Autorisatieregels

Op deze pagina vind je meer informatie over de mogelijkheden om toegang tot diensten via SURFconext te geven of beperken via autorisatieregels (er is een aparte pagina met een overzicht van alle manieren om diensten voor een beperkte groep beschikbaar te maken). Voor de duidelijkheid: de regels waar we het hier over hebben zijn niet bedoeld om te bepalen welke groepen gebruikers überhaupt toegang hebben tot SURFconext. Dit dient in de IdP zelf geconfigureerd te worden!

Algemene uitleg

We behandelen op deze pagina de volgende zaken:

Waarom 'autorisatieregels' in SURFconext?

Zoals op 'Beschikbare diensten activeren' genoemd (en in deze animatie behandeld), wil je soms niet dat iedereen van je instelling via SURFconext kan inloggen bij/op een dienst:

- Soms wil je dat alleen een bepaald onderdeel, bijvoorbeeld een bepaalde faculteit, bij een dienst kan (bijvoorbeeld omdat toegang geld /licenties kost)
- Soms is er een reden om alleen studenten of juist alleen docenten bij een dienst toe te laten
- Vaak mogen voorinschrijvers nergens bij, maar bij bepaalde diensten juist wel
- Soms mogen alleen bepaalde mensen die samen in een groep/team zitten bij een dienst

Zonder autorisatieregels krijgt iedere gebruiker van jouw instelling toegang tot een dienst, zodra de koppeling tussen de dienst en jouw Identity Provider geactiveerd is. Het is dan aan de Service Provider om autorisatiefunctionaliteit (wie mag waarbij) in de dienst te bouwen, indien gewenst. Dat kan bijvoorbeeld door in de dienst zelf gebruikers aan te maken en te beheren: alleen gebruikers die bekend zijn kunnen dan de dienst gebruiken (provisioning). Of door te controleren of een gebruiker in een bepaalde groep zit (via een VOOT-koppeling).

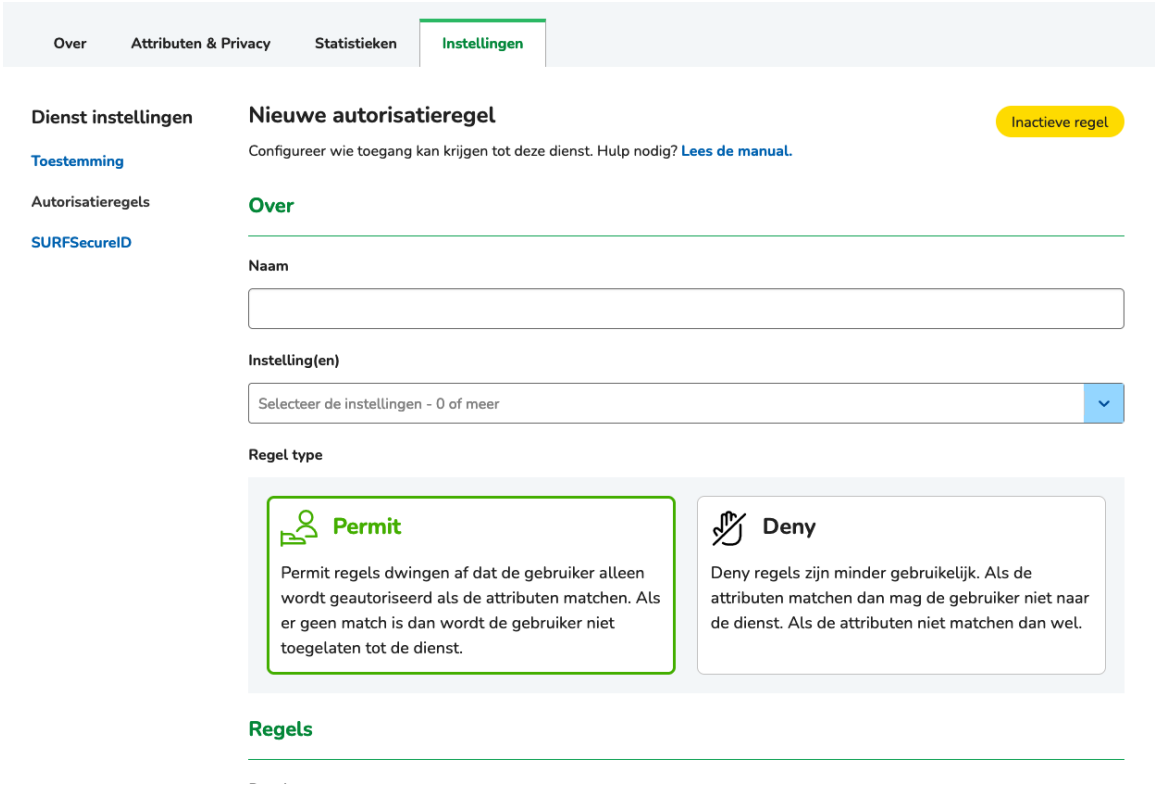
Helaas leert de praktijk dat diensten soms geen autorisatiefunctionaliteit willen of kunnen inbouwen, terwijl instellingen wel graag controle willen hebben over de toegang tot een dienst. Het gevolg is dat instellingen dan maar niemand toegang geven.

