

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: April 26, 2022

P. Hunt, Ed.  
IndependentId  
October 23, 2021

SCIM Protocol: Multi-Value Filtering Extension  
draft-hunt-scim-mv-filtering-00

Abstract

The System for Cross-Domain Identity Management (SCIM) specifications define a profile of HTTP protocol and a schema that enable managing identities in cross-domain scenarios. This specification extends SCIM protocol resource retrieval and query functions to enable paging and filtering of multi-valued attributes in a SCIM service provider resource.

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 April 26, 2022.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction and Overview . . . . .	2
1.1. Intended Audience . . . . .	2
1.2. Notational Conventions . . . . .	2
1.3. Definitions . . . . .	3
2. Multi-Value Paging Extension . . . . .	3
3. Service Provider Configuration Feature Discovery . . . . .	9
4. Security Considerations . . . . .	10
5. Privacy Considerations . . . . .	10
6. IANA Considerations . . . . .	10
7. Normative References . . . . .	10
Appendix A. Acknowledgments . . . . .	10
Appendix B. Change Log . . . . .	10
Author's Address . . . . .	11

## 1. Introduction and Overview

SCIM Protocol [RFC7644] is an application-level, HTTP protocol for provisioning and managing identity data on the web and in cross-domain environments such as enterprise to cloud, or inter-cloud scenarios. The protocol supports creation, modification, retrieval, and discovery of core identity resources such as Users and Groups, as well as custom resources and resource extensions.

The definition of resources, attributes, and overall schema are defined in the SCIM Core Schema document (see [RFC7643]).

This specification extends SCIM resource retrieval and query functions to enable filtering and paging of multi-valued attributes. For example, attributes that may contain large numbers of values such as a SCIM Group.

### 1.1. Intended Audience

This document is intended as a guide to extend SCIM protocol usage for both SCIM HTTP service providers and HTTP clients who may provision information to service providers or retrieve information from them.

### 1.2. Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]. These

keywords are capitalized when used to unambiguously specify requirements of the protocol or application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

For purposes of readability examples are not URL encoded. Implementers MUST percent encode URLs as described in Section 2.1 of [RFC3986].

Throughout this documents all figures may contain spaces and extra line-wrapping for readability and space limitations. Similarly, some URI's contained within examples, have been shortened for space and readability reasons.

### 1.3. Definitions

This specification uses the definitions from the SCIM Schema Specification [RFC7643] and the SCIM Protocol Specification [RFC7644].

## 2. Multi-Value Paging Extension

Detecting the availability of multi-valued attribute filtering and paging extension is covered in Section 3.

When supported, returned values for multi-valued attributes can be filtered or paged using filters and/or paging parameters appended to attributes specified in the SCIM "attributes" parameter. Attributes listed in the attributes parameter MAY be appended with value qualifiers using square brackets("[ ]") that contains a "valFilter" (see Figure 1 [RFC7644]), paging parameters (see Section 3.9 [RFC7644]), or a combination of both separated by the "&" character.

In order to qualify specific attributes without changing the default list of attributes returned for a query, an asterix "\*" MAY be used in the attributes parameter to indicate the default set of attributes is to be returned in addition to any specific attributes listed. For example: "attributes=\*,members[type eq \"user\"]" specifies all default attributes are to be returned and only values of "members" which have "type" set to "user".

When an attribute has a multi-value filter or paging qualifier, the service provider SHALL include additional "meta" sub-attributes (see Section 3.1 of [RFC7643]). The name of the multi-valued attribute plus the String "cnt" is used to indicate the count of attribute values available expressed as an Integer (see Section 2.3.4 of [RFC7643]). When a "valFilter" expression is used, the number SHALL

indicate the total number of matches that may be returned based on the filter. When no filter expression is specified, the number SHALL indicate the total number of values. For an example, see "emails.cnt" in Figure 2. This count indicates that there is only one value with "type" equal to "work".

When "startIndex" is used as an attribute paging qualifier and the value is greater than the number of values, the server SHALL omit the attribute from the result to indicate no values exist at that index.

