Autentikace uživatele

ESO9 intranet 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:
Dne: 29.6.2008

Revize: Urych Tomáš
Dne: 1.9.2025

Obsah

1. Konfigurační dialogy pro nastavení způsobu ověření uživatelů

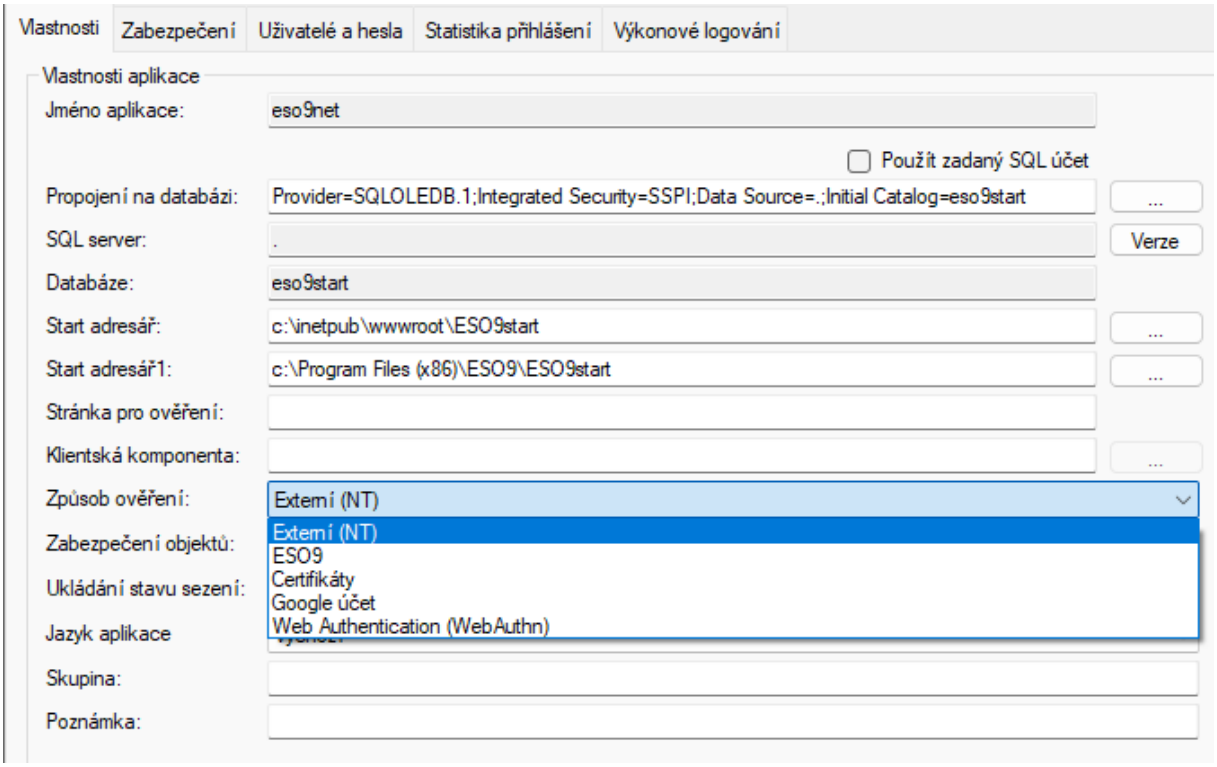
V dokumentu jsou popsány typické způsoby ověřování uživatele v nejčastějších situacích a jejich kombinace a potřebné nastavení aplikace a WEBU aplikace.

1.1 Nastavení aplikace

Nastavení způsobu ověření uživatele v aplikaci se provádí prostřednictvím **Správce ESO9** v položce *Způsob ověření*:

Způsob ověření:

1. ESO9 autentikace – jméno a heslo uživatele je získáno z přihlašovacího formuláře.
2. NT autentikace – jméno uživatele je získáno z IIS.
3. Certifikáty – jméno uživatele je získáno podle platného a zaregistrovaného certifikátu.
4. Google účet – uživatel se ověří svým Google účtem a spáruje se s uživatelem v ESO9 na základě e-mailové adresy.
5. Web Authentication – uživatel se ověří standardem WebAuthn oproti jednomu ze zaregistrovaných pověření (credentials).



Obrázek 1 - Nastavení aplikace

Nastavením způsobu ověření uživatele v programu **Správce ESO9** se zároveň nastaví zabezpečení webu aplikace (kapitola 1.2).

