

Uživatelská příručka  
**CityWare.NET**  
**Identity management**



# OBSAH

## Obsah

<b>1</b>	<b>ÚVOD DO PROBLEMATIKY .....</b>	<b>1</b>
<b>2</b>	<b>ZÁKLADNÍ PRÁCE S PROGRAMEM .....</b>	<b>2</b>
2.1	ZALOŽENÍ ZÁZNAMU.....	2
2.2	EDITACE ZÁZNAMU .....	2
2.3	ULOŽENÍ EDITOVANÉHO DETAILU .....	3
2.4	EDITACE VAZEB 1:N A M:N .....	3
2.5	SYSTÉM ODKAZŮ.....	4
<b>3</b>	<b>UŽIVATELÉ/ZAMĚŠTNANCI.....</b>	<b>5</b>
3.1	IDENTITA.....	5
3.1.1	<i>Dostupné akce nad Identitou .....</i>	<i>5</i>
3.2	ÚČET.....	6
3.2.1	<i>Dostupné akce nad Účtem .....</i>	<i>6</i>
3.3	ROLE.....	7
3.3.1	<i>Dostupné akce nad Rolí .....</i>	<i>7</i>
<b>4</b>	<b>UŽIVATELSKÝ PROSTOR .....</b>	<b>8</b>
4.1	DOSTUPNÉ AKCE NAD UŽIVATELSKÝM PROSTOREM .....	8
4.2	UŽIVATELSKÝ PROSTOR CITYWARE.NET .....	9
<b>5</b>	<b>ORGANIZAČNÍ STRUKTURA .....</b>	<b>10</b>
5.1	STRUKTURA ORGANIZACE .....	10
5.2	ORGANIZAČNÍ JEDNOTKA .....	10
5.3	FUNKČNÍ MÍSTO.....	10
5.4	TYP ORGANIZAČNÍ JEDNOTKY.....	11
5.5	ORGANIZAČNÍ STRUKTURA – STROM.....	11
<b>6</b>	<b>ORGÁN VEŘEJNÉ MOCI (OVM).....</b>	<b>12</b>
6.1	AGENDY A AGENDOVÉ ROLE.....	12
<b>7</b>	<b>INFORMAČNÍ SYSTÉM .....</b>	<b>13</b>
7.1	AGENDOVÝ INFORMAČNÍ SYSTÉM (AIS) .....	13
7.1.1	<i>Načtení agend z RPP .....</i>	<i>13</i>
7.2	CERTIFIKÁTY.....	14
7.3	APLIKACE .....	14
7.3.1	<i>Řízení zobrazovaných agendových činnostních rolí v koncových aplikacích .....</i>	<i>14</i>
7.4	DODAVATEL.....	15
<b>8</b>	<b>ATRIBUTY .....</b>	<b>16</b>
8.1	GLOBÁLNÍ ATRIBUTY .....	16
<b>9</b>	<b>SYSTÉM.....</b>	<b>17</b>