In the following example, a user is returned, but only "work" emails are to be returned.

```
GET /Users/2819c223-7f76-453a-919d-413861904646? \
  attributes=*,emails[type eq \"work\"]
Host: example.com
Accept: application/scim+json
Authorization: Bearer h480djs93hd8
```

Figure 1: Using a filter to return only work email values

The service provider responds with:

```
HTTP/1.1 200 OK
Content-Type: application/scim+json
Location:
  https://example.com/v2/Users/2819c223-7f76-453a-919d-413861904646
ETag: W/"f250dd84f0671c3"
```

```
{
  "schemas":["urn:ietf:params:scim:schemas:core:2.0:User"],
  "id":"2819c223-7f76-453a-919d-413861904646",
  "externalId":"bjensen",
  "meta":{
    "resourceType":"User",
    "created":"2011-08-01T18:29:49.793Z",
    "lastModified":"2011-08-01T18:29:49.793Z",
    "location":
      "https://example.com/v2/Users/2819c223-7f76-453a-919d-413861904646",
    "version":"W\\/\\"f250dd84f0671c3\\\"",
    "emails.cnt":1
  },
  "name":{
    "formatted":"Ms. Barbara J Jensen III",
    "familyName":"Jensen",
    "givenName":"Barbara"
  },
  "userName":"bjensen",
  "phoneNumbers":[
    {
      "value":"555-555-8377",
      "type":"work"
    }
  ],
  "emails":[
    {
      "value":"bjensen@example.com",
      "type":"work"
    }
  ]
}
```

Figure 2: Response with filtered emails attribute

In the following example, all Groups are searched and only Groups whose name starts with "Group" are selected. Additionally, the members attribute values are filtered return only member values with "type" equal to "groups" (as in sub-groups) returning only the first 5 values using the attributes paging qualifying parameters.

```
GET /v2/Groups?filter=displayName sw 'Group' & \
    attributes=*,members[type eq \"Group\"&count=5&startIndex=1]
Host: example.com
Accept: application/scim+json
Authorization: Bearer h480djs93hd8
```

Figure 3: Querying multiple groups with attribute qualifiers

The server responds with 2 matched resources. The first resource only has one Group member value, while the second resource has 7 member values and has been limited to the first 5 members per the "count" paging parameter .

```
HTTP/1.1 200 OK
Content-Type: application/scim+json

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:ListResponse"],
  "totalResults": 2,
  "Resources": [
    {
      "id": "c3a26dd3-27a0-4dec-a2ac-ce211e105f97",
      "schemas": ["urn:ietf:params:scim:schemas:core:2.0:Group"],
      "displayName": "Group A",
      "meta": {
        "resourceType": "Group",
        "created": "2011-08-01T18:29:49.793Z",
        "lastModified": "2011-08-01T18:29:51.135Z",
        "location":
"https://example.com/v2/Groups/c3a26dd3-27a0-4dec-a2ac-ce211e105f97",
        "version": "W\\\\"mvwNGaxB5SDq074p\\\"",
        "members.cnt":1
      },
      "members": [
        {
          "value": "6c5bb468-14b2-4183-baf2-06d523e03bd3",
          "$ref":
"https://example.com/v2/Groups/6c5bb468-14b2-4183-baf2-06d523e03bd3",
          "type": "Group"
        }
      ]
    },
  ],
}
```

```
{
  "id": "6c5bb468-14b2-4183-baf2-06d523e03bd3",
  "schemas": ["urn:ietf:params:scim:schemas:core:2.0:Group"],
  "displayName": "Group B",
  "meta": {
    "resourceType": "Group",
    "created": "2011-08-01T18:29:50.873Z",
    "lastModified": "2011-08-01T18:29:50.873Z",
    "location":
      "https://example.com/v2/Groups/6c5bb468-14b2-4183-baf2-06d523e03bd3",
    "version": "W\\\\"wGB85s2QJMjiNnuI\\\"",
    "members.cnt": 7
  },
  "members": [
    {
      "value": "c3a26dd3-27a0-4dec-a2ac-ce211e105f97",
      "$ref":
        "https://example.com/v2/Groups/c3a26dd3-27a0-4dec-a2ac-ce211e105f97",
      "type": "Group"
    }
    {
      "value": "596ec090-2f66-4d3e-ad4c-68d9ac05ad53",
      "$ref":
        "https://example.com/v2/Groups/596ec090-2f66-4d3e-ad4c-68d9ac05ad53",
      "type": "Group"
    }
    {
      "value": "aaf4c421-ceba-4ce0-a119-3d62418f5f9f",
      "$ref":
        "https://example.com/v2/Groups/aaf4c421-ceba-4ce0-a119-3d62418f5f9f",
      "type": "Group"
    }
    {
      "value": "58b64358-82e7-4a77-a8eb-9c6d644f9752",
      "$ref":
        "https://example.com/v2/Groups/58b64358-82e7-4a77-a8eb-9c6d644f9752",
      "type": "Group"
    }
    {
      "value": "3e32ee8c-246c-42ab-a750-2c2e84d57f1f",
      "$ref":
        "https://example.com/v2/Groups/3e32ee8c-246c-42ab-a750-2c2e84d57f1f",
      "type": "Group"
    }
  ]
}
```

