

Přístupová oprávnění

- Základní vlastnosti přístupových oprávnění
- Správa uživatelů
- Práva na dokumenty
- Práva na kontext
- Založení nového uživatele

Základní vlastnosti přístupových oprávnění

Přístupová práva obecně

Přístupová práva v systému **Atollon Server Platform** (dále jen ASP) jsou spravována na serverové úrovni prostřednictvím modulu **mod.access**. Na klientské straně modul access zpřístupňuje administrační rozhraní pro definici přístupových práv systému. Samotná kontrola přístupových oprávnění probíhá z bezpečnostních důvodů pouze na serverové straně.

Přístupová práva jsou spravována ve stromové struktuře **Atollon Directory**. Stromová struktura obsahuje množství administračních složek, obsahujících rozličné definice či číselníky a složky obsahující data společnosti (např. kontakty, zprávy, dokumenty, apod.).

Viz schematicky [Atollon Tree Model.pdf](#)

Veškeré položky systému (jak koncové objekty (leaf object) - data tak složky (node)) mají svou vlastní definici přístupů (**ACL = Access Control List**), tedy seznam uživatelů, skupin nebo uživatelů přiřazených do role na projektu (klientovi, apod.), kteří mají svá přístupová oprávnění na danou položku. Systém při každé žádosti o akci na položce, u které je definována ACL, kontroluje přístupová oprávnění uživatele, pod jehož přihlášením je žádost podávána. (Např. pokud chce uživatel položku v seznamu, musí mít na ní LIST práva. Pokud chce položku smazat, musí na ní mít DELETE práva, apod.)

Uživatel systému

Uživatel je definován svým uživatelským jménem a heslem.

Uživatel v systému získává přístupová práva k jednotlivým položkám buď přímým přiřazením uživatele k dané položce, případně děděním uživatelských práv, přiřazením uživatele do role na projektu nebo složky klienta nebo přiřazením uživatele do skupiny, která má daná přístupová oprávnění. Specifickou vlastností je přidělení práv "v zastoupení". Lze poskytnout plnou moc uživateli na jiného uživatele a tak předávat práva definovaná individuálně jednotlivým uživatelům, např. v době nepřítomnosti, apod.

[detail-uzivatele-nastaveni-prav.png](#)

Doporučení

Výchozí práva v systému na jednotlivé objekty (typy složek, projektů, funkce - fakturace, formuláře, apod.) by se měla definovat ideálně vůči uživatelským skupinám (např. "Fakturace - schvalovatelé" nebo "Přehled klientů") - tak, aby se zachovala flexibilita při případných změnách v uživatelských oprávněních, jako jsou příchod nového zaměstnance, změna v oprávněních stávajícího uživatele, apod.

Skupiny je vhodné vytvářet pro každé právo, které vyžaduje speciální pozornost (např. "Obchodní případy - čtení" nebo "Obchodní případy - plná práva", apod.)

Více o nastavení uživatelů najdete v dokumentaci [Správa uživatelů](#).

Uživatelské skupiny

Uživatelská skupina je seznam uživatelů systému, kterým jsou přidělena stejná práva. Skupině je možné přiřadit libovolná práva pro kteroukoli položku systému, přičemž uživatelé přiřazení do dané skupiny tato práva automaticky získávají.

Uživatelské role

Ve speciálním nastavení je možné např. k složkám klientů a projektům přiřazovat uživatele do rolí. Díky přiřazení uživatele do definované role pak uživatel získává práva dané role. Práva role mohou být definována obecně pro veškeré projekty nebo složky klientů, přičemž uživatel získává práva pouze na konkrétních subjektech a projektech, ke kterým byl (do dané role) přiřazen.

Na kartě uživatele se určuje, do kterých rolí může být daný uživatel zařazen. Pokud uživatel nemá danou roli uvedenou ve svém nastavení, nemůže být do role obsazen.

Upozornění

Práva na role u složek klientů nebo projektů musí být definována v šabloně složky nebo projektu **před vytvořením** konkrétní složky nebo role. Pokud chcete definovat práva dodatečně, je nutné do **existujících projektů** a složek práva rolí zadat ručně nebo pomocí hromadných změn v reportingu.

Úrovně uživatelských oprávnění

New / Nový	Umožňuje uživateli založit novou položku (právo je aplikovatelné pouze pro složky nebo objekty, pod kterými lze něco nového založit)
List / Seznam	Umožňuje uživateli zobrazit název a některé základní atributy položky, bez zobrazení obsahu položky.

