|  |
| --- |
| synchronizace IDM se školním systémem bakaláři |

Obsah

Základní informace o dokumentu 2

Obsah 3

Seznam zkratek 4

1. Úvod 5

2. Způsob komunikace 6

3. Průběh synchronizace organizační struktury a osob 7

3.1. Aktualizace zaměstnanců 7

3.1.1. Aktualizace číselníku organizačních jednotek 7

3.2. Aktualizace studentů 7

3.2.1. Aktualizace číselníku organizačních jednotek 8

3.3. Aktualizace zákonných zástupců 8

3.3.1. Aktualizace číselníku organizačních jednotek 9

4. Mapování atributů rozhraní 10

4.1. Organizační struktura 10

4.1.1. Studenti 10

4.2. Osoby, uživatelské účty 10

4.2.1. Zaměstnanci 10

4.2.2. Studenti 11

4.2.3. Zákonní zástupci 13

4.2.4. Nastavení loginu a emailu uživatele 14

4.2.5. Nastavení typu účtu uživatele 14

4.2.6. Vyjmutí identity ze synchronizace 14

Seznam zkratek

|  |  |
| --- | --- |
| **Zkratka** | **Význam** |
| AD | ActiveDirectory |
| HTTP | Hypertext Transfer Protocol (Internetový protokol pro výměnu dat) |
| IDM | Identity Management |
| OJ | Organizační jednotka |
| FM | Funkční místo |
| HR | Personální systém |
| URL | Uniform Resource Locator (adresa zdroje informací na Internetu) |
| WS | Webová služba |
| WSDL | Web Services Description Language - popis rozhraní WS |
| Š | Škola |

1. Úvod

Klíčovým zdrojovým systémem systému IDM je typicky personální systém HR jako hlavní zdroj informací o zaměstnancích – interních uživatelích. V prostředí Š se pro evidenci zaměstnanců a také studentů používá školní systém Bakalář. Školní systém Bakalář bude pro IDM zdrojem informací o identitách a pro studenty také informací o jejich začlenění do organizační struktury organizace (OJ dle třídy studenta).

Předávání dat o identitách bude probíhat formou synchronizace systémů v definovaných časových intervalech. Stejně jako pro další synchronizované systémy, i pro Bakaláře bude v IDM nastaven synchronizovaný systém a definována konfigurace komunikace, intervalu zpracování, možnost notifikace chyb zpracování.

1. Způsob komunikace

Data o zaměstnancích, studentech a organizační struktuře organizace budou ze systému Bakaláři získávána z rozhraní WS, které poskytuje systém Bakaláři. V IDM konfiguraci synchronizace bude možné nastavit URL webové služby. Provoz WS a zpřístupnění WS musí zajistit objednatel, jde o webovou službu typu REST. Interface je přístupný na následující adrese:

<protocol>://<server>:<port>/<web-prefix>/if/2/<end-point>?<par1>=<val1>&...&<parN>=<valN>

Pokud je například webová aplikace Bakaláři provozována na adrese

https://zs.cz/bakaweb, potom datový interface bude přístupný na adrese

https://zs.cz/bakaweb/is/2/

V konfiguraci konektoru na straně IDM bude nutné definovat kořenovou organizační jednotku pro studenty (defaultně bude nastaveno na STUDENTS) a kořenovou organizační jednotku pro zaměstnance (defaultně bude nastaveno na STAFF). Pro studenty bude možné nastavit zařazení do organizačních jednotek dle tříd (použije se, pokud v bakalářích bude třída odpovídat zvyklostem pro AD kontejnery). Pro zaměstnance se organizační struktura v systému bakaláři neeviduje. Rozdělení zaměstnanců do OJ na pedagogické zaměstnance, nepedagogické, vedení školy apod. bude možné evidovat ručně v IDM.

Synchronizace bude umožňovat také import zákonných zástupců (opět do definované kořenové OJ). V prostředí Š bude import zákonných zástupců vypnut.

Synchronizace bude vždy probíhat jako „kompletní“ – ze školního systému se vždy načte kompletní seznam osob a porovná se s aktuálním stavem v IDM.