Figure 4: Returning multiple results with paged attribute values

In Figure 3 the client may observe that the number of matches available for the second Group (whose "id" is "6c5bb468-14b2-4183-baf2-06d523e03bd3") is 7. In Figure 4, the client may return the second page, by repeating the query with "startIndex" set to 6.

In the following example, paging of member values of a specific group is requested.

```
GET /v2/Groups/6c5bb468-14b2-4183-baf2-06d523e03bd3? \
    attributes=*,members[type eq \"Group\"&count=5&startIndex=6]
Host: example.com
Accept: application/scim+json
Authorization: Bearer h480djs93hd8
```

Figure 5: Query returning the second page of values for an attribute



```
HTTP/1.1 200 OK
Content-Type: application/scim+json
Location:
  https://example.com/v2/Groups/e9e30dba-f08f-4109-8486-d5c6a331660a
ETag: W/"lha5bbazU3fNvfe5"

{
  "id": "6c5bb468-14b2-4183-baf2-06d523e03bd3",

  "schemas": ["urn:ietf:params:scim:schemas:core:2.0:Group"],
  "displayName": "Group B",
  "meta": {
    "resourceType": "Group",
    "created": "2011-08-01T18:29:50.873Z",
    "lastModified": "2011-08-01T18:29:50.873Z",
    "location":
      "https://example.com/v2/Groups/6c5bb468-14b2-4183-baf2-06d523e03bd3",
    "version": "W\\\\"wGB85s2QJMjiNnuI\\",
    "members.cnt": 7
  },

  "members": [
    {
      "value": "596ec090-2f66-4d3e-ad4c-68d9ac05ad53",
      "$ref":
        "https://example.com/v2/Groups/596ec090-2f66-4d3e-ad4c-68d9ac05ad53",
      "type": "Group"
    }
    {
      "value": "2e6afed5-282d-4563-83dc-9ef7183b0003",
      "$ref":
        "https://example.com/v2/Groups/2e6afed5-282d-4563-83dc-9ef7183b0003",
      "type": "Group"
    }
  ]
}
```

Figure 6: Returning the second page of values for an attribute

### 3. Service Provider Configuration Feature Discovery

Multi-value paging support may be determined by querying the `/ServiceProviderConfig` endpoint and looking up the Boolean attribute `"mvpaging"` indicating support for multi-valued paging and filtering.

#### 4. Security Considerations

To be completed

#### 5. Privacy Considerations

To be completed.

#### 6. IANA Considerations

No IANA considerations.

#### 7. 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/info/rfc2119>>.
- [RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <<https://www.rfc-editor.org/info/rfc3986>>.
- [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/info/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/info/rfc7644>>.

#### Appendix A. Acknowledgments

This draft is an updated submission based on the original ID draft-hunt-scim-mv-paging-00 contributed by Phil Hunt and Gregg Wilson.

#### Appendix B. Change Log

[[This section to be removed prior to publication as an RFC]]

Draft 00 - PH - Initial draft

Author's Address

Phil Hunt (editor)  
Independent Identity Inc.

Email: [phil.hunt@independentid.com](mailto:phil.hunt@independentid.com)

SCIM  
Internet-Draft  
Intended status: Informational  
Expires: 25 April 2022

D. Zollner  
Microsoft  
22 October 2021

SCIM Verified Domains Extension  
draft-zollner-scim-domain-extension-00

Abstract

The System for Cross-domain Identity Management (SCIM) protocol supports creation and management of identity resources such as users between a client and a service provider. In some instances, a SCIM service provider may maintain a list of DNS domains that an organization using that service has registered for their exclusive use with the service. This registration of domains is frequently tied to some form of ownership verification for each domain. This document defines an extension to the SCIM protocol introducing a new 'VerifiedDomains' resource type in order to allow a SCIM client to confirm what domains have had ownership verified by the SCIM service provider, as well as some information about whether the User resource's userName and emails attributes require domain verification in order for a value to possess that domain suffix.

