

# Autorisatie rollen beheren

## *Handleiding en autorisatiemodel*

Auteur: SURFnet

Versie: 3.8

Datum: December 2018

## Inhoudsopgave

<b>1</b>	<b>Inleiding .....</b>	<b>3</b>
<b>2</b>	<b>Filosofie autorisatiemodel .....</b>	<b>4</b>
2.1	Principe .....	4
2.2	Consequenties .....	4
<b>3</b>	<b>Het autorisatiemodel.....</b>	<b>5</b>
3.1	Diensten .....	5
3.2	Autorisatie rollen.....	5
<b>4</b>	<b>SURFnet Autorisatie Beheer .....</b>	<b>8</b>
4.1	Inleiding .....	8
4.2	Inloggen.....	8
4.3	Autorisatie rollen toekennen.....	10
4.4	Uitnodiging opnieuw versturen.....	11
4.5	Autorisaties ontnemen .....	13
<b>5</b>	<b>Een Onegini-account aanmaken .....</b>	<b>14</b>
5.1	Inleiding .....	14
5.2	Onegini-account aanmaken via een social account.....	14
5.3	Onegini-account aanmaken zonder social account .....	16
<b>Bijlage I</b>	<b>Autorisatiematrix .....</b>	<b>19</b>



# 1 Inleiding

SURFnet levert aangesloten instellingen dienstverlening op het gebied van Netwerkinfrastructuur en Samenwerkingsinfrastructuur.

Een aantal van deze diensten is toegankelijk via een afgeschermd webinterface. SURFnet streeft ernaar deze diensten via single login toegankelijk te maken, door middel van federatieve authenticatie. Het is echter goed denkbaar dat de instelling de toegang tot bepaalde informatie die via de diensten van SURFnet te verkrijgen is, wil beperken. Het kan bijvoorbeeld gaan om (potentieel) gevoelige informatie van de instelling of zelfs van een individueel persoon.

SURFnet biedt instellingen daarom de mogelijkheid om op eenvoudige wijze delen van de SURFnet-dienstverlening alleen beschikbaar te stellen aan door de instelling aangewezen personen. Dit gebeurt in de vorm van **autorisatie rollen**.

De toegang tot dienstverlening en/of gevoelige informatie wordt verleend via een authenticatie- en autorisatiemodel. Hierin heeft SURFnet autorisatie rollen vastgelegd waaraan rechten zijn gekoppeld.

In dit document wordt het autorisatiemodel voor SURFnet dienstverlening uiteengezet (hoofdstuk 2 en 3). U leest ook hoe het toewijzen van rollen in zijn werk gaat, via de webapplicatie SURFnet Autorisatie Beheer (hoofdstuk 4). In Bijlage I vindt u de autorisatiematrix waarin per dienst is aangegeven welke rol welke bevoegdheid heeft.



**Let op:** het autorisatiemodel geldt alleen voor de SURFnet-diensten die via federatieve authenticatie toegankelijk zijn. In Bijlage I vindt u welke diensten dit zijn.

## 2 Filosofie autorisatiemodel

### 2.1 Principe

De filosofie achter het autorisatiemodel is om specifieke rechten te koppelen aan de specifieke **autorisatirol** van een persoon binnen een op SURFnet aangesloten instelling. Deze autorisatirol is geen rol in het kader van de gebruiksovereenkomst met SURFnet (zoals ICP, ICO, HDB dat wel zijn) maar een rol die de (mate van) toegang tot de SURFnet-dienstverlening bepaalt.

Via een autorisatirol heeft een persoon voor elke SURFnet-dienst een specifiek toegangsniveau. Bijvoorbeeld: de DNS-beheerder heeft toegang tot diensten gerelateerd aan DNS, zoals SURFdomijnen, maar geen toegang tot de beheerdersapplicatie behorende bij de map van eduroam. Deze is voorbehouden aan de persoon met de rol AAlverantwoordelijke. Heeft een gebruiker verschillende autorisatirollen, dan wordt bij het opstarten van een dienst het hoogste toegangsniveau toegekend dat voor hem of haar beschikbaar is.

Alle SURFnet-diensten kunnen gebruik maken van dezelfde set autorisatirollen. SURFnet bepaalt welke functionaliteiten van een SURFnet-dienst beschikbaar zijn voor een bepaalde rol.

De autorisatirollen worden uitgebreid beschreven in hoofdstuk 3 en in de matrix in de bijlage.

### 2.2 Consequenties

Toepassing van het autorisatiemodel en bijbehorende beheerapplicatie (zie hoofdstuk 4) heeft de volgende consequenties:

- Single sign-on: een gebruiker hoeft zich maar één keer aan te melden om toegang te hebben tot alle voor hem beschikbare SURFnet-diensten.
- De instelling kan zelf eenvoudig autorisatirollen toekennen aan het instellingsaccount van een persoon. Instellingen die nog niet over federatieve authenticatie beschikken, kunnen gebruik maken van gast-identityprovider Onegini. Voor het aanmaken van een Onegini-account zie hoofdstuk 5.
- Doordat rechten gekoppeld zijn aan autorisatirollen en niet aan personen, is het eenvoudig nieuwe diensten en nieuwe gebruikers op te nemen. Er hoeft niet voor elke nieuwe applicatie een autorisatiestructuur te worden opgesteld. Wel moeten SURFnet (als dienstverlener) en de instelling (als autorisator) rekening houden met toegangsniveaus zoals in dit document zijn beschreven wanneer bijvoorbeeld een nieuwe dienst wordt geïntroduceerd.

