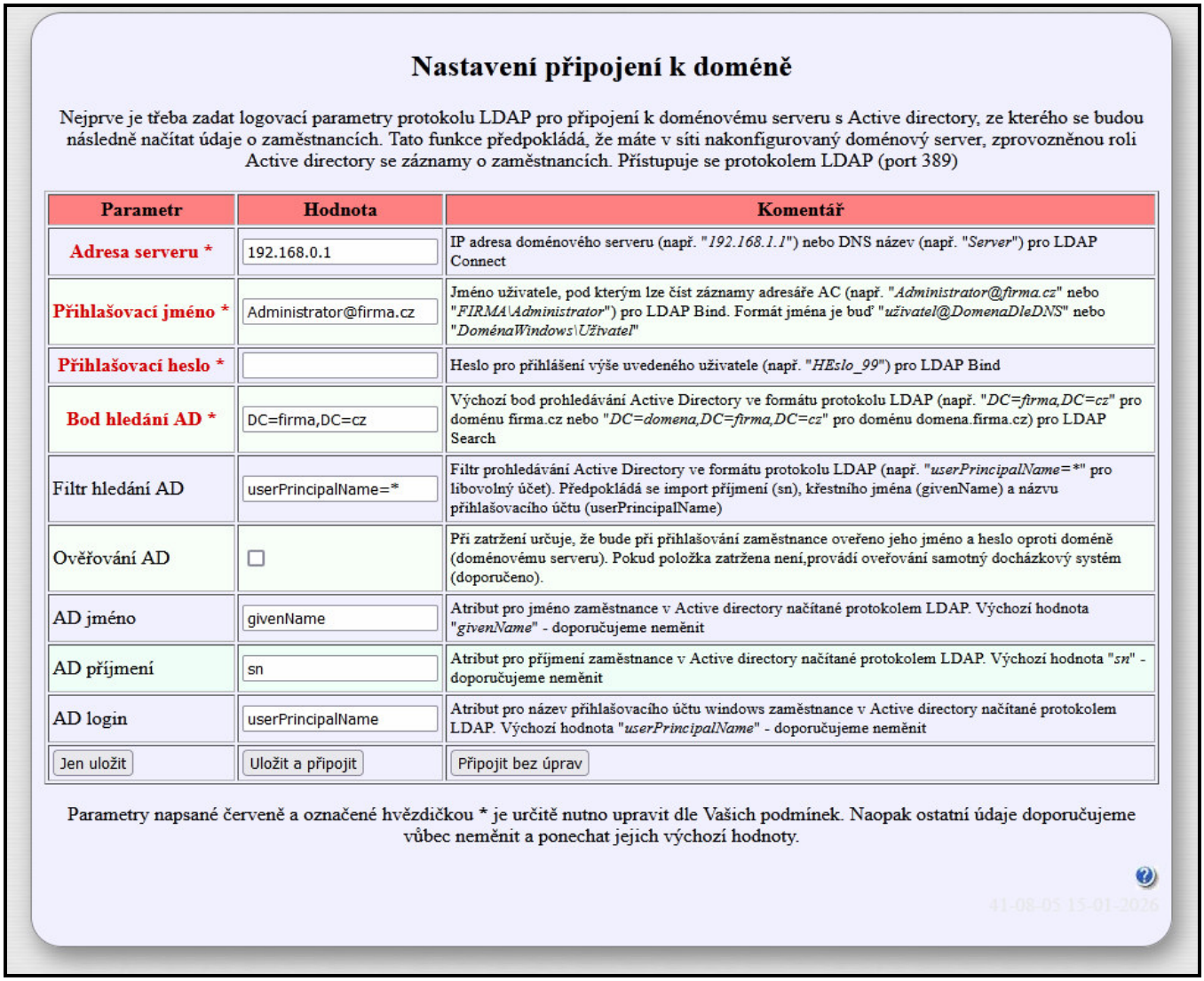
Docházka 3000 - možnosti napojení na doménový server

Níže naleznete základní nápovědu zkopírovanou z programu Docházka 3000 k možnostem napojení docházkového systému na doménový server protokolem LDAP.

Napojení docházky na doménový server (s použitím nešifrovaného LDAP protokolu) lze využít ke 3 účelům:
1. Import seznamu zaměstnanců z domény do nové instalace docházky, takže pak není nutné zadávat zaměstnance ručně. Hodí se zejména pokud máte vyšší desítky či spíše stovky pracovníků a z nějakého důvodu nechcete použít import z XLS nebo CSV souboru.
2. Export seznamu zaměstnanců z docházkového systému do doménového serveru.
3. Ověření přihlášení uživatele do docházky. Hodí se v případě kdy běžní zaměstnanci budou mít možnost přihlašovat se do docházkového systému do svého uživatelského menu například z důvodů kontroly své docházky a případně i pro čipování přes PC. Pak lze nastavit, aby přihlašovací heslo neověřovala docházka vůči své vlastní databázi, ale aby ověření provedl doménový server.

Níže uvedená nápověda obsahuje tučným písmem uvedený bod v menu programu ve kterém je tato konkrétní funkcionalita dostupná a pod ním pak popis odpovídající části. Samostatné celky jsou odděleny horizontální čarou.

Zaměstnanci / Editace údajů / Import/export z Active Directory (LDAP)
Tento modul umožňuje nastavení parametrů připojení k doménovému serveru protokolem LDAP. Stručná nápověda je u každé konfigurační položky přímo v programu. Zadává se adresa serveru, přihlašovací účet pod kterým lze číst údaje z adresáře a specifikace domény - připojovacího řetězce pro úvodní bod prohledávání. Tyto první 4 parametry označené červeně je nutné upravit tak, aby odpovídaly Vaší konkrétní konfiguraci.



Nastavení připojení k doméně

Nejprve je třeba zadat logovací parametry protokolu LDAP pro připojení k doménovému serveru s Active directory, ze kterého se budou následně načítat údaje o zaměstnancích. Tato funkce předpokládá, že máte v síti nakonfigurovaný doménový server, zprovozněnou roli Active directory se záznamy o zaměstnancích. Přístupuje se protokolem LDAP (port 389)

