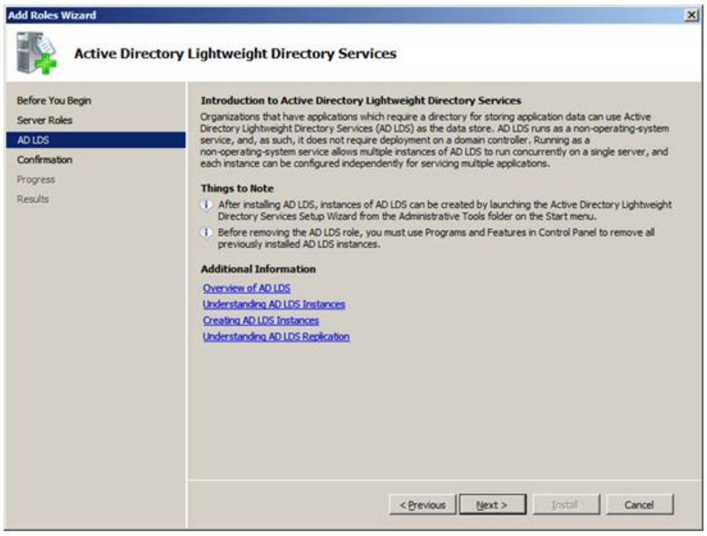
Roles:

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- ☑ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- □ File Services
- □ Network Policy and Access Services
- □ Print Services
- □ Terminal Services
- □ UDDI Services
- □ Web Server (IIS)
- □ Windows Deployment Services

Description:

Active Directory Lightweight Directory Services (AD LDS) provides a store for application-specific data, for directory-enabled applications that do not require the infrastructure of Active Directory Domain Services. Multiple instances of AD LDS can exist on a single server, each of which can have its own schema.

2. Click on **Add Roles**



Active Directory Lightweight Directory Services

Introduction to Active Directory Lightweight Directory Services

Organizations that have applications which require a directory for storing application data can use Active Directory Lightweight Directory Services (AD LDS) as the data store. AD LDS runs as a non-operating-system service, and, as such, it does not require deployment on a domain controller. Running as a non-operating-system service allows multiple instances of AD LDS to run concurrently on a single server, and each instance can be configured independently for servicing multiple applications.

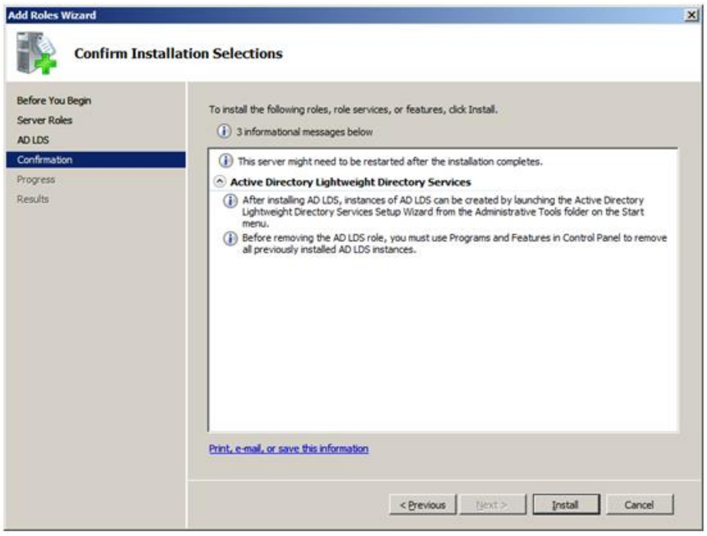
Things to Note

- After installing AD LDS, instances of AD LDS can be created by launching the Active Directory Lightweight Directory Services Setup Wizard from the Administrative Tools folder on the Start menu.
- Before removing the AD LDS role, you must use Programs and Features in Control Panel to remove all previously installed AD LDS instances.

Additional Information

Overview of AD LDS
Understanding AD LDS Instances
Creating AD LDS Instances
Understanding AD LDS Replication

3. Add the **`AD LDS Role`**



To install the following roles, role services, or features, click Install.