## 3 Het autorisatiemodel

### 3.1 Diensten

Het autorisatiemodel heeft betrekking op de SURFnet-diensten die opgenomen zijn in de autorisatiematrix in bijlage I. Deze lijst is afhankelijk van het dienstenportfolio van SURFnet, en daarom aan verandering onderhevig.

### 3.2 Autorisatie rollen

Het autorisatiemodel onderscheidt de volgende rollen:

- A. Instellingsbevoegde
- B. Beveiligingsverantwoordelijke
- C. AAIverantwoordelijke
- D. Operationeel beheerder
- E. Mailverantwoordelijke
- F. Domeinnamenverantwoordelijke
- G. Infraverantwoordelijke
- H. Infrabeheerder
- I. DNS-beheerder
- J. SURFconext-beheerder
- K. SURFconext-verantwoordelijke
- L. SURFdrive-beheerder
- M. SURFdrive-verantwoordelijke
- N. SURFwireless-beheerder
- O. Coördinerend SURF Contactpersoon
- P. SURFopzichter-beheerder

Deze lijst kan worden uitgebreid. De instelling is verantwoordelijk voor het koppelen van rollen aan gebruikersaccounts (zie hoofdstuk 4).

#### A. Instellingsbevoegde

De Instellingsbevoegde mag accounts en autorisatie rollen opvoeren in de applicatie SURFnet Autorisatie Beheer (<https://sab.surfnet.nl>), waarmee gebruikers toegang kunnen krijgen tot de SURFnet-dienstverlening. De Instellingsbevoegde kan tevens een instelling abonneren op een SURFnet-dienst.

De autorisatie rol Instellingsbevoegde kan niet door de instelling worden toegekend. Het is de enige autorisatie rol die door SURFnet aan een persoon wordt toegewezen. Als default is voor elke instelling de ICP (instellingscontactpersoon) aangewezen als Instellingsbevoegde. De ICP is namelijk, via de SURFnet Gebruiksovereenkomst, door de instelling gemachtigd als verantwoordelijke voor het toekennen van autorisatie rollen.

De ICP kan het verstrekken (en ontnemen) van autorisaties delegeren aan een collega. Deze persoon moet dan als BVI worden geregistreerd bij SURFnet en krijgt dan ook de rol van Instellingsbevoegde.

Via de tegel **Wijzigen Contactpersonen** in SURFdashboard (<https://dashboard.surfnet.nl>) kunt u nieuwe personen doorgeven die voor die rol in aanmerking komen.

## **B. Beveiligingsverantwoordelijke**

De Beveiligingsverantwoordelijke heeft toegang tot de SURFnet-dienstverlening op het gebied van beveiliging van het instellingsnetwerk en de waarborging van de privacy van de gebruikers. Hij kan beveiliging gerelateerde diensten inzien en configureren.

## **C. AAlverantwoordelijke**

De AAlverantwoordelijke (Autorisatie en Authenticatie Infrastructuur verantwoordelijke) is primair verantwoordelijk voor diensten zoals eduroam en SURFcertificaten.

## **D. Operationeel beheerder**

De Operationeel beheerder heeft basistoegang tot SURFnet-diensten en/of hun status.

## **E. Mailverantwoordelijke**

De Mailverantwoordelijke heeft volledige toegang tot de webinterface van SURFmailfilter.

## **F. Domeinnamenverantwoordelijke**

De Domeinnamenverantwoordelijke kan domeinnamen voor de instelling aanvragen plus alles wat daaraan gerelateerd is.

## **G. Infraverantwoordelijke**

De Infraverantwoordelijke is verantwoordelijk voor lichtpaden, SURFinternet-aansluiting en andere netwerkinfrastructuur-gerelateerde diensten en de koppelingen met SURFnet-resources. Hij kan via de diensten Bandwidth on Demand en het SURFnet-netwerk Dashboard zonder tussenkomst van SURFnet nieuwe lichtpaden activeren op de bestaande Multi Service -Poorten (MSPs) van de instelling.

## **H. Infrabeheerder**

De Infrabeheerder is verantwoordelijk voor het technisch beheer van lichtpaden, SURFinternet-aansluiting en andere netwerkinfrastructuur-gerelateerde diensten aan de kant van de instelling. Hij is bevoegd om de bij SURFnet afgenomen resources op het SURFnet-netwerk Dashboard in te zien. Hij is echter niet bevoegd om wijzigingen aan te brengen (zoals zelf lichtpaden opzetten op een Multi Service Port (MSP)). In het SURFnet-netwerk Dashboard kan hij storingen melden en feedback geven.

## **I. DNS-beheerder**

De DNS-beheerder krijgt toegang tot SURFdomeinen om de configuratie van het Domain Name System voor de instelling te regelen.

## **J. SURFconext-beheerder**

De SURFconext-beheerder heeft toegang tot het dashboard van SURFconext maar kan hier geen wijzigingen in aanbrengen.

## **K. SURFconext-verantwoordelijke**

De SURFconext-verantwoordelijke is de persoon binnen de instelling met de bevoegdheid om attributen vrij te geven en kan via het dashboard van SURFconext diensten van Service Providers aan- en uitzetten voor zijn of haar instelling.

#### **L. SURFdrive-beheerder**

De SURFdrive-beheerder heeft toegang tot het managementportal van SURFdrive, maar kan hier geen wijzigingen in aanbrengen.

#### **M. SURFdrive-verantwoordelijke**

De SURFdrive-verantwoordelijke is de persoon binnen de instelling met de bevoegdheid om gebruikers en hun data te verwijderen voor zijn of haar instelling.