Parametr	Hodnota	Komentář
Adresa serveru *	192.168.0.1	IP adresa doménového serveru (např. "*192.168.1.1*") nebo DNS název (např. "*Server*") pro LDAP Connect
Přihlašovací jméno *	Administrator@firma.cz	Jméno uživatele, pod kterým lze číst záznamy adresáře AC (např. "*Administrator@firma.cz*" nebo "*FIRMA\Administrator*") pro LDAP Bind. Formát jména je buď "*uživatel@DomenaDleDNS*" nebo "*DoménaWindows\Uživatel*"
Přihlašovací heslo *		Heslo pro přihlášení výše uvedeného uživatele (např. "*HEslo_99*") pro LDAP Bind
Bod hledání AD *	DC=firma,DC=cz	Výchozí bod prohledávání Active Directory ve formátu protokolu LDAP (např. "*DC=firma,DC=cz*" pro doménu firma.cz nebo "*DC=domena,DC=firma,DC=cz*" pro doménu domena.firma.cz) pro LDAP Search
Filtr hledání AD	userPrincipalName=*	Filtr prohledávání Active Directory ve formátu protokolu LDAP (např. "*userPrincipalName=**" pro libovolný účet). Předpokládá se import příjmení (sn), křestního jména (givenName) a názvu přihlašovacího účtu (userPrincipalName)
Ověřování AD	☐	Při zatržení určuje, že bude při přihlašování zaměstnance ověřeno jeho jméno a heslo oproti doméně (doménovému serveru). Pokud položka zatržena není,provádí ověřování samotný docházkový systém (doporučeno).
AD jméno	givenName	Atribut pro jméno zaměstnance v Active directory načítané protokolem LDAP. Výchozí hodnota "*givenName*" - doporučujeme neměnit
AD příjmení	sn	Atribut pro příjmení zaměstnance v Active directory načítané protokolem LDAP. Výchozí hodnota "*sn*" - doporučujeme neměnit
AD login	userPrincipalName	Atribut pro název přihlašovacího účtu windows zaměstnance v Active directory načítané protokolem LDAP. Výchozí hodnota "*userPrincipalName*" - doporučujeme neměnit
Jen uložit	Uložit a připojit	Připojit bez úprav

Parametry napsané červeně a označené hvězdičkou * je určitě nutno upravit dle Vašich podmínek. Naopak ostatní údaje doporučujeme vůbec neměnit a ponechat jejich výchozí hodnoty.

Primárně se předpokládá přístup do Actrive directory v doménové struktuře Microsoft pro servery Windows. Ale použitý protokol LDAP umí komunikovat s libovolnou adresářovou službou, takže je možné i připojení do adreářových služeb založených např. na Linuxu. Proto lze editovat i další položky, jako je filtr hledání a atributy adresáře, pomocí kterých docházka hledá jméno, příjmení a název přihlašovacího účtu uživatelů.

"Adresa serveru" - Určuje adresu doménového řadiče, který má nainstalovanou roli Active Directory a ze kterého je tedy možné importovat adresářová data o účtech zaměstnanců a případně vůči kterému lze provádět i ověřování hesel, pokud zapnete níže uvedenou položku "Ověřování AD". Může zde být buď IP adresa nebo DNS název. Pokud je docházka nainstalovaná přímo na řadiči domény s active directory, můžete zadat IP adresu smyčky, tedy 127.0.0.1
Pokud je docházka nainstalovaná na jiném PC než je doménový řadič, zadáte Ip adresu doménového serveru nebo jeho DNS název.
Zde zadaná adresa slouží pro příkaz ldap_connect.

"Přihlašovací jméno" - Jméno uživatele, pod kterým se lze přihlásit a číst data z Active directory. Pokud budete chtít i data do adresáře zapisovat, musí mít tento uživatel požadované oprávnění. Jméno je třeba zadat v plně kvalifikovaném tvaru. Takže například pokud máte doménu firma.cz a použijete uživatelské jméno administrátora, je třeba zadat buď administrator@firma.cz nebo (pokud to server umožňuje), lze použít i starší typ názvu, např. FIRMA\administrator.
Hodnota slouží pro příkaz ldap_bind.

"Přihlašovací heslo" - Heslo výše uvedeného uživatele.
Hodnota slouží pro příkaz ldap_bind.

"Bod hledání AD" - výchozí bod ve struktuře adresáře, od kterého bude docházka provádět hledání uživatelských účtů. Zapisuje se ve formátu protokolu LDAP, takže pro části s názvy domény se používá atribut DN, pro části větvení uvnitř struktury adresáře se používá atribut CN, pro organizační jednotky OU atd. Pokud tedy máte doménu firma.cz a chcete prohledávat celou doménu (všechny větve), lze použít např. zápis
DN=firma,DN=cz
Pokud chcete v adresáři hledat jen ve větvi účtů uživatelů nazvané users, zadáte zápis
CN=users,DN=firma,DN=cz
Jestliže máte zadanou organizační strukturu v doméně firma.cz a chcete hledat jen v oddělení "skladníci", zadáte zápis *OU=skladníci,DN=firma,DN=cz*
Hodnota slouží pro příkaz ldap_search jako parametr DN.

"Oveřování AD" má přímý vliv na přihlašovaní zaměstnanců do webového rozhraní docházkového systému. Standardně, pokud není položka zatržena, se ověřují hesla přímo v samotné docházce. Každý zaměstnanec má v docházce (v editaci údajů zaměstnanců) nastaveno heslo a při přihlašování se toto individuální heslo ověřuje proti databázi docházky. Pokud ale zatrhnete položku "Oveřování AD", tato hesla se ignorují a ověření provádí doménový server (nikoli docházka). Pokud tuto volbu použijete, je třeba mít na paměti několik důležitých věcí:
- Zde zadaná položka "Adresa serveru" musí ukazovat (nejlépe IP adresu) na správný doménový server.
- Tento doménový server musí být po síti dosažitelný z počítače, na kterém běží docházkový systém (pokud to není tentýž počítač)- heslo neověřuje klientská stanice, ale docházka je od klienta příjme a přepošle je na ověření do domény. Ověřování do domény tedy přichází z docházkového serveru.
- Záznamy zaměstnanců v docházce musí být správně svázány s uživatelskými účty v doméně (viz následující sekce nápovědy níže).
Proto tuto volbu zapínejte, jen pokud přesně víte, co tato úprava znamená. Pokud nebude doménový server dostupný, nebo nebudou účty správně svázány, bude znemožněno logování zaměstnanců přes webové rozhraní do docházky.
Vyjímkou je pouze účet administrátora docházky - ten se vždy ověřuje v docházce a jeho heslo je v ní nastaveno v menu Firma / Editace údajů. Administrátor docházky se tedy v doméně nikdy neověřuje a proto se lze jeho heslem do docházky přihlásit vždy bez ohledu na stav domény a konfiguraci spojení protokolem LDAP.

"Filtr hledání" - Určuje, které atributy adresáře se budou prohledávat a jaký je hledaný obsah. Například hodnota sn=* vyhledá všechny záznamy uživatelských účtů v zadané větvi výše uvedeného bodu hledání AD. Naproti tomu hodnota userPrincipalName=* vyhledá pouze takové záznamy účtů, které mají nastavený atribut

pro plně kvalifikovaný název uživatelského účtu ve formátu ucet@domena (např. karel@firma.cz). Takové nastavení je výchozí předvolené, protože nejlépe vůči těmto účtům je možné provádět přihlášení do domény z docházky, pokud je zapnuta výše uvedené volba Ověřování AD. A také tyto účty a jejich položka userPrincipalName jsou doporučeny pro svázání s účty zaměstnanců v docházce (lze ale případně použít i zápis DOMENA\ucet pokud to doménový server dovoluje).
Hodnota slouží pro příkaz ldap_search jako parametr Filtr. Musí být dodržena velká/malá písmena.