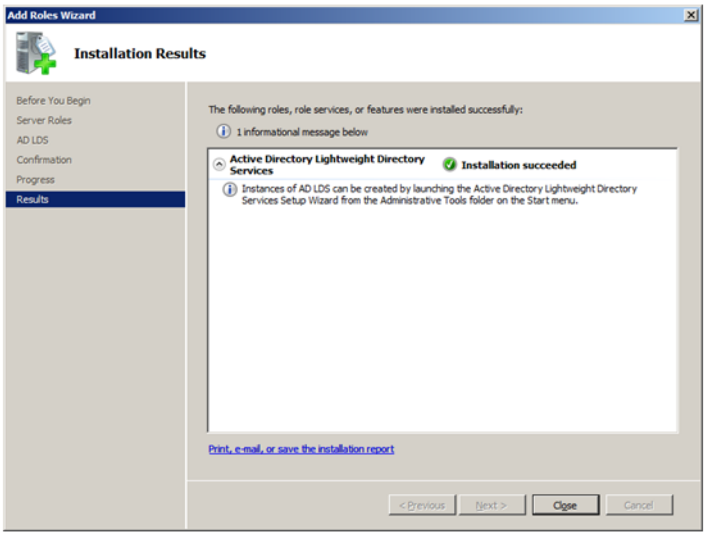
3 informational messages below

This server might need to be restarted after the installation completes.

Active Directory Lightweight Directory Services

After installing AD LDS, instances of AD LDS can be created by launching the Active Directory Lightweight Directory Services Setup Wizard from the Administrative Tools folder on the Start menu.

Before removing the AD LDS role, you must use Programs and Features in Control Panel to remove all previously installed AD LDS instances.



The following roles, role services, or features were installed successfully:

1 informational message below

Active Directory Lightweight Directory Services — Installation succeeded

Instances of AD LDS can be created by launching the Active Directory Lightweight Directory Services Setup Wizard from the Administrative Tools folder on the Start menu.

6.2.4 zenon administration with Active Directory

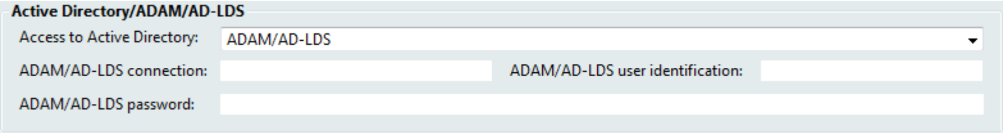
For use in zenon, first configure the settings in the Editor (on page 146) and then set the user identification at AD LDS level to Runtime (on page 147).

Information

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

Editor

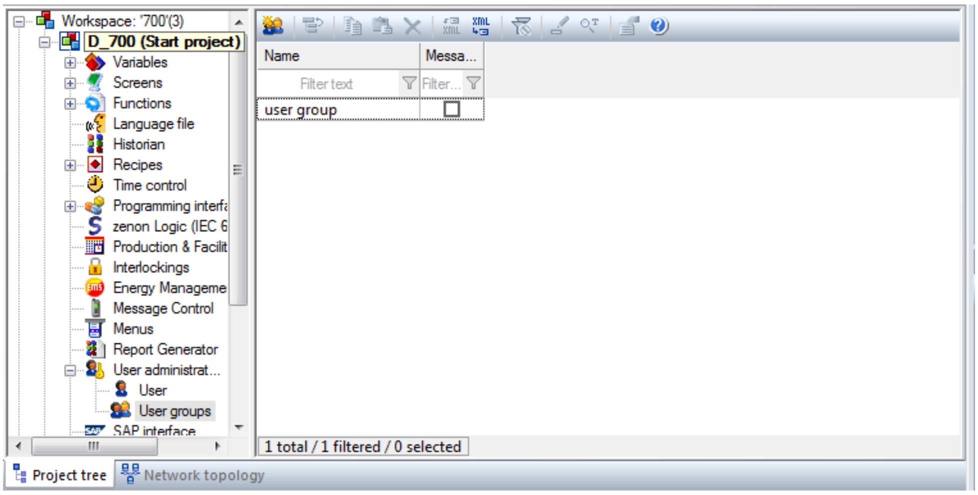
Configuration is carried out in the project properties in `User administration`:



Active Directory/ADAM/AD-LDS

Access to Active Directory:	ADAM/AD-LDS		
ADAM/AD-LDS connection:		ADAM/AD-LDS user identification:	
ADAM/AD-LDS password:			

