

WordPress

Da bi se davateljima usluga olakšala implementacija AAI@EduHr autentikacije u sustavu WordPress, razvijen je poseban dodatak (engl. plugin) pod nazivom *WP AAI@EduHr Auth*.

Dodatak *WP AAI@EduHr Auth* u sustavu WordPress omogućuje jednostavnu zamjenu standardnog WordPress autentikacijskog mehanizma s AAI@EduHr autentikacijom. Dodatak se može konfigurirati tako da dopusti prijavu samo određenim korisnicima ili može dopustiti prijavu svim korisnicima koji se autenticiraju preko AAI@EduHr sustava. Također, moguće je ograničiti prijave po određenim ustanovama. Dodatak se može koristiti u testnom ili producijskom AAI@EduHr okruženju.

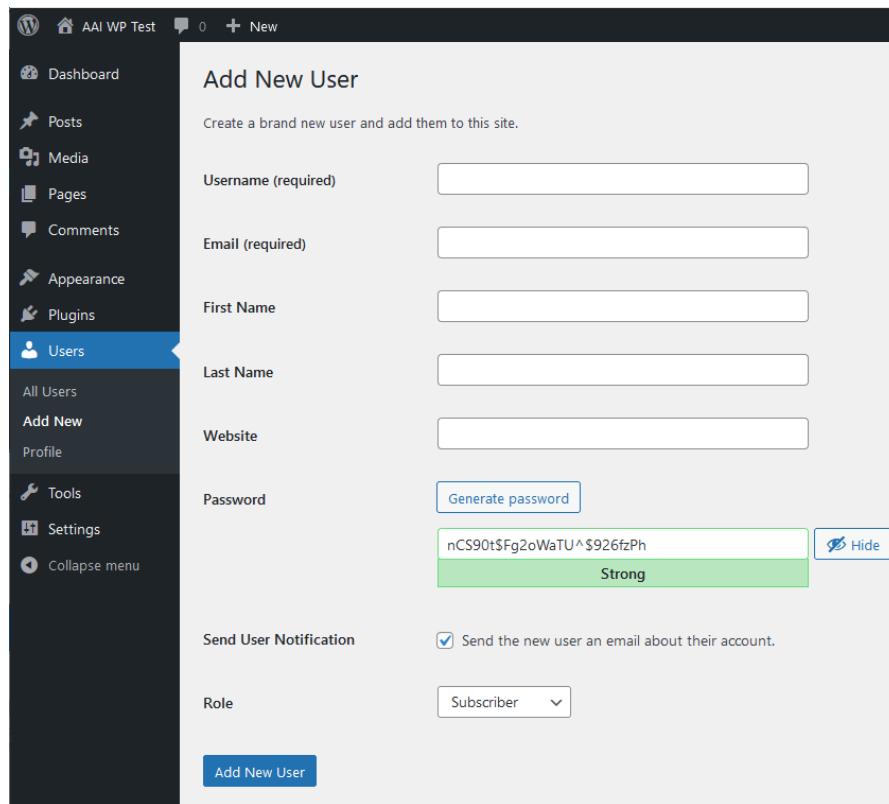
Dodatak je napisan poštjući WordPress standarde za pisanje dodataka, pa se u bilo kojem trenutku može omogućiti i onemogućiti. Iako se sustav WordPress redovno nadograđuje, ne očekuju se velike promjene u načinu rada s korisničkim računima, pa bi se dodatak trebao moći koristiti i na budućim verzijama sustava WordPress.

 Dodatak *WP AAI@EduHr Auth* je 'open source' i dostupan je kao git repozitorij na poveznici: <https://github.com/cicnavi/wp-aaieduhr-auth>. Za sve izazove i probleme s dodatkom potrebno je otvoriti 'issue' na spomenutom repozitoriju ili se obratiti originalnom autoru.

WordPress i korisnički računi

WordPress ima ugrađenu podršku za upravljanje korisničkim računima. Da bismo mogli uspješno zamijeniti ugrađeno upravljanje korisnicima s AAI@EduHr autentikacijom, ukratko ćemo se upoznati s postojećim mogućnostima povezanim s korisnicima i autentikacijom koje nudi WordPress.

