Sicherheitseinstellungen

ESO9 international a.s.
U Mlýna 2305/22, 141 Praha 4 – Záběhlice
tel.: +420 585 203 370-2
e-mail: info@eso9.cz
www.eso9.cz

Zpracoval:	Tomáš Urych
Dne:	28.7.2021
Revize:	Urych Tomáš
Dne:	29.7.2021

Table of contents

1. Sicherheitseinstellungen

Für die richtige Einstellung müssen Sie die Einstellungen in ESO9 Správce mit den Einstellungen in ESO9 kombinieren.

1.1 ESO9 Správce

Für die ausgewählte Applikation werden die Sicherheitseinstellungen auf den Registerkarten Eigenschaften, Sicherheit, Benutzer und Passwörter vorgenommen.

1.1.1 Eigenschaften

- Durch Anhaken „**ESO9 Benutzer anfordern“** wird der Zugriff für diejenigen Benutzer gesperrt, die nicht in der Datenbank sind, mit der die Applikation verbunden ist oder bei denen der **Zugriff** auf ESO9 (Benutzer) **deaktiviert** ist.
- Abhängig von der **Authentifizierungsmethode** wird die Authentifizierungsmethode der Benutzer bestimmt (der Administrator stellt auch die Authentifizierungsmethoden in **IIS** ein).
    - Extern (NT) – für die Anmeldung werden der Domänenname und das Passwort verwendet, womit sich der Benutzer bei Windows anmeldet
    - ESO9
    - Zertifikate
- Abhängig von der **Sicherheitsart** werden Vorlagen geprüft (Objekte – Formulare und Zusammensetzungen):
    - Nicht prüfen
    - Nur angegebene Vorlagen prüfen
    - Alle Vorlagen prüfen

1.1.2 Sicherheit

Wenn in der **Eigenschaft – Sicherheitsart „Nur angegebene Vorlagen überprüfen“** eingestellt ist, wird hier durch Anhaken bestimmt, welche Vorlagen (Objekte) überprüft werden sollen.

ACHTUNG, die Sicherheitsprüfung wird nur in dem Fall durchgeführt, wenn **in der Applikation ESO9** die Eigenschaft **„Sicherheit prüfen“** auf „JA“ eingestellt ist.