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 25 April 2022.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Conventions and Definitions . . . . .	3
3. IANA Considerations . . . . .	3
4. Definitions . . . . .	3
5. Verified Domains . . . . .	3
5.1. ServiceProviderConfig Extension . . . . .	3
5.2. VerifiedDomains Schema Extension . . . . .	4
5.3. Sample Requests . . . . .	4
5.3.1. Retrieving all verified domains . . . . .	4
5.3.2. Querying verified domains by domainName value . . . . .	5
6. Schema BNF . . . . .	6
7. Normative References . . . . .	7
Acknowledgments . . . . .	7
Author's Address . . . . .	7

## 1. Introduction

The System for Cross-domain identity Management (SCIM) protocol RFC7644 (<https://datatracker.ietf.org/doc/html/rfc7644>) supports creation, modification, and deletion of core identity resources. To allow for efficient interactions between SCIM clients and multi-customer SCIM service providers such as SaaS applications, the client may wish to avoid sending creation or update requests that are already known to contain attribute values that will be rejected by the SCIM service provider.

A common source of creation and update failures when interacting with SCIM service providers for SaaS applications is when the SCIM client attempts to create or update the `userName` (adhering to RFC5321 (<https://datatracker.ietf.org/doc/html/rfc5321>) format) or `emails` attribute on a user and the SCIM client provides a value with a domain suffix that is not verified in the customer's tenant in the service represented by the SCIM service provider.

This document defines a simple extension to the SCIM protocol and core schema that adds support for a "VerifiedDomains" resource type that can be queried to retrieve a list of verified domains in the

SCIM service provider's environment so that a SCIM client can utilize this information to apply additional logic and avoid sending requests that will fail.

## 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. IANA Considerations

This document has no IANA actions.

## 4. Definitions

Domain: At least a Second Level Domain (SLD) and a Top Level Domain(TLD) registered with public DNS registrars and ICANN. Further expansion to Third Level Domains (aka subdomains) are also permitted.

## 5. Verified Domains

A SCIM endpoint supporting the Domains extension MUST implement a /VerifiedDomains resource as outlined in this document. This extension is written with only the HTTP/REST GET method required, as the data provided by the SCIM service provider is intended to be read-only. POST, PUT, PATCH and DELETE requests to the /VerifiedDomains resource MUST result in a HTTP Bad Request (400).

### 5.1. ServiceProviderConfig Extension

SCIM endpoints that support the Verified Domains extension MUST advertise this support in the ServiceProviderConfig endpoint as defined:

**verifiedDomains**

A complex type that specifies Verified Domains configuration options. REQUIRED.

**supported**

A boolean type that specifies if the Verified Domains extension is supported.

**userNameProperties**

A complex type that specifies if the expected value for `userName` follows the RFC5321 format, and if accepted values following RFC5321 require a verified domain suffix.

**emailsVerifiedDomainRequired**

A boolean type that specifies if accepted values for emails require a verified domain suffix.

## 5.2. VerifiedDomains Schema Extension

Any SCIM service provider that supports the Verified Domains extension MUST implement the VerifiedDomains resource type with the `urn:ietf:params:scim:schemas:2.0:VerifiedDomain` schema defined in this section:

The following singular attributes are defined:

**domainName**

A string attribute containing at least the Second Level Domain (SLD) and Top Level Domain (TLD) of a domain verified in the SCIM service provider's system. Subdomains (Third Level Domains and below) are supported as well. REQUIRED.

**allowSubdomains**

A boolean attribute set to true for any verified domain resource that should be interpreted by the client to include all subdomains. REQUIRED.

**verifiedDate**

A `dateTime` attribute indicating the date and time at which the domain resource was verified in the SCIM service provider's system. OPTIONAL.

