zenon Handbuch

Benutzerverwaltung

v.7.00

© 2012 Ing. Punzenberger COPA-DATA GmbH

Alle Rechte vorbehalten.

Die Weitergabe und Vervielfältigung dieses Dokuments ist - gleich in welcher Art und Weise – nur mit schriftlicher Genehmigung der Firma COPA-DATA gestattet. Technische Daten dienen nur der Produktbeschreibung und sind keine zugesicherten Eigenschaften im Rechtssinn. Änderungen – auch in technischer Hinsicht - vorbehalten.

Inhalt

1. Willkommen bei der COPA-DATA Hilfe 5

2. Benutzerverwaltung 5

3. Projektieren im Editor 8

3.1 Benutzerverwaltung Detailansicht Symbolleiste und Kontextmenü 8

3.2 Anlegen eines Benutzers 10

3.2.1 Benutzer 11

3.2.2 Passwort ändern 13

3.2.3 Message Control 14

3.2.4 Berechtigungsebenen 16

3.2.5 Benutzergruppen 17

3.3 Anlegen einer Benutzergruppe 18

3.3.1 Benutzergruppe benennen 20

3.3.2 Berechtigungsebenen 21

3.3.3 Reihenfolge in Message Control 23

3.4 Ändern eines Benutzers 23

3.5 Änderung einer Benutzergruppe 24

3.6 Namensänderung der Berechtigungsebenen 25

3.7 Funktionsberechtigungen 25

3.8 Bild vom Typ Login anlegen 28

4. Active Directory (AD) 29

4.1 Allgemeines 30

4.2 Gleiche Benutzergruppen in zenon und im Active Directory 30

4.3 Setzen der zenon Berechtigungsebenen im Beschreibungsfeld einer Active Directory Gruppe 31

4.4 Schema-Erweiterung des Active Directory 32

4.4.1 Installieren der Schema Erweiterung 33

4.4.2 Zuweisen von Benutzerrechten 34

4.4.3 Schema Erweiterung - Details 38

5. Active Directory Lightweight Directory Services - AD LDS (ab Windows Vista) 43

5.1 AD LDS unter Windows 2008 43

5.2 Neue AD LDS Instanz erstellen ... 45
5.3 AD LDS Schema importieren ... 50
5.4 AD Schema Snap-in konfigurieren ... 52
5.5 Organisationseinheiten, Gruppen und Benutzer konfigurieren ... 57
5.5.1 Organisationseinheiten ... 60
5.5.2 Gruppen ... 61
5.5.3 Benutzer ... 63
5.6 Verwendung in zenon ... 68
5.6.1 Editor ... 68
5.6.2 Runtime - Systemtreibervariablen ... 69
5.7 AD LDS unter Windows 7 und Windows Vista ... 71
5.7.1 Problembehandlung unter Windows 7 und Windows Vista ... 71

6. Active Directory Application Mode - ADAM (für Windows XP) ... 73

6.1 Neue ADAM-Instanz erstellen ... 75
6.2 AD-Schema einspielen ... 78
6.3 ADAM-Schema Snap-in konfigurieren ... 79

7. Bedienen zur Runtime ... 80

7.1 Permanentes und temporäres Login ... 82
7.2 Passwortschutz im dynamischen Element ... 83
7.3 Passwort - Funktionen ... 84
7.3.1 Login mit Dialog ... 84
7.3.2 Login ohne Passwort ... 85
7.3.3 Logout ... 87
7.3.4 Passwort ändern ... 87
7.4 Löschen eines Benutzers ... 88
7.5 Bild vom Typ Login ... 88

1. Willkommen bei der COPA-DATA Hilfe

ALLGEMEINE HILFE

Falls Sie in diesem Hilfekapitel Informationen vermissen oder Wünsche für Ergänzungen haben, wenden Sie sich bitte per E-Mail an documentation@copadata.com (mailto:documentation@copadata.com).

PROJEKTUNTERSTÜTZUNG

Unterstützung bei Fragen zu konkreten eigenen Projekten erhalten Sie vom Support-Team, das Sie per E-Mail an support@copadata.com (mailto:support@copadata.com) erreichen.

LIZENZEN UND MODULE

Sollten Sie feststellen, dass Sie weitere Module oder Lizenzen benötigen, sind unsere Mitarbeiter unter sales@copadata.com (mailto:sales@copadata.com) gerne für Sie da.

2. Benutzerverwaltung

zenon sieht sowohl für den Editor als auch für den Onlinebetrieb (Runtime) eine Benutzerverwaltung vor. Das Passwortsystem erfüllt die Richtlinien der FDA (Food and Drug Administration, 21 CFR Part 11).

Lizenzinformation

In Standardlizenz für Editor und Runtime enthalten.

DAS KONZEPT

Das Passwortkonzept geht davon aus, dass unterschiedliche Anwender unterschiedliche Bedienrechte (Passwortebenen) besitzen. Auch Administratoren verfügen über unterschiedliche Berechtigungsebenen, haben aber zusätzliche verwaltungsbezogene Funktionen wie das Administrieren von Benutzern.

Im vorhandenen Passwortkonzept ist es möglich, jedem Benutzer mehrere selektive (einzeln definierte) Passwortebenen (Bedienrechte) zuzuweisen. Es sind maximal 128 (0-127, ab Version 6.20) Passwortebenen projektierbar. Die Zuordnung der Benutzer zu den einzelnen Passwortebenen und der damit verbundene Aufbau des projekt-spezifischen Passwortkonzeptes kann vollständig frei erfolgen. Jedem Benutzer können beliebige Ebenen zugewiesen werden. So kann z. B. der Benutzer 1 über die Ebenen 0, 1, 5, 6 verfügen und der Benutzer 2 über die Ebenen 0, 1, 6, 8, 10. Aber es können nur Berechtigungen vergeben werden, über die der Administrator selbst verfügt.

Das Anmelden des Benutzers im Onlinebetrieb erfolgt über die Aktivierung der Funktion Login (auf Seite 84) (Text Button, Bitmap Button etc.). Soll der Benutzer aufgrund eines Ereignisses automatisch angemeldet werden (z.B. Schlüsselschalterstellung als Meldung im System vorhanden), wird die Funktion Login ohne Passwort (auf Seite 85)verwendet. Die Funktion wird in einem Grenzwert bzw. in einer Rema der Variable in der Variablenverwaltung projektiert.

Das durch den Benutzer angeregte Abmelden im Onlinebetrieb erfolgt mit der Funktion Logout (auf Seite 87). Der neu am System angemeldete Benutzer ist SYSTEM.

Wird über einen projektierten Zeitraum lang keine neuerliche Bedienaktion vorgenommen, kann ein automatisches, zeitgesteuertes Abmelden erfolgen.

KONTEXTMENÜ PROJEKTMANAGER

KONTEXTMENU BENUTZERVERWALTUNG

Menüpunkt	Aktion
Editorprofile	Öffnet die Dropdownliste mit vordefinierten Editorprofilen.
Hilfe	Öffnet die Online-Hilfe

KONTEXTMENU BENUTZER

Menüpunkt	Aktion
Benutzer neu	Öffnet den Dialog zur Anlage eines neuen Benutzers und trägt diesen in die Liste der Detailansicht ein.
XML exportieren alle...	Exportiert alle Einträge in eine XML-Datei.
XML importieren	Importiert Einträge aus einer XML-Datei.
Editorprofil	Öffnet die Dropdownliste mit vordefinierten Editorprofilen.
Help	Öffnet die Online-Hilfe.

KONTEXTMENU BENUTZERGRUPPE

Menüpunkt	Aktion
Benutzergruppe neu	Öffnet den Dialog zur Anlage einer neuen Benutzergruppe und trägt diese in die Liste der Detailansicht ein.
XML exportieren alle...	Exportiert alle Einträge in eine XML-Datei.
XML importieren	Importiert Einträge aus einer XML-Datei.
Editorprofile	Öffnet die Dropdownliste mit vordefinierten Editorprofilen.
Help	Öffnet die Online-Hilfe.

Kontextmenü Detailansicht: siehe Benutzerverwaltung Detailansicht Symbolleiste und Kontextmenü (auf Seite 8)

3. Projektieren im Editor

Info

Wenn Sie den default-Wert für die maximale Passwortfehleingabe unter 'Projekteigenschaften -> Benutzerverwaltung -> Max. Passwortfehleing.' ändern, ist zu beachten, dass diese Änderung nur bei einem Neustart der Runtime aktiv wird. Die Funktion 'Nachladen' der Runtime übernimmt diese Änderung nicht, da sonst beliebig viele Versuche zur Passworteingabe möglich wären.

3.1 Benutzerverwaltung Detailansicht Symbolleiste und Kontextmenü

Menüpunkt/Symbol	Aktion
Benutzer neu	Öffnet den Dialog zur Anlage eines neuen Benutzers und trägt diesen in die Liste der Detailansicht ein.
Zurück zu Ausgangselement springen	Ist man über die Funktion **verknüpfte Elemente** in die Liste gelangt, führt das Symbol zurück zum Ausgangselement. Im Kontextmenü nur vorhanden, wenn als verknüpftes Element geöffnet.
Kopieren	Kopiert ausgewählte Einträge in die Zwischenablage.
Einfügen	Fügt den Inhalt der Zwischenablage ein. Ist bereits ein Eintrag mit gleichem Namen vorhanden, wird der Inhalt als "Kopie von" eingefügt.
Löschen	Löscht ausgewählte Einträge.
Selektierte XML exportieren..	Exportiert alle ausgewählten Einträge in eine XML-Datei.
XML importieren	Importiert Einträge aus einer XML-Datei.
Selektierte Zelle bearbeiten	Öffnet die ausgewählte Zelle zur Bearbeitung. Welche Zelle in einer markierten Zeile ausgewählt wurde, sehen Sie am Fernglas-Symbol in der Titelzeile.
Text in selektierter Spalte ersetzen	Öffnet Dialog zum Suchen und Ersetzen von Texten.
ALLE FILTER ENTFERNEN	Entfernt alle Filtereinstellungen.
XML importieren	Importiert aus XML-Datei.
Eigenschaften	Öffnet das Fenster **Eigenschaften** für den gewählten Eintrag.
Hilfe	Öffnet die Online-Hilfe.

KONTEXTMENU BENUTZERGRUPPE

Menüpunkt	Aktion
Benutzergruppe neu	Öffnet den Dialog zur Anlage einer neuen Benutzergruppe und trägt diese in die Liste der Detailansicht ein.
Kopieren	Kopiert ausgewählte Einträge in die Zwischenablage.
Einfügen	Fügt den Inhalt der Zwischenablage ein. Ist bereits ein Eintrag mit gleichem Namen vorhanden, wird der Inhalt als "Kopie von" eingefügt.

Löschen	Löscht ausgewählte Einträge.
XML exportieren alle...	Exportiert alle Einträge in eine XML-Datei.
XML importieren	Importiert Einträge aus einer XML-Datei.
Selektierte Zelle bearbeiten	Öffnet die ausgewählte Zelle zur Bearbeitung. Welche Zelle in einer markierten Zeile ausgewählt wurde, sehen Sie am Fernglas-Symbol in der Titelzeile.
Text in selektierter Spalte ersetzen	Öffnet Dialog zum Suchen und Ersetzen von Texten.
Eigenschaften	Öffnet das Fenster **Eigenschaften** für den gewählten Eintrag.
Selektierte XML exportieren	Exportiert ausgewählte Einträge in XML-Datei.
XML importieren	Importiert aus XML-Datei.
Alle Filter entfernen	Entfernt alle Filtereinstellungen.
Help	Öffnet die Online-Hilfe.

3.2 Anlegen eines Benutzers

Um einen neuen Benutzer anzulegen:

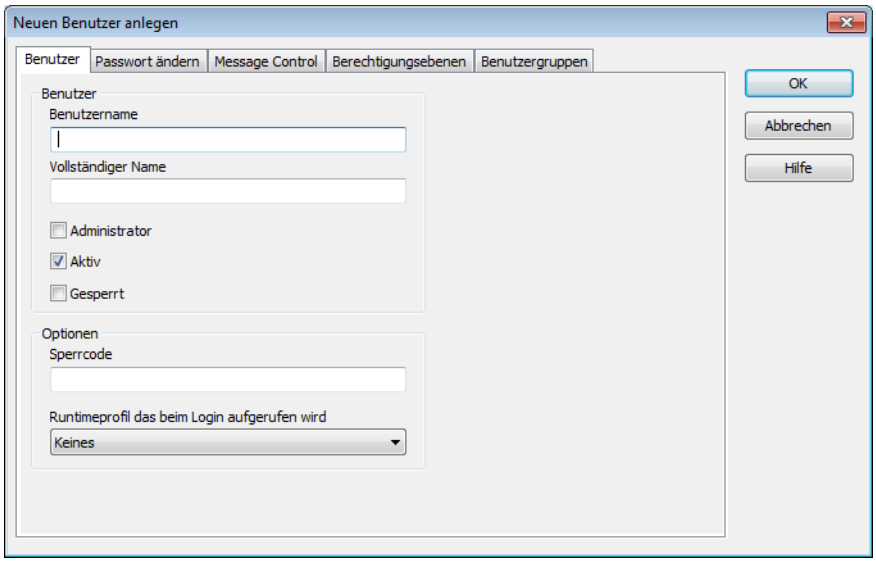
1. navigieren Sie zum Knoten Benutzerverwaltung/Benutzer
2. wählen Sie im Kontextmenü des Projektmanagers oder der Datailansicht oder ind er Symbolleiste Benutzer neu...
3. der Dialog zur Konfiguration wird geöffnet
4. legen Sie in den einzelnen Registerkarten die Einstellungen fest für:
   - Benutzer (auf Seite 11)
   - Passwort (auf Seite 13)
   - Message Control (auf Seite 14)
   - Berechtigungsebenen (auf Seite 16)
   - Benutzergruppen (auf Seite 17)

Info

Empfehlung: Legen Sie als ersten Benutzer einen Administrator ein. Nur dieser hat Zugriff auf alle Funktionen und kann damit auch Benutzer, die durch dreimalige Falscheingabe eines Passwortes gesperrt wurden, wieder frei schalten.

3.2.1 Benutzer

Konfiguration des Benutzers:



Parameter	Beschreibung
Benutzername	Geben Sie hier den Benutzernamen ein. Der Benutzer meldet sich mit seinem Benutzernamen am System an. Maximale Länge: 20 Zeichen. **Hinweis:** Dieser Name muss eindeutig sein.
Vollständiger Name	Geben Sie den vollständigen Namen des Benutzers ein. Damit ordnen Sie Benutzernamen realen Personen zu.
Administrator	Aktiv: Der Benutzer erhält den Status eines Administrators. Nur ein Administrator kann zur Laufzeit neue Benutzer anlegen, Benutzer editieren, Passwörter löschen usw.
Aktiv	Aktiv: Der Benutzer ist aktiv und kann sich zur Runtime anmelden. **Hinweis:** Nach den Regeln der FDA 21 CFR PART 11 darf ein Benutzer nie gelöscht werden, damit auch zu jedem späteren Zeitpunkt nachvollzogen werden kann, wer welche Aktion durchgeführt hat. Daher darf bei Projekten, die diesen Regeln unterliegen, ein Benutzer nur deaktiviert aber nicht gelöscht werden. Um das Löschen von Benutzern zu verhindern, deaktivieren Sie in den Projekteigenschaften die Eigenschaft Löschen von Benutzern in der Gruppe Benutzerverwaltung.
Gesperrt	Aktiv: Der Benutzer ist zur Runtime gesperrt und kann sich nicht anmelden. Diese Option wird automatisch gesetzt, wenn ein Benutzer sein Passwort drei Mal falsch eingegeben hat.
Sperrcode	4-stelliger PIN-Code ein. Dieser Code wird vom Benutzer in der Befehlsgabe verwendet, um Bereiche zu sperren bzw. wieder frei zu geben.
Runtimeprofil, das beim Login aufgerufen wird	Auswahl des Runtimeprofils aus Dropdownliste: ▸ Keines ▸ Default ▸ Last
OK	Übernimmt Änderungen aller Registerkarten und schließt Dialog.
Abbrechen	Verwirft Änderungen aller Registerkarten und schließt Dialog.

Hilfe	Öffnet die Online-Hilfe.

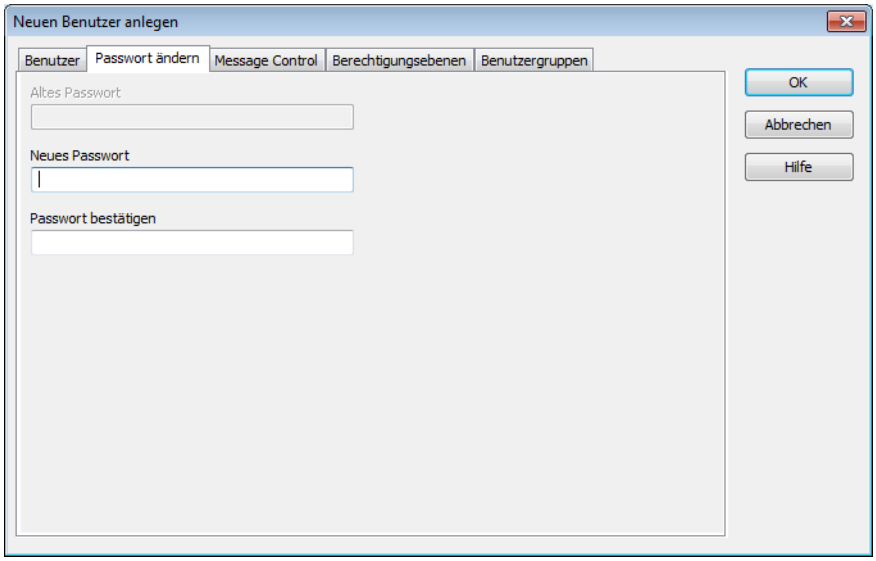
Info

Ein Administrator kann anderen Benutzern nur solche Gruppen frei geben, für die er selbst die Rechte besitzt.

3.2.2 Passwort ändern

Festlegung oder Änderung des Passworts.

Passwörter dürfen maximal 20 Zeichen lang sein. Die minimale Länge wird in den Projekteigenschaften in der Gruppe `Benutzerverwaltung` mit der Eigenschaft `Min. Passwortlänge` definiert. Der Standwardwert beträgt 6 Zeichen.

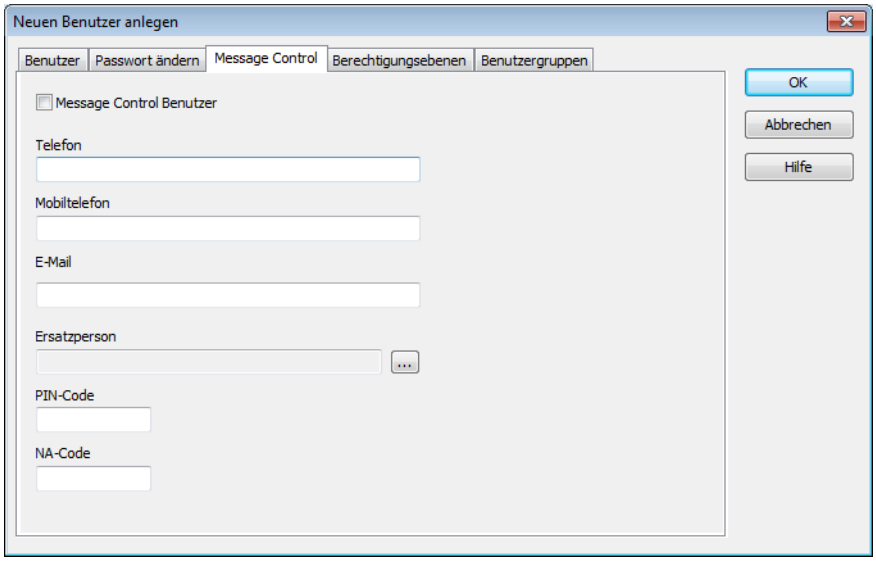


Parameter	Beschreibung
Altes Passwort	Aktuelles Passwort.
Neues Passwort	Eingabe Neues Passwort. Beachten Sie bei sprachübergreifenden Projekten, dass es möglich sein muss,die Zeichen auf der entsprechenden Tastatur zur Runtime einzugeben.
Passwort bestätigen	Wiederholung des neuen Passworts.
OK	Übernimmt Änderungen aller Registerkarten und schließt Dialog.
Abbrechen	Verwirft Änderungen aller Registerkarten und schließt Dialog.
Hilfe	Öffnet die Online-Hilfe.