1.1.3 Benutzer und Passwörter

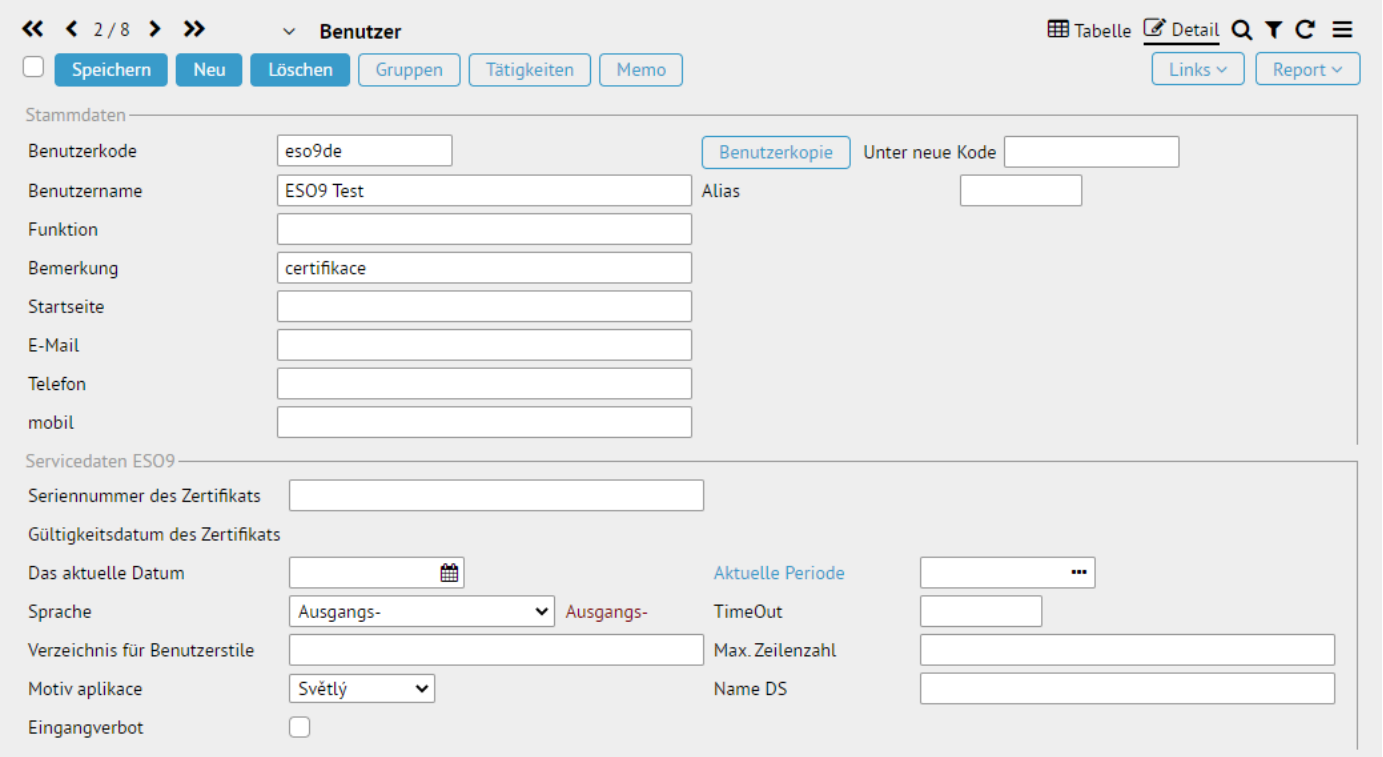
Es hat eine besondere Bedeutung für die Validierung von ESO9.

- Zeigt den Code und Benutzername und sein Passwort.
- Nur hier ist es möglich, dem Benutzer das Passwort einzustellen (oder abzubrechen) und auszuwählen, ob das Passwort von dem Benutzer bei dem ersten Eintritt geändert werden muss oder nicht.

1.2 ESO9 Applikation

1.2.1 Benutzer (9.1.5)

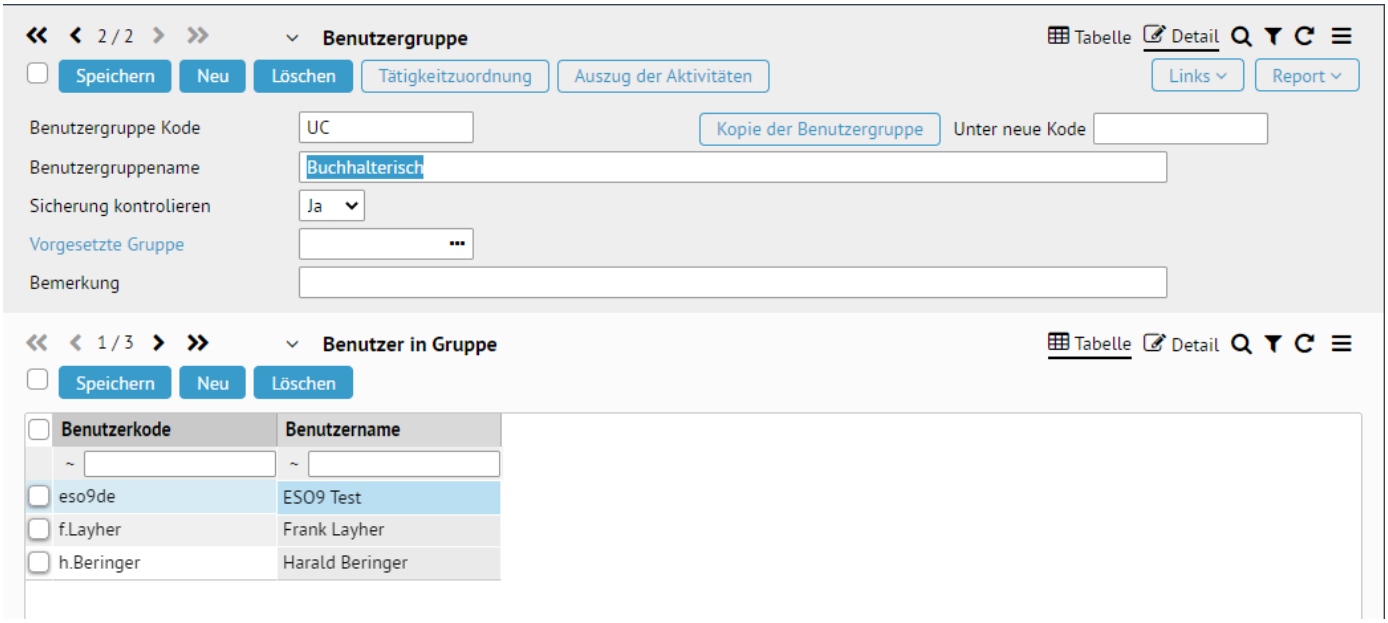
Es handelt sich um eine Schlüsselliste, durch die die Benutzer auf das System zugreifen können.



