

IPSIE SCIM 2.0 Profile

A conformance profile for interoperable enterprise identity lifecycle in SCIM 2.0.

IETF 126 Vienna, Austria

SCIM WG July 2026

Draft draft-schreiber-scim-ipsie-profile/

What is IPSIE?

Interoperability Profile for Secure Identity in the Enterprise — three cumulative assurance levels.

AL1 Deprovisioning

- Suspend, archive, or delete user accounts at IdP request.
- The floor for any identity provisioning integration.

// foundational

AL2 User & Group Mgmt

- Sync users, groups & memberships across IdP and App.
- Includes all AL1 deprovisioning capabilities.

// builds on AL1

AL3 Roles / Entitlements

- Expose app roles & entitlements to the IdP.
- Centralize role / entitlement assignment.

// in development

GOAL

Define conformance requirements that drive interoperability of critical security features in SCIM between identity providers and application vendors.

The Problem IPSIE Solves

CURRENT STATE Every SCIM implementation makes different design choices, so no two integrations behave alike.

Why it matters

A "SCIM-supporting" application is not guaranteed to work with your IdP's SCIM client. Engineering teams typically custom-code workarounds for every vendor pair.

WHAT VARIES

- Updates: some apps require PUT, others PATCH, with differing behaviors.
- PATCH syntax varies: explicit path vs. path-less, value-inferred intent.
- Lifecycle differs: active:false to suspend vs. DELETE-only, no standard mapping.

IPSIE ANSWER

Define explicit conformance requirements that guarantee interoperability between any IdP and any application, eliminating vendor-specific workarounds.

IPSIE & the Interoperability Profile

KEY DEPENDENCY IPSIE requires implementers to also conform to the SCIM 2.0 Interoperability Profile. This is a structural requirement, not optional.

WHY IT MATTERS

- The Interop Profile establishes baseline protocol behaviors IPSIE builds on.
- Covers pagination, filtering, PATCH semantics, and case sensitivity.
- IPSIE compliance = Interop Profile compliance + IPSIE assurance requirements.
- Guarantees a common protocol foundation before assurance levels apply.
- Without it, IPSIE requirements would rest on undefined protocol behavior.

AL1 — User Deprovisioning Requirements

Operation	Method	Required	Details
Query Users	GET	MUST	Filters: userName eq, externalId eq, emails[value eq]
Deactivate / Delete	PATCH / DELETE	One MUST	Set active: false, or DELETE /Users/{id}
Reactivate	PATCH	If deactivate	MUST allow setting active: true

SECURITY HIGHLIGHT • MINIMUM VIABLE PROVISIONING

FIND **OK**

locate a user via filter

DISABLE **OK**

PATCH active: false

DELETE **OK**

DELETE /Users/{id}

REACTIVATE **OK**

PATCH active: true

AL2 — User and Group Management

EXTENDS AL1 Adds full user and group management on top of AL1 deprovisioning.

NO CREDENTIALS Password attribute MUST NOT be supported; no passwords, hashes, keys, or TOTP seeds in SCIM payloads.

MUST REJECT Local user or group creation outside of SCIM is prohibited.

AL2 REQUIREMENTS (EXTENDS AL1)

Capability	Method	Requirement
User Schema	Schema	userName, displayName, active, externalId
Create / Update	POST + PATCH	/Users and /Groups
Group Members	PATCH	50+ member add/remove operations per request
List Operations	GET	/Users and /Groups with pagination

Shared Prerequisites (All Levels)

MUST ENFORCE

Authentication & Authorization

- OAuth 2.0 client_credentials + JWT Client Auth (RFC 7523)
- Bearer token in the Authorization header
- HTTP Basic Auth for credential transmission, not the body

MUST SUPPORT

Performance & Scale

- Rate limiting with 429 + Retry-After
- Minimum 25 SCIM requests / second
- /Bulk endpoint
- PATCH with multiple attribute updates

MUST LOG

Error Handling & Auditing

- All creates, deletes & modifications MUST be logged
- SCIM error format on failures
- No internal details leaked in error responses

Next Steps

1

SCIM WG scope

Is this sort of profile in scope for the SCIM Working Group? If not, should the charter be updated to bring it in scope, or should it be brought to another standards body such as the OpenID Foundation?

→ Inviting feedback on any aspect of the draft — the floor is open.