

Handleiding

Persoonlijke certificaten met nCare web & app

Inhoud

Toelichting.....	3
Waar en hoe stel je dit in?.....	3
Methode voor code verzenden	4
Whitelisting	5
Hoe werkt het?.....	6
nCare account.....	7
Microsoft Azure/Office365 account	9
Google account.....	11

Toelichting

Ruim 50% van alle supportvragen gaat over het aanvragen, vernieuwen en intrekken van certificaten. Het kost organisaties veel tijd en beheer om dit goed te regelen. Daarnaast gaan veel vragen over het installeren van een certificaat. De huidige werkwijze is niet duidelijk voor een zorgmedewerker en oogt erg complex.

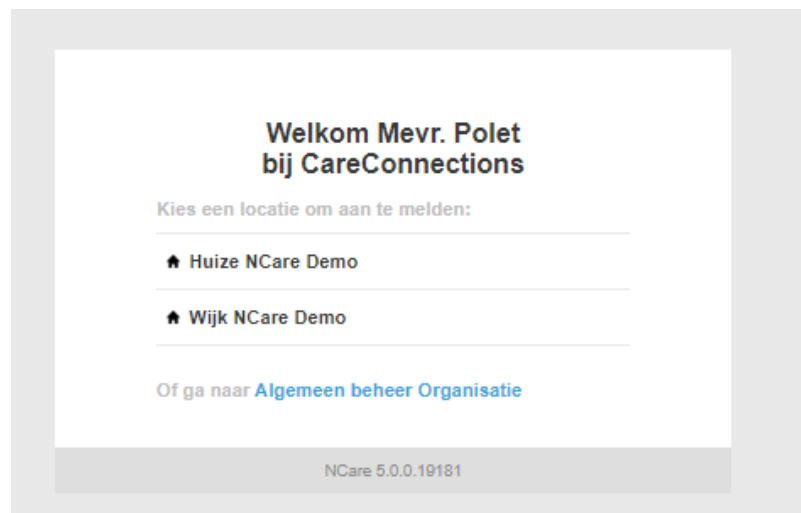
Daarom is er een verbeterde authenticatiemethode ontwikkeld die vrijwel geen beheer nodig heeft en eenvoudig is voor de gebruikers.

Waar en hoe stel je dit in?

Log in op nCare web. Druk op '[Aanpassen](#)' rechtsboven in het scherm:



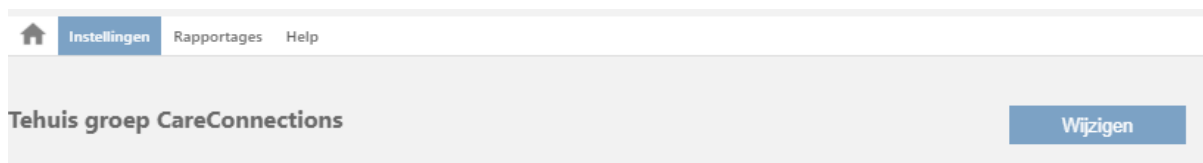
Je komt nu op het locatie-keuze scherm, kies voor '[Algemeen beheer Organisatie](#)'.



Ga vervolgens naar 'Instellingen' en dan naar 'Algemeen'



Kies hier voor 'Wijzigen' achter de **Tehuis groep**



Methode voor code verzenden

Bij 'Code versturen via' kan je op organisatie niveau instellen op welke wijze de code verzonden mag worden.

Je hebt de keuze uit:

- Mail
- SMS
- Authenticatie app

Je kan hier meerdere keuzes maken.

Wanneer je alleen voor SMS kiest, kunnen gebruikers de code alleen via SMS ontvangen.

Kies je hier voor SMS en MAIL dan heeft de gebruiker bij de eerste keer inloggen de keuze om de code via SMS of MAIL te ontvangen.

Dit zijn de enige acties die jij als beheerder voor de nieuwe authenticatie flow hoeft te doen.

Vanaf nu is het niet meer nodig om handmatig nieuwe certificaten aan te vragen of codes opnieuw te laten versturen wanneer deze kwijt zijn.

Whitelisting

Maakt jouw organisatie gebruik van whitelisting of wil jouw organisatie dit gaan gebruiken? Dan kan dat nu worden ingesteld in nCare zelf.

