FEIDE G-suite og SSO, erfaringer og

“Hva gjorde vi”.

Narvik kommune har i perioden 01.11.2016 til 31.12.2016 testet Single Sign-On, heretter forkortet SSO, mot G-Suite og foreslår følgende løsning.

Vi viser her punktvis hva som må gjøres før en “slår på SSO for G-suite”.

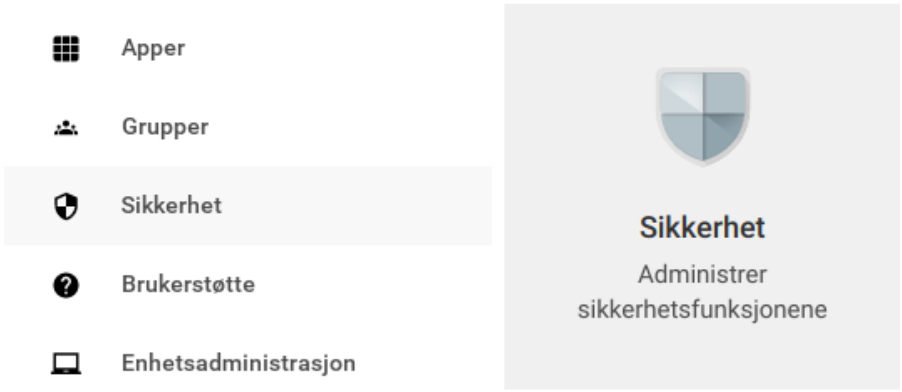
1. Vi har to domener for skolesektoren, et for elever - *elev.narvikskolen.no* og et for lærere/annet personell - *narvikskolen.no*. Vi slo på SSO mot FEIDE for domenet *elev.narvikskolen.no*
2. Alle brukere i *elev.narvikskolen.no* domenet vil få SSO for FEIDE, inklusiv kontoer opprettet manuelt i Admin Console. Kontoer som er administrator i G-suite vil ikke bli berørt av SSO for FEIDE.
3. System kontoer blir dermed utilgjengelig da de ikke kommer fra et skoleadministrativt system og ikke har FEIDE pålogging.
4. Opprette et nytt domene for systemkontoer, og dette domenet må bli satt som “trusted domain”[1] mot hoveddomenet. Vi la alle systemkontoer inn i *navikskolen.no* domenet.
5. Systemkontoer kan være følgende:
    a. En konto for cloud-print-connector, https://github.com/google/cloud-print-connector/wiki
    b. Egne skole-kontoer for deling av connector skrivere til skolene, hvor skolene får full admin control for deling internt på enheten.
    c. Kontoer for distribuering av apper for Android enheter som nettbrett.
    d. Egne kontoer for synkronisering av fellesområder.
    e. Egne kontoer for bruk av Chromebit, https://enterprise.google.com/chrome/devices/chromebit/ og bruk av apper som https://chrome.google.com/webstore/detail/chrome-sign-builder/odjaaghiehpobimgdjjfofmablbaleem
    f. Systemkontoer for våre skolenettsider.
6. Søk Google om å flytte eller opprette et domene for skoler/utdanning via: https://www.google.com/a/signup/?enterprise_product=GOOGLE.EDU#0

[1] https://support.google.com/a/answer/4399436 og https://support.google.com/a/answer/6160020

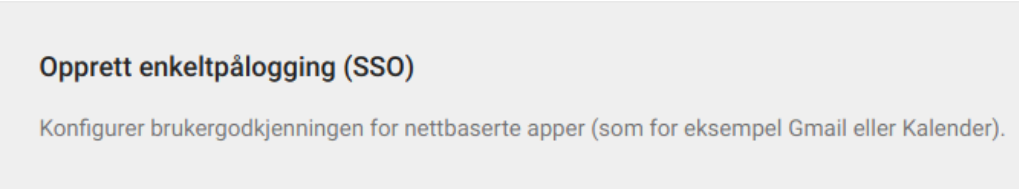
7. Etter at du har opprettet domenet får du 14 dager prøvetid og maksimalt 10 kontoer. Innenfor denne tiden kan du søke om å få utvidet antall kontoer og at domenet blir godkjent. Det sendes en e-post fra Google der du må legge ved en del informasjon, blant annet det som er beskrevet under:
    a. - Official documentation for non-profit status for private school (scanned copy), dette finner du under https://www.brreg.no/
    b. - Diplomas/certificates provided to the students - scanned copies: Malen for vitnemål på din skole, dette kan også finnes i skoleadministrativt system.
1. Når domenene er godkjent av Google så registrer tjenesten i Feides kundeportal, https://kunde.feide.no/
    a. Sett navnet på tjenesten til noe ala 'G Suite for <navn> Kommune' og entityID til 'google.com/a/<domenenavn>'
    b. Ditt domenenavn finner øverst til venstre etter at du har logget på i admin console.
    c. Så for Narvik sitt domene blir entityID 'google.com/a/elev.narvikskolen.no'.
8. Kontakt support@feide.no eller tlf: +47 73 55 79 90 og si at 'tjenesten er registrert, men i og med at det er G Suite har dere ikke noen metadata å sende over'.
9. Når du har fått svar fra FEIDE med bekreftelse på at SSO er satt opp på Feide sin side, samt at du/dere har informert skolene om dette, kan du endre i oppsettet.