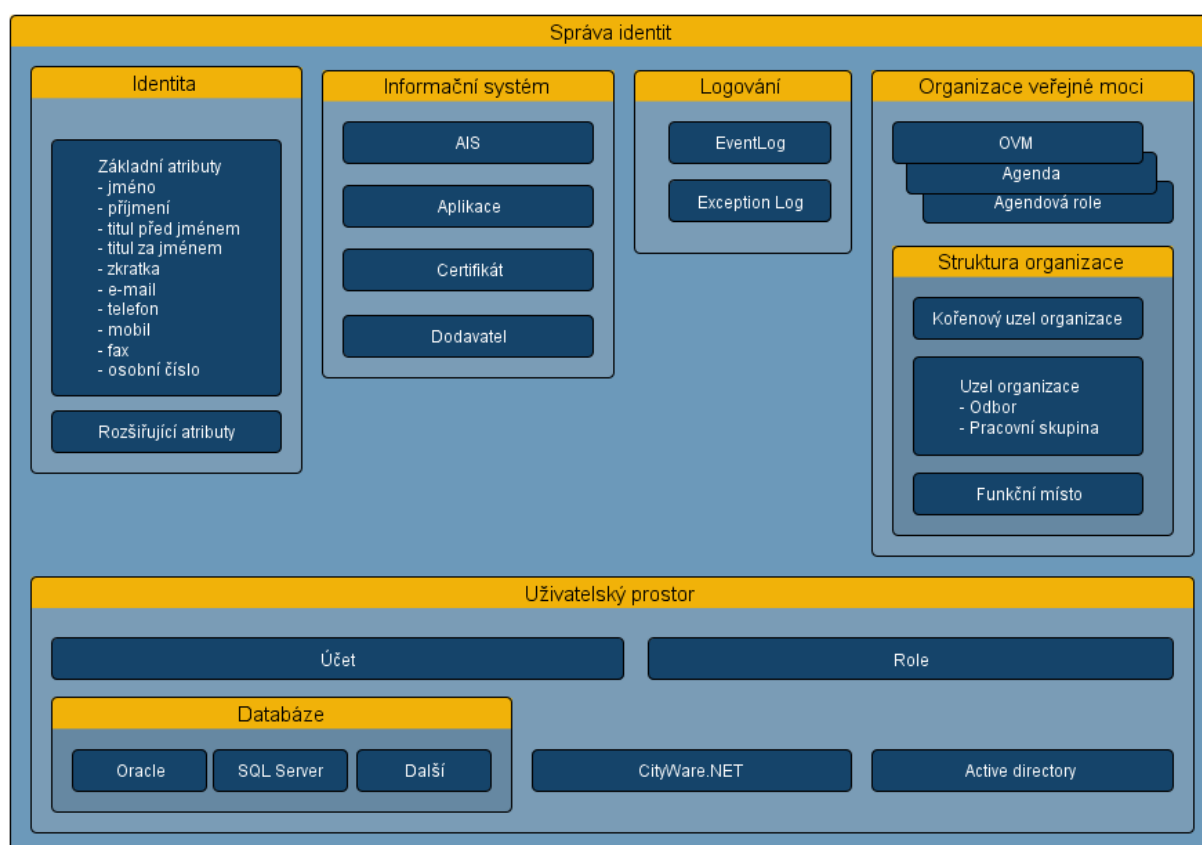
# 1 Úvod do problematiky

Identita – soubor vlastností, které jednoznačně určují konkrétního pracovníka/zaměstnance a jeho zařazení do funkčního schématu v rámci organizace. Na takto definovaný objekt je pak možné navazovat další vlastnosti – atributy k podrobné evidenci celého životního cyklu zaměstnance v organizaci.

Identity management je určen pro:

- správu a provázání účtů z různých uživatelských prostorů – jinak nesourodých systémů
- vedení informací o pracovníku/zaměstnanci
- delegování práv a povinností – přidělování rolí
- přehledné zobrazení aplikačních modulů, které jsou pro zaměstnance přístupné
- vedení AIS (agendový informační systém)
- vedení certifikátu k AIS a jejich uložení
- načítání a prohlížení agend a agendových činnostních rolí z RPP
- logování a archivaci změn

Schéma:

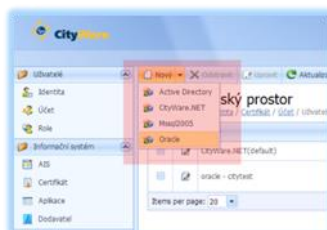


## 2 Základní práce s programem

Pro přehlednost uvádíme názvosloví uváděné na tlačítkách a jejich význam pro ukládání dat a vazeb.

### 2.1 Založení záznamu

Založení nového záznamu se provádí výběrem tlačítka Nový v levém horním rohu okna detailu - červeně podbarveno na obrázku vlevo. Pokud je klikem myši vybrán střed tlačítka – založí se záznam s prvním typem. Pokud je dispozici více možností typu daného záznamu a je vybrána šipka uvnitř tlačítka Nový, pak se nabídne v roletovém menu všechny dostupné typy záznamu. Po výběru se zobrazí formulář pro vyplnění údajů nového záznamu.

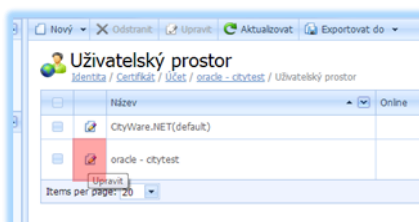


### 2.2 Editace záznamu

Editaci záznamu lze provádět dvojím způsobem, a to při zobrazení detailu tlačítkem Upravit.



Nebo tlačítkem zobrazeným v seznamu záznamů – podbarveno červeně.



## 2.3 Uložení editovaného detailu

Pro zakončení editace, popř. vkládání nového záznamu, slouží tlačítka nahoře a dole – na obrázku podbarveno červeně.

**Uložit** - záznam je uložen do databáze, ale zůstane v editačním módu pro další úpravy

**Uložit a Zavřít** - záznam je uložen do databáze a je pak zobrazen již jen v módu pro čtení

**Uložit a Nový** - záznam je uložen do databáze a je rovnou započata editace/vložení nového záznamu stejného typu

**Zrušit** - záznam není uložen a editace/založení nového záznamu je odvoláno

## 2.4 Editace vazeb 1:N a M:N

Například Identita může být navázána na více účtů. To se provádí přímo na detailu dané Identity na záložce Účet. Pro ovládání se použijí tlačítka přímo nad seznamem navázaných záznamů – účtů – červeně podbarvená tlačítka.

**Nový** – má stejný význam jako tlačítko popisované u detailu – má usnadnit ovládání v tom, že když uživatel zjistí, že daný účet ještě neexistuje, může ho založit rovnou zde a nemusí přebíhat do okna účtů.

**Odkaz** – vytvoří odkaz na již existující účet, otevře se nové okno, ve kterém se objeví seznam dostupných hodnot. Pokud je hodnot již mnoho, je třeba provést upřesnění navazovaného záznamu v horním řádku a stiskem tlačítka Hledej.

**Zrušit odkaz** – odebere účet od identity, ale účet bude nadále existovat

**Odstranit** – je zrušen odkaz a objekt – účet je nenávratně vymazán z databáze.

**!!! Pozor !!!**: V případě Odstranit je třeba si opravdu uvědomit, jaká akce se provádí. Je to čisté smazání záznamu a všech jeho návazností.

## 2.5 Systém odkazů

Dalším zjednodušením, které přináší nové rozhraní, je systém odkazů. Pokud se například účet odkazuje na Identitu, ke které patří, zobrazí se formou hyper-linku (na obrázku podbarveno červeně). Po kliknutí na hyper-link se rovnou přejde na detail daného objektu, v našem případě Identitu.

