Sisukord

SAML SSO seadistamise juhend

See juhend kirjeldab samm-sammult, kuidas seadistada SAML ühekordse sisselogimise (SSO) identiteedipakkuja (IdP) Directos.

Eeltingimused

- Teil on õigused Directo süsteemiseadete muutmiseks
- Administraatori õigused teie identiteedipakkujas (nt Microsoft Entra ID, Okta, Google Workspace)
- Teie IdP SAML seadistuse andmed (sisselogimise URL, metaandmete URL)

1. samm: Seadistage oma identiteedipakkuja

Enne Directo seadistamist peate registreerima Directo teenusepakkujana (SP) oma identiteedipakkujas. Kasutage järgmisi väärtusi:

Parameeter	Väärtus
Reply URL / ACS (Assertion Consumer Service)	`https://login.directo.ee/api/saml/callback`
Entity ID / Identifier	Vaikimisi väärtus `https://login.directo.ee/api/saml/callback`. SAML SSO Entity ID (ehk Identifier) on unikaalne nimeserveri ehk teenusepakkuja (Service Provider) tunnus. Kui süsteemi pakutud vaikimisi väärtus ei sobi, on tööstusstandardi kohaselt parim tava kasutada URI-formaadis unikaalset URL-i või kindlaksmääratud URN-i. **See peab olema süsteemis (identiteedipakkujas) rangelt unikaalne!**
Name ID formaat	`urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress` (e-posti vastendamise korral) või `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified` (kasutajanime vastendamise korral)

Kus seadistada:

- **Microsoft Entra ID**: Azure'i portaal → Ettevõtterakendused → Uus rakendus → Loo oma rakendus → Integreeri mis tahes muu rakendus (mitte galeriist) → Ühekordne sisselogimine → SAML → SAML põhiseadistus → Muuda
- **Okta**: Rakendused → Loo rakenduse integratsioon → SAML 2.0 → SAML seadistamine → Üldseaded
- **Google Workspace**: Halduskonsool → Rakendused → Veebi- ja mobiilirakendused → Lisa rakendus → Lisa kohandatud SAML rakendus → Teenusepakkuja andmed

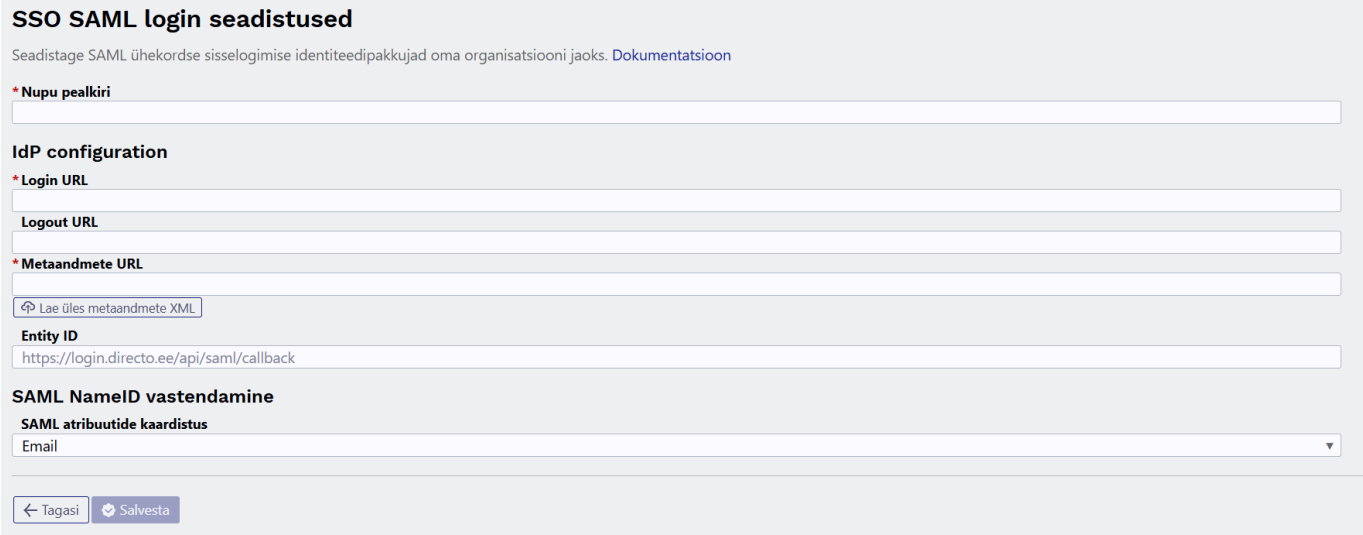
Oluline: Reply URL / ACS ja Entity ID väärtused peavad täpselt kattuma, sealhulgas protokoll (https) ja tee. Mittekattuvad väärtused põhjustavad autentimistõrkeid.

