

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: February 28, 2013

C. Mortimore, Ed.  
Salesforce  
P. Harding  
P. Madsen  
Ping  
T. Drake  
UnboundID  
August 27, 2012

**System for Cross-Domain Identity Management: Core Schema  
draft-ietf-scim-core-schema-00**

**Abstract**

The System for Cross-Domain Identity Management (SCIM) specification is designed to make managing user identity in cloud based applications and services easier. The specification suite builds upon experience with existing schemas and deployments, placing specific emphasis on simplicity of development and integration, while applying existing authentication, authorization, and privacy models. Its intent is to reduce the cost and complexity of user management operations by providing a common user schema and extension model, as well as binding documents to provide patterns for exchanging this schema using standard protocols. In essence, make it fast, cheap, and easy to move identity in to, out of, and around the cloud.

This document provides a platform neutral schema and extension model for representing users and groups in JSON and XML formats. This schema is intended for exchange and use with cloud service providers. Additional binding documents provide a standard REST API, SAML binding, and use cases.

**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 <http://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 February 28, 2013.

#### Copyright Notice

Copyright (c) 2012 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 (<http://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

<a href="#">1.</a>	<a href="#">Requirements Notation and Conventions</a>	<a href="#">4</a>
<a href="#">2.</a>	<a href="#">Overview</a>	<a href="#">4</a>
<a href="#">2.1.</a>	<a href="#">Definitions</a>	<a href="#">4</a>
<a href="#">3.</a>	<a href="#">SCIM Schema Structure</a>	<a href="#">5</a>
<a href="#">3.1.</a>	<a href="#">Attribute Data Types</a>	<a href="#">6</a>
<a href="#">3.1.1.</a>	<a href="#">String</a>	<a href="#">6</a>
<a href="#">3.1.2.</a>	<a href="#">Boolean</a>	<a href="#">6</a>
<a href="#">3.1.3.</a>	<a href="#">Decimal</a>	<a href="#">6</a>
<a href="#">3.1.4.</a>	<a href="#">Integer</a>	<a href="#">6</a>
<a href="#">3.1.5.</a>	<a href="#">DateTime</a>	<a href="#">6</a>
<a href="#">3.1.6.</a>	<a href="#">Binary</a>	<a href="#">7</a>
<a href="#">3.1.7.</a>	<a href="#">Complex</a>	<a href="#">7</a>
<a href="#">3.2.</a>	<a href="#">Multi-valued Attributes</a>	<a href="#">7</a>
<a href="#">4.</a>	<a href="#">Schema Extension Model</a>	<a href="#">8</a>
<a href="#">5.</a>	<a href="#">SCIM Core Schema</a>	<a href="#">8</a>
<a href="#">5.1.</a>	<a href="#">Common Schema Attributes</a>	<a href="#">8</a>
<a href="#">5.2.</a>	<a href="#">"schemas" Attribute</a>	<a href="#">10</a>
<a href="#">6.</a>	<a href="#">SCIM User Schema</a>	<a href="#">10</a>
<a href="#">6.1.</a>	<a href="#">Singular Attributes</a>	<a href="#">10</a>
<a href="#">6.2.</a>	<a href="#">Multi-valued Attributes</a>	<a href="#">12</a>
<a href="#">7.</a>	<a href="#">SCIM Enterprise User Schema Extension</a>	<a href="#">14</a>
<a href="#">8.</a>	<a href="#">SCIM Group Schema</a>	<a href="#">15</a>
<a href="#">9.</a>	<a href="#">Service Provider Configuration Schema</a>	<a href="#">16</a>
<a href="#">10.</a>	<a href="#">Resource Schema</a>	<a href="#">18</a>
<a href="#">11.</a>	<a href="#">JSON Representation</a>	<a href="#">20</a>
<a href="#">11.1.</a>	<a href="#">Minimal User Representation</a>	<a href="#">20</a>
<a href="#">11.2.</a>	<a href="#">Full User Representation</a>	<a href="#">20</a>
<a href="#">11.3.</a>	<a href="#">Enterprise User Extension Representation</a>	<a href="#">23</a>
<a href="#">11.4.</a>	<a href="#">Group Representation</a>	<a href="#">26</a>
<a href="#">11.5.</a>	<a href="#">Service Provider Configuration Representation</a>	<a href="#">26</a>
<a href="#">11.6.</a>	<a href="#">Resource Schema Representation</a>	<a href="#">28</a>
<a href="#">12.</a>	<a href="#">XML Representation</a>	<a href="#">32</a>
<a href="#">12.1.</a>	<a href="#">Minimal Representation</a>	<a href="#">32</a>
<a href="#">12.2.</a>	<a href="#">Full Representation</a>	<a href="#">33</a>
<a href="#">12.3.</a>	<a href="#">Enterprise User Extension Representation</a>	<a href="#">36</a>
<a href="#">12.4.</a>	<a href="#">Group Representation</a>	<a href="#">39</a>
<a href="#">13.</a>	<a href="#">Security Considerations</a>	<a href="#">39</a>
<a href="#">Appendix A.</a>	<a href="#">Contributors</a>	<a href="#">39</a>
<a href="#">14.</a>	<a href="#">Normative References</a>	<a href="#">40</a>
	<a href="#">Authors' Addresses</a>	<a href="#">40</a>



## **1. Requirements Notation and 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](#)] .

Throughout this document, values are quoted to indicate that they are to be taken literally. When using these values in protocol messages, the quotes MUST NOT be used as part of the value.

## **2. Overview**

While there are existing standards for describing and exchanging user information, many of these standards can be difficult to implement and/or use; e.g., their wire protocols do not easily traverse firewalls and/or are not easily layered onto existing web protocols. As a result, many cloud providers implement non-standard APIs for managing users within their services. This increases both the cost and complexity associated with organizations adopting products and services from multiple cloud providers as they must perform redundant integration development. Similarly, cloud services providers seeking to interoperate with multiple application marketplaces or cloud identity providers must be redundantly integrated.

SCIM seeks to simplify this problem through a simple to implement specification suite that provides a common user schema and extension model, as well as binding documents to provide patterns for exchanging this schema via a REST API. It draws inspiration and best practice, building upon existing user APIs and schemas from a wide variety of sources including, but not limited to, existing APIs exposed by cloud providers, PortableContacts, and LDAP directory services.

This document provides a platform neutral schema and extension model for representing users and groups in JSON and XML formats. This schema is intended for exchange and use with cloud service providers. Additional binding documents provide a standard REST API, SAML binding, and use cases.