Die Funktionalität **Kopieren und Einfügen** steht für die Eingabe in Passwortfeldern nicht zur Verfügung.

3.2.3 Message Control

Optionen für die Verwendung der Benutzer im Modul Message Control.



Parameter	Beschreibung
Message Control Benutzer	Aktiv: Der Benutzer wird vom Modul Message Control verwendet.
Telefon	Nummer des Festnetztelefons des Benutzers. Wird für Text-to-Speech verwendet. Eingabe in Ziffern. Ein führendes + als Abkürzung für 00 der internationalen Ländervorwahl ist erlaubt.
Mobiltelefon	Nummer des Mobiltelefons des Benutzers. Wird für Nachrichten über GSM und SMS verwendet. Eingabe in Ziffern, ein führendes + als Abkürzung für 00 der internationalen Ländervorwahl ist erlaubt.
E-Mail	E-Mail Adresse des Benutzers.
Ersatzperson	Auswahl einer Ersatzperson, falls der Benutzer nicht erreicht wird oder die Annahme der Nachricht verweigert. Klick auf Schaltfläche ... öffnet Dialog zur Auswahl.
PIN-Code	PIN-Code, mit dem der Benutzer die Nachricht bestätigt.
NA-Code	PIN-Code, mit dem der Benutzer die Annahme der Nachricht verweigert (not available). Nachricht wird dann an nächsten Benutzer in der Liste gesendet.
OK	Übernimmt Änderungen aller Registerkarten und schließt Dialog.
Abbrechen	Verwirft Änderungen aller Registerkarten und schließt Dialog.
Hilfe	Öffnet die Online-Hilfe.

Achtung

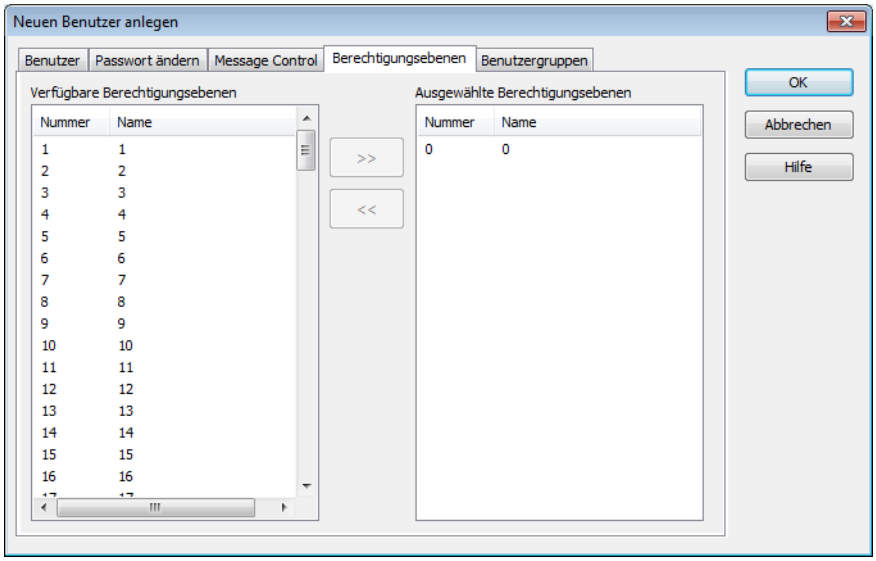
Die Quittier-Codes für PIN (Bestätigung) und NA (Ablehnung) müssen sich unterscheiden und sollten nicht zu ähnlich gewählt werden.

Sind beide Codes ident, wird der Code als PIN und damit als Bestätigung der Nachricht interpretiert.

Wird ein unbekannter Code empfangen, wird bei SMS und E-Mail die Nachricht an die Ersatzperson geschickt, bei Sprachnachrichten die Fehlernachricht abgespielt.

3.2.4 Berechtigungsebenen

Festlegung der Berechtigungsebenen für den Benutzer.



Parameter	Beschreibung
Verfügbare Berechtigungsebenen	Liste aller verfügbarer Berechtigungen
Ausgewählte Berechtigungsebenen	Liste der zugewiesenen Berechtigungen
Schaltfläche Doppelpfeil nach rechts	In der Liste **Verfügbare Berechtigungsebenen** ausgewählte Einträge werden zur Liste **Ausgewählte Berechtigungsebenen** hinzugefügt.
Schaltfläche Doppelpfeil nach links	In der Liste **Ausgewählte Berechtigungsebenen** ausgewählte Einträge werden aus dieser Liste entfernt.
OK	Übernimmt Änderungen aller Registerkarten und schließt Dialog.
Abbrechen	Verwirft Änderungen aller Registerkarten und schließt Dialog.
Hilfe	Öffnet die Online-Hilfe.

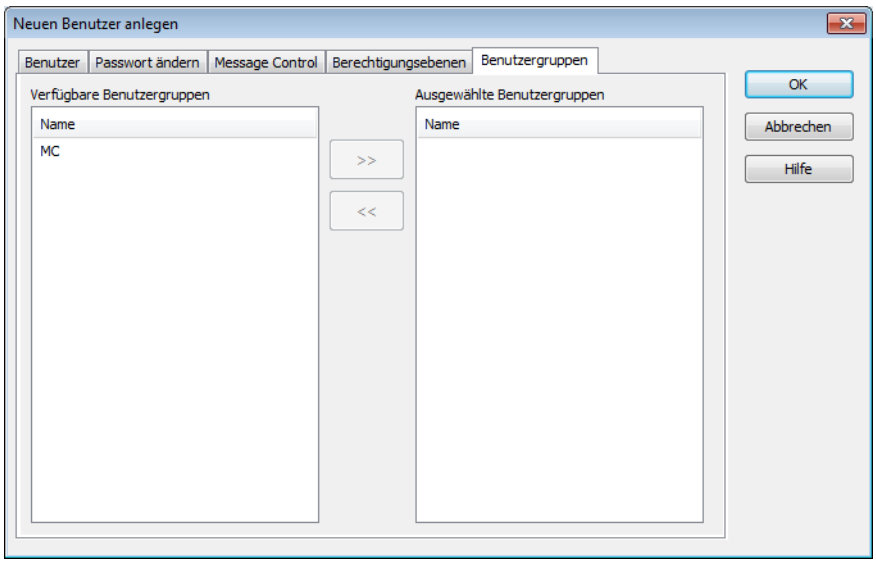
Info

Mithilfe von `Strg` bzw. `Umschalt` können Sie mehrere Einträge gleichzeitig selektieren.

- Bei gedrückter `Strg`-Taste können mehrere einzelne Einträge ausgewählt werden.
- Wenn Sie `Umschalt` gedrückt halten und zwei Einträge anklicken, werden alle Einträge ausgewählt, die sich zwischen den beiden Einträgen befinden.
- Bei gleichzeitigem Drücken und Halten von `Strg` und `Umschalt` und Auswählen von zwei Einträgen, werden alle dazwischen liegenden Einträge ausgewählt und die zuvor ausgewählten Einträge werden beibehalten.

3.2.5 Benutzergruppen

Zuweisung des Benutzers zu Benutzergruppen.



Parameter	Beschreibung
Verfügbare Benutzergruppen	Liste aller verfügbarer Benutzergruppen.
Ausgewählte Benutzergruppe	Liste der zugewiesenen Benutzergruppen.
Schaltfläche Doppelpfeil nach rechts	In der Liste **Verfügbare Benutzergruppen** ausgewählte Einträge werden zur Liste **Ausgewählte Benutzergruppe** hinzugefügt.
Schaltfläche Doppelpfeil nach links	In der Liste **Ausgewählte Benutzergruppe** ausgewählte Einträge werden aus dieser Liste entfernt.
OK	Übernimmt Änderungen aller Registerkarten und schließt Dialog.
Abbrechen	Verwirft Änderungen aller Registerkarten und schließt Dialog.
Hilfe	Öffnet die Online-Hilfe.

Info

Mithilfe von `Strg` bzw. `Umschalt` können Sie mehrere Einträge gleichzeitig selektieren.

- Bei gedrückter `Strg`-Taste können mehrere einzelne Einträge ausgewählt werden.
- Wenn Sie `Umschalt` gedrückt halten und zwei Einträge anklicken, werden alle Einträge ausgewählt, die sich zwischen den beiden Einträgen befinden.
- Bei gleichzeitigem Drücken und Halten von `Strg` und `Umschalt` und Auswählen von zwei Einträgen, werden alle dazwischen liegenden Einträge ausgewählt und die zuvor ausgewählten Einträge werden beibehalten.

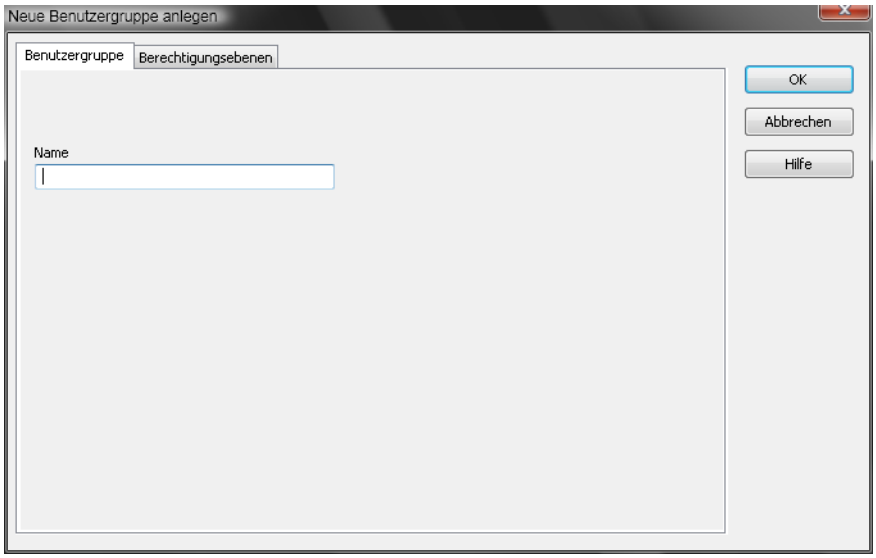
3.3 Anlegen einer Benutzergruppe

Um eine Benutzergruppe anzulegen:

1. markieren Sie in der Baumansicht des Projektmanagers unter dem Eintrag Benutzerverwaltung den Eintrag **`Benutzergruppen`**
2. klicken Sie mit der rechten Maustaste in den Bereich Detailansicht (Detailansicht des Projektmanagers) oder direkt auf den Eintrag **`Benutzergruppen`**
3. wählen Sie im Kontextmenü den Befehl **`Benutzergruppe neu`** oder klicken Sie alternativ dazu auf das entsprechende Symbol in der Symbolleiste
4. die Dialogbox **`Neue Benutzergruppe anlegen`** wird geöffnet
5. definieren Sie Namen (auf Seite 20) und Berechtigungsebenen (auf Seite 21)

> **Info**
>
> *In einem Projekt muss jede Benutzergruppe einen eindeutigen Namen haben.*
>
> *Es ist möglich im Globalprojekt und im lokalen Projekt Benutzergruppen mit gleichen Namen zu erstellen. Ist dies der Fall, werden bei einem Konflikt die Berechtigungen der Benutzergruppe aus dem Standardprojekt herangezogen. Wird die lokale Gruppe gelöscht, erhält der Benutzer nach kompilieren der Runtime-Dateien im Editor wiederum die Rechte aus der Gruppe des Globalprojektes.*
>
> ***Beispiel:***
>
> *Im lokalen Projekt und im Globalprojekt ist jeweils eine Benutzergruppe* **`A`** *vorhanden. Im Globalprojekt sind ihr die Berechtigungsebenen `1`, `2`, `3`, `100` und `101` zugewiesen, im lokalen Projekt die Berechtigungsebenen `1` und `2`. Zur Runtime gelten die Regeln aus dem lokalen Projekt, es werden also nur die Berechtigungsebenen `1` und `2` zugewiesen. Ist im lokalen Projekt keine Benutzergruppe A vorhanden, haben Mitglieder der Gruppe* **`A`** *die Berechtigungsebenen `1`, `2`, `3`, `100` und `101` aus dem Globalprojekt.*

3.3.1 Benutzergruppe benennen



Geben Sie den Namen für die Benutzergruppe ein, die Sie neu anlegen möchten.

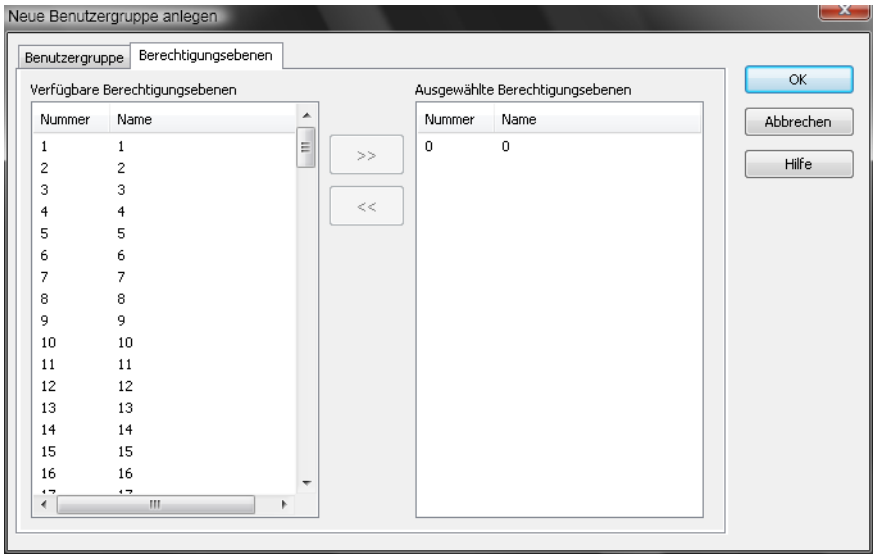
Info

Der Gruppenname kann nicht sprachumschaltbar angelegt werden, da er im Active Directory überprüfbar sein muss.

@ ist kein gültiges Zeichen für den Namen einer Benutzergruppe.

3.3.2 Berechtigungsebenen

Zuweisung der Berechtigungsebenen zur einer Benutzergruppe.



Parameter	Beschreibung
Verfügbare Berechtigungsebenen	Liste aller verfügbarer Berechtigungen
Ausgewählte Berechtigungsebenen	Liste der zugewiesenen Berechtigungen
Schaltfläche Doppelpfeil nach rechts	In der Liste **Verfügbare Berechtigungsebenen** ausgewählte Einträge werden zur Liste **Ausgewählte Berechtigungsebenen** hinzugefügt.
Schaltfläche Doppelpfeil nach links	In der Liste **Ausgewählte Berechtigungsebenen** ausgewählte Einträge werden aus dieser Liste entfernt.
OK	Übernimmt Änderungen aller Registerkarten und schließt Dialog.
Abbrechen	Verwirft Änderungen aller Registerkarten und schließt Dialog.
Hilfe	Öffnet die Online-Hilfe.

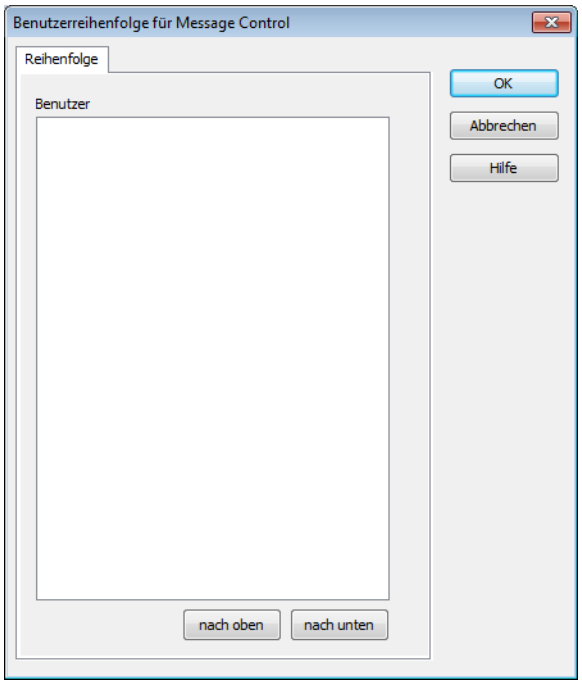
Info

Mithilfe von `Strg` bzw. `Umschalt` können Sie mehrere Einträge gleichzeitig selektieren.

- Bei gedrückter `Strg`-Taste können mehrere einzelne Einträge ausgewählt werden.
- Wenn Sie `Umschalt` gedrückt halten und zwei Einträge anklicken, werden alle Einträge ausgewählt, die sich zwischen den beiden Einträgen befinden.
- Bei gleichzeitigem Drücken und Halten von `Strg` und `Umschalt` und Auswählen von zwei Einträgen, werden alle dazwischen liegenden Einträge ausgewählt und die zuvor ausgewählten Einträge werden beibehalten.

3.3.3 Reihenfolge in Message Control

Legt die Reihenfolge der Benutzer innerhalb einer Gruppe für die Verwendung im Modul Message Control fest.



Parameter	Beschreibung
Benutzer	Liste aller verfügbarer Benutzer
Nach oben	Reiht ausgewählten Benutzer um eine Position nach oben.
Nach unten	Reiht ausgewählten Benutzer um eine Position nach unten.
OK	Übernimmt Änderungen aller Registerkarten und schließt Dialog.
Abbrechen	Verwirft Änderungen aller Registerkarten und schließt Dialog.
Hilfe	Öffnet die Online-Hilfe.

3.4 Ändern eines Benutzers

Das Ändern eines Benutzers erfolgt durch Selektion des Benutzers aus der Liste der Detailansicht. Dadurch wird im Eigenschaften-Fenster die betreffenden Parameter angezeigt. Sie können die

Parameter `Benutzername`, `Vollständiger Name`, `Passwort`, `Berechtigungsebenen` und `Benutzergruppen` ändern.

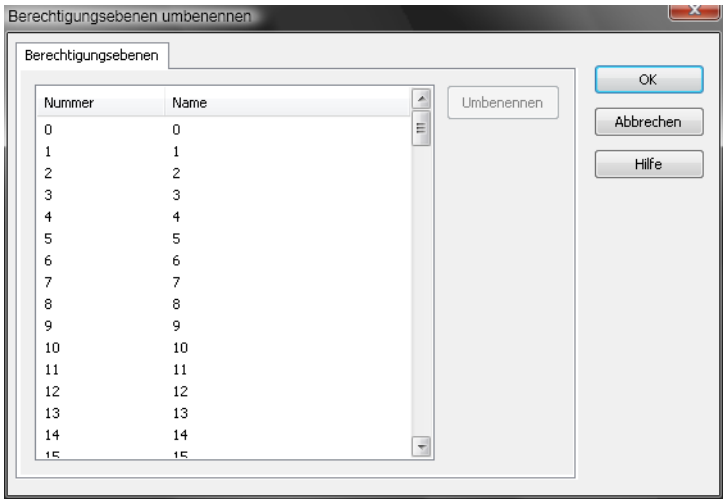
3.5 Änderung einer Benutzergruppe

Das Ändern einer Benutzergruppe erfolgt durch Selektion der Benutzergruppe aus der Liste der Detailansicht. Dadurch wird im Eigenschaften-Fenster die betreffenden Parameter angezeigt. Sie können die Parameter `Name`, und `Berechtigungsebenen` ändern.

> **Info**
>
> *Wenn Sie eine Benutzergruppe umbenennen, verlieren alle Benutzer, die mit dieser Benutzergruppe verknüpft waren, diese Verknüpfung. Die Benutzergruppe wird mit (del) angezeigt.*
>
> *Ist jedoch im Globalprojekt eine Benutzergruppe mit gleichem Namen vorhanden, übernehmen alle Benutzer, die zuvor mit der umbenannten Benutzergruppe verknüpft waren, die Berechtigungsebenen dieser Benutzergruppe.*

3.6 Namensänderung der Berechtigungsebenen

Die Namen der Berechtigungsebenen können Sie global für Ihr Projekt ändern. Dazu gehen Sie bei den Projekteigenschaften zur Gruppe `Benutzerverwaltung` und klicken dort auf die Eigenschaft `Berechtigungsebenen umbenennen`.