1. Průběh synchronizace organizační struktury a osob

V průběhu synchronizace IDM postupně načte ze školního systému seznam zaměstnanců, poté seznam studentů školy a nakokec seznam zákonných zástupců (import jednotlivých množin identit bude zapnut/vypnut v nastavení konektoru). Načte kompletní strukturu předaných dat a postupně zpracuje jednotlivé části struktury.

**Pro zpracování se berou pouze osoby, které mají ve školním systému nastaveno <Deleted>false</Deleted>, tj. nejsou zrušení.**

* 1. Aktualizace zaměstnanců

V prvním kroku proběhne aktualizace zaměstnanců.

Jednoznačným identifikátorem osoby ve školním systému bude identifikátor ID.

Pro jednu osobu ze školního systému bude vytvořen záznam osoby s jedním uživatelským účtem v doméně organizace.

1. Služba vyhledá ve vstupních datech osoby, které pro danou organizaci dosud nejsou zaevidovány a provede zaevidování požadavku na změnu - zavedení nové identity včetně přiřazení do organizační jednotky dle definice v nastavení konektoru (kód OJ v rámci organizace). Při zavedení nové identity vygeneruje IDM přihlašovací jméno (login) podle platných pravidel pro vytváření uživatelských účtů.
2. Služba identifikuje uživatele chybějící ve vstupních datech. Zaeviduje nový změnový požadavek na deaktivaci uživatele.
3. Služba porovná údaje kompletní identity ve vstupních datech a v systému IDM a změny zaeviduje do změnových požadavků identity.

Ze školního systému jsou načítáni pouze aktivní uživatelé (tj. <Deleted>false</Deleted>). Neaktivní uživatele se ze školního systému nenačítají.

* + 1. Aktualizace číselníku organizačních jednotek

Ve školním systému není pro zaměstnance evidována informace ohledně organizačního členění. Synchronizace tedy organizační jednotky pro zaměstnance nespravuje, jejich správu je možné provádět ručně v IDM. Nový zaměstnanec po importu ze školního systému dostává přiřazenou OJ dle nastavení konektoru. Následně ho správce IDM může přesunout do libovolné OJ v rámci organizace. Další synchronizace ze školního systému již nemění OJ uživatele.

* 1. Aktualizace studentů

V dalším kroku proběhne aktualizace studentů.

Jednoznačným identifikátorem osoby ve školním systému bude identifikátor ID.

Pro jednu osobu ze školního systému bude vytvořen záznam osoby s jedním uživatelským účtem v doméně organizace.

1. Služba vyhledá ve vstupních datech osoby, které pro danou organizaci dosud nejsou zaevidovány a provede zaevidování požadavku na změnu - zavedení nové identity včetně přiřazení do organizační jednotky dle třídy studenta a definice v nastavení konektoru (kód OJ v rámci organizace). Při zavedení nové identity vygeneruje IDM přihlašovací jméno (login) podle platných pravidel pro vytváření uživatelských účtů.
2. Služba identifikuje uživatele chybějící ve vstupních datech. Zaeviduje nový změnový požadavek na deaktivaci uživatele.
3. Služba porovná údaje kompletní identity ve vstupních datech a v systému IDM a změny zaeviduje do změnových požadavků identity.

Ze školního systému jsou načítáni pouze aktivní uživatelé (tj. <Deleted>false</Deleted>). Neaktivní uživatele se ze školního systému nenačítají.

* + 1. Aktualizace číselníku organizačních jednotek

Pokud při importu studenta dosud nebude v IDM existovat organizační jednotka s kódem dle třídy studenta, bude OJ třídy vytvořena (rodičem bude OJ dle definice kořene OJ pro studenty v nastavení konektoru), kód a název OJ bude dle třídy. Správce IDM může vytvořenou OJ ručně upravit (mimo změny kódu).

Z logiky importu je zřejmé, že existující OJ studentů se needitují ani nedeaktivují.

* 1. Aktualizace zákonných zástupců

V dalším kroku proběhne aktualizace zákonných zástupců (**na Š bude import zákonných zástupců vypnut).**

Jednoznačným identifikátorem osoby ve školním systému bude identifikátor ID.

