VYUŽITÍ SLUŽEB ACTIVE DIRECTORY
V PRODUKTECH SPOLEČNOSTI
YAMACO SOFTWARE

PRO ÚČELY:

- VYUŽITÍ EXISTUJÍCÍCH PARAMETRŮ ÚČTŮ V ACTIVE DIRECTORY
- NASTAVENÍ POTŘEBNÝCH VLASTNOSTÍ PŘIPOJENÍ

1. Úvodem

Přihlašování do databázových aplikací společnosti YAMACO Software je možné trojím způsobem:

- klasicky pomocí uživatelského jména a hesla
- pomocí tzv. automatického přihlašování, kdy je přebírán login uživatele do Windows a pro přihlášení se do databáze je použit účet YAMACO
- pomocí služby Active Directory

2. Stručný popis funkcionality připojení k Active Directory

Základní myšlenkou propojení s Active Directory (AD) je přebírání existujícího přihlášení uživatele do operačního systému a jeho využití jak pro přihlášení se do systému Active Directory, tak k databázovému serveru.

Funkcionalita propojení se systémem Active Directory je pro uživatele zcela bezplatná a není třeba ji žádným způsobem dokupovat nebo aktivovat.

3. Potřebná nastavení na straně databázového serveru FireBird (verze 3.0, 4.0)

FireBird umožňuje kromě tradičního způsobu přihlašování pomocí jména a hesla a ověření těchto pověření oproti Security Database (tzv. Srp mód) i režim, kdy je přebírán login uživatele z Windows (tzv. Win_Ssspi mód).

Pro využití služeb Active Directory je třeba provést kontrolu parametrů **AuthServer, AuthClient** a **UserManager** v konfiguračním souboru FIREBIRD.CONF (nachází se v kořenovém adresáři dané verze Firebirdu). Je třeba, aby řádky se zmíněnými parametry vypadaly takto:

AuthServer = Srp, Win_Sspi
#AuthClient = Srp, Srp256, Win_Sspi, Legacy_Auth #Windows clients
#UserManager = Srp

V naprosté většině případů nebude třeba konfigurační soubor FIREBIRD.CONF měnit s výjimkou parametru AuthServer, který musí být doplněn o plugin Win_Sspi (červeně zvýrazněno).

Postup při úpravě FIREBIRD.CONF:

a) zastavte službu Firebird
b) upravte konfigurační soubor
c) spusťte službu Firebird

Druhým potřebným krokem je vytvoření mapování pro uživatelské role. To se provede pod účtem SYSDBA takto:

a) Z instalačního adresáře FB 3.0 spusťte ISQL.EXE.
b) Připojte se k produktové databázi (např. SOD.FDB) takto:

CONNECT *databáze* user 'SYSDBA' password '*heslo*';

V praxi například:

CONNECT server_1:c:\temp\sod.fdb user 'SYSDBA' password 'masterkey';

a stiskněte Enter

c) Vložte příkaz pro vytvoření mapování:

CREATE GLOBAL MAPPING TRUSTED_AUTH USING PLUGIN WIN_SSPI FROM ANY USER TO USER;