Mit einem Doppelklick in die gewünschte Zeile der Spalte **`Name`** öffnen Sie das Editierfeld. Nehmen Sie die Änderungen vor. Die Eingabe wird beendet, sobald der Fokus nicht länger im Feld steht bzw. wenn Sie mit `Enter` bestätigen. Die Namensänderung wird nicht durchgeführt, wenn Sie `Esc` drücken oder Sie das Editierfeld leer lassen.

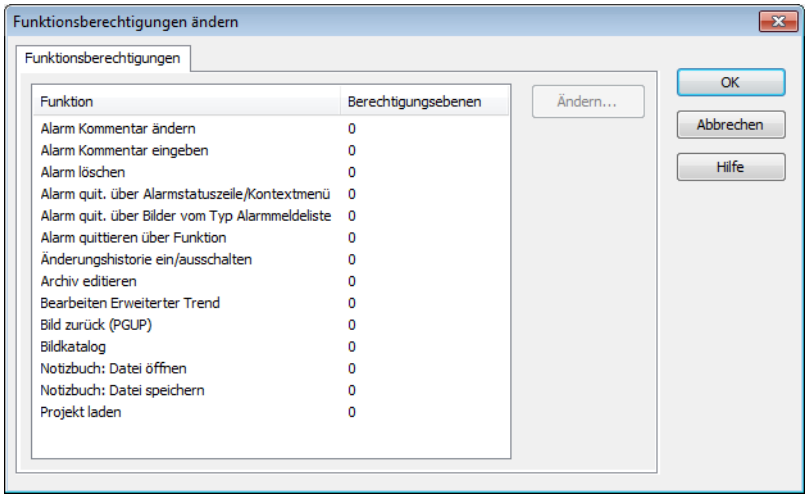
3.7 Funktionsberechtigungen

Funktionsberechtigungen stellen sicher, dass bestimmte Aktionen zur Runtime nur von dazu berechtigten Benutzern ausgeführt werden können.

Um eine Funktionsberechtigung zu vergeben:

1. navigieren Sie in den Projekteigenschaften zum Knoten `Benutzerverwaltung`
2. klicken Sie auf die Eigenschaft `Funktionsbererechtigungen`
3. der Dialog zur Konfiguration wird geöffnet
4. weisen Sie der gewünschten Berechtigung eine Berechtigungseben zu

5. weisen Sie den berechtigten Benutzern diese Berechtigungseben zu und entziehen Sie allen anderen Benutzern diese Berechtigungsebene



Parameter	Beschreibung
Alarm Kommentar ändern	Ein für die Quittierung nötiger Kommentar darf geändert werden.
Alarm Kommentar eingeben	Ein für die Quittierung nötiger Kommentar darf eingegeben werden.
Alarm löschen	Alarme dürfen zur Runtime gelöscht werden.
Alarm quit.über Alarmstatuszeile/Kontextmenü	Quittieren des Alarms über die Alarmstatuszeile oder das Kontextmenü ist nur möglich, wenn die Berechtigung in dem Projekt zum aktuell angezeigten Alarm vorhanden ist. **Bei Mehrprojektverwaltung:** Quittieren der Systemmeldung in der Alarmstatuszeile oder über das Kontextmenü ist nur möglich, wenn die Berechtigung im I-Projekt vorhanden ist. **Anmerkung:** Systemmeldungen sind jene Meldungen, die beim Erreichen einer einstellbaren Alarmanzahl in der Alarmstatuszeile ausgegeben werden.
Alarm quit. über Bilder vom Typ Alarmmeldeliste	Quittieren über ein Bild vom Typ ALarmmeldeliste ist nur mit der Berechtigung in dem mit der Variablen verknüpften Projekt möglich (Mehrprojektverwaltung). **Hinweis:** Wenn die Berechtigung fehlt, wird zwar das Blinken abgestellt, aber der Alarm nicht quittiert.
Alarm quittieren über Funktion	Das Quittieren über eine Funktion ist nur möglich, wenn die Berechtigung zu den ausgewählten Alarmen in den jeweiligen Projekten vorhanden ist.
Änderungshistorie ein/ausschalten	Die Änderungshistorie kann im Editor nur ein/ausgeschalten werden, wenn der eingeloggte Benutzer über die entsprechende Berechtigungsgruppe verfügt.
Archiv editieren	Archivdaten (Archiv Server) können zur Runtime gändert werden.
Bearbeiten Erweiterter Trend	Kurven im Erweiterten Trend können zur Runtime bearbeitet werden. Bei fehlender Berechtigung sind folgende Kotrollelemente nicht aktiviert: ▸ Diagramm ▸ Kurven ▸ Rahmen

	▸ activate ▸ axis
Bild zurück (PGUP)	Bild zurück- Funktion können in der Runtime ausgeführt werden.
Bildkatalog	Die Funktion Bildumschaltung (Bild - Funktionen) mit gesetzter Option diesen Dialog zur Runtime anbieten kann nur ausgeführt werden, wenn der eingeloggte Benutzer über die entsprechende Berechtigungsgruppe verfügt.
Notizbuch: Datei öffnen	Die Funktion Datei `öffnen` im Bild Typ Notizbuch kann nur ausgeführt werden, wenn der eingeloggte Benutzer über die entsprechende Berechtigungsgruppe verfügt.
Notizbuch: Datei speichern	Die Funktion `speichern` im Bild Typ Notizbuch kann nur ausgeführt werden, wenn der eingeloggte Benutzer über die entsprechende Berechtigungsgruppe verfügt.
Projekt laden	Die Projektdatenbank kann im Editor nur geladen werden, wenn der eingeloggte Benutzer über die entsprechende Berechtigungsgruppe verfügt.

Für alle Aktionen muss der Benutzer angemeldet sein und über die entsprechende Berechtigungseben verfügen.

> **Info**
>
> *Das Quittieren eines Alarms ist nur möglich, wenn die Berechtigung zu den ausgewählten Alarmen in den jeweiligen Projekten vorhanden ist.*

Sie können für jede dieser Quittiermethoden unterschiedliche Berechtigungsgruppen einstellen. Damit können Sie z.B. festlegen, dass eine Benutzergruppe nur über die Alarmstatuszeile quittieren kann und nicht anders.

3.8 Bild vom Typ Login anlegen

Die Bedienung durch unterschiedliche Benutzer wird während der Runtime über ein Bild vom Typ Login (auf Seite 88) ermöglicht . Dieses Bild muss zunächst im Editor angelegt werden.

Nähere Informationen zu den vordefinierten Bildtypen finden Sie im 'Bilder / Vordefinierte Bildtypen'.)

Nach dem Öffnen des Bildes wird ein leeres Bild aufgeschaltet. Die Standard-Kontrollelemente können Sie über das Menü Kontrollelemente -> Vorlage einfügen erstellen.

4. Active Directory (AD)

Active Directory kann in zenon zur Benutzerverwaltung in der zenon Runtime verwendet werden. Für den zenon Editor steht AD nicht zur Verfügung.

Das Active Directory kann auf drei Arten von zenon genutzt werden:

1. Der Name der Berechtigungsgruppe in der zenon Benutzerverwaltung stimmt mit dem Gruppennamen einer Benutzergruppe im Active Directory überein: Automatische Zuordnung der Active Directory Benutzer zu der zenon Berechtigungsgruppe. Alle Benutzer der AD Gruppe erhalten die Benutzerrechte, die in der zenon Berechtigungsgruppe definiert sind. Siehe Benutzergruppen in zenon und Gruppen im Active Directory haben den selben Namen (auf Seite 30)

2. In der Beschreibung der Active Directory Gruppe werden die zenon Berechtigungsebenen und das Projekt in einer eine bestimmte Syntax hinterlegt. Alle Benutzer der Gruppe enthalten in zenon die in der AD Gruppe hinterlegten Benutzerrechte. Siehe Zuordnung eines Active Directory Benutzers zu zenon Berechtigungsebenen (auf Seite 31)

3. Das Active Directory Schema wird um Felder erweitert, in denen die zenon Berechtigungsebenen abgespeichert werden. Das erfordert eine Schema Erweiterung des Active Directorys . Diese eignet sich allerdings nicht für den Einsatz im FDA 21 CFR Part11 reglementierten Umfeld. Siehe: Schema-Erweiterung des Active Directory (auf Seite 32).

> **Info**
>
> *Bei der Passwortprüfung in zenon wird auch* `Max. password age` *aus dem Active Directory geprüft.*

Info

Active Directory und ADAM/AD LDS stehen unter Windows CE nicht zur Verfügung.

4.1 Allgemeines

Um in zenon die Benutzer aus dem ActiveDirectory (in Folge: AD genannt) verwenden zu können ist eine Domäne auf Basis eines Windows Server Betriebssystems die Grundvoraussetzung. Um Benutzer im ActiveDirectory verwalten zu können, muss der Server ein DNS Server sein.

Es muss also ein Domaincontroller mit DNS und ActiveDirectory zur Verfügung stehen um diese Benutzerkonten dann auch auf einem PC in der Domäne als Benutzer in zenon verwenden zu können.

Der Zugriff auf die Benutzer des ActiveDirectory muss in den Eigenschaften des Projekts aktiviert werden.

Grundlegendes Wissen über das ActiveDirectory und Windows Server - Technologie wird vorausgesetzt.

Achtung

Wenn die Anmeldung über Active Directory erfolgt, müssen ausnahmslos alle Rechner auf Active Directory Zugriff haben. Das gilt auch für Clients und Webclients!

Hintergrund: Die Anmeldung eines Clients erfolgt direkt vom Client zum Active Directory. Der zenon Runtime-Server ist daran nicht beteiligt.
Ein Active Directory Benutzer kann also nur angemeldet werden, wenn ein Client:

- Mitglied der Domäne ist
  und
- Zugriff hat auf die Domäne hat

4.2 Gleiche Benutzergruppen in zenon und im Active Directory

Für Benutzer in zenon und im Active Directory gilt:

- Existiert ein benutzer im AD, aber nicht in zenon, dann:
  - werden die Benutzergruppen in zenon überprüft
  - die Berechtigungsebenen der Gruppen, denen der Benutzer angehört, werden dem AD Benutzer zugewiesen
- Existiert ein Benutzer sowohl im AD und in zenon und der Benutzer loggt sich in die Runtime ein, dann:
  - hat der lokale zenon Benutzer Vorrang vor dem AD Benutzer
  - werden in AD keine Berechtigungsebenen überprüft, da der lokale Benutzer eingeloggt ist

4.3 Setzen der zenon Berechtigungsebenen im Beschreibungsfeld einer Active Directory Gruppe

Die Windows Benutzer aus dem Active Directory können in zenon verwendet werden.

Einzelne Benutzer können im Active Directory Gruppen zugewiesen werden. Die Namen der Gruppen müssen wie in folgender Syntax beschrieben lauten:

zenon Projektname##freier Text

In ihrer Beschreibung wird die Berechtigung des Benutzers mit folgender Syntax hinterlegt:

freier Text ##GRP=HEX-Zahl## freier Text

Info

Die Groß-/Kleinschreibung spielt beim Gruppennamen und der Gruppenbeschreibung keine Rolle.

Um eine bessere Lesbarkeit zu gewährleisten, wird die HEX-Zahl in vier Teile (je ein Teil für jede Berechtigungsgruppe) geteilt, die jeweils mit einem Bindestrich unterteilt werden.

Aufbau der Hex-Zahl			
FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF
Berechtigungseben 1	Berechtigungseben 2	Berechtigungsene 3	Berechtigungseben 4

Beispiel

Gruppenname: MASCHINE01##Servicepersonal

Gruppenbeschreibung: freier Text##GRP=FFFFFFFF-FFFFFFFF-FFFFFFFF-FFFFFFFF##freier Text

Die Benutzer, die der Gruppe MASCHINE01##Servicepersonal zugeordnet sind, erhalten in zenon die Berechtigungsebenen 0 - 127.

Es ist nicht nötig alle 32 Stellen anzugeben. Nicht vorhandene Stellen werden als 0 interpretiert.

Beispiel

Gruppenbeschreibung: freier Text##GRP=7##freier Text

Benutzer, die der Gruppe mit dieser Beschreibung zugeordnet sind, erhalten in zenon die Berechtigungsebenen 0, 1 und 2.

7 hexadezimal entspricht in binärer Darstellung 111. Für jede 1 in der Binärzahl, wird die entsprechende Berechtigungsebene gesetzt. Das rechteste Bit steht für die Berechtigungsebene 0. Das Bit links daneben steht für die Berechtigungsebene 1 usw.

Eine Benutzer kann auch mehrere Gruppen zugehörig sein. Er erhält dann die Summe der Berechtigungsebenen der einzelnen Gruppen.

Wird ein Benutzer in zenon eingeloggt, wird erst überprüft, ob der Benutzer lokal in zenon vorhanden ist. Wenn nicht, wird nach dem Benutzer im Active Directory gesucht. Existiert der Benutzer dort auch nicht, wird der Benutzer nicht eingeloggt und ein entsprechender Eintrag in der CEL angelegt. Falls der Benutzer im AD vorhanden ist, jedoch keine Berechtigungsebenen in zenon für diesen Benutzer definiert sind, wird folgender Eintrag in der CEL angelegt: 'Keine Benutzerrechte für den Benutzer im AD definiert'. Der Benutzer wird mit Level 0 eingeloggt.

4.4 Schema-Erweiterung des Active Directory

Hinweis: Diese Erweiterung sollte nicht im FDA 21 CFR Part11 reglementierten Umfeld eingesetzt werden. Nutzen Sie für FDA 21 CFR Part11 kompatible Benutzerverwaltung entweder die Methode

Benutzergruppen in zenon und Gruppen im Active Directory (auf Seite 30) oder Zuordnung eines Active Directory Benutzers zu zenon Berechtigungsebenen (auf Seite 31).

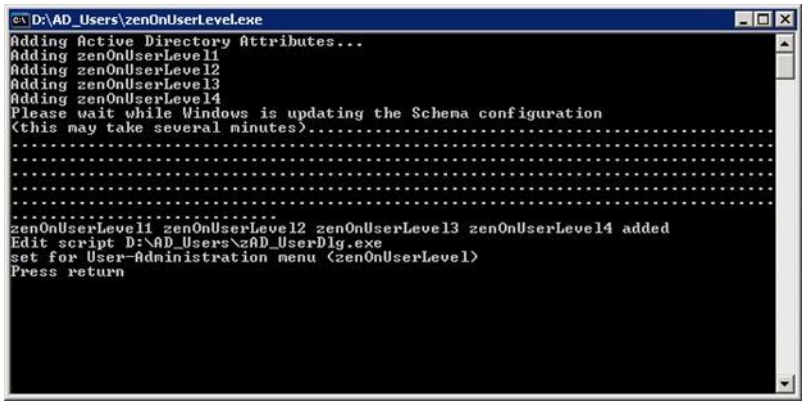
> **Info**
>
> *Active Directory und ADAM/AD LDS stehen unter Windows CE nicht zur Verfügung.*

4.4.1 Installieren der Schema Erweiterung

Damit den Benutzern im AD auch die 128 Berechtigungsebenen von zenon zugewiesen werden können, muss das AD-Schema um diese Einträge (4 Integerwerte) ergänzt werden.

Dazu werden 2 Dateien (`zenonUserLevel.exe`, `zAD_UserDlg.exe`) auf den Server kopiert (am besten in ein eigenes Verzeichnis). Sobald das Setup (`zenonUserLevel.exe`) gestartet wurde, darf dieser Ordner und die enthaltenen Dateien nicht mehr umbenannt oder gelöscht werden.

> **Achtung**
>
> *Die beiden Dateien **`zenonUserLevel.exe`** und **`zAD_UserDlg.exe`** finden Sie auf der zenon DVD im Ordner `/Software/zenonUserLevel/`*



Es wird vom Setup ein Verweis auf die Datei `zAD_UserDlg.exe` im AD-Schema hinterlegt.

Weiters werden 4 Integerwerte (zenonUserLevel1, zenonUserLevel2, zenonUserLevel3, zenonUserLevel4) dem AD-Schema hinzugefügt.

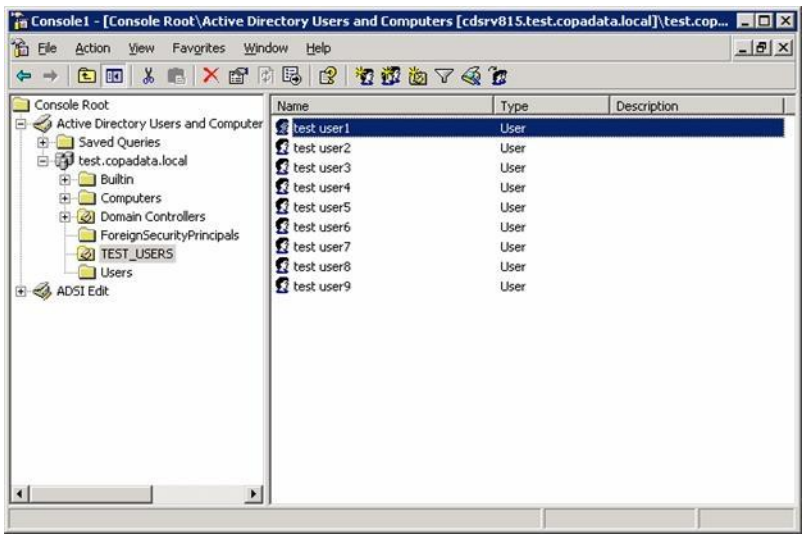
Info

Nur ein Benutzer der Gruppe **`Schema Administratoren`** *darf diese Änderungen durchführen! Der Domain-Administrator hat im Normalfall diese Rechte.*

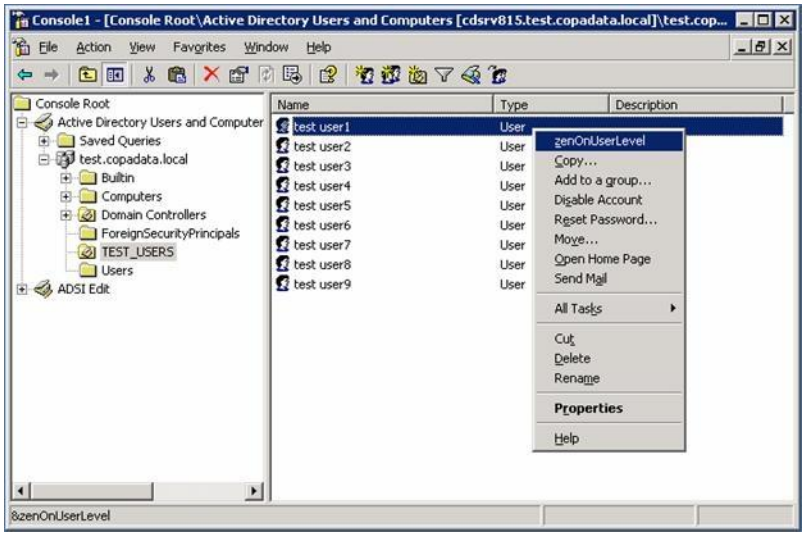
4.4.2 Zuweisen von Benutzerrechten

Nach der erfolgreichen Schema Erweiterung können nun den einzelnen Benutzern die Berechtigungsebenen zugewiesen werden.

Dazu wird die Microsoft Management Konsole (MMC) mit dem Plug-in **`Active Directory Users and Computers`** geöffnet.

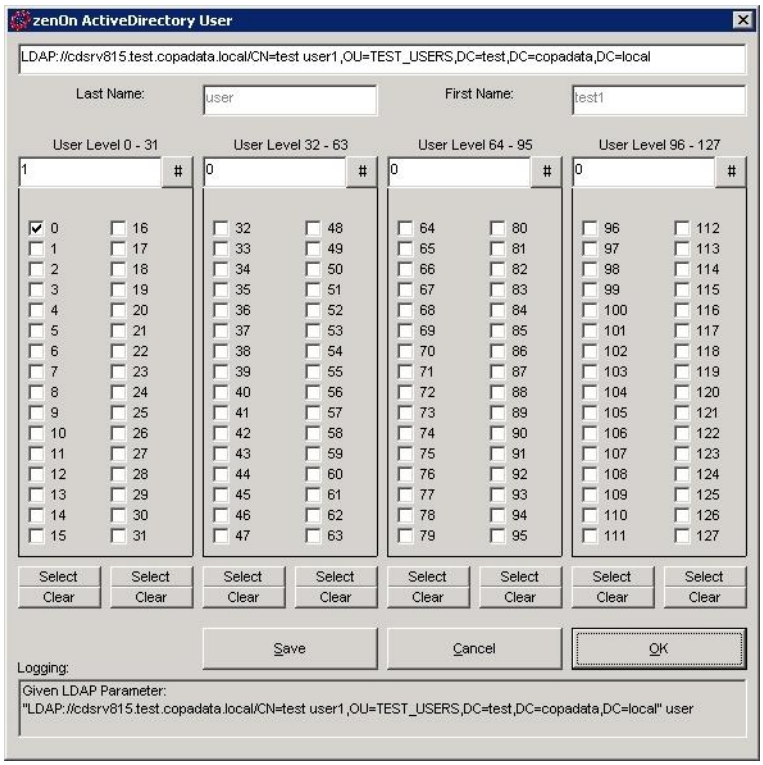


Durch anklicken des gewünschten Benutzers mit der rechten Maustaste öffnet sich ein Kontextmenü. Im Kontextmenü wird ein neuer Menüpunkt sichtbar: **`zenonUserLevel`**.