#### **N. SURFwireless-beheerder**

De SURFwireless-beheerder heeft toegang tot het SURFwireless portal en tot Hivemanager (de wifi-beheeromgeving), maar kan hier geen wijzigingen in aanbrengen.

#### **O. Algemeen Contactpersoon SURF**

De rol Algemeen Contactpersoon SURF geeft toegang tot SURFdashboard en SURFrapportage en geeft inzicht in de status en rapportages van de verschillende diensten, maar kan hier geen wijzigingen in aanbrengen.

#### **P. SURFopzichter-beheerder**

De SURFopzichter-beheerder heeft toegang tot de dienst SURFopzichter en kan wijzigingen aanbrengen aan de configuratie.


## 4 SURFnet Autorisatie Beheer

### 4.1 Inleiding

Via de webapplicatie SURFnet Autorisatie Beheer kunnen instellingen zelf gebruikers uitnodigen en autorisatie rollen toekennen.

SURFnet Autorisatie Beheer is uitsluitend toegankelijk voor accounts met de autorisatie rol Instellingsbevoegde (ICP's of BVI's van de instellingen). Zie paragraaf 3.2 voor meer informatie over deze autorisatie rol.

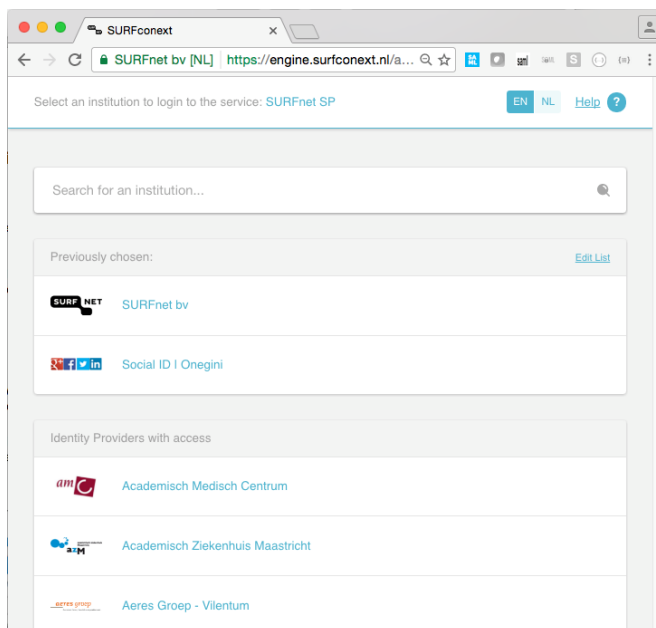
### 4.2 Inloggen

1. Ga naar SURFnet Autorisatie Beheer via <https://sab.surfnet.nl>. Vanuit SURFdashboard: klik op de tegel **Algemeen**, klik op  en kies **Autorisaties beheren**.
2. De startpagina verschijnt. Klik daarin op **Inloggen**.



**Let op** het is mogelijk dat u het vinkje **Sla deze pagina voortaan over** ooit hebt aangeklikt. U gaat in die gevallen direct naar de volgende stap.

De volgende pagina verschijnt:



3. Selecteer uw instelling door op het logo te klikken. Als uw instelling er niet bij staat, dan heeft uw instelling waarschijnlijk nog geen federatieve authenticatie. U kunt dan Onegini gebruiken. Deze staat ook in de lijst (Social ID | Onegini).



**Tip** Als u de naam of de afkorting van uw instelling invoert, wordt uw instelling direct zichtbaar.  
**Tip** Als u al een keer ingelogd hebt, dan wordt uw instelling bij **Onze suggestie** getoond. Klik op het logo van uw instelling en u gaat direct naar de inlogpagina van uw instelling.



**Tip** Staat uw instelling er niet bij maar heeft zij wel federatieve authenticatie, mail dan naar [dashboard-beheer@surfnet.nl](mailto:dashboard-beheer@surfnet.nl)

4. De inlogpagina van uw instelling of van Onegini verschijnt. Vul uw inloggegevens in.

**Tip** Controleer altijd de URL van deze pagina. Als uw inlogt via uw instelling, moet deze het formaat 'https://xxx.<domeinvanuwinstelling>.nl/xxxx' hebben

De volgende pagina verschijnt:

5. U ontvangt een sms met een eenmalig wachtwoord op uw mobiele telefoon. Voer het wachtwoord in en klik op **Login**.
6. U wordt nu automatisch doorgestuurd naar de pagina waar u de gewenste taak kunt uitvoeren.

**Let op** Hebt u problemen met uw instellingsaccount, neem dan contact op met de technisch beheerder van uw instelling. SURFnet heeft geen kennis van deze accounts en kan u hiermee dan ook niet helpen. Wilt u weten wie de technisch beheerder is, mail dan naar [dashboard-beheer@surfnet.nl](mailto:dashboard-beheer@surfnet.nl).

**Tip** bent u eenmaal ingelogd, dan hoeft u niet opnieuw in te loggen, tenzij u uw browser afsluit.

### 4.3 Autorisatie rollen toekennen

Na inloggen verschijnt het de overzichtspagina met alle autorisatieprofielen die u al hebt toegekend.