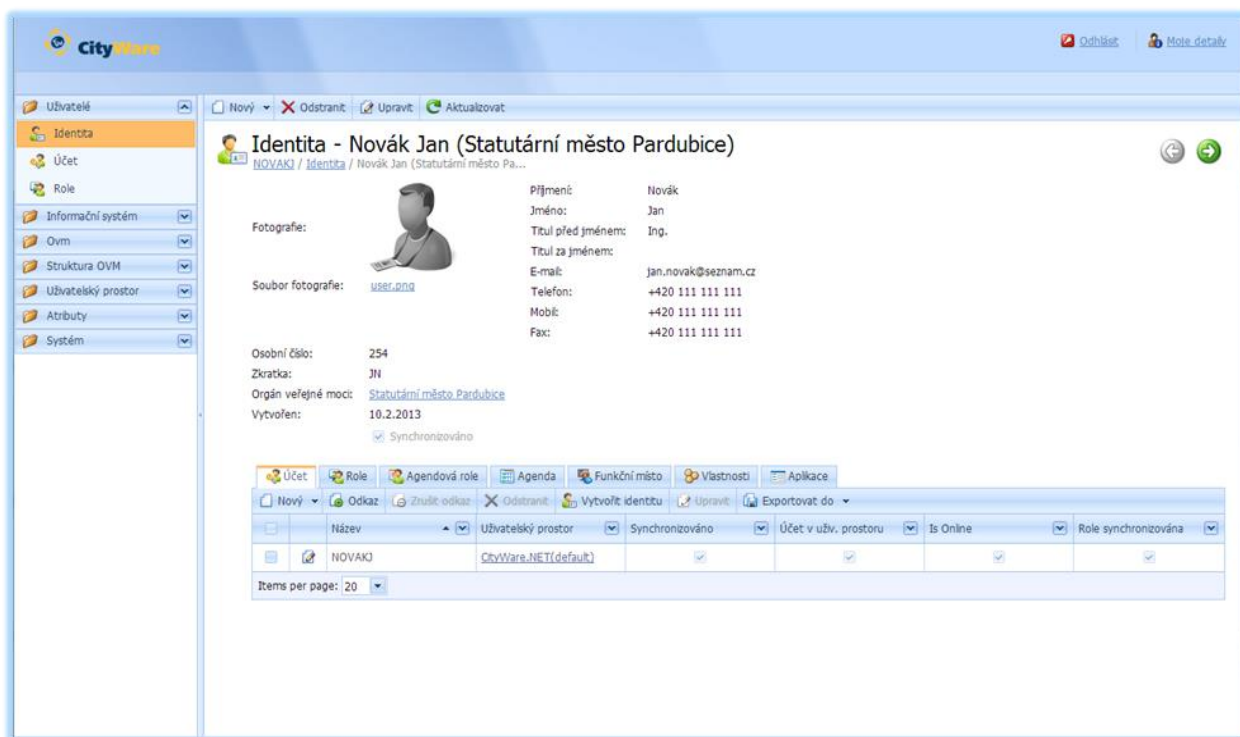


### 3 Uživatelé/zaměstnanci

V tomto oddíle se provádí rutinní správa Identity a jejích účtů.

#### 3.1 Identita

Základem celého systému je Identita uživatele, která u sebe spojuje evidenci popisných atributů zaměstnance s evidencí účtů a rolí v jednotlivých uživatelských prostorech. Dále s příchodem Základních registrů je pro Identitu nezbytné napojení na agendy a agendové činnostní role evidované v Registru práv a povinností jako jednoho ze Základních registrů. Pro snadnější správu identit je možné zařadit zaměstnance na funkční místo, které s sebou nese seznam rolí z jednotlivých uživatelských prostorů a agendových činnostních rolí, které musí mít zaměstnanec přiděleny pro výkon své funkce na dané pozici v organizační struktuře. Dále pak je možno rozšiřovat identitu o vlastní atributy v různých formátech (text, datum, číslo).



##### 3.1.1 Dostupné akce nad Identitou

- založení/editace/rušení Identity
- přiřazování/odebírání účtů
- přiřazování agendových činnostních rolí
- přiřazování/odebírání funkčních míst
- zobrazení přiřazených agend, aplikací a rolí ze všech uživatelských prostorů

Vlastnosti některých akcí:

- Role z jednotlivých uživatelských prostorů se přidělují v konkrétním účtu přiděleném identitě
- Přidělením funkčního místa identitě se automaticky přidělí účtům role podle typů uživatelských prostorů – pokud bude funkční místo obsahovat roli z uživatelského prostoru, ke kterému nemá identita přidělen účet, dojde k chybě. Stejně tak dojde i k přidělení agendových činnostních rolí.