In diesem Kontextmenü muss der Menüpunkt **`zenonUserLevel`** ausgewählt werden, damit sich das AdministrationsTool (zAD_UserDlg.exe) für den gewählten Benutzer öffnet.

> **Info**
>
> *Es können die Berechtigungsgruppen für zenonnur direkt beim Benutzer hinterlegt werden, Gruppen und Organisationseinheiten werden nicht unterstützt.*



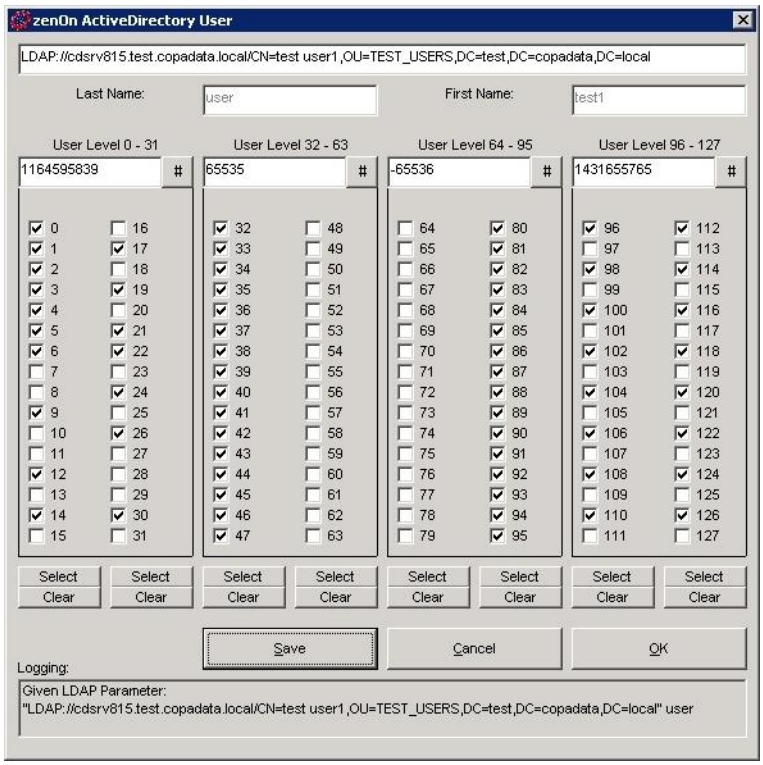
Mit Hilfe dieses Administrationstools können für jeden Benutzer bis zu 128 Berechtigungsebenen definiert werden.

Info

Die Berechtigungsebene 0 ist per Default jedem Benutzer zugewiesen, diese kann mit dem Administrationstool auch nicht deaktiviert werden.

*Diese Ebene entspricht dem Benutzer **SYSTEM** von zenon.*

Beschreibung des AdministrationsTools



Parameter	Beschreibung
[erste Zeile]	LDAP-Parameter, der als Connectionstring dient.
`Last Name`	Nachname des selektieren Benutzers.
`First Name`	Vorname des selektieren Benutzers.
`User Level`	4 Integerwerte repräsentieren je 32 Berechtigungsebenen. Eingabe durch aktivieren bzw. deaktivieren der Checkboxen oder direkte Eingabe in Feld.
#	Aktualisiert Darstellung der Berechtigungsebenen.
`Select`	Aktiviert alle Checkboxen in einer Spalte.
`Clear`	Deaktiviert alle Checkboxen in einer Spalte.
`Save`	Speicher aktuelle Einstellungen.
`Cancel`	Verwirft alle Einstellungen seit letztem Speichern und schließt Dialog.
`OK`	Speichert alle Einstellungen und schließt Dialog.
`Logging`	Zeigt Logginginformationen an.

4.4.3 Schema Erweiterung - Details

Um die Hintergründe etwas zu verdeutlichen, werden hier die Schema Erweiterungen im Detail erklärt, damit diese bei Problemen auch kontrolliert bzw. überprüft werden können.

Damit die Details des AD-Schema betrachtet werden können, muss **`ADSI Edit`** auf dem Server installiert sein. Dieses Tool steht zur Verfügung, sobald die Support Tools von der Microsoft Server CD installiert worden sind.

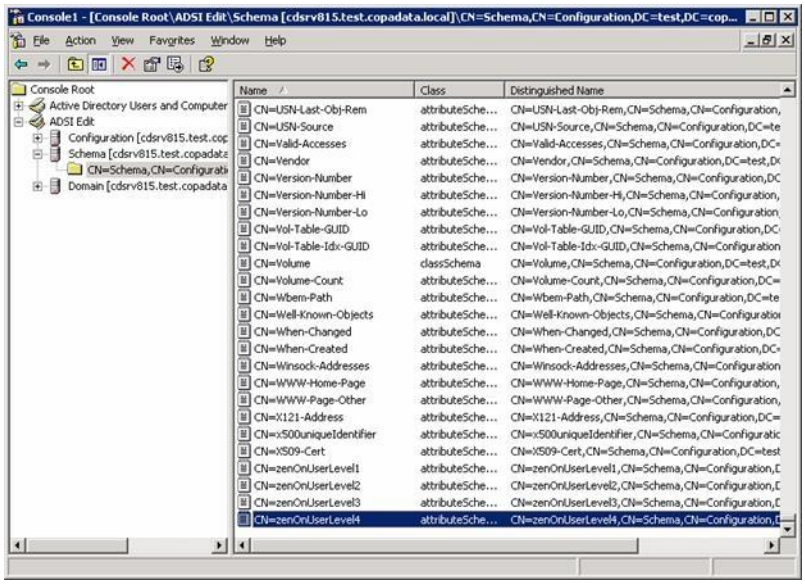
Zu finden auf der CD unter: `CD_ROOT/SUPPORT/TOOLS/SUPTOOLS.msi`

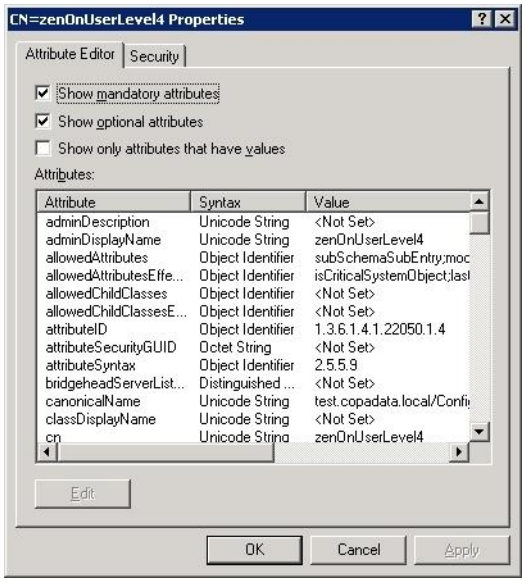
Das **`ADSI Edit`** Plug-in kann dann in der Microsoft Management Konsole (MMC) geöffnet werden. Danach können verschiedene Verbindungen hergestellt werden.

Schema

Im Schema können die zusätzlichen Attribute kontrolliert werden. Diese sind im Normalfall ganz unten aufgelistet.

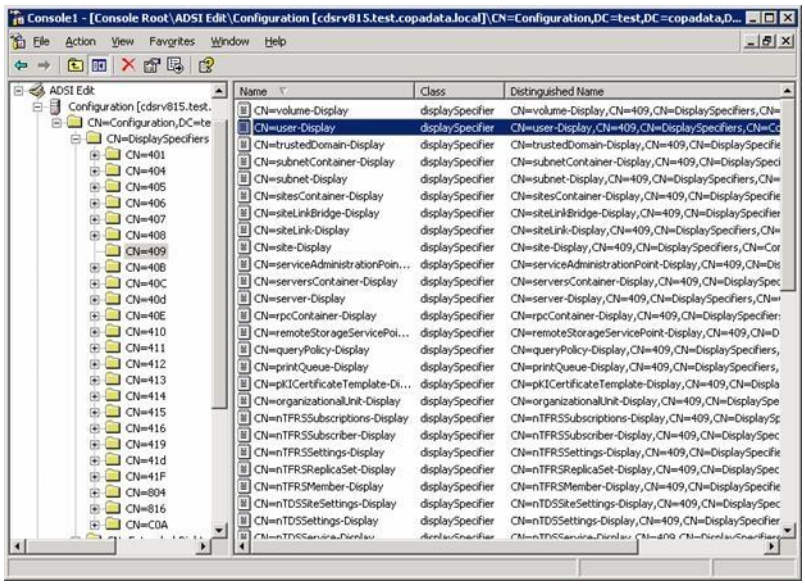
`zenonUserLevel1 - zenonUserLevel4`

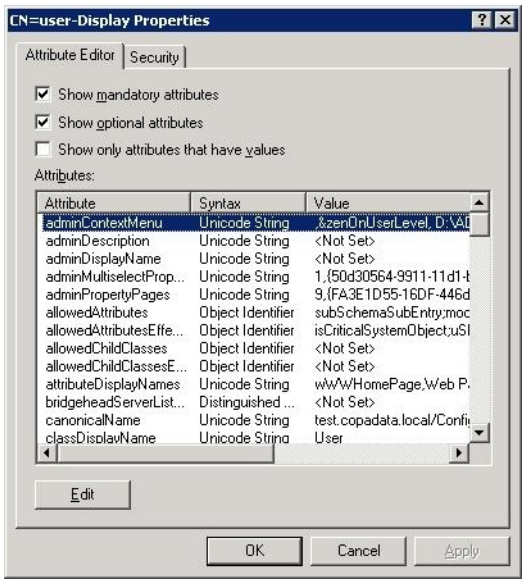




Configuration

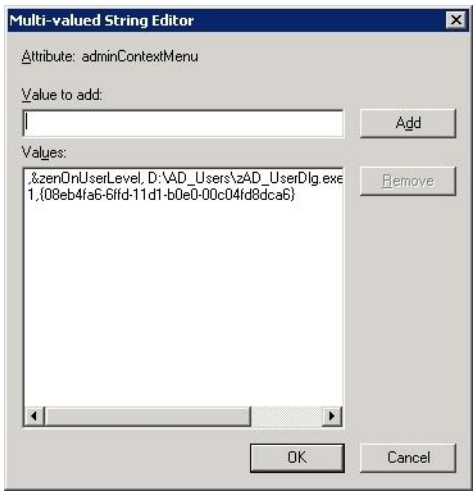
Wenn die Verbindung auf Configuration eingerichtet wurde, können Details der einzelnen AD Objekte begutachtet und geändert werden. In diesem Fall ist jedoch nur das Objekt user-Display in den einzelnen DisplaySpecifiers von Interesse, da hier die Verknüpfung zwischen Benutzerobjekt und Administrationstool hergestellt wird.





Die Eigenschaften des Objektes **`user-Display`** enthalten ein Attribut mit dem Namen `adminContextMenu`.

Dieses Attribut beinhaltet die Verknüpfung zum Administrationstool (**`zAD_UserDlg.exe`**).



Man kann diesen Eintrag auch per Hand ändern, wenn dies notwendig sein sollte.

Dazu:

1. Eintrag auswählen
2. Schaltfläche **`Remove`** drücken
3. den Parameter anpassen
4. mit **`Add`** wieder hinzufügen

Der Parameter setzt sich wie folgt zusammen:

`,Bezeichnung des Menüeintrages,Pfad zur zAD_UserDlg.exe Datei`

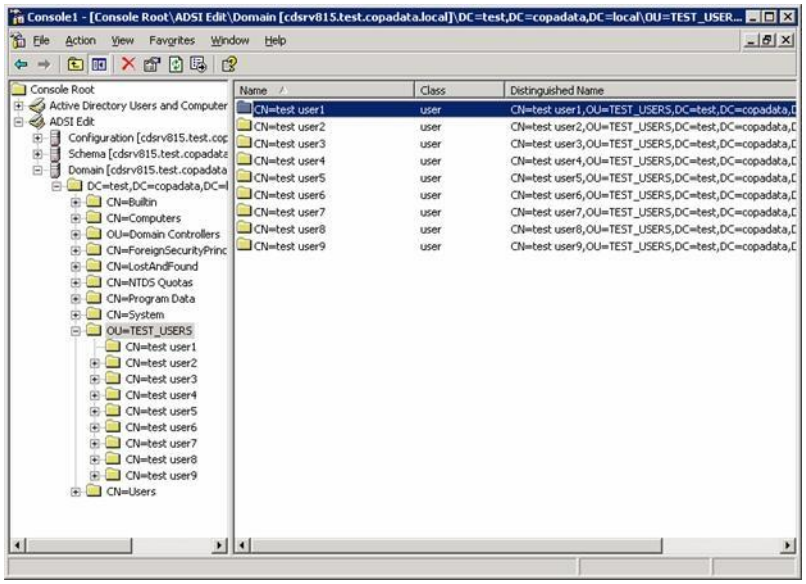
Beispiel

Beispiel, wenn die EXE Datei im Verzeichnis `D:/AD_Users` hinterlegt ist.

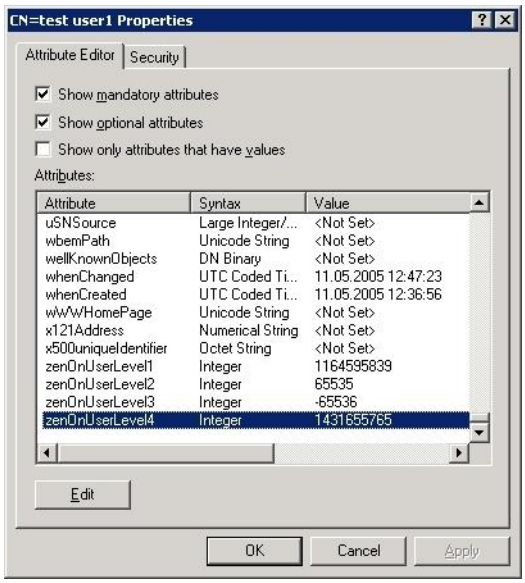
`,&zenonUserLevel,D:/AD_Users/zAD_UserDlg.exe`

Domain

Wenn die Verbindung **Domain** geöffnet wird, sieht man auf den ersten Blick parallelen zur MMC mit dem Plug-in **Active Directory Users and Computers**. Genau diese Information kann man auch hier wieder finden, jedoch etwas detaillierter.



Untersucht man beispielsweise die Eigenschaften eines Benutzer Objekts und scrollt dabei in der Liste ganz nach unten, findet man auch hier wieder die 4 Integerwerte für die Berechtigungsebenen.



5. Active Directory Lightweight Directory Services - AD LDS (ab Windows Vista)

Active Directory Lightweight Directory Services (kurz: AD LDS) ist eine vereinfachte Version des Active Directory (auf Seite 29) und eignet sich für den Einsatz auf normalen Desktop-Betriebssystemen, es muss also kein Server-Betriebssystem eingesetzt werden. Wie AD (auf Seite 29) unterstützt auch AD LDS:

1. Der Name der Berechtigungsgruppe in der zenon Benutzerverwaltung stimmt mit dem Gruppennamen einer Benutzergruppe im Active Directory überein: Automatische Zuordnung der Active Directory Benutzer zu der zenon Berechtigungsgruppe. Alle Benutzer der AD Gruppe erhalten die Benutzerrechte, die in der zenon Berechtigungsgruppe definiert sind. Siehe Benutzergruppen in zenon und Gruppen im Active Directory haben den selben Namen (auf Seite 30)
2. In der Beschreibung der Active Directory Gruppe werden die zenon Berechtigungsebenen und das Projekt in einer eine bestimmte Syntax hinterlegt. Alle Benutzer der Gruppe enthalten in zenon die in der AD Gruppe hinterlegten Benutzerrechte. Siehe Zuordnung eines Active Directory Benutzers zu zenon Berechtigungsebenen (auf Seite 31)

AD LDS können Sie verwenden unter:

- Windows Vista
- Windows 7
- Windows Server 2008

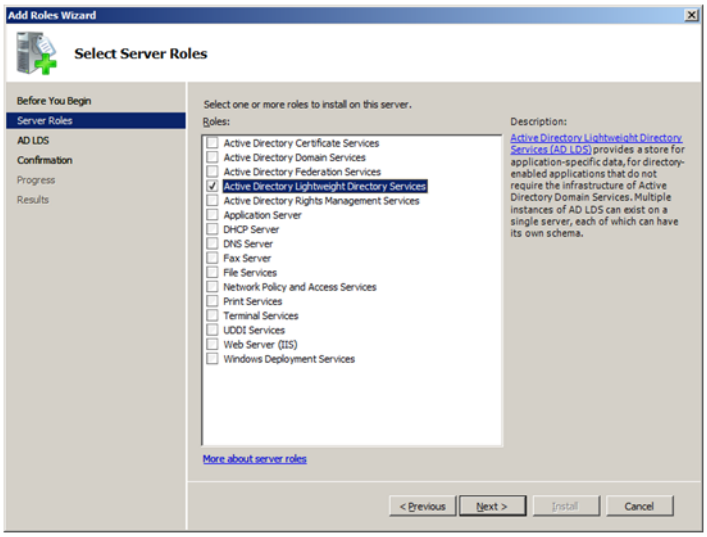
Für Windows XP benutzen Sie ADAM (auf Seite 73).

In dieser Anleitung wird die Installation und Konfiguration unter Windows Server 2008 erklärt. Die Nutzung unter Windows Vista und Windows erfolgt analog. Details dazu siehe Kapitel AD LDS unter Windows 7 und Windows Vista (auf Seite 71).