- Wenn die Authentifizierungsmethode **Extern (NT)** im Administrator eingestellt ist, muss der Benutzercode mit dem Anmeldenamen des Benutzers zu Windows übereinstimmen. Es ist möglich, den Benutzern den Zugriff auf das System zu deaktivieren (bei ESO9-Administrator muss „**ESO9-Benutzer anzufordern“** ausgewählt werden).
- Wenn beim ESO9 Administrator die **Zertifizierungsmethode** eingestellt ist, muss die „Seriennummer des zugehörigen Zertifikats in das Feld **„Seriennummer der Zertifizierung“** eingetragen werden.
- Unter dem Link „**Gruppen**“ können die Benutzer in eine ausgewählte Gruppe (oder mehrere Gruppen) zugeordnet werden. Die Zugriffrechte der Gruppen zu einzelnen Funktionen werden in der Funktion ***9.1.6 Benutzergruppen*** eingestellt, siehe unten. **ACHTUNG**, Hinzufügen und Entfernen eines Benutzers aus der Gruppe 00 kann nur von einem Benutzer in der Gruppe 00 durchgeführt werden. Dasselbe gilt auch für die Funktion ***9.1.6 Benutzergruppen***, siehe unten.
- Wenn die Taste **„Kopie des Benutzers“** eine Kopie des aktuellen Benutzers erstellt (auch mit der Zuordnung in die Benutzergruppen), muss ein neuer (nicht vorhandener) Benutzercode eingegeben werden, noch vor der Erstellung der Kopie. Ein neu erstellter Benutzer muss bearbeitet werden (der Name und andere Angaben müssen geändert werden).

1.2.2 Benutzergruppen (9.1.6)

Gruppen erhalten Rechte für einzelne Funktionen.



- Über den Link "**Zuordnung der Funktion**" können der Benutzergruppe einzelne Funktionen zugeordnet werden, durch die Zuordnung der Funktion werden automatisch die untergeordneten Aktivitäten zugeordnet (wenn beispielsweise die Funktion 2.2 zugeordnet wird, dann werden automatisch auch die Funktionen 2.2, 2.2.1, 2.2.2 usw. zugeordnet)
- Durch die Option **„Sicherheit prüfen“** wird eingestellt, ob die Benutzergruppe überprüft wird. Mehr finden Sie in dem Kapitel ***ESO9 Administrator***.
- Die Option **„Übergeordnete Gruppe“** dient lediglich dazu, die hierarchische Struktur zwischen den Gruppen zu definieren.
- Die Taste **„Kopie der Benutzergruppe“** erstellt eine Kopie der aktuellen Benutzergruppe (einschließlich der zugewiesenen Benutzer in der Gruppe), ein neuer (nicht vorhandener) Benutzergruppencode muss eingegeben werden, noch vor der Erstellung der Kopie. Eine neu erstellte Gruppe muss bearbeitet werden (der Name muss geändert werden und die Funktionen müssen zugeordnet werden).
- **Im unteren Bereich** werden diejenigen Benutzer eingegeben, die in die ausgewählte Gruppe hingehören sollte. Ein Benutzer kann auch mehreren Benutzergruppen zugewiesen werden, er muss dann in jeder Benutzergruppe zugewiesen werden, wohin er hingehören soll.

