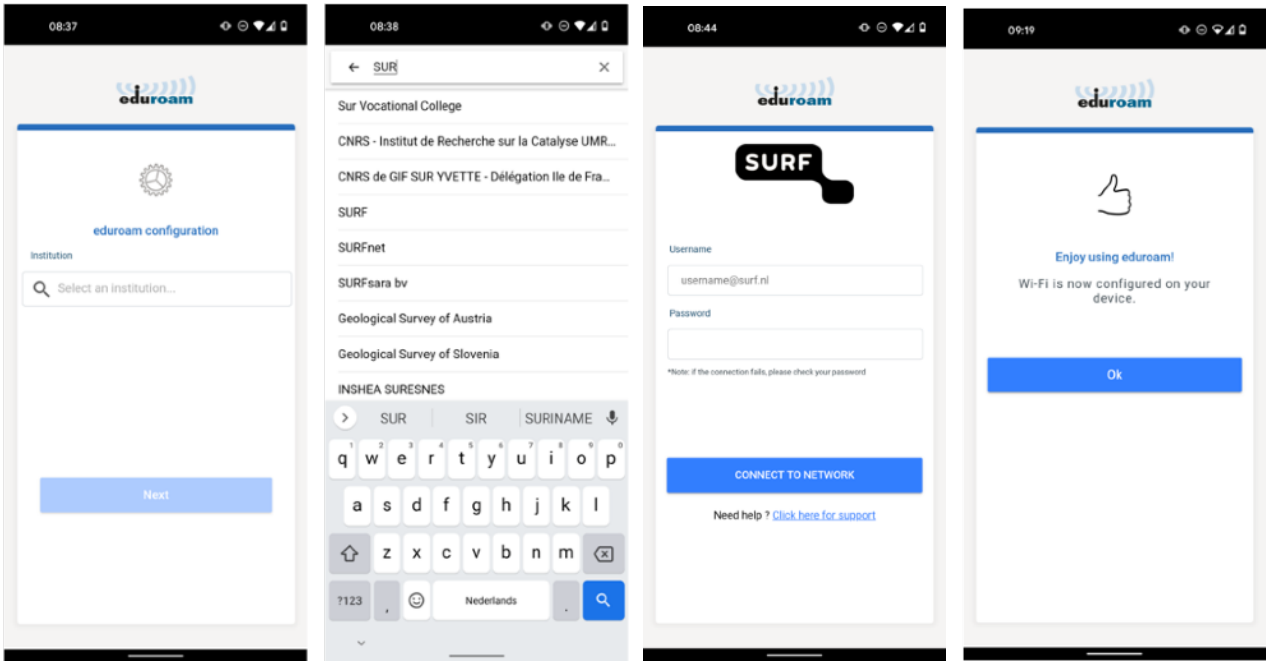
Werking van geteduroam

Voor eindgebruikers is geteduroam dé manier om eduroam op je apparaat te configureren op een gemakkelijke, juiste en veilige manier.

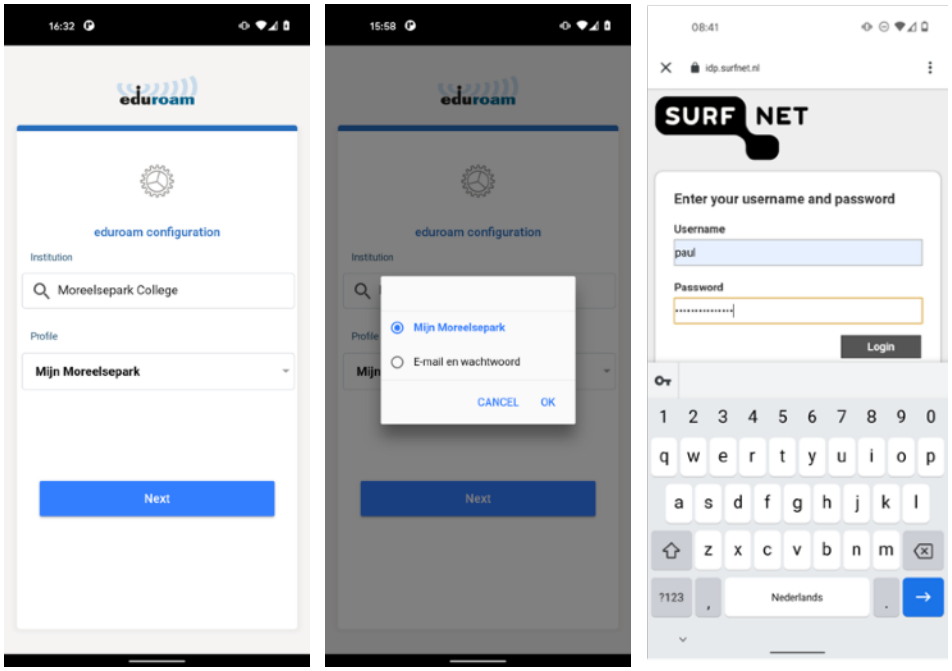
Deze app configureert eduroam-accounts met behulp van per instelling op maat gemaakte profielen. Minder beheerlast dus voor instellingen, gebruikers kunnen zelf eduroam op de juiste manier op hun device zetten.