**SURF** NET SURFnet Autorisaties Beheer


Monday 15 October 2012

PROFIELEN **Nieuwe uitnodiging**

Search:

id	Naam	Rollen	Account
11	[Redacted]	AA-verantwoordelijke DNS-Beheerder Beveiligingsverantwoordelijke Domeinnamenverantwoordelijke Mailverantwoordelijke OperationeelBeheerder Infra-verantwoordelijke Instellingsbevoegde	[Redacted]
448	[Redacted]	Instellingsbevoegde AA-verantwoordelijke	[Redacted]

SURFnet bv | Postbus 190-35, 3501 DA Utrecht | T +31 302 305 305 | F +31 302 305 329 | [admin@surfnet.nl](mailto:admin@surfnet.nl)

1. Klik op **Nieuwe uitnodiging** als de persoon die u autorisaties wilt toekennen nog geen profiel heeft. Als de persoon al een profiel heeft, klik dan op  achter de naam.

Maakt u een nieuw profiel aan, dan verschijnt de volgende pagina:

**SURF** NET SURFnet Autorisaties Beheer

Monday 15 October 2012

**AUTORISATIEPROFIEL AANMAKEN** **TOELICHTING**

**Personalia**

Voornaam:

Achternaam:

**Account**

Autorisatieprofielen dienen door gebruikers zelf gekoppeld te worden aan een federatief instellingsaccount of een SURFguest account. Geef een e-mail adres waar een uitnodiging naar toe kan worden gestuurd. Uitnodigingen blijven 2 weken geldig.

Uitnodiging naar:

Status: **Nieuwe Uitnodiging**

**Step-up authenticatie**

Afhankelijk van het door de gebruiker gekoppelde account kan SURFnet voor enkele toepassingen een extra controle verlangen van de identiteit (zie het document autorisatiemodel). Gebruikers krijgen, als zij zo'n toepassing willen gebruiken, na inloggen een extra eenmalig wachtwoord via SMS. Geef optioneel een persoonlijk mobielnummer waarop deze persoon een SMS met een eenmalig password kan ontvangen.

Mobiel nummer:

**Autorisatie rollen**

☐ AA-verantwoordelijke ☐ Beveiligingsverantwoordelijke

☐ DNS-Beheerder ☐ Domeinnamenverantwoordelijke

☐ Mailverantwoordelijke ☐ OperationeelBeheerder

☐ Infra-verantwoordelijke

**Annuleren** **Uitnodigen**

Wilt u meer weten over SURFnet autorisatie rollen en deze applicatie? In [dit document \(pdf\)](#) vindt u meer informatie.

Heeft u vragen? Neem dan contact op met [AA@surfnet.nl](mailto:AA@surfnet.nl). Wij beantwoorden uw vragen zo snel mogelijk.

De pagina voor een bestaand profiel heeft ingevulde velden en ziet er onder **Account** iets anders uit.

2. Vul dit formulier volledig in.

- **Uitnodiging naar:** e-mailadres van de persoon die u wilt autoriseren. Als uw instelling nog geen federatieve authenticatie heeft, dan moet dit e-mailadres gelijk zijn aan het adres waarop het Onegini-account is geregistreerd
- **Mobiel nummer:** alleen nodig als deze persoon een taak moet uitvoeren die tweefactorauthenticatie vereist.
- **Autorisatie rollen:** vink hier de gewenste rollen aan.

3. Klik op **Uitnodigen**.

De overzichtspagina met profielen verschijnt weer. Bij het in de vorige stappen aangemaakte of gewijzigde account staat in de kolom **Account** 'Account nog niet gekoppeld'.

Het systeem heeft nu een e-mail verzonden naar het opgegeven adres. In deze e-mail staat een link die twee weken geldig is. Als de gebruiker op deze link klikt, kan hij zijn autorisatieprofiel koppelen aan zijn instellingsaccount of aan een Onegini-account.


#### 4.4 Uitnodiging opnieuw versturen


Een uitnodiging om een autorisatieprofiel te koppelen aan een federatief account blijft twee weken geldig. Als de gebruiker dit niet binnen twee weken doet, kunt u:

- een nieuwe uitnodiging sturen naar hetzelfde e-mailadres;
- een nieuwe uitnodiging sturen naar een ander adres.

In beide gevallen begint u in de overzichtspagina van autorisatieprofielen, dat verschijnt na inloggen (zie paragraaf 4.2). Het autorisatieprofiel van de persoon staat hierbij. In de kolom **Account** staat 'Account niet gekoppeld'.

## Nieuwe uitnodiging naar hetzelfde adres sturen

1. Klik op  achter het account. De volgende pagina verschijnt:



# SURFnet Autorisaties Beheer

Monday 15 October 2012

### AUTORISATIEPROFIEL WIJZIGEN

**Personalia**

Voornaam:

Achternaam:

**Account**

Autorisatieprofielen dienen door gebruikers zelf gekoppeld te worden aan een federatief instellingsaccount of een SURFguest account. Geef een e-mail adres waar een uitnodiging naar toe kan worden gestuurd. Uitnodigingen blijven 2 weken geldig.

Uitnodiging naar:

Status: Account nog niet gekoppeld

**Herzenden**

**Step-up authenticatie**

Afhankelijk van het door de gebruiker gekoppelde account kan SURFnet voor enkele toepassingen een extra controle verlangen van de identiteit (zie het document autorisatiemodel). Gebruikers krijgen, als zij zo'n toepassing willen gebruiken, na inloggen een extra eenmalig wachtwoord via SMS. Geef optioneel een persoonlijk mobielnummer waarop deze persoon een SMS met een eenmalig wachtwoord kan ontvangen.

Mobiel nummer:

**Autorisatie rollen**

<input type="checkbox"/> AA-verantwoordelijke	<input type="checkbox"/> Beveiligingsverantwoordelijke
<input type="checkbox"/> DNS-Beheerder	<input type="checkbox"/> Domeinnamenverantwoordelijke
<input type="checkbox"/> Mailverantwoordelijke	<input checked="" type="checkbox"/> Operationeel Beheerder
<input type="checkbox"/> Infra-verantwoordelijke	

**Annuleren** **Bewaren**

Wilt u meer weten over SURFnet autorisatie rollen en deze applicatie? In [dit document \(pdf\)](#) vindt u meer informatie.