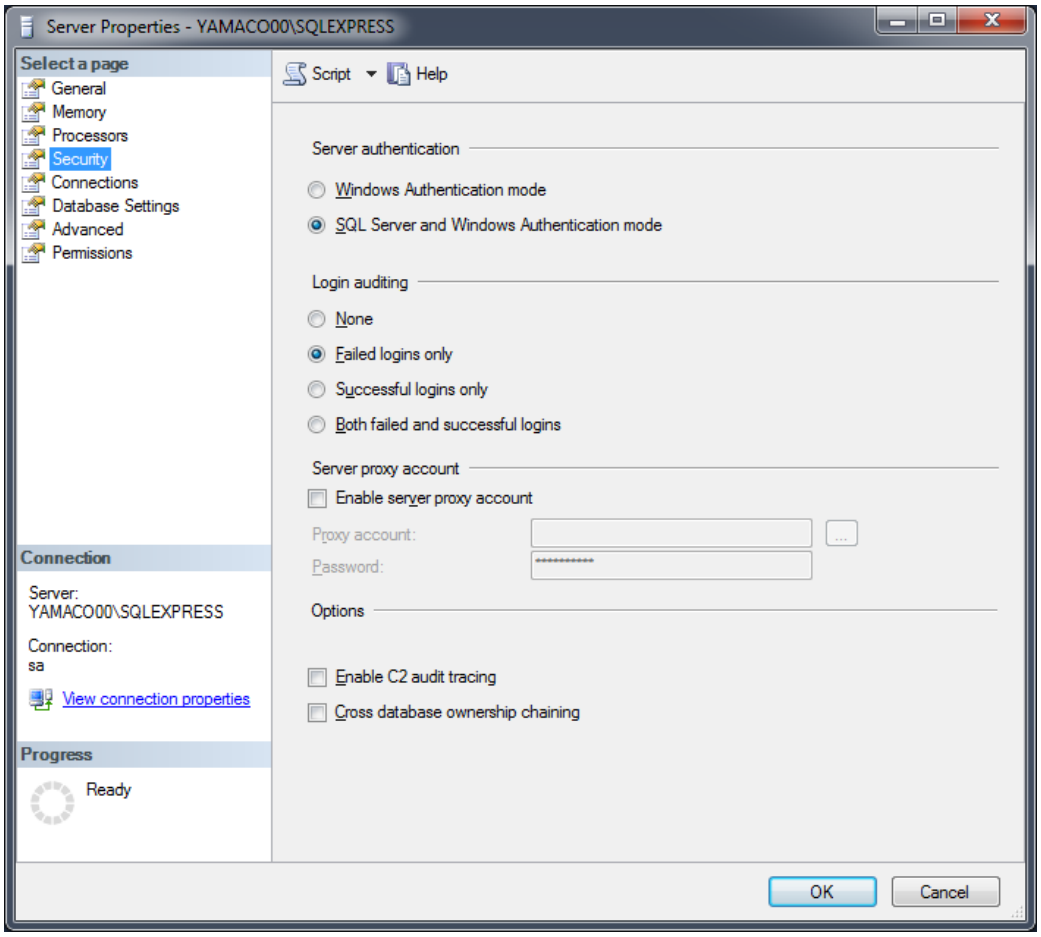
a stiskněte Enter

Upozornění: Režim Win_Sspi není podporován na serverech s operačním systémem Linux. Pokud chcete AD funkcionalitu využívat i pro Firebird běžící na OS Linux, je třeba v dialogu AD na záložce Obecné zatrhnout volbu Firebird server běží na OS Linux. Dále musí být na úrovni databázového serveru Firebird vytvořeny všechny uživatelské účty, jejichž pověření (uživatelské jméno a heslo) se bude z AD přebírat.

4. POTŘEBNÁ NASTAVENÍ NA STRANĚ DATABÁZOVÉHO SERVERU M S SQL SERVER

Microsoft SQL Server umožňuje kromě tradičního způsobu přihlašování pomocí jména a hesla a ověření těchto pověření (tzv. SQL Server Authentication) i režim, kdy je přebírán login uživatele z Windows (tzv. trusted mód) anebo režim, kombinující obě předchozí metody (tzv. Windows Authentication).