Pro jednu osobu ze školního systému bude vytvořen záznam osoby s jedním uživatelským účtem v doméně organizace.

1. Služba vyhledá ve vstupních datech osoby, které pro danou organizaci dosud nejsou zaevidovány a provede zaevidování požadavku na změnu - zavedení nové identity včetně přiřazení do organizační jednotky dle definice v nastavení konektoru (kód OJ v rámci organizace). Při zavedení nové identity vygeneruje IDM přihlašovací jméno (login) podle platných pravidel pro vytváření uživatelských účtů.
2. Služba identifikuje uživatele chybějící ve vstupních datech. Zaeviduje nový změnový požadavek na deaktivaci uživatele.
3. Služba porovná údaje kompletní identity ve vstupních datech a v systému IDM a změny zaeviduje do změnových požadavků identity.

Ze školního systému jsou načítáni pouze aktivní uživatelé (tj. <Deleted>false</Deleted>). Neaktivní uživatele se ze školního systému nenačítají.

* + 1. Aktualizace číselníku organizačních jednotek

Ve školním systému není pro zákonné zástupce evidována informace ohledně organizačního členění. Synchronizace tedy organizační jednotky pro zákonné zástupce nespravuje, jejich správu je možné provádět ručně v IDM. Nový zákonný zástupce po importu ze školního systému dostává přiřazenou OJ dle nastavení konektoru. Následně ho správce IDM může přesunout do libovolné OJ v rámci organizace. Další synchronizace ze školního systému již nemění OJ uživatele.

1. Mapování atributů rozhraní
   1. Organizační struktura
      1. Studenti

Pouze vytváření nových OJ, viz kapitola Aktualizace číselníku organizačních jednotek. Vytváření OJ dle tříd pro studenty musí být zapnuto v konektoru.

|  |  |  |
| --- | --- | --- |
| **Atribut response WS** | **Atribut IDM** | **Poznámka** |
| Student.ClassName | Organizační jednotka – kód | Musí být unikátní v rámci organizace  Povinný údaj |
| Student.ClassName | Organizační jednotka - název | Povinný údaj |
| Viz poznámka | Organizační jednotka – nadřazená položka | Konstanta dle nastavení konektoru, kde je uveden kód rodičovské OJ pro studenty. |
| Viz poznámka | Organizační jednotka – typ | Konstanta  Kód „TR“, název „Třída“.  Musí dle kódu existovat v číselníku typů OJ, jinak nebude nastaveno. |

* 1. Osoby, uživatelské účty
     1. Zaměstnanci

|  |  |  |
| --- | --- | --- |
| **Atribut response WS** | **Atribut IDM** | **Poznámka** |
| Staff.ID | Uživatel – synchronizované systémy – mapování | Jednoznačný identifikátor ve zdrojovém systému |
| Staff.PersonalNum | Osoba – osobní číslo | Unikátní v rámci organizace. Může se měnit (předpokládá se změna pouze při chybném zadání v HR a následné opravě).  Nepovinný údaj. |
| Staff.RodneCislo | Osoba – rodné číslo | Nepovinný údaj. |
| Staff.Email | -- |  |
| Staff.Deleted | Uživatel – stav | Pokud je deleted false, pak aktivní. Jinak ukončený.  Povinný údaj. |
| Viz poznámka | Uživatel – aktivní od | Nastaví se na aktuální datum při vytvoření zaměstnance.  Povinný údaj |
| Viz poznámka | Uživatel – aktivní do | Datum ukončení pracovního poměru. Při zakládání účtu se nevyplňuje, nastaví se na předchozí den při deaktivaci uživatele. Maže se při aktivaci uživatele. |
| Staff.Title | Osoba – titul | Akademický titul před jménem. |
| Nesynchronizuje se, zatím není v response z WS API Bakalářů. V budoucnu bude pravděpodobně v Staff.Title2 | Osoba – titul za jménem | Akademický titul za jménem. |
| Staff.FirstName | Osoba – jméno | Povinný údaj |
| Staff.LastName | Osoba – příjmení | Povinný údaj |
| Viz poznámka | Uživatel – organizační jednotka | Kód primární organizační jednotky uživatele. Pro nové uživatele se nastaví dle definice v nastavení konektoru (kód OJ v rámci organizace).  Pro existující účty se nemění. Povinný údaj |
| Nesynchronizuje se, nebo konstantní FM | Uživatel – primární pracovní pozice | Kód primární pracovní pozice (FM) uživatele. Nepovinný údaj  Při implementaci si zákazník zvolí, zda IDM nemá pole synchronizovat, nebo nastavit konstantní FM (učitel). |
| Staff.PhoneMobile | Osoba – kontakty – hodnota kontaktu pro typ kontaktu mobil soukromý | Mobil soukromý |
| Staff.AddressStreet | Osoba – kontakty – adresa trvalá – ulice |  |
| Staff.AddressNumber | Osoba – kontakty – adresa trvalá – číslo popisné |  |
| Staff.AddressCity | Osoba – kontakty – adresa trvalá – město |  |
| Staff.AddressZIP | Osoba – kontakty – adresa trvalá – PSČ |  |
| **Staff.ExtraItems.ExtraItem[.Name=NET\_RFID].Value** | Osoba – uživatelské atributy - Číslo čipu | V systému bakaláři je název pole NET\_RFID  Je nutné volat WS s parametrem udávající název pole v DB, tj. GET na URL:  /if/2/common/staff?Fields=NET\_RFID |