Identita může mít přiřazeno:


- více účtů z různých uživatelských prostorů, ale vždy pouze jeden účet za jeden uživatelský prostor.
- více rolí i více agendových činnostních rolí
- více funkčních míst, ale jedno funkční místo může být přiřazeno pouze jedné identitě

Doplňkové informace:

- **Aplikace** – u identity se zobrazují ty aplikace, u kterých má alespoň jeden z účtů identity přiřazenu roli dané aplikace
- **Agendy** – zobrazují se ty agendy, ze kterých má identita přidělena alespoň jednu agendovou činnostní roli

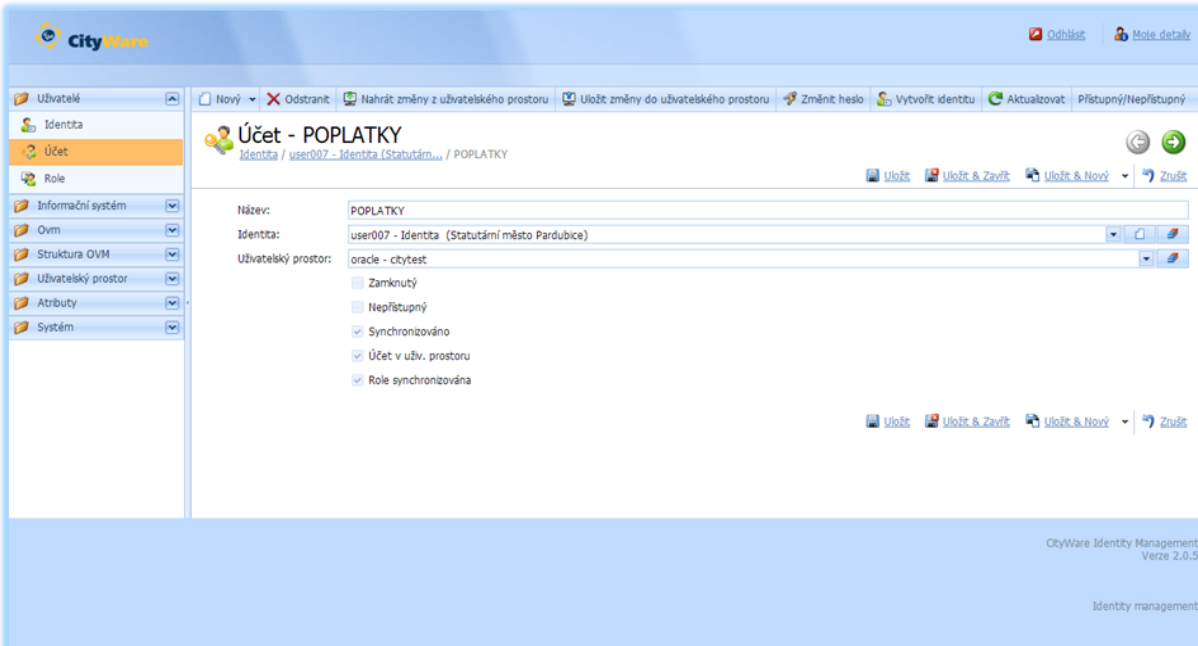
## 3.2 Účet

Účet vedený v IDM je chápán jako obecný účet, který má obraz v některém uživatelském prostoru např. ORACLE, MS SQL, CityWare.NET. Používá se k rutinní správě a zobecňuje nutné akce prováděné nad jinak nesoudržnými účty v různých uživatelských prostorech.

 **Video ukázka:** Založení účtu v uživatelském prostoru CityWare.NET (default) pro přiřazení aplikační role CityWare.NET ISZR Viewer a činnostních rolí Matriky z RPP (systém základních registrů) pro přihlášení pomocí NT Autentikace.

### 3.2.1 Dostupné akce nad Účtem

- **Založení/rušení**
- **Přiřazení účtu identitě** – stejně tak lze přiřazovat účet ze strany Identity
- **Vytvoření Identity z již existujícího účtu** – je využitelné zejména u účtů, které s sebou nesou další atributy – Jméno, Příjmení, e-mail, apod. (např. Active Directory)
- **Přístupný/Nepřístupný** – provedení zamčení, popř. odemčení účtu v cílovém uživatelském prostoru, provede se přímo do uživatelského prostoru, i když je Online
- **Změna hesla** – změna hesla se promítá přímo do uživatelského prostoru, i když je cílový uživatelský prostor označen jako Online
- **Nahrát změny z uživatelského prostoru** – promítne skutečný seznam rolí k účtu, potřebných tehdy, pokud někdo provede změny přímo v uživatelském prostoru, např. konzolí ORACLE, popř. příkazem přímo v databázi
- **Nahrát změny do uživatelského prostoru** – používá se v případě, že je cílový uživatelský prostor Offline a změna ještě nebyla promítnuta – přiřazení rolí