Prilikom instalacije sustava WordPress definira se glavni administratorski korisnički račun. Nakon što se prijavimo pomoću glavnog administratorskog računa, možemo ručno dodavati nove korisnike kojima se želi omogućiti prijava na stranice. Forma za dodavanje novih korisnika izgleda ovako:



The screenshot shows the 'Add New User' page in the WordPress admin interface. The left sidebar is dark-themed and includes links for Dashboard, Posts, Media, Pages, Comments, Appearance, Plugins, and Users (which is highlighted). The main content area has a title 'Add New User' and a sub-instruction 'Create a brand new user and add them to this site.' Below this are several input fields: 'Username (required)', 'Email (required)', 'First Name', 'Last Name', 'Website', and 'Password'. The 'Password' field contains a generated password: 'nCS90t\$Fg2oWaTU^\$926fzPh' with a 'Strong' indicator. There is also a 'Generate password' button. Below the password field is a 'Send User Notification' checkbox, which is checked. At the bottom, there is a 'Role' dropdown set to 'Subscriber' and a large blue 'Add New User' button.

Na formi je moguće postaviti lozinku za korisnika. Nakon što administrator doda korisnika, korisniku može sam javiti početnu lozinku ili može odabratи opciju slanja e-maila u kojem će biti obavijest o otvorenom računu. Korisnik će nakon toga moći postaviti svoju novu lozinku za buduće korištenje. Kod stvaranja korisnika administrator može postaviti i ulogu za korisnika. Dostupne uloge su:

- *Super Admin* – osoba s potpunim pristupom administraciji na mrežnoj razini (kad stranica ima više podstranica)
- *Administrator* – osoba s pristupom administraciji određene stranice
- *Editor* – osoba koja može objaviti svoje članke ili članke drugih osoba
- *Author* – osoba koja može objaviti svoje članke

- *Contributor* – osoba koja može pisati članke, ali ih ne može objaviti
- *Subscriber* – osoba koja samo može uređivati svoj profil.

Uz ručno dodavanje, moguće je dopustiti i da korisnici sami naprave korisnički račun (da se registriraju na stranicu). Opcija za omogućavanje registracije nalazi se u *Settings > General*.

The screenshot shows the 'General Settings' page in the WordPress admin interface. The left sidebar is visible with various menu items like Posts, Media, Pages, etc., and 'Settings' is currently selected. The main area displays several configuration options:

- Site Title:** WP Demo
- Tagline:** Just another WordPress site
In a few words, explain what this site is about.
- WordPress Address (URL):** https://apps.unizg.hr/stage/wordpress
- Site Address (URL):** https://apps.unizg.hr/stage/wordpress
Enter the address here if you want your site home page to be different from your WordPress installation directory.
- Email Address:** marko.ivancic@srce.hr
This address is used for admin purposes, like new user notification.
- Membership:** Anyone can register (this field is highlighted with a yellow box)
- New User Default Role:** Subscriber
- Site Language:** English (United States)
- Timezone:** UTC+0

Kada se korisnici sami registriraju, prema početnim postavkama dobit će ulogu *Subscriber*, što je najslabija uloga za prijavljene korisnike u sustavu WordPress.