"AD jméno" - Používá se pro import záznamů účtů z active directory do docházky a určuje název atributu s křestním jménem uživatele (zaměstnance).
Výchozí hodnota je givenName

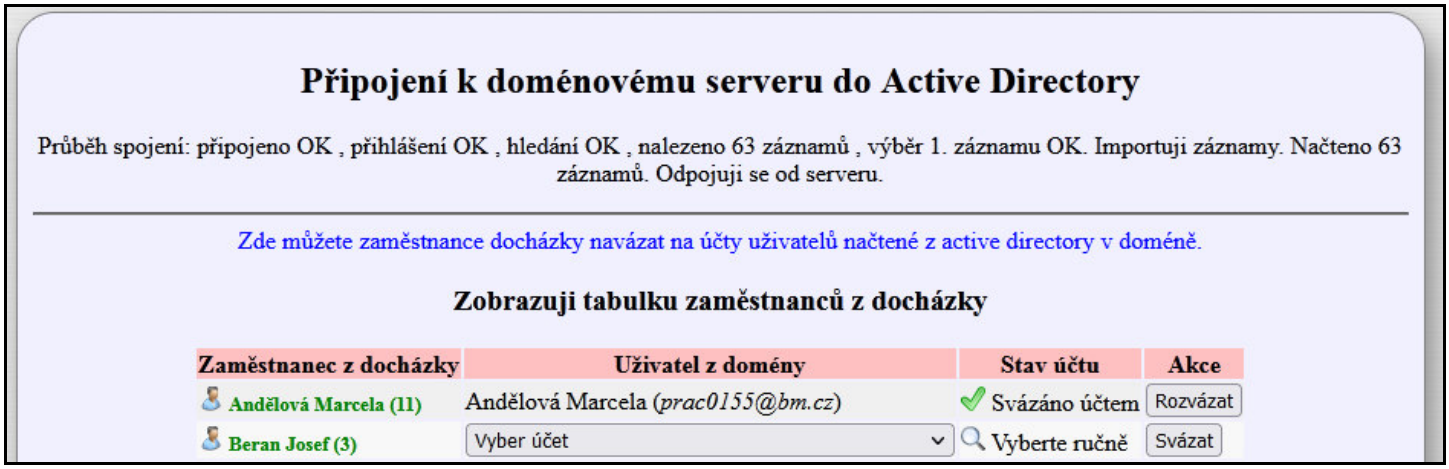
"AD příjmení" - Používá se pro import záznamů účtů z active directory do docházky a určuje název atributu s příjmením uživatele (zaměstnance).
Výchozí hodnota je sn

"AD login" - Používá se pro import záznamů účtů z active directory do docházky a určuje název atributu s plným názvem účtu, pod kterým se uživatel přihlašuje. Adresář by měl v této položce obsahovat plně kvalifikovaný název účtu včetně domény nejlépe ve formátů uživatel@doména (např. karel@firma.cz) nebo případně starší typ hodnoty ve formátu DOMÉNA\účet (např. FIRMA\karel) pokud doménový server toto podporuje.
Výchozí hodnota položky je userPrincipalName a předpokládá se, že adresář v tomto atributu obsahuje plně kvalifikovaný název účtu (např. karel@firma.cz).

Pokud jste upravili některý z parametrů, je třeba nastavení uložit. Doporučujeme použít tlačítko "Uložit a připojit", které zároveň provede načtení adresáře z domény a jeho zobrazení (viz další sekce), čímž se zároveň ověří, že zadané parametry fungují. Případně pokud nechcete nic upravovat a chcete přímo přejít na záznamy z domény, použijte tlačítko "Připojit bez úprav".

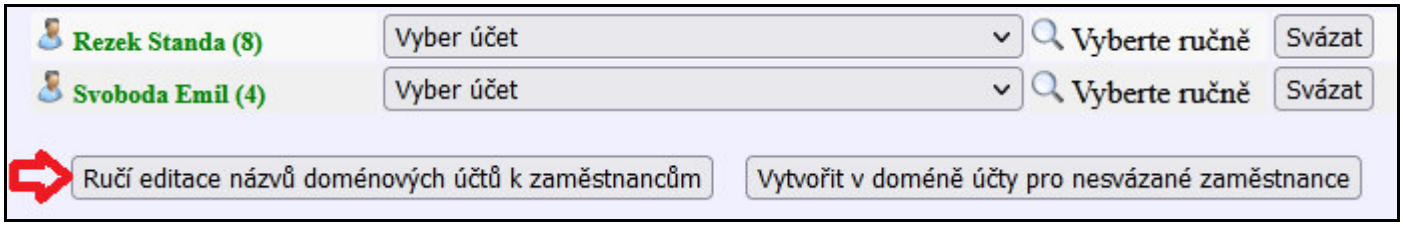
Zaměstnanci / Editace údajů / Import/export z Active Directory (LDAP) / ..Připojit
V tomto mudulu se provádí svazování účtů uživatelů z domény se záznamy zaměstnanců v docházce. Celé okno je rozděleno na tyto 4 části:

1. Připojení k doménovému serveru - Program se snaží připojit k doménovému serveru pomocí konfigurace z předchozí sekce a z tohoto serveru se snaží načíst záznamy adresáře uživatelských účtů. V této první části se zobrazuje log z průběhu připojení. Jednotlivé kroky jsou buď uvedeny stavem OK, nebo pokud nastane chyba, je uveden bod, ve kterém k problému došlo a připojení se zastaví.
Docházka nejprve provede vyhledání počítače - řadiče domény, poté se do něj snaží přihlásit. Dále prohledává jeho adresářovou službu, načte z ní všechny záznamy dle konfigurace z předchozí sekce a nakonec se od doménového řadiče odpojí.
Pokud vše proběhlo v pořádku, je zobrazena druhá až čtvrtá část:



2. Zobrazení tabulky zaměstnanců z docházky a jejich navázání na uživatelské účty z domény.
Pokud byl účet zaměstnance již dříve svázán s doménovým účtem, zobrazí se svazovací údaje a je případně možné účty rozvázat.
Jestliže ještě účty svázány nejsou, je možné k zaměstsnanci vybrat účet ručně ze zozbazeného seznamu účtů, které se v předchozím bodě podařilo z domény načíst. Program se dle jména a příjmení zaměstnance snaží nalézt uživatelský účet sám - jméno z domény se musí shodovat se jménem v docházce, zrovna tak obě příjmení musí být shodná. Pak stačí jen kliknout na tlačítko "Svázat" a účty se propojí.
Pokud program automaticky nenalezne vyhovující účet, zobrazí výzvu a účet musíte vybrat ze seznamu sami.
Ve sloupečku "Stav účtu" je stručná informace o zobrazených údajích. Uvádí se zde, zda je účet již svázán nebo zda je potřeba jej teprve svázat atd. Svázané účty jsou označeny zelenou fajkou. Na všechny ostatní případy je třeba se podívat a upravit je.
V případě, že více zaměstnanců docházky svážete s jedním určitým účtem z domény, je zobrazeno varování o kolizi účtů a červeně blikající šipky tyto kolizní záznamy označují. Ne vždy musí být tyto kolize chybou, proto je docházka toleruje. Například když Vaše firma zajišťuje evidenci docházky i pro cizí zaměstnance (například jiné firmy sídlící ve stejné budově), nemusíte pro tyto cizí pracovníky zadávat účty do Vaší domény. Stačí vybrat jeden doménový účet (host) a oproti němu ověřovat více cizích zaměstnanců. Spíše ale doporučujeme se této situaci vyhnout.