Følgende innstillinger ble endres i admin console for å aktivere SSO for domenet vårt, *elev.narvikskolen.no*

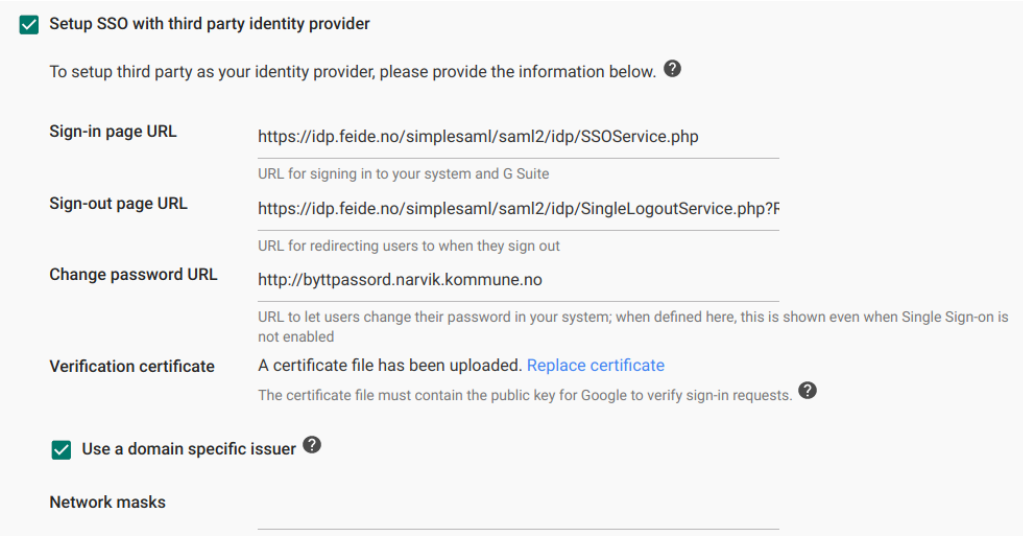
    a. Logg på ditt domene i Google > http://admin.google.com
    b. Klikk på "Sikkerhet"



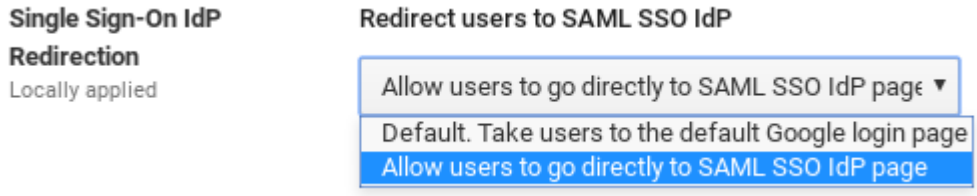
c. Gå inn i Opprett enkeltpålogging (SSO)



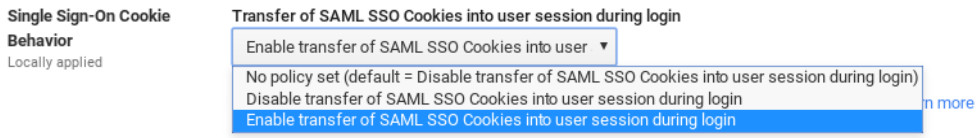
d. Fyll inn nødvendig info og hent sertifikatet fra feide idp. Sertifikatet finnes nederst på: https://idp.feide.no/simplesaml/saml2/idp/metadata.php?output=xhtml, last den ned og last det opp som vist her i "Replace certificate"



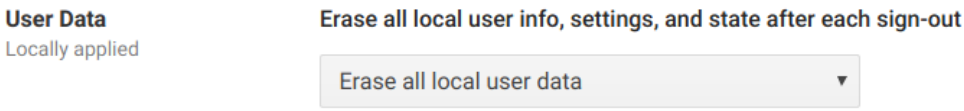
e. Fyll inn Sign-in-page URL https://idp.feide.no/simplesaml/saml2/idp/SSOService.php
f. Fyll inn Sign-out page URl: https://idp.feide.no/simplesaml/saml2/idp/SingleLogoutService.php?ReturnTo=https://www.feide.no/
g. Fyll inn Change password URL, om dere har en lokal adresse.
h. Husk å merk av Use a domain specific issuer, uten at denne er merket av vil ikke SSO for FEIDE fungere.
i. Videre: Device management > Chrome Management > Device settings > **Single Sign-On IdP Redirection > Redirect users to SAML SSO Idp > Allow users to go directly to saml SSO idp page.**



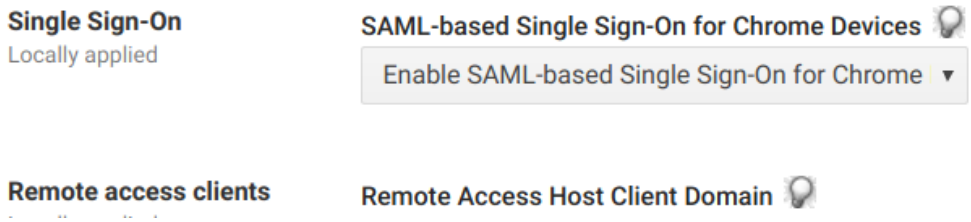
j. Device management > Chrome Management > Device settings > **Single Sign-On Cookie Behavior >Transfer of SAML SSO Cookies into user session during login**



k. **Device management > Chrome Management > Device settings > User Data Erase all local user info, settings, and state after each sign-out:** Denne må være slått på ellers vil ikke feide pålogging fungere ved neste pålogging.



l. **Device management> Chrome > User Settings > SAML-based Single Sign-On for Chrome Devices > Enable….**



Lykke til med SSO mot FEIDE og G-Suite.