Met de autorisatieregels krijgen instellingen een extra mogelijkheid om zelf te bepalen wie toegang heeft tot een dienst via SURFconext.

En voor gebruikers heeft gebruik van autorisatieregels nog een privacy-voordeel: bij gebruik van autorisatieregels, krijgt de SP alleen de gegevens van gebruikers die 'door' SURFconext heen komen; van iedereen die door een autorisatieregel 'wordt tegengehouden', gaan geen gegevens naar de SP. In situaties waarbij binnen een applicatie ('door de SP') wordt bepaald of een gebruiker de applicatie mag gebruiken, krijgt de SP van elke gebruiker die een toegangspoging doet de attributen, dus ook als de SP de gebruiker om welke reden dan ook toegang weigert.

Waar kan ik die regels beheren?

Autorisatieregels worden ingesteld per dienst. Ga naar het SURFconext IdP Dashboard en klik de betreffende dienst aan. Onder het tabblad 'instellingen', vind je 'autorisatieregels'. SURFconext-verantwoordelijken kunnen daar regels beheren, activeren en deactiveren. In de schermen waarin je regels maakt of wijzigt, tref je ook invul-instructies aan:



Wat voor soort regels kan ik maken?

In het SURFconext Dashboard zijn regels aan te maken die:

- de identiteiten die voldoen aan de opgestelde regels toegang ***geven*** tot de dienst (en de rest van de identiteiten dus tegenhouden). Dit heet een 'Permit'-regel
- de identiteiten die voldoen aan de opgestelde regels toegang ***weigeren*** tot de dienst (en de rest van de identiteiten dus doorlaten). Dit heet een 'Deny'-regel

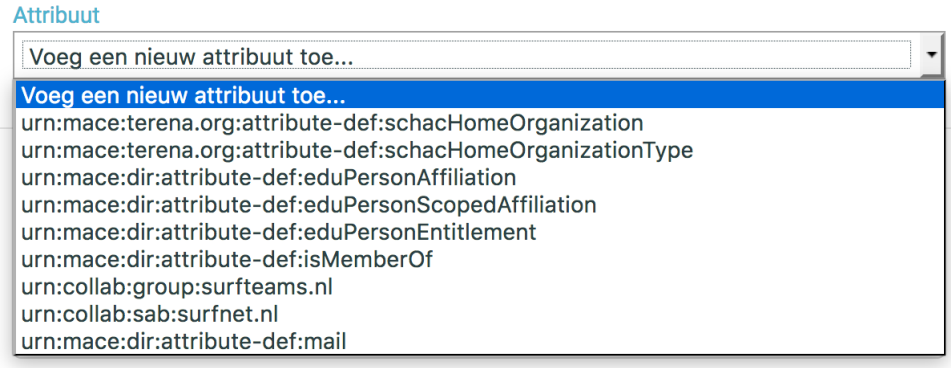
We adviseren in hoge mate 'Permit'-regels te definiëren. De praktijk wijst uit dat Deny-regels vaak leiden tot onbedoelde effecten en toename van complexiteit in relatie tot andere elementen die toegang beinvloeden.

In het scherm waarin je een regel aanmaakt wordt gevraagd voor welke Instellingen/Institutions de regel geldt. Daar geldt:

- Je kunt een IdP (voor zover je daarvoor als beheerder bekend staat) kiezen. De regel geldt dan voor identiteiten die worden uitgegeven door die IdP. Onder "Service" kun je dan een service kiezen waarop de geselecteerde IdP is aangesloten via SURFconext.
- Je kunt ook kiezen om de regel te laten gelden "voor alle IdP's". Dat is voor als je als IdP ook diensten aanbiedt en dus SP bent. Een voorbeeld: instelling X biedt een studenten-portaal aan en heeft die open gezet voor gebruik door mensen van andere IdP's. Instelling X kan nu een regel aanmaken die fijnmaziger filtert wie wel en wie niet toegang kan krijgen, b.v. alleen identiteiten waarvan een attribuut een bepaalde waarde heeft, of die lid zijn van een bepaalde groep. Onder "Service" kun je dan de SP kiezen die jouw IdP aanbiedt.