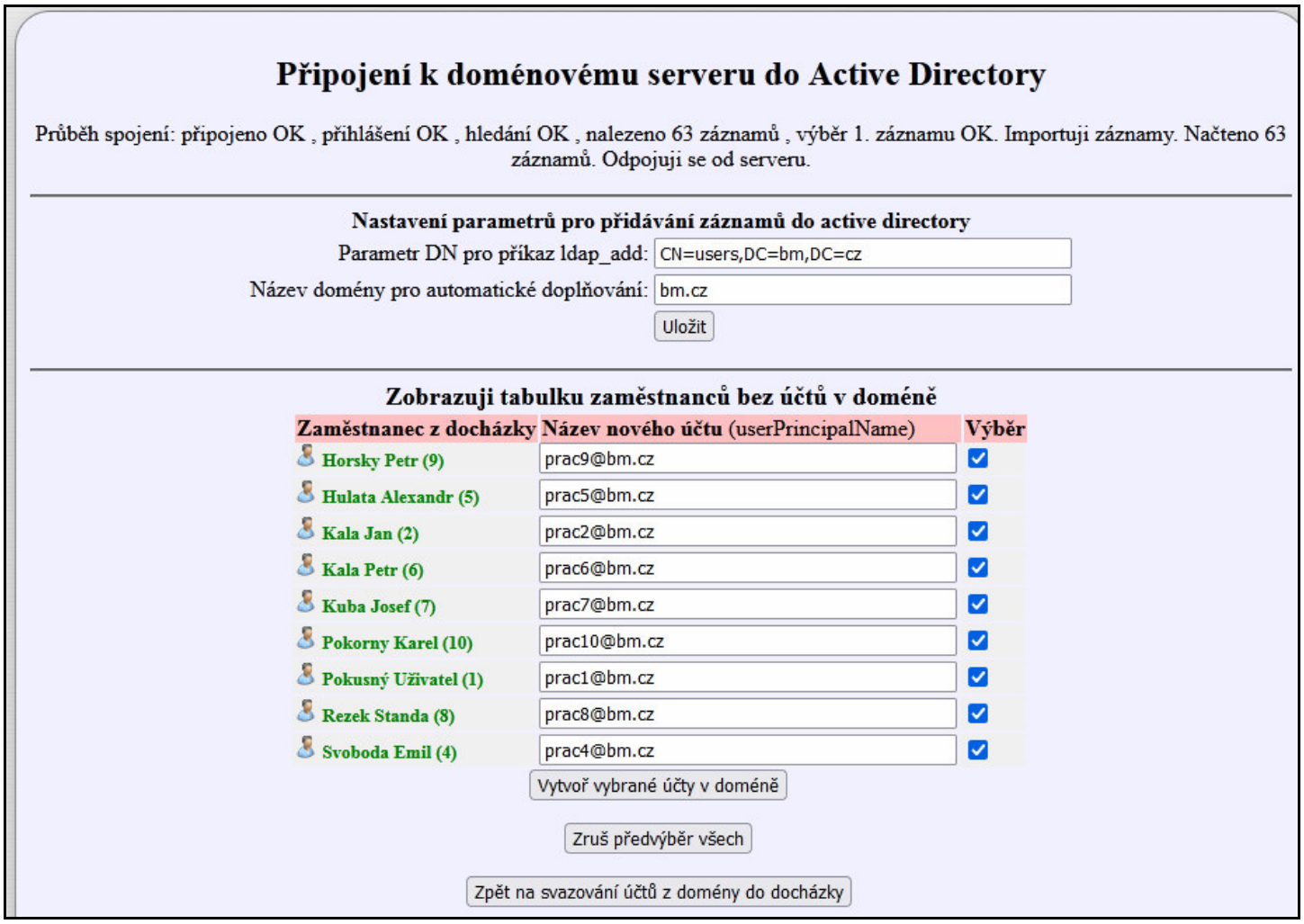
Pod tabulkou ještě naleznete tlačítko pro ruční editaci názvů doménových účtů.



Toto umožňuje zadat přihlašvací jméno zcela libovolně. Lze to využít například v situaci, kdy zaměstnanec z docházky ještě nemá založený účet v doméně a ten bude založen později. Podrobná nápověda je v další sekci pod čarou.

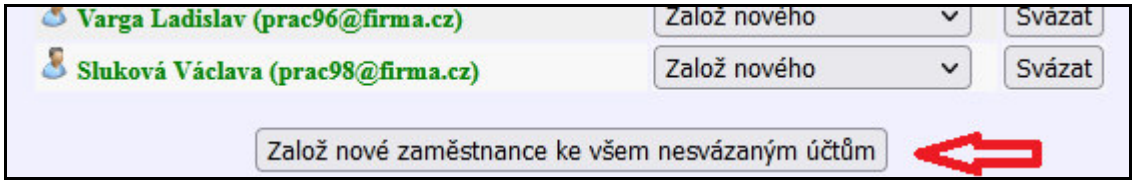
Jestliže jsou v tabulce nějací zaměstnanci, kteří ještě nemají svázaný účet s doménou a případně v doméně ani účty nemají, je možné jejich záznamy na doménový server nahrát - přímo z docházky založit účty v active directory. Docházka tedy umí z adresáře domény záznamy nejen načítat, ale i do něj zapisovat nové. V tomto případě se zobrazí tlačítko *"Vytvořit v doméně účty pro nesvázané zaměstnance"*

Přes které se zobrazí potřebné údaje. Viz nápověda přímo v jeho vlastním menu a ukázka níže:



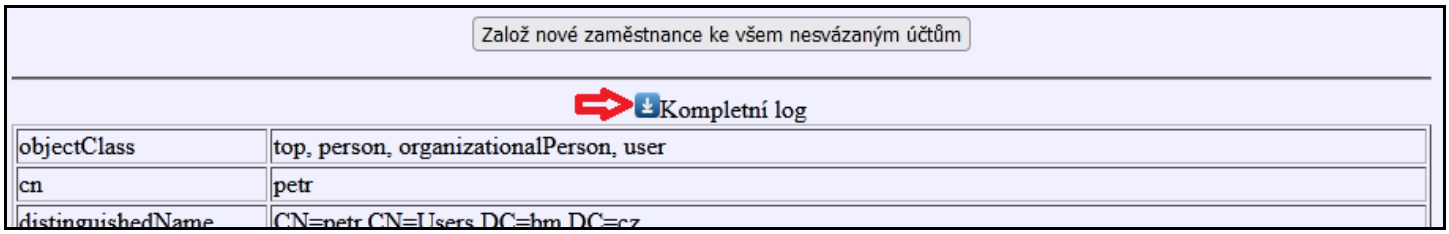
3. Třetí část úvodního okna umožňuje k účtům z domény, které ještě nejsou spárované se žádným zaměstnancem, vybrat správného zaměstnance pomocí výběrového menu ze seznamu zaměstnanců docházky. Umožňuje také k tomuto účtu založit v docházce zcela nového zaměstnance. V tomto případě se do docházky založí zaměstnanec jehož jméno a příjmení se načte z domény. Pokud nejsou zadána, nastaví se na text "Doplnit". Jako index je použito nejvyšší volné číslo, kategorie se nastaví na jedničku, oddělení se vybere první v pořad dle abecedy a nastaví se minimální práva. Takto založeného zaměstnance je téměř vždy nutné v docházce dále upravit (Zaměstnanci / Editace údajů ...) a doporučuje se v nastavení terminálového rozvodu, pokud používáte řídící jednotku BM-RJ02, kliknout na synchronizaci subjektů.
Pokud ale v doméně není žádný nesvázaný účet, tato tabulka se vůbec nezobrazí.