## 5.3. Sample Requests

### 5.3.1. Retrieving all verified domains

#### 5.3.1.1. Request

```
GET /VerifiedDomains
Host: example.com
Accept: application/scim+json
Authorization: Bearer 123456abcd
```

#### 5.3.1.2. Response

```
HTTP/1.1 200 OK
Content-Type: application/scim+json
```

```
{
  "schemas":["urn:ietf:params:scim:api:messages:2.0:ListResponse"],
  "totalResults":2,
  "itemsPerPage":100,
  "startIndex":1,
  "Resources":[
    {
      "id":"1",
      "domainName":"contoso.com",
      "allowSubdomains":true,
    },
    {
      "id":"2",
      "domainName":"fabrikam.com",
      "allowSubdomains":true
    }
  ]
}
```

#### 5.3.2. Querying verified domains by domainName value

##### 5.3.2.1. Request

```
GET /VerifiedDomains?filter=domainName contains "contoso.com"
Host: example.com
Accept: application/scim+json
Authorization: Bearer 123456abcd
```

##### 5.3.2.2. Response



HTTP/1.1 200 OK

Content-Type: application/scim+json

```
{
  "schemas":["urn:ietf:params:scim:api:messages:2.0:ListResponse"],
  "totalResults":1,
  "itemsPerPage":100,
  "startIndex":1,
  "Resources":[
    {
      "id":"1",
      "domainName":"contoso.com",
      "allowSubdomains":true
    }
  ]
}
```

## 6. Schema BNF

```
[
  {
    "id" : "urn:ietf:params:scim:schemas:2.0:VerifiedDomain",
    "name" : "Domain",
    "description" : "DNS Domains",
    "attributes" : [
      {
        "name" : "domainName"
        "type" : "string"
        "multiValued" : false
        "description" : "Value for a domain name registered and
        optionally verified in the SCIM service provider. The
        value should represent a DNS domain name such as
        'contoso.com' and optionally may contain
        one or more subdomain levels such as 'scim.contoso.com'.
        REQUIRED.",
        "required" : true,
        "caseExact" : false,
        "mutability" : "readOnly",
        "returned" : "default",
        "uniqueness" : "server"
      },
      {
        "name" : "allowSubdomains",
        "type" : "boolean",
        "multiValued" : false,
        "description" : "A Boolean value indicating if subdomains
        below the domain specified in domainName should be
        treated identically to the value provided in domainName."
      }
    ]
  }
]
```

```
    OPTIONAL",
    "required" : true,
    "mutability" : "readOnly",
    "returned" : "default"
  },
  {
    "name" : "verifiedDate",
    "type" : "dateTime",
    "multiValued" : false,
    "description" : "An optional dateTime value indicating
the time at which the domain specified in domainName
was verified. OPTIONAL",
    "required" : false
    "mutability" : "readOnly",
    "returned" : "default"
  }
]
"meta" : {
  "resourceType" : "Schema",
  "location" :
"/v2/Schemas/urn:ietf:params:scim:schemas:2.0:VerifiedDomain"
}
]
```

## 7. 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/info/rfc2119>>.
- [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/info/rfc8174>>.

## Acknowledgments

TODO acknowledge.

## Author's Address

Danny Zollner  
Microsoft

Email: [danny@zollnerd.com](mailto:danny@zollnerd.com)

SCIM  
Internet-Draft  
Intended status: Informational  
Expires: 25 April 2022

D. Zollner  
Microsoft  
22 October 2021

SCIM Roles and Entitlements Extension  
draft-zollner-scim-roles-entitlements-extension-00

Abstract

The System for Cross-domain Identity Management (SCIM) protocol's schema RFC RFC7643 (<https://datatracker.ietf.org/doc/html/rfc7643>) defines the complex core schema attributes "roles" and "entitlements". For both of these concepts, frequently only a predetermined set of values are accepted by a SCIM service provider. The values that are accepted may vary per customer or tenant based on customizable configuration in the service provider's application or based on other criteria such as what services have been purchased. This document defines an extension to the SCIM 2.0 standard to allow SCIM service providers to represent available data pertaining to roles and entitlements so that SCIM clients can consume this information and provide easier management of role and entitlement assignments.

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 25 April 2022.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction	2
2. Conventions and Definitions	3
3. IANA Considerations	3
4. Roles and Entitlements	3
4.1. ServiceProviderConfig Extension	3
4.2. Roles Resource Schema	4
4.3. Entitlements Resource Schema	5
4.4. Sample Requests	5
4.4.1. Retrieving all roles	5
4.4.2. Retrieving all entitlements	6
5. Roles Schema BNF	7
6. Entitlements Schema BNF	8
7. Normative References	10
Acknowledgments	10
Author's Address	10

## 1. Introduction

The System for Cross-domain Identity Management (SCIM) protocol's schema RFC RFC7643 (<https://datatracker.ietf.org/doc/html/rfc7643>) defines the complex core schema attributes "roles" and "entitlements". For both of these concepts, frequently only a predetermined set of values are accepted by a SCIM service provider. Available roles and entitlements may change based on a variety of factors, such as what features are enabled or what customizations have been made in a specific instance of a multi-tenant application. The core SCIM 2.0 RFC documents (RFC7642, RFC7643 and RFC 7644) do not provide a method for retrieving the available roles or entitlements as part of the SCIM 2.0 standard.