Wanneer nCare benaderd wordt vanaf een IP adres dat op de whitelist staat, zal en hoeft er geen persoonlijk certificaat worden geïnstalleerd.

IP adressen kan je op de whitelist zetten bij 'Algemeen Beheer Organisatie' > 'Algemeen' > 'Wijzigen'.

Heb je meerdere IP-adressen die je wilt whitelisten?

Dan zet je de IP-adressen onder elkaar zonder spaties of (punt)komma's om ze te scheiden, zoals in het voorbeeld hieronder.

Login zonder 2FA vanaf IP adressen:

```
1.2.3.4  
5.6.7.8
```

Optie: 7 dagen persoonlijk certificaat toestaan voor gebruiker

Wanneer er een vinkje wordt gezet bij '*Gebruikers toestaan persoonlijk certificaat te installeren voor 7 dagen*', dan krijgt de gebruiker de mogelijkheid om deze optie bij het inloggen aan te vinken.

Een gebruiker kan dan 7 dagen lang inloggen zonder nogmaals een code te moeten invoeren ter authenticatie.

(Verderop in deze handleiding wordt deze optie vanuit de gebruiker beschreven.)

Persoonlijke certificaten

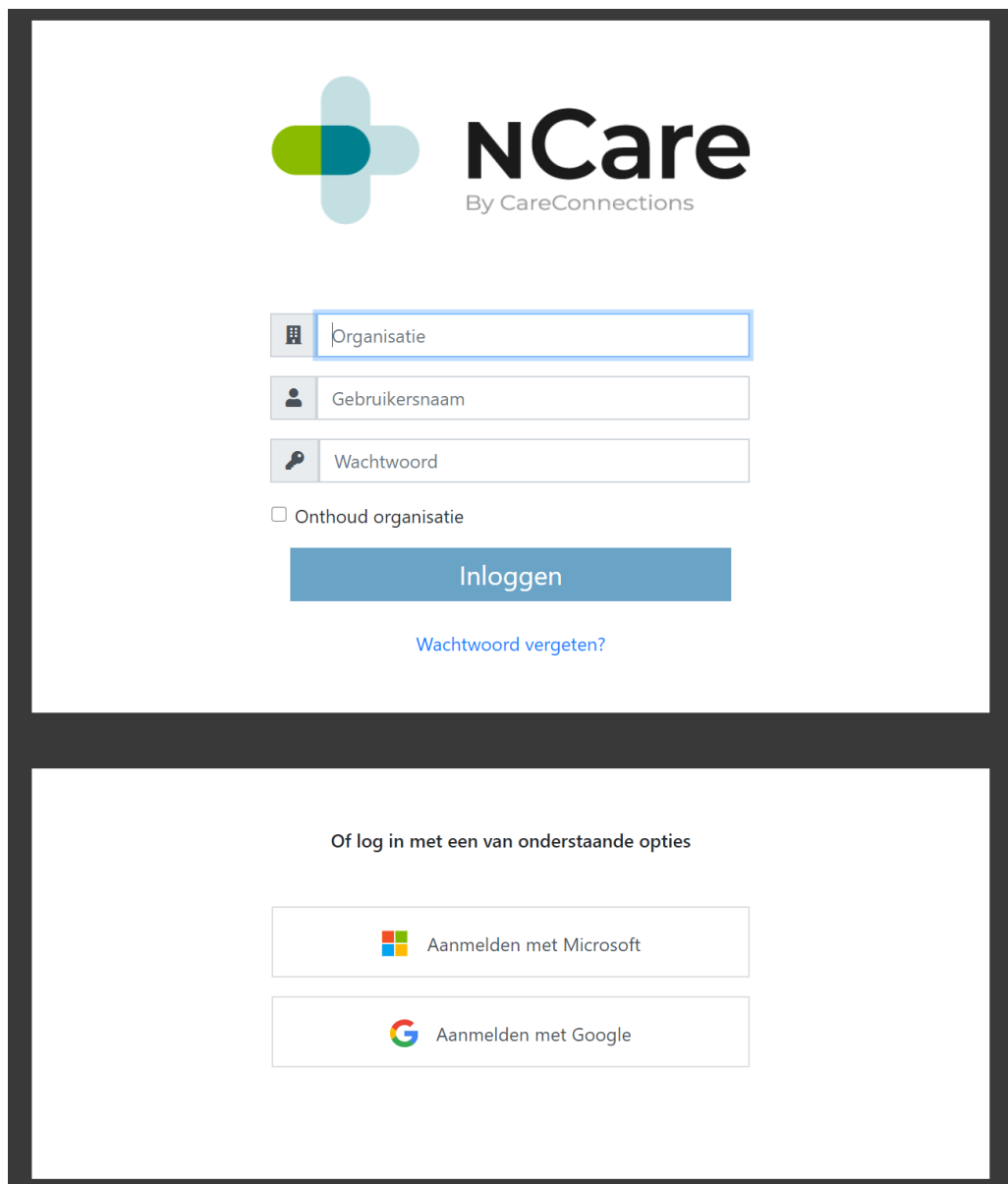
Gebruikers toestaan persoonlijk certificaat te installeren voor 7 dagen:

Annuleren

Opslaan

Hoe werkt het?

Wanneer een gebruiker de nCare app opent of naar nCare web gaat, zal het inlogscherm er zo uit zien:



The screenshot shows the nCare login interface. At the top left is the nCare logo, a stylized cross with green and blue segments, followed by the text 'nCare By CareConnections'. Below the logo are three input fields: 'Organisatie' (with a building icon), 'Gebruikersnaam' (with a person icon), and 'Wachtwoord' (with a key icon). There is a checkbox labeled 'Onthoud organisatie'. A blue 'Inloggen' button is positioned below the fields. A link 'Wachtwoord vergeten?' is located below the button. The bottom section of the screen is titled 'Of log in met een van onderstaande opties' and contains two buttons: 'Aanmelden met Microsoft' (with the Microsoft logo) and 'Aanmelden met Google' (with the Google logo).

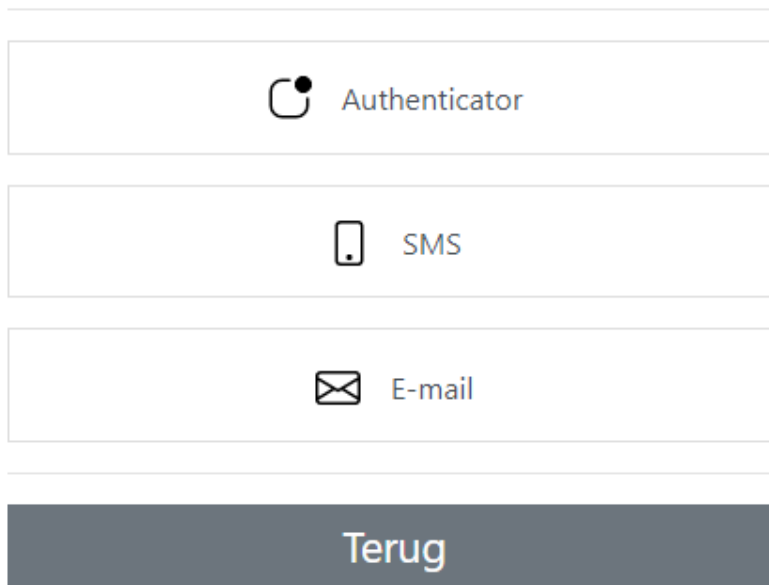
Je kan in dit scherm inloggen met de volgende accounts:

- nCare account
- Microsoft-account
- Google-account

nCare account

Na het inloggen met je nCare account krijg je onderstaand scherm te zien.

Kies de gewenste 2-factor methode.



The screenshot shows a selection screen for 2-factor authentication. It features three rectangular buttons stacked vertically, each with a small icon and a text label. The top button has a circular icon with a dot and is labeled 'Authenticator'. The middle button has a mobile phone icon and is labeled 'SMS'. The bottom button has an envelope icon and is labeled 'E-mail'. Below these buttons is a dark grey button with the white text 'Terug'.

De methode die je kiest bepaalt hoe en waar je de code op krijgt. Kies je voor SMS dan wordt voortaan de code gestuurd per SMS naar het mobiele nummer dat bekend is bij jouw nCare account.

Wanneer er geen mobiele nummer of mail adres bij jouw account bekend is kan je deze optie niet selecteren. Deze is dan uit gegrijsd.

Na het kiezen van een methode wordt de code verzonden en krijg je een scherm te zien waar je deze moet invullen.

Na het invullen van de code wordt op de achtergrond het persoonlijke certificaat geïnstalleerd.