View / Zobrazit	Umožňuje uživateli zobrazení obsahu položky. Toto právo je většinou nutné kombinovat s právem list.
Edit / Upravit	Umožňuje uživateli měnit obsah dané položky (pokud je položka upravitelná). Toto právo však může být v různých částech systému omezeno v případě nutnosti schvalování, apod.
Delete / Smazat	Umožňuje uživateli smazat danou položku (pokud mazání položky umožňuje systém).
Authorize / Schválit	Umožňuje uživateli schvalovat danou položku (aplikováno pouze u některých položek systému).
Admin / Správa	Specifické právo, které může být definováno pouze uživatelem root . Pokud je toto právo v systému nastaveno, práva pro daného uživatele nebo skupinu nemohou být jakýmkoli uživatelem systému měněna. Toto právo se nastavuje zejména z důvodu zamezení náhodného odejmutí práv správcům systému (uživatelům, kteří jsou ve skupině Administrátoři).
Rights / Práva	Umožňuje uživateli měnit práva dané položky.
Finalize / Ukončit	Specifické právo, jež označuje zákaz dědění tohoto konkrétního nastavení v ACL. Využívá se např. při potřebě listovat složky / projekty. S tím, že je následně zakázáno dědění práv do zpráv na projektu, dokumentů, apod.

Další vlastnosti

Dědění práv

Z důvodu snadnější správy přístupových práv systém umožňuje dědění práv ve stromové struktuře. Výchozí dědění práv je nastaveno dle stromové struktury **Atollon Directory**, přičemž práva podřízených položek jsou vytvořena na základě **šablonových práv položky**.

Některé objekty dědí práva a podmiňují zobrazení z **vícero nadřazených objektů**. Např. faktura dědí všechna svá práva z nastavení administračního uzlu **Fakturace** + požaduje práva LIST na **Kontext**, ve kterém je faktura uložena + VIEW práva na **Deník**, do kterého faktura náleží.

Výchozí nastavení systému definuje, že všechny zakládané objekty dědí práva ze své nadřazené složky.

Příklad dědění práv ke zprávě "Poznámka" / e-mailu / dokumentu

Když napíšete poznámku na projekt u klienta, tento je umístěn na kartě klienta, klient je umístěn v organizaci, organizace v instanci a instance v rootu stromové struktury. Dokud se v celé této cestě práva dědí, tak všechny nadřazené složky ovlivňují práva dané zprávy.

Strom dědění práv může být košatý, jelikož např. práva projektu jsou ovlivněna právy uživatelů na Typ projektu + na složku klienta, ve které je projekt umístěn.

Obrázek výše znázorňuje cestu práv dané zprávy:

1. ACL dané zprávy (zde by bylo možné nastavit práva jednotlivým uživatelům, kteří mohou danou zprávu vidět/smazat, apod.)
2. ACL složky zpráv pro daný projekt
3. ACL projektu
4. ACL složky klienta
5. Proklik na: a) Definici typu složky Klient (PROJ...), b) ACL organizace ... a šlo by pokračovat na instanci + kořen stromu (top level)

Nastavení vlastních práv pro objekt = zakázání dědění

Pokud chcete nastavit na objekt zcela jiná oprávnění, než určuje nadřazená složka, je nutné zrušit dědění. Dědění je možné zastavit tím, že se odkazy na nadřazené uzly vymažou. Poté je možné nastavit práva pro každý objekt v Atollonu individuálně.

Práva na jednotlivé funkcionality

Níže naleznete odkazy na dokumentaci k nastavení práv jednotlivých modulů. Neváhejte kontaktovat svého konzultanta v Atollonu se žádostí o případné rozšíření / doplnění a vysvětlení kroků.

Práva na kontext

Definujte práva na typy složek (klienty), typy projektů (obchodní případy, služby, podpora, ...) nebo typy aktivit.

Práva na dokumenty

Definujte práva na dokumentové složky nebo dokumenty samotné.

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/kontakty 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](#)

Práva na dokumenty

Dokumenty jsou ukládány do libovolného uzlu stromové struktury v Atollonu. Tímto uzlem může být kontext (složky, projekty nebo aktivity), případně individuálně vytvořené složky pro ukládání pouze dokumentů (mimo nebo v rámci kontextu).

Postup nastavení individuálního oprávnění uživatelů na dokumentovou složku

Založte složku (např. v kontextu interní složky pro obchodní oddělení)

[dokumenty-zalozeni-slozky.png](#)

Zvolte nastavení práv složky

V kontextovém menu před dokumentovou složkou je volba na nastavení vlastních práv složky.

[dokumenty-slozky-nastaveni-prav.png](#)

Upravte nastavení práv složky

V této obrazovce můžete nastavit kteří uživatelé a skupiny uživatelů budou mít práva k dané složce.

Každá nově založená dokumentová složka má výchozí práva nastavena ze své nadřazené složky. Pokud chcete, aby ke složce měli přístup pouze vyjmenovaní uživatelé (nebo skupiny), je **nutné zrušit dědění** (odstranit odkaz na nadřazenou složku).

Upozornění

Zrušit dědění lze pouze tehdy, pokud vám zůstanou práva na administraci dané složky i po zrušení děděných práv. Nezapomeňte tedy před zrušením dědění práv nastavit sobě / skupině administrátorů plná práva, která umožní s nastavením složky dále pracovat. Odstraněním dědění na složce o práva definovaná v nadřazených složkách přijdete. Systém se vám v této procesní chybě pokusí zabránit.

