

Identity provider migratie

Een migratie van een identity provider is gebruikelijk als er een upgrade aan je identity provider wordt uitgevoerd of overgestapt wordt op een ander systeem. Bij het upgraden van de oude Microsoft ADFS naar bijvoorbeeld Azure veranderen end-points, single sign-on locaties en het entityID van de IdP. Dat laatste is van belang omdat SURFconext het entityID gebruikt ter identificatie van de IdP. Deze mag maar één keer voorkomen in SURFconext. Als de nieuwe IdP eenzelfde entityID houdt, moet een ander pad gevolgd worden.

Hoe je deze nieuwe IdP inricht is te vinden op de pagina met [handleidingen en richtlijnen](#). Zorg er voor dat de attribuutwaarden van de nieuwe identiek blijven aan die de oude IdP vrijgeeft. Denk hierbij ook aan hoofd/kleine letters. Bereid dit voor voordat je ons bericht over de migratie. De stappen voor migratie zijn hieronder toegelicht.

Voorbereiden migratie

We beginnen als je de nieuwe IdP klaar hebt staan.

1. Stuur ons de metadata van de nieuwe. Deze wordt op onze [test](#)- of [productieomgeving](#) toegevoegd. Geef bij ons aan waar je aan de slag wilt en gebruik de corresponderende SP Proxy metadata van SURFconext [test](#) of [productie](#) in jouw [configuratie](#).
2. We gaan controleren of de attributen van de oude- en nieuwe IdP gelijk zijn. **Uid** en **schacHomeOrganization** zijn essentieel. Wijzig deze niet. Het uid, schacHomeOrganization en het daarop gebaseerde NameID (eduPersonTargetedID) worden door veel diensten gebruikt ter identificatie. Wijziging heeft tot gevolg dat gebruikers geen toegang meer hebben tot hun profielen.
 - a. Stuur ons de attributen van de oude en de nieuwe IdP door te navigeren naar <https://engine.surfconext.nl/authentication/sp/debug> en te klikken op "Mail naar SURFconext-Beheer". Als je op test werkt, gebruik dan <https://engine.test.surfconext.nl/authentication/sp/debug>. Zie ook onze [attributenpagina](#) voor meer informatie over attributen.
3. Zorg dat de SingleSignOnService-locaties minstens een score 'B' heeft op [SSL-Labs](#). Als dit niet het geval is, sluiten we de IdP niet aan op productieomgeving. Je hebt nog tot de dag van de migratie om dit [op te lossen](#).
4. Voordat de migratie gedaan wordt moet alles getest zijn. Gebruik hiervoor de [Profiel](#) ([Profiel](#), [test](#)) of [debugpagina](#) zoals in stap 2 aangegeven. Controleer of alle voor jullie gangbare browsers. Stuur ons bij deze stap niet de debug info. Controleer op onze test pagina's zelf of je de attributen ziet zoals verwacht.
5. Geef aan wanneer je de migratie wilt uitvoeren. Het volgende hangt hier mee samen:
 - a. Een vooraankondiging van de migratie wordt door ons een week voordien verstuurd naar de technisch contactpersoon van diensten met een eigen WAYF (Where Are You From).
 - b. Indien nodig wordt de nieuwe één dag voor migratie toegevoegd aan de eduGAIN-feed. De IdP is dan op de dag van de migratie opgenomen in eduGAIN.
 - c. Indien van toepassing, worden statische Step-up, MFA en Consent-regels van de oude IdP naar de nieuwe IdP overgezet.
 - d. Waar van toepassing zal de nieuwe IdP worden opgenomen in de access- en step-up policies van de SURFconext Policy Engine (PDP).

De migratie

Op de dag van migratie doorlopen we de volgende stappen:

1. We verplaatsen de nieuwe IdP naar de productie omgeving van SURFconext. Zorg dat de IdP naar de [productieomgeving van SURFconext](#) verwijst.
2. Wij zetten alle diensten over van de oude naar de nieuwe IdP. Diensten met een eigen WAYF blijven verbonden met beide.
3. Jullie testen de nieuwe IdP op diensten die gebruik maken van de SURFconext WAYF. Stel ons op de hoogte als er problemen zijn.
 - a. Bij problemen zal er overlegd worden. Indien nodig vallen we terug op de oude IdP.
 - b. Test met alle accounttypes (employee, student, etc).
 - c. Test statische step-up (MFA en/of SURFsecureID) en controleer de access- en step-up policy rules.

De dagen na migratie

1. Wij sturen herinneringen naar diensten die een WAYF gebruiken om de nieuwe instantie te gebruiken. Controleer dit in de dagen (en soms weken) na migratie. **De oude IdP blijft in gebruik totdat de laatste dienst over is!**
2. De oude IdP wordt uit eduGAIN verwijderd.
3. Als de laatste dienst is ontkoppeld, gaat de oude IdP offline. Deze wordt verwijderd uit SURFconext. Wij hebben een backup tot ons beschikking.



Omdat een dienst zelf kan bepalen of de WAYF van SURFconext of de eigen WAYF wordt getoond, hebben wij niet direct inzicht in de implementatie bij migratie. Zelfs bij diensten waarbij de metadata wel automatisch wordt bijgewerkt is een kortstondige uitval onvermijdelijk. De tijd tussen deze updates kunnen tussen de 5 minuten of zelfs 24 uur liggen. Soms duurt de overgang weken.

Als we alle stappen hebben doorlopen ben je gemigreerd. Als wij het goed hebben gedaan hebben gebruikers niets gemerkt en hebben ze gedurende de migratie gewoon gebruik kunnen maken van de op SURFconext aangesloten diensten.