1.2.3 Applikationsparameter (9.6.1)

Für die Authentifizierungsmethode ESO9 (Anmeldung durch Name und Passwort) ist die Parametergruppe „Passwörter“ von Bedeutung.

Hesla_Encrypt

Hier wird eingegeben, ob die Passwörter in der Benutzertabelle verschlüsselt werden sollen. Sobald die Verschlüsselung (auf 1) eingestellt ist, kann dieser Wert nicht geändert werden. Möglichkeiten:

- 0 = nicht verschlüsseln
- 1 = verschlüsseln

Hesla_PovolZmenu

Hier wird eingegeben, ob die Benutzer selbst ihr Passwort ändern können. Möglichkeiten:

- 0 = die Benutzer selbst dürfen nicht das Passwort ändern
- 1 = die Benutzer selbst dürfen das Passwort ändern

Heslo_EmailInfo

Hier können auch mehrere E-Mailadressen, die durch Semikolon getrennt werden, eingegeben werden.

Falls einem Benutzer aus dem Grunde des wiederholend falsch angegebenen Passworts das Konto gesperrt ist, wird eine informative E-Mail an diese Adresse zugesendet.

Heslo_Min_Delka

Hier wird die mindestzulässige Länge von Benutzerpasswörtern eingegeben.

Heslo_Platn_Upozorn

Hier wird die Anzahl der Tage vor dem Ablauf des Passworts, wo die Warnung an den Benutzer generiert wird, eingegeben.

Heslo_Platnost_Dny

Hier wird die Gültigkeit von Benutzerpasswörtern in Tagen für die gesamte Applikation eingegeben.

Heslo_Pocet_Pouziti

Hier wird die Anzahl der in der Historie aufbewahrten Benutzerpasswörter eingegeben.

Heslo_Slozitost

Hier wird die Passwortkomplexität eingegeben. Möglichkeiten:

- 0 = keine Einschränkung
- 1 = Groß- und Kleinbuchstaben,
- 2 = Groß- und Kleinbuchstaben und Ziffern
- 3 = Groß- und Kleinbuchstaben, Ziffern und spezifische Zeichen

2. Cryptographics

2.1 Database encryption

Transparent Data Encryption (TDE) is implemented on demand in customer's applications. Database once encrypted cannot be restored or attached on another server. TDE encrypts data in physical database files, so data cannon be read without Database Encryption Key (DEK).

Customer's system administrator is responsible for Database Encryption Key and its management.

2.2 Application database objects encryption

Application logic is implemented in stored procedures, views and functions. All of these objects are encrypted using *„With Encryption"* option in production Start version. The only place decrypted objects are accessible is our company's internal SVN repository.

Our developers are liable to keep internal rules for source code handling.

2.3 User password encryption

See chapter 1.2.3.

2.4 Communication encryption

Client communicates with server with HTTPS protocol. Specific security protocol depends on IIS Server used encryption (TLS/SSL version) and used web-server certificate. Level of communication encryption may vary depending on intranet or Internet operation.

Customer's system administrator is responsible for choosing encryption level.

2.5 URL encryption

Every activity in ESO9 could be represented by URL. Every URL in application is encrypted. URL encryption can be combined with all options described in chapter 1.1, i.e. method of verifying and security method.