

G Suite (Google Apps) for Education

Ustanovama koje koriste G Suite (Google Apps) for Education Google omogućuje Single Sign-On autentikaciju uporabom SAML protokola koji je podržan i od strane AAI@EduHr sustava. Stoga je prilikom pristupanja pojedinim Google web aplikacijama moguća autentikacija korisnika uporabom njihovih AAI@EduHr elektroničkih identiteta. Više informacija o usluzi G Suite for Education te prednostima i eventualnim nedostacima uporabe Single Sign-On autentikacije za G Suite možete pronaći na sljedećim stranicama:

<https://edu.google.com/products/productivity-tools/>

<https://support.google.com/a/answer/60224?hl=en>

U nastavku su navedene upute za konfiguriranje G Suite tako da se autentikacija korisnika može vršiti putem sustava AAI@EduHr.

Važno

Ove upute nastale su u namjeri da se ustanovama koje to žele omogućiti prijava korisnika u G Suite for Education uporabom elektroničkih identiteta u sustavu AAI@EduHr. Međutim, administratori sustava AAI@EduHr nemaju nikakve formalne veze s uslugom G Suite for Education niti pružaju bilo kakvu podršku pri uporabi aplikacija obuhvaćenih navedenom uslugom. Za odgovore na sva pitanja vezana uz uslugu G Suite for Education, kao i rješavanje eventualnih problema prilikom korištenja usluge trebate kontaktirati izravno Google.

Preduvjeti

Da bi autentikacija korisnika na G Suite for Education putem sustava AAI@EduHr bila moguća, korisnici moraju imati prethodno kreirane Google korisničke račune koji moraju biti identični njihovim korisničkim oznakama u sustavu AAI@EduHr. Uz pojedinačno dodavanje korisnika, G Suite ima mogućnost uvoza korisnika iz CSV datoteke, pa se ta funkcionalnost može iskoristiti za inicijalno kreiranje korisničkih računa.

Podešavanje parametara na strani sustava AAI@EduHr

Za početak je putem [AAI@EduHr registra resursa](#) potrebno registrirati G Suite za vašu ustanovu kao novu uslugu u sustavu AAI@EduHr.

Ako nemate dozvolu pristupa Registru resursa, pošaljite nam svoju korisničku oznaku elektroničkom poštom na adresu aai@srce.h pa ćemo vam omogućiti pristup Registru.

Nakon što se prijavite u Registar resursa, kliknite u glavnoj traci izbornika na poveznicu **R registracija resursa**. Otvorit će vam se forma za unos općih podataka o novom resursu:

- U polje **Naziv resursa** upišite: G Suite za [naziv_ustanove]
- U polje **Opis resursa** upišite: G Suite za domenu [LDAP_domena_ustanove]
- U izborniku **Vrsta resursa** odaberite **produkcija**
- U izborniku **Matična ustanova s kojom je resurs povezan** odaberite vašu matičnu ustanovu
- U izborniku **Partner federacije s kojim je resurs povezan** odaberite opciju **resurs nije povezan niti s jednim partnerom federacije**
- U izborniku **Globalna usluga s kojom je resurs povezan** odaberite **G Suite**
- U polje **Web adresa (URL) na kojoj se aplikacija nalazi** upišite https://google.com/a/LDAP_domena_ustanove
- U polja odjeljka **Kontakt osobe i službe** upišite najmanje po jednu osobu za svaku od tri kategorije: voditelj proizvoda, tehnička podrška, podrška korisnicima. Objašnjenje kako se pojedina kategorija koristi u sustavu AAI@EduHr možete naći na stranici [Registar resursa](#).
- Odjeljak **Administratori resursa** koristite ako želite dodati još nekoga tko će osim vas moći ažurirati podatke o resursu.

Ostale podatke popunite po vlastitom nahođenju. Nakon što pošaljete zahtjev za registracijom resursa, prikazat će vam se stranica s općim podacima koje ste zatražili. Kliknite na karticu **Odabir autentifikacijskog segmenta** i potom na gumb **SAML**. Otvorit će vam se forma za unos parametara SAML konfiguracije:

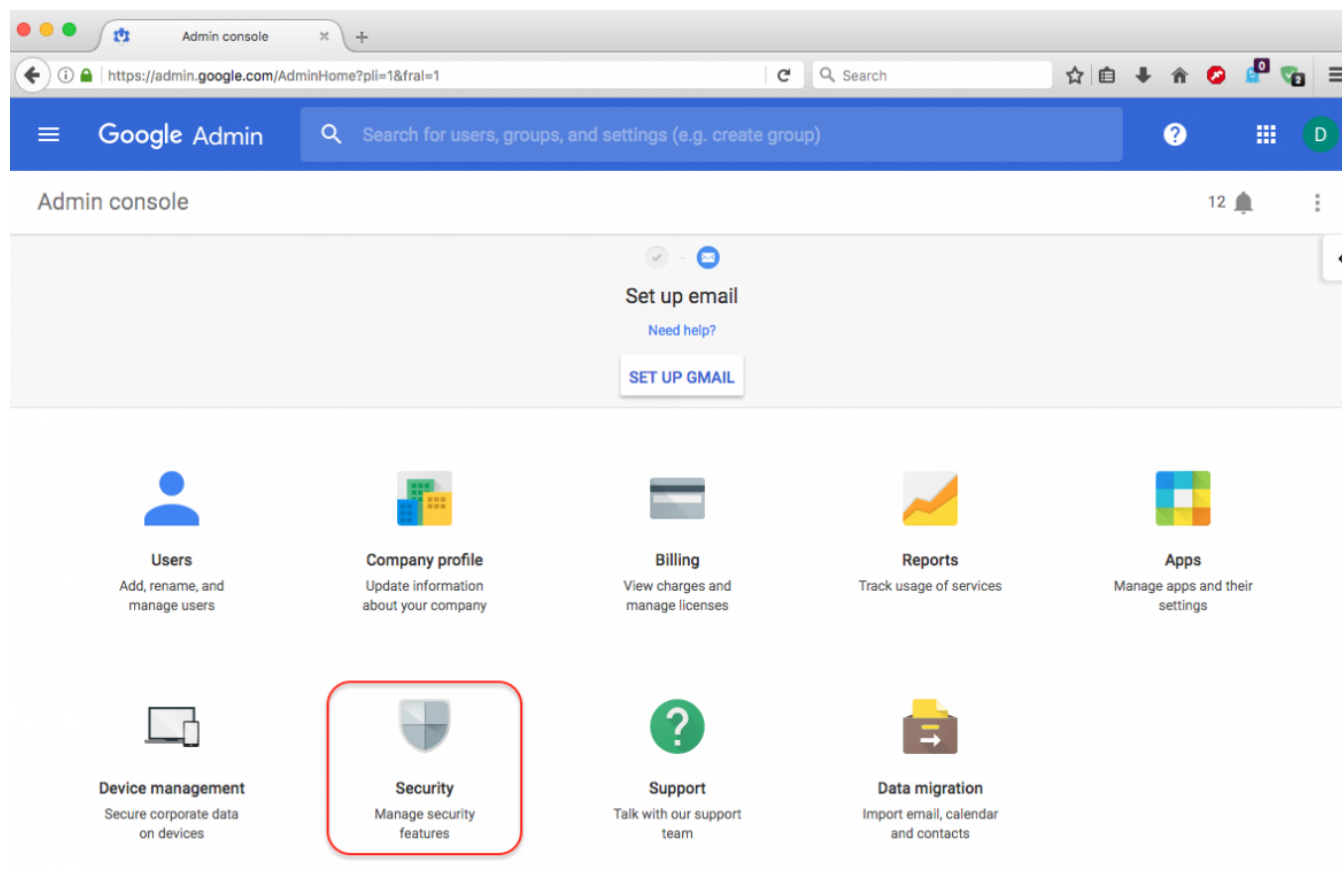
- U izborniku **AuthModule** odaberite **Univerzalni**
- U izborniku **AttributeMapping** mora stajati opcija "nijedna".
- U izborniku **NameIDAttribute** odaberite **hrEduPersonUniqueID** (Korisnička oznaka)
- U izborniku **NameIDFormat** treba stajati **urn:oasis:names:tc:SAML:2.0:nameid-format:transient**
- U polje **entityID** upišite google.com/a/LDAP_domena_ustanove
- U polje **assertionConsumerService** upišite https://www.google.com/a/LDAP_domena_ustanove/acs

- Polje **singleLogoutService** mora ostati prazno!
- Na popisu atributa koje sustav AAI@EduHr treba isporučivati aplikaciji moraju biti odabrani atributi **hrEduPersonHomeOrg** i **hrEduPersonUniqueID**
- U obaveznom polju za **namjenu** odabranog atributa **hrEduPersonHomeOrg** upišite: Identifikacija matične ustanove korisnika

