

Microsoft Office 365

Ustanovama koje koriste Microsoft Office 365 omogućuje se Single Sign-On autentikaciju uporabom SAML protokola koji se podržan i od strane AAI@EduHr sustava. Stoga je prilikom pristupanja pojedinim Microsoft Office 365 aplikacijama moguća autentikacija korisnika uporabom njihovih AAI@EduHr elektroničkih identiteta.

Važno!

Slike i poveznice na ovoj stranici odgovaraju aktualnom stanju u trenutku nastanka tog dijela uputa. Obzirom da se usluga Microsoft Office 365 s vremena na vrijeme proširuje novim funkcionalnostima, moguće je da informacije prikazane na slikama ne odgovaraju u potpunosti sadržaju izbornika koji se prikazuju u administrativnom sučelju, ali generalne smjernice kako iskonfigurirati Office 365 za autentikaciju korisnika putem sustava AAI@EduHr trebale bi ostati nepromijenjene.

Popis ustanova koje prema ugovoru Ministarstva znanosti i obrazovanja te Microsofta imaju pravo na besplatno korištenje Office 365 usluge naveden je u [ovoj datoteci](#).

Navedene ustanove imaju pravo na besplatno korištenje Office 365 programskih alata obuhvaćenih **Education E1** licencom. Više informacija o programskim alatima obuhvaćenim navedenom licencom možete pronaći na [Microsoftovim stranicama](#). Na istoj stranici odabirom opcije **Get started for free** možete registrirati vašu ustanovu za korištenje Office 365 usluge.

Postupak registracije svoje ustanove za korištenje Office 365 programskih alata započnite tako da otvorite korisnički račun u Office 365 sustavu koji ćete koristiti u nastavku ovih uputa. Otvaranje korisničkog računa prvi je korak u postupku registracije domene vaše ustanove u sustavu Office 365, a započet ćete ga tako da na adresi: <http://products.office.com/en-us/academic> odaberete **Get started**.

Bitno je naglasiti da taj korisnički račun treba biti oblika:

proizvoljna_kor_oznaka@nekadomena.onmicrosoft.com

Ako je netko s vaše ustanove već prošao kroz proces samoregistracije, u procesu registracije vaše domene pojaviti će se poruka koja kaže da ne možete registrirati domenu jer je već registrirana. U tom slučaju trebate preuzeti ovlasti nad svojom domenom na način opisan u [ovim uputama](#). Po preuzimanju ovlasti nad domenom, administratorski korisnički račun u sustavu Office 365 potreban za nastavak postupka možete otvoriti kroz web sučelje Office 365.

Minimalna potrebna programska podrška

Prilikom izrade ovih uputa korištena je sljedeća programska podrška:

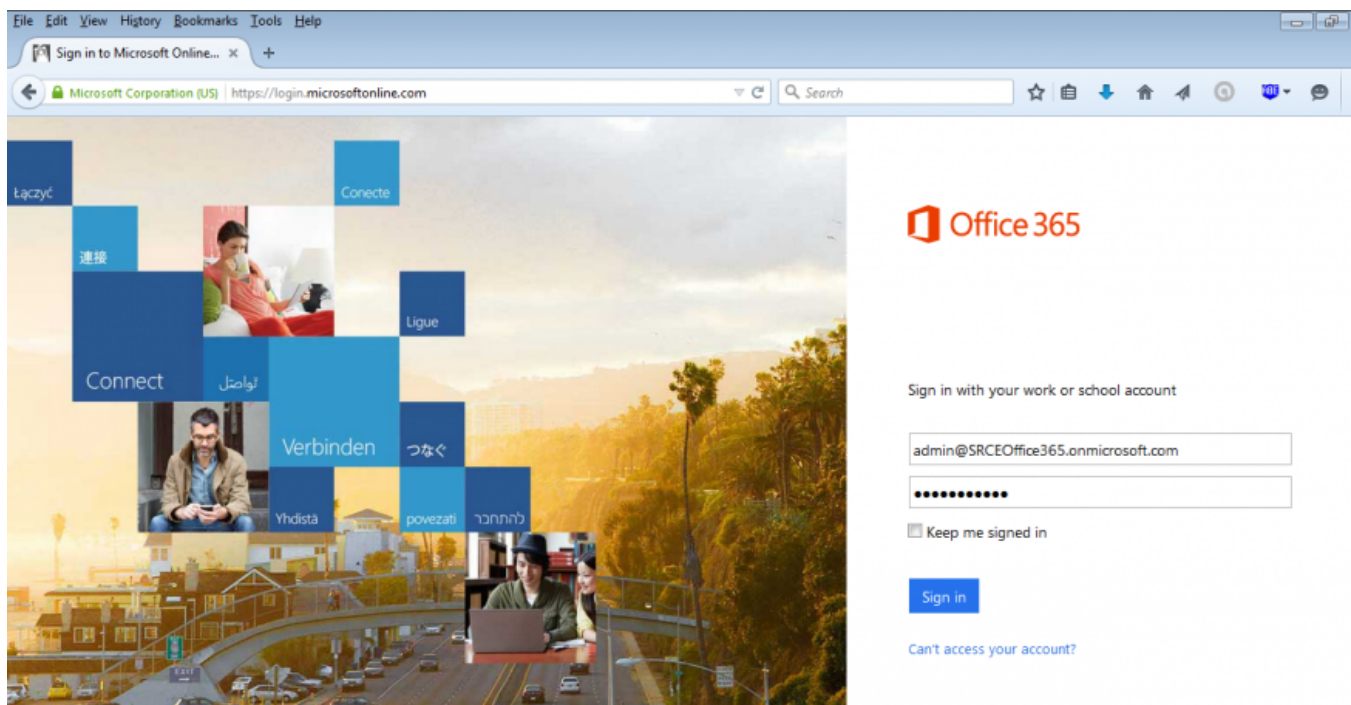
- Microsoft Windows 7 Professional;
- Windows Powershell s implementiranim Windows Azure Active Directory modulom za što je potrebno instalirati [Microsoft Online Services Sign-In Assistant](#)

Registracija ustanove za korištenje usluge Microsoft Office 365

Prilikom registracije za korištenje usluge Microsoft Office 365 otvorit ćete korisnički račun za administriranje usluga u Windows Azure oblaku (oblika proizvoljna_kor_oznaka@nekadomena.onmicrosoft.com). Uporabom web preglednika prijavite se s navedenim korisničkim računom na Office 365 administrativno sučelje koje se nalazi na adresi:

<https://portal.office.com>

- Minimalna potrebna programska podrška
- Registracija ustanove za korištenje usluge Microsoft Office 365
- Registracija usluge u sustavu AAI@EduHr
- Podešavanje usluge Microsoft Office 365 za autentikaciju korisnika putem sustava AAI@EduHr
- Registracija plugina za sinkronizaciju podataka iz LDAP imenika sa Azure AD-om
- Instalacija i podešavanje libo365connect-aosi-aaai plugina
- Prijenos postojećih korisnika u Azure AD
- Često postavljana pitanja
 - U log-u /var/log/aosi/o365connect/o365connectTransferToAzure.log mi se pojavljuju greške. U čemu je problem?
 - Kako se korisnici prijavljuju u Office 365 svojim elektroničkim identitetom iz sustava AAI@EduHr?
 - Je li moguće čitati e-mail desktop klijentom u slučaju kad se korisnici za pristup usluzi Office 365 autenticiraju putem sustava AAI@EduHr?
 - Kako riješiti problem s nemogućnošću pohrane lokalno uređenih dokumenata iz aplikacija koje su dio Office 365 ProPlus paketa u oblak (OneDrive)?
 - Je li moguće uspostaviti vezu sustava AAI@EduHr i Office 365 ako koristim uslugu ugošćavanja AAI servisa na računalu hosting.aaiedu.hr?
 - U 3. koraku uputa, kod odabira opcije Azure AD sučelje traži ponovnu registraciju te unos broja kreditne kartice. Što dalje?
 - Kako izvršiti zamjenu certifikata za provjeru SSO autentikacije?



Nakon prijave kliknite na ikonu **Administrator** i zatim u izborniku s lijeve strane odaberite opciju **DOMENE**:

Office 365

Sveučilišni računski centar Sveučilišta u Zagrebu (uređivanje)

Centar za administratore sustava Office 365

NADZORNA PLOČA

POSTAVLJANJE

KORISNICI

PROFIL TVRTKE

UVOZ

KONTAKTI

ZAJEDNIČKI POŠTANSKI

SANDUČIĆI

SOBE ZA SASTANKE

GRUPE

DOMENE

JAVNO WEB-MJESTO

NAPLATA

VANJSKO ZAJEDNIČKO

KORIŠTENJE

POSTAVKE SERVISA

IZVJEŠĆA

STANJE SERVISA

PODRŠKA

KUPNJA SERVISA

CENTAR ZA PORUKE

ADMINISTRATOR

Dobro došli u Office 365!

[Pogledajte videozapis](#) da biste dobili pregled

[Postavite servise](#)

[Preuzmite softver](#)

[Informirajte se o servisu Yammer](#)

[Pogledajte videozapis](#) da biste brzo započeli s radom

Pregled servisa

Stanje servisa

Nema servisnih problema

Servisni zahtjevi

Nema otvorenih zahtjeva za uslugu

Zaštita pošte

Primljeno poruka: 1, obrađeno filtriranjem: 0.

Centar za poruke

Nema novih poruka u zadnjih 7 dana

Trenutno stanje

Exchange	Nema problema
Office 365 Portal	Nema problema
Pretplata na Office	Nema problema
SharePoint	Nema problema
Skype za tvrtke	Nema problema
Usluga s identitetom	Nema problema
Usluga upravljanja pravima	Nema problema

[Prikaži pojedinosti i povijest](#)

[Povratne informacije](#)

Prikazat će vam se tablica s popisom domena za koje možete koristiti Office 365 uslugu. Ako se DNS/LDAP domena vaše ustanove ne nalazi na tom popisu, dodajte je odabirom opcije **Dodaj domenu**:

File Edit View History Bookmarks Tools Help

https://portal.office.com/Admin/Default.aspx#DomainManagerPageLayout

Office 365

Centar za administratore sustava Office 365

DOMENE

JAVNO WEB-MJESTO

► NAPLATA

► VANJSKO ZAJEDNIČKO KORIŠTENJE

► POSTAVKE SERVISA

IZVJEŠĆA

► STANJE SERVISA

► PODRŠKA

KUPNJA SERVISA

CENTAR ZA PORUKE

ADMINISTRATOR

Exchange

Skype za tvrtke

SharePoint

NADZORNA PLOČA | DOMENE

University of Zagreb, University Computing Centre (uređivanje)

Upravljanje domenama

Sustavu Office 365 dodajte domenu koju već posjedujete ili kupite novu. [Što je domena?](#)

+ Dodaj domenu Kupi domenu

NAZIV DOMENE	STATUS	RADNJA
SRCETESTO		
ffice365.on		
microsoft.c om (zadano)	Postavljanje je dovršeno	Nije potrebna radnja

SRCETESTOffice3

Upravljanje DNS-om

Povratne informacije

Da biste Microsoftu dokazali da je dodana domena zaista u vlasništvu vaše ustanove, morat ćete na vašem DNS poslužitelju dodati odgovarajući zapis sukladno uputama koje će vam se ispisati na ekranu:

File Edit View History Bookmarks Tools Help

https://portal.office.com/Admin/Default.aspx#@/Domains/AddDomainWizard.aspx?Sce

Office 365

Provjera ispunjavanja uvjeta za Microsoft Office 365 za obrazovne ustanove

1. Dobro došli
2. Navedite naziv domene
- 3. Potvrdite vlasništvo**
4. Dovršetak

potvrdite da ste vlasnik domene srce.hr

Prije no što postavite domenu na usluzi Office 365, moramo provjeriti jeste li vlasnik domene. Da biste to učinili, dodat ćete specifični zapis u DNS zapise davatelja usluga hostinga DNS-a. Potražiti ćemo zapis da bismo potvrdili vlasništvo.