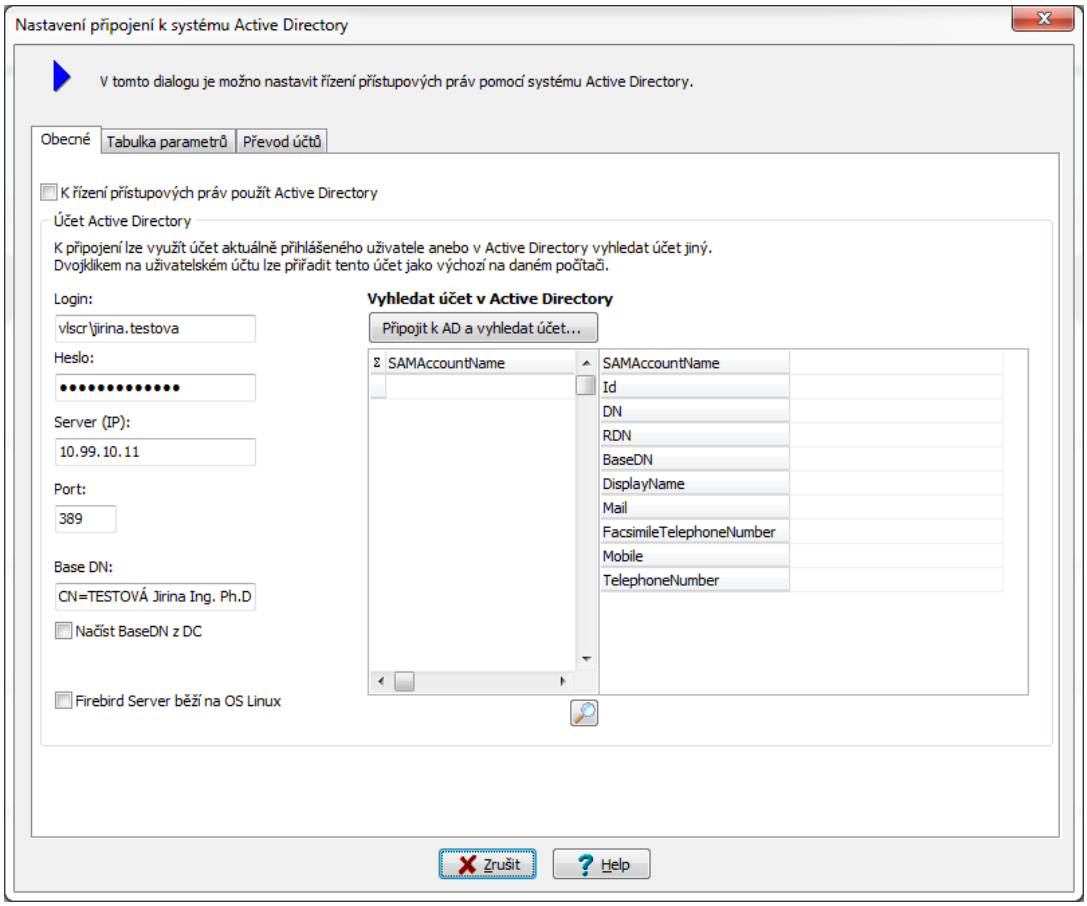
Pro využití služeb Active Directory je třeba zvolený server nakonfigurovat na Window Authentication režim – to lze provést jednoduše v Enterprise Manageru klepnutím pravým tlačítkem myši na štítek zvoleného serveru a ve stromu voleb vybrat list Security:



5. NASTAVENÍ PROPOJENÍ S ACTIVE DIRECTORY PŘED PRVNÍM POUŽITÍM

Před prvním použitím je třeba otevřít dialog Active Directory na pásu Servis a nastavit potřebné parametry připojení a uživatelského účtu.

Dialogové okno obsahuje všechny potřebné prostředky pro nastavení parametrů připojení:



Záložka Obecné umožňuje využít účet aktuálně přihlášeného uživatele nebo v systému Active Directory vyhledat účet jiný a ten následně použít.

Přepínač K řízení přístupových práv použít Active Directory slouží k zapnutí nebo vypnutí propojení aplikace s Active Directory.

Využití účtu aktuálně přihlášeného uživatele

Ze systému je převzat login uživatele, stačí tedy doplnit heslo k tomuto účtu a IP adresu serveru, na němž sídlí Active Directory. Komunikační port je defaultně nastaven na výchozí hodnotu 389.
Údaj Base DN je možno v závislosti na stavu přepínače Načíst BaseDN z DC buď načíst z řadiče domény anebo zadat ručně.

