

TECHNISCHE SPECIFICATIE

SCIM — User Provisioning

Technische documentatie voor developers

VERTROUWELIJK





Inhoudsopgave

Overzicht & scope	3
Aan de slag & dev-omgeving	3
Beveiliging	4
Transport (TLS)	4
Authenticatie & autorisatie	4
Per endpoint	4
Conventies (SCIM 2.0)	5
Correlatie & idempotentie	5
Foutafhandeling	5
Throttling & rate limiting	6
Aanbevolen client-gedrag	6
Endpoints op hoofdlijnen	7
Credentials & de Eduarte-extensie	8
Richtlijnen voor implementatie	9
Beschikbaarheid & SLA	9
Uitgangspunten	9
Versiebeheer & standaard	10

VERTROUWELIJK



Overzicht & scope

SCIM is het **SCIM 2.0 Service Provider-endpoint** van Eduarte: een schrijvende API waarmee een aangesloten partij accounts, e-mailadressen en inlogidentiteiten (credentials) in Eduarte beheert. In tegenstelling tot de Eduarte-specifieke (E-)koppelingen volgt SCIM een **externe standaard**, met eigen paden, attribuutnamen, paginering en foutformaat. De gezaghebbende definitie staat extern:

Officiële standaard: SCIM 2.0 — [RFC 7643](#) (schema) en [RFC 7644](#) (protocol).

Deze specificatie beschrijft SCIM **zoals geïmplementeerd in Eduarte Connect** (een subset) en verwijst voor de volledige definitie, schema's en conventies naar de standaard.

- **Standaard:** SCIM 2.0 (RFC 7643/7644)
- **Versie:** 2.0
- **Pad-prefix:** `/connect/scim/v2_0`
- **Content-type:** `application/scim+json`
- **Volledige OpenAPI-specificatie:** meegeleverd als `SCIM_v2.0.yml`.
- **Interactieve referentie online:** [API-referentie van SCIM](#)

Rol van Eduarte: *Service Provider* in SCIM-termen. De aanroepende partij is de *Identity Provider* / provisioning-client; Eduarte ontvangt en registreert.

Status — in ontwikkeling. Het endpointcontract is nog niet definitief; de meegeleverde OpenAPI-specificatie heeft de status **concept**. Paden en schema's kunnen nog wijzigen. Stem een implementatie af met Eduarte voordat je eraan begint.

Aan de slag & dev-omgeving

1. **Toegang aanvragen** — vraag via Eduarte (connect@eduarte.nl) OAuth2-clientgegevens aan. Geef daarbij aan welke rol je vervult (eduID-koppelen of breder accountbeheer); daarop worden de scopes toegekend.
2. **Scopes** — zie de tabel hieronder; je krijgt uitsluitend de scopes die bij je rol horen.
3. **Token ophalen** — haal een access-token op via de OAuth2 Client Credentials-flow. De **tenant (school)** zit als `organisatieuuid`-claim in het token; je hoeft de school dus niet in de request mee te geven.
4. **Aanroepen** — stuur het token mee als `Authorization: Bearer <token>`, gebruik `Content-Type: application/scim+json` en roep de endpoints aan onder `/connect/scim/v2_0`.
5. **Testen** — gebruik de beschikbare ontwikkel-/testomgeving voordat je in productie gaat.

Scope	Geeft recht op
<code>scim.eduid.link</code>	Een eduID koppelen aan of ontkoppelen van een bestaand account. Maakt nooit personen of accounts aan.
<code>scim.user.read</code>	Gebruikers lezen en zoeken, en de discovery-endpoints opvragen.



Scope	Geeft recht op
scim.account.provision	Accounts met credentials aanmaken voor bestaande deelnemers, ouders of bedrijven; accounts (de)activeren.
scim.medewerker.create	Een medewerker aanmaken — persoon én account.
scim.credential.manage	Credentials zetten en roteren op een bestaand account.