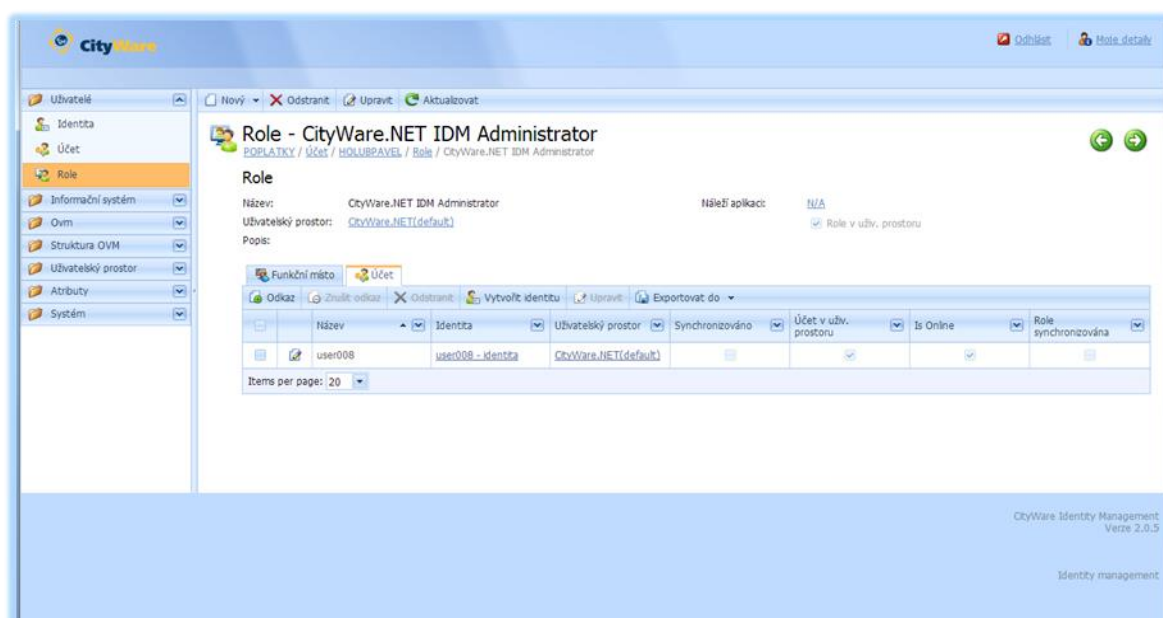
### 3.3 Role

Role, jsou stejně jako účty, popsané v předchozí kapitole, zobecněním všech rolí ze všech uživatelských prostorů zobrazené na jednom místě. V detailu role je pak patrné, zda je přidělena nějakému účtu a rovněž zda je synchronizována se svým uživatelským prostorem – tzn., že v něm existuje. Dále je v detailu přehledně zobrazeno, jak je role navázána na účty, popř. funkční místa.

**Jak vzniká role v systému:** vznikne ve chvíli instalaci aplikace, která role definuje a založí při instalaci, protože jediné aplikace zná způsob, jak se podle této role zachovat.

#### 3.3.1 Dostupné akce nad Rolí

- **Založení/editace/rušení** – samotné založení a editace nebude mít význam v tom směru, že role se nezakládají a ani jejich změny se nepromítají do cílového uživatelského prostoru, viz. popis výše, jak vzniká role v systému.
- **Přiřazení/Odebírání role účtu** – má smysl pouze přiřazení role účtu ze stejného uživatelského prostoru.
- **Přiřazení/Odebírání funkčního místa roli** – přiřazením role na funkční místo je okamžitě přiřazena i účtu XX pokud je funkční místo obsazeno identitou s navázaným účtem XX ze stejného uživatelského prostoru.



## 4 Uživatelský prostor

Uživatelský prostor je definován:

- účty s minimálně jménem, heslem, popř. autentizací vůči Active Directory
- role - opravňují účet s touto rolí k provádění akcí nad uživatelským prostorem
- účtu je možno přidělovat a odebírat role
- účtu je možné změnit heslo

Implementované uživatelské prostory:

- Databáze ORACLE, MS SQL Server
- CityWare.NET – uživatelský prostor nově tvořených aplikací, např. Cwn.IszrViewer.Web pro nahlížení do dat Základních registrů
- Active Directory (MS Windows Server 2003, MS Windows Server 2008)

Online/Offline:

- **Online** – změny prováděné v IDM se automaticky promítají do cílového uživatelského prostoru
- **Offline** – změny se provedou pouze v IDM a je nutné je do cílového uživatelského prostoru promítnout ručně u detailu konkrétního účtu. Změna hesla se vždy provádí pouze online, i pokud je uživatelský prostor offline.

### 4.1 Dostupné akce nad uživatelským prostorem

založení/editace/smazání uživatelského prostoru daného typu

aktualizace lokální kopie – pro rychlejší práci s IDM je vytvářeno lokální zrcadlo účtů a rolí – nelze je editovat pouze pro účely načtení účtů a rolí a zjištění stavu synchronizace



[Video ukázka](#): Založení uživatelského prostoru ORACLE, aktualizace lokální kopie účtů a rolí, nahrání vybraných účtů a rolí do IDM s možností pozdějšího využití pro přidělení identitě.

## 4.2 Uživatelský prostor CityWare.NET

Uživatelský prostor CityWare.NET je prostorem, kde jsou definováni uživatelé a role nového informačního systému, budované nad jednotným aplikačním frameworkem. Tzn., že všichni uživatelé pro aplikaci CwnlszrViewer musí být v tomto uživatelském prostoru definováni.

Existují dva možné způsoby založení účtu:

**jménem a heslem** – na jméno a heslo nejsou kladeny speciální nároky, velikost písmen je důležitá podle typu databáze, kde je IDM uloženo (ORACLE – ano, MS SQL – ne)

**NT autentikací** – jméno musí být velkými písmeny a uvedeno ve tvaru XXX\YYY kde XXX je doména a YYY je jméno uživatele z Active Direktory, na hesle v tomto případě nezáleží, ale může být uvedeno a pak lze i tento účet použít k přihlášení pomocí jména a hesla, kde jako jméno se použije kompletní XXX\YYY.