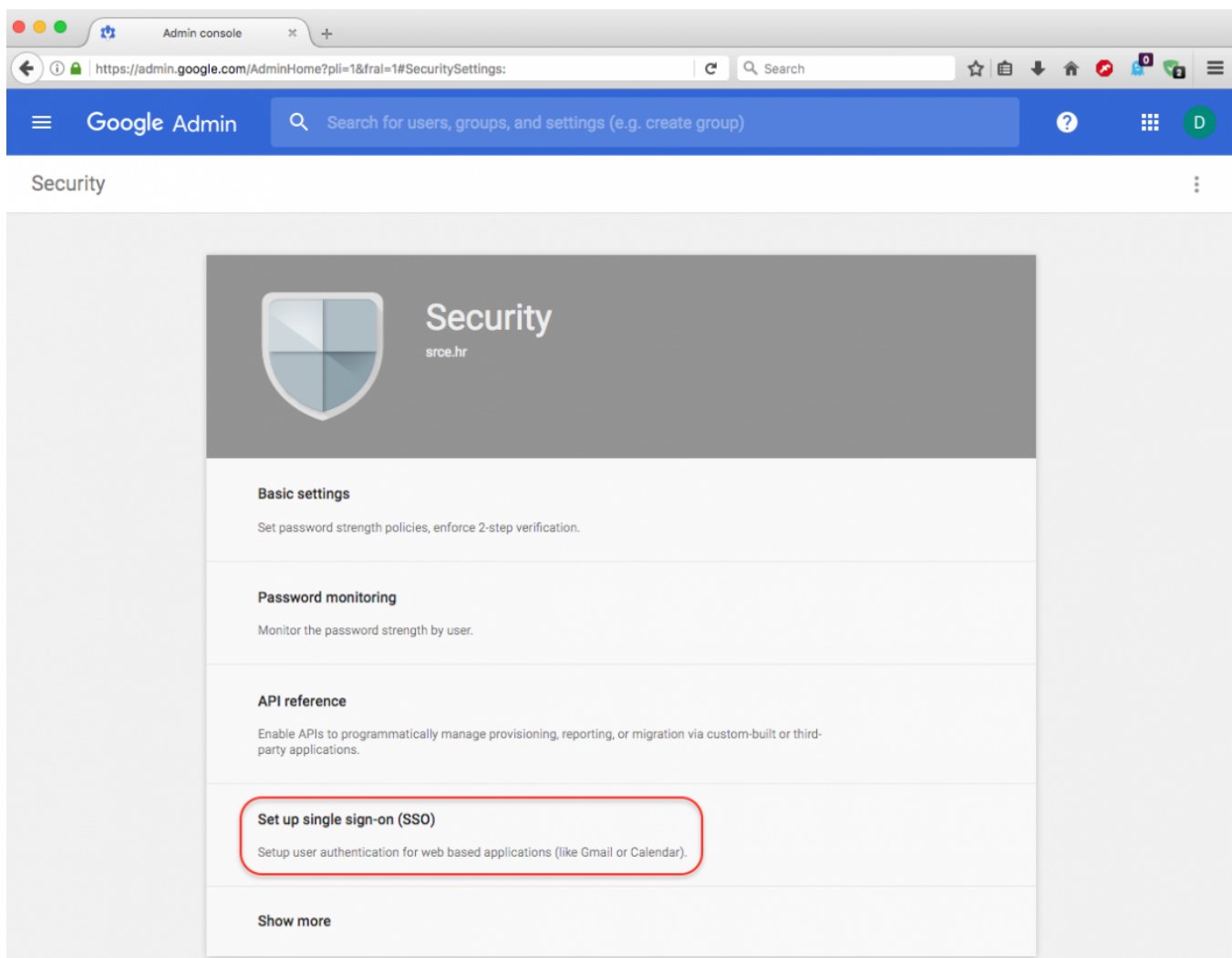
Ostala polja i opcije ostavite prazne (neoznačene). Na kraju kliknite na gumb **Zatraži dodavanje konfiguracije** i pričekajte da netko od administratora sustava AAI@EduHr odobri vaš zahtjev. Obavijest o odobravanju zahtjeva dobit ćete elektroničkom poštom.

Podešavanje parametara na strani G Suite for Education

Nakon što se uporabom administratorske korisničke oznake i zaporka koju vam je dodijelio Google prijavite u [Google administrativno sučelje](#) kliknite na ikonicu **Security** (ako ne vidite navedenu ikonicu, nalazi se u izborniku **More controls** pri dnu ekrana):



i potom odaberite opciju **Set up single sign-on (SSO)**:



Otvorit će vam se izbornik **Set up single sign-on (SSO)** kao što je prikazano na sljedećoj slici:

Admin console

https://admin.google.com/AdminHome?pli=1&frai=1#SecuritySettings:flyout=sso

Google Admin

Search for users, groups, and settings (e.g. create group)

Security

----- OR -----

Option 2

IDP metadata [DOWNLOAD](#)

☐ **Setup SSO with third party identity provider**

To setup third party as your identity provider, please provide the information below. ?