### **2.1. Definitions**

Service Provider: A web application that provides identity information via the SCIM protocol.



**Consumer:** A website or application that uses the SCIM protocol to manage identity data maintained by the Service Provider.

**Resource:** The Service Provider managed artifact containing one or more attributes; e.g., User or Group

**Singular Attribute:** A Resource attribute that contains 0..1 values; e.g., displayName.

**Multi-valued Attribute:** A Resource attribute that contains 0..n values; e.g., emails.

**Simple Attribute:** A Singular or Multi-valued Attribute whose value is a primitive; e.g., String.

**Complex Attribute:** A Singular or Multi-valued Attribute whose value is a composition of one or more Simple Attributes.

**Sub-Attribute:** A Simple Attribute contained within a Complex Attribute.

### **3. SCIM Schema Structure**

SCIM schema provides a minimal core schema for representing users and groups (resources), encompassing common attributes found in many existing deployments and schemas.

A resource is a collection of attributes identified by one or more schemas. Minimally, an attribute consists of the attribute name and at least one Simple or Complex value either of which may be Multi-valued. SCIM schema defines the data type, plurality and other distinguishing features of an attribute. Unless otherwise specified all attributes are modifiable by Consumers. Immutable (read-only) attributes SHALL be specified as 'READ-ONLY' within the attribute definition. Additionally, Service Providers MAY choose to make some or all Resource attributes immutable and SHOULD identify those attributes via the associated Resource's schema endpoint ([Section 5.2](#)).

Both XML and JSON formats are defined. Resource and attribute names MUST conform to XML naming rules; i.e., SCIM names MUST be valid XML names and SHOULD be camelCased. When marshalling or extending SCIM resources in XML implementors MUST use the normative, SCIM, XML schema (.xsd). SCIM resources represented in a schema-less format; e.g., JSON, MUST specify schema via the schemas attribute ([Section 5.2](#)).





### **[3.1.](#) Attribute Data Types**

Attribute data types are derived from XML schema [\[1\]](#) and unless otherwise specified are optional, modifiable by Consumers, and of type String ([Section 3.1.1](#)). The JSON format defines a limited set of data types, hence, where appropriate, alternate JSON representations are defined below. SCIM extensions SHOULD not introduce new data types.

#### **[3.1.1.](#) String**

A sequence of characters as defined in [section 3.2.1](#) of the XML Schema Datatypes Specification. A String attribute MAY specify a required data format. Additionally, when Canonical Values are specified Service Providers SHOULD conform to those values if appropriate, but MAY provide alternate String values to represent additional values.

#### **[3.1.2.](#) Boolean**

The literal "true" or "false" as specified in [section 3.2.2](#) of the XML Schema Datatypes Specification.

#### **[3.1.3.](#) Decimal**

A real number with at least one digit to the left and right of the period as specified in [section 3.2.3](#) of the XML Schema Datatypes Specification.

Values represented in JSON MUST conform to the XML constraints above and are represented as a JSON Number [\[2\]](#).

#### **[3.1.4.](#) Integer**

A Decimal number with no fractional digits as defined in [section 3.3.13](#) of the XML Schema Datatypes Specification.

Values represented in JSON MUST conform to the XML constraints above and are represented as a JSON Number [\[2\]](#).

#### **[3.1.5.](#) DateTime**

A dateTime (e.g. 2008-01-23T04:56:22Z) as specified in [section 3.2.7](#) of the XML Schema Datatypes Specification.

Values represented in JSON MUST conform to the XML constraints above and are represented as a JSON String [\[2\]](#).



### **[3.1.6.](#) Binary**

The attribute value MUST be encoded as a valid `xsd:base64Binary` value as specified in [section 3.2.16](#) of the XML Schema Datatypes Specification.

Values represented in JSON MUST conform to the XML constraints above and are represented as a JSON String [2].

### **[3.1.7.](#) Complex**

A Singular or Multi-valued Attribute whose value is a composition of one or more Simple Attributes as specified in [section 3.4](#) XML Schema Datatypes Specification.

JSON values are represented as JSON Objects [2].

## **[3.2.](#) Multi-valued Attributes**

Multi-valued attributes are unordered lists of attributes. Each attribute MAY contain Sub-Attributes and therefore multi-valued attributes may contain Complex Attributes. The below Sub-Attributes are considered normative and when specified SHOULD be used as defined.

`type` A label indicating the attribute's function; e.g., "work" or "home".

`primary` A Boolean value indicating the 'primary' or preferred attribute value for this attribute, e.g. the preferred mailing address or primary e-mail address. The primary attribute value 'true' MUST appear no more than once.

`display` A human readable name, primarily used for display purposes. READ-ONLY.

`operation` The operation to perform on the multi-valued attribute during a PATCH request. The only valid value is "delete", which signifies that this instance should be removed from the Resource.

`value` The attribute's significant value; e.g., the e-mail address, phone number, etc. Attributes that define a "value" sub-attribute MAY be alternately represented as a collection of primitive types. For example:



```
{
  "emails": [
    {"value": "bjensen@example.com"},
    {"value": "babs@example.com"}
  ]
}
```

May also be represented as:

```
{
  "emails": ["bjensen@example.com", "babs@example.com"]
}
```

When returning multi-valued attributes, Service Providers SHOULD canonicalize the value returned, if appropriate (e.g. for e-mail addresses and URLs). Providers MAY return the same value more than once with different types (e.g. the same e-mail address may be used for work and home), but SHOULD NOT return the same (type, value) combination more than once per Attribute, as this complicates processing by the Consumer.

#### **[4.](#) Schema Extension Model**

SCIM schema follows an object extension model similar to ObjectClasses used in LDAP. Unlike LDAP there is no inheritance model; all extensions are additive (similar to LDAP Auxiliary Object Classes [\[3\]](#)). Each value indicates additive schema that may exist in a SCIM representation as specified by extensions not defined in this suite. Schema extensions MUST NOT redefine any attributes defined in this specification and SHOULD follow conventions defined in this specification. Each schema extension must identify a URI used to identify the extension. XML MUST use XML namespaces and JSON formats MUST use the "schemas" attribute ([Section 5.2](#)) to distinguish extended resources and attributes.

#### **[5.](#) SCIM Core Schema**

##### **[5.1.](#) Common Schema Attributes**

Each SCIM Resource (Users, Groups, etc.) includes the below common attributes. These attributes MUST be included in all Resources, including any extended Resource types. It is not necessary to specify the schemas attribute if the Resource is fully defined in this document as the core schema is implicitly included.