**CityWare.NET (default)** je uživatelský prostor, kde je nainstalován systém Cwnldm.

## 5 Organizační struktura

Organizační struktura umožňuje udržovat aktuální informace o zařazení zaměstnance na pracovní místo. Je možno založit několik organizačních struktur od hlavní až po jednotlivé pracovní skupiny. Celý strom je možno členit pomocí organizačních jednotek a koncovým funkčním místům přidělovat účty a role z jednotlivých uživatelských prostorů a agendové činnosti role pro vazbu na systém Základních registrů.

### 5.1 Struktura organizace

Každá organizační struktura má kořen, kterému je možno přiřadit název a příslušnost k OVM (orgán veřejné moci). Je tak možno definovat více nezávislých organizačních struktur.

### 5.2 Organizační jednotka

Slouží k dalšímu členění, může být napojena na kořen organizace, spravovat podřízené organizační jednotky a funkční místa. Funkční místa lze přezazovat z jedné ORJ do jiné.

### 5.3 Funkční místo

Funkční místo sdružuje předpis rolí a agendových činnostních rolí, které má mít zaměstnanec přiděleny, aby mohl vykonávat činnost svého pracovního místa.

Pokud je Identitě přiděleno funkční místo, jsou všechny činnostní role přiděleny účtům přiřazeným k identitě. Pokud pro danou roli neexistuje u identity účet, akce skončí s chybou.

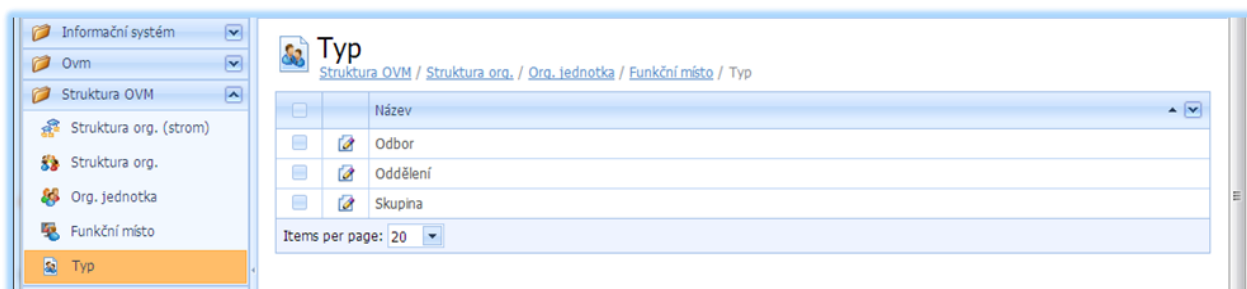
Odebráním funkčního místa identitě se opět odeberou role z účtů, které s sebou identita nesla.

Identitě, popř. účtům identity, mohou být přiděleny role a činnostní role i mimo funkční místo.

Funkční místa mohou existovat i mimo organizační strukturu.

## 5.4 Typ organizační jednotky

Každé organizační jednotce je možné přiřadit vlastní typ.



## 5.5 Organizační struktura – strom

Pro přehlednost je možné zobrazit organizační strukturu ve tvaru stromu s možností procházení a editace.



## 6 Orgán veřejné moci (OVM)

Orgán veřejné moci – číselník OVM, pro který jsou spravované identity. Je možné spravovat identity pro více než jedno OVM. V zobrazení detailu je možno rychle a přehledně zobrazit, kteří zaměstnanci jsou vedeni, jaké agendové role a agendy OVM vykonává a jaké spravuje AIS (agendové informační systémy).

Seznam agend je možno zakládat ručně nebo načítat z RPP (systému Základních registrů) poloautomaticky.

Název	Kód
Agenda o podmínkách provozu na pozemních komunikacích	A998
Agenda Rejstříku trestů	A483
Agenda řidičů	A1046
Agenda zákona o pohonných hmotách	A1104
Archivnictví a spisová služba	A1343
Autorské právo	A432
Celnictví	A392
Cestovní doklady občanů České republiky	A118

### 6.1 Agendy a agendové role

Menu agendy a agendové role umožňuje celkový přehled vykonávaných agend. Oba číselníky je možné naplnit přímým importem z RPP (registru práv a povinností).

Název	Kód	Kód agendy	Platné od
Doplnění IČO do IS EZP obecním úřadem obce s rozšířenou působností	CR2364	A944	2.3.2012
Editace údajů v ROS	CR2373	A944	2.3.2012
Kontrola	CR2370	A944	2.3.2012

## 7 Informační systém

Tato položka umožňuje vedení a správu AIS, které dané OVM provozuje i s vazbou na fyzické aplikační moduly.

### 7.1 Agendový informační systém (AIS)

AIS obsahuje informace pro možnosti napojení na ISZR. Informace o webových službách pro komunikaci s rozhraním ISZR, služby pro vyhledání adres GEOVAP, spol. s r.o. a vazbou na certifikáty AIS.

