

Správa uživatelů

Zakládání nových uživatelů

Po spuštění formuláře Uživatelé (pod Volby & Nástroje) je možné zakládat nové uživatele.

[image-1625213021074.png](#)

[uzivatele-novy.png](#)

Podrobnější návod naleznete na stránce [Založení nového uživatele](#).

Uživatelé se zakládají dle přednastavených šablon. **Šablony uživatelů** je vhodné vytvářet v případě zakládání většího počtu stejně nastavených lidí vstupujících do systému.

Obecná nastavení

[uzivatel-detail.png](#)

Uživatelské jméno

musí být v celém systému unikátní, jelikož slouží k jednoznačné identifikaci uživatele. Je vhodné uživateli rovnou přiřadit nesnadně odhadnutelné heslo. V případě internetových (portálových) uživatelů je doporučeno využití e-mailové adresy jako uživatelského jména.

Heslo uživatele

je vhodné přednastavit, není povinné, pokud je však zadané, je samozřejmě vyžadováno. Heslo rozlišuje malá a velká písmena, je možné využít libovolný znak.

Přeposílací e-mail

Je možné nastavit uživateli, pokud chce zasílat upozornění ze systému na externí e-mailovou adresu.

Výchozí organizace

Uživateli je vhodné vybrat **výchozí organizaci**.

Aktivní uživatel

Příznak **aktivní** slouží k blokaci účtu uživatele, v případě že nechcete aby měl do systému přístup.

Typ uživatele

Plnohodnotný vs Externí. Externí uživatelé jsou omezeni ve svých oprávněních a používají se pouze pro přístup prostřednictvím zákaznických webových aplikací (např. online přístup k projektům nebo fakturám pomocí webové stránky).

Správce

Ano/Ne. Správce je uživatel s přístupem ke specifickému nastavení systému. Aby mohl správce efektivně vykonávat svou činnost, měl by být zároveň zařazen do jedné ze skupin "Správce systému / Administrátor" apod.

Preferovaný jazyk

Jazyk je volbou nastavení multi-jazyčných číselníků použitých uživatelem. Nastavení neslouží k určení jazyka aplikace, to si každý uživatel určuje sám (při přihlašování).

Přiřazení uživatele do skupin

Je vhodné obecná práva systému nastavovat na uživatelské skupiny, a poté relevantně zařadit uživatele do dané skupiny. Standardní interní uživatel systému by měl být zařazen alespoň ve skupině Everyone.

Přiřazení role uživateli

Každý uživatel by měl být přiřazen do role Creator (pro případ, že je tato role v systému používána). Tato role je využívána v nastavení výchozích práv uživatele v libovolných složkách Atollon Directory (dle konfigurace).

Plná moc poskytnuta

Proxy users je seznam uživatelů, jejichž oprávnění daný uživatel přebírá formou jejich „**Plné moci**“ udělené uživateli. Tato práva je vhodné nastavit např. u vedoucích týmů v organizaci (touto formou je možné pružně definovat práva v rámci hierarchické organizační struktury). Dalším možným využitím tohoto nastavení je zastoupení uživatele v době jeho nemoci nebo nepřítomnosti jiným uživatelem.

Pozor 1:

Nastavením těchto práv získává uživatel přístup i do standardně **soukromých složek** uživatelů, získává tedy veškerá jejich práva.

Pozor 2:

Při nastavování Proxy práv se vyvarujte nastavení **cyklických** plných mocí, tedy např. schema: Uživatel Běda má právo na uživatele Anna, uživatel Anna na uživatelku Káťa a uživatelka Káťa na uživatele Běda. Nastavením těchto cyklických oprávnění ohrozíte chod systému.

Pokročilá nastavení uživatele

Uživatel si smí změnit heslo

V opačném případě nesmí, je využíváno zejména u sdílených účtů.

Uživatel musí změnit heslo při příštím přihlášení

Tento parametr je po prvním přihlášení uživatele a zároveň opětovném zadání hesla zrušen.

Víceuživatelský

Pouze pro super-administrátory. Parametr používaný pro univerzální uživatele (opět např. „internet“). Systém tomuto uživateli umožní multi-session přístup.

Uživatel může exportovat data

Uživatel smí exportovat např. kontakty, reporty, položky, apod. Funkce ovlivňuje pouze dostupnost této funkce na straně klienta. Při jiném přístupu k systému než prostřednictvím klientské aplikace tento parametr není platný.

Uživatel může importovat data

Uživatel smí importovat např. kontakty nebo položky. Funkce ovlivňuje pouze dostupnost této funkce na straně klienta. Při jiném přístupu k systému než prostřednictvím klientské aplikace tento parametr není platný.

Zobrazit pouze kontakty uživatele

Systém na klientské straně filtruje pouze kontakty, které uživatel založil nebo kde je odpovědnou osobou na nějakém ze souvisejících subjektů. Ostatní kontakty mu nejsou znepřístupněny, jsou však v jeho pohledu skryty. Funkce je využívána u implementací, kde uživatelé standardně nezískávají oprávnění zobrazit detaily subjektů ostatních uživatelů. Souvisí nejen s definováním pohledu uživatele, ale též s výkonností zobrazení systému. Jelikož systém vyhledává mezi subjekty, na které má uživatel oprávnění, je potřeba tímto parametrem systém navést, kde má data uživatele hledat.

V případě proxy-users (vedoucích týmů) jsou zobrazovány důvěrníkům i data/kontaky jemu zpřístupněných uživatelských účtů.