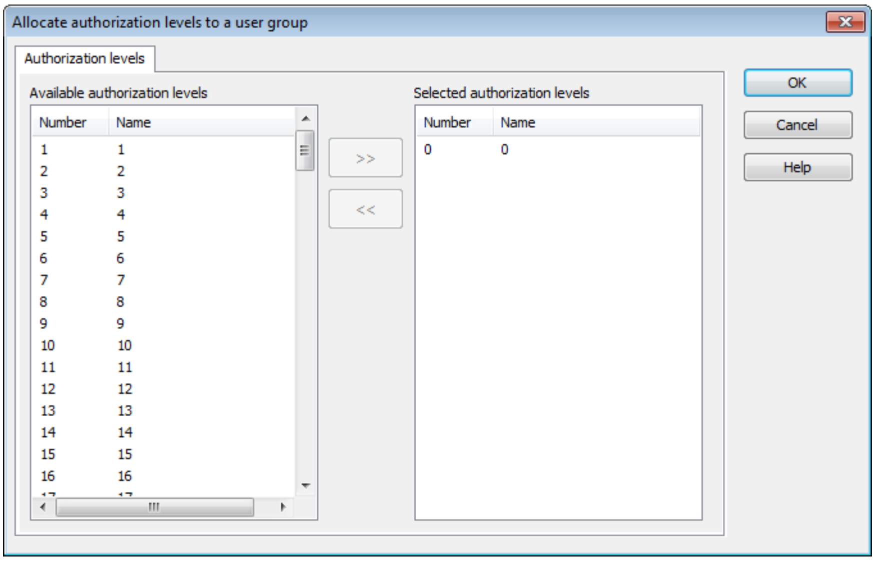
- A user group with the name `zenon user group` was created



Name	Messa...
Filter text	Filter...
user group	□

1 total / 1 filtered / 0 selected

- and authorization levels were added



Allocate authorization levels to a user group

Authorization levels

Available authorization levels

Number	Name
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	10
11	11
12	12
13	13
14	14
15	15
16	16

Selected authorization levels

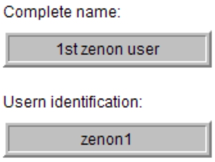
Number	Name
0	0

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`.

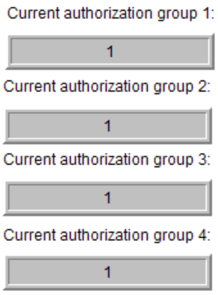
The `User identification` property corresponds to the AD LDS attribute `sAMAccountName`.



Complete name: 1st zenon user

Usern identification: zenon1

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



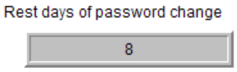
Current authorization group 1: 1

Current authorization group 2: 1

Current authorization group 3: 1

Current authorization group 4: 1

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



Rest days of password change

8

TROUBLESHOOTING

If errors in Runtime occur, check if:

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

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

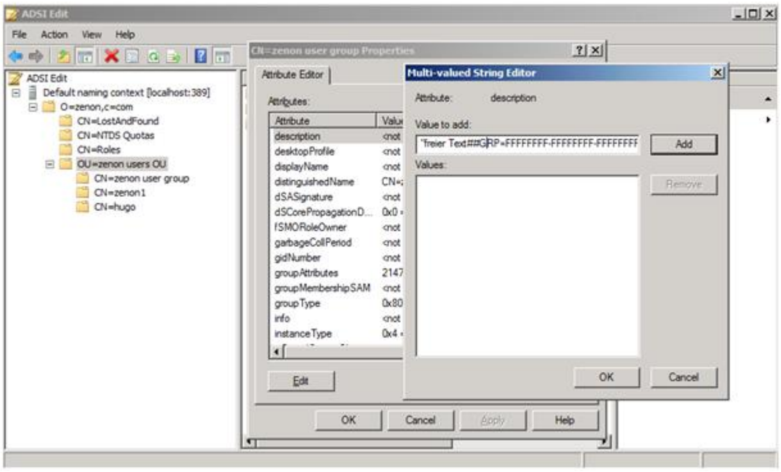
- The names correspond to each other
- sAMAccountName of the group in **AD LDS** was set
- The user in AD **LDS** was added to the group