**AIS - CityWare**

Odevzdání řidičského průkazu... / Agenda / Činnosti dle zákona o zeměděls... / AIS / CityWare

**Ais**

Název: CityWare  
 Identifikátor ISVS: 744  
 Správce AIS: Statutární město Pardubice  
 Dodavatel: Geovap  
 Url pro CwnIszrWs: http://10.101.0.73/CwnIszrWs/CwnIszrWs.asmx  
 Url pro CwnGvpUirWs: http://ws.cityware.cz/UirRulan/UirWebServices.asmx  
 Url pro CwdIszrWs:

Název	Kód	Zkratka	Uživatelský prostor	Trusted App	Acc
CityWare.NET ISZR Viewer	67	CwnIszrViewer	CityWare.NET(default)	<input checked="" type="checkbox"/>	
Poplatky	1	POPL	oracle-citytest	<input checked="" type="checkbox"/>	

Items per page: 20

#### 7.1.1 Načtení agend z RPP

V seznamu agend bude neustále docházet ke změnám. Budou přidávány nové a již existující se mohou měnit. Agenda a agendová činnostní role se načítá do systému jen jednou a pak se aktualizuje podle čísla agendy, popř. role.

Načtení se spustí v okně seznamu AIS, kde se vybere jeden AIS a z menu se spustí *Data z RPP*, viz obrázek. Pro správné načtení musí být správně nakonfigurovaný AIS a musí existovat alespoň jedna agenda s rolí označená – Použít pro čtení z RPP.

**AIS**

Název: CityWare  
 Identifikátor ISVS: 744  
 Správce AIS: Statutární město Pardubice  
 Dodavatel: Geovap  
 Sériové číslo aktivního ce:

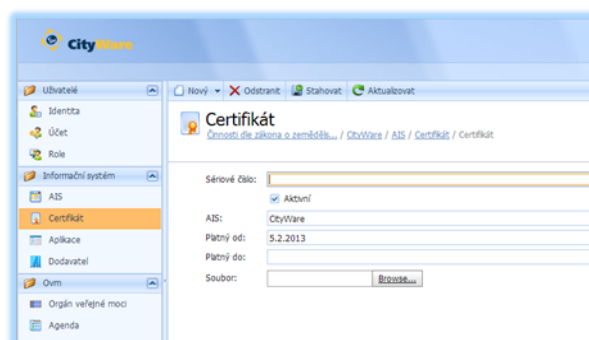
Název	Identifikátor ISVS	Správce AIS	Dodavatel	Sériové číslo aktivního ce
CityWare	744	Statutární město Pardubice	Geovap	

Items per page: 20



## 7.2 Certifikáty

Certifikáty umožňují uložit jak informace o platnosti certifikátu pro jejich jednoduchou správu a přehled, kdy který certifikát bude mít ukončenu platnost, tak provázání na AIS.



## 7.3 Aplikace

Aplikace je část IDM pro evidenci provozovaných aplikací s vazbou na AIS a provozované role. Je pak možné přehledně zjistit, jaká aplikace jaké používá role z jednotlivých uživatelských prostorů. Podle přidělených rolí se pak zobrazují aplikace přímo u Identity.

### 7.3.1 Řízení zobrazovaných agendových činnostních rolí v koncových aplikacích

Každá aplikace komunikující s IDM má přidělen kód, pod kterým vystupuje. Pokud by jedna aplikace vystupovala jako instance v rámci IDM vícekrát, musí být uvedena s jiným kódem.

**Proces:** Požadavek aplikace na seznam agendových činnostních rolí přihlášeného uživatele

Aplikace se identifikuje Kódem aplikace a uživatelským jménem, heslem, pod kterým je uživatel do aplikace přihlášen.

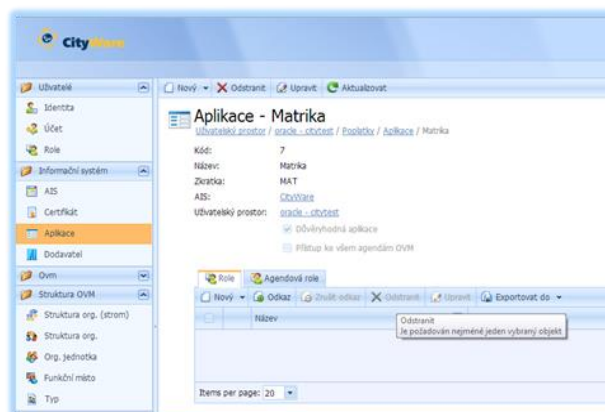
IDM identifikuje uživatele v uživatelském prostoru podle jména.

Pokud je aplikace v IDM označena jako Důvěryhodná tak se uživatel neověřuje (aplikace CityWare), jinak se ověřuje login do cílového uživatelského prostoru.

Podle zjištěného účtu IDM zjistí, ke které Identitě je účet přiřazen.

Zjistí se průnik agendových činnostních rolí, které jsou přístupné aplikaci a které jsou přístupné identitě a ty jsou vráceny aplikaci, ve které se nabídnou uživateli.