* + 1. Studenti

|  |  |  |
| --- | --- | --- |
| **Atribut response WS** | **Atribut IDM** | **Poznámka** |
| Student.ID | Uživatel – synchronizované systémy – mapování | Jednoznačný identifikátor ve zdrojovém systému |
| Student.EvidNum | Osoba – osobní číslo | Unikátní v rámci organizace. Může se měnit (předpokládá se změna pouze při chybném zadání v HR a následné opravě).  Nepovinný údaj. |
| Student.RodneCislo | Osoba – rodné číslo | Nepovinný údaj. |
| Student.Email | -- |  |
| Student.Deleted | Uživatel – stav | Pokud je deleted false, pak aktivní. Jinak ukončený.  Povinný údaj. |
| Viz poznámka | Uživatel – aktivní od | Nastaví se na aktuální datum při vytvoření zaměstnance.  Povinný údaj |
| Viz poznámka | Uživatel – aktivní do | Datum ukončení pracovního poměru. Při zakládání účtu se nevyplňuje, nastaví se na předchozí den při deaktivaci uživatele. Maže se při aktivaci uživatele. |
| Nesynchronizuje se | Osoba – titul | Akademický titul před jménem. |
| Nesynchronizuje se | Osoba – titul za jménem | Akademický titul za jménem. |
| Student.FirstName | Osoba – jméno | Povinný údaj |
| Student.LastName | Osoba – příjmení | Povinný údaj |
| Student.ClassName | Uživatel – organizační jednotka | V konfiguraci konektoru bude možno nastavit, zda OJ studentů nastavovat dle tříd. Pokud bude zapnuto, synchronizace bude udržovat kód primární organizační jednotky uživatele dle třídy ve zdrojovém systému. Dohledá se OJ dle třídy, pokud neexistuje, vytváří se pod kořenovou OJ nastavenou v definici konektoru. Pokud třída není uvedena, OJ studenta se nastaví na kořenovou OJ v definici konektoru. Povinný údaj |
| Student.ClassName | Uživatel – uživatelské atributy – Třída studenta | Nepovinný údaj |
| Nesynchronizuje se, nebo konstantní FM | Uživatel – primární pracovní pozice | Kód primární pracovní pozice (FM) uživatele. Nepovinný údaj  Při implementaci si zákazník zvolí, zda IDM nemá pole synchronizovat, nebo nastavit konstantní FM (student). |
| Student.PhoneMobile | Osoba – kontakty – hodnota kontaktu pro typ kontaktu mobil soukromý | Mobil soukromý |
| Student.AddressStreet | Osoba – kontakty – adresa trvalá – ulice |  |
| Student.AddressNumber | Osoba – kontakty – adresa trvalá – číslo popisné |  |
| Student.AddressCity | Osoba – kontakty – adresa trvalá – město |  |
| Student.AddressZIP | Osoba – kontakty – adresa trvalá – PSČ |  |
| **Student.ExtraItems.ExtraItem[.Name=NET\_RFID].Value** | Osoba – uživatelské atributy - Číslo čipu | V systému bakaláři je název pole NET\_RFID  Je nutné volat WS s parametrem udávající název pole v DB, tj. GET na URL:  /if/2/common/students?Fields=NET\_RFID |