2. samm: Avage SAML SSO seadistus

Navigeerige Directos SAML SSO seadistuste lehele. Näete olemasolevate IdP seadistuste loendit või tühja loendit, kui ühtegi pole veel seadistatud.

3. samm: Looge uus seadistus

1. Klõpsake nupul **Lisa uus**.
2. Avaneb IdP seadistamise vorm.



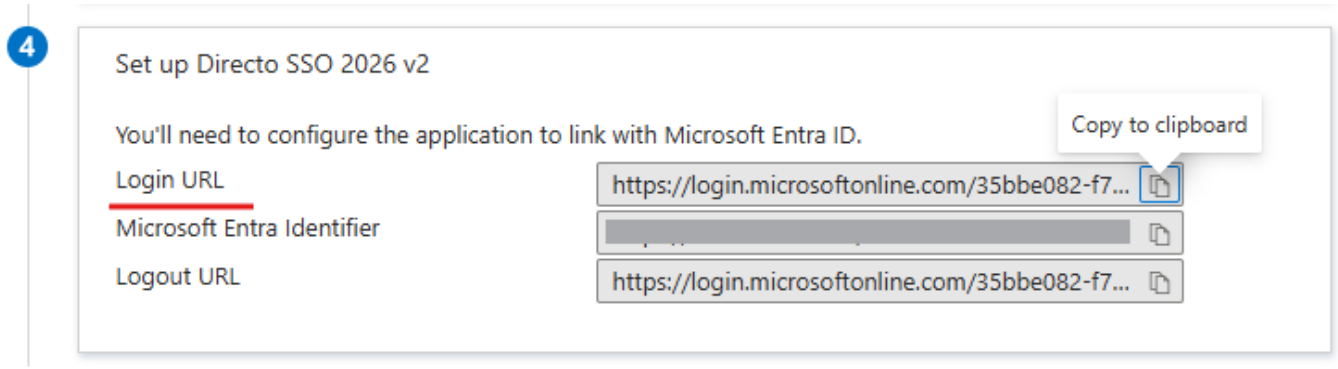
4. samm: Sisestage nupu pealkiri

Sisestage väljale **Nupu pealkiri** kirjeldav nimi. See on tekst, mis kuvatakse SSO sisselogimisnupul Directo sisselogimislehel (nt „Logi sisse Azure AD-ga“ või „Ettevõtte SSO“).

5. samm: Seadistage IdP andmed

Sisselogimise URL (kohustuslik)

Sisestage oma identiteedipakkuja **sisselogimise URL** (tuntud ka kui SSO URL või SAML Endpoint). See on lõpp-punkt, kuhu Directo saadab SAML autentimispäringuid.



Kust leida:

- **Microsoft Entra ID**: Azure'i portaal → Ettevõtterakendused → Teie rakendus → Ühekordne sisselogimine → Sisselogimise URL
- **Okta**: Rakendused → Teie rakendus → Sign On vahekaart → Identity Provider Single Sign-On URL
- **Google Workspace**: Halduskonsool → Rakendused → Veebi- ja mobiilirakendused → Teie rakendus → SSO URL

Väljalogimise URL (valikuline)

Sisestage **väljalogimise URL** (tuntud ka kui SLO URL või Single Logout Endpoint). See võimaldab ühekordset väljalogimist — kui kasutaja logib Directost välja, logitakse ta välja ka IdP sessioonist.