Napomena: to ne utječe na način funkcioniranja vaše domene. [Saznajte više](#)

Pogledajte postupne upute za izvođenje ovog koraka s:

Stvaranje zapisa provjere valjanosti kod davatelja usluga DNS hostinga

- DNS vam nije poznat? Umjesto da sami stvorite zapis za provjeru valjanosti, obratite se tvrtki koja hostira DNS zapise i zatražite neka umjesto vas stvore zapis. Ovo je primjer poruke kakvu im možete poslati.
Kada primite potvrdu da je zapis stvoren, vratite se u Office 365 i kliknite dolje **Gotovo, provjeri valjanost odmah**.

Poštovani,
Koristim Microsoft Office 365 i htio bih koristiti svoju domenu, no Office 365 mora najprije provjeriti jesam li vlasnik naziva domene. Da bi to učinio, moram stvoriti TXT ili MX zapis za svoju domenu. S obzirom na to da ste vi moj davatelj servisa DNS hostiranja, biste li mogli umjesto mene stvoriti zapis? Zapis mora obuhvaćati podatke navedene un tablici u nastavku.

Napomena: morate stvoriti samo jedan od zapisa. Možete odabrati koje želite stvoriti.

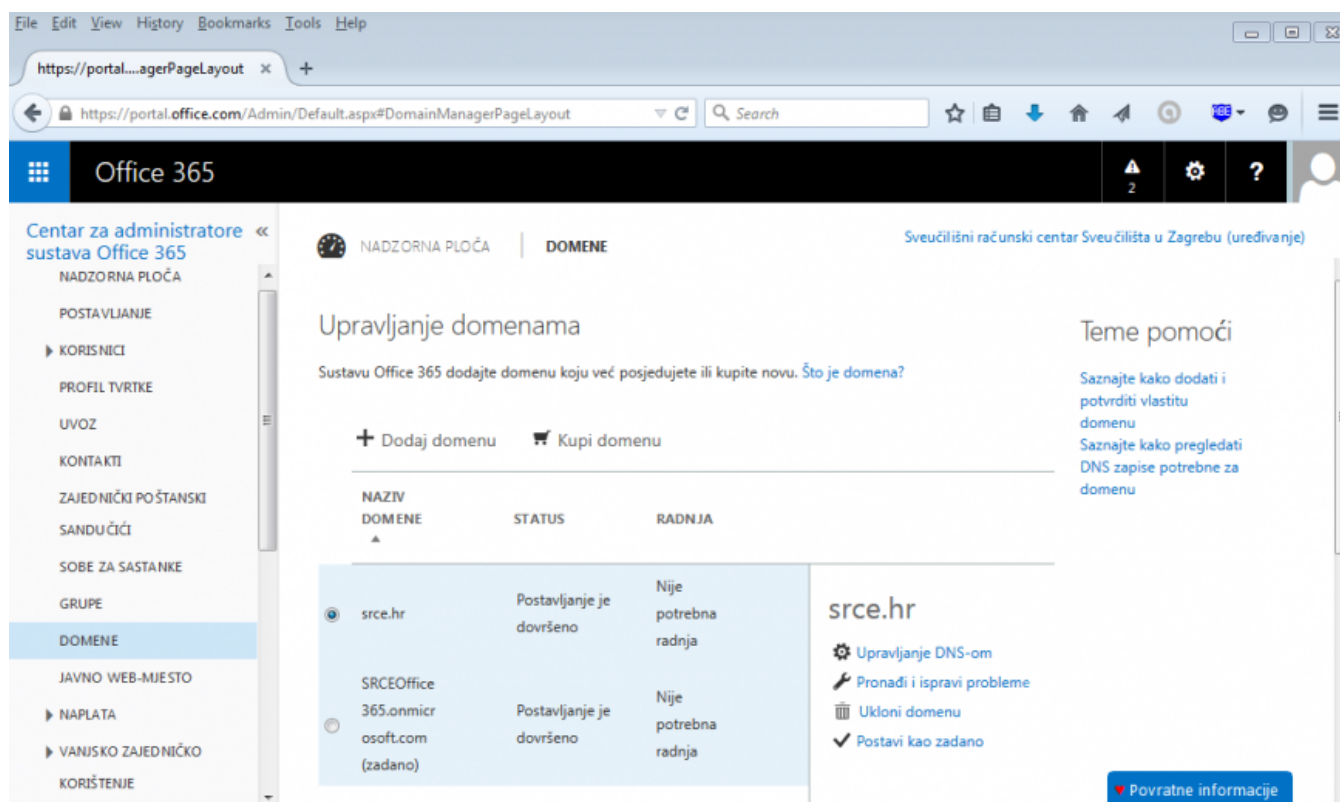
Vrsta zapisa (odaberite jednu)	Pseudonim ili naziv glavnog računala	Određite ili adresu na koju upućuje	TTL
TXT	@ ili srce.hr	MS=ms25662772	1 h
MX	@ ili srce.hr	ms25662772.msv1.invalid.outlook.com	1 h

[Povratne informacije](#)

Obzirom da je potrebno neko vrijeme da se podaci uneseni na DNS poslužitelju propagiraju, odjavite se iz administratorskog sučelja i pričekajte barem sat vremena prije nego što nastavite s procedurom opisanom u ovim uputama.

Nakon što se ponovo prijavite u Office 365 administratorsko sučelje, odaberite opciju **Kliknite da biste ovjerali domenu**. Ako ste ispravno unijeli podatke na vašem DNS poslužitelju i ako su se ti podaci uspješno propagirali, dobit ćete odgovor da je vlasništvo domene potvrđeno, a u tablici će se pored naziva domene vaše ustanove pojaviti natpis da je postavljanje uspješno dovršeno.

Važno: da biste u nastavku procedure autentikaciju za svoju domenu mogli prepustiti SSO servisu sustava AAI@EduHr, kao zadana (defaultna) domena za vašu ustanovu mora biti odabrana ona u kojoj je vaša korisnička oznaka oblika **proizvoljna_kor_oznaka@nekadomena.onmicrosoft.com** (kao na slici dolje SRCEOffice365.onmicrosoft.com - ispod te domene treba pisati zadana ili default).



Registracija usluge u sustavu AAI@EduHr

Da bi prijava u Office 365 putem sustava AAI@EduHr za određenu LDAP domenu funkcionirala, potrebno je registrirati Office 365 uslugu u sustavu AAI@EduHr. Registracija se vrši putem Registra resursa, web aplikacije koja se nalazi na adresi

<https://registar.aaiedu.hr/>

Registru mogu pristupiti davatelji/vlasnici usluga uporabom elektroničkog identiteta u sustavu AAI@EduHr.

Zahtjev za registracijom u registar, a zatim i korištenje registra davatelji/vlasnici usluga mogu ostvariti i putem računa neke od društvenih mreža: Facebook, Google, LinkedIn, Twitter. Nakon poslanog zahtjeva, administrator registra prihvaća/ne prihvaća zahtjev korisnika.

Nakon što se prijavite u registar, na popisu opcija u gornjem izborniku izaberite **Registracija resursa**. Otvorit će vam se prozor s formom za upis općih podataka o resursu, kontakata povezanih sa resursom te administratorima resursa.

Pri vrhu forme za unos podataka o novom resursu, u polju "**Kao administrator usluge potvrđujem da će usluga biti pružana sukladno odredbama Pravilnika o ustroju AAI@EduHr**" trebate staviti kvačicu kako biste potvrdili da prihvaćate uvjete korištenja AAI@EduHr infrastrukture definirane [Pravilnikom o ustroju autentifikacijske i autorizacijske infrastrukture sustava znanosti i visokog obrazovanja u Republici Hrvatskoj](#).

☐ **Kao administrator usluge potvrđujem da će usluga biti pružana sukladno odredbama Pravilnika o ustroju AAI@EduHr.**

U odjeljku **Općih informacija** potrebno je unijeti sljedeće podatke:

- **Naziv resursa:** Microsoft Office 365 za korisnike iz (naziv ustanove)
- **Opis resursa:** Autentikacija putem sustava AAI@EduHr za korisnike iz domene (LDAP domena ustanove)
- **Vrsta resursa:** produkcija
- **Matična ustanova s kojom je resurs povezan:** odaberite ustanovu za koju se registrira autentikacija za Office 365
- **Partner federacije s kojim je resurs povezan:** - nijedan -
- **Globalna usluga s kojom je resurs povezan:** Microsoft Office 365
- **Web adresa (URL) na kojoj se aplikacija nalazi:** <http://login.microsoftonline.com>


Kao na primjeru na sljedećoj slici:

Naziv resursa ?	Microsoft Office 365 za korisnike iz (naziv ustanove)
Opis resursa ?	Autentikacija putem sustava AAI@EduHr za korisnike iz domene (LDAP domena ustanove)
Vrsta resursa ?	Produkcija
Matična ustanova s kojom je resurs povezan	odaberite ustanovu za koju se registrira autentikacija za Office 365
Partner federacije s kojim je resurs povezan	- nijedan -
Globalna usluga s kojom je resurs povezan ?	Microsoft Office 365
URL sjedišta usluge ?	http://login.microsoftonline.com
URL na kojem je dostupan logotip usluge ?	"http://www.primjer.com/logo.png"
URL na kojem se nalaze upute za korisnike ?	"http://www.primjer.com/upute"
URL na kojem se nalaze pravila privatnosti usluge ?	"http://www.primjer.com/privacy-policy"

Nakon što ste ispunili dio forme s općim podacima ispunite informacije o kontaktima te administratorima resursa, te spremite resurs.

Važno je naglasiti da odabirom osobe toj osobi NEĆETE dodijeliti administrativne ovlasti nad Office 365 sustavom, nego samo ovlasti administriranja podataka o Office 365 usluzi u registru resursa!

Sljedeće je potrebno resursu dodati SAML autentikacijski modul.

 **Opće informacije**

Odabir autentikacijskog segmenta

Odaberite autentikacijski protokol:

SAML

RADIUS

CAS

U formi **SAML konfiguracije** potrebno je unijeti tzv. SAML metapodatke Office 365 servisa u skladu s sljedećim uputama:

- U izborniku **"Auth Service"** odaberite **Univerzalni**
- U izborniku **"NameID Format"** odaberite **urn:oasis:names:tc:SAML:2.0:nameid-format:persistent**
- U izborniku **"NameID Attribute"** treba stajati **hrEduPersonPersistentID**
- Uključite opciju **"Sign Response"**
- U polje **EntityID** upišite: <https://login.aaiedu.hr/office365/module.php/saml/sp/metadata.php/srcce.hr> (umjesto srcce.hr potrebno upisati LDAP domenu matične ustanove za koju registrirate resurs)

- U polje **AssertionConsumerService URL** upišite: <https://login.aaiedu.hr/office365/module.php/saml/sp/saml2-acss.php/srce.hr> (umjesto srce.hr potrebno upisati LDAP domenu matične ustanove za koju registrirate resurs)
- U polje **SingleLogoutService URL** upišite: <https://login.aaiedu.hr/office365/module.php/saml/sp/saml2-logout.php/srce.hr> (umjesto srce.hr potrebno upisati LDAP domenu matične ustanove za koju registrirate resurs)

U dijelu forme "**Atributi**" trebaju biti označena tri atributa:

- hrEduPersonUniqueID (Korisnička oznaka)
- hrEduPersonHomeOrg (Oznaka matične ustanove)
- hrEduPersonPersistentId (Trajna korisnička oznaka)

U prazno polje "**Namjena**" za svaki ručno označeni atribut treba upisati: "Identifikacija i autorizacija korisnika u sustavu Office365"

Nakon što popunite formu prema uputama i kliknete na opciju **Zatraži dodavanje konfiguracije**, obavijest o postavljanju novog zahtjeva za registracijom bit će automatski dostavljena administratorima sustava AAI@EduHr koji će pregledati unesene podatke i odobriti zahtjev ili vas eventualno upozoriti na neke nedostatke koje treba ispraviti da bi zahtjev mogao biti odobren.