[dokumenty-slozky-nastaveni-prav-zruseni-dedeni.png](#)

Práva na kontext

Nastavení práv na složky, projekty a aktivity

Všechny nově zakládané složky, projekty nebo aktivity mají v systému nastaveny práva vycházející z dvou základních informací o nově založené složce:

1. Právo na **nadřazenou složku** (např. právo projektu se odvíjí od schopnosti uživatele listovat (LIST právo) složku / klienta, na kterém je projekt umístěn, právo aktivity na projektu se odvíjí od schopnosti listovat projekt, na kterém je aktivita umístěna - odstraněním práva na projekt se odstraní i práva na veškeré jeho aktivity)
2. Právo na **typ složky, projektu** nebo **aktivity** (veškerá výchozí práva složky, projektu nebo aktivity se odvíjí od toho, zda-li daný uživatel má práva NEW, LIST, VIEW, EDIT, DELETE, ... na typu dané složky, projektu nebo aktivity)

Příklad

Uživatel ve skupině *Obchodníci* nemusí mít práva na projekt *Interní*, případně *Dodavatelé*. Úpravu provedete tak, že zkontrolujete, jaká práva má skupina *Obchodníci* na typ projektu *Interní* a typ složky *Dodavatelé*. Práva odeberete odstraněním dědení práv na konkrétním typu a celkovým nastavením práv individuálně pro daný typ složky nebo projektu. Dejte pozor, že po odstranění dědení práv je nutné znovu přidat práva pro skupiny, které mají s danou složkou pracovat, např. *Správce* nebo *Management*.

Příklad ověření práv na složce klienta

Než začnete měnit nastavení práv na typy složek (projektů, aktivit), je vhodné si překontrolovat aktuální nastavení na příkladu konkrétní složky. Viz např. složka klienta "Car Making Corporate".

[prava-pro-slozku-klienta.png](#)

Detail práv u konkrétní složky klienta

[prava-pro-slozku-klienta-detail.png](#)

Nastavení práv na typ složky

Nastavení kontextu - typu složky - práva

Úprava nastavení práv pro typy složek, projektů nebo aktivit je k dispozici prostřednictvím tlačítka pro nastavení práv typu složky, projektu nebo aktivity v **Nastavení kontextu**.

[08editon-context-rights.png](#)

Založení specifické skupiny pro typ složky

Je vhodné si založit pro každý kontrolovaný typ složky vlastní skupinu uživatelů. Typ složky pak uživatelům snadno zpřístupníte pouze tak, že uživatele do dané skupiny přidáte. Nebo kdykoli odeberete...

[prava-nova-skupina.png](#)

Úprava nastavení práv na typ složky

Nově vytvořenou specifickou skupinu (např. "Dodavatelé - plná práva") přidáte k typu složky "Dodavatelé". Přidáte práva pro správce systému (Administrátoři), případně Management a po uložení se vrátíte + odstraníte dědění. Nově již do složky budou mít přístup správci, management a všichni uživatelé, které vložíte do **skupiny Dodavatelé - plná práva**.

[prava-pro-typ-slozky-individualne.png](#)

Založení nového uživatele

1. V Options & Tools spustíte nastavení "Uživatelé".

[Snímek obrazovky 2024-05-23 v 9.01.17.png](#)

2. Klikněte na tlačítko "Nový uživatel".

[Snímek obrazovky 2024-05-23 v 8.51.17.png](#)

3. Zadejte detaily nového uživatele.

1. Nastavte uživateli odpovídající šablonu.
2. Vyplňte uživatelské jméno.
3. Zadejte nové heslo a zopakujte jej do pole "Potvrdit".
4. Zvolte nový kontakt a vyplňte uživatelské jméno, příjmení a e-mailovou adresu.

[Snímek obrazovky 2024-05-23 v 8.53.39.png](#)

4. Upravte nastavení nového uživatelského účtu.

1. Správce: Ano / Ne
2. Language: Czech
3. Přidejte či odeberte přístupové skupiny a role.

[Snímek obrazovky 2024-05-23 v 8.57.54.png](#)

5. V aplikaci Kontakty myší přetáhněte kontakt uživatele na "Náš kolega". Tímto vytvoříte složku uživatele.

[Snímek obrazovky 2024-05-23 v 9.03.42.png](#)

V Options & Tools spustíte "Editace poštovních schránek".

uziv6.png und or type unknown

6. Klikněte na tlačítko "Nový".

7. Vytvořte nový mailbox pro vaši doménu.

1. Ze seznamu vyberte uživatele.
2. Přepište název schránky na stejný, jaký mu byl vytvořen ve vašem primárním e-mailovém systému.
3. Ze seznamu domén vyberte "vasefirma.atollon.com".
4. V identitě upravte doménu na vaší primární. (adresa odesílatele musí odpovídat adrese nastavené v primárním e-mailovém systému).

uziv8.png und or type unknown