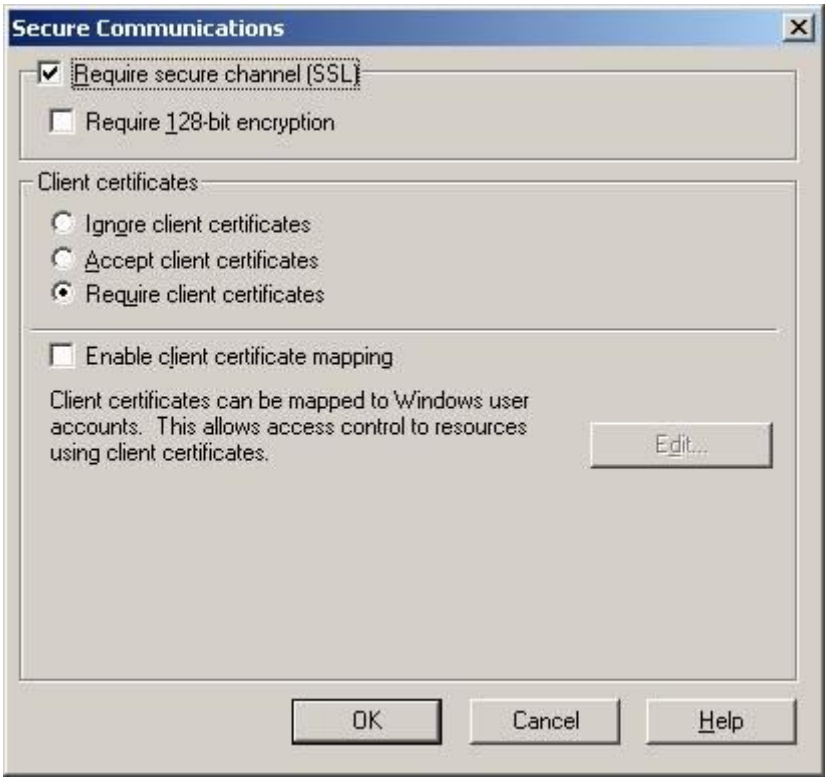
1.2 Nastavení webu aplikace

Nastavení se provádí prostřednictvím programu **Správce ESO9**, který zajistí i správnou konfiguraci webu v IIS. Způsob nastavení je uveden v nápovědě tohoto programu.

Kontrola, případně manuální nastavení webu aplikace se provádí v nastavení IIS

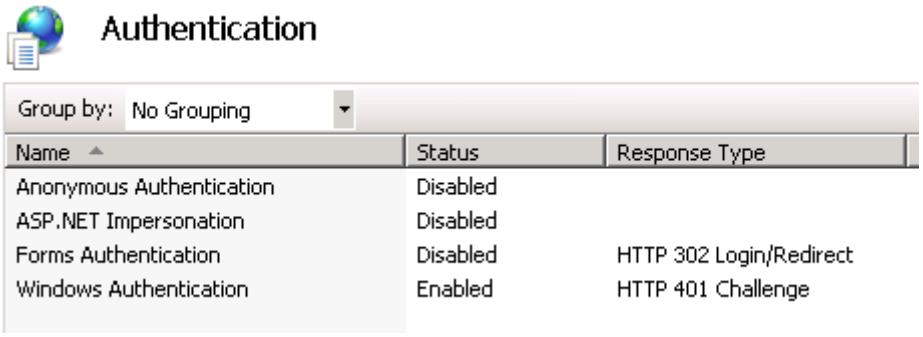
1.2.1 Příklad pro Windows 2003 server

Obrázek 2 - Nastavení pro ESO9 autentikaci (pro externí NT autentizaci se ponechá pouze Interated Windows authentication)



Obrázek 3 - Nastavení v případě použití certifikátů

1.2.2 Příklad pro Windows 2008/2012 Server



Obrázek 4 - Nastavení pro externí (NT) autentikaci

2. Způsoby ověřování pro uživatele stejného typu

2.1 Uživatelé s doménovým účtem

2.1.1 V lokální síti

Nejčastější způsob přihlašování uživatele.

- Aplikace se nastaví na externí NT autentikaci
- WEB aplikace se nastaví pouze na *Integrované ověřování Windows* (Windows Authentication)

2.1.2 Přes internet

V případě použití VPN je konfigurace stejná jako v lokální síti. Pokud není k dispozici VPN připojení, je potřeba takového uživatele považovat za uživatele bez doménového účtu.