Obavijest o odobravanju zahtjeva dobit ćete elektroničkom poštom, a sama autentikacija bi trebala proraditi u roku od najviše 5 minuta od trenutka kada zahtjev bude odobren.

Podešavanje usluge Microsoft Office 365 za autentikaciju korisnika putem sustava AAI@EduHr

U sljedećih nekoliko koraka potrebno je koristiti **Windows Powershell konzolu**. Neki su nam korisnici prijavili da su naišli na probleme pri instalaciji i pokretanju Powershell konzole. Najčešći problem, kao i njegovo rješenje opisan je na [Stack Overflow stranici](#).

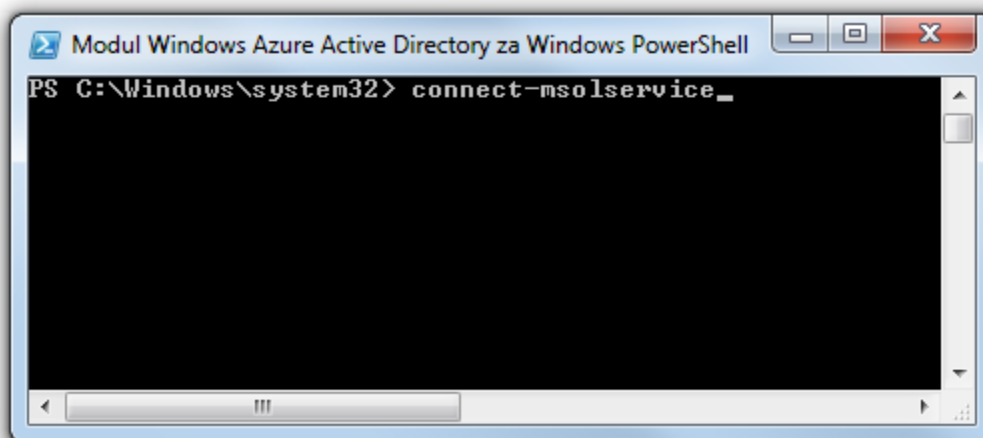
Za omogućavanje autentikacija korisnika putem sustava AAI@EduHr potrebno je izvršiti sljedeću proceduru:

1. Dohvatite poslužiteljski certifikat s adrese <https://login.aaiedu.hr/office365/module.php/saml/idp/certs.php/idp.crt> i pohranite ga u neki direktorij na vašem računalu, npr. C:\Users\korisnik\Downloads\
2. Na svom računalu **pokrenite Windows Powershell konzolu**, izvršite naredbu

```
connect-msolservice
```

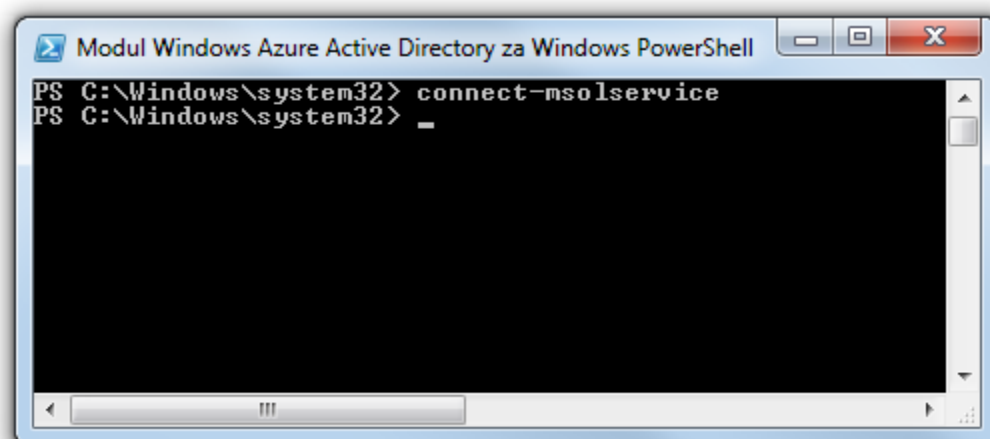
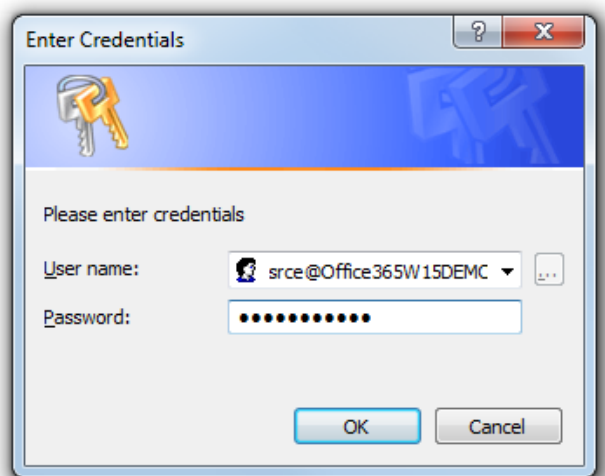
i prijavite se uporabom administratorskog korisničkog računa (onog koji ste otvorili u prvom koraku i koji je oblika **proizvoljna_kor_oznaka@nekadomena.onmicrosoft.com**, dakle ne AAI@EduHr elektroničkim identitetom):

VAŽNO: Za prijavu u PowerShell konzolu **OBAVEZNO** koristiti korisnički račun oblika **proizvoljna_kor_oznaka@nekadomena.onmicrosoft.com**. Ni u kom slučaju korisnički račun oblika jednakog vašem elektroničkom identitetu iz sustava AAI@EduHr!!!



VAŽNO: zbog povećanog broja upite korisnika koji su ignorirali prethodnu uputu naglašavamo opet:

Za prijavu u PowerShell konzolu **OBAVEZNO** koristiti korisnički račun oblika **proizvoljna_kor_oznaka@nekadomena.onmicrosoft.com**. Ni u kom slučaju korisnički račun oblika jednakog vašem elektroničkom identitetu iz sustava AAI@EduHr!!!



3. Nakon toga potrebno je u Windows Powershell konzoli izvršiti jednu za drugom sljedeće naredbe (pritom u prvoj naredbi umjesto **domena.hr** trebate upisati DNS/LDAP domenu vaše ustanove, a u šestoj naredbi trebate upisati ispravnu putanju do certifikata koji ste dohvatili u prvom koraku i spremili ga u neki direktorij na vašem računalu):

```
$dom = "domena.hr"

$fedbrandname = "AAI@EduHr"
$url = "https://login.aaiedu.hr/office365/saml2/idp/SSOService.php?entityID=https://login.aaiedu.hr/office365/" + $dom
$uri = "https://login.aaiedu.hr/office365/" + $dom
$logourl = "https://login.aaiedu.hr/office365/saml2/idp/SingleLogoutService.php?ReturnTo=https://login.aaiedu.hr/office365/logout.php"
$cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("C:\Users\korisnik\Downloads\new_idp.crt")
$certdata = [system.convert]::toBase64string($cert.rawdata)
set-msoldomainauthentication -domainname $dom -federationbrandname $fedbrandname -authentication Federated -passivelogonuri $url -signingcertificate $certdata -issueruri $uri -logoffuri $logourl -preferredauthenticationprotocol SAML
```

Postupak i rezultat izvršavanja trebali bi izgledati otprilike kao na sljedećoj slici:

```
Modul Windows Azure Active Directory za Windows PowerShell
PS C:\Windows\system32> $dom = "srce.hr"
PS C:\Windows\system32> $fedbrandname = "AAI@EduHr"
PS C:\Windows\system32> $url = "https://login.aaiedu.hr/sso/saml2/idp/SSOService.php"
PS C:\Windows\system32> $uri = "urn:geant:edugain:component:be:aaieduhr:aaiedu.hr"
PS C:\Windows\system32> $logouturl = "https://login.aaiedu.hr/sso/saml2/idp/SingleLogoutService.php"
PS C:\Windows\system32> $cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
PS C:\Windows\system32> $certdata = [system.convert]::toBase64String($cert.RawData)
PS C:\Windows\system32> set-msoldomainauthentication -domainname $dom -federationbrandname $fedbrandname -federated -passivelogonuri $url -signingcertificate $certdata -issueruri $uri -logoffuri $logouturl
PS C:\Windows\system32>
```

Ako prilikom izvršavanja prethodno navedenih naredbi unesete neki pogrešan podatak i Single Sign-On autentikacija ne funkcioniše ispravno, konfiguraciju možete poništiti naredbom:

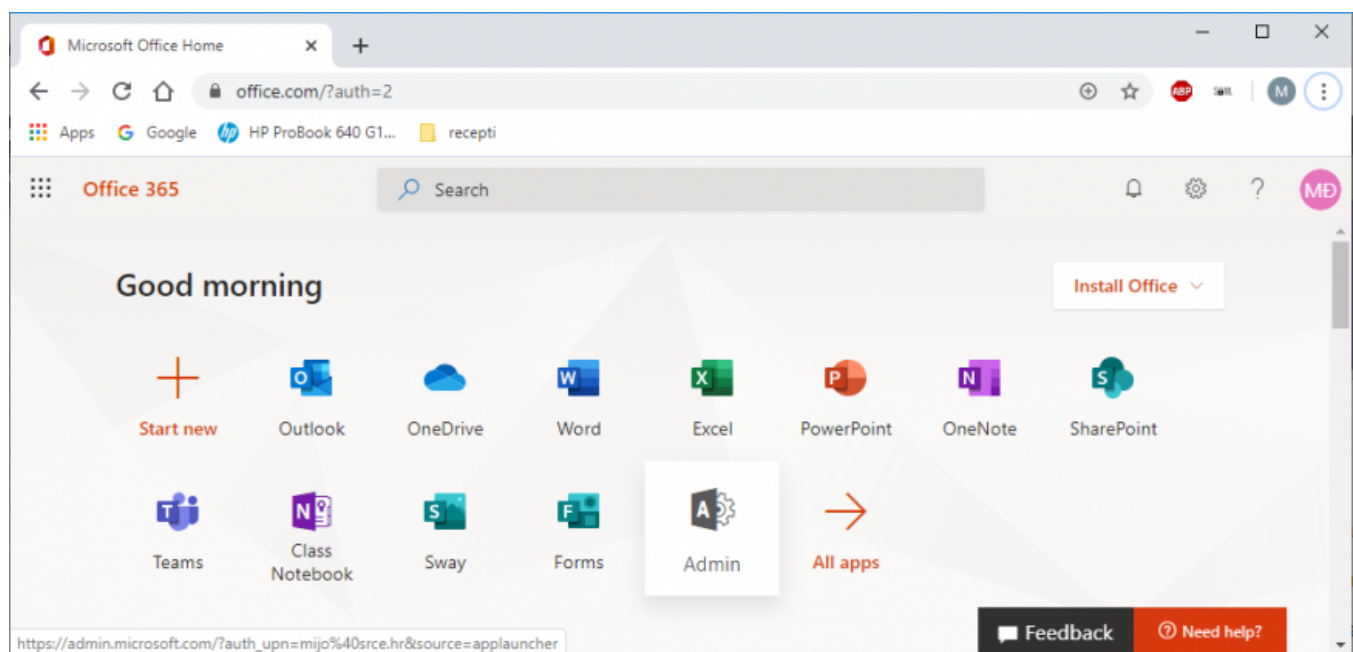
```
set-msoldomainauthentication -authentication Managed -domainname domena.hr
```

pri čemu **domena.hr** treba zamijeniti DNS/LDAP domenom vaše ustanove. Nakon toga za omogućavanje Single Sign-On autentikacije potrebno je ponovo izvršiti naredbe navedene u koraku 3.