**id** Unique identifier for the SCIM Resource as defined by the Service Provider. Each representation of the Resource MUST include a non-empty id value. This identifier MUST be unique across the Service Provider's entire set of Resources. It MUST be a stable, non-reassignable identifier that does not change when the same Resource is returned in subsequent requests. The value of the id attribute is always issued by the Service Provider and MUST never be specified by the Service Consumer. bulkId: is a reserved keyword and MUST NOT be used in the unique identifier. REQUIRED and READ-ONLY.

**externalId** An identifier for the Resource as defined by the Service Consumer. The externalId may simplify identification of the Resource between Service Consumer and Service provider by allowing the Consumer to refer to the Resource with its own identifier, obviating the need to store a local mapping between the local identifier of the Resource and the identifier used by the Service Provider. Each Resource MAY include a non-empty externalId value. The value of the externalId attribute is always issued by the Service Consumer and can never be specified by the Service Provider. The Service Provider MUST always interpret the externalId as scoped to the Service Consumer's tenant.

**meta** A complex attribute containing resource metadata. All sub-attributes are OPTIONAL

**created** The DateTime the Resource was added to the Service Provider. The attribute MUST be a DateTime. READ-ONLY.

**lastModified** The most recent DateTime the details of this Resource were updated at the Service Provider. If this Resource has never been modified since its initial creation, the value MUST be the same as the value of created. The attribute MUST be a DateTime. READ-ONLY.

**location** The URI of the Resource being returned. This value MUST be the same as the Location HTTP response header. READ-ONLY.

**version** The version of the Resource being returned. This value must be the same as the ETag HTTP response header. READ-ONLY.

**attributes** The names of the attributes to remove from the Resource during a PATCH operation.





## **5.2. "schemas" Attribute**

SCIM supports resources of different types, with extensible schemas. Each resource **MUST** be indicated using fully qualified URLs.

Where a specific representation has existing support for expressing schema, the traditional convention of that representation **MUST** be applied. For example, when representing users using XML, XML Namespace should be used.

When a representation does not explicitly provide support for indicating a schema, such as JSON, a schemas attribute is used to indicate the version of SCIM schema as well as any schema extensions.

**schemas** The schemas attribute is an array of Strings which allows introspection of the supported schema version for a SCIM representation as well any schema extensions supported by that representation. Each String value must be a unique URI. This specification defines URIs for User, Group, and a standard "enterprise" extension. All representations of SCIM schema **MUST** include a non-zero value array with value(s) of the URIs supported by that representation. Duplicate values **MUST NOT** be included. Value order is not specified and **MUST NOT** impact behavior. **REQUIRED.**

## **6. SCIM User Schema**

SCIM provides a schema for representing Users, identified using the following URI: 'urn:scim:schemas:core:1.0'. The following attributes are defined in addition to those attributes defined in SCIM Core Schema:

### **6.1. Singular Attributes**

**userName** Unique identifier for the User, typically used by the user to directly authenticate to the service provider. Often displayed to the user as their unique identifier within the system (as opposed to id or externalId, which are generally opaque and not user-friendly identifiers). Each User **MUST** include a non-empty userName value. This identifier **MUST** be unique across the Service Consumer's entire set of Users. **REQUIRED.**

**name** The components of the User's real name. Providers **MAY** return just the full name as a single string in the formatted sub-attribute, or they **MAY** return just the individual component attributes using the other sub-attributes, or they **MAY** return both. If both variants are returned, they **SHOULD** be describing



the same name, with the formatted name indicating how the component attributes should be combined.

**formatted** The full name, including all middle names, titles, and suffixes as appropriate, formatted for display (e.g. Ms. Barbara Jane Jensen, III.).

**familyName** The family name of the User, or "Last Name" in most Western languages (e.g. Jensen given the full name Ms. Barbara Jane Jensen, III.).

**givenName** The given name of the User, or "First Name" in most Western languages (e.g. Barbara given the full name Ms. Barbara Jane Jensen, III.).

**middleName** The middle name(s) of the User (e.g. Jane given the full name Ms. Barbara Jane Jensen, III.).

**honorificPrefix** The honorific prefix(es) of the User, or "Title" in most Western languages (e.g. Ms. given the full name Ms. Barbara Jane Jensen, III.).

**honorificSuffix** The honorific suffix(es) of the User, or "Suffix" in most Western languages (e.g. III. given the full name Ms. Barbara Jane Jensen, III.).

**displayName** The name of the User, suitable for display to end-users. Each User returned MAY include a non-empty displayName value. The name SHOULD be the full name of the User being described if known (e.g. Babs Jensen or Ms. Barbara J Jensen, III), but MAY be a username or handle, if that is all that is available (e.g. bjensen). The value provided SHOULD be the primary textual label by which this User is normally displayed by the Service Provider when presenting it to end-users.

**nickName** The casual way to address the user in real life, e.g. "Bob" or "Bobby" instead of "Robert". This attribute SHOULD NOT be used to represent a User's username (e.g. bjensen or mpepperidge).

**profileUrl** A fully qualified URL to a page representing the User's online profile.

**title** The user's title, such as "Vice President."



**userType** Used to identify the organization to user relationship. Typical values used might be "Contractor", "Employee", "Intern", "Temp", "External", and "Unknown" but any value may be used.

**preferredLanguage** Indicates the User's preferred written or spoken language. Generally used for selecting a localized User interface. Valid values are concatenation of the ISO 639-1 two letter language code [4], an underscore, and the ISO 3166-1 2 letter country code [5]; e.g., 'en\_US' specifies the language English and country US.

**locale** Used to indicate the User's default location for purposes of localizing items such as currency, date time format, numerical representations, etc. A locale value is a concatenation of the ISO 639-1 two letter language code [4], an underscore, and the ISO 3166-1 2 letter country code [5]; e.g., 'en\_US' specifies the language English and country US.

**timezone** The User's time zone in the "Olson" timezone database format [6]; e.g., 'America/Los\_Angeles'.

**active** A Boolean value indicating the User's administrative status. The definitive meaning of this attribute is determined by the Service Provider though a value of true infers the User is, for example, able to login while a value of false implies the User's account has been suspended.

**password** The User's clear text password. This attribute is intended to be used as a means to specify an initial password when creating a new User or to reset an existing User's password. No accepted standards exist to convey password policies, hence Consumers should expect Service Providers to reject password values. This value MUST never be returned by a Service Provider in any form.

