Vertrouwelijk — niet verspreiden

Eduarte
van topicus

PRODUCTDOCUMENT

SCIM — User Provisioning

Functionele documentatie — accounts, identiteiten en credentials

VERTROUWELIJK



Versie 2.0 11 augustus 2026

Inhoudsopgave

Doel & introductie 3
Domein & standaard 3
Doelgroep & use cases 4
Scope & reikwijdte 4
Functionele flows 4
Gegevens op hoofdlijnen 5
Randvoorwaarden & afspraken 5
Verwijzingen 6

VERTROUWELIJK

Doel & introductie

SCIM is de **user-provisioningkoppeling** van Eduarte Connect. Waar de meeste koppelingen gegevens *uit* Eduarte ontsluiten, schrijft deze koppeling gegevens *in* Eduarte: het **aanmaken en wijzigen van accounts** — in de eerste plaats medewerkeraccounts — en het **beheren van de identiteiten waarmee die accounts inloggen**.

Een aangesloten partij beheert via deze koppeling:

- **het account zelf** — aanmaken, bijwerken en deactiveren;
- **het e-mailadres** van het account;
- **de credentials** waarmee de gebruiker inlogt: een lokaal wachtwoord, of een externe identiteit zoals eduID, SURFconext, Microsoft Entra ID, een ADFS/SAML-identiteit, de eigen OpenID Connect-server van de school of een KeyHub-identiteit.

De koppeling volgt **SCIM 2.0** (*System for Cross-domain Identity Management*), de internationale standaard voor het uitwisselen van identiteitsgegevens tussen systemen. Daardoor sluit een school of IAM-partner Eduarte aan met dezelfde middelen die zij voor hun overige systemen al gebruiken.

> **Status — in ontwikkeling.** Deze koppeling is in ontwikkeling; het endpointcontract is nog niet definitief en de OpenAPI-specificatie heeft de status *concept*. Deze documentatie beschrijft de beoogde werking, zodat aansluitende partijen kunnen meelezen en meedenken. Neem contact op met Eduarte voordat je een implementatie inplant.

VERTROUWELIJK

Domein & standaard

SCIM valt binnen het domein **Provisioning** en is een **externe standaard**: de gezaghebbende definitie wordt buiten Eduarte beheerd (IETF, RFC 7643 en RFC 7644). Deze documentatie beschrijft de koppeling **zoals geïmplementeerd in Eduarte Connect** — een deel van de standaard — en verwijst voor de volledige definitie naar de standaard zelf.

Anders dan bij de O-koppelingen gaat het hier niet om een onderwijsstandaard maar om een algemene identiteitsstandaard; SCIM houdt daarom zijn eigen naam als connectorcode.

Verhouding tot EKP — Provisioning. De twee koppelingen zijn complementair en wijzen in tegengestelde richting:

	EKP	SCIM
Richting	leest **uit** Eduarte	schrijft **in** Eduarte
Inhoud	basisgegevens: studenten, verbintenissen, groepen, medewerkers	accounts, e-mail en inlogidentiteiten
Typische afnemer	de school (eigen ESB of één integratiepartner)	de IAM-partij die accounts en identiteiten beheert

Een school die haar accountbeheer volledig automatiseert, gebruikt in de praktijk beide: EKP om te weten *wie* er is, SCIM om vast te leggen *waarmee* die persoon inlogt.

Doelgroep & use cases

De koppeling kent twee soorten afnemers, met bewust verschillende rechten:

1. **SURFconext Invite — eduID koppelen.** Invite koppelt een eduID aan een **bestaand** Eduarte-account. Deze route mag **uitsluitend koppelen**: er worden nooit personen of accounts aangemaakt.
2. **IAM-integratiepartners — accountbeheer.** Een partij die namens de school het identiteitsbeheer verzorgt, mag breder: accounts aanmaken voor bestaande personen, medewerkers aanmaken, credentials zetten en roteren, en accounts deactiveren.

Wat een partij daadwerkelijk mag, wordt **per partij afzonderlijk toegekend**. De rechten zijn fijnmazig verdeeld, zodat een koppelpartij niet meer kan dan waarvoor zij is aangesloten; zie *Randvoorwaarden & afspraken*.