Een regel is gebaseerd op attributen. Mogelijke attributen zijn:

- Attributen die worden doorgegeven vanuit de instelling:



- Lidmaatschap van een groep in SURFconext Teams (https://teams.surfconext.nl)

Je kunt ook reguliere expressies gebruiken, waaronder '.*'. Dit kun je ook gebruiken om met .* op attribuut urn:mace:dir:attribute-def:mail te controleren of een waarde ingevuld is, en zo niet, een boodschap te tonen.

AND? OR?

Een van de keuzes die je bij het maken van een regel hebt is of je een AND-regel wil maken of een OR-regel:

- bij een AND-regel moeten alle controles op attributen waar zijn
- bij een OR-regel moet 1 van de controles op attributen waar zijn

Als je met regels aan de slag gaat, kom je mogelijk voor situaties waarin je complexere regels wil maken, van het type "(X OR Y) AND (W OR Z)". Alhoewel de techniek die we gebruiken dat toestaat, hebben we de volgende afweging gemaakt: een zo complexe regel, is ook te maken door hem te splitsen in 2 of meer regels. Het alternatief zou zijn dat we de regel-beheer-interface zo maken dat zulke complexe regels in 1 regel kunnen worden ondergebracht, maar wij denken dat de interface dan zo complex wordt, dat de huidige oplossing (de complexe regel splitsen in meerdere simpele regels) te prefereren is.

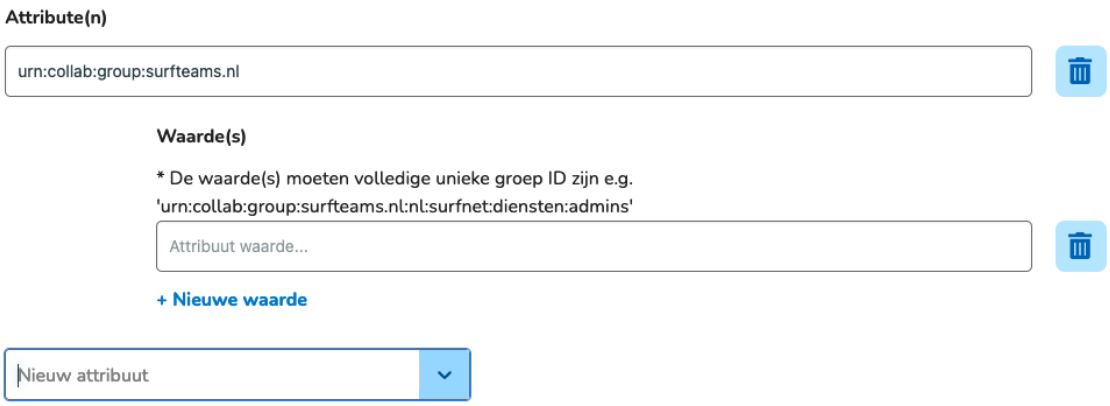
Filteren op groepslidmaatschap

Je kunt toegang ook verlenen (of ontzeggen) op basis van lidmaatschap van een groep. Wanneer je een group-provider-koppeling hebt of installeert, kun je ook lokaal bijgehouden groepen, b.v. groepen in de Active Directory, gebruiken om toegang te regelen!

In de huidige versie gaat het gebruik van team-informatie vanuit SURFconext Teams nog wat omslachtig (we onderzoeken of dat makkelijker kan). Dat heeft o.a. te maken met privacy: we willen geen lijst van alle bekende groepen geven die er bestaan in SURFconext Teams. Aan de andere kant moet een SURFconext-verantwoordelijke niet alleen groepen kunnen gebruiken waar hij/zij zelf beheerder of lid van is: mogelijk zitten mensen van zijn instelling in een groep waar de SURFconext-verantwoordelijke geen toegang toe heeft, maar die hij wel kan gebruiken in een regel.

Hoe werkt het dan? Als je wilt filteren op een groepslidmaatschap van een SURFconext Teams, gaat degene met toegang tot dat team naar SURFconext Teams. Hij logt in en klikt op de desbetreffende groep. Boven de groep staat de "Identificatiecode" die nodig is in de autorisatieregel. Met het pictogram op het eind van de regel kopieer je die naar het klembord.