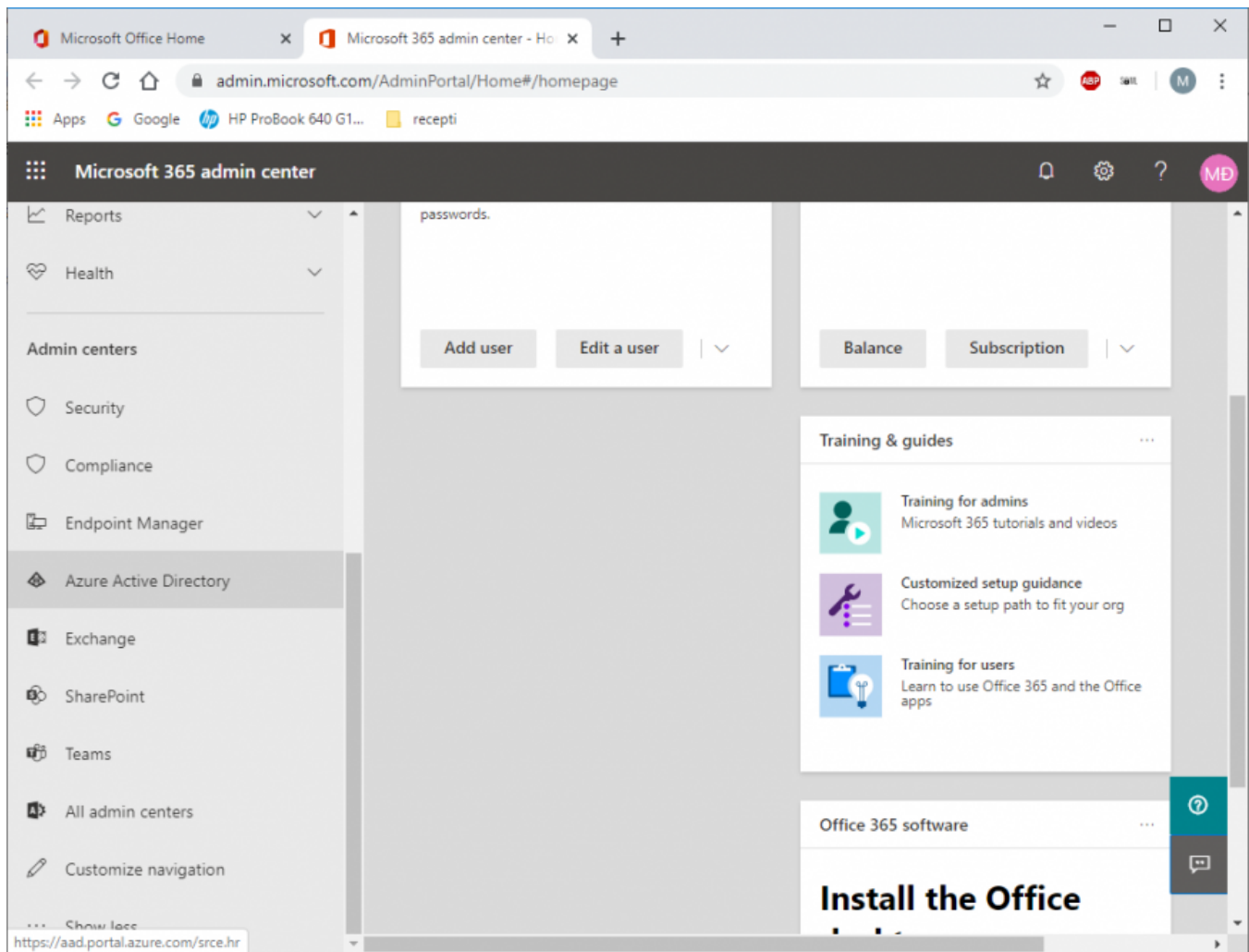
Registracija plugina za sinkronizaciju podataka iz LDAP imenika sa Azure AD-om

Da bi se klijentska aplikacija (u ovom slučaju [libo365connect-aosi-aa](#) plugin) mogla spojiti na Azure AD (Microsoftov imenik u cloudu iz kojeg se autoriziraju korisnici za upotrebu Office 365 usluge nakon uspješne autentikacije na našem SSO servisu), potrebno ju je registrirati u Azure web sučelju, iz sučelja prekopirati parametre potrebne za njeno spajanje na Azure (client ID i key), te ovlastiti plugin da čita i piše podatke o korisnicima s vaše ustanove u Azure AD.

1. Prijavite se u web sučelje na adresi: <https://portal.office.com> (onim korisničkim računom koji ste otvorili u prvom koraku i koji je oblika **proizvoljna_kor_oznaka@nekadomena.onmicrosoft.com**, dakle ne AAI@EduHr elektroničkim identitetom);
2. U izborniku koji se otvori odaberite **Admin**:



3. U izborniku s lijeve strane kliknite na Show all, pa odaberite opciju **Azure AD**. Nakon toga ćete biti preusmjereni na upravljačko sučelje Azure AD. U tom procesu ćete možda morati opet unijeti zaporku:



4. Sad kliknite na **Azure Active Directory**, pa na **App registrations**, pa na **New registration**:

Microsoft Office Home x Microsoft 365 admin center - Ho x Sveučilišni računski centar Sveuč...

← → ↻ 🔍 aad.portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/RegisteredApps ☆ 🔒 🔒 🔒

Apps Google HP ProBook 640 G1... recepti

Azure Active Directory admin center

Dashboard > Sveučilišni računski centar Sveučilišta u Zagrebu | App registrations

Sveučilišni računski centar Sveučilišta u Zagrebu | App registrations

Search (Ctrl+/)

+ New registration Endpoints Troubleshooting Got feedback?

Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed.

All applications Owned applications

Start typing a name or Application ID to filter these results

Display name	Application (client) ID	Created on	Certificates &
--------------	-------------------------	------------	----------------

Overview
Getting started
Diagnose and solve problems

Manage

- Users
- Groups
- Organizational relationships
- Roles and administrators (Pr...
- Administrative units (Preview)
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Licenses
- Azure AD Connect

5. Upišite naziv aplikacije (npr. AOSI-o365 plugin) i kliknite na **Register**:

Microsoft Office Home | Microsoft 365 admin center - Home | Register an application - Azure

aad.portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/RegisteredApps

Apps | Google | HP ProBook 640 G1... | recepti

Azure Active Directory admin center

Dashboard > Sveučilišni računski centar Sveučilišta u Zagrebu | App registrations > Register an application

Register an application

The user-facing display name for this application (this can be changed later).

AOSI-o365 plugin ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Sveučilišni računski centar Sveučilišta u Zagrebu only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

Redirect URI (optional)

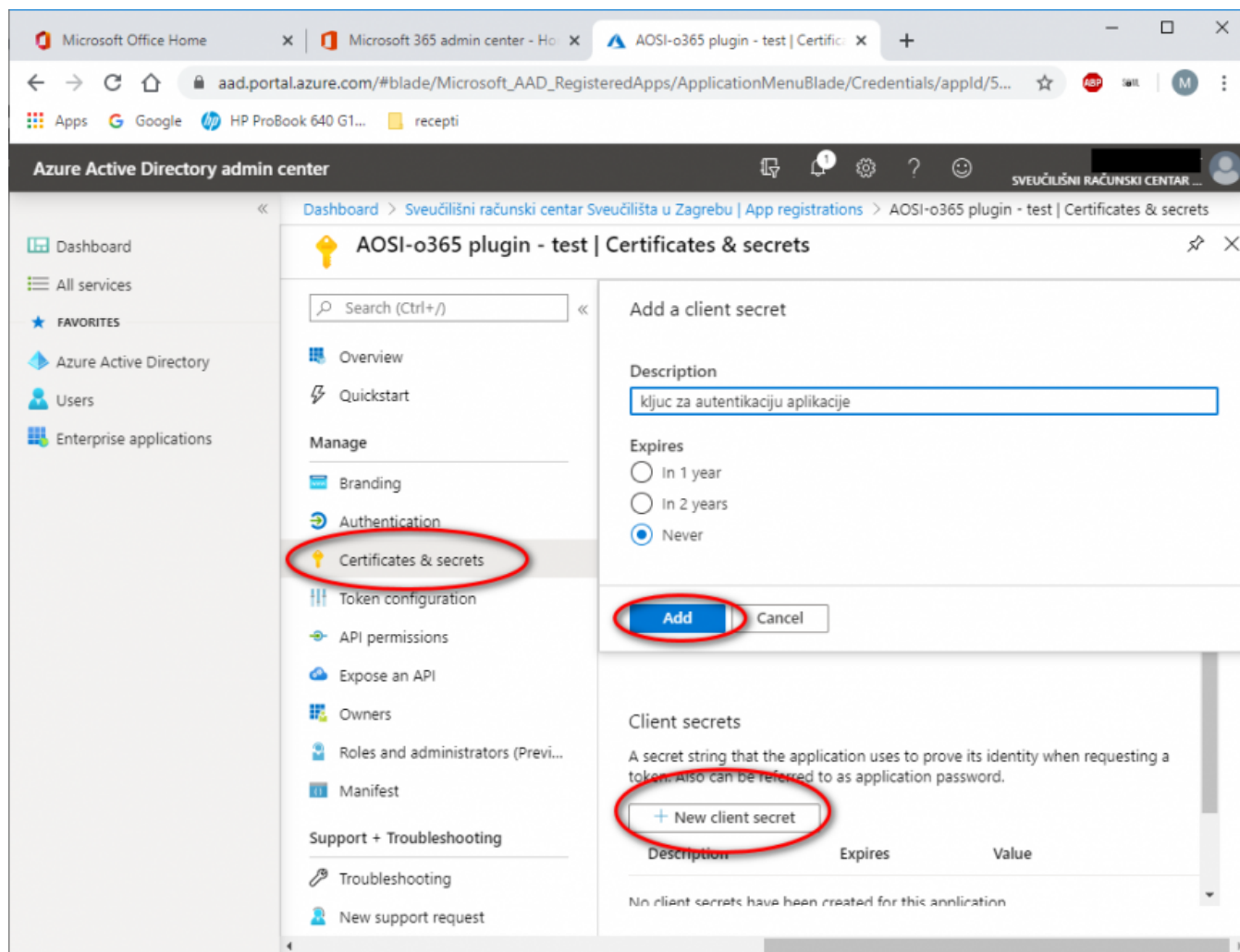
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | e.g. https://myapp.com/auth

[By proceeding, you agree to the Microsoft Platform Policies](#)

Register

6. U ovom koraku je potrebno izgenerirati ključ kojim će se vaš plugin predstavljati Azure AD. U novododanoj aplikaciji kliknite na **Certificates & secrets**, pa na **New client secret**, upišite opis, odaberite željeno vrijeme trajanja i kliknite na **Add**.