* + 1. Zákonní zástupci

V prostředí Š bude import zákonných zástupců vypnutý.

|  |  |  |
| --- | --- | --- |
| **Atribut response WS** | **Atribut IDM** | **Poznámka** |
| Controller.ID | Uživatel – synchronizované systémy – mapování | Jednoznačný identifikátor ve zdrojovém systému |
| Controller.StudentID | Uživatel – uživatelské atributy – Student (zákonný zástupce pro) | Doplní se ID studenta z bakalářů, jméno, příjmení a třída.  Nepovinný údaj. |
| Controller.Deleted | Uživatel – stav | Pokud je deleted false, pak aktivní. Jinak ukončený.  Povinný údaj. |
| Viz poznámka | Uživatel – aktivní od | Nastaví se na aktuální datum při vytvoření identity.  Povinný údaj |
| Viz poznámka | Uživatel – aktivní do | Datum ukončení platnosti. Při zakládání účtu se nevyplňuje, nastaví se na předchozí den při deaktivaci uživatele. Maže se při aktivaci uživatele. |
| Nesynchronizuje se | Osoba – titul | Akademický titul před jménem. |
| Nesynchronizuje se | Osoba – titul za jménem | Akademický titul za jménem. |
| Controller.FirstName | Osoba – jméno | Povinný údaj |
| Controller.LastName | Osoba – příjmení | Povinný údaj |
| Viz poznámka | Uživatel – organizační jednotka | Kód primární organizační jednotky uživatele. Pro nové uživatele se nastaví dle definice v nastavení konektoru (kód OJ v rámci organizace).  Pro existující účty se nemění. Povinný údaj |
| Nesynchronizuje se, nebo konstantní FM | Uživatel – primární pracovní pozice | Kód primární pracovní pozice (FM) uživatele. Nepovinný údaj  Při implementaci si zákazník zvolí, zda IDM nemá pole synchronizovat, nebo nastavit konstantní FM (zákonný zástupce). |

* + 1. Nastavení loginu a emailu uživatele

Login ani email uživatele se z Bakalářů nepřebírá (Login uživatele v systému Bakaláři není). Login generuje IDM dle dohodnutého algoritmu (bude popsáno v návrhu AD integrace). Email bude generován dle dohodnutého algoritmu (bude popsáno v návrhu AD integrace).

* + 1. Nastavení typu účtu uživatele

Pro všechny osoby z HR budou v IDM vytvořeny účty s typem účtu AD + email účet.

Typ účtu je atribut uživatele v IDM, možnosti nastavení typu účtu jsou:

* Interní účet (používá se pro účty v IDM doméně)
* Účet AD
* Účet AD + mail

Typ účtu má většinou pouze informativní charakter. Zda má mít uživatel v nějakém dalším systému vytvořen AD účet nebo mailový účet většinou závisí na přiřazení aplikační role pro konkrétní systém, viz detailní dokument integrace pro daný systém.

* + 1. Vyjmutí identity ze synchronizace

Pro nově vytvořené identity synchronizace automaticky na založeného uživatele přiřadí aplikační roli BakalariSynchro.

AC jednorázově přiřadí všem uživatelům z AD domény tuto aplikační roli před prvním spuštěním synchronizace se systémem bakaláři.

Pokud v IDM bude uživateli odebrána nebo zakázána aplikační role BakalariSynchro, uživatel se nebude synchronizovat. Obecně v IDM platí, že uživatel může mít aplikační roli přímo přidělenou nebo ji může zdědit z OJ, FM nebo skupiny. Pokud uživatel má stejnou roli z více míst (např. přímo přiřazenou uživateli a také na jeho FM a OJ), z nichž jedna bude z příznakem zakázáno. Zákaz vždy vyhrává, synchronizace se chová jako by uživatel roli neměl.