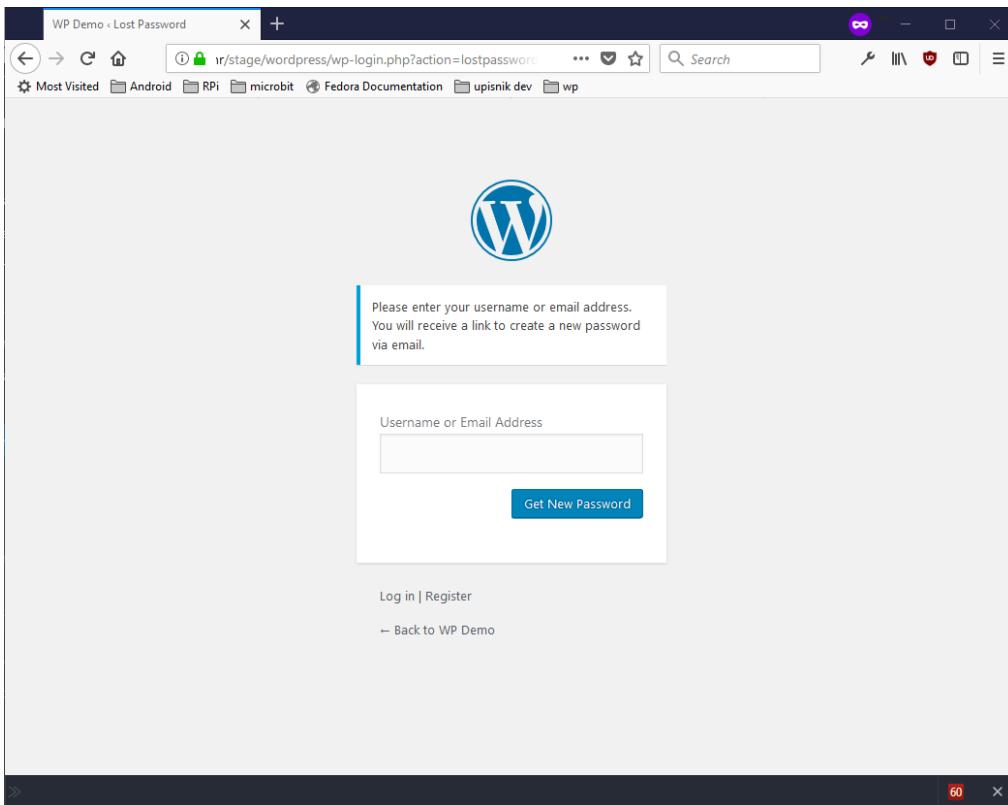
Korisnici koji imaju korisnički račun mogu se prijaviti preko poveznice `{wordpress-instalacija}/wp-login.php`, a forma izgleda ovako:

A screenshot of a web browser showing a WordPress login page. The title bar says "WP Demo < Log In". The address bar shows the URL "https://apps.unizg.hr/stage/wordpress/wp-login.php". The page features the classic blue "W" logo at the top. Below it is a form with two input fields: "Username or Email Address" and "Password", both with placeholder text. There is a "Remember Me" checkbox and a "Log In" button. At the bottom of the form are links for "Register" and "Lost your password?". Below the form is a link to "Back to WP Demo".

Ako je omogućena registracija, korisnici se mogu registrirati na stranice preko poveznice `{wordpress-instalacija}/wp-login.php?action=register`, a forma izgleda ovako:

A screenshot of a web browser showing a WordPress registration form. The title bar says "WP Demo < Registration Form". The address bar shows the URL "https://nizg.hr/stage/wordpress/wp-login.php?action=register". The page features the blue "W" logo at the top. Below it is a form titled "Register For This Site" with two input fields: "Username" and "Email". A note below the fields states "Registration confirmation will be emailed to you." There is a "Register" button. At the bottom of the form are links for "Log in" and "Lost your password?". Below the form is a link to "Back to WP Demo".

Korisnici imaju mogućnost resetiranja lozinke u slučaju da su je zaboravili. Korisnici to mogu učiniti preko poveznice `{wordpress-instalacija}/wp-login.php?action=lostpassword`, a forma izgleda ovako:



Kada se korisnici prijave na stranicu, u svom korisničkom profilu mogu mijenjati e-mail adresu i mogu generirati novu lozinku (uz ostale opcije):

Email (required) marko.ivancic@sre.hr

Website

About Yourself

Biographical Info

Share a little biographical information to fill out your profile. This may be shown publicly.

Profile Picture

You can change your profile picture on [Gravatar](#).

New Password

Sessions

Did you lose your phone or leave your account logged in at a public computer? You can log out everywhere else, and stay logged in here.

Update Profile

Thank you for creating with [WordPress](#).

Version 4.8.2

Prilikom ažuriranja korisnika administratori mogu zatražiti resetiranje lozinke preko opcije "Send password reset".

The screenshot shows the 'Users' page in the WordPress admin interface. A dropdown menu under the 'Bulk actions' button is open, with 'Send password reset' selected. The table lists two users: 'mivanci@srce.hr' (Marko Ivančić) and 'cicnavi@gmail.com'. The 'cicnavi@gmail.com' row has a 'Send password reset' link next to the user's name.

