System for Cross-domain Identity Management
Internet-Draft
Intended status: Informational
Expires: 20 February 2026

M. Wahl
Microsoft

19 August 2025

System for Cross-domain Identity Management: Agentic Identity Schema
draft-wahl-scim-agent-schema-01

Abstract

The System for Cross-domain Identity Management (SCIM) specifications are designed to make identity management in cloud-based applications and services easier.

This document provides a platform-neutral schema for representing AI agents' identities in JSON format, enabling them to be transferred in the SCIM protocol to the service. This establishes an agentic identity so that an agent can subsequently be authenticated and authorized to interact with the service.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-wahl-scim-agent-schema/.

Discussion of this document takes place on the System for Cross-domain Identity Management Working Group mailing list (mailto:scim@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/scim/. Subscribe at https://www.ietf.org/mailman/listinfo/scim/.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 20 February 2026.

Table of Contents

1. Introduction

The SCIM protocol [RFC7644] and core schema [RFC7643] are widely implemented for provisioning records for users into services. The default schema for those user records includes attributes such as a person's name, their desired group memberships, and a password that the user. This enables a SCIM client to inform a SCIM server component of a service of a new user, so that user can be identified in and subsequently authenticated to the service. SCIM also enables lifecycle controls for the SCIM client to update and remove that user record in that service, and associate that user with groups, roles and entitlements.

With the growth of agentic AI, agents will also need to be able to interact with services. Some services will require an agent to have identities represented in those services. The attributes of an agent identity in a SCIM server can be different from the attributes of a human user identity. Some services allow OAuth [RFC6749] protocols such as token exchange [RFC8693] for an agent's authentication to the service, without needing a shared secret credential between each agent and the service. However, similar to users, an agent's identity might have access rights in the service, represented through relationships of the agent's identity with groups, roles and entitlements in a service.

As SCIM is familiar within the enterprise and agents often need the same lifecycle signals and group, role or entitlement memberships as users, defining a schema to transport agentic identities in the SCIM protocol simplifies deployment and enables subsequent authentication interactions, consistent controls for those agent's identities and access rights.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. SCIM Schema for Agentic Identity

As an extension to SCIM schema, [RFC7643] sections 3.2 and 3.3, this specification includes one new resource type:

* AgenticIdentity: A resource of this type represents an identity of an agent to the service. It includes attributes of an agentic identity needed to be known by a service, including OPTIONAL references to the agentic identity's group memberships, roles and entitlements.

Resources of this type are conveyed in the SCIM protocol [RFC7644] using JSON [RFC8259]. Extension schemas can be defined to extend this resource type, allowing additional attributes.

3.1. Single-valued Attributes

The resource type AgenticIdentity has the following single-valued attributes. A SCIM server which implements the Agentic Identity schema MUST recognize these attributes.

* active: A boolean value indicating the agentic identity's administrative status. If absent, then an agentic identity is assumed to be active. A SCIM client can indicate that an agentic identity is inactive by setting it to false. The definitive meaning of this attribute is determined by the SCIM server. Support for this attribute in a SCIM client is OPTIONAL.

* agenticApplicationId: The value of this attribute is a string with the id of an agentic application, that is assigned by the SCIM client, enabling correlation and reporting in the service for an agentic application that has multiple identities. The attribute MAY be included when the AgenticIdentity is created. The definitive meaning of this attribute is determined by the SCIM client. Support for this attribute in a SCIM client is OPTIONAL.

* description: The value of this attribute is a string with the agentic identity's human-readable description. Support for this attribute in a SCIM client is OPTIONAL.

* displayName: The value of this attribute is a string with the human-readable name of the agentic identity, suitable for display to end-users. Support for this attribute in a SCIM client is RECOMMENDED.

In addition, the AgenticIdentity also has the attributes "externalId", "id", "meta" and "schemas", as described in sections 3 and 3.1 of [RFC7643].

3.2. Multi-valued Attributes

The resource type AgenticIdentity has the following multi-valued attributes. A SCIM server which implements the Agentic Identity schema SHOULD recognize the attributes "entitlements", "groups", "owners" and "roles". A SCIM server in a service that also supports OAuth token exchange [RFC8693] for agent authentication SHOULD recognize the attribute "oAuthClientIdentifiers".