Pod výše uvedenou tabulkou (je-li zobrazena) ještě naleznete tlačítko, které umožňuje všechny nesvázané účty z domény převést na nové zaměstnance do docházky.



Tuto volbu ale využijete asi pouze v případě, kdy provádíte novou instalaci docházky, nebo jste do domény přidali hodně nových účtů novým zaměstnancům, kteří ještě nejsou ani v docházce. Pokud tuto funkci využijete a k čipování docházky používáte off-line variantu s řídící jednotkou BM-RJ02, doporučujeme po importu kliknout na tlačítko "Synchronizace subjektů" v menu "Firma / Terminálový rozvod". Tím se připraví záznamy pro řídící jednotkou BM-RJ02 a je pak možné přidělit zaměstnancům ID média (karty, čipy) v menu "Zaměstnanci / Editace údajů / Správa ID médií".
Toto tlačítko tedy umožní prvotní import zaměstnanců z domény do databáze docházky. Záznamy je pak ale většinou nutné v docházce "doladit" - nastavit kategorie pracovní doby, práva atd. atd. Funkce tedy umožní hlavně rychlý import jmen, příjmení a navázání na účty domény.

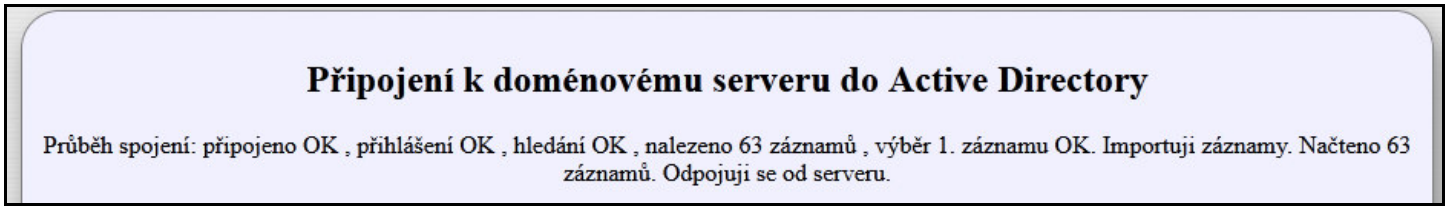
4. Poslední čtvrtá část umožňuje kliknutím na šipku vlevo dole zobrazit kompletní podrobný přehled přenesených záznamů - log přenosu z první části této sekce. Log může pomoci odborným administrátorům podrobně obeznámeným se strukturou adresářové služby dohledat případné nesrovnalosti v přenesených záznamech z domény - tedy chybně zadané údaje v doméně.



K výše uvedeným informacím ještě drobná poznámka. Docházka vnitřně používá kódování znaků iso-8859-2 a sama při importu textové položky překonvertovává ze znakové sady utf-8, kterou používají pro záznamy v active directory servery Windows. Pokud použijete jako doménový server například Linux a české znaky se Vám nebudou do docházky importovat správně, je třeba kódování změnit na serveru nebo si u výrobce docházky vyžádat úpravu programu.

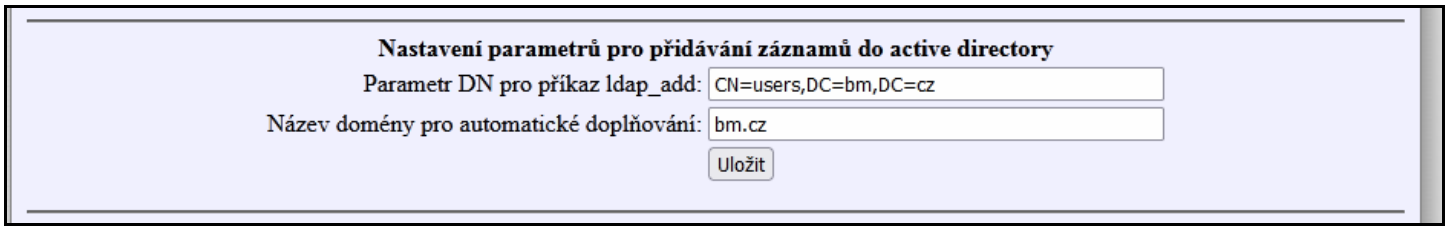
Zaměstnanci / Editace údajů / Import/export z Active Directory (LDAP) / ..Připojit / Ruční editace ...
Tato volba umožňuje zadat zaměstnancům v docházce ručně názvy účtů pro doménu, pokud se v předchozí části nedá nalézt účet v adresáři z domény. Tato volba by za normální situace neměla být potřebná. Pouze pokud budete účty v doméně zakládat později, můžete je v docházce zadat dopředu i když v doméně zatím neexistují. Určitě je ale vhodné po založení účtů v doméně zkontrolovat, zda se informace o účtech správně svázaly (nedošlo-li při ručním zadávání k překlepu atd.). I zde program hlídá a označuje kolizní záznamy a také prázdné položky.

Zaměstnanci / Editace údajů / Import/export z Active Directory (LDAP) / ..Připojit / Vytvořit v doméně účty ...
Jestliže jsou v docházce nějací zaměstnanci, kteří ještě nemají svázaný účet s doménou a případně v doméně ani účty nemají, je možné jejich záznamy na doménový server nahrát - přímo z docházky založit účty v active directory. Docházka zde tedy umí poslat do domény nové účty - zapsat do active directory nové záznamy.
Toto okno je opět rozděleno na několik čístí. V horní části je log soubor z průběhu připojení k doménovému serveru a načtení jeho záznamů.