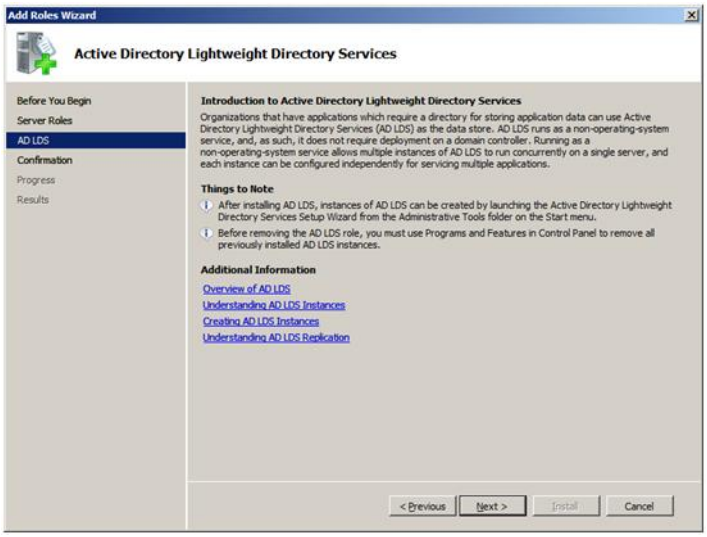
5.1 AD LDS unter Windows 2008

Um die AD LDS Server Role zu installieren:

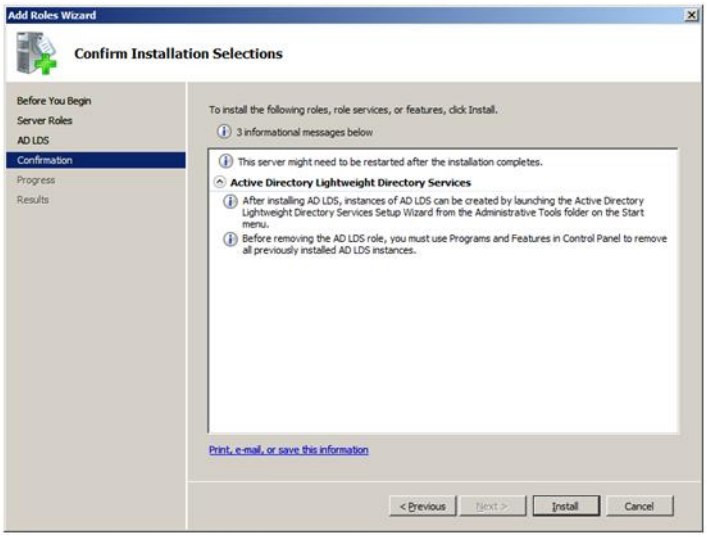
1. wählen Sie in den Administrative Tools **`Server Manager`**

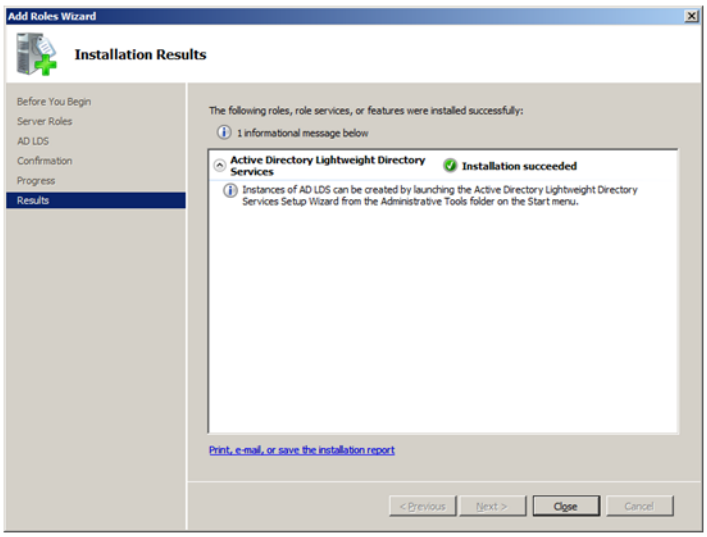


2. klicken Sie auf **`Add Roles`**



3. fügen Sie die `AD LDS Role` hinzu





5.2 Neue AD LDS Instanz erstellen

Um eine neue AD LDS Instanz zu erstellen:

1. Rufen Sie im Active Directory Lightweight **`Directory Services Control Panel`** den **`AD LDS Setup Wizard`** auf.

2. Starten Sie den Wizard:

3. Wählen Sie die Option `A unique instance.`

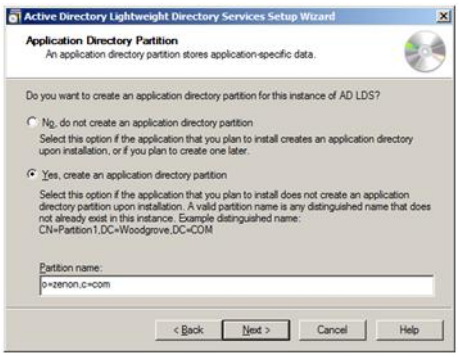
4. Vergeben Sie einen Namen für die Instanz.

5. Konfigurieren Sie die Ports. Default:
   - LDAP: `389`
   - SSL: `636`

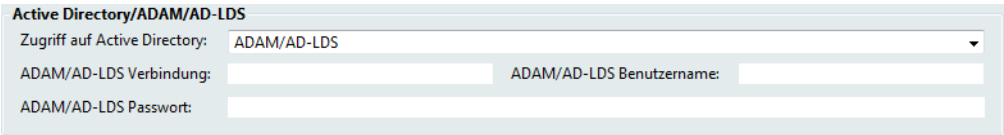
Hinweis: Wenn Sie hier den voreingestellten Port ändern, müssen Sie auch in einigen der folgenden Einstellungen den Port anpassen.

6. Spezifizieren Sie den **`Partition Name`**.

In unserem Beispiel: `o=zenon,c=com`



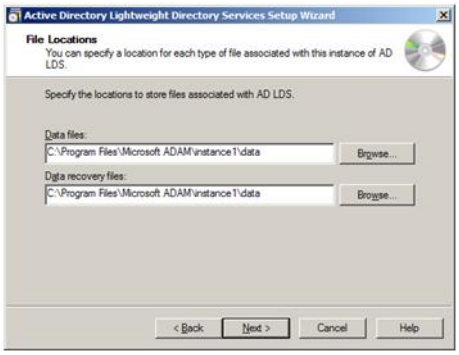
Der **`Partition Name`** wird zusammen mit dem Port und dem Servernamen später in zenon benutzt.



Diese Konfiguration in zenon kann später erfolgen. Fahren Sie mit der Konfiguration im Wizard fort.

7. Definieren Sie den Speicherort.

   Die Einstellung kann auf der Default-Einstellung belassen werden.



8. Definieren Sie den Service Account für AD LDS.

In unserem Beispiel: **`Network service account`**

Falls der Computer, auf dem AD LDS installiert wird, kein Mitglied einer Domäne ist, erhalten Sie eine Warnmeldung:

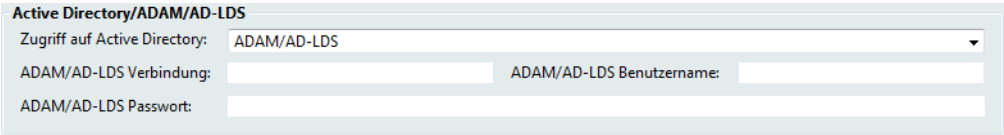
Das beeinträchtigt die Funktionalität von AD LDS nicht. Ausnahme: Sie verwenden die Funktion Replication.

Bestätigen Sie die Warnung mit einem Klick auf die Schaltfläche **`Yes`**.

9. Definieren Sie den Benutzer, der Administratorechte erhält.

In unserem Beispiel verwenden wir `Currently logged on user`. In unserem Fall ein lokaler Benutzer mit Administratorrechten.

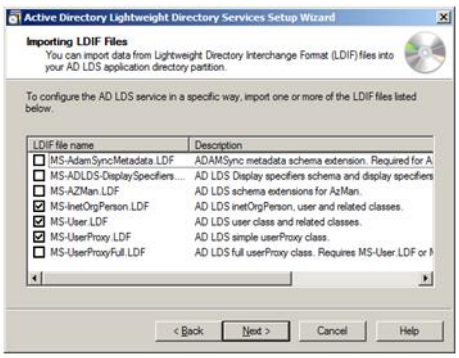
Der Benutzer und sein Passwort werden später in zenon verwendet.



Diese Konfiguration kann später erfolgen. Fahren Sie mit der Konfiguration im Wizard fort.

10. Importieren Sie die benötigten LDIF-Dateien:

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



11. Beenden Sie die Installation

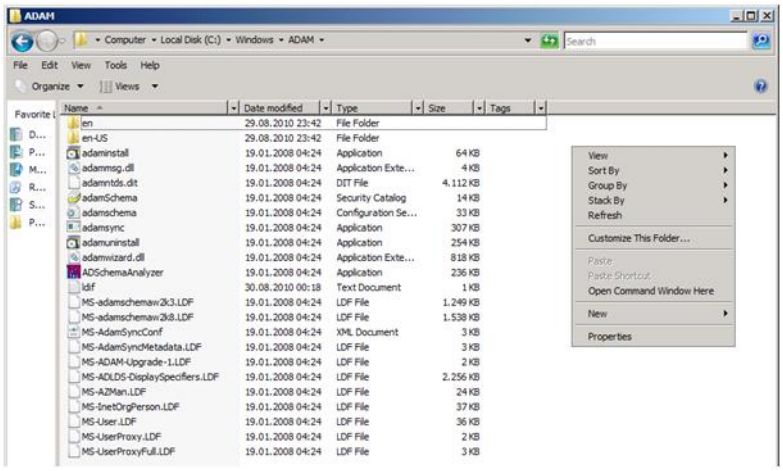
5.3 AD LDS Schema importieren

Zum Import der AD LDS Schemata:

1. Navigieren Sie im Windows Explorer zum Ordner `%WINDIR%\ADAM`.

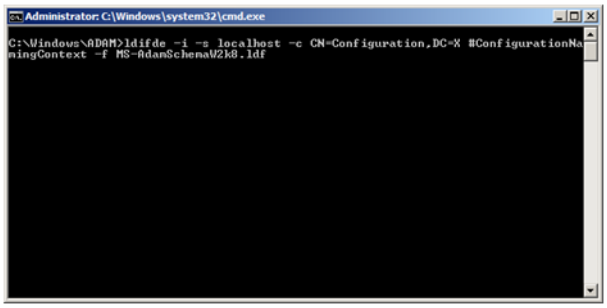
2. Wählen Sie im Kontextmenü [`Taste Umschalt+rechter Mausklick`]:

   `Eingabeaufforderung hier öffnen.`

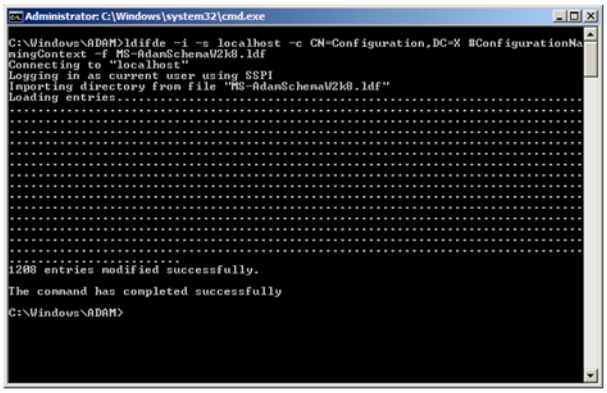


3. Geben Sie folgende Zeichenfolge ein:

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



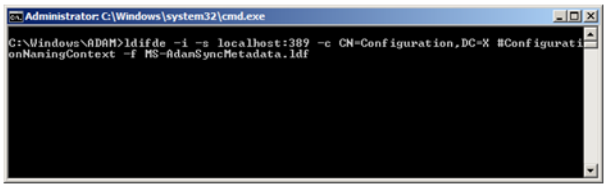
4. Drücken Sie die Eingabetaste:



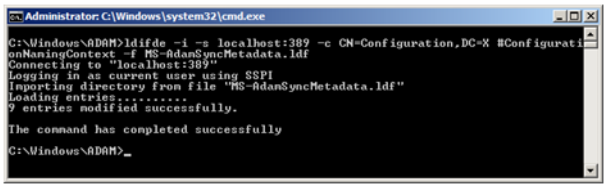
5. Geben Sie folgende Zeichenfolge ein:

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

Hinweis: Falls Sie einen Port geändert haben, muss dieser hier angepasst werden.



6. Drücken Sie die Eingabetaste:



5.4 AD Schema Snap-in konfigurieren

Um das Schema Snap-in zu konfigurieren, registrieren Sie es zuerst über die Eingabeaufforderung (Administratorrechte nötig):

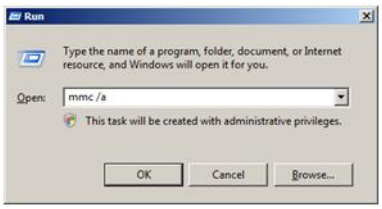
1. klicken Sie auf die Schaltfläche **`Start`**
2. navigieren Sie zur **`Eingabeaufforderung`**
3. wählen Sie im Kontextmenü `Als Administrator ausführen`
4. geben Sie in der Eingabeaufforderung ein: **`regsvr32 schmmgmt.dll`**
5. bestätigen Sie mit Druck auf die Taste **`Eingabe`**

KONFIGURATION

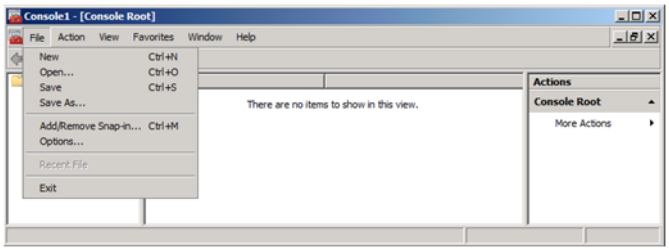
1. klicken Sie auf die Schaltfläche **`Start`**

2. öffnen Sie **`Ausführen`**

3. geben Sie ein: **`mmc /a`**



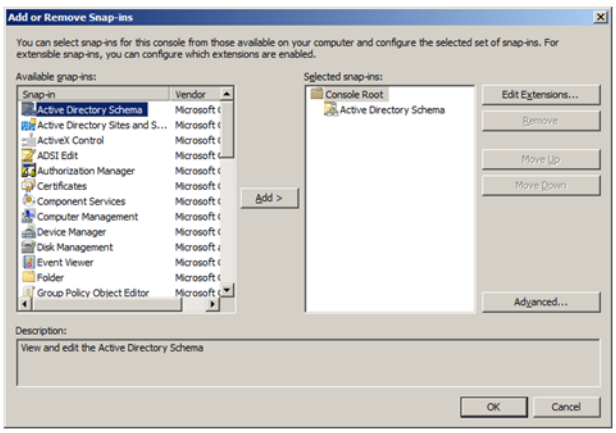
4. klicken Sie auf *File -> Add/Remove Snap-in...*



5. wählen Sie **`Active Directory Schema`**

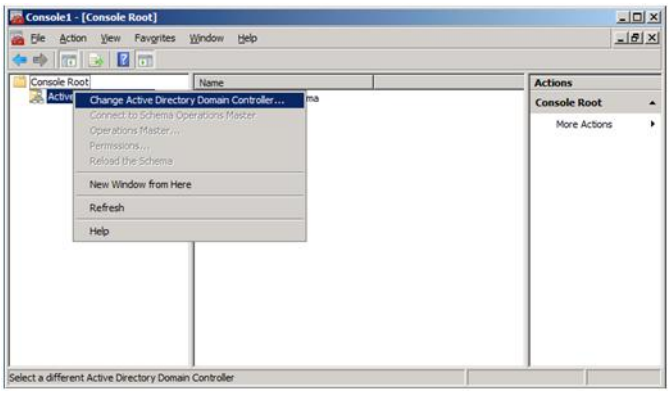
6. klicken Sie auf **`Add`**

7. klicken Sie auf **`OK`**

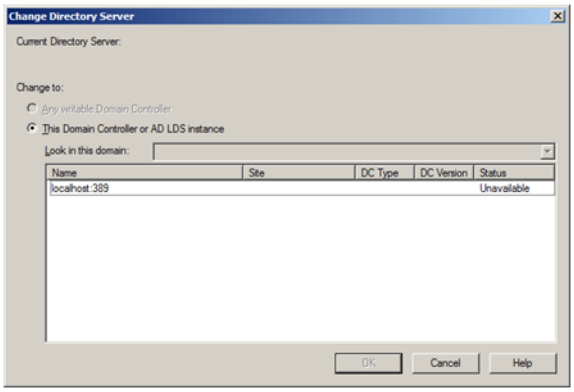


8. navigieren Sie zu **`Active Directory Schema`**

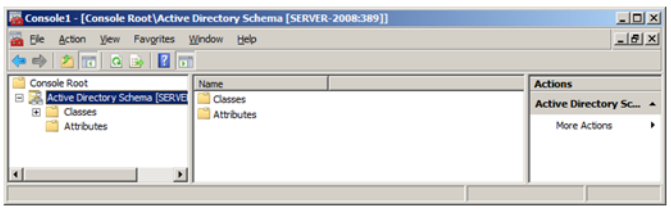
9. wählen Sie im Kontextmenü `Change Active Directory Domain Controller...`



10. Geben Sie Server und Port ein (in diesem Beispiel: `localhost:389`)

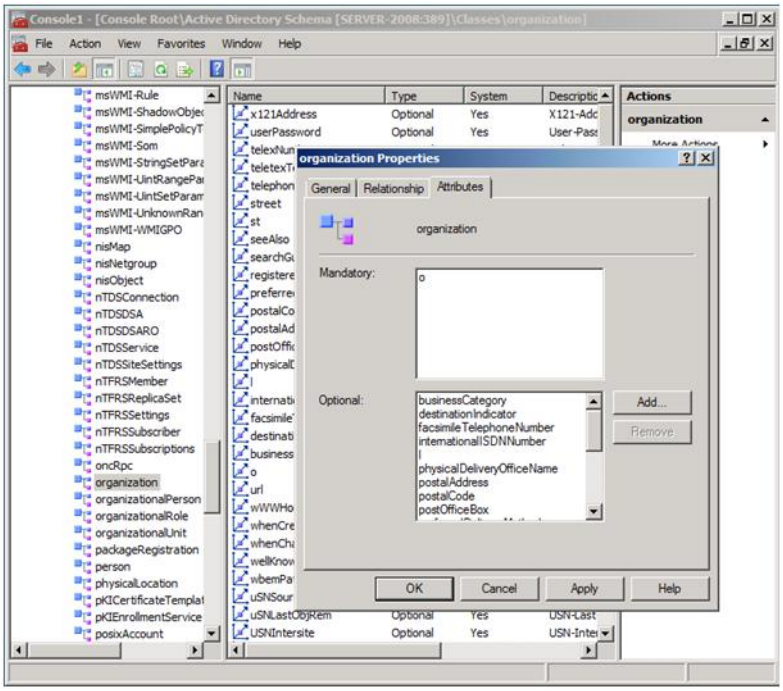


11. Sie sollten jetzt dieses Fenster sehen:



12. navigieren Sie zu *Classes -> organization*

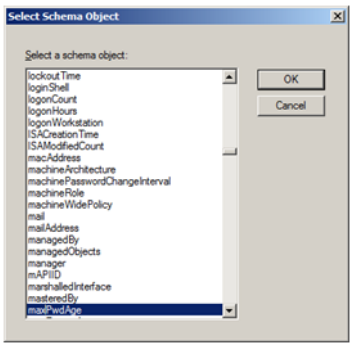
13. öffnen Sie **Properties**



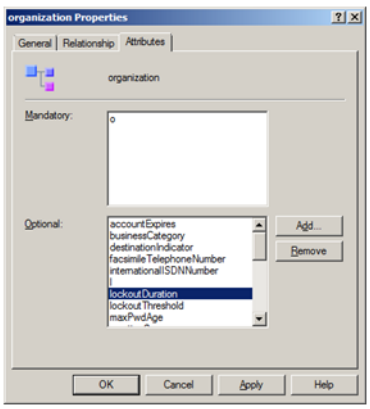
14. klicken Sie auf **Add**

    a) suchen Sie nach `maxPwdAge`

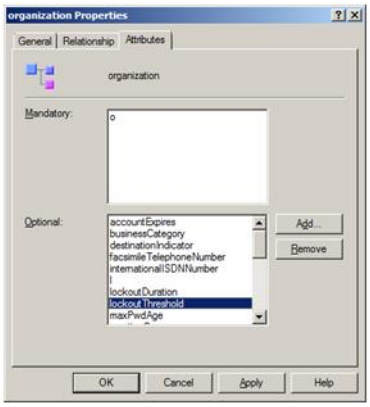
    b) klicken Sie auf **OK**



c) wiederholen Sie diesen Schritt für `lockoutDuration`



d) und für `lockoutThreshold`



15. klicken Sie auf ok

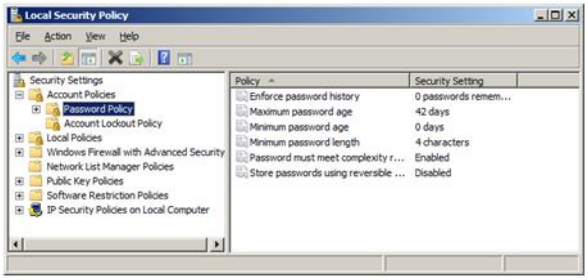
Diese Schritte sind unbedingt nötig, um das `maxPwdAge` in der Organisationseinheit (auf Seite 60) zur Verfügung zu haben, die im Anschluss konfiguriert wird.

- `maxPwdAge` definiert die maximale Zeitspanne, nach der ein benutzer ein Passwort ändern muss.

- `lockoutDuration` definiert den Zeitraum, für den ein Benutzer gesperrt wird, nachdem er sein Passwort mehrmals falsch eingegeben hat.
- `lockoutThreshold` definiert die Anzahl der möglichen Fehlversuche, bevor ein Benutzer für einen bestimmten Zeitraum gesperrt wird.