* entitlements: A list of entitlements for the agentic identity that represent a thing the agentic identity has. This attribute is analogous to the "entitlements" attribute of a user as described in section 4.1.2 of [RFC7643].

* groups: A list of groups to which the agentic identity belongs, either through direct membership, through nested groups, or dynamically calculated. This attribute is analogous to the "groups" attribute of a user as described in section 4.1.2 of [RFC7643].

* oAuthClientIdentifiers: Each value of the attribute is a complex type that describes the OAuth parameters of an agentic identity, for agentic identities that will be authenticating to a service using OAuth token exchange [RFC8693]. Support for this attribute is OPTIONAL. This attribute has six string-valued sub-attributes.

  - audiences: The values of this sub-attribute MAY be present. They are included by the SCIM server in a POST, GET or other response. The format of each value is defined as that of the "aud" claim of section 4.1.3 of [RFC7519].

  - clientId: The value of this sub-attribute is a client identifier, as described of section 2.2 of [RFC6749]. It is returned by the SCIM server. They are included by the SCIM server in a POST, GET or other response.

  - description: An OPTIONAL human-readable string that further describes the oAuth client identity.

  - issuer: The identity of the identity provider of the agent. The format of the value is defined as that of "iss" claim of section 4.1.1 of [RFC7519].

  - name: A human-readable name for the OAuth client identity that will be be used by the agent.

  - subject: The identifier of the agent within the identity provider. The format of the value is defined as that of the "sub" claim of section 4.1.2 of [RFC7519].

* owners: A list of the responsible parties for an agentic identity. Each value is a complex type that allows referencing the "id" attribute of a user, a group or other resource already known to the SCIM server. Each value has the following three string sub-attributes.

  - value: The "id" of the SCIM resource representing the an owner of an agentic identity. RECOMMENDED.

  - $ref: The URI of the SCIM resource representing an owner of an agentic identity. RECOMMENDED.

  - displayName: The displayName of the agentic identity’s owner. This attribute is OPTIONAL, and mutability is "readOnly".

* roles: A list of roles for the agentic identity. This attribute is analogous to the "roles" attribute of a user as described in section 4.1.2 of [RFC7643].

3.3. AgenticIdentity Resource Schema

The AgenticIdentity resource type is for Agentic identity resources. The schema for AgenticIdentity is identified using the following schema URI: "urn:ietf:params:scim:schemas:core:2.0:AgenticIdentity".

The following is a non-normative example of the SCIM schema representation of an agentic identity in JSON format. Long URL values have been trimmed for formatting.

```
{
 "schemas":[
   "urn:ietf:params:scim:schemas:core:2.0:AgenticIdentity"
 ],
 "id": "95cfaafb-0827-4c60-8236-523ad04b3cba",
 "agenticApplicationId":"8bb1afd8-ae68-40cf-8d53-c7f39ad3d0db",
 "displayName":"Agent for tour guides",
 "externalId":"67890",
 "oAuthClientIdentifiers":[
   {
       "audiences":["https://api.example.com"],
       "issuer":"https://oidc.example.com",
       "name":"an agent",
       "subject":"agent",
       "description":"An agent",
       "clientId": "c002"
   }
 ],
 "groups":[
  {
    "value": "e9e30dba-f08f-4109-8486-d5c6a331660a",
    "$ref":"https://example.com/v2/Groups/e9e...-d5c6a331660a",
    "display": "Tour Guides"
  },
  {
    "value": "9ce138e5-7296-4e3a-94a0-1ea8ce6d6aff",
    "$ref": "https://example.com/v2/Groups/9ce1...-1ea8ce6d6aff",
    "display": "Agentic identities"
  }
 ],
 "meta": {
   "resourceType":"AgenticIdentity"
 }
}
```


3.4. Updates to Existing Schema

To allow an agentic identity to be a member of a group, this memo augments the definition of the "members" attribute of [RFC7643] as follows:

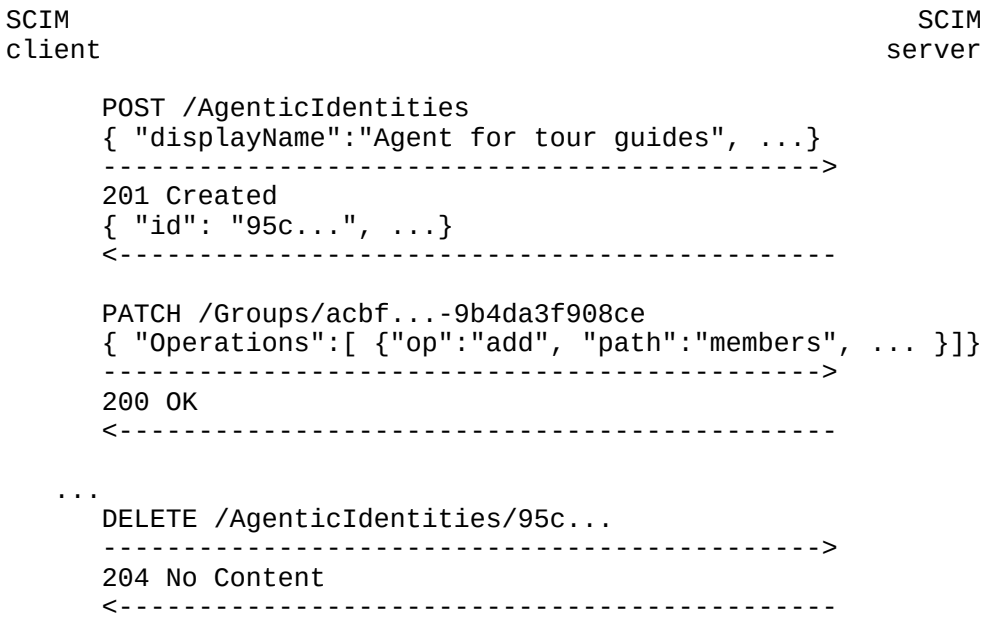
* allow the referenceTypes of the members "$ref" sub-attribute to also refer to an AgenticIdentity

* allow the canonicalValues of the members "type" sub-attribute to also allow for "AgenticIdentity"

4. Operations on an Agentic Identity

A SCIM client and SCIM server exchange agentic identity resources using the SCIM protocol of section 3 of [RFC7644]. Support for bulk operations, as described in section 3.7 of [RFC7644] is OPTIONAL. How the SCIM client authenticates to the SCIM server and is authorized by the SCIM server to perform protocol operations for agentic identities is outside the scope of this document.

The following is a non-normative example of a SCIM client using two SCIM operations, to create an agentic identity record in the SCIM server and then add the agentic identity to a group, and then using a SCIM operation to remove that agentic identity from the SCIM server.



4.1. Agentic Identity Creation

To inform a service of an agent’s identity, a SCIM client sends a POST request containing a "AgenticIdentity" to the "/AgenticIdentities" endpoint. The POST request MUST include the following attributes "schemas" and MAY include the following attributes "externalId", "active", "agenticApplicationId", "description", "displayName", "entitlements", "oAuthClientIdentifiers", "owners", "roles".

In response, a SCIM server signals successful creation with an HTTP status code 201 (Created) and returns a representation of the resource created. The response MUST include the following attributes "id", and "meta". In addition, if the request included the "oAuthClientIdentifiers" attribute, then values of the "issuer", "name" and "subject" sub-attributes MUST be included by the SCIM client in each attribute value, and the response MUST include the "oAuthClientIdentifiers" attribute.

4.2. Agentic Identity Retrieval

A SCIM client can retrieve an agentic identity resource using the patterns shown in [RFC7644] section 3.4.

4.3. Agentic Identity Updates

An agentic identity resource’s attributes can be modified by a SCIM client using the patterns shown in [RFC7644] section 3.5.