Generalno gledajući, osnovne podatke koje sustav WordPress zahtijeva za korisničke račune su:

- korisničko ime (engl. *username*)
- e-mail
- lozinka
- uloga (ako nije dana, početna uloga bit će *Subscriber*).

Što se tiče baze podataka, svi podaci o korisnicima spremaju se u tablice 'users' i 'usermeta'.

Dakle, ako u WordPress želimo uvesti autentikaciju pomoću AAI@EduHr sustava, moramo onemogućiti skoro sve ugrađene funkcionalnosti u vezi s kreiranjem korisničkih računa i prijave korisnika na stranice. Budući da sustav WordPress ovisi o lokalnim korisničkim računima, morat ćemo ih i dalje koristiti iako imamo aktivnu AAI@EduHr autentifikaciju.

Na sreću, sustav WordPress je relativno lako proširiv preko dodataka, pa smo za tu potrebu napravili dodatak *WP AAI@EduHr Auth* koji može na standardni način omogućiti autentifikaciju preko AAI@EduHr sustava te sam stvoriti i koristiti lokalne WordPress korisničke račune.

Preduvjeti za rad dodatka *WP AAI@EduHr Auth*

Da bi se mogao koristiti dodatak *WP AAI@EduHr Auth*, na poslužitelju na kojem će se koristiti WordPress s AAI@EduHr autentifikacijom potrebno je instalirati programski alat *simpleSAMLphp*. Također, potrebno je imati registriran resurs u sustavu AAI@EduHr. Upute kako instalirati simpleSAMLphp i kako registrirati resurs dostupne su na stranici: <http://www.aai.edu.hr/za-davatelje-usluga/za-web-aplikacije/kako-implementirati-autentifikaciju-potom-sustava-aai-eduhru-u-php>.

Prilikom registracije resursa, prilikom odabira korisničkih atributa koji će se isporučivati usluzi, preporučamo odabrati sljedeće attribute:

- hrEduPersonUniqueID (korisnička oznaka - obavezno)
- mail (e-mail - opcionalno, ali poželjno)
- givenName (ime - opcionalno)
- sn (prezime - opcionalno)

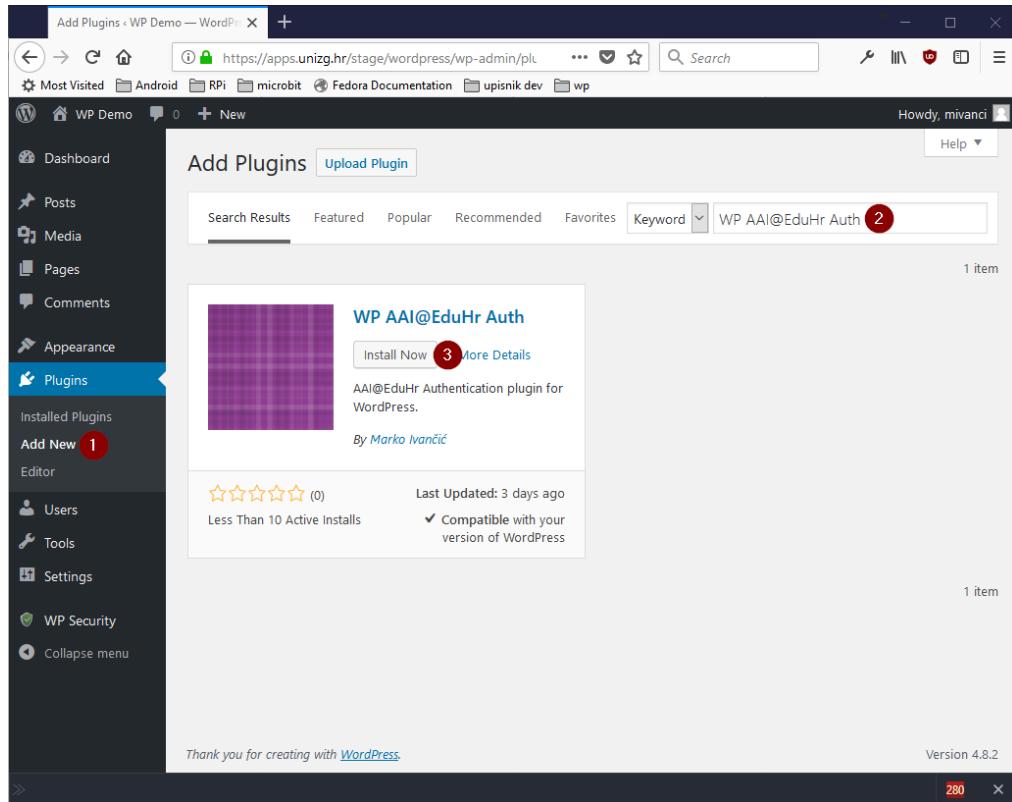
Naime, da bi se mogao napraviti novi korisnički račun u sustavu WordPress, obavezno se moraju postaviti korisnička oznaka i e-mail. Opcionalno, mogu se postaviti ime i prezime.