In den lokalen Sicherheitsrichtlinien des Computers legen Sie die Regeln fest für:

- `password complexity`
- `minimum password length`
- `age`



5.5 Organisationseinheiten, Gruppen und Benutzer konfigurieren

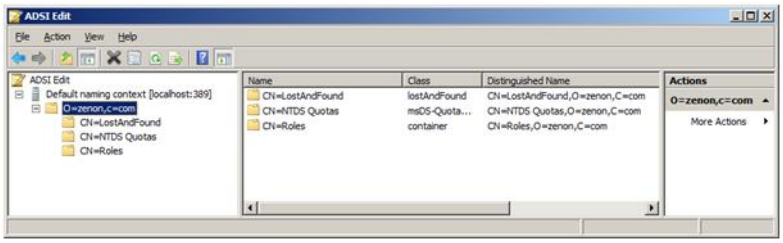
Zur Konfiguration von Organisationseinheiten, Gruppen und Benutzern:

1. öffnen Sie *Start -> Administrative Tools -> ADSI Edit*

2. wählen Sie im Kontextmenü `Connect to...`
3. benutzen Sie folgende Einstellungen (ändern, falls andere Einstellungen zuvor konfiguriert wurden):
   a) `Connection Point`: `o=zenon,c=com`

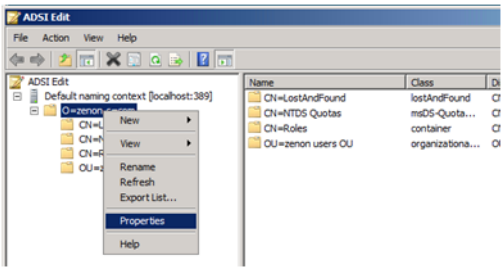
b) `Computer: localhost:389`

Sie sollten jetzt folgende Konfiguration sehen:



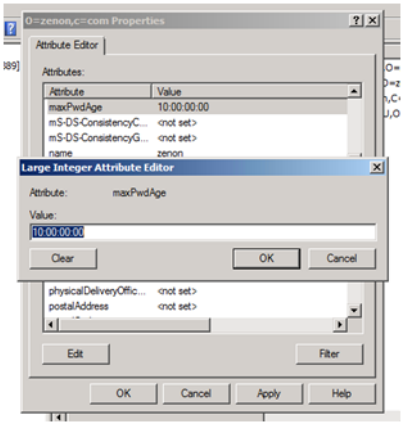
MAXPWDAGE KONFIGURIEREN

1. markieren Sie **`O=zenon,c=com`**
2. klicken Sie auf **`Refresh`**
3. schließen Sie **`ADSI Edit`**
4. öffnen Sie **`ADSI Edit`** erneut
5. markieren Sie **`O=zenon,c=com`**
6. wählen Sie im Kontextmenü **`Properties`**



7. navigieren Sie zu `maxPwdAge`
   a) geben Sie einen gültigen Wert ein

b) Format: `DD:HH:MM:SS` (in unserem Beispiel `10:00:00:00`)

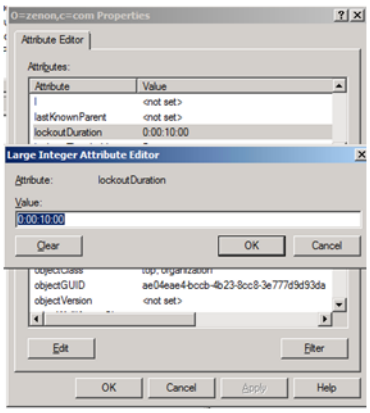


Hinweis: Falls die Eigenschaft `maxPwdAge` nicht sichtbar ist, überprüfen Sie, ob sie korrekt hinzugefügt (auf Seite 52) worden ist. Eventuell beseitigt auch ein Refresh oder das Schließen und Öffnen von **`ADSI Edit`** oder ein Neuladen des Schemas das Problem.

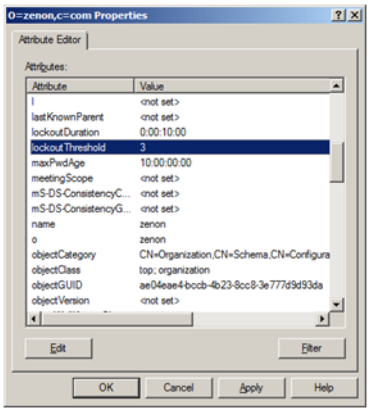
8. navigieren Sie zu `lockoutDuration`

   a) geben Sie einen gültigen Wert ein

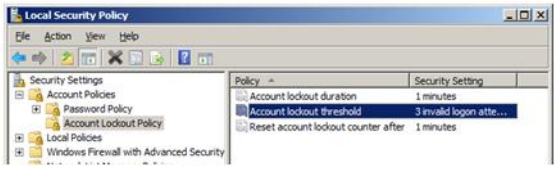
   b) Format: `DD:HH:MM:SS` (in unserem Beispiel `00:00:10:00`, -> 10 Minuten)



9. navigieren Sie zu `lockoutThreshold`



10. geben Sie den gleichen Wert ein, wie in den lokalen Sicherheitsrichtlinien (z. B. `3`)



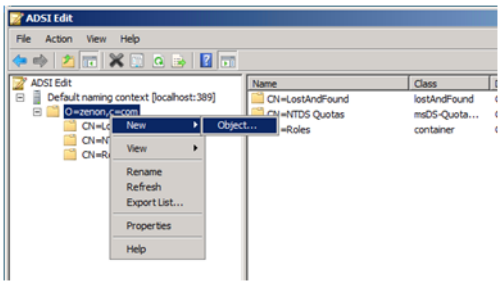
Hinweis: Die Einstellungen für die Dauer der Accountsperre werden in AD LDS ignoriert. Es wird die Eigenschaft `lockoutDuration` (`O=zenon,c=com`) verwendet .

5.5.1 Organisationseinheiten

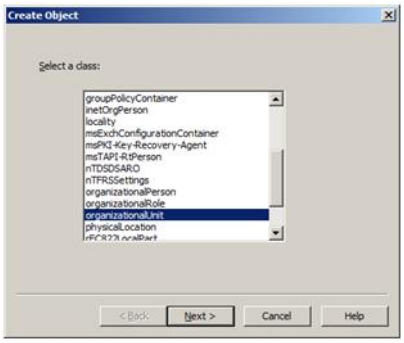
Um eine Organisationseinheit zu erstellen:

1. markieren Sie **`O=zenon,c=com`**

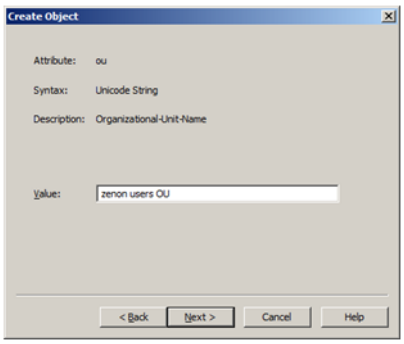
2. wählen Sie im Kontextmenü *New -> Object*



3. wählen Sie **`organizationalUnit`**



4. geben Sie einen Namen ein (in unserem Beispiel: `zenon users OU`)



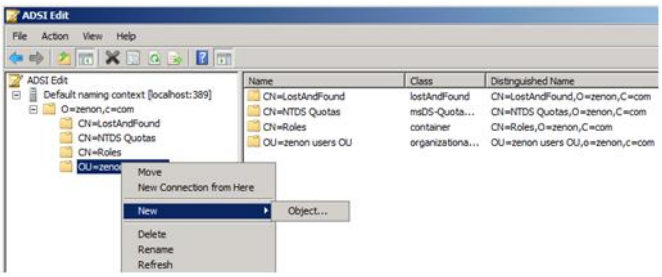
5. klicken Sie auf **`Next`** und dann auf **`Finish`**

5.5.2 Gruppen

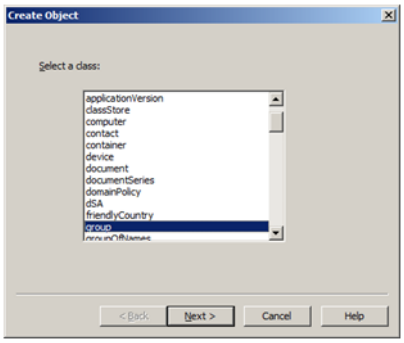
Um eine Gruppe zu erstellen:

1. markieren Sie die Organisationseinheit (auf Seite 60)

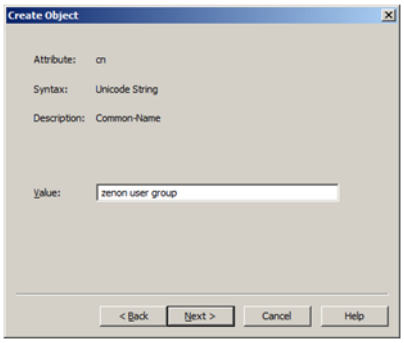
2. wählen Sie im Kontextmenü *New -> Object*



3. wählen Sie **`group`**



4. geben Sie einen Namen ein (in unserem Beispiel: **`zenon user group`**)



5. klicken Sie auf **`Next`**

6. wechseln Sie zur Registerkarte **`Attributes`**

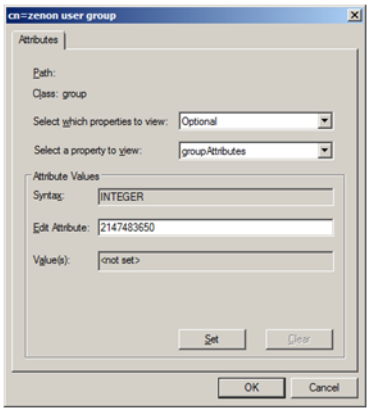
7. klicken Sie auf **`More Attributes`**

   a) navigieren Sie zur Eigenschaft `Select a property to view`

   b) wählen Sie in der Dropdownliste `groupAttributes`

   c) navigieren Sie zu `Edit Attribute`

d) geben Sie den Wert `2147483650` ein (repräsentiert eine **`account group`**)

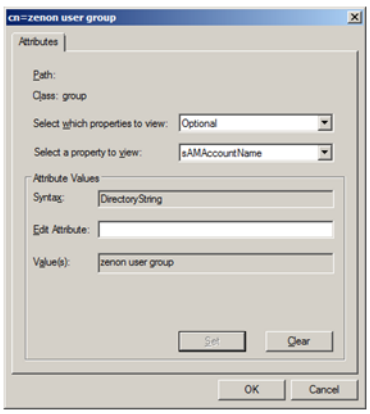


8. klicken Sie auf **`Set`**

9. wählen Sie bei der Eigenschaft `Select a property to view` jetzt `sAMAccountName`

10. geben Sie den gleichen Wert wie für die Gruppe ein (**`zenon user group`**)

Hinweis: Diese Einstellung ist nötig, damit die Benutzergruppen in zenon konfiguriert werden können



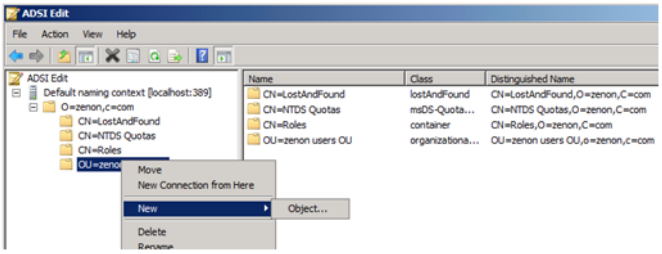
11. Klicken Sie auf **`OK`** und dann auf **`Finish`**

5.5.3 Benutzer

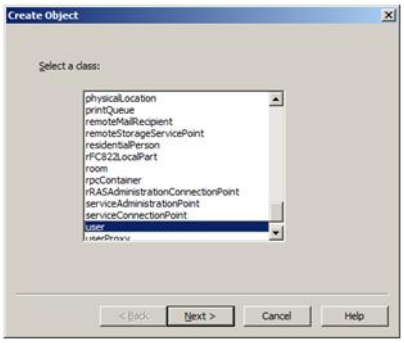
Um einen Benutzer zu erstellen:

1. markieren Sie die Organisationseinheit (auf Seite 60)

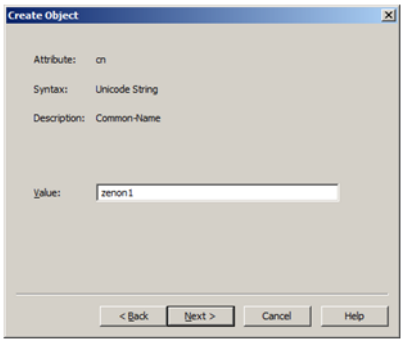
2. wählen Sie im Kontextmenü *New -> Object*



3. wählen Sie die Klasse **`user`**



4. geben Sie einen Namen ein (in unserem Beispiel: **`zenon1`**)



5. klicken Sie auf **`Next`**

6. wechseln Sie zur Registerkarte **`Attributes`**

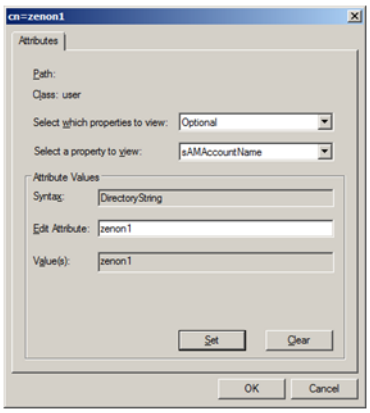
7. klicken Sie auf **`More Attributes`**

   a) navigieren Sie zur Eigenschaft `Select a property to view`

   b) wählen Sie in der Dropdownliste `sAMAccountName`

   c) navigieren Sie zu `Edit Attribute`

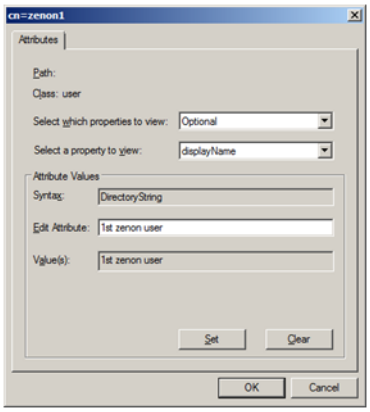
d) geben Sie den gleichen Wert ein wie für den Benutzer (`zenon1`) ein
(Diese Konfoguration ist nötig, damit der benutzer in zenon genutzt werden kann.)



8. klicken Sie auf **`Set`**

9. wählen Sie bei der Eigenschaft `Select a property to view` jetzt `displayName`

10. geben Sie einen Wert für die Anzeige des namens ein, z. B. **`1st zenon user`**



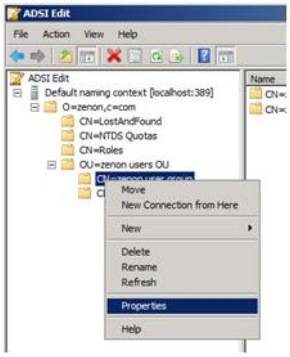
11. klicken Sie auf **`Set`**, dann auf **`OK`** und auf **`Finish`**

BENUTZER ZUR GRUPPE HINZUFÜGEN

Um Benutzer zu einer Gruppe hinzuzufügen:

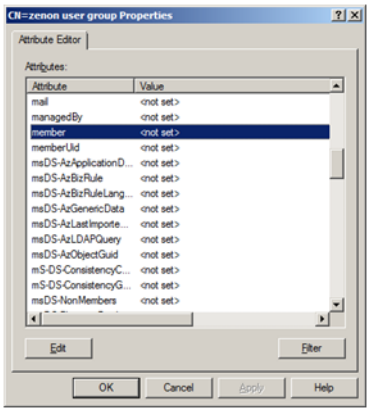
1. wählen Sie **`zenon user group`**

2. wählen Sie im Kontextmenü **`Properties`**



3. markieren Sie **`member`**

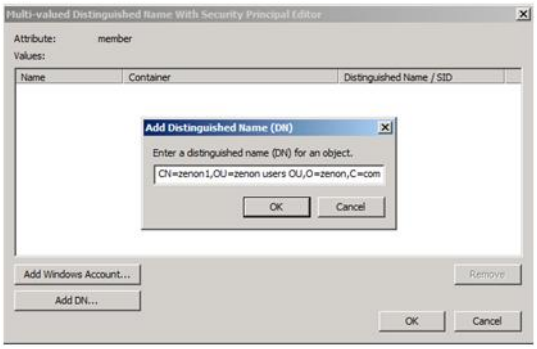
4. klicken Sie auf **`Edit`**



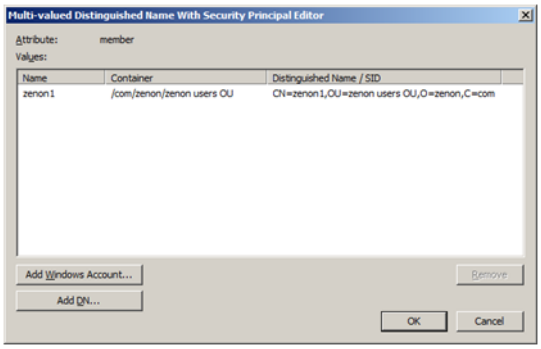
5. um den zuvor erstellten AD LDS Account (**`user`**) hinzuzufügen:

   a) klicken Sie auf **`Add DN...`**

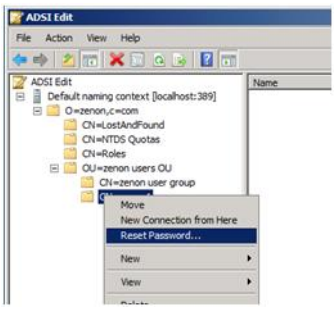
   b) geben Sie in die Eingabemaske ein: `CN=zenon1,OU=zenon users OU,O=zenon,C=com`



c) Sie erhalten als Ergebnis:

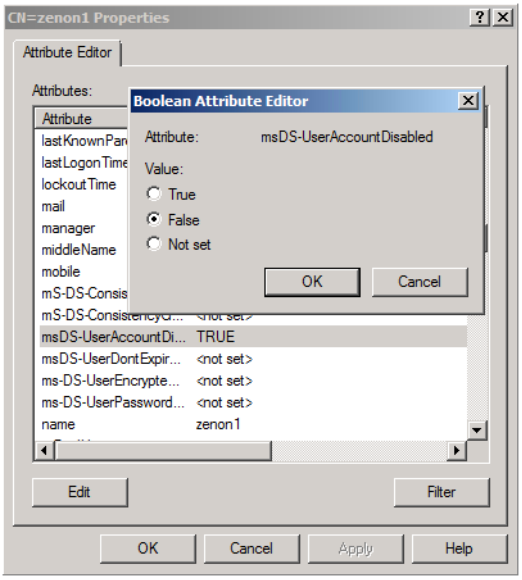


6. definieren Sie ein Passwort für den Benutzer **`zenon1`**



Hinweis: Das Passwort muss die Anforderungen der lokalen Sicherheitsrichtlinien erfüllen

7. setzen Sie für den Benutzer zenon1 die Eigenschaften `set msDS-UserAccountDisabled` auf `False`



Der Benutzer ist jetzt angelegt und kann in zenon verwendet werden.

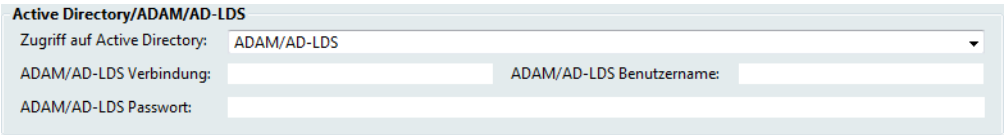
5.6 Verwendung in zenon

Für die Verwendung in zenon konfigurieren Sie erst die Einstellungen im Editor (auf Seite 68) und setzen dann die Benutzerkennung auf AD LDS Ebene zur Runtime (auf Seite 69) ein.