Heeft u vragen? Neem dan contact op

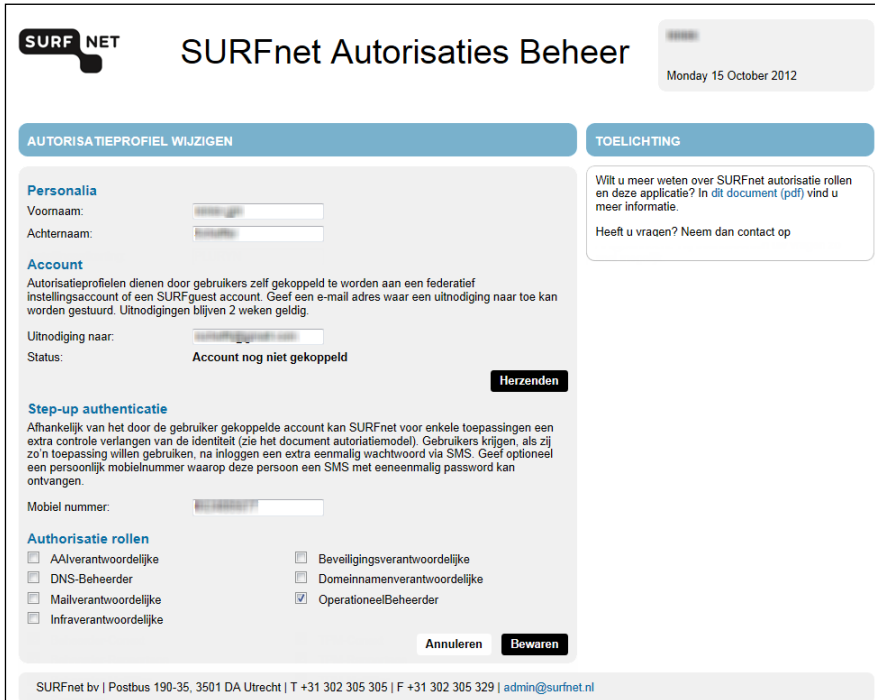
SURFnet bv | Postbus 190-35, 3501 DA Utrecht | T +31 302 305 305 | F +31 302 305 329 | [admin@surfnet.nl](mailto:admin@surfnet.nl)

2. Klik op **Herzenden**.

Een melding verschijnt dat de uitnodiging opnieuw is verzonden. De persoon ontvangt onmiddellijk deze nieuwe uitnodiging.

## Nieuwe uitnodiging naar ander adres sturen

1. Klik op  achter het account. De volgende pagina verschijnt:



**SURF** NET **SURFnet Autorisaties Beheer** Monday 15 October 2012

**AUTORISATIEPROFIEL WIJZIGEN** **TOELICHTING**

**Personalia**  
 Voornaam:   
 Achternaam:

**Account**  
 Autorisatieprofielen dienen door gebruikers zelf gekoppeld te worden aan een federatief instellingsaccount of een SURFguest account. Geef een e-mail adres waar een uitnodiging naar toe kan worden gestuurd. Uitnodigingen blijven 2 weken geldig.  
 Uitnodiging naar:   
 Status: Account nog niet gekoppeld **Herzenden**

**Step-up authenticatie**  
 Afhankelijk van het door de gebruiker gekoppelde account kan SURFnet voor enkele toepassingen een extra controle verlangen van de identiteit (zie het document [autorisatiemodel](#)). Gebruikers krijgen, als zij zo'n toepassing willen gebruiken, na inloggen een extra eenmalig wachtwoord via SMS. Geef optioneel een persoonlijk mobielnummer waarop deze persoon een SMS met een eenmalig wachtwoord kan ontvangen.  
 Mobiel nummer:

**Authorisatie rollen**

<input type="checkbox"/> AA-verantwoordelijke	<input type="checkbox"/> Beveiligingsverantwoordelijke
<input type="checkbox"/> DNS-Beheerder	<input type="checkbox"/> Domeinnamenverantwoordelijke
<input type="checkbox"/> Mailverantwoordelijke	<input checked="" type="checkbox"/> Operationeel Beheerder
<input type="checkbox"/> Infra-verantwoordelijke	

**Annuleren** **Bewaren**


SURFnet bv | Postbus 190-35, 3501 DA Utrecht | T +31 302 305 305 | F +31 302 305 329 | [admin@surfnet.nl](mailto:admin@surfnet.nl)

2. Wijzig het e-mailadres in het juiste adres.
3. Klik op **Bewaren**.

De uitnodiging wordt verzonden naar het nieuwe adres.

## 4.5 Autorisaties ontnemen

U kunt autorisatieprofielen verwijderen door alle rollen van een persoon te ontnemen. Het profiel wordt dan automatisch uit het systeem verwijderd.

1. Log in zoals beschreven in paragraaf 4.2.
2. Klik op de overzichtspagina met profielen op  achter het profiel waarvan u de autorisaties wilt ontnemen.
3. Vink de autorisatie rollen uit en klik op **Bewaren**.