If the "oAuthClientIdentifiers" attribute is supplied by a SCIM client in a PUT or PATCH request to update an AgenticIdentity, then values of the "issuer", "name" and "subject" sub-attributes MUST be included by the SCIM client in each attribute value.

4.4. Update Group Membership of an Agentic Identity

A group membership of an agentic identity can be changed by a SCIM client updating the "members" of the group to add, remove or replace the agentic identity as one of the values. The following is an example representation of a PATCH request for a group to add an agentic identity as a member, showing the basic JSON structure (non-normative):

```
PATCH /Groups/acbf3ae7-8463-...-9b4da3f908ce

{ "schemas":
    ["urn:ietf:params:scim:api:messages:2.0:PatchOp"],
  "Operations":[
    {
     "op":"add",
     "path":"members",
     "value":[
      {
        "display": "Agent for tour guides",
        "$ref":
"https://example.com/v2/AgenticIdentities/95cfaafb...4b3cba",
        "value": "95cfaafb-0827-4c60-8236-523ad04b3cba"
      }
     ]
    }
  ]
}
```

4.5. Agentic Identity Deletion

A SCIM client can retrieve an agentic identity resource using the patterns shown in [RFC7644] section 3.6.

5. Security Considerations

SCIM data is intended to be exchanged using the SCIM protocol. It is important when handling data to implement the security considerations outlined in Section 7 of [RFC7644].

When the agentic identity is intended to be used in subsequent OAuth interactions, the guidance from section 10 of [RFC6749] also applies, and when it is intended to be used with OAuth token exchange interactions, the guidance from section 5 of [RFC8693] also applies.

5.1. Privacy

The text of this privacy section is derived from the corresponding privacy section of [RFC7643].

Information should be shared on an as-needed basis. A SCIM client should limit information to what it believes a SCIM server requires, and a SCIM server should only accept information it needs. Clients and servers should take into consideration that sensitive information is being conveyed across technical (e.g., protocol and applications), administrative (e.g., organizational, corporate), and jurisdictional boundaries. In particular, information security and privacy must be considered.

Security service level agreements for the handling of these attributes are beyond the scope of this document but are to be carefully considered by implementers and deploying organizations.

Please see the Privacy Considerations section of [RFC7644] for more protocol-specific considerations regarding the handling of SCIM information.

6. IANA Considerations

6.1. New Schema

When published as an RFC, the IANA is requested to add the following to the "SCIM Schema URIs for Data Resources" established in [RFC7643]:

Schema URI	Name	Reference
urn:ietf:params:scim:schemas:core:2.0:AgenticIdentity	Agentic Identity Resource	This memo, section 3

Table 1: SCIM Schema URI for Agentic Identity

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/rfc/rfc6749>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/rfc/rfc7519>.

[RFC7643] Hunt, P., Ed., Grizzle, K., Wahlstroem, E., and C. Mortimore, "System for Cross-domain Identity Management: Core Schema", RFC 7643, DOI 10.17487/RFC7643, September 2015, <https://www.rfc-editor.org/rfc/rfc7643>.

[RFC7644] Hunt, P., Ed., Grizzle, K., Ansari, M., Wahlstroem, E., and C. Mortimore, "System for Cross-domain Identity Management: Protocol", RFC 7644, DOI 10.17487/RFC7644, September 2015, <https://www.rfc-editor.org/rfc/rfc7644>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/rfc/rfc8259>.

7.2. Informative References

[RFC8693] Jones, M., Nadalin, A., Campbell, B., Ed., Bradley, J., and C. Mortimore, "OAuth 2.0 Token Exchange", RFC 8693, DOI 10.17487/RFC8693, January 2020, <https://www.rfc-editor.org/rfc/rfc8693>.

Appendix A. Changes From Earlier Versions

* Changes in -01: Added missing page header and table labels; no protocol or data model changes.

* -00: Initial revision.

Acknowledgments

The editor would like to acknowledge the contribution and work of the authors of the SCIM RFCs [RFC7643] and [RFC7644] and of other SCIM Internet-Drafts, the participants of the IETF SCIM WG, and the SCIM Community.

Author’s Address

Mark Wahl
Microsoft

Email: mwahl@microsoft.com