In order to allow for SCIM clients to avoid easily predictable errors when interacting with SCIM service providers, this document aims to provide a method for SCIM service providers to provide data on what roles and/or entitlements are available so that SCIM clients can consume this data to more efficiently manage resources between directories.

## 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. IANA Considerations

This document has no IANA actions.

## 4. Roles and Entitlements

The Roles and Entitlements SCIM Extension consists of two new resource types, /Roles and /Entitlements, as well as accompanying ServiceProviderConfig details to advertise support for this extension.

### 4.1. ServiceProviderConfig Extension

SCIM endpoints that have implemented one or both of the endpoints from this extension MUST advertise which elements are implemented in the ServiceProviderConfig endpoint as defined:

#### RolesAndEntitlements

A complex type that specifies Roles and Entitlements extension configuration options. REQUIRED.

#### roles

A complex type that specifies configuration options related to the Roles resource type. REQUIRED.

#### enabled

A boolean type that indicates if the SCIM service provider supports the /Roles endpoint defined in this extension. REQUIRED.

#### multipleRolesSupported

A boolean type that indicates if the SCIM service provider supports multiple values for the "roles" attribute on the User resource. REQUIRED.

#### primarySupported

A boolean type that indicates if the SCIM service provider supports the "primary" sub-attribute for the "roles" attribute on the User resource. REQUIRED.

**typeSupported**

A boolean type that indicates if the SCIM service provider supports the "type" sub-attribute for the "roles" attribute on the User resource. REQUIRED.

**entitlements**

A complex type that specifies configuration options related to the Entitlements resource type. REQUIRED.

**enabled**

A boolean type that indicates if the SCIM service provider supports the /Entitlements endpoint defined in this extension. REQUIRED.

**multipleEntitlementsSupported**

A boolean type that indicates if the SCIM service provider supports multiple values for the "entitlements" attribute on the User resource. REQUIRED.

**primarySupported**

A boolean type that indicates if the SCIM service provider supports the "primary" sub-attribute for the "entitlements" attribute on the User resource. REQUIRED.

**typeSupported**

A boolean type that indicates if the SCIM service provider supports the "type" sub-attribute for the "entitlements" attribute on the User resource. REQUIRED.

#### 4.2. Roles Resource Schema

The /Roles resource type has a schema consisting of most of the attributes defined for the User resource's complex attribute "roles" in RFC7643 (<https://datatracker.ietf.org/doc/html/rfc7643>), as well as an additional "Enabled" attribute so that SCIM service providers can indicate if the role is currently enabled and intended for use in their service.

The following singular attributes are defined:

**value**

The value of a role. REQUIRED.

**display**

A human-readable name, primarily used for display purposes.  
OPTIONAL.

**type**

A label indicating the role's function. OPTIONAL

**enabled**

A boolean type that indicates if the role is enabled and usable  
in the SCIM service provider's system. REQUIRED.

#### 4.3. Entitlements Resource Schema

The /Entitlements resource type has a schema consisting of most of the attributes defined for the User resource's complex attribute "entitlements" in RFC7643 (<https://datatracker.ietf.org/doc/html/rfc7643>), as well as an additional "Enabled" attribute so that SCIM service providers can indicate if the entitlement is currently enabled and intended for use in their service.

The following singular attributes are defined:

**value**

The value of an entitlement. REQUIRED.

**display**

A human-readable name, primarily used for display purposes.  
OPTIONAL.

**type**

A label indicating the entitlement's function. OPTIONAL.

**enabled**

A boolean type that indicates if the entitlement is enabled  
and usable in the SCIM service provider's system. REQUIRED.