Fijnmazige regels worden **server-side afgedwongen**. De belangrijkste: de eduID-route is *link-only* — met `scim.eduid.link` kun je geen persoon of account laten ontstaan, ook niet via een `POST /Users`.

Beveiliging

Alle Connect API's worden uniform beveiligd. De maatregelen hieronder gelden voor elke connector; afwijkingen staan in de connector-specifieke secties.

Transport (TLS)

Alle communicatie verloopt verplicht via **HTTPS**. Minimaal **TLS 1.2**, bij voorkeur TLS 1.3. Er zijn geen HTTP-endpoints, ook niet voor redirects. Een geldig servercertificaat is vereist. Hierin volgen we de aanbeveling van de [NSCT](#)

Authenticatie & autorisatie

Authenticatie verloopt via **OAuth 2.0 met de Client Credentials-flow** (server-to-server):

- Token-endpoint: `https://login.educus.nl/oauth2/token?organisatieuuid=<uuid>`
- De client wisselt zijn `client_id` en `client_secret` in voor een access-token.
- Het verkregen token wordt bij elke aanroep meegestuurd in de `Authorization: Bearer <token>` -header.

Scopes bepalen de toegangsrechten volgens het principe van *least privilege*. Elke API kent één of meer scopes; een token bevat alleen de scopes die de client nodig heeft. De vereiste scope(s) per connector staan in de connector-specifieke sectie.

Waar OAuth 2.0 niet mogelijk is (bijvoorbeeld bij legacy-integraties), kan als terugvaloptie een **Bearer-token (JWT)** worden gebruikt.

Per endpoint

Elk endpoint heeft een expliciete `security` -definitie. Onjuiste of ontbrekende autorisatie leidt tot een `401 Unauthorized` (niet geauthenticeerd) of `403 Forbidden` (onvoldoende rechten); zie *Foutafhandeling*.



Conventies (SCIM 2.0)

SCIM volgt de conventies van de standaard, die **afwijken van de Connect-conventies** van de E-koppelingen. De belangrijkste verschillen:

- **Engelstalige resources met een hoofdletter:** `/Users` , `/ServiceProviderConfig` , `/ResourceTypes` , `/Schemas` . Attribuutnamen zijn camelCase: `userName` , `externalId` , `displayName` , `active` .
- **Content-type** `application/scim+json` voor requests én responses, niet `application/json` .
- **Pagineren met startIndex (1-based) en count** , niet met `offset / pageSize` . Het antwoord is een `ListResponse` met `totalResults` , `startIndex` en `itemsPerPage` .
- **Zoeken met een SCIM- filter** . Ondersteund op minimaal `externalId` en `userName` — genoeg om vóór een create te controleren of de gebruiker al bestaat.
- **Partieel bijwerken via PatchOp** (`add` , `remove` , `replace`) op `PATCH /Users/{id}` , niet met JSON Merge Patch.
- **Elke resource draagt zijn schemas -array**, inclusief de Eduarte-extensie `urn:ietf:params:scim:schemas:extension:eduarte:2.0:User` .
- **/Groups wordt niet ondersteund** en wordt als zodanig geadverteerd in `ServiceProviderConfig` en `ResourceTypes` .

Waar de standaard botst met de Connect-conventies is dat vastgelegd met `x-suppress-rules` in de specificatie, met verwijzing naar de standaard. Raadpleeg de standaard en de meegeleverde `SCIM_v2.0.yml` voor de exacte conventies, parameters en schema's.

Correlatie & idempotentie

- De SCIM- id is het **Eduarte account-UUID** — read-only, en het kenmerk waarop beide kanten correleren. SURFconext Invite geeft dit mee als `internalPlaceholderIdentifier` .
- `externalId` is het kenmerk van de **aanroepende partij** (Invite of de IAM-partner); Eduarte bewaart het, maar leidt er geen gedrag uit af.
- **Zoek vóór create:** doe een `GET /Users?filter=...` op `externalId` of `userName` voordat je een `POST` doet, zodat een herhaalde run geen dubbele registratie oplevert.