## 5 Een Onegini-account aanmaken

### 5.1 Inleiding

Als uw instelling geen federatieve authenticatie heeft, kunt u gebruik maken van een Onegini-account om in te loggen op SURFnet Autorisatie Beheer. Bij het aanmaken van een Onegini-account hebt u twee opties:

1. U maakt een Onegini-account aan waarmee u inlogt via een bestaand social account (Facebook, Twitter, LinkedIn, Microsoft, Google). U hoeft daardoor geen aparte gebruikersnaam en wachtwoord meer te onthouden (zie paragraaf 5.2).
2. U maakt een Onegini-account aan waarmee u inlogt via een nieuw aan te maken gebruikersnaam en wachtwoord (zie paragraaf 5.3).



**Tip** Hebt u na het lezen van dit hoofdstuk nog vragen over Onegini, lees dan de FAQ: <https://wiki.surfnet.nl/display/conextsupport/Onegini>.

### 5.2 Onegini-account aanmaken via een social account

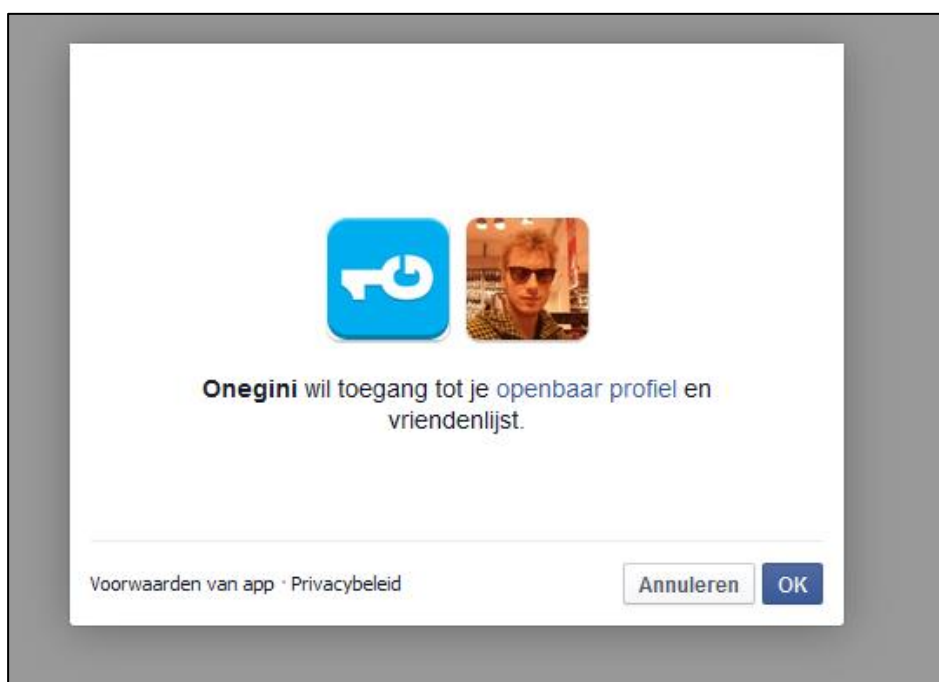
1. Ga naar <https://www.onegini.me/>



2. Klik op het social account waarmee u wilt inloggen (van links naar rechts: Facebook, Google, LinkedIn, Microsoft, Twitter).

De loginpagina van het gekozen account verschijnt, in onderstaand voorbeeld de loginpagina van Facebook.

3. Log in op het gekozen account.  
U ziet nu tot welke gegevens Onegini toegang krijgt.



4. Klik op **OK**.

**onegini** English

**Vul uw informatie in om uw identiteit aan te maken**

**Algemeen**

Voornaam \*

Achternaam \*

E-mailadres \*

Mobiele nummer \* Nederland

**Gebruiksvoorwaarden**

☐ Ik ga akkoord met de [gebruiksvoorwaarden](#). \*

\* is een verplicht veld

**Aanmaken**

5. Vul uw gegevens in en klik op **Aanmaken** om uw Onegini-account aan te maken.



**Let op** Hier moet u het e-mailadres invullen waarop u de uitnodiging voor autorisatie van SURFnet-diensten ontvangen hebt.

Vanaf nu gebruikt u de gebruikersnaam en wachtwoord van het gekozen social account om in te loggen op SURFnet Autorisatie Beheer.



**Tip** U kunt meerdere social accounts koppelen aan uw Onegini-account.

### 5.3 Onegini-account aanmaken zonder social account

1. Ga naar <https://www.onegini.me/>.





2. Klik op **hier** (in “Klik **hier** als u de voorkeur heeft om niet een account van een derde partij te gebruiken”).

E-mailadres \*

Wachtwoord \*

**Inloggen** [Wachtwoord vergeten?](#)

OF

Als u nieuw bent bij Onegini

**Registreer hier**

U kunt ook [een ander account gebruiken om in te loggen](#)