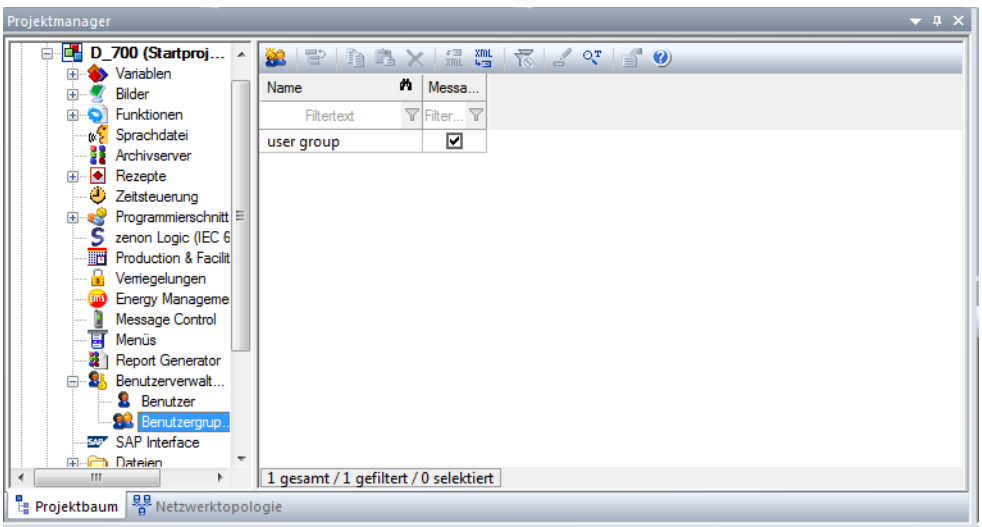
> **Info**
>
> *Active Directory und ADAM/AD LDS stehen unter Windows CE nicht zur Verfügung.*

5.6.1 Editor

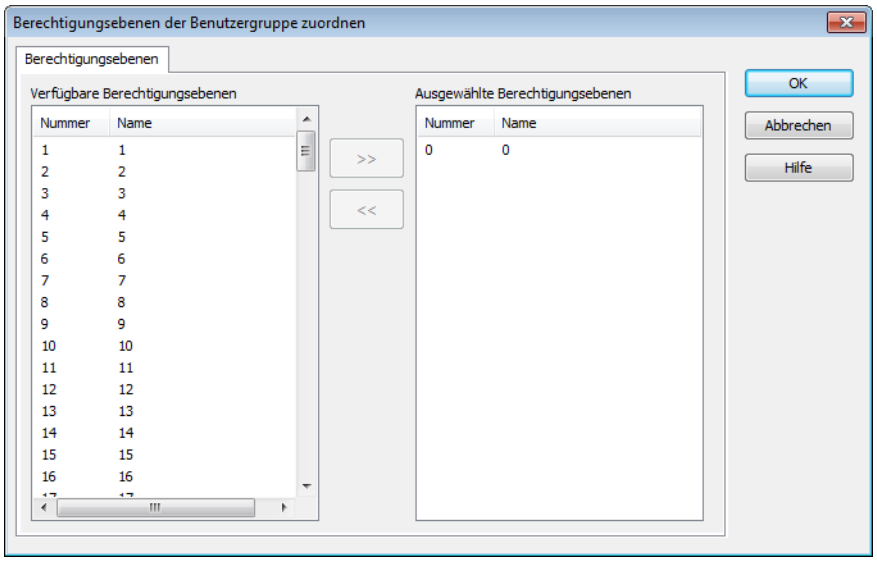
Die Konfiguration erfolgt in den Projekteigenschaften im Abschnitt `Benutzerverwaltung`:



- Eine Benutzergruppe mit dem Namen `zenon user group` wurde erstellt

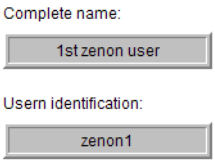


- und Berechtigungsebenen wurden hinzugefügt

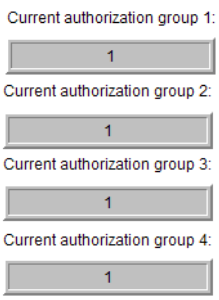


5.6.2 Runtime - Systemtreibervariablen

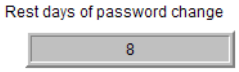
- Der Benutzer zenon1 kann sich in zenon einloggen:



- Der Benutzer erhält seine Berechtigungsebenen von der zenon Gruppe:



- Die restlichen Tage, bis das Passwort geändert werden muss, werden angezeigt (mit einem Tag Unterschied):



FEHLERBEHANDLUNG

Treten zur Runtime Fehler auf, überprüfen Sie ob:

- die Einstellungen korrekt gesetzt wurden:
  - Benutzername
  - `sAMAccountName`
- die Firewall-Einstellungen korrekt gesetzt wurden
- die Editor-Konfiguration korrekt ist für:
  - Verbindung
  - Passwort

Falls der Benutzer keine Berechtigungsebenen von der zenon group bekommt, überprüfen Sie ob:

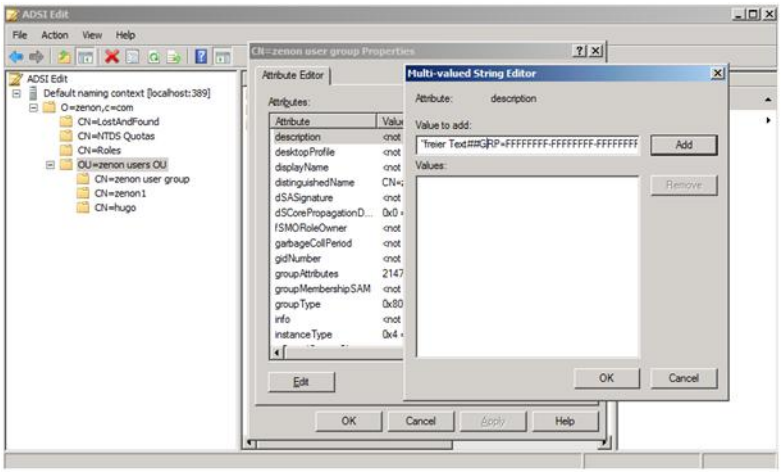
- die Namen übereinstimmen
- sAMAccountName der Gruppe in **AD LDS** gesetzt wurde
- der Benutzer in AD **LDS** zur Gruppe hinzugefügt wurde

AD/ADAM

Wenn Bedienberechtigungen aus der Benutzergruppe in **AD/ADAM** kommen sollen, muss in **AD LDS**:

- bei der Gruppe die Eigenschaft `description` angepasst werden

- die Gruppe genau so wie das Projekt benannt werden



Weitere Informationen zur Konfiguration finden Sie im Abschnitt Setzen der zenon Berechtigungsebenen im Beschreibungsfeld einer Active Directory Gruppe (auf Seite 31).

5.7 AD LDS unter Windows 7 und Windows Vista

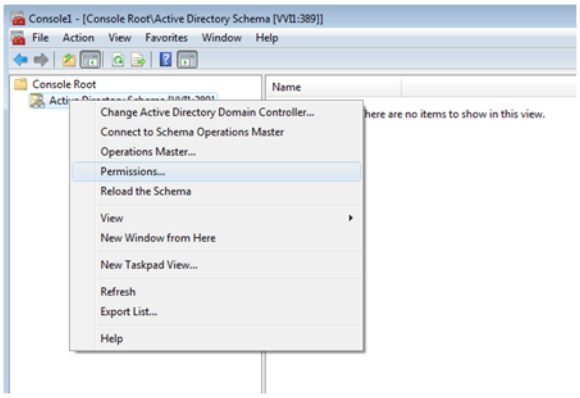
AD LDS kann auch unter Windows Vista und Windows 7 verwendet werden. Die Setups dafür erhalten Sie auf der Microsoft Website http://www.microsoft.com/downloads/en/default.aspx.

Nach der Installation erfolgt die Konfiguration über *Systemsteuerung -> Verwaltung* analog zur Beschreibung für Windows Server 2008 (auf Seite 43).

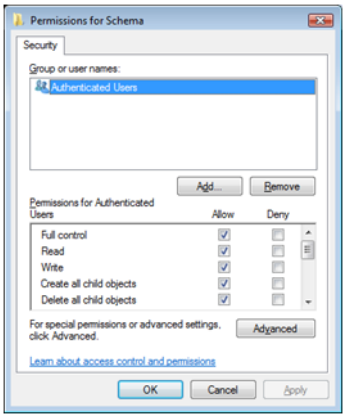
5.7.1 Problembehandlung unter Windows 7 und Windows Vista

Werden nach dem Öffnen des Active Directory Schema Snap-ins keine Inhalte angezeigt, müssen die Zugriffsrechte angepasst werden. Dazu:

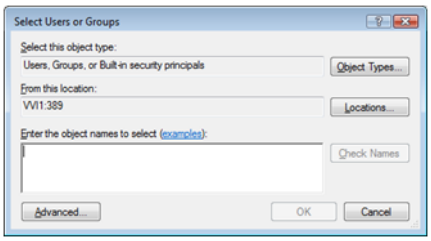
1. wählen Sie im Kontextmenü **Permissions...**



2. ordnen Sie den nötigen Benutzern die entsprechenden Rechte zu (neue Benutzer fügen Sie über Klick auf **Add** hinzu)



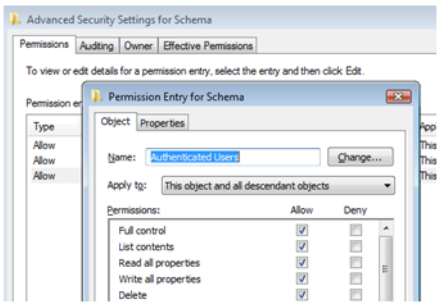
3. klicken Sie auf die Schaltfläche **Advanced**



4. klicken Sie auf die Schaltfläche **Advanced**

5. öffnen Sie die Registerkarte **Permissions**

6. aktivieren Sie die Option `Apply to This object and all descedant objects` für den jeweiligen Benutzer aus



7. schließen Sie die Konsole und öffnen Sie diese erneut (**`mmc /a`**) für die weitere Konfiguration

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

Active Directory Application Mode (ADAM) ist für den Einsatz unter Windows XP gedacht.

Für

- Windows Vista
- Windows 7
- Windows Server 2008

verwenden Sie Active Directory Lightweight Directory Services (auf Seite 43)

VORAUSSETZUNGEN

Um Active Directory Application Mode für zenon verwenden zu können, müssen Sie bei der Konfiguration von ADAM folgende Punkte berücksichtigen.

1. Erstellen Sie eine neue ADAM Instanz (auf Seite 75)
2. Spielen Sie ein AD Schema (auf Seite 78) ein

3. Um dem ADAM Benutzer den Zugriff zu ermöglichen, klicken Sie *Programme -> Verwaltung -> Lokale Sicherheitsrichtlinien*. Im sich öffnenden Dialog klicken Sie *Sicherheitseinstellungen-> Kontorichtlinien*. Hier legen Sie die gewünschten Einstellungen für Kennwortrichtlinien und Kontosperrungsrichtlinien fest.

4. Konfigurieren Sie das ADAM Schema Snap-In (auf Seite 79).

5. Im Snap-In führen Sie unter Klassen -> Organisation einen Rechtsklick aus und selektieren Eigenschaften. Dann geben Sie in der Registerkarte **`Attribute`** als optionales Attribut `maxPwdAge` ein. Dadurch stellen Sie sicher, dass die Kennwortüberprüfung und Kennwortänderung anlaog zum Active Directory funktioniert.

Hinweis: Sie müssen die Gültigkeitsdauer des Passworts in Nanosekunden angeben.

6. Legen Sie in ADAM Benutzer und Benutzergruppe an. Beachten Sie dabei folgende Punkt:
   - Beim Benutzer und bei der Benutzergruppe müssen Sie unter Eigenschaft -> Attribut-Editor beim Attribut `sAMAccountName` nochmals den Namen manuell eintagen.
   - Bei der Benutzergruppe müssen Sie den Namen wie unter Nutzung des Active Directory (auf Seite 29) beschrieben eingeben.
   - Die zenon Berechtigungsebenen legen Sie wie unter Nutzung des Active Directory (auf Seite 29) beschrieben unter dem Attribut `description` an.

> **Info**
>
> *Um den Benutzernamen mithilfe der Systemtreibervariable anzuzeigen, müssen Sie in ADAM beim Benutzer unter Eigenschaften -> Attribut-Editor beim Attribut `displayName` den Benutzernamen manuell setzen.*

6.1 Neue ADAM-Instanz erstellen

SO INSTALLIEREN SIE EINE ADAM-INSTANZ MITHILFE DES ACTIVE DIRECTORY-ANWENDUNGSMODUS-SETUP-ASSISTENTEN

- Klicken Sie zum Starten des Active Directory-Anwendungsmodus-Setup-Assistenten auf Start, zeigen Sie auf Alle Programme und dann auf ADAM, und klicken Sie dann auf ADAM-Instanz erstellen.
- Klicken Sie auf der Seite Willkommen auf Weiter.
- Auf der Seite Setup-Optionen können Sie wählen, ob Sie eine eindeutige ADAM-Instanz installieren oder einem vorhandenen Konfigurationssatz eine neue Instanz zuordnen möchten. Da Sie die erste ADAM-Instanz installieren, klicken Sie auf Eine eindeutige Instanz installieren. Klicken Sie anschließend auf Weiter.
- Geben Sie auf der Seite Instanzname einen Namen für die zu installierende ADAM-Instanz an. Der Name wird auf dem lokalen Computer zur eindeutigen Identifikation der ADAM-Instanz verwendet. Klicken Sie dann auf Weiter.
- Geben Sie auf der Seite Ports die Kommunikationsports an, die von der ADAM-Instanz zur Kommunikation verwendet werden. ADAM kann mithilfe von LDAP (Lightweight Directory Access-Protokoll) oder SSL (Secure Sockets Layer) kommunizieren. Daher müssen Sie für beide Ports einen Wert angeben. Klicken Sie dann auf Weiter.

> **Info**
>
> *Wird auf dem Computer, auf dem Sie ADAM installieren, einer der Standardports bereits verwendet, wird vom Active Directory-Anwendungsmodus-Setup-Assistenten automatisch nach dem ersten verfügbaren Port gesucht, beginnend mit 50000. Beispielsweise werden von Active Directory die Ports 389 und 636 sowie die Ports 3268 und 3269 auf globalen Katalogservern verwendet. Daher werden beim Installieren von ADAM auf einem Domänencontroller die Standardwerte 50000 für den LDAP-Port und 50001 für den SSL-Port bereitgestellt.*

- Auf der Seite Anwendungsverzeichnispartition können Sie eine Anwendungsverzeichnispartition (oder einen Namenskontext) erstellen, indem Sie auf Ja, eine Anwendungsverzeichnispartition erstellen klicken. Wenn Sie stattdessen auf Nein, keine Anwendungsverzeichnispartition erstellen klicken, müssen Sie nach der Installation manuell eine Anwendungsverzeichnispartition

erstellen. Wenn Sie eine Anwendungsverzeichnispartition erstellen, müssen Sie einen definierten Namen für die neue Partition angeben. Klicken Sie dann auf Weiter.

> **Info**
>
> *ADAM unterstützt definierte Namen im X.500- und im DNS-Stil (Domain Name System) für Verzeichnispartitionen der obersten Ebene.*

- Auf der Seite Dateipfade können Sie die Installationsverzeichnisse für ADAM-Daten- und Wiederherstellungsdateien (Protokolldateien) anzeigen und ändern. Standardmäßig werden ADAM-Daten- und Wiederherstellungsdateien unter %ProgramFiles%\Microsoft ADAM\Instanzname\data gespeichert. Dabei stellt Instanzname den ADAM-Instanznamen dar, den Sie auf der Seite Instanzname angeben. Klicken auf Weiter, um die Standardpfade zu übernehmen.

> **Info**
>
> *Beim Installieren von ADAM auf einem Computer unter Windows XP müssen Sie diese Dateien auf demselben logischen Volume installieren. Beim Installieren von ADAM unter Windows Server 2003 und Windows Server 2003 R2 in einer Produktionsumgebung wird empfohlen, die Dateien auf separaten physikalischen Datenträgern zu installieren.*
>
> *Programmdateien und Verwaltungsprogramme werden von ADAM in %windir%\ADAM installiert.*

- Auf der Seite Dienstkontoauswahl wählen Sie ein Konto aus, das als Dienstkonto für ADAM verwendet wird. Das ausgewählte Konto bestimmt den Sicherheitskontext, in dem die ADAM-Instanz ausgeführt wird. Wenn Sie ADAM nicht auf einem Domänencontroller installieren, wird standardmäßig das Netzwerkdienstkonto vom Active Directory-Anwendungsmodus-Setup-Assistenten verwendet. Klicken Sie auf Weiter, um die Standardeinstellung Netzwerkdienstkonto zu übernehmen. Beim Installieren von ADAM auf einem Domänencontroller klicken Sie stattdessen auf Dieses Konto und wählen dann ein Domänenbenutzerkonto als ADAM-Dienstkonto aus.

Info

Sie können das ADAM-Dienstkonto nach der Installation von ADAM mit dem Befehlszeilenprogramm dsmgmt ändern. Beim Installieren von ADAM auf einem Domänencontroller müssen Sie ein Domänenbenutzerkonto als ADAM-Dienstkonto auswählen.

- Auf der Seite ADAM-Administratoren wählen Sie einen Benutzer oder eine Gruppe als Standardadministrator für die ADAM-Instanz aus. Der ausgewählte Benutzer oder die ausgewählte Gruppe verfügt über vollständige Verwaltungsfunktionalität für die ADAM-Instanz. Standardmäßig wird vom Active Directory-Anwendungsmodus-Setup-Assistenten der aktuell angemeldete Benutzer angegeben. Sie können diese Auswahl in jedes lokale Konto oder Domänenkonto bzw. in jede Gruppe im Netzwerk ändern. Klicken Sie auf den Standardwert Zurzeit angemeldeter Benutzer, und klicken Sie dann auf Weiter.
- Auf der Seite Importieren von LDIF-Dateien können Sie zwei LDF-Dateien mit Benutzerklassen-Objektdefinitionen in das ADAM-Schema importieren. Das Importieren dieser Benutzerklassen-Objektdefinitionen ist optional.
  - Klicken Sie auf Die ausgewählten LDIF-Dateien für diese ADAM-Instanz importieren.
  - Klicken Sie auf MS-InetOrgPerson.LDF und dann auf Hinzufügen.
  - Klicken Sie auf MS-User.LDF und dann auf Hinzufügen.
  - Klicken Sie auf MS-UserProxy.LDF, auf Hinzufügen und dann auf Weiter.
- Auf der Seite Installationsbereit können Sie die ausgewählten Installationsoptionen überprüfen. Wenn Sie auf Weiter klicken, beginnt der Active Directory-Anwendungsmodus-Setup-Assistent mit dem Kopieren von Dateien und mit der Installation von ADAM auf dem Computer.
- Wenn der Active Directory-Anwendungsmodus-Setup-Assistent die Installation von ADAM erfolgreich abgeschlossen hat, wird die folgende Meldung angezeigt: "Der Active Directory-Anwendungsmodus-Setup-Assistent wurde erfolgreich abgeschlossen." Wenn die Seite Fertigstellen des Assistenten angezeigt wird, klicken Sie auf Fertig stellen, um den Assistenten zu schließen.

Info

Wird der Active Directory-Anwendungsmodus-Setup-Assistent nicht erfolgreich abgeschlossen, wird auf der Seite Zusammenfassung eine Fehlermeldung mit dem Grund für den Fehler angezeigt.

- Wenn im Active Directory-Anwendungsmodus-Setup-Assistenten ein Fehler auftritt, bevor die Seite Zusammenfassung geöffnet wird, können Sie die angezeigte Fehlermeldung überprüfen. Darüber hinaus können Sie auf Start und dann auf Ausführen klicken und einen der folgenden Dateinamen eingeben:
  %windir%\Debug\Adamsetup.log
  %windir%\Debug\Adamsetup_loader.log
  Die Dateien %windir%\Debug\Adamsetup.log und %windir%\Debug\Adamsetup_loader.log enthalten nützliche Informationen zur Problembehandlung bei ADAM-Setup-Fehlern.

6.2 AD-Schema einspielen

So verwenden Sie erstmalig das Active Directory/ADAM-Synchronisierungsprogramm

- Klicken Sie auf **Start**,
- öffnen Sie **Alle Programme**,
- klicken Sie auf **ADAM** und
- dann auf **ADAM-Verwaltungsprogramme**:

ein Befehlsfenster im ADAM-Verzeichnis öffnet sich.

Zum Erweitern des ADAM-Schemas auf die Standardschemaobjekte von Windows Server in Active Directory:

- geben Sie in der Eingabeaufforderung den folgenden Befehl in einer Zeile ein:

```
ldifde -i -s localhost -c CN=Configuration,DC=X #ConfigurationNamingContext -f MS-AdamSchemaW2k3.ldf
```

- Drücken Sie die Eingabetaste.