#### 4.4. Sample Requests

##### 4.4.1. Retrieving all roles

###### 4.4.1.1. Request

```
GET /Roles
Host: example.com
Accept: application/scim+json
Authorization: Bearer 123456abcd
```

#### 4.4.1.2. Response

```
HTTP/1.1 200 OK
Content-Type: application/scim+json
```

```
{
  "schemas":["urn:ietf:params:scim:api:messages:2.0:ListResponse"],
  "totalResults":3,
  "itemsPerPage":100,
  "startIndex":1,
  "Resources":[
    {
      "value":"admin"
      "display":"Administrator"
      "enabled":True
    },
    {
      "value":"user"
      "display":"User"
      "enabled":True
    },
    {
      "value":"teamlead"
      "display":"Team Leader"
      "enabled":True
    }
  ]
}
```

#### 4.4.2. Retrieving all entitlements

##### 4.4.2.1. Request

```
GET /Entitlements
Host: example.com
Accept: application/scim+json
Authorization: Bearer 123456abcd
```

##### 4.4.2.2. Response



HTTP/1.1 200 OK

Content-Type: application/scim+json

```
{
  "schemas":["urn:ietf:params:scim:api:messages:2.0:ListResponse"],
  "totalResults":4,
  "itemsPerPage":100,
  "startIndex":1,
  "Resources":[
    {
      "value":"1"
      "display":"Printing"
      "enabled":True
    },
    {
      "value":"2"
      "display":"Scanning"
      "enabled":True
    },
    {
      "value":"3"
      "display":"Copying"
      "enabled":True
    },
    {
      "value":"4"
      "display":"Collating"
    }
  ]
}
```

#### 5. Roles Schema BNF

```
[
  {
    "id" : "urn:ietf:params:scim:schemas:2.0:Roles",
    "name" : "Role",
    "description" : "Roles available for use with the User
resource's 'roles' attribute",
    "attributes" : [
      {
        "name" : "value",
        "type" : "string",
        "multiValued" : false,
        "description" : "The value of a role",
        "required" : true,
        "caseExact" : false,
        "mutability" : "readOnly",
```

```
        "returned" : "default",
        "uniqueness" : "server"
    },
    {
        "name" : "display",
        "type" : "string",
        "multiValued" : false,
        "description" : "A human-readable name, primarily
        used for display purposes.",
        "required" : false,
        "caseExact" : false,
        "mutability" : "readOnly",
        "returned" : "default",
        "uniqueness" : "server"
    },
    {
        "name" : "type",
        "type" : "string",
        "multiValued" : false,
        "description" : "A label indicating the role's
        function.",
        "required" : false,
        "caseExact" : false,
        "mutability" : "readOnly",
        "returned" : "default",
        "uniqueness" : "server"
    },
    {
        "name" : "enabled",
        "type" : "boolean",
        "multiValued" : false,
        "description" : "A boolean type that indicates if the
        role is enabled and usable in the SCIM service
        provider's system.",
        "required" : true,
        "caseExact" : false,
        "mutability" : "readOnly",
        "returned" : "default"
    }
  ]
}
```

## 6. Entitlements Schema BNF

```
[
  {
    "id" : "urn:ietf:params:scim:schemas:2.0:Entitlements",
    "name" : "Entitlement",
    "description" : "Entitlements available for use with the User
resource's 'entitlements' attribute",
    "attributes" : [
      {
        "name" : "value",
        "type" : "string",
        "multiValued" : false,
        "description" : "The value of an entitlement",
        "required" : true,
        "caseExact" : false,
        "mutability" : "readOnly",
        "returned" : "default",
        "uniqueness" : "server"
      },
      {
        "name" : "display",
        "type" : "string",
        "multiValued" : false,
        "description" : "A human-readable name, primarily
used for display purposes.",
        "required" : false,
        "caseExact" : false,
        "mutability" : "readOnly",
        "returned" : "default",
        "uniqueness" : "server"
      },
      {
        "name" : "type",
        "type" : "string",
        "multiValued" : false,
        "description" : "A label indicating the role's
function.",
        "required" : false,
        "caseExact" : false,
        "mutability" : "readOnly",
        "returned" : "default",
        "uniqueness" : "server"
      },
      {
        "name" : "enabled",
        "type" : "boolean",
        "multiValued" : false,
        "description" : "A boolean type that indicates if the
role is enabled and usable in the SCIM service"
      }
    ]
  }
]
```

```
        provider's system.",
        "required" : true,
        "caseExact" : false,
        "mutability" : "readOnly",
        "returned" : "default"
      }
    ]
  }
]
```

## 7. 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/info/rfc2119>>.
- [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/info/rfc8174>>.

## Acknowledgments

TODO acknowledge.

## Author's Address

Danny Zollner  
Microsoft

Email: [danny@zollnerd.com](mailto:danny@zollnerd.com)