2.2 Uživatelé bez doménového účtu

2.2.1 Ověření jménem a heslem

Uživatel musí být uveden v tabulce uživatelů a musí mít uvedeno heslo.

- Aplikace se nastaví na ESO9 autentikaci
- WEB aplikace musí mít nastaven pouze anonymní přístup

2.2.2 Ověření certifikátem

Uživatel musí mít instalován klientský certifikát.

Uživatel musí být uveden v tabulce uživatelů se jménem a heslem pro první přihlášení. Registraci certifikátu do tabulky uživatelů lze provést při prvním přihlášení zadáním jména a hesla.

Po prvním přihlášení je certifikát zaevidován v tabulce uživatelů a při dalším přihlášení se použije automaticky a přihlašovací heslo je zrušeno.

- Aplikace se nastaví na autentikaci Certifikáty
- WEB aplikace musí mít nastaven pouze anonymní přístup, vyžadovat klientský certifikát a 128 bitové šifrování
- Server muší mít nainstalován serverový certifikát a musí být nakonfigurován pro HTTPS

protokol

Podrobnější popis viz dokument Certifikátová autentikace v ESO9.

2.2.3 Ověření standardem WebAuthn

Uživatel musí být uveden v tabulce uživatelů a pro každý způsob ověření své identity (autentikátor, např. biometrie, USB token atd.) má v aplikaci zaregistrován jedno pověření (credentials).

Podrobnější popis viz dokument Ověřování uživatelů standardem WebAuthn.

3. Pravidla pro ověření uživatele v systému ESO9

Cílem ověření uživatele v systému ESO9 je získat jméno uživatele, které je pak vyhledáno v tabulce uživatelů.

3.1 Postup při získání jména uživatele pro konfiguraci externí (NT) autentikace

- Jméno je předáno z IIS.
- Pokud jméno není předáno, server ESO9 požádá IIS o ověření uživatele a očekává jméno (v tomto případě je to již signálem chyby, kterou je nutné odstranit).
- Jméno uživatele je ověřeno procedurou *spAutenticateUser.*
- V případě že selže vynucení, nebo není jméno ověřeno, je hlášena chyba.

3.2 Postup při získání jména uživatele pro konfiguraci ESO9 autentikace

- Server ESO9 odešle uživateli formulář s dotazem na jméno a heslo.
- Pokud není vyplněné jméno a heslo ověřeno procedurou *spAutenticateUser*, je hlášena chyba.

3.2.1 HASHování hesel uživatelů

Pro ESO9 autentikaci jsou hesla uložena v databázi v tabulce *UZIVATEL*, položce *UZIV_HESLO*. Ve výchozím nastavení jsou uložena v otevřeném formátu. Pro zvýšení zabezpečení je doporučeno zapnout jejich hashování aplikačním parametrem *Hesla_Encrypt* ze skupiny parametrů *Hesla*. Při zahashování uživatelských hesel se tato prokládají s náhodně generovaným řetězcem *SALT* v tabulce *UZIVATEL*; dva uživatelé se stejným heslem tedy nebudou mít v tabulce uložen stejný hash. Z hashe uloženého v tabulce *UZIVATEL* nelze zpětně zrekonstruovat heslo.

3.2.2 Položky tabulky UZIVATEL pro práci s hesly

- Sloupec *UZIV_HESLO* – obsahuje uživatelské heslo v otevřeném formátu nebo jeho hash.
- Sloupec *VLAKCE_HESLO* (SmallInt) – obsahuje příznak pro stav uživatelského hesla:
  - 0 = výchozí hodnota, žádná akce
  - 1 = vynucení změny hesla uživatelem, po změně se vrací na stav 0
  - 2,3,4 = čítač po sobě jdoucích neúspěšných pokusů o přihlášení ze stránky pro zadání jména a hesla. Hodnoty 2, 3, 4 znamenají 1, 2, 3 neúspěšné pokusy.

  - 5,6,7 = čítač po sobě jdoucích neúspěšných pokusů o přihlášení ze stránky pro vynucenou změnu hesla. Hodnoty 5, 6, 7 znamenají 1, 2, 3 neúspěšné pokusy.
  - 8+ = pro budoucí využití
- Sloupec *DTPLATNOSTHESLA_DO* (DateTime) – obsahuje datum platnosti stávajícího hesla. Hodnota NULL = heslo platné stále.
- Sloupec *UZIV_HESLO_OLD* (VarChar) – obsahuje historii uživatelských hesel. Jednotlivá hesla jsou uložena v zahashovném tvaru s daným oddělovačem. Počet hesel uchovávaných v historii bude dán aplikačním parametrem.