Scope & reikwijdte

De koppeling beheert **accounts en identiteiten**, geen onderwijsgegevens. Bewust buiten scope:

- **Geen groepen of rollen.** Rol- en groepsprovisioning (de SCIM-resource `Groups`) wordt niet ondersteund; de koppeling adverteert dit ook expliciet als niet-ondersteund.
- **Geen definitieve verwijdering.** Deprovisioning is altijd *zacht*: een identiteit wordt ontkoppeld of een account gedeactiveerd. Er wordt niets uit Eduarte weggegooid.
- **Geen personen aanmaken voor deelnemers, ouders of bedrijven.** Voor die doelgroepen kan wél een account bij een **bestaande** persoon worden aangemaakt; de persoon zelf ontstaat in Eduarte via de reguliere aanmeld- en inschrijfprocessen. Alleen voor **medewerkers** kan de koppeling ook de persoon aanmaken.
- **Geen keuze van de login-methode.** Welke inlogmethode een gebruiker krijgt, bepaalt de **school** per doelgroep. De koppeling legt identiteiten vast; ze kiest niet hoe er wordt ingelogd.

Functionele flows

1. **eduID koppelen** — SURFconext Invite meldt het eduID van een gebruiker aan bij het bestaande Eduarte-account. Eduarte legt dat eduID vast als extra identiteit bij dat account; de gebruiker kan daarna met eduID inloggen.
2. **Medewerkeraccount aanmaken** — een IAM-partner meldt een nieuwe medewerker aan. Eduarte maakt de persoon en het account aan, met het opgegeven e-mailadres en de opgegeven identiteit.
3. **Account bij een bestaande persoon** — voor een deelnemer, ouder of bedrijf dat al in Eduarte bekend is, wordt een account met bijbehorende identiteit aangemaakt.

VERTROUWELIJK

4. **Credential beheren of roteren** — een identiteit wordt toegevoegd, vervangen of ingetrokken, bijvoorbeeld wanneer een school van identity provider wisselt.
5. **Deactiveren** — bij uitdiensttreding wordt het account gedeactiveerd of wordt alleen de betreffende identiteit ontkoppeld. Het account en de historie blijven bestaan.

Gegevens op hoofdlijnen

Gegeven	Functionele omschrijving
Account	De gebruiker in Eduarte, met een stabiel eigen kenmerk waarop beide kanten correleren.
Naam & weergavenaam	Voor- en achternaam en de weergavenaam van de gebruiker.
E-mailadres	Het e-mailadres van het account.
Doelgroep	Het soort gebruiker: medewerker, deelnemer, ouder of bedrijf.
Medewerker- of studentnummer	Het nummer waarmee de persoon binnen de school bekend is.
Identiteit (credential)	Waarmee de gebruiker inlogt: lokaal wachtwoord, eduID, SURFconext, Entra ID, ADFS/SAML, de eigen OIDC-server van de school of KeyHub.
Actief-status	Of het account gebruikt kan worden.

VERTROUWELIJK

Randvoorwaarden & afspraken

- **Rechten per partij.** Elke aangesloten partij krijgt precies de rechten die bij haar rol horen. De eduID-route van SURFconext Invite is bewust beperkt tot koppelen; alleen een IAM-partner met een expliciete afspraak mag accounts aanmaken of credentials beheren.
- **Eén partij voert de regie.** Accountbeheer laat zich slecht verdelen: laat één partij per school verantwoordelijk zijn voor het aanmaken en muteren van accounts.
- **De school kiest de login-methode**, per doelgroep — niet de individuele gebruiker en niet de koppelpartij. De koppeling legt vast welke identiteiten bij een account horen; de school bepaalt welke daarvan bij inloggen wordt gebruikt.
- **Beheeraccounts worden niet via deze koppeling aangemaakt.** Voor beheertoegang tot Eduarte geldt een eigen, afgedwongen inlogmethode. Dat een KeyHub-identiteit als credential kan worden vastgelegd, verandert daar niets aan: vastleggen welke identiteiten bij een account horen is iets anders dan bepalen waarmee er ingelogd mag worden.
- **Regie en AVG.** De koppeling verwerkt persoonsgegevens en inlogidentiteiten. De school is verantwoordelijk voor de afspraken met de koppelpartij en voor dataminimalisatie: lever niet meer gegevens aan dan voor het accountbeheer nodig is.

- **Toegang & consent** — toegang verloopt via Connect; zie de technische specificatie voor authenticatie en de rechten per operatie.

Verwijzingen

- **Technische specificatie:** SCIM — Technische specificatie (PDF).
- **OpenAPI-specificatie:** meegeleverd als `SCIM_v2.0.yml`.
- **Online referentie:** API-referentie van SCIM
- **Standaard:** SCIM 2.0 — RFC 7643 (schema) en RFC 7644 (protocol).

VERTROUWELIJK