Da bi dodatak *WP AAI@EduHr Auth* mogao raditi, prilikom autentifikacije obavezno mora dobiti korisnički atribut 'hrEduPersonUniqueID', kojeg će iskoristiti za provjeru postojanja ili kreiranja korisničkog računa u sustavu WordPress. Ako prilikom autentifikacije dodatak ne dobije atribut 'mail', atribut 'hrEduPersonUniqueID' će se iskoristiti za definiranje korisničke oznake i e-maila.

Instalacija dodatka *WP AAI@EduHR Auth*

Dodatak *WP AAI@EduHr Auth* dostupan je kao WordPress dodatak te ga se može preuzeti na standardni način iz službenog WordPress repozitorija dodataka.

Dakle, u kontrolnoj ploči možemo kliknuti na *Plugins > Add New*. U tražilicu možemo unijeti naziv dodatka '*WP AAI@EduHr Auth*'. Nakon toga možemo kliknuti na gumbić '*Install Now*'.



Nakon instalacije možemo otići na *Plugins > Installed Plugins*. Na listi instaliranih dodataka potrebno je pronaći dodatak *WP AAI@EduHr Auth* i aktivirati ga klikom na gumbić *Activate*.

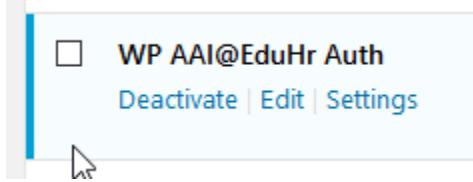
The screenshot shows the WordPress admin interface under the 'Plugins' menu. The left sidebar has 'Plugins' selected. The main area displays a list of installed plugins. The 'WP AAI@EduHr Auth' plugin is visible in the list, with its status set to 'Activate'. A yellow box highlights this action.

Postavke dodatka *WP AAI@EduHr Auth*

Nakon aktivacije potrebno je unijeti postavke dodatka. Sve dok se postavke ne unesu, neće biti moguće koristiti AAI@EduHr autentikaciju. Na vrhu kontrolne ploče vidljiv je status o tome je li AAI@EduHr autentikacija aktivna ili ne. Budući da trenutačno nismo unijeli postavke, vidimo da AAI@EduHr autentikacija još uvijek nije aktivirana:

The screenshot shows the WordPress admin interface under the 'Plugins' menu. The left sidebar has 'Plugins' selected. A yellow box at the top of the main area contains the text: 'AAI@EduHr authentication is NOT applied. Please check WP AAI@EduHr Auth settings. >> Can not load simpleSAMLphp. Service type is not valid.' Below this, a green box says 'Plugin activated.' The 'WP AAI@EduHr Auth' plugin is listed in the plugin list with its status set to 'Activate'.