7. Nakon dodavanja ključa, obavezno kliknite na **Copy to clipboard** da kopirate ključ u memoriju i zalijepite ga negdje jer će trebati u nastavku ovih uputa za podešavanje plugina.

Microsoft Office Home | Microsoft 365 admin center - Home | AOSI-o365 plugin - test | Certificates & secrets

aad.portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/Credentials/applId/5...

Apps | Google | HP ProBook 640 G1... | recepti

Azure Active Directory admin center

Dashboard > Sveučilišni računski centar Sveučilišta u Zagrebu | App registrations > AOSI-o365 plugin - test | Certificates & secrets

AOSI-o365 plugin - test | Certificates & secrets

Search (Ctrl+/)

- Overview
- Quickstart
- Manage
 - Branding
 - Authentication
 - Certificates & secrets**
 - Token configuration
 - API permissions
 - Expose an API
 - Owners
 - Roles and administrators (Previous)
 - Manifest
- Support + Troubleshooting
 - Troubleshooting
 - New support request

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

[Upload certificate](#)

Thumbprint	Start date	Expires
No certificates have been added for this application.		

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

Description	Expires	
kljuc za autentikaciju ...	12/31/2299	FDg=HnN7pFf=h63... Copy to clipboard

8. Da bi plugin mogao prenositi korisnike u Azure AD, mora moći čitati podatke iz imenika i pisati podatke u imenik. Zato mu morate dati odgovarajuće dozvole. Kliknite na **Api permissions**, pa na **Add permission**

Microsoft Office Home | Microsoft 365 admin center - Home | AOSI-o365 plugin - test | API permissions

aad.portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/CallAnAPI/appld/5d...

Apps | Google | HP ProBook 640 G1... | recepti

Azure Active Directory admin center

Dashboard > AOSI-o365 plugin - test | API permissions

AOSI-o365 plugin - test | API permissions

Search (Ctrl+ /) | Refresh

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission | Grant admin consent for Sveučilišni računski...

API / Permissions n...	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

9. Odaberite **Microsoft Graph**

Microsoft Office Home x Microsoft 365 admin center - Home x Request API permissions - Azure x +

← → ↻ 🏠 aad.portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/CallAnAPI/appld/5d... ☆ 🔒 🔒 🔒 M

Apps Google HP ProBook 640 G1... recepti

Azure Active Directory admin center


Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications


Request API permissions


Select an API


Microsoft APIs | APIs my organization uses | My APIs


Commonly used Microsoft APIs


**Microsoft Graph**
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.


**Azure DevOps**
Integrate with Azure DevOps and Azure DevOps server

**Azure Rights Management Services**
Allow validated users to read and write protected content

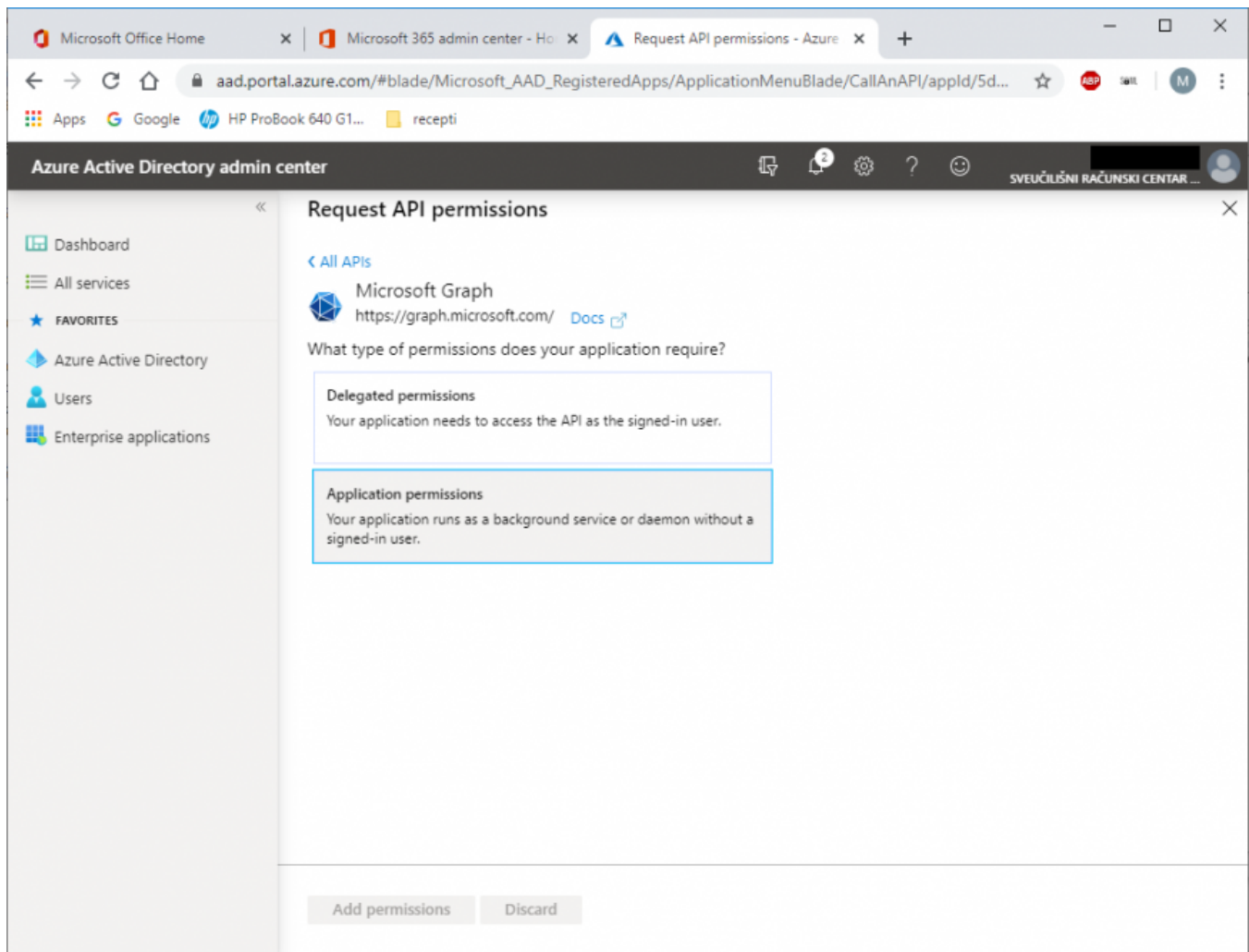
**Azure Service Management**
Programmatic access to much of the functionality available through the Azure portal

**Data Export Service for Microsoft Dynamics 365**
Export data from Microsoft Dynamics CRM organization to an external destination

**Dynamics 365 Business Central**
Programmatic access to data and functionality in Dynamics 365 Business Central

**Dynamics CRM**
Access the capabilities of CRM business software and ERP systems

10. Kliknite na **Application permissions**.



11. Odaberite **User**, pa označite kao na slici dolje potrebne dozvole čitanja i pisanja u Azure AD i kliknite na **Add permissions**.

Microsoft Office Home | Microsoft 365 admin center - Home | AOSI-o365 plugin - test | API permissions

aad.portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/CallAnAPI/appld/5d...

Apps | Google | HP ProBook 640 G1... | recepti

Azure Active Directory admin center

Dashboard > AOSI-o365 plugin - test | API permissions

AOSI-o365 plugin - test | API permissions

Search (Ctrl+/) | Refresh

Warning: You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

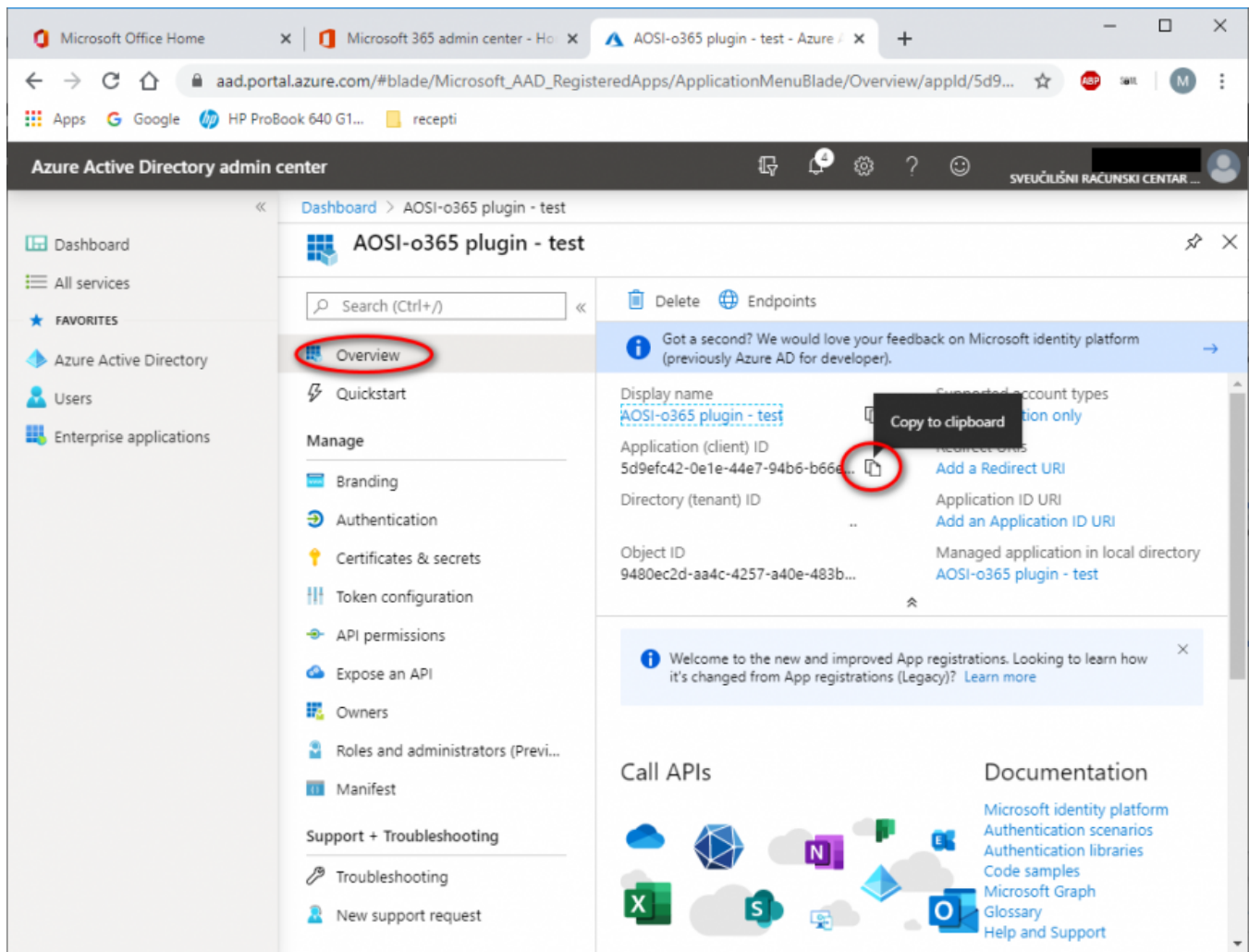
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) | **Grant admin consent for Sveučilišni računski...**

API / Permissions n...	Type	Description
▼ Microsoft Graph (4)		
User.ManageIdent	Application	Manage all users' identities
User.Read	Delegated	Sign in and read user profile
User.Read.All	Application	Read all users' full profiles
User.ReadWrite.All	Application	Read and write all users' full profiles