3.2.3 Ověření přes Google účet

Podrobnější popis nastavení ověřování přes Google účet je k dispozici v samostatném dokumentu na adrese https://wiki.eso9.cz/doku.php/techdoc:overovani_uzivatelu_pomoci_google_uctu.

3.2.4 Aplikační parametry pro práci s hesly

Všechny aplikační parametry pro práci s uživatelskými hesly jsou zařazeny ve skupině parametrů *Hesla*:

- *HESLA_ENCRYPT* – parametr, kterým se nastavuje hashování uživatelských hesel.
- *HESLO_PLATNOST_DNY* – parametr pro centrální nastavení doby platnosti uživatelských hesel ve dnech pro celou aplikaci. Hodnota 0 = bez omezení. Při zakládání nového uživatele se tato hodnota použije v NewRecu jako výchozí nastavení. Při pravidelné změně hesla se automaticky posune hodnota data platnosti stávajícího hesla (*DTPLATNOSTHESLA_DO*) o hodnotu parametru. Zůstává možnost nastavit/změnit platnost pro jednotlivé uživatele individuálně.
- *HESLO_MIN_DELKA* – parametr pro stanovení minimální povolené délky zadávaného hesla. 0 = bez omezení.
- *HESLO_POCET_POUZITI* – parametr pro stanovení počtu uchovávaných a kontrolovaných hesel v historii daného uživatele.
- *HESLO_PLATNOST_UPOZORNENI* – nový parametr udávající kolik dnů před vypršením hesla se má uživateli generovat upozornění (na změnu hesla).
- *HESLO_SLOZITOST* – parametr určující míru komplexnosti hesla:
  - 0 = bez omezení.
  - 1 = velká a malá písmena.
  - 2 = velká a malá písmena a číslice.
  - 3 = velká a malá písmena, číslice a spec.znaky.
- *HESLA_POVOLZMENU* – parametr definuje, zda si uživatelé sami mohou provádět změnu hesla. Hodnota 1 = povolit změnu hesla pouze administrátorům (skupina *„00“*) systému.
- *HESLO_EMAILINFO* – e-mailová adresa (-y) správce, kterému je zaslána notifikace v případě, že si uživatel opakovaným chybným zadání hesla zablokuje účet.

3.2.5 Postup založení nového uživatele s heslem

- V aplikaci založíme nového uživatele (popř. kopií ze stávajícího).
- V aplikaci Správce ESO9 novému uživateli přidělíme heslo …
- … a popř. vynutíme jeho změnu při prvním přihlášení.

3.2.6 Postup změny uživatelského hesla

- Uživatel si může heslo změnit sám v činnosti *9. 8. 8 Nastavení hesla* (pokud je to povoleno parametrem *HESLA_POVOLZMENU*).
- Nebo si jej musí změnit při přihlášení v okamžiku, kdy mu buď vypršela platnost původního hesla, nebo mu správce aplikace nastavil nové heslo a vynutil si jeho změnu při prvním přihlášení.
- Nebo mu jej může změnit správce v aplikaci **Správce ESO9** (doporučeno zároveň vynutit změnu hesla při přihlášení tak, aby správce aplikace uživatelské heslo neznal).

3.3 Postup při získání jména uživatele pro konfiguraci Certifikáty

- IIS musí předat informaci o certifikátu uživatele.
- Pokud procedura *spAutenticateUser* nenalezne uživatele podle certifikátu, je uživateli odeslán formulář s dotazem na jméno a heslo pro registraci certifikátu.
- Pokud registrace certifikátu neproběhne, je hlášena chyba.

4. Skupinový uživatel

Pro přístup skupiny uživatelů bez dalšího rozlišení jednotlivých uživatelů je třeba vytvořit uživatele systému ESO9 a v jeho vlastnostech nastavit vlastnost skupina =1.

Je vhodný pro zajištění přístupu skupinám uživatelů s definovanými právy do systému - např. všichni oprávnění pracovníci jednoho dodavatele apod.

Všichni mohou pod jedním jménem pracovat současně, při uzavření Internet Exploreru je nutno se znovu přihlásit.