3. Klik op **Registreer hier**.



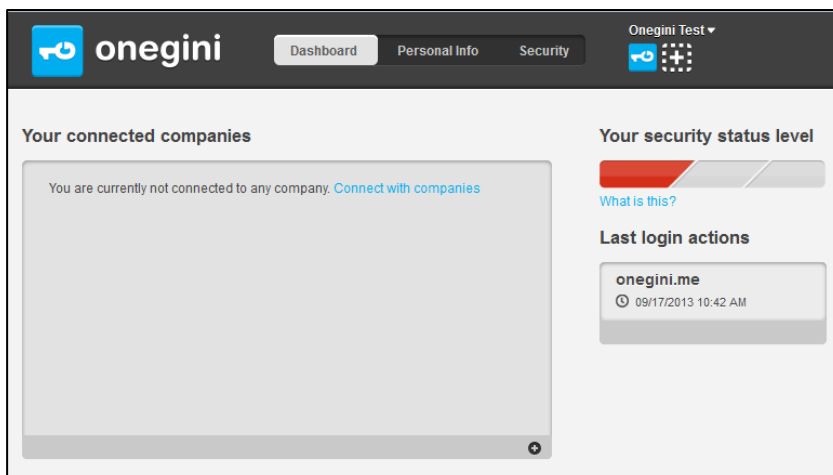
The screenshot shows the Onegini account creation interface. At the top, there is a header with the Onegini logo and the word 'English'. Below the header, the main heading reads 'Vul uw informatie in om uw identiteit aan te maken'. The form is divided into three sections: 'Algemeen' (General), 'Inloggegevens' (Login details), and 'Gebruiksvoorwaarden' (Terms of use). In the 'Algemeen' section, there are input fields for 'Voornaam \*', 'Achternaam \*', and 'Mobiele nummer \*' (which includes a dropdown for country code, currently showing 'Nederland', and a field for the number starting with '+31'). The 'Inloggegevens' section contains fields for 'E-mailadres \*', 'Wachtwoord \*', and 'Bevestig wachtwoord \*'. The 'Gebruiksvoorwaarden' section has a checkbox labeled 'Ik ga akkoord met de [gebruiksvoorwaarden](#). \*'. A note at the bottom left states '\* is een verplicht veld'. A blue 'Aanmaken' button is located at the bottom right.

4. Vul uw gegevens in en klik op **Aanmaken** om uw Onegini-account te maken.



**Let op** Hier moet u het e-mailadres invullen waarop u de uitnodiging voor autorisatie van SURFnet-diensten ontvangen hebt.

Als uw account succesvol is aangemaakt, verschijnt dit venster:



The screenshot shows the Onegini dashboard after a successful account creation. The header includes the Onegini logo, navigation tabs for 'Dashboard', 'Personal Info', and 'Security', and a user profile section labeled 'Onegini Test' with a dropdown arrow. The main content area is divided into two columns. The left column, titled 'Your connected companies', contains a message: 'You are currently not connected to any company. [Connect with companies](#)'. The right column contains two sections: 'Your security status level' with a red progress bar and a link 'What is this?', and 'Last login actions' which shows a single entry for 'onegini.me' with a timestamp '09/17/2013 10:42 AM'.

U logt vanaf nu in op SURFnet Autorisatie Beheer via de zojuist aangemaakte gebruikersnaam en wachtwoord.



**Tip** U kunt later alsnog een of meer social accounts koppelen aan uw Onegini-account.

## Bijlage I Autorisatiematrix

In onderstaande tabel is te zien welke autorisaties nodig zijn voor de online applicaties bij de SURFnet-diensten. Achter de dikke streep staat welk type account gebruikt kan worden.

Niet alle diensten zijn al ingericht conform het model. Zij gebruiken nog applicatiespecifieke autorisatie. Op SURFdashboard is te vinden hoe voor deze diensten autorisatie kan worden aangevraagd.

SURFnet-dienst	toepassing	(√ = wel toegang - = geen toegang)	Instellingsbevoegde	Beveiligingsverantwoordelijke	AAI verantwoordelijke	Operationeel beheerder	Mailverantwoordelijke	Domeinnamenverantwoordelijke	Infraverantwoordelijke	Infrabeheerder	DNS-beheerder	SURFconext-beheerder	SURFconext-verantwoordelijke	SURFdrive-beheerder	SURFdrive-verantwoordelijke	SURFwireless-beheerder	Algemeen Contactpersoon SURF	SURF opzichter-beheerder	Federatief ontsloten	Sterke authenticatie vereist	Applicatiespecifiek account
<b>SURFdashboard</b>																					
	Algemeen toegang		√	√	√	√	√	√	√	-	√	√	√	√	√	√	√	√	√	•	•
	Inzien dienstrapportages		√	√	√	√	√	√	√	-	√	√	√	√	√	√	√	√	√	•	•
	Aanvragen diensten		√	-	•	•	•	•	•	•	•	•	•	•	•	•	•	•	√	√	•
	Wijzigen contactpersoneninformatie		√	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	√	√	•

SURFnet-dienst toepassing (✓ = wel toegang - = geen toegang)	SURFnet-dienst																		
	Instellingsbevoegde	Beveiligingsverantwoordelijke	AAI verantwoordelijke	Operationeel beheerder	Mailverantwoordelijke	Domeinnamenverantwoordelijke	Infraverantwoordelijke	Infrabeheerder	DNS-beheerder	SURFconext-beheerder	SURFconext-verantwoordelijke	SURFdrive-beheerder	SURFdrive-verantwoordelijke	SURFwireless-beheerder	Algemeen Contactpersoon SURF	SURFopzichter-beheerder	Federatief ontsloten	Sterke authenticatie vereist	Applicatiespecifiek account
<b>SURFnet Autorisatie Beheer</b>																			
Autorisaties inzien	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	✓	✓	-
Accounts aanmaken	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	✓	✓	-
Autorisaties toekennen	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	✓	✓	-
<b>SURFinternet</b>																			
Gebruik van monitoring tools (SURFstat, Trafmon, SURF)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	-
Aanvragen nieuwe IPv6- en IPv4-ranges (via SURFdashboard)	✓	-	-	-	-	-	✓	-	-	-	-	-	-	-	-	-	✓	✓	-
Inzage verkeer per service (op SURFnet-netwerk Dashboard)	-	-	-	-	-	-	✓	✓	-	-	-	-	-	-	-	-	✓	-	-
<b>SURFinternetpinnen</b>	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt

SURFnet-dienst toepassing (√ = wel toegang - = geen toegang)	SURFnet-dienst													
	Applicatiespecifiek account	Sterke authenticatie vereist	Federatief ontsloten	SURFopzichter-beheerder	Algemeen Contactpersoon SURF	SURFwireless-beheerder	SURFdrive-verantwoordelijke	SURFdrive-beheerder	SURFconext-verantwoordelijke	SURFconext-beheerder	DNS-beheerder	Infrabeheerder	Infraverantwoordelijke	Domeinnamenverantwoordelijke
	Mailverantwoordelijke	Operationeel beheerder	AAI verantwoordelijke	Beveiligingsverantwoordelijke	Instellingsbevoegde									
<b>SURFlichtpaden</b>														
Online aanvragen offerte voor lichtpaden	•	√	√	•	•	•	•	•	•	•	•	•	•	•
On-demand lichtpadpoorten beheren	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Vrijgeven MSP-capaciteit aan gebruikers groepen in Bandwidth on Demand	•	•	√	•	•	•	•	•	•	•	•	•	•	•
Opzetten, bewerken en verwijderen on-demand lichtpaden via SURFnet-netwerk Dashboard	•	•	√	•	•	•	•	•	•	•	•	•	•	•
Inzien actueel en historisch verkeer op alle lichtpaden	•	•	√	•	•	•	•	•	•	•	•	•	•	•
Melden van storingen gerelateerd aan lichtpaden via het SURFnet-netwerk Dashboard dashboard	•	•	√	•	•	•	•	•	•	•	•	•	•	•

SURFnet-dienst toepassing (✓ = wel toegang - = geen toegang)																
	Applicatiespecifiek account	Sterke authenticatie vereist	Federatief ontsloten	SURFopzichter-beheerder	Algemeen Contactpersoon SURF	SURFwireless-beheerder	SURFdrive-verantwoordelijke	SURFdrive-beheerder	SURFconext-verantwoordelijke	SURFconext-beheerder	DNS-beheerder	Infrabeheerder	Infraverantwoordelijke	Domeinnamenverantwoordelijke	Mailverantwoordelijke	Operationeel beheerder
<b>SURFdomeinen</b>  Online technisch beheren nameserving records (reverse DNS, zones etc.)  Online aanvragen van domeinnamen en verhuizen domeinen	✓	✓	✓	-	-	-	-	-	-	-	✓	-	-	-	-	-
	✓	✓	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
<b>eduroam</b>  Beheren locatiehotspots op eduroam.nl  eduroam Visitor Access  eduroam Monitoring Service	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	✓	-
	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-

<b>SURFnet-dienst</b> toepassing (√ = wel toegang - = geen toegang)																			Applicatiespecifiek account
<b>SURFcertificaten</b>																			
Online aanvragen persoonsgebonden certificaten	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	√	-	-
Online aanvragen macro- en server-certificaten	-	-	-	-	-	-	-	nvt	-	-	-	-	-	-	-	-	-	-	√ <sup>1</sup>
<b>SURFteams</b>	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	√	-	-
<b>SURFconext</b>																			
Online aan- en afsluiten diensten van Service Providers	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	-	√	nvt	nvt	nvt	nvt	nvt	√	-	-
Overzicht beschikbare diensten via dashboard van SURFconext	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	√	√	nvt	nvt	nvt	nvt	nvt	√	-	-

<sup>1</sup> Authenticatie via een dongle welke door SURFnet wordt uitgereikt aan de door de instelling gemachtigde personen

SURFnet-dienst toepassing (√ = wel toegang - = geen toegang)	Instellingsbevoegde	Beveiligingsverantwoordelijke	AAI verantwoordelijke	Operationeel beheerder	Mailverantwoordelijke	Domeinnamenverantwoordelijke	Infraverantwoordelijke	Infrabeheerder	DNS-beheerder	SURFconext-beheerder	SURFconext-verantwoordelijke	SURFdrive-beheerder	SURFdrive-verantwoordelijke	SURFwireless-beheerder	Algemeen Contactpersoon SURF	SURFopzichter-beheerder	Federatief ontsloten	Sterke authenticatie vereist	Applicatiespecifiek account
<b>SURFmailfilter</b>																			
Configuratie eindgebruiker	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	√	-	√
Configuratie domein	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Online wijzigen van te filteren maildomeinen	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	√	-	√
<b>SURFopzichter</b>	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	√	√	-	-
<b>SURFdrive</b>																			
Overzicht gebruikers in managementportal	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	√	√	nvt	nvt	nvt	nvt	nvt	nvt
Verwijderen gebruikers en data in managementportal	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt	-	√	nvt	nvt	nvt	nvt	nvt	nvt



<b>SURFnet-dienst</b>  toepassing      (√ = wel toegang - = geen toegang)	Applicatiespecifiek account	nvt
	Sterke authenticatie vereist	nvt
	Federatief ontsloten	nvt
	SURFopzichter-beheerder	nvt
	Algemeen Contactpersoon SURF	nvt
	SURFwireless-beheerder	√
	SURFdrive-verantwoordelijke	nvt
	SURFdrive-beheerder	nvt
	SURFconext-verantwoordelijke	nvt
	SURFconext-beheerder	nvt
	DNS-beheerder	nvt
	Infrabeheerder	nvt
	Infraverantwoordelijke	nvt
<b>SURFwireless</b>  Toegang tot Hivemanager en de SURFwireless portal	Domeinnamenverantwoordelijke	nvt
	Mailverantwoordelijke	nvt
	Operationeel beheerder	nvt
	AAI verantwoordelijke	nvt
	Beveiligingsverantwoordelijke	nvt
	Instellingsbevoegde	nvt