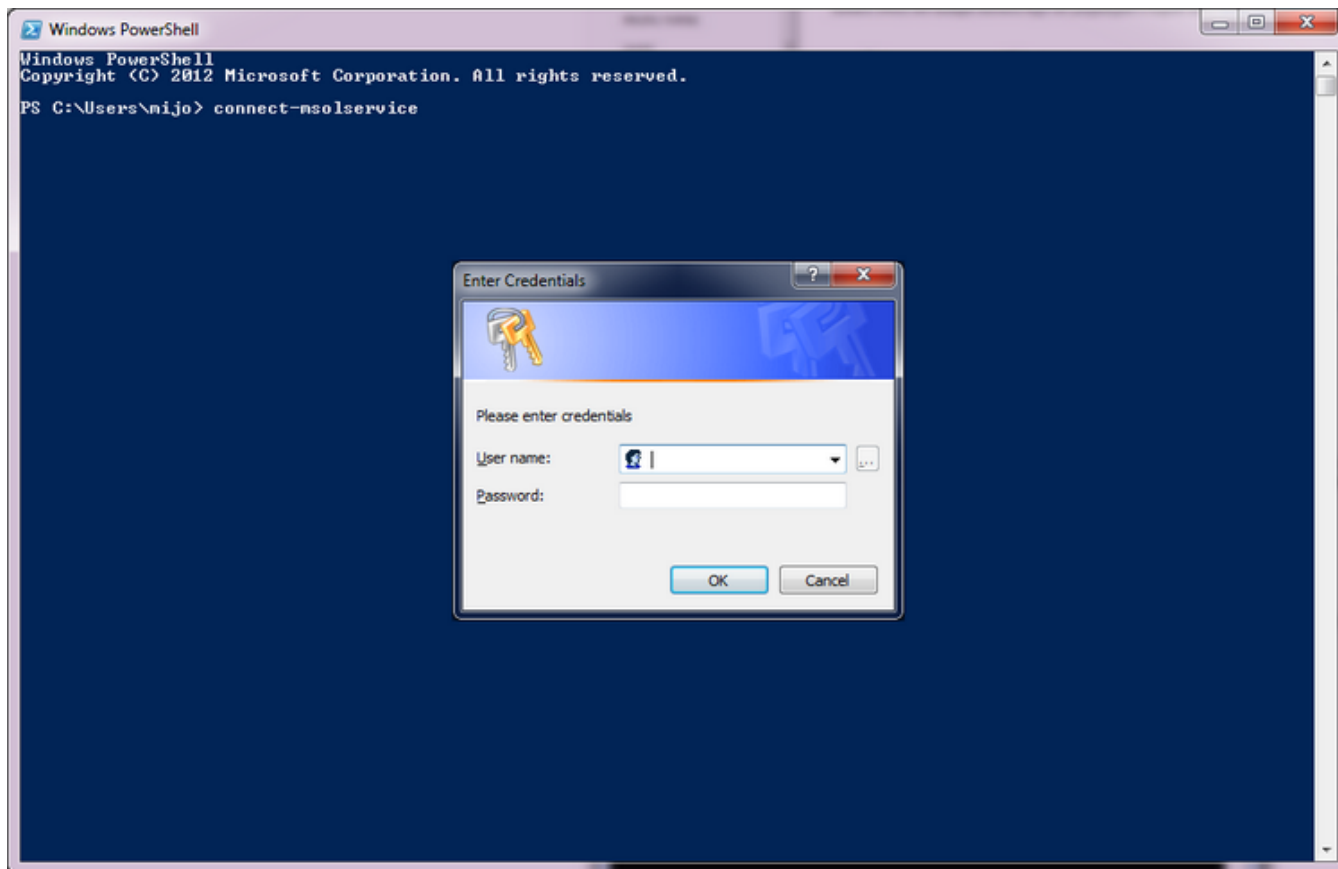
13. Za nastavak podešavanja plugina, potreban je application (client) ID. Kliknite na **Overview**, pa na ikonicu pored Client ID, kopirajte ga u memoriju i zalijepite u neku datoteku da ga iskoristite u nastavku uputa



14. Da bi vaša aplikacija ([libo365connect-aosi-aa1 plugin](#)) imala sve potrebne dozvole, potrebno ju je dodati u grupu administratora. Za tu operaciju na svom računalu pokrenite **Windows Powershell konzolu**, izvršite naredbu:

```
PS C:\> connect-msolservice
```

i prijavite se uporabom administratorskog korisničkog računa kojeg ste koristili i u prethodnom koraku (onog koji ste otvorili u prvom koraku i koji je oblika `proizvoljna_kor_oznaka@nekadomena.onmicrosoft.com`, dakle ne `AA1@EduHr` elektroničkim identitetom):



15. U ovom koraku ćete koristiti **CLIENT ID** koji ste prije nekoliko koraka kopirali. U prvu naredbu unutar jednostrukih navodnika iskopirajte svoj CLIENT ID i izvršite sljedeći niz naredbi:

```
PS C:\> $ClientIdWebApp = 'OVDJE ISKOPIRAJTE SVOJ CLIENT ID'
PS C:\> $webApp = Get-MsolServicePrincipal -AppPrincipalId $ClientIdWebApp
PS C:\> Add-MsolRoleMember -RoleName "Company Administrator" -RoleMemberType ServicePrincipal -
RoleMemberObjectId $webApp.ObjectId
```

16. Time ste završili podešavanje Azure AD za sinkronizaciju s vašim imenikom. Prije nego krenete instalirati plugin, još trebate biti sigurni da imate dovoljno licenci za dodjelu svojim korisnicima koje ćete iz LDAP imenika uvesti u Azure AD. Broj aktivnih licenci možete provjeriti tako da u web sučelju Office 365 usluge na adresi <https://portal.office.com> u izborniku s lijeve strane, odaberete podizbornik **Naplata** pa u njemu kliknete na **Licence** i pogledate koliko valjanih licenci kojeg tipa imate, te od njega oduzmite broj dodijeljenih licenci kako biste saznali koliko Vam je licenci ostalo za dodjelu. Plugin omogućava da se različite vrste licenci dodijele različitim vrstama korisnika ovisno o vrijednosti atributa **hrEduPersonPrimaryAffiliation** (primarna povezanost s ustanovom) zbog toga je važno provjeriti imate li dovoljno licenci za studente/djelatnike.

Office 365

Centar za administratore sustava Office 365

NADZORNA PLOČA | LICENCE

University of Zagreb, University Computing Centre (uređivanje)

Naziv	Valjano	Isteklo	Dodijeljeno
Office 365 Education E3 za nastavničko osoblje	25	0	4
Office 365 Education E3 za učenike i studente	25	0	3

Povratne informacije

Isti podatak sa šifrom licence možete dobiti kroz **Windows Powershell konzolu** pokretanjem naredbe:

```
PS C:\> get-msolaccountsku
```

Na slici su istaknute šifre licenci potrebne za podešavanje plugina, a zaokružen je broj valjanih licenci analogno podatku koji je vidljiv kroz web sučelje.

```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\nijo> connect-msolservice
PS C:\Users\nijo> get-msolaccountsku

AccountSkuId                                     ActiveUnits  WarningUnits  ConsumedUnits
-----
SRCEOffice365:STANDARDWOFFPACK_FACULTY           150          0            1
SRCEOffice365:STANDARDWOFFPACK_IW_FACULTY       500000       0            1
SRCEOffice365:STANDARDWOFFPACK_STUDENT          150          0            0

PS C:\Users\nijo> _
```

Instalacija i podešavanje libo365connect-aosi-aai plugina

AOSI plugin [libo365connect-aosi-aa](#) služi sinkronizaciji korisnika iz LDAP imenika ustanove u Azure AD. Detaljan opis plugina, svih njegovih funkcionalnosti i postavki možete pronaći na [stranici s opisom plugina](#). U procesu instalacije trebat ćete upisati **CLIENT ID** i **KEY** koji ste iskopirali u koracima 6. i 7. prethodnog poglavlja pa ih imajte spremne prije nego krenete u postupak instalacije. Plugin ćete instalirati na svom Linux Debian poslužitelju (na poslužitelju morate imati **root ovlasti**) na kojem je instaliran vaš AOSI web servis naredbom:

```
# apt-get install libo365connect-aosi-aa
```

Prijenos postojećih korisnika u Azure AD

Ako plugin instalirate prvi put, potrebno je napraviti početnu sinkronizaciju korisnika iz LDAP imenika u Azure AD. Sinkronizacija se izvodi na način da pokrenete skriptu koja će napraviti eksport korisnika u .ldif datoteku, a sinkronizacijski mehanizam koji je dio plugina će u prvom sljedećem pokretanju (dakle, u sljedećih 10 minuta) korisnike iz .ldif datoteke upisati u Azure AD. Sinkronizacijski mehanizam ne trebate pokretati Vi, već se on pokreće automatski svakih 10 minuta.

Ako u Azure AD / Office 365 već postoje neki korisnici naša je preporuka izbrisati ih prije pokretanja sinkronizacije. Pri tom posebnu pažnju treba obratiti na podatke koje bi ti korisnici mogli imati u Office 365 sustavu. Korisnici koji postoje u Office 365 prije sinkronizacije se više neće moći prijaviti u Office 365 nakon što autentikaciju korisnika preuzme login servis sustava AAI@EduHr zato što im je immutableID već postavljen prilikom otvaranja korisničkog računa u Office 365, a da bi se korisnički račun u Office 365 povezao s e-identitetom vrijednost atributa immutableID u Office 365 treba biti jednaka vrijednosti atributa hrEduPersonPersistentID u imeniku.

Da biste eksportirali sadržaj imenika, na poslužitelju morate imati root ovlasti i pokrenuti naredbu:

```
# /usr/lib/aosi/Plugins/o365connectLdapExport.pl
```

Često postavljana pitanja

U log-u `/var/log/aosi/o365connect/o365connectTransferToAzure.log` mi se pojavljuju greške. U čemu je problem?

Ako Vam se u logu `/var/log/aosi/o365connect/o365connectTransferToAzure.log` pojavljuju greške:

```
Use of uninitialized value in string eq at /usr/lib/aosi/Plugins/o365connectTransferToAzure.pl line 149,  
Use of uninitialized value in concatenation (.) or string at /usr/lib/aosi/Plugins/o365connectTransferToAzure.  
pl line 164
```

potrošili ste licence koje su u postavkama plugina podešene da se dodjeljuju korisnicima. U koraku 16 ovih uputa opisano je kako provjeriti broj dostupnih licenci.