Foutafhandeling

SCIM heeft een **eigen foutformaat** en gebruikt dus **niet** het `problem+json` -foutobject (RFC 7807) van de E-koppelingen. Een fout is een resource van het type `urn:ietf:params:scim:api:messages:2.0>Error` :

Veld	Betekenis
<code>schemas</code>	Altijd <code>["urn:ietf:params:scim:api:messages:2.0>Error"]</code>
<code>status</code>	De HTTP-statuscode, als string (bijvoorbeeld <code>"400"</code>)
<code>scimType</code>	Het SCIM-fouttype, bijvoorbeeld <code>invalidValue</code> of <code>invalidFilter</code>



Veld	Betekenis
detail	Toelichting, bedoeld voor de ontwikkelaar

Status	Wanneer
400 Bad Request	Ongeldige payload, ongeldig filter of een ongeldige PatchOp
401 Unauthorized	Geen of ongeldig token
403 Forbidden	Token mist de vereiste scope, of de operatie is voor deze rol niet toegestaan (bijvoorbeeld een account willen aanmaken op de eduID-route)
404 Not Found	Onbekende id binnen deze tenant
409 Conflict	De identiteit is al aan een ander account gekoppeld
500 Internal Server Error	Onverwachte fout aan Eduarte-zijde

Handel fouten af op de **statuscode** en **scimType**, niet op de tekst van detail.

Throttling & rate limiting

Alle endpoints kennen **rate limiting** om misbruik en overbelasting te voorkomen. Dit wordt op infrastructuurniveau afgedwongen via de Topicus API-gateway.

Bij overschrijding van de limiet antwoordt de API met **429 Too Many Requests**. De response kan de volgende headers bevatten:

Header	Betekenis
Retry-After	Aantal seconden tot een volgende aanroep is toegestaan
X-RateLimit-Limit	Maximum aantal aanroepen per tijdsperiode
X-RateLimit-Remaining	Resterend aantal aanroepen in de huidige periode

Aanbevolen client-gedrag

- Respecteer **Retry-After** en wacht ten minste het opgegeven aantal seconden.
- Gebruik **exponential backoff** met jitter bij herhaalde **429** -responses.
- Verspreid bulk-aanroepen over de tijd in plaats van ze gelijktijdig te versturen.



Endpoints op hoofdlijnen

Zoals geïmplementeerd in Eduarte Connect. Voor de volledige definities: zie de meegeleverde SCIM_v2.0.yml of de [API-referentie](#).

Users

Endpoint	Methode	Toelichting	Scope(s)
/Users	POST	Gebruiker aanmaken of koppelen — gedrag hangt af van de scope (zie hieronder)	scim.eduid.link · scim.account.provision · scim.medewerker.create
/Users	GET	Zoeken met filter , gepagineerd met startIndex / count	scim.user.read
/Users/{id}	GET	Één gebruiker lezen	scim.user.read
/Users/{id}	PUT	Volledige vervanging van attributen en credentials	scim.account.provision · scim.credential.manage
/Users/{id}	PATCH	Partieel bijwerken: credential toevoegen of verwijderen, account (de)activeren via active	scim.eduid.link · scim.account.provision · scim.credential.manage
/Users/{id}	DELETE	Zachte deprovisioning: eduid ontkoppelen of account deactiveren. Nooit een hard delete.	scim.eduid.link · scim.account.provision

POST /Users doet drie verschillende dingen, afhankelijk van de scope van het token:

Scope	Gedrag
scim.eduid.link	Upsert van een eduid-credential op het account dat via id wordt gecorreleerd. Er ontstaat geen persoon en geen account.
scim.account.provision	Account en credential voor een bestaande deelnemer, ouder of bedrijf.
scim.medewerker.create	Persoon en account voor een medewerker.

Discovery



Endpoint	Methode	Toelichting	Scope
/ServiceProviderConfig	GET	Welke features worden ondersteund (patch , filter met maxResults) en de authenticationSchemes	scim.user.read
/ResourceTypes	GET	De ondersteunde resourcetypen	scim.user.read
/Schemas	GET	De schema's, inclusief de Eduarte-extensie	scim.user.read

Lees /ServiceProviderConfig uit in plaats van ondersteuning te veronderstellen — daar staat onder meer of filter beschikbaar is en wat de maximale resultaatgrootte is.