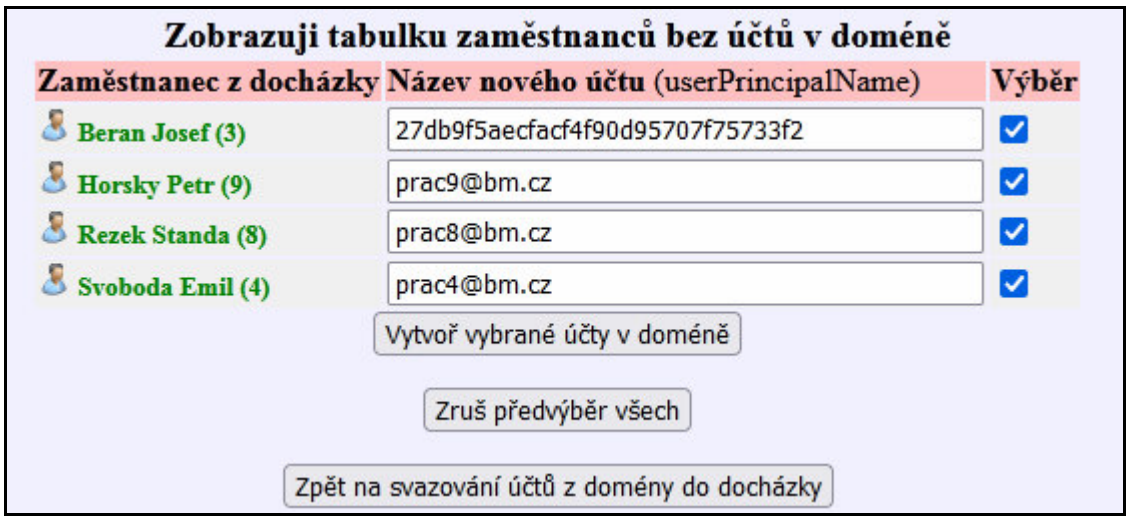


Druhá část slouží ke konfiguraci spojení. Konfigurace by se měla vytvořit sama - program se snaží provést potřebné úpravy v parametrech zadaných při vytváření spojení s doménou a nemělo by být nutné je měnit. Přesto je zde stručně popíšeme
Parametr DN pro příkaz ldap_add - určuje větev ve struktuře adresáře, do které se budou zapisovat nové účty. Standardně je nastaven na CN=users,DN=... kde se automaticky doplní hodnota položky "Bod hledání AD" konfigurované na první obrazovce pro spojení s doménou. Pokud chcete zapisovat údaje do jiné větve, můžete parametr náležitě upravit. Například když máme doménu firma.cz a chceme přímo do ní zapisovat do hlavní větve uživatelů, nastaví se zde hodnota CN=users,DN=firma,DN=cz
Nebo pokud máte zadanou organizační strukturu s odděleními a máte například založeno odděleni

"mojestredisko", pak nastavíte znak OU - např. OU=mojestredisko,DN=firma,DN=cz
Název domény pro automatické doplňování - udává samotné jméno domény, které se program opět snaží sám předvyplnit z položky "Bod hledání AD" tak, že použije pouze hodnoty DN=.... Takže pokud máte např. doménu firma.cz doplni sem program přesně tento název, tedy firma.cz a tuto koncovku používá pro přednastavení účtu zaměstnanců, kteří ještě nemají v doméně žádný účet - jméno účtu navrhne program z osobního čísla pracovníka (indexu), před který ještě doplní text "prac" a na konec doplní @ a jméno domény. Například pokud máme doménu firma.cz a pracovník má osobní číslo 15, navrhne program název účtu *prac15@firma.cz* ale toto můžete ručně změnit.



Další sekce již obsahuje hlavní tabulku, ve které jsou uvedeny zaměstnanci z docházky, kteří ještě nemají vyplněný doménový účet nebo jej sice vyplněný mají (někdo jej zadal ručně), ale tento účet v samotné doméně není - nebyl při prohledávání domény nalezen. Tabulka tedy obsahuje jména zaměstnanců z docházky a ve druhém sloupci navržené názvy pro účty v doméně. Název účtu samozřejmě můžete upravit ručně. V posledním sloupci je zatrhávací políčko. Pokud jej zatrhnete a dole pod tabulkou kliknete na tlačítko *"Vytvoř vybrané účty v doméně"*, pokusí se program do adresáře active directory na řadiči domény (doménovém serveru) vytvořit nové uživatelské účty pro vybrané zaměstnance. V horní části se zobrazí log soubor, ze kterého je poznat, zda se opravdu podařilo účty založit.
V případě problému je vypsáno odpovídající chybové hlášení. Pokud se některý účet nezaloží, může to být z několika důvodů:
- Účet zakládaného uživatele už v doméně existuje. Zejména při ruční úpravě jména účtu může k této situaci dojít.
- Zadaný účet má špatný tvar nebo příponu doménového jména (účet by měl správně vypadat jako e-mailová adresa)
- Uživatel, pod který se do active directory hlásíte (nastavený na první obrazovce) nemá právo vytvářet záznamy v adresáři.
- Máte špatně nastavenou položku *Parametr DN pro příkaz ldap_add*. Tedy ukazuje na špatnou větev struktury adresáře (záznamy CN) nebo do špatné domény (záznamy DN).



Program do adresáře sám doplňuje některé další parametry, které jsou v něm nastaveny napevno. Jedná se o tyto údaje:
["cn"][0] = *jméno účtu* *bez @ a doménové části*
["samaccountname"][0] = *jméno účtu* *bez @ a doménové části*
["objectclass"][0] = *konstata "top"*
["objectclass"][1] = *konstata "person"*
["objectclass"][2] = *konstata "organizationalPerson"*

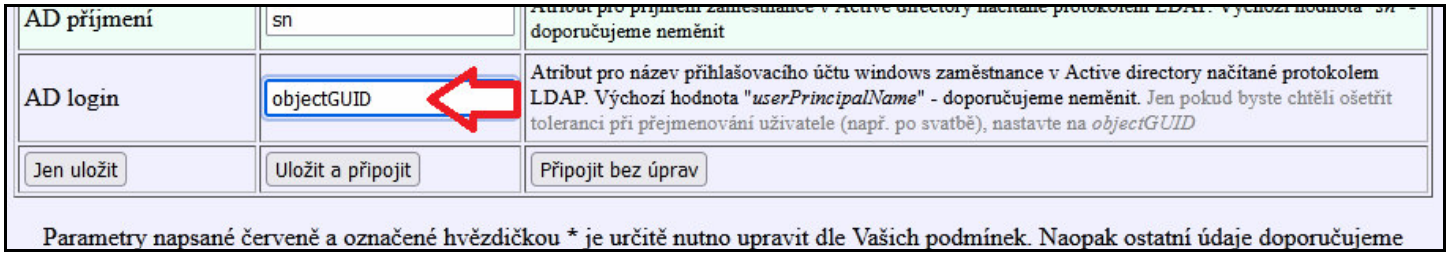
["objectclass"][3] = *konstata "user"*
["displayname"][0] = *příjmeni a jméno zaměstnance*
["name"][0] = *jméno účtu bez @ a doménové části*
["givenname"][0] = *jméno zaměstnance*
["sn"][0] = *příjmení zaměstnance*
["description"][0] = *konstanta "Index" a osobní číslo zaměstnance (index v docházce)*
["department"][0] = *Název oddělení, do kterého je zaměstnanec v docházce zařazen*
["mail"][0] = *e-mailová adresa v podstatě odpovídající celému jménu účtu včetně @ a domény*
["userprincipalname"][0] = *celé jméno účtu včetně @ a domény*