Deze reeks, "urn:collab:group:surfteams.nl:nl:surfnet:diensten:surfconext_eerstelijns_support", dient bekend te zijn bij de SURFconext-verantwoordelijke: die moet die tekenreeks namelijk plakken in een veld bij het aanmaken van een regel. Wanneer de SURFconext-verantwoordelijke geen toegang heeft tot het team, moet iemand met toegang die tekenreeks even opzoeken, kopiëren en naar de SURFconext-verantwoordelijke sturen (bijvoorbeeld via mail).



Zorg je voor een goede foutmelding?

Per regel kun je een 'Deny-melding' invoeren. Stel je voor dat je door een regel wordt tegengehouden om bij een dienst te komen. Dan is het zowel voor jou als gebruiker, maar ook voor mensen die eventueel alsnog toegang moeten geven, goed te weten waarom toegang nu is geweigerd. Vul dus iets in wat informatief is. Bijvoorbeeld: "Alleen medewerkers hebben toegang tot deze dienst.", of "U heeft geen toegang omdat u geen lid bent van de groep XYZ. Meer weten? Neem contact op met helpdesk@instelling.nl."

Regels aan- en uit zetten, en wat kan ik maximaal fout doen?

Het is belangrijk te beseffen dat:

- Regels veel impact kunnen hebben. Het is mogelijk grote groepen (zelfs iedereen) toegang te geven of juist te ontzeggen.
- Standaard staan regels na het aanmaken uit. Je dient een regel expliciet aan te zetten. Dit kun je doen als laatste stap bij het aanmaken van een regel, of in het overzichtsscherm waarin alle regels staan vermeld.
- Indien je een regel wijzigt die al aan staat, zal die regel bij het opslaan ook direct aanstaan, tenzij je de regel eerst uit hebt gezet. Twijfel je of een wijziging goed uitpakt, dan kun je er voor kiezen een nieuwe regel te maken, dan de oude uit te zetten en de nieuwe aan te zetten. Zo nodig kun je de oude situatie snel herstellen.

Regels testen

We raden je sterk aan je regels te testen. Hoe grondig je wil testen en op welke manier, hangt af van je regel, en of het bijvoorbeeld om een SP gaat die al door veel mensen gebruikt wordt. Aspecten om te overwegen voor een test:

- Bepaal wie op basis van je regel wel en juist geen toegang meer zou moeten hebben tot een bepaalde dienst. Zorg dat je gebruikers 'bij de hand' hebt die direct na het actief maken van de regel, voor je kunnen testen en kunnen laten weten of de regel lijkt te werken zoals je bedoelde (helaas zijn test-accounts op SURFconext niet toegestaan).
- Test de regel eventueel eerst op een test-SP. Op productie kun je hier de SURFconext demo SP voor gebruiken die je zelf kunt koppelen via het IdP Dashboard.

Wanneer is mijn regel actief?

SURF krijgt een signaal zodra er een eerste regel bij een Service Provider wordt aangemaakt; die wordt door SURF bekeken en handmatig geactiveerd. Zodra er eenmaal een regel is bij een SP, b.v. omdat een andere instelling een regel bij die SP heeft aangemaakt, zal elke volgende regel voor die SP direct actief worden zodra je die regel zelf activeert. Maar om performance-redenen staat het autorisatieregel-management-systeem los van het deel van SURFconext dat de inlog-acties afhandelt. Elke 2 minuten wordt er bekeken of er wijzigingen op autorisatieregels zijn en worden die ververst. Dus maximaal 2 minuten nadat je een regel aan hebt gemaakt of gewijzigd is die actief.

Wat zijn de achterliggende technologie en standaarden?

De 'rijke autorisatie'-functie, zoals SURF dat noemt, is gebaseerd op de XACML-standaard. Op Wikipedia is meer informatie over XACML beschikbaar. SURF heeft kunnen voortbouwen op het werk van OpenAZ, open source gepubliceerde software om XACML-regels af te handelen; dat betekende dat SURF minder kosten had en alleen hoefde te zorgen dat de software aansloot op SURFconext, en er een beheer-portal kwam voor het maken van XACML-policies ('toegangs-regels'). SURF heeft de door haar ontwikkelde software open source beschikbaar gesteld in de OpenConext-bibliotheek.

XACML onderscheidt 4 functionele componenten:

- de PAP: Policy Administration Point, waar je de autorisatieregels beheert
- de PIP: Policy Information Point, een punt waar informatie wordt verkregen die belangrijk is voor het besluit om wel/niet toegang te geven
- de PDP: Policy Decision Point, de module die beslist of toegang moet worden verleend of niet (de portier)
- de PEP: Policy Enforcement Point, de module die daadwerkelijk zorgt dat een gebruiker wel of geen toegang krijgt (het hek)