Další pokročilá nastavení

Kontext zpráv

V této záložce je možné definovat složky zpráv, které mají být součástí upozornění na nové zprávy daného uživatele. Pokud je do definované složky uložena nová zpráva, uživatel je o tom informován pop-up plachetkou v tray ikonce systému. Po založení uživatele se výchozí složka zpráv uživatele do seznamu složek pro upozorňování přidává automaticky.

Úkoly po vytvoření uživatele

Kontrola nastavených práv uživatele

Je vhodné zkontrolovat, zda-li práva na nově vytvořeného uživatele jsou správně definována. Práva jsou definována jednak přímo na kartě uživatele, avšak také ve stromové struktuře, která vznikne založením složek My Messages a Documents pod osobní složkou uživatele v User home.

V případě, že jste definovali uživatele s velmi specifickým oprávněním, může aplikace práv do systému trvat i několik hodin, v závislosti na objemu dat v systému. Je potřeba se tedy na příchod takovéhoho pracovníka připravit alespoň den předem.

Pro to, aby ostatní uživatelé mohli sdílet kalendář tohoto uživatele, je nutné přidat skupinu Interní uživatelé k právům Timesheet Access Rights, která jsou definována na kartě uživatele po jeho založení. Právo Authorize v tomto případě dává možnost určit uživatele nebo skupinu uživatelů, která má právo na schvalování výkazů práce daného uživatele.

Přihlášení se pod daným uživatelem pro kontrolu

V případě zcela nových nastavení práv je vhodné zkontrolovat jeho nastavení prostým testem, tj. přihlášením se do systému pod daným uživatelem a odzkoušením základních úkonů. Pokud se v průběhu přihlašování a práce nezobrazí žádné varovné hlášení nebo se zobrazí pouze žádaná varovná hlášení, je uživatel správně založen a organizace pravděpodobně správně nastavena.

Přístupová práva pro kalendář

Přístupová práva pro kalendář jsou nastavována a kontrolována odlišně od principu přiřazení práv k položce (např. e-mailu nebo dokumentu). Práva na práci s kalendářovými položkami (událostmi, úkoly nebo problémy) jsou určena kombinací dvou práv:

1. v nastavení **uživatele**, s jehož kalendářovými záznamy mohou ostatní uživatelé (či samotný uživatel) pracovat
2. v nastavení práv **kontextu**, ve kterém jsou kalendářové záznamy uloženy

Pokud tedy například uživatel Karel může nahlížet do kalendáře uživatele Petra, ale nemá právo na projekt BETA, detaily kalendářových položek Petra na tomto projektu uživatel Karel neuvidí. Naopak, pokud uživatel Karel má přístup na složku projektu ALFA, ale nikoliv na kalendářové položky uživatele Pepa, jeho položky na projektu ALFA nezobrazí.

Nastavení práv kalendářových položek pro daného uživatele je prováděno změnami v nastavení Práv výkazů práce (Timesheet access rights) na kartě uživatele (Nastavení > Access > User > Edit). Nastavením těchto práv se určuje, kdo (který uživatel nebo která skupina uživatelů) má právo na práci s kalendářovými položkami tohoto uživatele. Sám uživatel musí být v tomto nastavení uveden, pokud má mít na svůj kalendář přístup.

Nastavení práv kontextu je určeno právy na subjekt, projekt nebo aktivitu.

Práva na práci s kalendářovými položkami v systému jsou určena analogicky, jako u jiných položek. Tedy z pohledu nastavení práv na uživatele:

zakládání kalendářových položek	New
úprava	Edit
mazání	Delete
zobrazení	List a View

Výjimku z uvedených pravidel pro manipulaci s událostmi tvoří organizátor schůzky (uživatel, označený u víceuživatelské události jako HEAD), který může obejít nastavená práva ve víceuživatelských událostech. Práva, která zde obchází jsou Delete a Edit. Organizátor události může tedy danou událost mazat a měnit, bez ohledu na nastavení jeho práv u ostatních uživatelů.

Smazání nebo blokace uživatele

Dočasné zablokování uživatelského účtu

1. Volby & Nástroje -> Uživatelé -> dvojklik na uživatele -> nastavte volbu **Aktivní** na Ne.
2. [Přesměrujte uživatele e-mailovou adresou](#)

[image-1625219450034.png](#)

Trvalé odstranění uživatelského účtu

1. Volby & Nástroje -> Uživatelé
2. Označte uživatele a zvolte Smazat

[image-1625219630096.png](#)

Prosím mějte na paměti, že po odstranění účtu nebude dále možno filtrovat záznamy, které byly tímto uživatelem vytvořeny (včetně vytvořených pracovních výkazů, projektů, klientů atd.) V případě, že by tyto údaje měly být zachovány, uživatele ze systému nemažte, ale účet pouze deaktivujte.

V případě potřeby lze deaktivované účty znovu aktivovat.

Uživatelské účty nejsou po smazání technicky odstraněny z databáze. V případě, že jste omylem smazali záznam uživatele a potřebujete jej vrátit do předchozího stavu, můžete požádat o pomoc technickou podporu Atollon. Upozorňujeme, že tato operace vyžaduje restart serveru a je povolena pouze ve vyhrazených instancích Atollonu.

Profil uživatele

Profilová fotografie

Obrázek s podpisem uživatele

Podpis pod dokumenty generované uživatelem je možné nahrát v profilu uživatele.

[profil-uzivatele-fotka-podpis.png](#)

Revision #12

Created 24 July 2020 04:57:32 by safka

Updated 15 July 2023 08:04:09 by safka