Er is een verificatiecode verstuurd naar het mobiele nummer zoals vastgelegd bij je gebruikersgegevens. Geef hieronder de code die u heeft ontvangen om verder te kunnen gaan.

Token

Vertrouw dit apparaat voor 7 dagen

Terug

Inloggen

Wanneer er een vinkje wordt gezet bij 'Vertrouw dit apparaat voor 7 dagen' dan zal het certificaat 7 dagen geldig zijn.

Een gebruiker kan dan 7 dagen lang inloggen zonder nogmaals een code te moeten invoeren ter authenticatie.

Standaard staat dit vinkje aan in de app en uit in web.

Microsoft Azure/Office365 account

Alle organisaties die gebruik maken van Microsoft Azure en/of Office365 kunnen een SSO-koppeling leggen met nCare ([Zie documentatie SSO OpenId](#)).

Bij een SSO kan je kiezen om twee factor authenticatie via nCare te laten lopen of via Microsoft.

Verloopt twee factor authenticatie via Microsoft? Dan is onderstaande flow niet van toepassing.

Flow

Als gebruiker open ik de nCare app of ik ga naar nCare web.

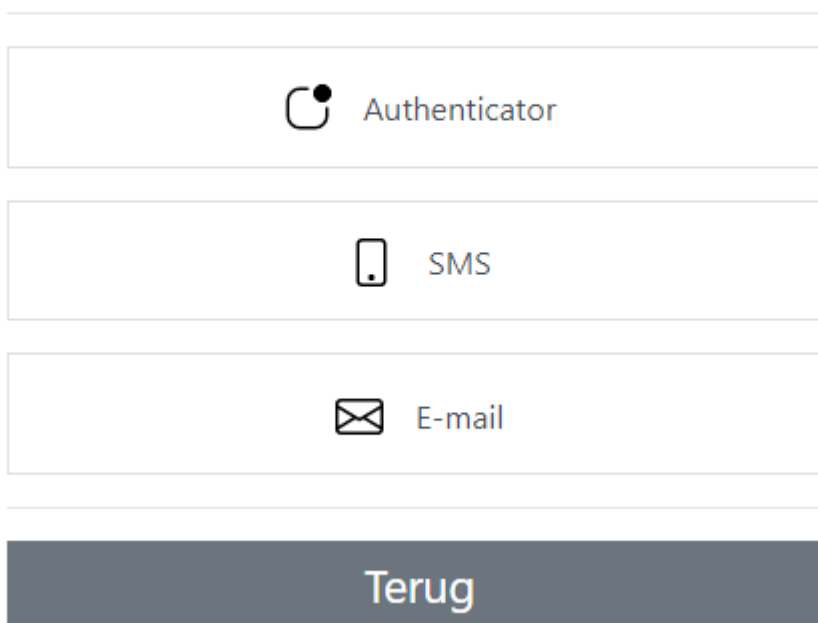
In het inlogscherf kies ik voor 'Aanmelden met Microsoft'

Ik vul hier mijn organisatie account: tom@organisatienaam.nl en het wachtwoord dat bij dit account hoort.

Wanneer alles is ingevuld kies ik voor 'Inloggen'

Wanneer is aangegeven om twee factor authenticatie via nCare te laten verlopen moet je bij je 1^e inlog een methode kiezen.

Kies de gewenste 2-factor methode.



The screenshot shows a selection screen for 2-factor authentication. It features three rectangular buttons stacked vertically, each with an icon and text. The top button has a circular icon with a dot and the text 'Authenticator'. The middle button has a mobile phone icon and the text 'SMS'. The bottom button has an envelope icon and the text 'E-mail'. Below these buttons is a dark grey button with the text 'Terug' in white.

De methode die je kiest bepaalt hoe en waar je de code op krijgt.

Kies je voor SMS dan wordt voortaan de code gestuurd per SMS naar het mobiele nummer dat bekend is bij jouw nCare account.

Wanneer er geen mobiele nummer of mail adres bij jouw account bekend is kan je deze optie niet selecteren. Deze is dan uit gegrijpsd.

Na het kiezen van een methode wordt de code verzonden en krijg je een scherm te zien waar je deze moet invullen.

Na het invullen van de code wordt op de achtergrond het persoonlijke certificaat geïnstalleerd.



Er is een verificatiecode verstuurd naar het mobiele nummer zoals vastgelegd bij je gebruikersgegevens. Geef hieronder de code die u heeft ontvangen om verder te kunnen gaan.