## **6.2. Multi-valued Attributes**

The following multi-valued attributes are defined.

**emails** E-mail addresses for the User. The value SHOULD be canonicalized by the Service Provider, e.g. bjensen@example.com instead of bjensen@EXAMPLE.COM. Canonical Type values of work, home, and other.

**phoneNumbers** Phone numbers for the User. The value SHOULD be canonicalized by the Service Provider according to format in [RFC3966](#) [7] e.g. 'tel:+1-201-555-0123'. Canonical Type values of work, home, mobile, fax, pager and other.



**ims** Instant messaging address for the User. No official canonicalization rules exist for all instant messaging addresses, but Service Providers SHOULD, when appropriate, remove all whitespace and convert the address to lowercase. Instead of the standard Canonical Values for type, this attribute defines the following Canonical Values to represent currently popular IM services: aim, gtalk, icq, xmpp, msn, skype, qq, and yahoo.

**photos** URL of a photo of the User. The value SHOULD be a canonicalized URL, and MUST point to an image file (e.g. a GIF, JPEG, or PNG image file) rather than to a web page containing an image. Service Providers MAY return the same image at different sizes, though it is recognized that no standard for describing images of various sizes currently exists. Note that this attribute SHOULD NOT be used to send down arbitrary photos taken by this User, but specifically profile photos of the User suitable for display when describing the User. Instead of the standard Canonical Values for type, this attribute defines the following Canonical Values to represent popular photo sizes: photo, thumbnail.

**addresses** A physical mailing address for this User. Canonical Type Values of work, home, and other. The value attribute is a complex type with the following sub-attributes. All Sub-Attributes are OPTIONAL.

**formatted** The full mailing address, formatted for display or use with a mailing label. This attribute MAY contain newlines.

**streetAddress** The full street address component, which may include house number, street name, P.O. box, and multi-line extended street address information. This attribute MAY contain newlines.

**locality** The city or locality component.

**region** The state or region component.

**postalCode** The zipcode or postal code component.

**country** The country name component. When specified the value MUST be in ISO 3166-1 alpha 2 "short" code format [5]; e.g., the United States and Sweden are "US" and "SE", respectively.





**groups** A list of groups that the user belongs to, either thorough direct membership, nested groups, or dynamically calculated. The values are meant to enable expression of common group or role based access control models, although no explicit authorization model is defined. It is intended that the semantics of group membership and any behavior or authorization granted as a result of membership are defined by the Service Provider. The Canonical types "direct" and "indirect" are defined to describe how the group membership was derived. Direct group membership indicates the User is directly associated with the group and SHOULD indicate that Consumers may modify membership through the Group Resource. Indirect membership indicates User membership is transitive or dynamic and implies that Consumers cannot modify indirect group membership through the Group resource but MAY modify direct group membership through the Group resource which MAY influence indirect memberships. If the SCIM Service Provider exposes a Group resource, the value MUST be the "id" attribute of the corresponding Group resources to which the user belongs. Since this attribute is read-only, group membership changes MUST be applied via the Group Resource ([Section 8](#)). READ-ONLY.

**entitlements** A list of entitlements for the User that represent a thing the User has. That is, an entitlement is an additional right to a thing, object or service. No vocabulary or syntax is specified and Service Providers/Consumers are expected to encode sufficient information in the value so as to accurately and without ambiguity determine what the User has access to. This value has NO canonical types though type may be useful as a means to scope entitlements.

**roles** A list of roles for the User that collectively represent who the User is; e.g., 'Student', "Faculty". No vocabulary or syntax is specified though it is expected that a role value is a String or label representing a collection of entitlements. This value has NO canonical types.

**x509Certificates** A list of certificates issued to the User. Values are Binary ([Section 3.1.6](#)) and DER encoded x509. This value has NO canonical types.

## **[7.](#) SCIM Enterprise User Schema Extension**

The following SCIM extension defines attributes commonly used in representing users that belong to, or act on behalf of a business or enterprise. The enterprise user extension is identified using the following URI: 'urn:scim:schemas:extension:enterprise:1.0'.



The following Singular Attributes are defined:

`employeeNumber` Numeric or alphanumeric identifier assigned to a person, typically based on order of hire or association with an organization.

`costCenter` Identifies the name of a cost center.

`organization` Identifies the name of an organization.

`division` Identifies the name of a division.

`department` Identifies the name of a department.

`manager` The User's manager. A complex type that optionally allows Service Providers to represent organizational hierarchy by referencing the "id" attribute of another User.

`managerId` The id of the SCIM resource representing the User's manager. REQUIRED.

`displayName` The displayName of the User's manager. OPTIONAL and READ-ONLY.

## **8. SCIM Group Schema**

SCIM provides a schema for representing groups, identified using the following URI: 'urn:scim:schemas:core:1.0'.

Group resources are meant to enable expression of common Group or role based access control models, although no explicit authorization model is defined. It is intended that the semantics of group membership and any behavior or authorization granted as a result of membership are defined by the Service Provider are considered out of scope for this specification.

The following Singular Attribute is defined in addition to the common attributes defined in SCIM Core Schema:

`displayName` A human readable name for the Group. REQUIRED.

The following multi-valued attribute is defined in addition to the common attributes defined in SCIM Core Schema:



members A list of members of the Group. Canonical Types "User" and "Group" are READ-ONLY. The value must be the "id" of a SCIM resource, either a User, or a Group. The intention of the Group type is to allow the Service Provider to support nested Groups. Service Providers MAY require Consumers to provide a non-empty members value based on the "required" sub attribute of the "members" attribute in Group Resource Schema.

## **9. Service Provider Configuration Schema**

SCIM provides a schema for representing the Service Provider's configuration identified using the following URI:  
'urn:scim:schemas:core:1.0'

The Service Provider Configuration Resource enables a Service Provider to expose its compliance with the SCIM specification in a standardized form as well as provide additional implementation details to Consumers. All attributes are READ-ONLY.

The following Singular Attributes are defined in addition to the common attributes defined in Core Schema:

documentationUrl An HTTP addressable URL pointing to the Service Provider's human consumable help documentation.

patch A complex type that specifies PATCH configuration options.  
REQUIRED.

supported Boolean value specifying whether the operation is supported. REQUIRED.

bulk A complex type that specifies BULK configuration options.  
REQUIRED

supported Boolean value specifying whether the operation is supported. REQUIRED.

maxOperations An integer value specifying the maximum number of operations. REQUIRED.

maxPayloadSize An integer value specifying the maximum payload size in bytes. REQUIRED.