De geteduroam Apps staan in de Google Play store en Apple App store voor Android en iOS/ iPadOS. Voor Windows is er een installer (.exe) en voor macOS kunnen er profielen (.mobileconfig) worden gedownload. Deze worden via een website aangeboden. Native macOS, Linux opties zijn nog in ontwikkeling. (ChromeOS is nog onzeker, maar kan met client-certificaten werken.)

Gebruikers doorlopen een aantal configuratiestappen en hoeven naast de naam van de organisatie geen verdere kennis te hebben van de specifieke wifi-instellingen.



Er kunnen eventueel meerdere profielen worden aangeboden per organisatie: ook een mengvorm van profielen en accounts afgeleid van SURFconext-authenticatie zoals verderop beschreven.



De Apps zorgen voor de juiste en veilige configuratie.

Bij pseudo-accounts is bij afronding direct duidelijk of de ingevulde gegevens correct zijn, anders blijkt dat uit de eerste authenticatie-poging.

Mobiele browser voor pseudo-accounts

Inzetten van geteduroam

Instellingen kunnen de geteduroam Apps op twee manieren inzetten:

1. **Instellingsprofielen**: Voor de configuratie van eduroam instellingsaccounts op basis van profielen;
2. **Hosted geteduroam via SURFconext**: Voor de configuratie met een pseudo-account, afgeleid van de authenticatie via SURFconext.

Instellingsprofielen

Voor configureren van instellingsaccounts moet de beheerder inloggen in de eduroam Configuration Assistance Tool (CAT, https://cat.eduroam.org/) om een profiel aan te maken. Denk hierbij aan het juiste realm, het juiste EAP type en gegevens over de server certificaten.

Gebruikers vullen alleen hun gegevens in in de Apps, en die worden tijdens de eduroam authenticatie bij de instelling via RADIUS geverifieerd.

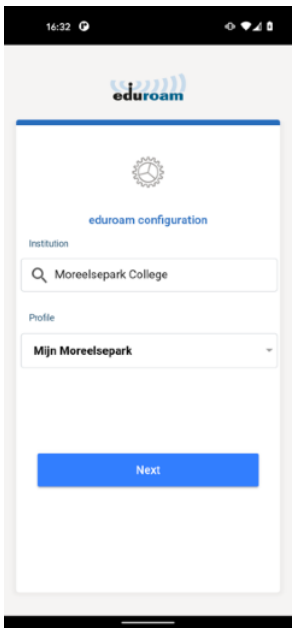
Een handleiding voor CAT is te vinden op:
https://wiki.geant.org/display/H2eduroam/A+guide+to+eduroam+CAT+for+IdP+administrators

Toegang tot eduroam CAT kan worden aangevraagd via beheer@eduroam.nl en de authenticatie voor beheerders is via het SURFconext dashboard aan te vragen onder “eduroam supporting services”.

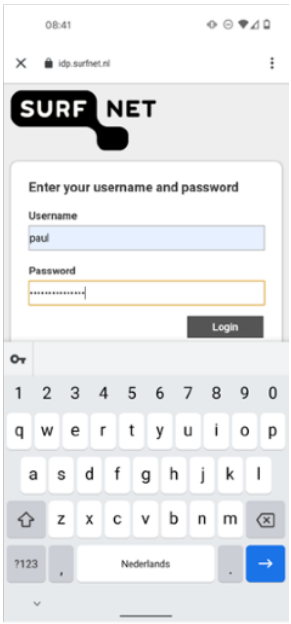
Hosted geteduroam via SURFconext

Een speciale methode in de Apps is de configuratie van pseudo-accounts, afgeleid van de authenticatie via SURFconext. In dit geval loggen eindgebruikers in via de App en krijgt het apparaat na de SURFconext-authenticatie bij de eigen instelling een certificaat van SURF dat (bijvoorbeeld) een jaar geldig is. SURF doet hiermee de eduroam (RADIUS) authenticatie.