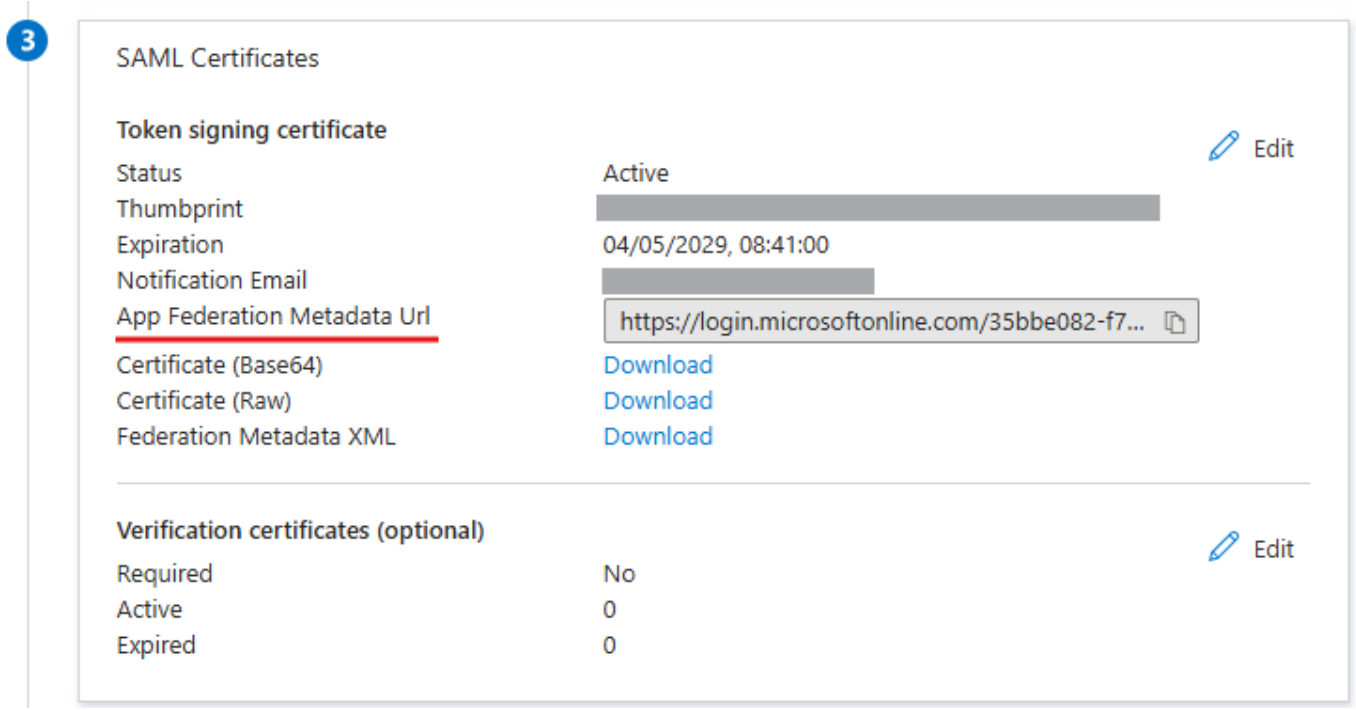
Kust leida: Otsige „SLO URL“, „Logout URL“ või „Single Logout Endpoint“ samast kohast, kus sisselogimise URL teie IdP-s.

Metaandmete URL (kohustuslik)

Sisestage **metaandmete URL**, mis viitab teie IdP SAML metaandmete XML-dokumendile. See URL sisaldab IdP allkirjastamissertifikaate, lõpp-punkte ja muid seadistuse üksikasju.

Kust leida:

- **Microsoft Entra ID**: Azure'i portaal → Ettevõtterakendused → Teie rakendus → Ühekordne sisselogimine → Rakenduse föderatsiooni metaandmete URL
- **Okta**: Rakendused → Teie rakendus → Sign On vahekaart → Metadata URL
- **Google Workspace**: Halduskonsool → Rakendused → Veebi- ja mobiilirakendused → Teie rakendus → Laadi metaandmed alla (kasutage URL-i, mitte faili)



6. samm: Seadistage Name ID vastendamine

Jaotises **SAML NameID vastendamine** valige, kuidas IdP kasutajaid tuvastab:

- **Email** — IdP saadab kasutaja e-posti aadressi Name ID-na. Directo vastendab selle kasutaja e-posti aadressiga süsteemis.
- **Username** — IdP saadab kasutajanime Name ID-na. Directo vastendab selle kasutajanimega süsteemis.