**filter** A complex type that specifies FILTER options. REQUIRED.

**supported** Boolean value specifying whether the operation is supported. REQUIRED.

**maxResults** Integer value specifying the maximum number of Resources returned in a response. REQUIRED.

**changePassword** A complex type that specifies Change Password configuration options. REQUIRED.

**supported** Boolean value specifying whether the operation is supported. REQUIRED.

**sort** A complex type that specifies Sort configuration options. REQUIRED.

**supported** Boolean value specifying whether sorting is supported. REQUIRED.

**etag** A complex type that specifies Etag configuration options. REQUIRED.

**supported** Boolean value specifying whether the operation is supported. REQUIRED.

**xmlDataFormat** A complex type that specifies whether the XML data format is supported. REQUIRED.

**supported** Boolean value specifying whether the operation is supported. REQUIRED.

The following multi-valued attribute is defined in addition to the common attributes defined in Core Schema:

**authenticationSchemes** A complex type that specifies supported Authentication Scheme properties. Instead of the standard Canonical Values for type, this attribute defines the following Canonical Values to represent common schemes: oauth, oauth2, oauthbearertoken, httpbasic, and httpdigest. To enable seamless discovery of configuration, the Service Provider SHOULD, with the appropriate security considerations, make the authenticationSchemes attribute publicly accessible without prior authentication. REQUIRED.





name The common authentication scheme name; e.g., HTTP Basic.  
REQUIRED.

description A description of the Authentication Scheme.  
REQUIRED.

specUrl A HTTP addressable URL pointing to the Authentication  
Scheme's specification. OPTIONAL.

documentationUrl A HTTP addressable URL pointing to the  
Authentication Scheme's usage documentation. OPTIONAL.

## **10. Resource Schema**

The Resource schema specifies the Attribute(s) and meta-data that constitute a Resource. Schema Resources are READ-ONLY and identified using the following URI: 'urn:scim:schemas:core:1.0'. Unlike other core Resources the schema Resource MAY contain a complex object within a Sub-Attribute and all Attributes are REQUIRED unless other specified.

The following Singular Attributes are defined:

name The Resource name. When applicable Service Providers MUST specify the name specified in the core schema specification; e.g., "User" or "Group".

description The Resource's human readable description. When applicable Service Providers MUST specify the description specified in the core schema specification.

schema The Resource's associated schema URI; e.g.,  
urn:scim:schemas:core:1.0.

endpoint The Resource's HTTP addressable endpoint relative to the  
Base URL; e.g., /Users.

The following multi-valued attribute is defined:

attributes A complex type that specifies the set of Resource  
attributes.

name The attribute's name.



**type** The attribute's data type; e.g., String.

**multiValued** Boolean value indicating the attribute's plurality.

**multiValuedAttributeChildName** String value specifying the child XML element name; e.g., the 'emails' attribute value is 'email', 'phoneNumbers', is 'phoneNumber'. REQUIRED when the multiValued attribute value is true otherwise this attribute MUST be omitted.

**description** The attribute's human readable description. When applicable Service Providers MUST specify the description specified in the core schema specification.

**schema** The attribute's associated schema; e.g.,  
urn:scim:schemas:core:1.0.

**readOnly** A Boolean value that specifies if the attribute is mutable.

**required** A Boolean value that specifies if the attribute is required.

**caseExact** A Boolean value that specifies if the String attribute is case sensitive.

The following multi-valued attributes are defined. There are no canonical type values defined and the primary value serves no useful purpose.

**subAttributes** A list specifying the contained attributes.  
OPTIONAL.

**name** The attribute's name.

**type** The attribute's data type; e.g., String.

**description** The attribute's human readable description.  
When applicable Service Providers MUST specify the description specified in the core schema specification.

**readOnly** A Boolean value that specifies if the attribute is mutable.

**required** A Boolean value that specifies if the attribute is required.



**caseExact** A Boolean value that specifies if the String attribute is case sensitive.

**canonicalValues** A collection of canonical values. When applicable Service Providers MUST specify the canonical types specified in the core schema specification; e.g., "work", "home". OPTIONAL.

## **[11.](#) JSON Representation**

### **[11.1.](#) Minimal User Representation**

The following is a non-normative example of the minimal required SCIM representation in JSON format.

```
{
  "schemas": ["urn:scim:schemas:core:1.0"],
  "id": "2819c223-7f76-453a-919d-413861904646",
  "userName": "bjensen@example.com"
}
```

### **[11.2.](#) Full User Representation**

The following is a non-normative example of the fully populated SCIM representation in JSON format.

```
{
  "schemas": ["urn:scim:schemas:core:1.0"],
  "id": "2819c223-7f76-453a-919d-413861904646",
  "externalId": "701984",
  "userName": "bjensen@example.com",
  "name": {
    "formatted": "Ms. Barbara J Jensen III",
    "familyName": "Jensen",
    "givenName": "Barbara",
    "middleName": "Jane",
    "honorificPrefix": "Ms.",
    "honorificSuffix": "III"
  },
  "displayName": "Babs Jensen",
  "nickName": "Babs",
  "profileUrl": "https://login.example.com/bjensen",
  "emails": [
    {
      "value": "bjensen@example.com",
```



```
    "type": "work",
    "primary": true
  },
  {
    "value": "babs@jensen.org",
    "type": "home"
  }
],
"addresses": [
  {
    "type": "work",
    "streetAddress": "100 Universal City Plaza",
    "locality": "Hollywood",
    "region": "CA",
    "postalCode": "91608",
    "country": "USA",
    "formatted": "100 Universal City Plaza\nHollywood, CA 91608 USA",
    "primary": true
  },
  {
    "type": "home",
    "streetAddress": "456 Hollywood Blvd",
    "locality": "Hollywood",
    "region": "CA",
    "postalCode": "91608",
    "country": "USA",
    "formatted": "456 Hollywood Blvd\nHollywood, CA 91608 USA"
  }
],
"phoneNumbers": [
  {
    "value": "555-555-5555",
    "type": "work"
  },
  {
    "value": "555-555-4444",
    "type": "mobile"
  }
],
"ims": [
  {
    "value": "someaimhandle",
    "type": "aim"
  }
],
"photos": [
  {
    "value": "https://photos.example.com/profilephoto/72930000000Ccne/F",
```





```
    "type": "photo"
  },
  {
    "value": "https://photos.example.com/profilephoto/72930000000Ccne/T",
    "type": "thumbnail"
  }
],
"userType": "Employee",
"title": "Tour Guide",
"preferredLanguage": "en_US",
"locale": "en_US",
"timezone": "America/Los_Angeles",
"active": true,
"password": "t1meMa$heen",
"groups": [
  {
    "display": "Tour Guides",
    "value": "003000000005N2Y6AA"
  },
  {
    "display": "Employees",
    "value": "003000000005N34H78"
  },
  {
    "display": "US Employees",
    "value": "003000000005N98YT1"
  }
],
"x509Certificates": [
  {
    "value":
      "MIIDQzCCAQygAwIBAgICEAAwDQYJKoZIhvcNAQEFBQAwTjELMAkGA1UEBhMCVVMx
      EzARBgNVBAgMCkNhbgG1mb3JuaWExFDASBgNVBAoMC2V4YW1wbGUuY29tMRQwEgYD
      VQQDDAtleGFtcGx1LmNvbTAeFw0xMTEwMjIwMzFaFw0xMjEwMDQwNjIwMzFa
      MH8xCzAJBgNVBAYTA1VTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRQwEgYDVQQKDATl
      eGFtcGx1LmNvbTEhMB8GA1UEAwYTXMuIEJhcmJhcmEgSiBKZW5zZW4gSU1JMSIw
      IAYJKoZIhvcNAQkBFhNiamVuc2VuQGV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0B
      AQEFAAOCAQ8AMIIBCgKCAQEAE7Kr+Dcds/
      JQ5GwejJFcBIP682X3xpjis56AK02bc
      1FLgzdLI8auoR+cC9/
      Vrh5t66HkQI0dA4unHh0AaZ4xL5PhVbXIPMB5vAPKpzz5i
      PSi8x08SL7I7SDhcBVJhqVqr3Hg1lEG6UC1DdH07nkLuwXq8HcISKkBT5WFTVfFZ
```