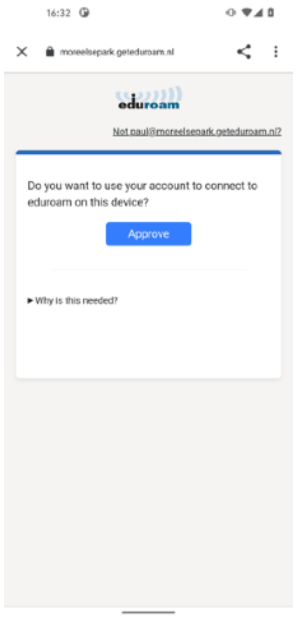
profiel @CAT



IdP @organisatie



authenticatie @SURF



Op deze manier is het ook mogelijk een eduroam-account aan te maken met een SURFconext-IdP, zoals ADFS, Shibboleth, SimpleSAMLphp, een Cloud IdP als Azure AD of de Google Workspace IdP - elke IdP, als deze maar aan SURFconext is gekoppeld.

Ook is het mogelijk om extra eisen te stellen aan de authenticatie, zoals MFA.

Een profiel voor pseudo-accounts moet ook in CAT worden aangemaakt, maar SURF regelt dit als dit het enige profiel is.

De workflow voor geteduroam is voor gebruikers vergelijkbaar met een instellings-account; de authenticatie van het echte gebruikersaccount verloopt alleen via de (mobiele) browser en de App. Voordeel is dat de manier van authenticeren in een browser is een voor gebruikers bekende manier is.

Autorisatie

Gebruikers zijn herkenbaar aan het realm (@[instelling].geteduroam.nl), waardoor alsnog VLAN toekenning kan worden gedaan.

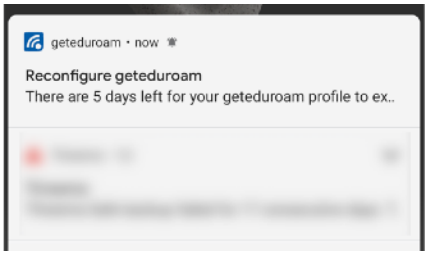
Het is ook mogelijk gebruikers te onderscheiden op basis van het eduPersonAffiliation attribuut in SURFconext. Zo kan een student dan een realm krijgen @student.[instelling].geteduroam.nl en een medewerker @medewerker.[instelling].geteduroam.nl
Hierdoor kan ook VLAN toekenning binnen de organisatie toegepast worden op gebruikersgroep.

Security en privacy

Profielen zorgen er in het algemeen voor dat de instellingen goed zijn waardoor het onderscheppen van een gebruikersnaam en wachtwoord niet kunnen. Daarom is elke inzet van geteduroam voor eindgebruikers veilig.

De pseudo-accounts worden gemaakt puur voor wifi-toegang, en werken op basis van certificaten. Dit zijn credentials die bij het opzetten van de verbinding nooit onderschept kunnen worden, en zijn daarmee veiliger dan een gebruikersnaam en wachtwoord. Tegelijk zijn de accounts minder waardevol, omdat ze niet voor andere toepassingen gebruikt kunnen worden.

De certificaten zijn (standaard) een jaar geldig, waarna de Apps waar mogelijk een push bericht geven voor verlenging/ herauthenticatie via SURFconext. Dat is bij Android pas in de mogelijk vanaf Android 12. Met Android 11 en eerder moeten gebruikers moeten er zelf aan denken dat na een jaar er een nieuw profiel nodig is.



Bij misbruik kan op basis van de gebruikersnaam en eventueel andere kenmerken de oorspronkelijke gebruiker aangeschreven worden en worden geblokkeerd.

De gebruikersnamen zijn random en via de omgeving van SURF herleidbaar om privacy te waarborgen. Instellings-beheerders kunnen hier toegang toe krijgen.

eduroam IdP as a Service

De pseudo-accounts van geteduroam worden geauthenticeerd door een RADIUS-omgeving van SURF. Hierdoor kan de RADIUS-koppeling tussen instelling en SURF beperkt blijven tot uitgaande authenticatieverzoeken, er is geen IdP RADIUS-koppeling meer nodig.

SURFconext

Voor de authenticatie van eindgebruikers voor pseudo-accounts moet de dienst “geteduroam” in het SURFconext dashboard (https://dashboard.surfconext.nl/) worden aangevraagd.