Poslední parametr (userprincipalname) poté používá docházka pro svázání záznamu zaměstnance s jeho doménovým účtem v adresáři a právě tento zadáváte ručně (nebo se jej program snaží odhadnout dám) v tabulce popsané výše v předchozím odstavci. Od verze 10.11 lze pro svazování použít i unikátní identifikátor *objecdGUID* - viz níže část věnovaná novinkám verze 10.11

Ještě je nutné připomenout, že nahrání účtů z docházky do adresáře v doméně neznamená, že tyto účty půjde okamžitě použít k přihlašování do Windows nebo k přihlašování do docházky. Na doménovém serveru se účty v adresáři sice zobrazí, ale nemají vytvořená hesla a nejsou v doméně povoleny. Tyto operace je nutné dokončit pomocí standardních nástrojů serveru domény. Minimálně tedy založit hesla a účty odblokovat.
Dalším napevno nastaveným kritériem je konverze znakových sad. Docházka vnitřně používá kódování iso-8859-2 a sama při exportu textové položky překonvertovává do znakové sady utf-8, kterou používají pro záznamy v active directory servery Windows. Pokud máte jako doménový server např. Linux a nastaveno kódování jiné než utf-8, je třeba jej buď změnit nebo si vyžádat úpravu docházkového sytému u výrobce.

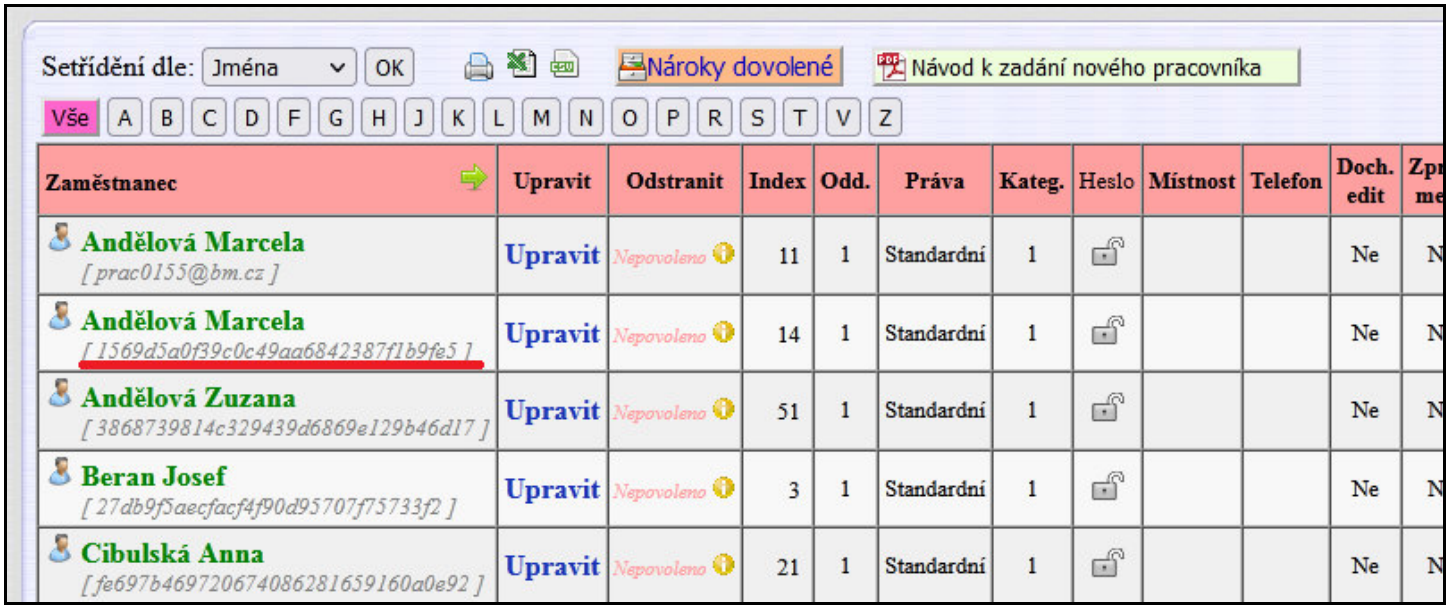
Novinky verze 10.11 - provázání uživatelů přes *objectGUID* místo *userPrincipalName*

Od verze 10.11 programu Docházka 3000 lze pro ověřování uživatelů vůči doméně použít jednoznačný identifikátor účtu v doméně nazvaný *objectGUID* obsahující unikátní 256 bitovou hodnotu. Výhodou tohoto řešení je, že pokud se změní jméno či příjmení zaměstnance (například po svatbě), nebo uživatele přesunete do jiné větve vaší domény, mění se i standardně používaná hodnota *userPrincipalName*, takže pak by bylo potřeba zaměstnance v docházce znovu svázat se správným uživatelským účtem v doméně, protože původní *userPrincipalName* se v doméně změnilo a docházka sama automaticky tuto změnu nepozná. Byl by tedy potřeba ruční zásah v docházce v menu *Zaměstnanci / Editace údajů / Import/export z Active Directory (LDAP) / ..Připojit.* Pokud ale v menu *Zaměstnanci / Editace údajů / Import/export z Active Directory (LDAP)* vložíte do položky *AD login* hodnotu *objectGUID*, tomuto problému se vyhnete:



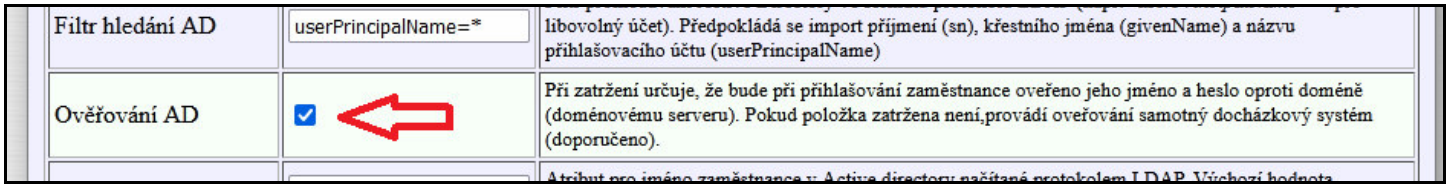
Docházka pak bude pro identifikaci záznamu v doméně používat tento jedinečný číselný identifikátor

V docházce v menu *Zaměstnanci / Editace údajů* je pak vidět jaký identifikátor je pro svázání s doménou použitý. Systém umožňuje smíšený režim, kdy povolí jak *userPrincipalName*, tak i *objectGUID*. Viz obrázek níže, kde první zaměstnanec používá původní *userPrincipalName* protože s ním byl svázán původně a před provedením změny konfigurační položky *AD login*, kdežto druhý a další zaměstnanci již byli svázaní nově po změně položky *AD login* na *objectGUID*.