Token

Vertrouw dit apparaat voor 7 dagen

Terug

Inloggen

Wanneer er een vinkje wordt gezet bij 'Vertrouw dit apparaat voor 7 dagen' dan zal het certificaat 7 dagen geldig zijn.

Een gebruiker kan dan 7 dagen lang inloggen zonder nogmaals een code te moeten invoeren ter authenticatie.

Standaard staat dit vinkje aan in de app en uit in web.

Google account

Alle organisaties die gebruik maken van Google accounts kunnen een SSO-koppeling leggen met nCare ([Zie documentatie SSO OpenId](#)).

Bij een SSO kan je kiezen om twee factor authenticatie via nCare te laten lopen of via Google.

Verloopt twee factor authenticatie via Google? Dan is onderstaande flow niet van toepassing.

Flow

Als gebruiker open ik de nCare app of ik ga naar nCare web.

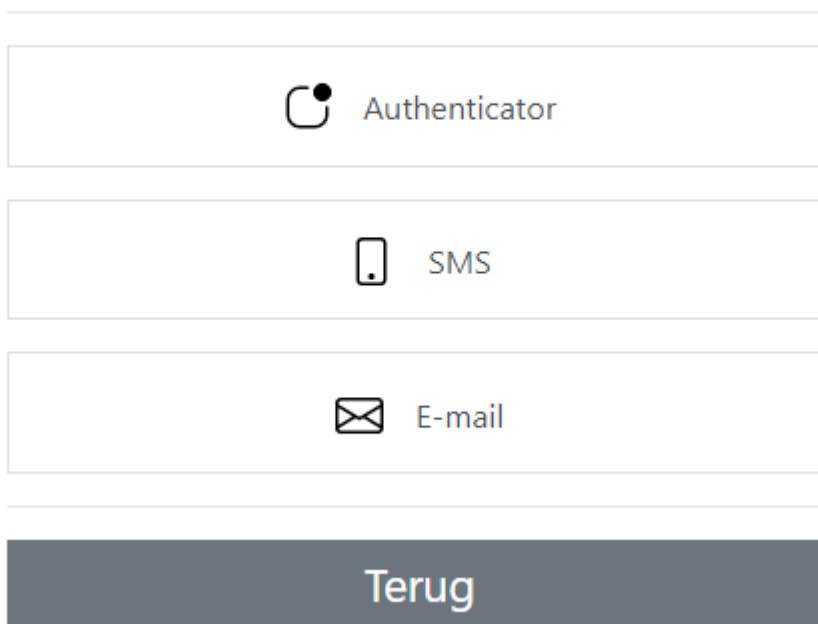
In het inlogscherf kies ik voor 'Aanmelden met Google'

Ik vul hier mijn organisatie account: tom@organisatienaam.nl en het wachtwoord dat bij dit account hoort.

Wanneer alles is ingevuld kies ik voor 'Inloggen'

Wanneer is aangegeven om twee factor authenticatie via nCare te laten verlopen moet je bij je 1^e inlog een methode kiezen.

Kies de gewenste 2-factor methode.



Authenticator

SMS

E-mail

Terug

De methode die je kiest bepaalt hoe en waar je de code op krijgt.

Kies je voor SMS dan wordt voortaan de code gestuurd per SMS naar het mobiele nummer dat bekend is bij jouw nCare account.

Wanneer er geen mobiele nummer of mail adres bij jouw account bekend is kan je deze optie niet selecteren. Deze is dan uit gegrijpsd.

Na het kiezen van een methode wordt de code verzonden en krijg je een scherm te zien waar je deze moet invullen.

Na het invullen van de code wordt op de achtergrond het persoonlijke certificaat geïnstalleerd.



Er is een verificatiecode verstuurd naar het mobiele nummer zoals vastgelegd bij je gebruikersgegevens. Geef hieronder de code die u heeft ontvangen om verder te kunnen gaan.

Token

Vertrouw dit apparaat voor 7 dagen

Terug

Inloggen

Wanneer er een vinkje wordt gezet bij 'Vertrouw dit apparaat voor 7 dagen' dan zal het certificaat 7 dagen geldig zijn.

Een gebruiker kan dan 7 dagen lang inloggen zonder nogmaals een code te moeten invoeren ter authenticatie.

Standaard staat dit vinkje aan in de app en uit in web.