Deze koppeling is niet nodig voor het gebruik van eigen instellings-profielen via eduroam CAT. Daarvoor is een koppeling op “eduroam supporting services” nodig.

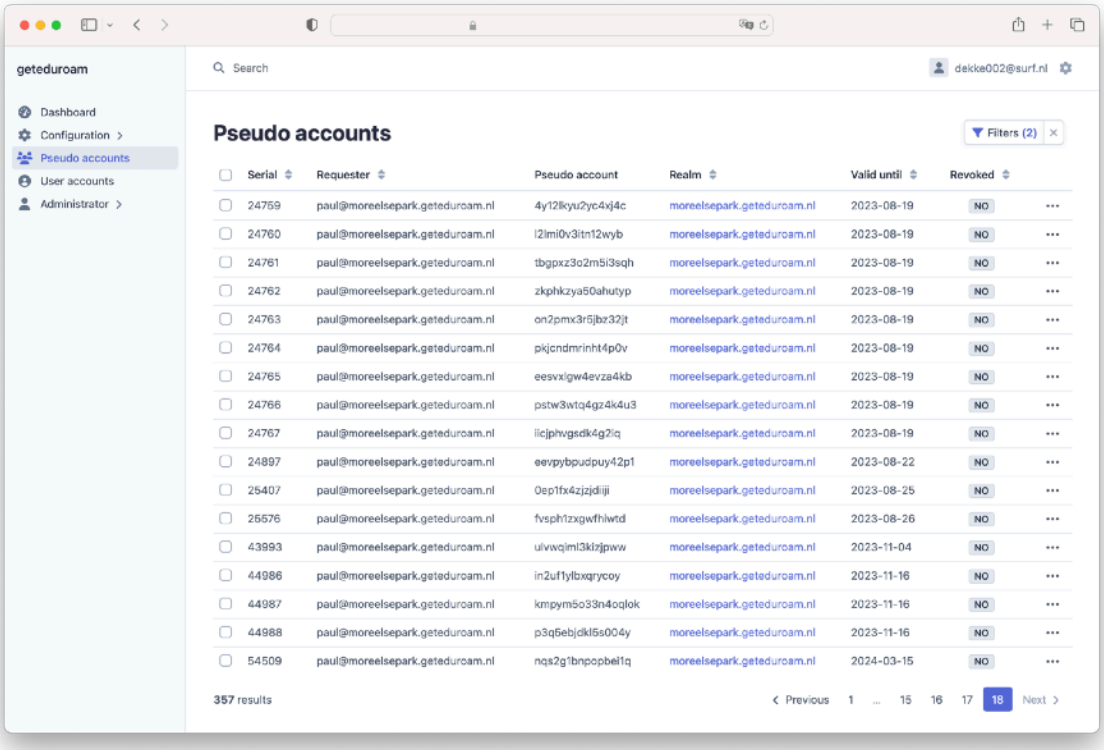
Neem na het koppelen van de dienst op SURFconext contact op met beheer@eduroam.nl voor het afronden van de configuratie.

Herleidbaarheid

Gebruikers op geteduroam krijgen een gerandomiseerde gebruikersnaam, en zijn daarmee niet direct identificeerbaar. Tijdens het aanmaken van het account slaat geteduroam een kenmerk uit de SURFconext authenticatie op voor de herleidbaarheid.

De opties zijn hiervoor de eduPersonPrincipalId (ePPN, de standaard optie), en de persistent Name Identifier. Met de ePPN kan vanuit geteduroam inzichtelijk gemaakt worden welke gebruiker een account heeft gekregen; bij de persistent NameID heeft de support van SURFconext een rol in het herleiden op het eigenlijke account.

Beheerders kunnen toegang krijgen tot de portal waarmee de gebruikers kunnen worden opgespoord, en waarmee de accounts kunnen worden teruggetrokken.



Een gebruiker zou kunnen proberen de (outer) username aan te passen in de client. Gebruikers kunnen hun realm niet aanpassen, die moet overeenkomen met het uitgegeven certificaat.

De username mag anonymous@ bevatten (dit is ook gebruikelijk bij Passpoint netwerken) maar de daadwerkelijke User-Name uit het certificaat komt vanuit SURF terug in het RADIUS Access-Accept packet in het User-Name attribuut. Ook zorgen we voor adequate logging van deze gegevens en het serial number van het certificaat, waardoor er altijd een relatie is te maken bij een incident.