AD/ADAM

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

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

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



ADSI Edit
- Default naming context [localhost:389]
  - O=zenon,c=com
    - CN=LostAndFound
    - CN=NTDS Quotas
    - CN=Roles
    - OU=zenon users OU
      - CN=zenon user group
      - CN=zenon1
      - CN=hugo

Attributes:

Attribute	Valu
description	<not
desktopProfile	<not
displayName	<not
distinguishedName	CN=:
dSASignature	<not
dSCorePropagationD...	0x0
fSMORoleOwner	<not
garbageCollPeriod	<not
gidNumber	<not
groupAttributes	2147
groupMembershipSAM	<not
groupType	0x80
info	<not
instanceType	0x4

Attribute: description

Value to add: "freier Text##GRP=FFFFFFFF-FFFFFFFF-FFFFFFFF

Values:

For further information, see the Setting the zenon authorization levels in the description field of an Active Directory group (on page 73) 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

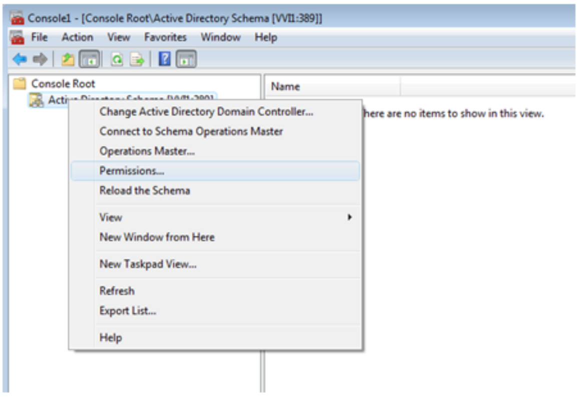
THE USER DOES NOT RECEIVE ALL AUTHORIZATION LEVELS THAT WERE ASSIGNED TO THEM.

- 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

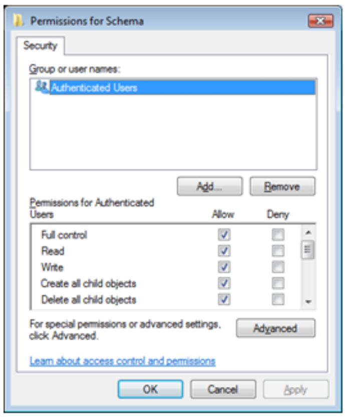
If no content is displayed after the Active Directory schema is opened, the access rights must be amended. To do this:

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



here are no items to show in this view.

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



Group or user names:

Authenticated Users

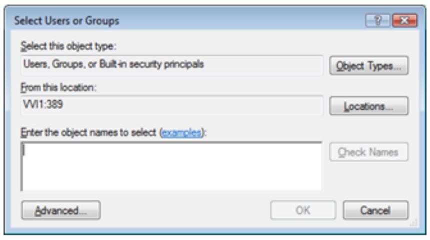
Permissions for Authenticated Users

Permissions for Authenticated Users	Allow	Deny
Full control	☑	□
Read	☑	□
Write	☑	□
Create all child objects	☑	□
Delete all child objects	☑	□

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

3. Click on the **Advanced** button



Select this object type:

Users, Groups, or Built-in security principals

From this location:

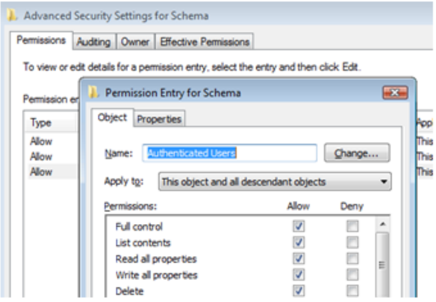
VVI1:389

Enter the object names to select (examples):

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



To view or edit details for a permission entry, select the entry and then click Edit.

Name: Authenticated Users

Apply to: This object and all descendant objects

Permissions:	Allow	Deny
Full control	☑	□
List contents	☑	□
Read all properties	☑	□
Write all properties	☑	□
Delete	☑	□

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 85):

- Windows Vista
- 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 153)
2. Bring in an AD schema (on page 156)
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 156) 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 71).
- You can create the zenon authorization levels as described in Using the Active Directory (on page 71) under attribute`description`.

> **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.

> **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:

```
ldifde -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.