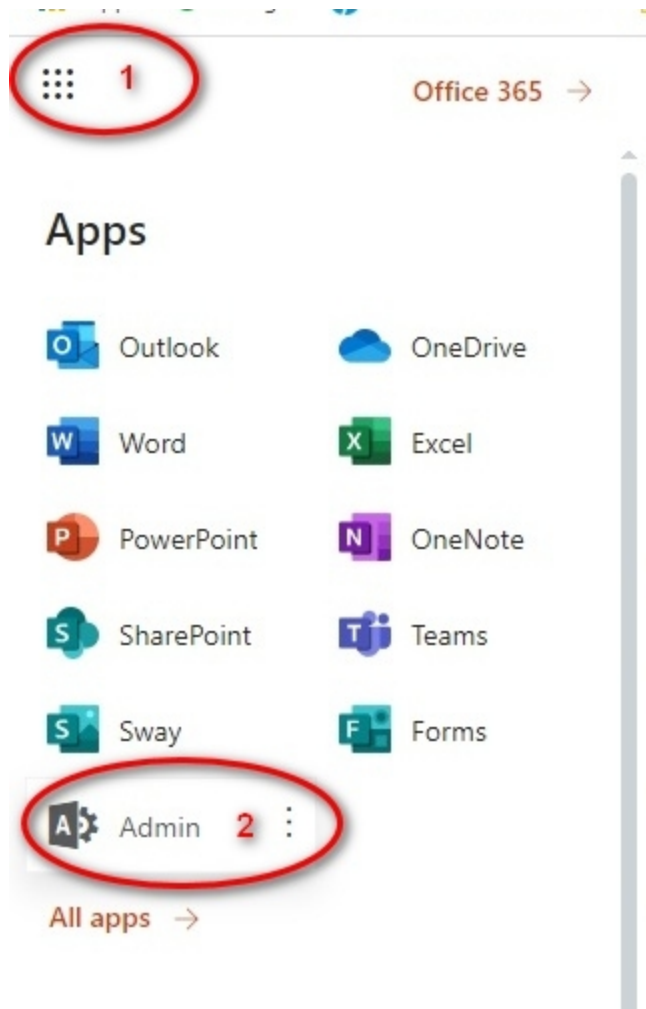
Ako se u logu `/var/log/aosi/o365connect/o365connectTransferToAzure.log` pojavljuju greške:

```
Tue Sep 26 08:10:01 CEST 2017 : status:401 Unauthorized
```

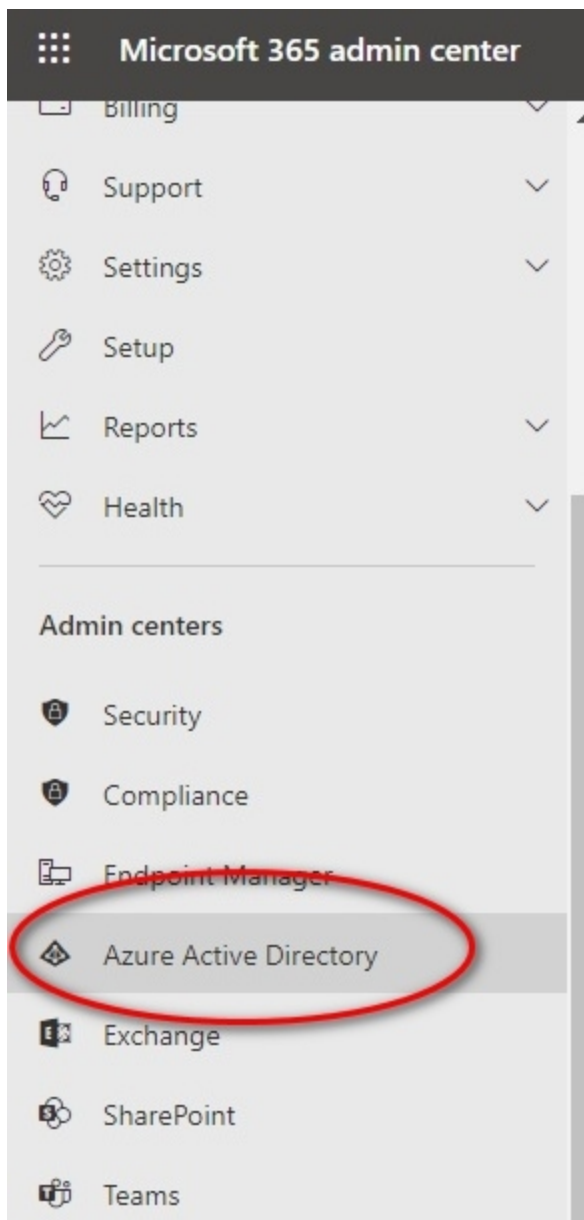
Istekao je ključ koji ste generirali u koraku 6 ovih uputa. Potrebno je generirati novi ključ i upisati ga u [konfiguracijsku datoteku plugina](#) na stazi `/etc/aosi/plugins/o365connect.conf` u parametar `ofc_clientSecret`.

Ključ ćete izgenerirati na sljedeći način:

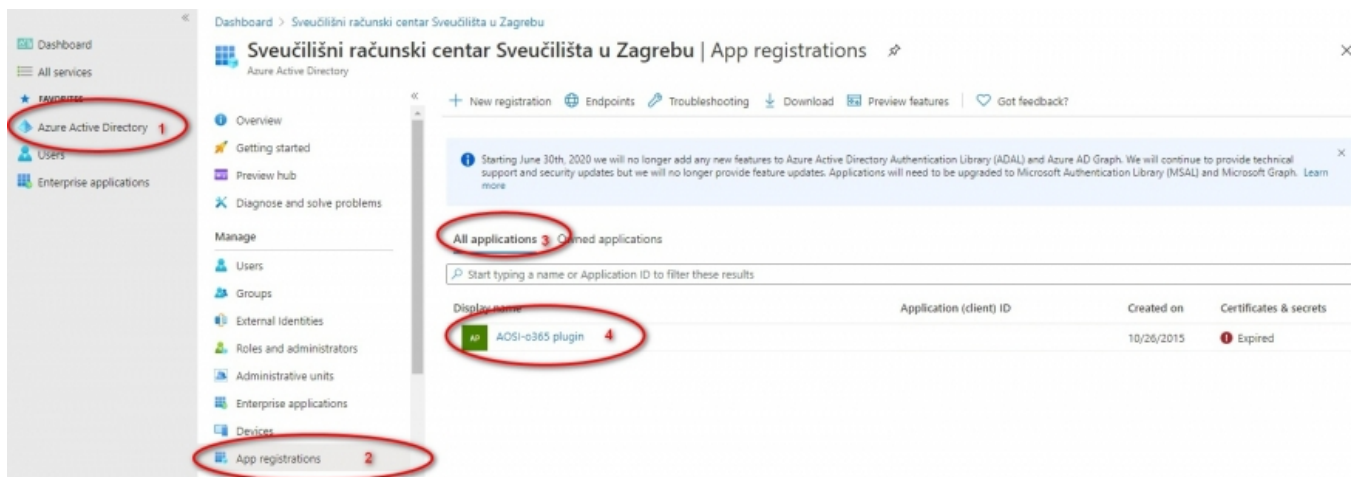
Prijavite se u Office 365 korisničkim računom koji ima administratorska prava. U sučelju kliknite na ikonicu u gornjem lijevom kutu, pa u izborniku odaberite Admin kao na slici dolje:



Nakon toga u izborniku odaberite Admin centers, pa Azure AD kao na slici dolje



U sljedećem koraku iz izbornika odaberite Azure Active Directory, pa App registrations, kliknete na All applications i odaberete AOSI o365 plugin (odnosno svoj plugin ovisno o nazivu plugina koji ste upisali prilikom uspostave veze)



Kliknite na Certificates & secrets i prikazat će Vam se svi do sad generirani ključevi za pligin. Među njima je i onaj istekli kojeg trenutno koristite. Odaberite New client secret

Integration assistant | Preview

Manage

- Branding
- Authentication
- Certificates & secrets 1**
- Token configuration
- API permissions
- Expose an API
- Owners
- Roles and administrators | Preview
- Manifest