Da bismo došli do stranice s postavkama, možemo kliknuti na gumbić 'Settings' koji se nalazi ispod naziva samog dodatka:



Također možemo otići na 'Settings' > 'WP AAI@EduHr Auth':

A screenshot of the 'WP AAI@EduHr Auth' settings page. On the left, a dark sidebar shows various menu items like 'Dashboard', 'Posts', 'Media', etc., with 'Settings' being the active tab. The main area has a title 'WP AAI@EduHr Auth'. A yellow warning box says 'AAI@EduHr authentication is NOT applied. Please check WP AAI@EduHR Auth settings. >> Can not load simpleSAMLphp. Service type is not valid.' Below it, 'Main configuration' is listed. Under 'Path to simpleSAMLphp', there's a text input field containing '/var/www/simpleSAMLphp/lib/_autoload.php'. Under 'Service type', there's another input field with a placeholder 'Valid options are: fedlab-sp or default-sp'. Other sections include 'Create a user if it doesn't exist' (with a checked checkbox), 'Allowed realms' (empty input field), and 'AAI@EduHr Auth Bypass Secret' (input field with placeholder 'Secret'). At the bottom right is a blue 'Save Changes' button.

Prva postavka koju moramo unijeti je putanja do alata simpleSAMLphp (engl. *Path to simpleSAMLphp*). U našem slučaju putanja za učitavanje alata simpleSAMLphp je `/var/www/projects/aaai/ssp-aaai/simpleSAMLphp-aaai-1.18.8-aaai/lib/_autoload.php`.

Druga postavka koju moramo unijeti je tip servisa (engl. *Service type*). Moguće opcije su '*fedlab-sp*' ili '*default-sp*'. Opcija '*fedlab-sp*' označava testni autentikacijski servis, a '*default-sp*' označava produkcijski autentikacijski servis. U našem slučaju unijet ćemo '*default-sp*'.

Dalje, možemo odabrat da li želimo automatski stvoriti lokalne korisničke račune ili ćemo sami definirati koji korisnički računi će se moći prijaviti na stranice. Ako odaberemo automatsko stvaranje korisničkih računa, dodatak *WP AAI@EduHr Auth* će sam stvoriti lokalni korisnički račun za sve korisnike koji se uspešno autenticiraju preko *AAI@EduHr* sustava, a do te prijave nisu imali lokalni korisnički račun. Ako ne odaberemo opciju za automatsko stvaranje korisničkih računa, morat ćemo ručno dodati svakog korisnika preko forme koja se nalazi na 'Users' > 'Add New'. U tom slučaju za svakog korisnika kojeg ručno dodajemo, kao korisničko ime moramo navesti korisničku oznaku iz *AAI@EduHr* sustava.

Dalje, preko postavke '*Allowed realms*' možemo ograničiti prijave na korisnike samo s određenih ustanova. Ako tu postavku ostavimo praznom, korisnici s bilo koje ustanove moći će se prijaviti na stranice. Ako želimo postaviti ograničenje na određene ustanove, možemo unijeti listu LDAP domena ustanova odvojenih zarezom (popis matičnih ustanova s naznakom LDAP domene dostupan je na stranici: <http://www.aaiedu.hr/statistika-i-stanje-sustava/maticne-ustanove/popis>). Na primjer, ako želimo ograničiti prijave samo na korisnike s ustanova Sveučilišni računski centar i Sveučilište u Zagrebu, unijeli bismo: `srce.hr, unizg.hr`.

Dalje, za omogućavanje prijave za korisnike koji ne posjeduju *AAI@EduHr* elektronički identitet, moguće je popuniti opciju '*AAI@EduHr Auth Bypass Secret*'. Ako se u to polje unese tajni string, on će se moći iskoristiti za pristup standardnom WordPress sučelju za prijavu lokalnih korisnika. Ova opcija se može iskoristiti u scenariju kada osobe održavatelji WordPress sjedišta nisu sa ustanovama koja je vlasnik web sjedišta. Tajni string se može iskoristiti definiranjem '*aabs*' parametra prilikom pristupa *wp-login.php* formi, npr.: `{wordpress-instalacija}/wp-login.php?aabs=some-secret`

Nakon spremanja postavki pojavit će se obavijest da je *AAI@EduHr* autentikacija sada aktivna (ako su postavke ispravne).