Credentials & de Eduarte-extensie

De User -resource is de standaard SCIM- User , uitgebreid met urn:ietf:params:scim:schemas:extension:eduarte:2.0:User :

Veld	Betekenis
doelgroep	MEDEWERKER , DEELNEMER , OUDER of BEDRIJF — het persoonstype van het account
medewerkernummer	Het medewerkernummer, bij doelgroep MEDEWERKER
studentnummer	Het studentnummer, bij doelgroep DEELNEMER
credentialType	Het type identiteit waarop userName betrekking heeft (zie hieronder)

userName is de **login-identifier**: de waarde waarmee de identity provider de gebruiker aanduidt — bijvoorbeeld het eduID-pseudoniem of de OIDC- sub . In combinatie met credentialType bepaalt dat welke identiteit wordt vastgelegd:

credentialType	Identiteit
EDUID	eduID-pseudoniem (SURFconext Invite) — alleen koppelen
SURFCONEXT	SURFconext-identiteit
ENTRA_OIDC	Microsoft Entra ID via OIDC
ADFS_SAML	ADFS/SAML-identiteit
SCHOOL_OIDC	De eigen OpenID Connect-server van de school



credentialType	Identiteit
LOCAL_PASSWORD	Lokaal wachtwoord
KEYHUB	KeyHub-identiteit

Een account kan **meerdere credentials** hebben: identiteiten worden verzameld, ze sluiten elkaar niet uit. Dat een account zowel een eduID als een Entra-identiteit heeft, betekent niet dat de gebruiker kan kiezen — welke methode bij inloggen wordt gebruikt, bepaalt de school per doelgroep.

Vastleggen is niet hetzelfde als toestaan. Een KEYHUB -credential vastleggen kan, maar zegt niets over de inlogmethode: voor beheertoegang is KeyHub afgedwongen, ongeacht welke andere credentials een account draagt. **Beheeraccounts worden niet via deze koppeling aangemaakt** — doelgroep kent geen waarde BEHEER .

Het e-mailadres gaat via het standaard SCIM- emails -attribuut (value , type , primary).

Richtlijnen voor implementatie

- Implementeer backoff bij 429 Too Many Requests en respecteer de Retry-After -header.
- Pin op een major-versie in het pad en test tegen de testomgeving vóór productie.

Beschikbaarheid & SLA

Eduarte Connect wordt aangeboden als beheerde dienst. Beschikbaarheid, onderhoud en support zijn vastgelegd in de partnerovereenkomst en bijbehorende SLA.

Uitgangspunten

- De API's zijn ontworpen voor continue beschikbaarheid tijdens kantoor- en uren.
- Gepland onderhoud wordt vooraf aangekondigd via de gangbare communicatiekanalen en zo veel mogelijk buiten piekuren uitgevoerd.
- Storingen en vragen kunnen worden gemeld bij Eduarte via de beklende servicedesk meldingen
- Partner vragen kunnen worden gemeld bij info@eduarte.nl.

Let op: concrete SLA-cijfers (beschikbaarheidspercentage, reactietijden, onderhoudsvensters) worden vastgelegd in de partnerovereenkomst en zijn **nog te bevestigen** voor deze documentatie.



Versiebeheer & standaard

De koppeling volgt **SCIM 2.0**; het versienummer in het pad (v2_0) is de versie van de standaard, niet een Eduarte-eigen versienummer.

Aspect	Waarde
Standaard	SCIM 2.0 — RFC 7643 (schema) en RFC 7644 (protocol)
Bron	https://www.rfc-editor.org/rfc/rfc7644
Status in Eduarte Connect	In ontwikkeling — subset (Users + discovery), Groups niet ondersteund; contract nog niet definitief

VERTROUWELIJK