Upload certificate

Thumbprint

Start date

No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be

+ New client secret 2

Description	Expires
ključ za autentikaciju aplikacije	12/31/2299

Upišite potrebne podatke - opis ključa, odaberite rok trajanja i kliknite na Add

Add a client secret

Description

Ključ za autentikaciju plugina

Expires

☐ In 1 year

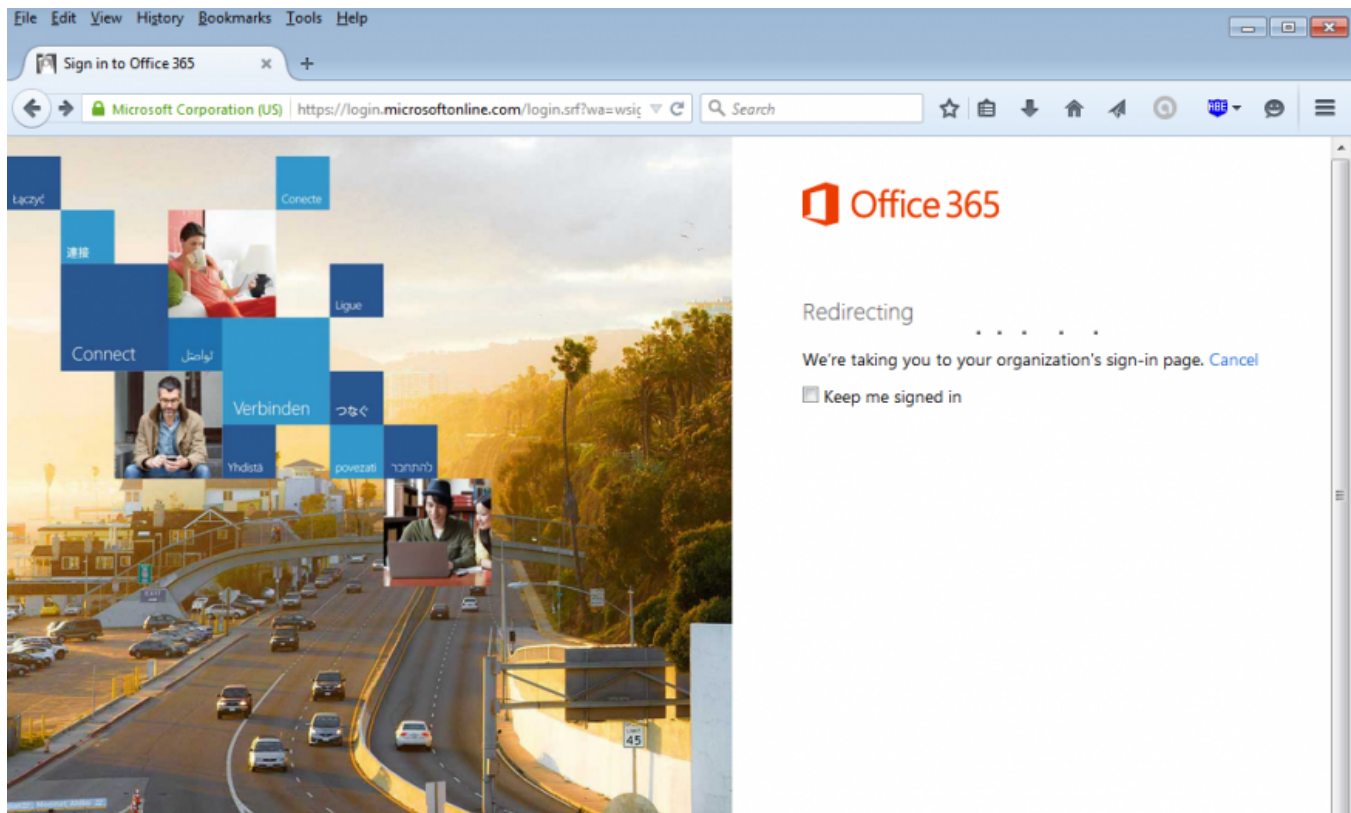
☐ In 2 years

☒ Never

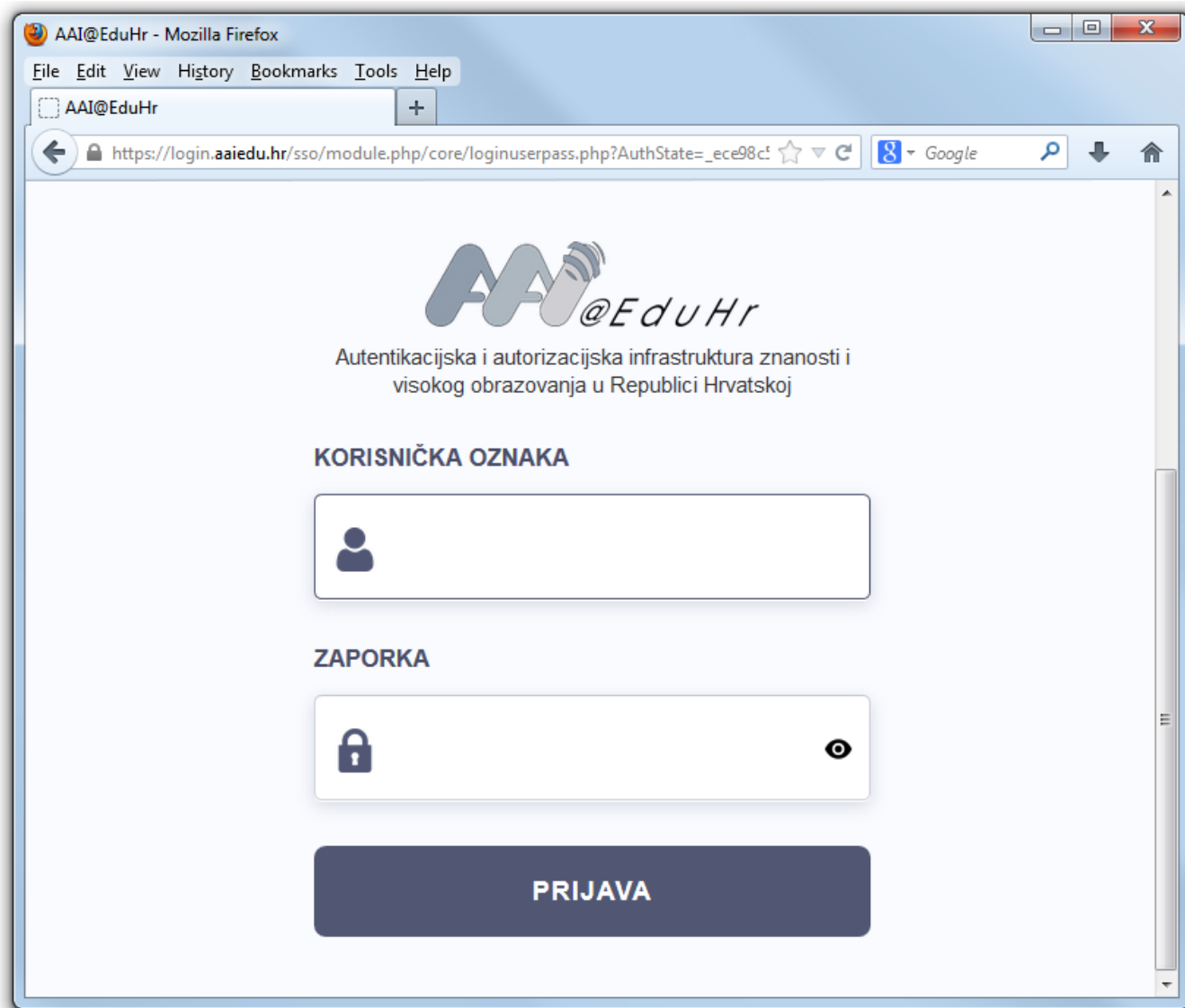
Add Cancel

Client secrets

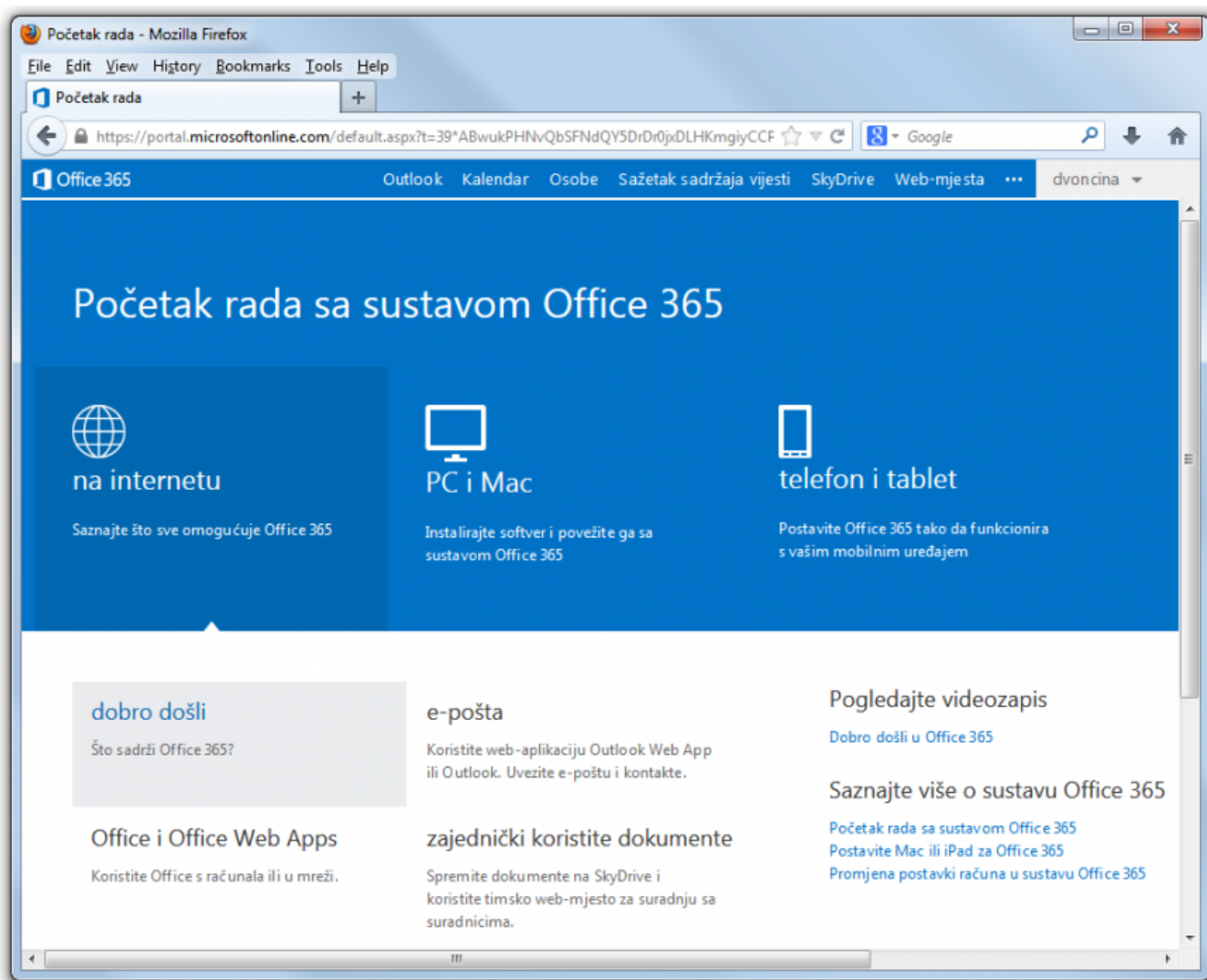
Nakon što je novi ključ kreiran, jako je bitno da ključ u ovom koraku kopirate jer ga poslije nećete moći više vidjeti. Za kopiranje ključa kliknite na ikonicu Copy to clipboard kao na slici dolje. Taj ključ trebate upisati u [konfiguracijsku datoteku plugina](#). Ako su vaši primarni servisi udomljeni na računalu Srca, to je ključ koji trebate dostaviti AAI@EduHr timu.



...u kojem je potrebno unijeti AAI@EduHr korisničku oznaku i zaporku:



Nakon uspješno provedene autentikacije putem sustava AAI@EduHr, uz uvjet da je korisnik registriran za korištenje Office 365 usluge, korisniku će biti omogućen pristup Office 365 portalu:



Je li moguće čitati e-mail desktop klijentom u slučaju kad se korisnici za pristup usluzi Office 365 autenticiraju putem sustava AAI@EduHr?

Uz određene postavke, može se omogućiti čitanje maila iz Outlook 2016 aplikacije. Upute kako su dostupne na adresi:

<https://social.technet.microsoft.com/wiki/contents/articles/36101.office-365-enable-modern-authentication.aspx>

Kako riješiti problem s nemogućnošću pohrane lokalno uređenih dokumenata iz aplikacija koje su dio Office 365 ProPlus paketa u oblak (OneDrive)?

U radu s lokalno instaliranim Office 365 ProPlus aplikacijama uočen je problem da nije moguće pohraniti dokument uređen lokalno u bilo kojoj od aplikacija koje su dio Office 365 ProPlus paketa u cloud (OneDrive, SharePoint) ako se za prijavu koristi AAI@EduHr elektronički identitet.

Opisani problem odnosi se na Office 2013 aplikacije i trebao bi biti riješen objavom novih Office paketa u siječnju 2016. Do objave novog Office paketa, Microsoft preporučuje da uz pomoć uputa dostupnih na adresi:

<https://support.office.com/en-us/article/Office-365-release-options-3B3ADFA4-1777-4FF0-B606-FB8732101F47>

omogućite korištenje Office 365 First release opcije, koja će korisnicima na stranici za preuzimanje Office 365 ProPlus paketa omogućiti preuzimanje najnovije verzije aplikacija. Nakon što se First Release opcija omogući za domenu, korisnici moraju putem portala preuzeti najnoviju verziju Office 365 ProPlus paketa s kojom ne bi trebali imati problema prilikom prijave korištenjem AAI@EduHr elektroničkih identiteta.

Je li moguće uspostaviti vezu sustava AAI@EduHr i Office 365 ako koristim uslugu ugošćavanja AAI servisa na računalu hosting.aiedu.hr?

Da, moguće je. Za uspostavu te veze potrebno je:

- Proći sve korake iz ovih uputa osim koraka **Instalacija i podešavanje libo365connect-aosi-aai plugina i Prijenos postojećih korisnika u Azure AD**;
- Zatražiti povezivanje sustava AAI@EduHr i Office 365 za svoju ustanovu e-mailom na adresu aai@srce.hr;
- Za uspostavu usluge potrebno je pripremiti sljedeće podatke:
 - Client ID - iz koraka 6. ovih uputa
 - Key - iz koraka 13. ovih uputa
 - Kojim grupama korisnika prema vrijednosti atributa temeljna povezanost s ustanovom - hrEduPersonPrimaryAffiliation (cjeloživotno obrazovanje, djelatnik, gost, korisnik usluge, student, učenik, vanjski suradnik) će biti inicijalno dodijeljena koja licenca. Kako doznati koliko pojedinih licenci imate na raspolaganju opisano je u koraku 16. uputa.

U 3. koraku uputa, kod odabira opcije Azure AD sučelje traži ponovnu registraciju te unos broja kreditne kartice. Što dalje?

Opisani problem javlja se zato što Microsoft vašu ustanovu još uvijek nije prepoznao kao edukacijsku, odnosno onu koja ima pravo na besplatan pristup uslugama unutar Office 365 sustava. Ako ste u procesu registracije dobili upitnik o vašoj ustanovi, ispunite ga i pošaljite. Proces registracije ustanove kao edukacijske i dodjele prava na uslugu Office 365, te odgovarajućih licenci može potrajati do 5 dana. Nakon što taj proces završi, moći ćete pristupiti navedenoj opciji bez potrebe za unosom broja kreditne kartice.

Kako izvršiti zamjenu certifikata za provjeru SSO autentikacije?

Procedura zamjene certifikata opisana je [ovdje](#).