The screenshot shows the WordPress admin interface with the 'WP AAI@EduHr Auth' plugin active. The left sidebar has a dark theme with various menu items like Dashboard, Posts, Media, Pages, Comments, Appearance, Plugins, Users, Tools, and Settings. The 'Settings' item is currently selected. The main content area is titled 'WP AAI@EduHr Auth' and contains the following configuration fields:

- Main configuration**: A note stating "AAI@EduHr authentication is applied. Users need to use AAI@EduHr identities to log in." and a link to the "official AAI@EduHr webpage".
- Path to simpleSAMLphp**: Set to "/var/www/projects/aai/ssp-aai/simplesamlphp-aai-1.1". A note says "For example: /var/www/simplesamlphp/lib/_autoload.php".
- Service type**: Set to "default-sp". A note says "Valid options are: fedlab-sp or default-sp".
- Create a user if it doesn't exist**: A checked checkbox with a note explaining it creates local users automatically if authenticated through AAI@EduHr.
- Allowed realms**: Set to "srce.hr". A note says "Leave empty if users from any realm are allowed to authenticate through AAI@EduHr. If you want to limit authentication to specific realms, enter comma separated list of realms. For example, to limit authentication only to srce.hr and sfzg.hr realms, enter: srce.hr, sfzg.hr".
- AAI@EduHr Auth Bypass Secret**: A field containing a long random string: "nRaIEkiseOsvOdy/GDlr4134sOHZRu9W". A note explains it's used to bypass authentication for regular WordPress logins and provides a URL example: "/wp-login.php?abs=some-secret". It also notes to make sure the secret is long enough and unique.

A "Save Changes" button is at the bottom of the form.

Onemogućene WordPress funkcionalnosti

Nakon aktiviranja dodatka *WP AAI@EduHr Auth*, određene WordPress funkcionalnosti povezane s korisnicima bit će onemogućene:

- Više neće biti moguće koristiti standardni link za registraciju `korisnika/{wordpress-instalacija}/wp-login.php?action=register`. Ako netko pokuša otvoriti tu stranicu, dodatak *WP AAI@EduHr Auth* javit će poruku da je registracija na stranicu onemogućena.
- Akcija vraćanja izgubljene lozinke koja se mogla obaviti na stranici `{wordpress-instalacija}/wp-login.php?action=lostpassword` također je onemogućena.
- Nadalje, kod dodavanja novog korisnika kroz standardno WordPress sučelje više nije moguće definirati korisničku lozinku niti je kod uređivanja postojećeg korisničkog profila moguće mijenjati korisničke lozinke. Dodatak *WP AAI@EduHr Auth* generirat će slučajne lozinke (iako se te lozinke neće koristiti).

Deaktivacija dodatka *WP AAI@EduHr Auth*

Iako je redovna praksa da aplikacije koje jednom počnu koristiti AAI@EduHr autentikaciju nastave raditi na taj način do kraja svog životnog vijeka, dodatak *WP AAI@EduHr Auth* može se deaktivirati u bilo kojem trenutku. U slučaju da to odlučite, treba imati na umu nekoliko stvari.

- Svi lokalni korisnički računi koji su stvoreni dok se koristio dodatak *WP AAI@EduHr Auth* ostat će evidentirani u sustavu WordPress.
- Sve prethodno spomenute onemogućene akcije ponovno će postati aktivne, što znači da će korisnici ponovno moći koristiti standardne akcije za vraćanje i resetiranje lozinke te za prijavu i registraciju na stranicu.
- U slučaju deaktiviranja dodatka treba razmotriti da li treba određene AAI@EduHr korisnike obrisati iz sustava WordPress kako si ne bi mogli resetirati lozinke i na taj si način ponovno omogućiti pristup stranici.

Poveznice

Dodatak *WP AAI@EduHr Auth* napisan je pod licencijom GPL-3.0+, a trenutačno je dostupan na engleskom i hrvatskom jeziku.

Službena stranica dodatka je: <https://wordpress.org/plugins/wp-aaieduhru-auth/>.

Git repozitorij dostupan je na adresi: <https://github.com/cicnavi/wp-aaieduhru-auth>.

SVN repozitorij dostupan je na adresi: <https://plugins.svn.wordpress.org/wp-aaieduhru-auth/>.

Pozivamo vas da isprobate dodatak i da nam javite svoja iskustva. Također, programere pozivamo da pogledaju izvorni kod i da sudjeluju u dalnjem razvoju dodatka. Možete koristiti mogućnosti koje nude spomenuti repozitoriji ili se možete javiti direktno autoru na e-mail. Svi prijedlozi su dobrodošli.