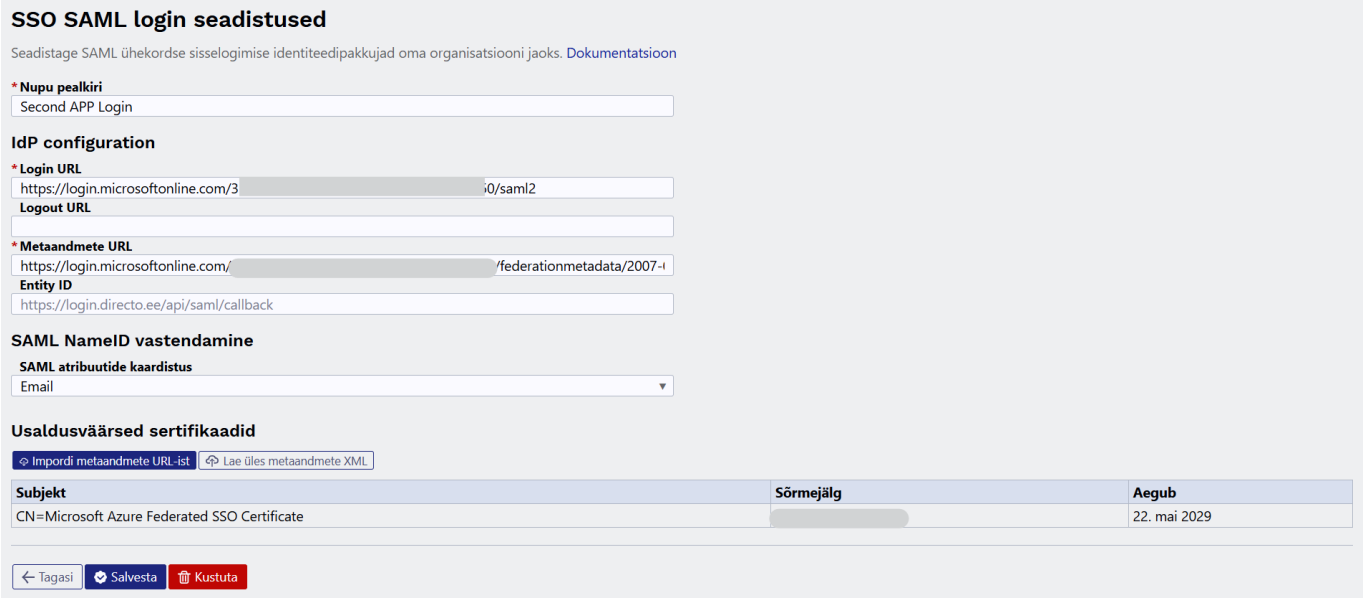
Valige variant, mis vastab sellele, kuidas teie IdP on seadistatud Name ID väidet saatma.

7. samm: Salvestage seadistus

Klõpsake nupul **Salvesta**. Kui sisestasite metaandmete URL-i, impordib Directo esimesel salvestamisel automaatselt IdP allkirjastamissertifikaadid.

8. samm: Sertifikaatide haldamine

Pärast salvestamist ilmub vormi alla jaotis **Usaldusväärsed sertifikaadid**. See jaotis näitab teie IdP metaandmetest imporditud allkirjastamissertifikaate.



Sertifikaatide importimine

- Sertifikaadid imporditakse automaatselt metaandmete URL-ist esimesel salvestamisel.
- Sertifikaatide käsitsi importimiseks või uuesti importimiseks klõpsake nupul **Impordi metaandmete URL-ist**.

Sertifikaadi vahetamine

Kui teie IdP vahetab allkirjastamissertifikaati:

1. Lisage uus sertifikaat oma IdP seadistuses.
2. Avage Directos vastav IdP seadistus.
3. Klõpsake nupul **Impordi metaandmete URL-ist**, et importida uus sertifikaat.
4. Üleminekuperioodi ajal usaldatakse nii vana kui ka uut sertifikaati.