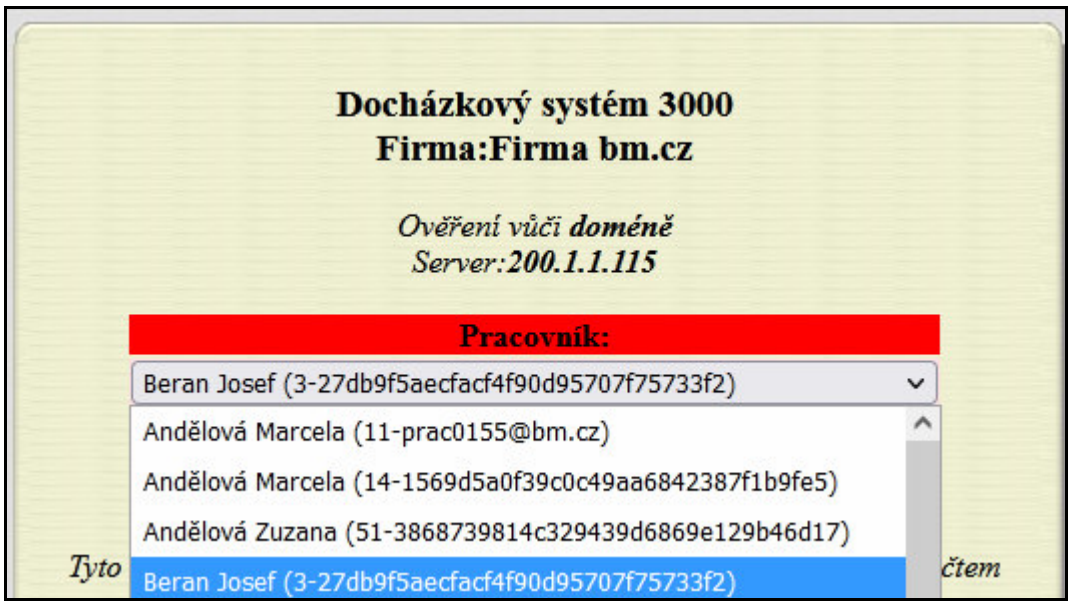


Sjednocení provedete novým svázáním v menu *Zaměstnanci / Editace údajů / Import/export z Active Directory (LDAP) / ..Připojit*, pokud by vám tento smíšený režim vadil.

A pokud v úvodním nastavení zatrhnete volbu *Ověřování AD* pro ověření přihlášení do docházky vůči doméně



bude i při přihlašování uživatele možné ověřovat jak oproti původnímu *userPrincipalName*, tak pokud se používá jednoznačný číselný identifikátor, tak vůči *objectGUID* a program při přihlašování zaměstnance v závorce za jménem zobrazuje který identifikátor má kdo nastavený



Ostatní informace

Jelikož docházka pro komunikaci s řadičem domény standardně používá nešifrovaný protokol LDAP, doporučujeme jí instalovat přímo na stejný server na kterém řadič domény běží a položku *Adresa serveru* tedy nastavit na 127.0.0.1, aby po síti nechodily informace v nešifrované podobě. Toto omezení se týká jen komunikace mezi docházkovým serverem a řadičem domény, nikoli externího přenosu dat od zaměstnanců. Při samotném přihlašování uživatelů z jejich PC je již šifrování použito, pokud nasadíte https protokol dle návodu v menu „*Firma / Návody PDF / Nastavení HTTPS*“.

Pokud v položce *AD login* použijete *objectGUID* místo *userPrincipalName*, budou se účty docházky svazovat s účty v doméně pomocí jedinečného 256 bitového identifikátoru (GUID) - viz část s novinkami verze 10.11. Zde ale upřesněme, že i když začnete používat objectGUID, tak pokud aktivujete ověřování přihlašování do docházky vůči doméně zatržením volby *Ověřování AD*, tak samotný příkaz *LDAP_Bind()* pro ověření hesla vždy vyžaduje *userPrincipalName*. V tomto případě si tedy musí docházka v doméně *userPrincipalName* nejprve dohledat pomocí *LDAP_search()* s parametrem filtru nastaveným na *objectGUID*. Za účelem tohoto hledání se však musí k řadiči domény přihlásit jako uživatel s vyšším oprávněním pomocí jména a hesla uživatele, pod kterým lze číst kompletní záznamy adresáře AD. K tomuto tedy použije parametry zadané v menu *Zaměstnanci / Editace údajů / Import/export z Active Directory (LDAP)* v položkách pro *Přihlašovací jméno* a *Přihlašovací heslo* (plus samozřejmě *Adresa serveru*) a v *LDAP_search()* použije i *Bod hledání AD* v jehož podřízené hierarchii se *objectGUID* vyhledává. To znamená, že pro přihlašování zaměstnanců do docházky s ověřením hesla v doméně AD pomocí *objectGUID* je nutné, aby první čtyři parametry (nadepsané červeně) v menu *Zaměstnanci / Editace údajů / Import/export z Active Directory (LDAP)* byly uloženy do databáze (přes tlačítko *Jen uložit* nebo lépe *Uložit a připojit*). Myslete tedy na to, že v databázi docházky jsou citlivé údaje nutné pro spolupráci programu s doménou. Zálohy databáze docházky proto udržujte chráněné tak, aby se k nim nedostala nepovolaná osoba. Což ale platí obecně, nikoli jen z důvodu ochrany údajů pro logování do AD.
Pokud byste nechtěli mít citlivé přihlašovací parametry do řadiče AD v databázi docházky uložené (přihlašovací jméno a heslo, adresa serveru a bod hledání uloženy být musí) a vždy tedy zadáváte jméno a heslo ručně znovu s tím, že klikáte na tlačítko *Připojit bez úprav* aby se parametry do DB docházky neuložily, nelze používat ověřování přihlášení do docházky vůči doméně pomocí *objectGUID*, ale je nutné párovat zaměstnance pomocí výchozího *userPrincipalName*, které nevyžaduje úvodní hledání přes *LDAP_search()* a přímo provede ověření pomocí *LDAP_Bind()*, protože zná *userPrincipalName* jednotlivých zaměstnanců.

Pokud je v nastavení napojení na AD zapnuto *Ověřování AD*, tak vůči doménovému serveru se ověřují jen přihlášení přes klasický přístup popsaná v Uživatelské příručce. Tedy úvodní obrazovku programu a její žluté menu vpravo *Přihlášení do systému* bez zadání admin. hesla. Jiné možnosti přihlášení se neověřují přes doménu ale čistě přes heslo v docházce. Jedná se například o přihlášení přes virtuální terminál (lokální či cloudový) popsané v menu *Firma / Návody PDF / Virtuální terminál*, přihlášení hashem či QR kódem které se nastavují v menu *Zaměstnanci / Editace údajů / Přihlášení hashem nebo QR kódem*, přihlášení přímo do modulu objednávek obědů v modulu stravovacího systému nastavované v menu *Ostatní / Obědy / Možnosti přihlášení* (kromě první zde popsané možnosti). Pokud tedy používáte virtuální terminál pro čipování docházky, nebo přímé přihlášení do docházky nebo modulu stravovacího systému heslem, hashem nebo QR kódem, tak zde se ověření vůči doméně neprovádí a to je tedy využito jen při vstupu zaměstnanců do plného uživatelského menu přes úvodní obrazovku programu.

Další technické podrobnosti k napojení na Active directory najdete přímo v programu v menu *Zaměstnanci / Editace údajů / Import/export z Active Directory (LDAP)* kliknutím na ikonu modrého otazníku vpravo dole.