zidPl8HZ7DhXkZIRtJwBweq4bvm3hM10s7UQH05ZS6cVDgweKNwdLLrT51ikSQG3

DYr1+ft781UQRIqxgwqCfXEuDiinPh0kkvIi5jivVu1Z9QiwlyEdRbLJ4zJQBmDr  
SGTMYn4lRc2HgH04DqB/  
bnMVorHB0CC6AV1QoFK4GPe1LwIDAQABo3sweTAJBgNV

HRMEAjAAMCwGCWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZp  
Y2F0ZTAdBgNVHQ4EFgQU8pD0U0vsZIsaA16lL8En8bx0F/  
gWHwYDVR0jBBgwFoAU

dGeKitcaF7gnzsNwDx708kqaVt0wDQYJKoZIhvcNAQEFBQADgYEA81SsFnOdYJt  
Ng5Tcq+/  
ByEDrBgnusx0jloUhByPMEVkoMZ3J7j1ZgI8rAb0kNngX8+pKfTiDz1R  
C4+dx8oU6Za+4NJXUjlL5CvV6BEYb1+QAEJwitTVvxB/A67g42/  
vzgAtoRUeDov1  
+GFibZ+GNF/cAYKcMtGcrs2i97ZkJMo="

```
    }
  ],
  "meta": {
    "created": "2010-01-23T04:56:22Z",
    "lastModified": "2011-05-13T04:42:34Z",
    "version": "W\\\\"a330bc54f0671c9\\\"",
    "location": "https://example.com/v1/Users/
2819c223-7f76-453a-919d-413861904646"
  }
}
```

### **11.3. Enterprise User Extension Representation**

The following is a non-normative example of the fully populated User using the enterprise User extension in JSON format.

```
{
  "schemas": ["urn:scim:schemas:core:1.0",
"urn:scim:schemas:extension:enterprise:1.0"],
  "id": "2819c223-7f76-453a-919d-413861904646",
  "externalId": "701984",
  "userName": "bjensen@example.com",
  "name": {
    "formatted": "Ms. Barbara J Jensen III",
    "familyName": "Jensen",
    "givenName": "Barbara",
    "middleName": "Jane",
    "honorificPrefix": "Ms.",
    "honorificSuffix": "III"
  },
  "displayName": "Babs Jensen",
  "nickName": "Babs",
  "profileUrl": "https://login.example.com/bjensen",
  "emails": [
    {
      "value": "bjensen@example.com",
      "type": "work",
      "primary": true
    },
    {
      "value": "babs@jensen.org",
      "type": "home"
    }
  ],
  "addresses": [
    {
      "streetAddress": "100 Universal City Plaza",
```

```
"locality": "Hollywood",  
"region": "CA",
```

Mortimore, et al.