Vyhledání jiného účtu (např. v případě, kdy nastavení provádí správce systému pro jiného uživatele)

Přihlaste se pod svým účtem do systému Active Directory pomocí údajů Login, Heslo a adresa AD serveru. Údaj BaseDN můžete ponechat buď prázdný nebo jej zadat v potřebném rozsahu. Klepněte na tlačítko Připojit k AD a vyhledat účet – v levém seznamu se zobrazí všechny uživatelské účty, které se nacházejí v daném rozsahu BaseDN. Pro vyhledání účtu lze použít tlačítko pro hledání.

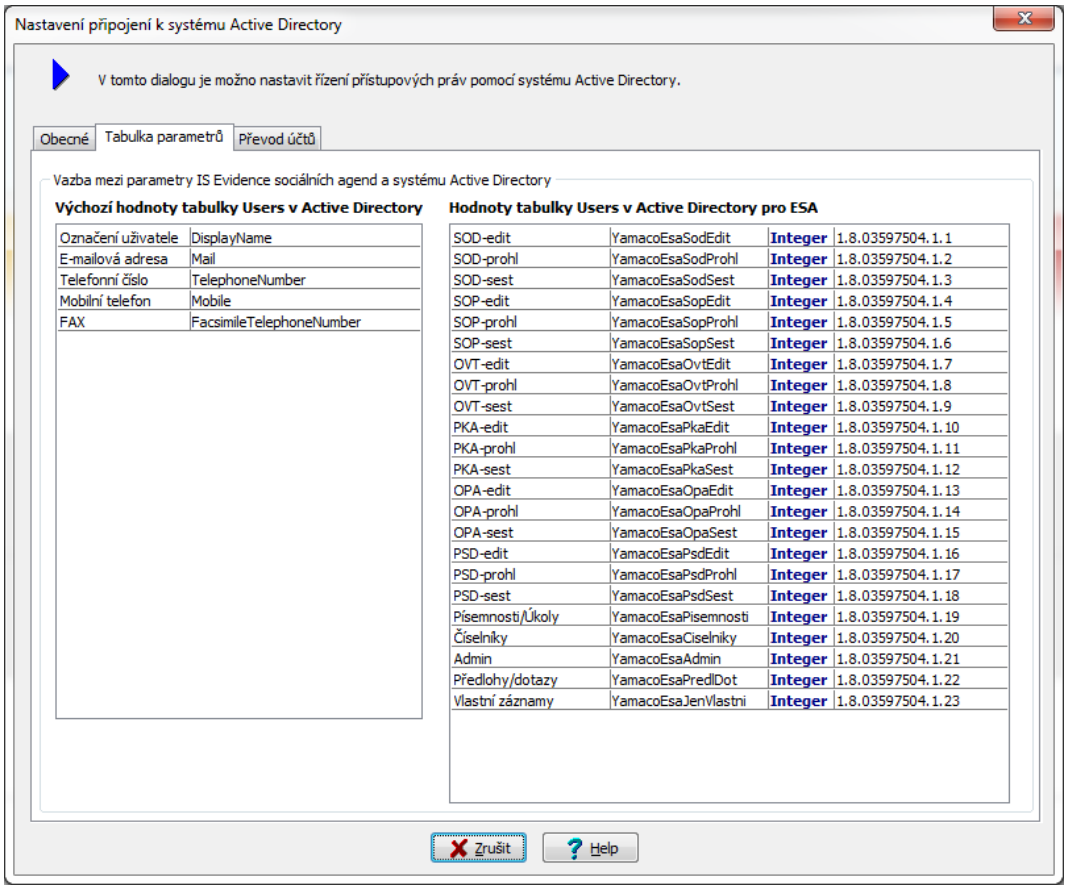
Vyhledaný účet se nastaví dvojklikem na název účtu v levém seznamu – převezmou se všechny atributy účtu s výjimkou hesla, jež je nutno zadat samostatně. Po zavření dialogu se zadané hodnoty uloží do konfiguračního souboru a po restartu aplikace se již provede automatické přihlášením uživatele bez zobrazení dialogu pro zadání jména a hesla.

Záložka Tabulka parametrů obsahuje dva seznamy údajů – první obsahuje obecné identifikační údaje, jejichž existence se v systému Active Directory standardně předpokládá.