Sign-in page URL

URL for signing in to your system and G Suite

Sign-out page URL

URL for redirecting users to when they sign out

Change password URL

URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled

Verification certificate A certificate file has been uploaded. [Replace certificate](#)

The certificate file must contain the public key for Google to verify sign-in requests. ?

☐ **Use a domain specific issuer** ?

Network masks

Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16). For ranges, use a dash. Example: (64.233.167-204.99/32). All network masks must end with a CIDR. ?

[DISCARD](#) [SAVE](#)

Polja **Enable Single Sign-On** i **Use a domain specific issuer** potrebno je označiti (staviti kvačicu).

U polje **Sign-in page URL** potrebno je upisati adresu AAI@EduHr Single Sign-On autentikacijskog servisa:

<https://login.aaiedu.hr/sso/saml2/idp/SSOService.php>

a u polje **Sign-out page URL** treba upisati sljedeći URL:

<https://login.aaiedu.hr/sso/logout.php>

U polje **Change password URL** upišite adresu web sučelja za administraciju korisničkih podataka u LDAP imeniku vaše ustanove.

Pod opcijom **Verification certificate** učitajte odgovarajući certifikat za središnji autentikacijski servis (kliknite na **Browse...**, odaberite putanju do certifikata i na kraju kliknite na **Upload**). Certifikat možete dohvatiti s [ove adrese](#) na način da na prethodni link kliknete desnim gumbom miša i odaberete opciju **Save Link As...**

Polje **Network masks** možete ostaviti prazno, osim ako sigurnosna politika vaše ustanove ne nalaže drugačije.

Nakon što popunite sve podatke, obrazac bi trebao izgledati otprilike kao što je prikazano na sljedećoj slici:

The screenshot shows the Google Admin console interface. At the top, the 'Admin console' tab is active in the browser. The address bar shows the URL: <https://admin.google.com/AdminHome?pli=1&f=1#SecuritySettings:flyout=sso>. The page title is 'Security'. The main content area is titled 'Option 2' and 'IDP metadata'. There is a 'DOWNLOAD' button. Below this, a checkbox 'Setup SSO with third party identity provider' is checked. A note says: 'To setup third party as your identity provider, please provide the information below.' The form fields are: 'Sign-in page URL' with value 'https://login.aaiedu.hr/sso/saml2/idp/SSOService.php'; 'Sign-out page URL' with value 'https://login.aaiedu.hr/sso/logout.php'; 'Change password URL' with value 'http://www.aaiedu.hr/statistika-i-stanje-sustava/maticne-ustanove/pc'; and 'Verification certificate' with a message 'A certificate file has been uploaded. Replace certificate'. Below these, another checkbox 'Use a domain specific issuer' is checked. At the bottom, there is a 'Network masks' section with explanatory text. At the very bottom right, there are 'DISCARD' and 'SAVE' buttons.

Option 2

IDP metadata [Download](#)

☒ Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below. ?

Sign-in page URL
URL for signing in to your system and G Suite

Sign-out page URL
URL for redirecting users to when they sign out

Change password URL
URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled

Verification certificate
The certificate file must contain the public key for Google to verify sign-in requests. ?

☒ Use a domain specific issuer ?

Network masks
Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16). For ranges, use a dash. Example: (64.233.167-204.99/32). All network masks must end with a CIDR. ?

[DISCARD](#) [SAVE](#)

Kliknite na **Save changes**.

Nakon toga korisnici iz vaše ustanove prilikom prijave na poveznicu:

<https://accounts.google.com>

ili direktno na određeni servis:

https://naziv_servisa.google.com/a/LDAP_domena_ustanove.hr (npr. za Gmail: <https://mail.google.com/a/neka-domena.hr>)

bit će preusmjeravani na središnji AAI@EduHr autentikacijski servis gdje trebaju unijeti svoju AAI@EduHr korisničku oznaku i zaporku. U slučaju uspješne autentikacije korisniku će biti dozvoljen pristup te će biti automatski preusmjeren na odgovarajuću Google aplikaciju.

G Suite administratori će se i dalje moći prijavljivati na administratorsko sučelje <https://admin.google.com> putem Google korisničke oznake i zaporka (bez preusmjeravanja na središnji AAI@EduHr autentikacijski servis). Detalje oko toga u kojem slučaju će se koristiti središnji AAI@EduHr autentikacijski servis, a u kojem će biti potrebno unijeti Google korisničke podatke možete provjeriti na poveznici [Signing in with SSO i Network Mapping results](#).