Sertifikaatide tabel

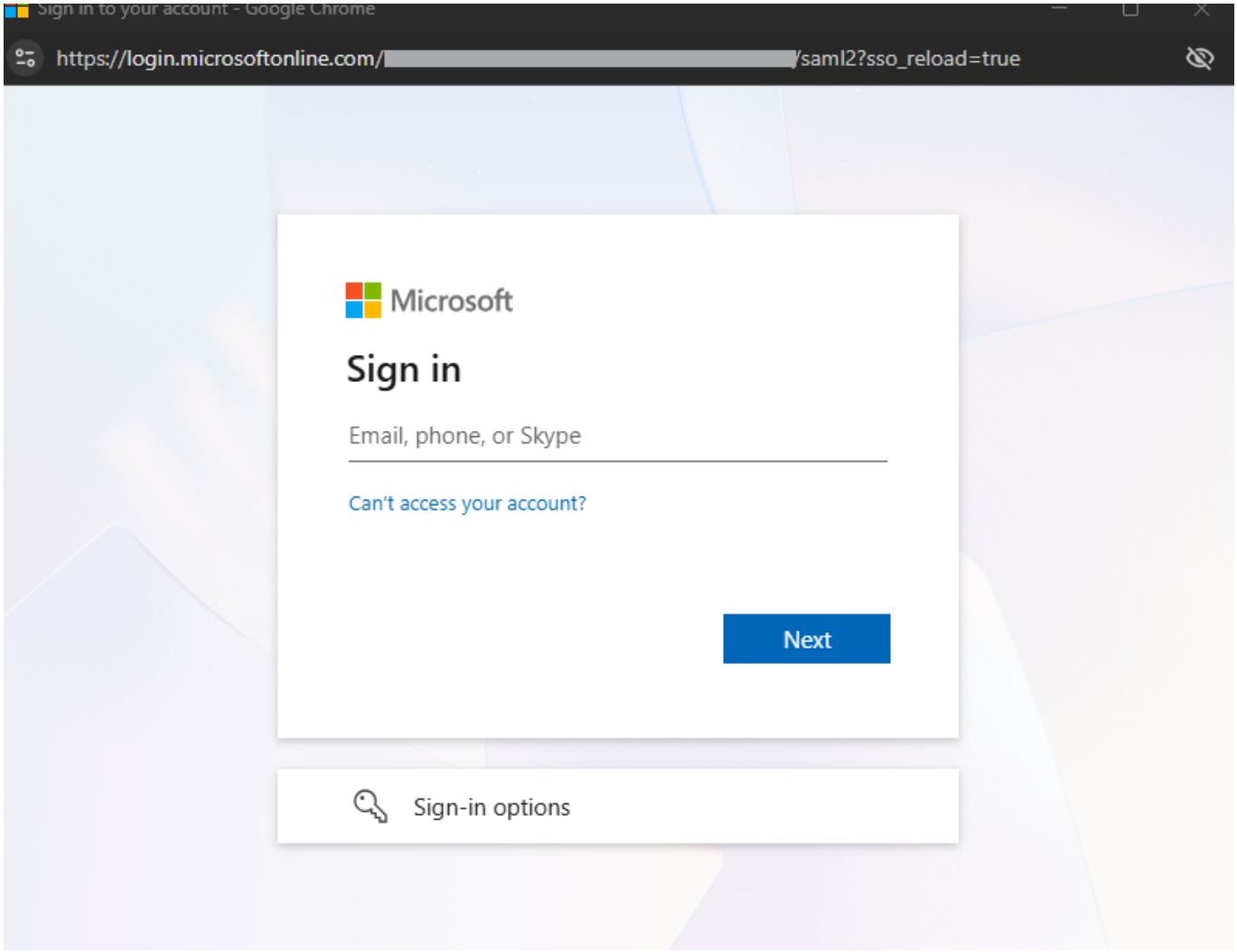
Sertifikaatide tabelis kuvatakse:

Veerg	Kirjeldus
Subjekt	Sertifikaadi subjekt (tavaliselt IdP domeen)
Sõrmejälg	Sertifikaadi unikaalne tunnus (lühendatud loetavuse huvides)
Aegub	Sertifikaadi aegumiskuupäev. Kui sertifikaat on aegunud, kuvatakse hoiatusikoon.

9. samm: Testige seadistust

1. Avage Directo sisselogimisleht uues brauseriaknas või privaatses/inkognito aknas.
2. Peaksite nägema uut SSO nuppu teie seadistatud pealkirjaga.
3. Klõpsake nupul ja veenduge, et teid suunatakse teie IdP sisselogimislehele.


Directo
develop baas OÜ
Kasutaja
ID-kaart
Mobiil-ID
Smart-ID
Kasutaja
Parool
Sisene
SSO Login
Näita parooli
Unustasid parooli?
Wiki
65553334
info@directo.ee
Isikuandmete kaitse



1. Pärast IdP-s autentimist peaksite olema suunatud tagasi Directosse ja sisse logitud.

Olemasoleva seadistuse muutmine

1. Klõpsake loendis soovitud seadistuse real.
2. Uuendage vajalikke välju.
3. Klõpsake nupul **Salvesta**.

Seadistuse kustutamine

1. Klõpsake loendis soovitud seadistuse real.
2. Klõpsake nupul **Kustuta**.
3. Kinnitage kustutamine dialoogiaknas.

Hoiatus: IdP seadistuse kustutamine takistab koheselt kasutajatel selle SSO meetodiga sisselogimist.

Veaotsing

Probleem	Lahendus
SSO nupp ei ilmu sisselogimislehel	Veenduge, et seadistus on salvestatud ja nupu pealkiri on määratud.
„Vigane allkiri“ viga pärast sisselogimist	Importige sertifikaadid uuesti metaandmete URL-ist. IdP võib olla vahetanud allkirjastamissertifikaati.
Kasutajat ei leita pärast SSO sisselogimist	Kontrollige NameID vastendamise seadistust. Veenduge, et IdP saadab õige atribuudi (e-post või kasutajanimi) ja et see vastab kasutaja kirjele Directos.
Metaandmete URL tagastab vea	Veenduge, et URL on õige ja kättesaadav. Mõned IdP-d nõuavad rakenduse aktiveerimist enne, kui metaandmete URL on saadaval.