Expires February 28, 2013

[Page 23]

```
    "postalCode": "91608",
    "country": "USA",
    "formatted": "100 Universal City Plaza\nHollywood, CA 91608 USA",
    "type": "work",
    "primary": true
  },
  {
    "streetAddress": "456 Hollywood Blvd",
    "locality": "Hollywood",
    "region": "CA",
    "postalCode": "91608",
    "country": "USA",
    "formatted": "456 Hollywood Blvd\nHollywood, CA 91608 USA",
    "type": "home"
  }
],
"phoneNumbers": [
  {
    "value": "555-555-5555",
    "type": "work"
  },
  {
    "value": "555-555-4444",
    "type": "mobile"
  }
],
"ims": [
  {
    "value": "someaimhandle",
    "type": "aim"
  }
],
"photos": [
  {
    "value": "https://photos.example.com/profilephoto/72930000000Ccne/F",
    "type": "photo"
  },
  {
    "value": "https://photos.example.com/profilephoto/72930000000Ccne/T",
    "type": "thumbnail"
  }
],
"userType": "Employee",
"title": "Tour Guide",
"preferredLanguage": "en_US",
"locale": "en_US",
"timezone": "America/Los_Angeles",
"active": true,
```



```
"password": "t1meMa$heen",
"groups": [
  {
    "value": "e9e30dba-f08f-4109-8486-d5c6a331660a",
    "display": "Tour Guides"
  },
  {
    "value": "fc348aa8-3835-40eb-a20b-c726e15c55b5",
    "display": "Employees"
  },
  {
    "value": "71ddacd2-a8e7-49b8-a5db-ae50d0a5bfd7",
    "display": "US Employees"
  }
],
"x509Certificates": [
  {
    "value":
      "MIIDQzCCAQygAwIBAgICEAAwDQYJKoZIhvcNAQEFBQAwTjELMAkGA1UEBhMCVVMx
      EzARBgNVBAgMCkNhbmG1mb3JuaWExFDASBgNVBAoMC2V4YW1wbGUuY29tMRQwEgYD
      VQDDAtleGFtcGx1LmNvbTAeFw0xMTEwMjIwMzFaFw0xMjEwMDQwNjI0MzFa
      MH8xCzAJBgNVBAYTA1VTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRQwEgYDVQQKDA1l
      eGFtcGx1LmNvbTEhMB8GA1UEAwYTXMuIEJhcmJhcmEgSiBKZW5zZW4gSULJMSIw
      IAYJKoZIhvcNAQkBFhNiamVuc2VuQGV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0B
      AQEFAAOCAQ8AMIIBCgKCAQEA7Kr+Dcds/
      JQ5GwejJFcBIP682X3xpjis56AK02bc
      1FLgzdLI8auoR+cC9/
      Vrh5t66HkQIOdA4unHh0AaZ4xL5PhVbXIPMB5vAPKpzz5i
      PSi8x08SL7I7SDhcBVJhqVqr3Hg1lEG6UC1DdH07nkLuwXq8HcISKkbT5WFTVfFZ
      zidPl8HZ7DhXkZIRtJwBweq4bvm3hM10s7UQH05ZS6cVDgweKNwdLLrT51ikSQG3
      DYrl+ft781UQRIqxgwcFxEuDiinPh0kkvIi5jivVu1Z9QiwlyEdRbLJ4zJQBmDr
      SGTMYn4lRc2HgH04DqB/
      bnMVorHB0CC6AV1QoFK4GPe1LwIDAQABo3sweTAJBgNV
      HRMEAjaAMCwGCWCGSAGG+EIBDQqFh1PcGVuU1NMIEdlbmVyYXRlZCBZJ0aWZp
      Y2F0ZTAdbGNVHQ4EFgQU8pD0U0vsZIsa16lL8En8bx0F/
      gwHwYDVR0jBBgwFoAU
      dGeKitcaF7gnzsNwDx708kqaVt0wDQYJKoZIhvcNAQEFBQADgYEAA81SsFnOdYJt
      Ng5Tcq+
      ByEDrBgnusx0jloUhByPMEVkoMZ3J7j1ZgI8rAb0kNngX8+pKfTiDz1R
```



```
C4+dx8oU6Za+4NJXUjlL5CvV6BEYb1+QAEJwitTVvxB/A67g42/
vzgAtoRUeDov1
    +GFiBZ+GNF/cAYKcMtGcrs2i97ZkJMo="
  }
],
"urn:scim:schemas:extension:enterprise:1.0": {
  "employeeNumber": "701984",
  "costCenter": "4130",
  "organization": "Universal Studios",
  "division": "Theme Park",
  "department": "Tour Operations",
  "manager": {
    "managerId": "26118915-6090-4610-87e4-49d8ca9f808d",
    "displayName": "John Smith"
  }
},
```

```
"meta": {
  "created": "2010-01-23T04:56:22Z",
  "lastModified": "2011-05-13T04:42:34Z",
  "version": "W\/"3694e05e9dff591\"",
  "location": "https://example.com/v1/Users/
2819c223-7f76-453a-919d-413861904646"
}
```

#### [11.4.](#) Group Representation

The following is a non-normative example of SCIM Group representation in JSON format.

```
{
  "schemas": ["urn:scim:schemas:core:1.0"],
  "id": "e9e30dba-f08f-4109-8486-d5c6a331660a",
  "displayName": "Tour Guides",
  "members": [
    {
      "value": "2819c223-7f76-453a-919d-413861904646",
      "display": "Babs Jensen"
    },
    {
      "value": "902c246b-6245-4190-8e05-00816be7344a",
      "display": "Mandy Pepperidge"
    }
  ]
}
```

#### [11.5.](#) Service Provider Configuration Representation

The following is a non-normative example of the SCIM Service Provider Configuration representation in JSON format.



```
{
  "schemas": ["urn:scim:schemas:core:1.0"],
  "documentationUrl": "http://example.com/help/scim.html",
  "patch": {
    "supported": true
  },
  "bulk": {
    "supported": true,
    "maxOperations": 1000,
    "maxPayloadSize": 1048576
  },
  "filter": {
    "supported": true,
    "maxResults": 200
  },
  "changePassword": {
    "supported": true
  },
  "sort": {
    "supported": true
  },
  "etag": {
    "supported": true
  },
  "xmlDataFormat": {
    "supported": true
  },
  "authenticationSchemes": [
    {
      "name": "OAuth Bearer Token",
      "description": "Authentication Scheme using the OAuth Bearer Token
Standard",
      "specUrl": "http://tools.ietf.org/html/draft-ietf-oauth-v2-bearer-01",
      "documentationUrl": "http://example.com/help/oauth.html",
      "type": "oauthbearertoken",
      "primary": true
    },
    {
      "name": "HTTP Basic",
      "description": "Authentication Scheme using the Http Basic Standard",
      "specUrl": "http://www.ietf.org/rfc/rfc2617.txt",
      "documentationUrl": "http://example.com/help/httpBasic.html",
      "type": "httpbasic"
    }
  ]
}
```



### **11.6. Resource Schema Representation**

The following is a normative example of the SCIM Resource Schema representation in JSON format.

```
{
  "id": "urn:scim:schemas:core:1.0:User",
  "name": "User",
  "description": "Core User",
  "schema": "urn:scim:schemas:core:1.0",
  "endpoint": "/Users",
  "attributes": [
    {
      "name": "id",
      "type": "string",
      "multiValued": false,
      "description": "Unique identifier for the SCIM resource as defined by the
Service Provider. Each representation of the resource MUST include a non-empty
id value. This identifier MUST be unique across the Service Provider's entire
set of resources. It MUST be a stable, non-reassignable identifier that does
not change when the same resource is returned in subsequent requests. The value
of the id attribute is always issued by the Service Provider and MUST never be
specified by the Service Consumer. REQUIRED.",
      "schema": "urn:scim:schemas:core:1.0",
      "readOnly": true,
      "required": true,
      "caseExact": false
    },
    {
      "name": "name",
      "type": "complex",
      "multiValued": false,
      "description": "The components of the user's real name. Providers MAY
return just the full name as a single string in the formatted sub-attribute, or
they MAY return just the individual component attributes using the other sub-
attributes, or they MAY return both. If both variants are returned, they SHOULD
be describing the same name, with the formatted name indicating how the
component attributes should be combined.",
      "schema": "urn:scim:schemas:core:1.0",
      "readOnly": false,
      "required": false,
      "caseExact": false,
      "subAttributes": [
        {
          "name": "formatted",
          "type": "string",
          "multiValued": false,
          "description": "The full name, including all middle names, titles, and
```