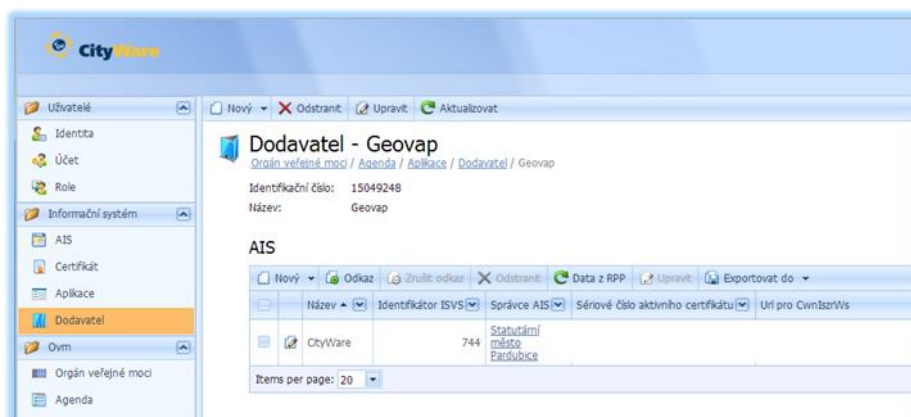
Pokud má některá aplikace nárok na všechny agendové činnostní role jako tomu je např. u CityWare.NET ISZR Viewer, tak lze využít volbu „Přístup ke všem agendám OVM“, která zajistí, že není třeba jmenovitě u aplikace udržovat přístupné role.





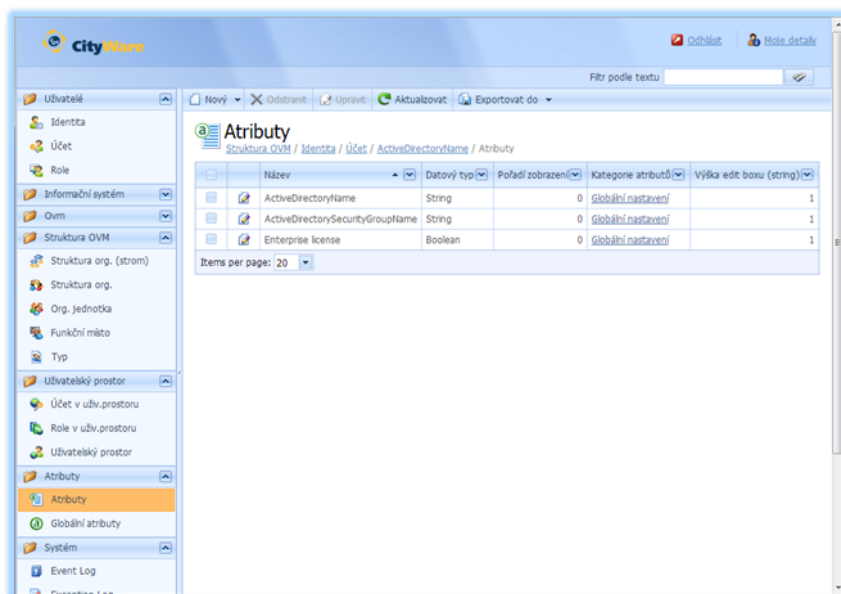
## 7.4 Dodavatel

Tato část umožňuje přehlednou správu dodavatelů s vazbou na AIS a dodávané aplikace.



## 8 Atributy

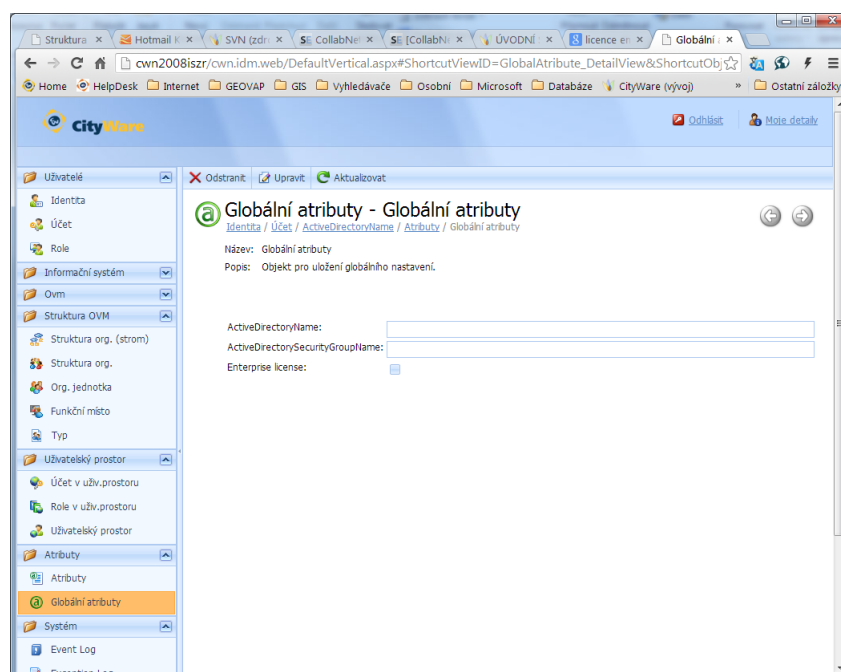
Část atributy umožňuje přidávat k základním atributům vedeným u IDM i atributy vlastní.



### 8.1 Globální atributy

Globální atributy pak slouží k nastavení některých atributů pro celé IDM.

ActiveDirectoryName a ActiveDirectorySecurityGroupName nyní není využíváno. Budou zde přibývat další nastavení.



## 9 Systém

V systémové části jsou logy prováděných akcí a komunikace s ISZR s možností fulltextového vyhledávání.

**Event Log** - Zapisuje se provádění akcí v IDM s možností vyhledávání a exportem, popř. tiskem do PDF, apod.

**Exception Log** - zachycují se zde výjimky při komunikaci s uživatelskými prostory.