6.3 ADAM-Schema Snap-in konfigurieren

KONFIGURIEREN DES VERWALTUNGSPROGRAMMS ADAM-SCHEMA SNAP-IN

Mit einem weiteren ADAM-Verwaltungsprogramm, dem ADAM-Schema Snap-In, können Sie das ADAM-Schema verwalten. Wenn Sie das Active Directory-Schema-Snap-In bereits verwendet haben, sollte Ihnen das ADAM-Schema Snap-In bekannt vorkommen. Bevor Sie das ADAM-Schema Snap-In verwenden können, müssen Sie eine MMC-Datei dafür erstellen, wie in diesem Verfahren beschrieben.

- Klicken Sie auf Start, auf Ausführen, geben Sie mmc /a ein, und klicken Sie anschließend auf OK.
- Klicken Sie im Menü Datei auf Snap-In hinzufügen/entfernen, und klicken Sie dann auf Hinzufügen.
- Klicken Sie in Verfügbare eigenständige Snap-Ins auf ADAM-Schema, auf Hinzufügen, auf Schließen, und klicken Sie dann auf OK.
- Klicken Sie zum Speichern dieser Konsole im Menü Datei auf Speichern.
- Geben Sie in Dateiname Folgendes ein, und klicken Sie dann auf Speichern: %windir%\system32\adamschmmgmt.msc
- Stellen Sie über das ADAM-Schema Snap-In eine Verbindung mit der ADAM-Instanz her. Dazu klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf ADAM-Schema, klicken Sie auf ADAM-Server ändern. Geben Sie `localhost` bei ADAM-Server und `389` bei Port ein.
- Klicken Sie auf OK. Das ADAM-Schema Snap-In sieht jetzt wie folgt aus. Sie können die Klassen und Attribute des ADAM-Schemas durchsuchen und anzeigen.
- Führen Sie zum Erstellen einer Verknüpfung für das ADAM-Schema-Snap-In im Menü Start folgende Aktionen aus:
  - Klicken Sie mit der rechten Maustaste auf Start, klicken Sie auf Öffnen – Alle Benutzer, doppelklicken Sie auf den Ordner Programme, und doppelklicken Sie dann auf den Ordner ADAM.
  - Zeigen Sie im Menü Datei auf Neu, und klicken Sie dann auf Verknüpfung.
  - Geben Sie im Assistenten zum Erstellen von Verknüpfungen in Geben Sie den Speicherort des Elements ein die Zeichenfolge adamschmmgmt.msc ein, und klicken Sie dann auf Weiter.

- Geben Sie auf der Seite Programmbezeichnung auswählen in Geben Sie den Namen für die Verknüpfung ein den Namen ADAM-Schema ein, und klicken Sie dann auf Fertig stellen.

7. Bedienen zur Runtime

Jeder Benutzer hat zur Runtime die Möglichkeit, sein eigenes Passwort zu editieren. Er kann jedoch keinen anderen Benutzer editieren. Dies kann nur der Administrator. Änderungen zur Runtime müssen in den Editor zurückgelesen werden, um dort zur Verfügung zu stehen. Beachten Sie beim Übertragen von Runtime-Dateien die Eigenschaft `RT änderbare Daten`. Hier wird festgelegt, ob die Projektierung der Benutzerverwaltung zur Runtime übertragen wird und die Konfiguration in der Runtime überschreibt.

Der Administrator kann über die Funktion **`Benutzer ändern`**:

- neue Benutzer anlegen
- vorhandene Benutzer ändern (ausgenommen Benutzername für Anmeldung)
- Benutzergruppen anlegen, ändern und löschen

  Legt ein Administrator zur Runtime eine neue Benutzergruppe an, wird er automatisch Mitglied dieser Gruppe.

- Berechtigungsebenen vergeben

  Der Administrator kann nur Berechtigungsebenen vergeben, die er selbst besitzt. Damit wird verhindert, dass sich ein Administrator das System komplett freischaltet.

Hinweis: Benutzer und Benutzergruppen aus dem Editor-Globalprojekt werden zur Runtime mit den Benutzern und Benutzergruppen des Projekts zusammengeführt. Sie können daher zur Runtime weder editiert, noch in den Editor zurückgelesen werden.

Achtung

Konformität mit FDA 21 CFR Part 11:

- Weder Benutzer noch Administrator können zur Runtime den Benutzernamen ändern.
- Das Löschen von Benutzern kann in den Projekteigenschaften mit der Eigenschaft `Löschen von Benutzern` in der Gruppe `Benutzerverwaltung` unterbunden werden.

LOGIN

Nach dem Starten der Runtime ist der aktuelle Benutzer `SYSTEM` mit der freigegebenen Bedienebenen `LEVEL 0` angemeldet.

Beim Einloggen in der Runtime gibt es folgende Sicherheitsvorkehrungen:

- Passwort

  Bei einer dreimaligen Falscheingabe des Passwortes erfolgt eine Sperre des Benutzers und er wird automatisch ausgeloggt. Das System ist somit für diesen Benutzer für alle Elemente die einen höhere Berechtigungsebene als `0` verlangen, unbedienbar. Er kann also keine mit einem Benutzerlevel verbundenen Bedienaktionen mehr durchführen.
  Folgende Meldung wird angezeigt:

  Der Administrator muss dann den entsprechenden Benutzer wieder freischalten (Eigenschaft **`Gesperrt`** deaktivieren).

  Der Benutzername des Benutzers, der sich fälschlicherweise versucht einzuloggen, wird in der Chronologischen Ereignisliste protokolliert.

- Benutzername

  Bei Eingabe eines nicht existierenden Benutzernamens oder bei leerem Passwortfeld wird die Fehlermeldung "**`Ungültiger Benutzername`**" ausgegeben. Nach drei Fehleingaben wird das System für alle Elemente die eine höhere Berechtigungsebene als `0` verlangen, gesperrt. Kein Benutzer ist damit in der Lage, mit einer Benutzerebene geschützte Bedienaktionen durchführen. Eine Aufhebung dieser Sperre kann nur durch den Administrator erfolgen.

  Der Benutzername des Benutzers, der sich fälschlicherweise versucht einzuloggen, wird in der Chronologischen Ereignisliste als Ereignis für den aktuell eingeloggten Benutzer protokolliert.

- Einloggen nach Deaktivierung

  Ist ein Benutzer deaktiviert und versucht sich dennoch einzuloggen, ist ein Einloggen nicht möglich. Dieser Versuch wird in der Chronologischen Ereignisliste protokolliert.

PASSWORT

Der jeweilige Benutzer ist der einzige, der Kenntnis über sein Passwort besitzt. Er ist auch der einzige, der sein Passwort ändern kann. Nachdem dem Benutzer ein Passwort durch den Administrator zugeteilt worden ist, muss der Benutzer beim erstmaligen Login sein Passwort neu festlegen. Damit wird sichergestellt, dass kein Administrator ein Benutzerpasswort kennt und dadurch falsche Signaturen auslöst. (Wichtig für FDA 21 CFR Part 11).

Wenn ein Benutzer sein Passwort vergisst, kann der Administrator das Passwort löschen und ein neues Initialpasswort vergeben. Der Administrator benötigt für diese Interventionen keine Kenntnis des Passwortes. Beim nächsten Einloggen muss der entsprechende Benutzer das Passwort wieder ändern.

Nähere Informationen zu geänderten Runtime-Dateien finden Sie im Kapitel: Projekt und Arbeitsbereich/RT änderbare Dateien

Achtung

Login über Bild vom Typ ***`Login`****: Wird bei einer Anmeldung über ein Bild vom Typ* ***`Login`*** *(auf Seite 88) für einen gültigen Benutzer kein Passwort eingegeben, erhalten Sie keine Fehlermeldung. Der Benutzer wird nicht eingeloggt. Das System wird auch nach dreimaligem Anmeldeversuch mit leerem Passwort nicht gesperrt.*

Bei Eingabe eines falschen Passwortes und/oder eines nicht existierenden Benutzernamens wird das System wie gewohnt nach drei Versuchen gesperrt.

7.1 Permanentes und temporäres Login

Benutzer können permanent oder temporär eingeloggt werden.

PERMANENTES LOGIN

Das permanente Login erfolgt über die Funktion (auf Seite 84) `Login mit Dialog` oder über die Funktion (auf Seite 85) `Login ohne Passwort`. Der Benutzer ist damit permanent angemeldet und kann alle Bedienhandlungen durchführen, für die er berechtigt (auf Seite 16) ist. Bei Handlungen, für die er keine Bedienberechtigung besitzt, wird eine entsprechende Meldung angezeigt.

Tipp: Für eingeloggte Benutzer können mit Passwort geschützte Text-Buttons auf unsichtbar gesetzt werden. Dazu muss die Eigenschaft `Gesperrte Buttons` (`Projekteigenschaften` -> `Benutzerverwaltung` -> `Temporäres Login`) aktiviert werden.

Hinweis: Temporäres Einloggen ist für eingeloggte Benutzer nicht möglich. Damit erhalten eingeloggte Benutzer bei Funktionen, für die sie keine ausreichende Berechtigung besitzen, keinen Dialog zur Anmeldung eines temporären Logins.

TEMPORÄRES LOGIN

Ist für einen nicht eingeloggten Benutzer eine Bedienhandlung nötig, die eine Authentifizierung erfordert, kann er temporär eingeloggt werden. Dazu muss in den Projekteigenschaften die Eigenschaft `Temp. Login aktiv` (-> `Benutzerverwaltung` -> `Temporäres Login`) aktiv geschaltet sein.

Login zur Runtime:

- beim Ausführen einer passwortgeschützen Funktion wird der Dialog zum Login geöffnet
- der Benutzer kann sich einloggen und entsprechend seinen Rechten die Bedienhandlung ausführen oder er erhält eine Meldung über fehlende Rechte
- der Benutzer wird sofort nach der Bedienhandlung automatisch ausgeloggt

Info

Temporäres Login:

- ist nur bei einer Funktionsausführung wirksam
- unterstützt Schalter, aber keine Taster
- ist für permanent eingeloggte Benutzer deaktiviert

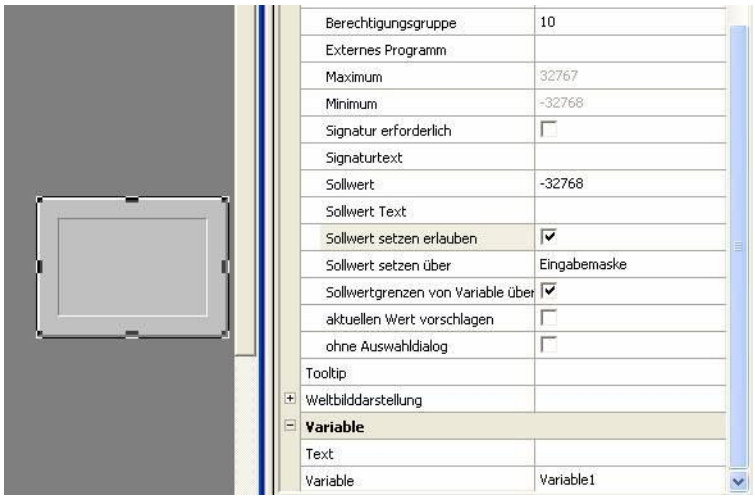
7.2 Passwortschutz im dynamischen Element

Zur Laufzeit können alle Dynamische Bildelemente, die eine Funktionsausführung bzw. eine Sollwert absetzen - Funktion erlauben, mit einer Berechtigungsgruppe verknüpft werden.

Legen Sie dazu ein dynamisches Element an. Beispielsweise einen Textbutton. Nun erscheinen im Eigenschaften-Fenster alle projektierbaren Eigenschaften für dieses dynamische Element.

Selektieren Sie bei den Eigenschaften in der Gruppe 'Benuzter' die Eigenschaft '`Berechtigungsgruppe`'. Hier können Sie die zur Funktionsausführung nötige Berechtigungsgruppe einstellen.

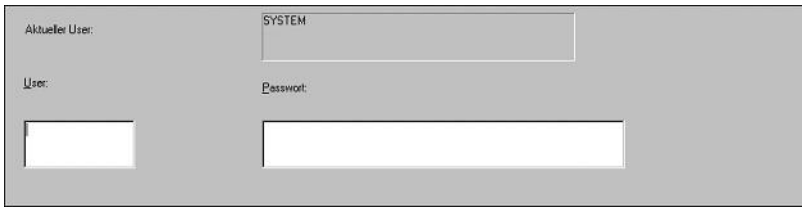
Bei dynamischen Elementen, bei denen eine Sollwertaktion geschützt werden soll, muss zuerst über das Eigenschaften-Fenster eine Variable verknüpft und das Sollwert Setzen aktiviert werden, bevor die Berechtigungsgruppe eingestellt werden kann.



7.3 Passwort - Funktionen

7.3.1 Login mit Dialog

Dieser Funktion öffnet zur Runtime die Login-Maske für ein erneutes Anmelden an zenon.



Die Anmeldung wird in der Chronologische Ereignisliste protokolliert.

Für den Login kann auch ein Bild vom Typ Login (auf Seite 88) verwendet werden.

GRÖßE UND POSITION

Größe und Position des Anmeldefensters zur Runtime können in der **zenon6.ini** festgelegt werden:

1. öffnen Sie die zenon 6.ini
2. erstellen oder modifizieren Sie den Bereich:

   [Befehlsgabe]

3. tragen Sie die Werte ein für

   POSITION= links, rechts, oben, unten

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

Achtung: Die Größe bezieht sich auf die Bildgröße und nicht auf die Größe der Hauptfensters.

> **Info**
>
> *Die zenon6.ini finden Sie im Pfad:*
>
> *Windows Vista/7:* `C:\ProgramData\COPA-DATA\System\`
>
> *Windows XP:* `C:\Dokumente und Einstellungen\All users\Anwendungsdaten\COPA-DATA\System`

7.3.2 Login ohne Passwort

Diese Funktion ermöglicht es, zur Runtime einen Benutzer an zenon ohne Passworteingabe anzumelden. Dafür wird der Benutzer direkt benannt oder per Chip Ident System angemeldet. Der Funktionsaufruf kann über ein Ereignis (Meldungszustand von Schlüsselschalter) oder die Zeitsteuerung ausgelöst werden. In der Chronologische Ereignisliste wird das Anmelden protokolliert.

Um die Funktion Login ohne Passwort anzulegen:

- legen Sie eine neue Funktion an
- navigieren Sie zum Knoten Benutzerverwaltung

- wählen Sie Login ohne Passwort
- der Dialog zur Auswahl des Benutzers öffnet sich
- wählen Sie die Art des Logins

Parameter	Beschreibung
`Benutzer direkt`	Meldet den ausgewählten Benutzer an.
`Benutzer aus Variable`	Meldet den Benutzer mit dem Benutzernamen aus der übergebenen Variablen an. Ermöglicht die Anmeldung über ein Chip Ident System. Klick auf die Schaltfläche ... öffnet den Dialog zur Auswahl einer String-Variablen. Details siehe Absatz "Anmeldung über Chip Ident System".

ANMELDUNG ÜBER CHIP IDENT SYSTEM

Die Anmeldung `Benutzer aus Variable` ermöglicht die Nutzung von Chip Ident Systemen wie z. B. Euchner oder Keba Identsystem. Um Die Anmeldung über eine Variable zu nutzen, beachten Sie:

- Der Benutzer muss in der zenon Benutzerverwaltung oder im Active Directory mit dem gleichen Benutzernamen wie im Chip angelegt sein.

zum Beispiel: Benutzername im Chip ist J. Smith, dann muss in der Benutzerverwaltung oder im Active Directory ein J. Smith mit entsprechenden Rechten existieren.

- Hält der Benutzer seinen Chip vor den Chipleser wird die String-Variable (z.B. `username`) mit den Daten des Chips befüllt (z. B. J. Smith) und der Benutzer angemeldet.
- Damit die Funktion ausgeführt wird, muss eine **`Reaktionsmatrix`** vom Typ `String` existieren, die auf jede Wertänderung reagiert und die Funktion ausführt.
  - Diese Rema muss mit der Variablen (z.B. username) verknüpft sein.

7.3.3 Logout

Mit der Verwendung dieser Funktion wird im Onlinebetrieb (Runtime) der aktuelle Benutzer abgemeldet und der Benutzer SYSTEM mit dem Bedienlevel 0 angemeldet. In der Chronologische Ereignisliste wird das Anmelden des Systembenutzers protokolliert.

Es sind keine Übergabeparameter notwendig.

Achtung

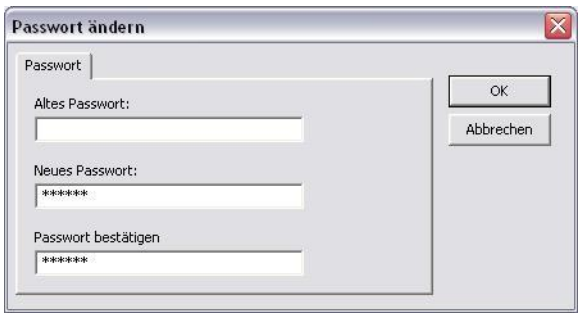
Automatischer Logout vs. Automatische Funktion:

- `Automatischer Logout`: Passiert `permanent` ab dem Ablauf der Zeit der letzten Bedienungsaktion.
- `Automatische Funktion`: Passiert `nur ein Mal` ab dem Ablauf der Zeit der letzten Bedienungsaktion.

7.3.4 Passwort ändern

Mit der Verwendung dieser Funktion kann der angemeldete Benutzer sein aktuelles Passwort im Onlinebetrieb (Runtime) ändern. Für die systeminternen Benutzer ist keine Änderung möglich. Die Funktion wird nicht ausgeführt.

Im Onlinebetrieb wird eine Eingabemaske aufgeschaltet.



Die notwendigen Eingaben sind

Parameter	Beschreibung
altes Passwort	aktuelles Passwort eingeben
neues Passwort	neues Passwort eingeben
Sicherheitsabfrage	Sicherheitsabfrage für das neue Passwort

Wurde dem Benutzer kein Passwort zugewiesen, kann er es sich im Onlinebetrieb beim ersten Aufruf der Funktion selbst definieren. In der Maske wird kein altes Passwort abgefragt.

7.4 Löschen eines Benutzers

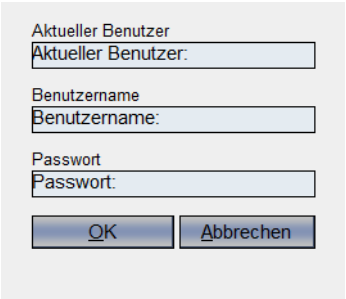
Selektieren Sie den zu löschenden Benutzer in der Listenansicht und öffnen Sie mit einem rechten Mausklick das Kontextmenü. Gehen Sie auf **Löschen** und bestätigen Sie auch die zusätzliche Sicherheitsabfrage.

7.5 Bild vom Typ Login

Mit der Verwendung eines Bildes für das Einloggen ist die individuelle Gestaltung eines Login-Fensters möglich. (Nähere Informationen zu den vordefinierten Bildtypen finden Sie im 'Bilder / Vordefinierte Bildtypen'.)

Das Anlegen des Login-Bildes im Editor erfolgt durch Definition eines neuen Bildes der Bildtyp **Login**.

Nach dem Öffnen des Bildes wird ein leeres Bild aufgeschaltet und in der Menüzeile wird die Dropdownliste **Kontrollelemente** gefüllt.



Kontrollelemente:

Kontrollelement	Beschreibung
Aktueller Benutzer	Beschriftung Aktueller Benutzer
Anzeige - Aktueller Benutzer	Anzeige des aktuell angemeldeten Benutzers
Kennung	Beschriftung Benutzername
Eingabe Kennung	Eingabebereich für Benutzername
Passwort	Beschriftung Passwort
Eingabe Passwort	Eingabebereich für das Passwort
OK	Schaltfläche zum Einloggen und Schließen des Fensters
Abbruch	Schaltfläche für Abbruch
Login	Schaltfläche zum Einloggen ohne Schließen des Fensters

LOGIN

Beim Einloggen in der Runtime gilt:

- Nach dreimaliger Falscheingabe des Passwortes, wird der Benutzer für das System gesperrt. Diese Sperre kann nur ein Administrator aufheben.
- Nach dreimaliger Falscheingabe eines Benutzernamens wird das System gesperrt. Das System ist für keinen Benutzer mehr bedienbar und muss von einem Administrator wieder frei geschaltet werden.

- Wird bei der Anmeldung ein korrekter Benutzername angegeben, aber das Passwortfeld leer gelassen, erfolgt keine Reaktion. Das System wird nicht gesperrt.

Details siehe Kapitel **Bedienen zur Runtime** (auf Seite 80).