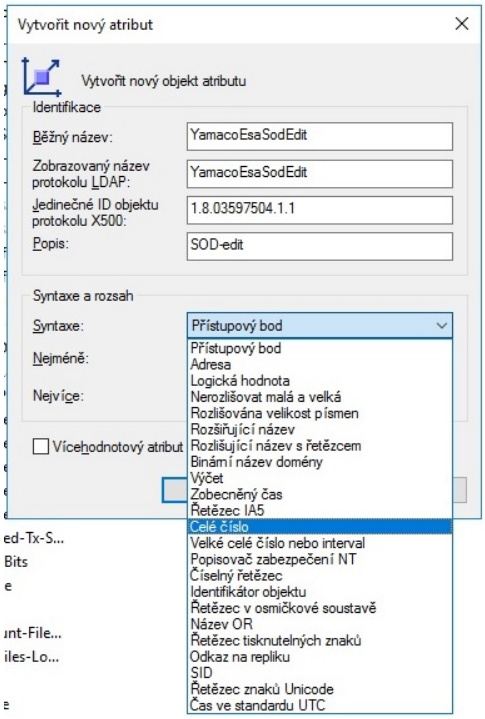
Druhý seznam je závislý na typu informačního systému společnosti YAMACO Software a prakticky obsahuje všechny parametry nastavení, dostupné v dané aplikace pro jednotlivé uživatele. Tyto položky včetně jejich typu je třeba doplnit do tabulky „User“ v systému Active Directory – naplnění hodnotami pro existující účty provedou naše aplikace automaticky pomocí funkcí na záložce Převod účtů (popsáno dále).

Pro položky typu Integer využíváme kladné hodnoty pro povolení dané funkce, záporné hodnoty pro jejich zakázání. Číslo 0 se nevyužívá.

Vlastní přidělení práv k ovládání aplikace pak probíhá prostřednictvím těchto nových položek, nastavení přístupových práv na úrovni uživatelských účtů na pásu Servis v našich aplikacích se nadále nevyužívá.



Příklad vytvoření odpovídající hodnoty pro Evidenci sociálních agend je na následujícím obrázku:



Pro nastavení identifikátoru Jedinečné ID objektu protokolu LDAP je doporučeno použít následující syntaxi:

1.8.03597504. plus kód informačního systému společnosti YAMACO Software tečka plus pořadové číslo atributu v seznamu výše

Kódy informačních systémů společnosti YAMACO Software pro účely konstrukce identifikátoru jsou následující:

1 – Evidence sociálních agend
2 – Evidence myslivosti
3 – Evidence dopravních agend
4 – Myslivecké a rybářské průkazy
5 – Evidence přestupků samostatná
6 – Evidence smluv a objednávek
7 – Plánování pracovních cest
8 – Plán dovolených

Příklad:

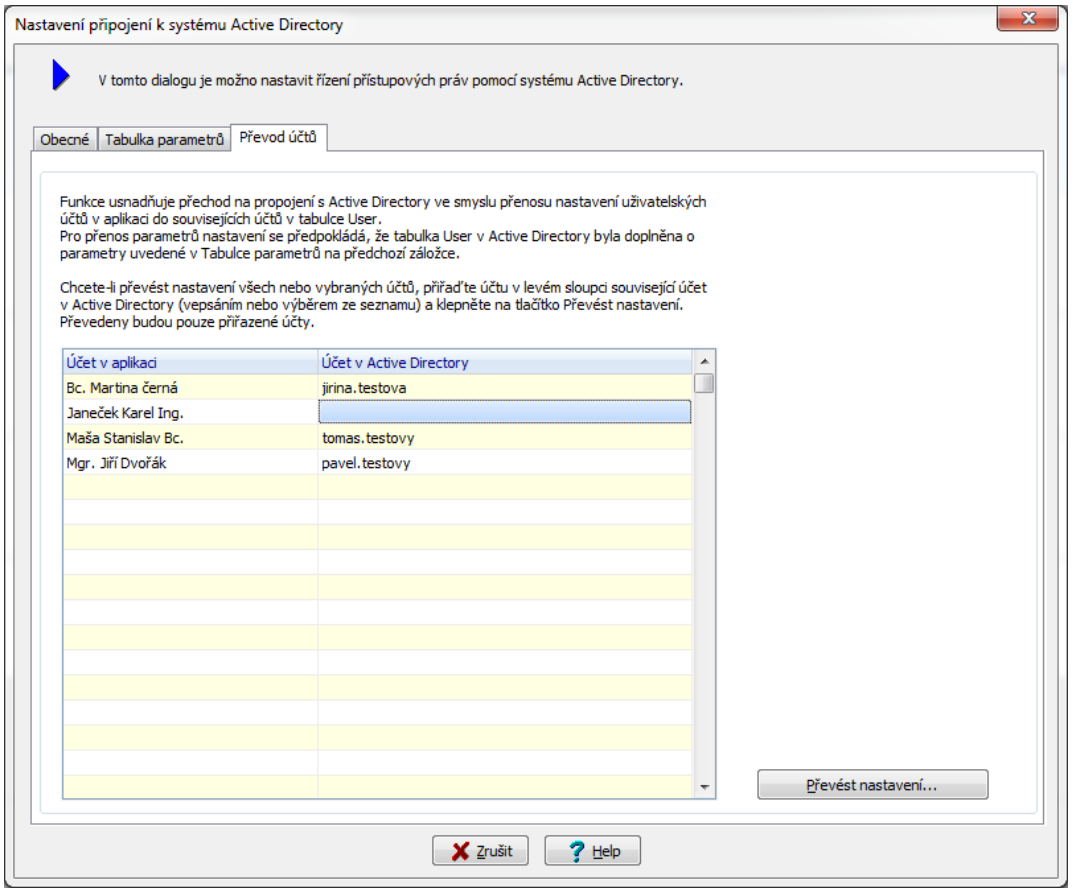
Jedinečné ID objektu protokolu LDAP pro Myslivecké a rybářské průkazy, přístup na prohlížení dat průkazů, bude 1.8.03597504.4.2.

6. PŘEVOD EXISTUJÍCÍCH DAT ÚČTŮ Z NAŠICH APLIKACÍ DO ACTIVE DIRECTORY

Pro usnadnění práce jsou systémy společnosti YAMACO Software vybaveny nástrojem pro převod dat existujících účtů. Filozofie je taková, že na záložce Převod dat správce vybere dvojice účtů v aplikaci a v Active Directory. Pro všechny takto spárované účty je následně možné tlačítkem Převést nastavení importovat parametry nastavení z našeho projektu do Active Directory.

Převod dat existujících účtů předpokládá, že cílový uživatelský účet již v AD existuje. Převod se provádí pouze pro spárované účty, nespárované jsou v průběhu převodu ignorovány.

Převod dat účtů je možné neomezeně opakovat, dojde vždy k aktualizaci stávajícími údaji a nedochází k žádným duplicitám.


Nastavení připojení k systému Active Directory
V tomto dialogu je možno nastavit řízení přístupových práv pomocí systému Active Directory.
Obecné
Tabulka parametrů
Převod účtů
Funkce usnadňuje přechod na propojení s Active Directory ve smyslu přenosu nastavení uživatelských účtů v aplikaci do souvisejících účtů v tabulce User.
Pro přenos parametrů nastavení se předpokládá, že tabulka User v Active Directory byla doplněna o parametry uvedené v Tabulce parametrů na předchozí záložce.
Chcete-li převést nastavení všech nebo vybraných účtů, přiřaďte účtu v levém sloupci související účet v Active Directory (vepsáním nebo výběrem ze seznamu) a klepněte na tlačítko Převést nastavení.
Převedeny budou pouze přiřazené účty.
Účet v aplikaci
Účet v Active Directory
Bc. Martina černá
jirina.testova
Janeček Karel Ing.
Maša Stanislav Bc.
tomas.testovy
Mgr. Jiří Dvořák
pavel.testovy
Převést nastavení...
Zrušit
Help