suffixes as appropriate, formatted for display (e.g. Ms. Barbara J Jensen, III.)." ,

```
    "readOnly":false,  
    "required":false,  
    "caseExact":false
```

```
  },
```

```
  {
```

```
    "name":"familyName",
```

```
    "type":"string",
```

```
    "multiValued":false,
```

```
    "description":"The family name of the User, or Last Name in most  
Western languages (e.g. Jensen given the full name Ms. Barbara J Jensen,  
III.).",
```

```
    "readOnly":false,
```

```
    "required":false,
```

```
        "caseExact":false
      },
      {
        "name":"givenName",
        "type":"string",
        "multiValued":false,
        "description":"The given name of the User, or First Name in most
Western languages (e.g. Barbara given the full name Ms. Barbara J Jensen,
III.).",
        "readOnly":false,
        "required":false,
        "caseExact":false
      },
      {
        "name":"middleName",
        "type":"string",
        "multiValued":false,
        "description":"The middle name(s) of the User (e.g. Robert given the
full name Ms. Barbara J Jensen, III.).",
        "readOnly":false,
        "required":false,
        "caseExact":false
      },
      {
        "name":"honorificPrefix",
        "type":"string",
        "multiValued":false,
        "description":"The honorific prefix(es) of the User, or Title in most
Western languages (e.g. Ms. given the full name Ms. Barbara J Jensen, III.).",
        "readOnly":false,
        "required":false,
        "caseExact":false
      },
      {
        "name":"honorificSuffix",
        "type":"string",
        "multiValued":false,
        "description":"The honorific suffix(es) of the User, or Suffix in
most Western languages (e.g. III. given the full name Ms. Barbara J Jensen,
III.).",
        "readOnly":false,
        "required":false,
        "caseExact":false
      }
    ]
  },
  {
    "name":"emails",
```



```
"type":"complex",
"multiValued":true,
"multiValuedAttributeChildName":"email",
"description":"E-mail addresses for the user. The value SHOULD be
canonicalized by the Service Provider, e.g. bjensen@example.com instead of
bjensen@EXAMPLE.COM. Canonical Type values of work, home, and other.",
"schema":"urn:scim:schemas:core:1.0",
"readOnly":false,
```

```
"required":false,
"caseExact":false,
"subAttributes":[
  {
    "name":"value",
    "type":"string",
    "multiValued":false,
    "description":"E-mail addresses for the user. The value SHOULD be
canonicalized by the Service Provider, e.g. bjensen@example.com instead of
bjensen@EXAMPLE.COM. Canonical Type values of work, home, and other.",
    "readOnly":false,
    "required":false,
    "caseExact":false
  },
  {
    "name":"display",
    "type":"string",
    "multiValued":false,
    "description":"A human readable name, primarily used for display
purposes. READ-ONLY.",
    "readOnly":true,
    "required":false,
    "caseExact":false
  },
  {
    "name":"type",
    "type":"string",
    "multiValued":false,
    "description":"A label indicating the attribute's function; e.g.,
'work' or 'home'.",
    "readOnly":false,
    "required":false,
    "caseExact":false,
    "canonicalValues":["work","home","other"]
  },
  {
    "name":"primary",
    "type":"boolean",
    "multiValued":false,
    "description":"A Boolean value indicating the 'primary' or preferred
attribute value for this attribute, e.g. the preferred mailing address or
primary e-mail address. The primary attribute value 'true' MUST appear no more
than once.",
    "readOnly":false,
    "required":false,
    "caseExact":false
  }
],
```

```
{
  "name":"addresses",
  "type":"complex",
  "multiValued":true,
  "multiValuedAttributeChildName":"address",
  "description":"A physical mailing address for this User, as described in
(address Element). Canonical Type Values of work, home, and other. The value
attribute is a complex type with the following sub-attributes.",
  "schema":"urn:scim:schemas:core:1.0",
```

```
"readOnly":false,
"required":false,
"caseExact":false,
"subAttributes":[
  {
    "name":"formatted",
    "type":"string",
    "multiValued":false,
    "description":"The full mailing address, formatted for display or
use with a mailing label. This attribute MAY contain newlines.",
    "readOnly":false,
    "required":false,
    "caseExact":false
  },
  {
    "name":"streetAddress",
    "type":"string",
    "multiValued":false,
    "description":"The full street address component, which may include
house number, street name, PO BOX, and multi-line extended street address
information. This attribute MAY contain newlines.",
    "readOnly":false,
    "required":false,
    "caseExact":false
  },
  {
    "name":"locality",
    "type":"string",
    "multiValued":false,
    "description":"The city or locality component.",
    "readOnly":false,
    "required":false,
    "caseExact":false
  },
  {
    "name":"region",
    "type":"string",
    "multiValued":false,
    "description":"The state or region component.",
    "readOnly":false,
    "required":false,
    "caseExact":false
  },
  {
    "name":"postalCode",
    "type":"string",
    "multiValued":false,
    "description":"The zipcode or postal code component.",
```

```
"readOnly":false,  
"required":false,  
"caseExact":false
```

```
    },
    {
      "name": "country",
      "type": "string",
      "multiValued": false,
      "description": "The country name component.",
      "readOnly": false,
      "required": false,
      "caseExact": false
    },
    {
      "name": "type",
      "type": "string",
      "multiValued": false,
      "description": "A label indicating the attribute's function; e.g.,
'work' or 'home'.",
      "readOnly": false,
      "required": false,
      "caseExact": false,
      "canonicalValues": ["work", "home", "other"]
    },
  ],
},
{
  "name": "employeeNumber",
  "type": "string",
  "multiValued": false,
  "description": "Numeric or alphanumeric identifier assigned to a person,
typically based on order of hire or association with an organization.",
  "schema": "urn:scim:schemas:extension:enterprise:1.0",
  "readOnly": false,
  "required": false,
  "caseExact": false
}
]
```

## [12.](#) XML Representation

### [12.1.](#) Minimal Representation

The following is a non-normative example of the minimal required SCIM User representation in XML format.

```
<User xmlns="urn:scim:schemas:core:1.0">
```

<id>2819c223-7f76-453a-919d-413861904646</id>  
<userName>bjensen@example.com</userName>

</User>

## 12.2. Full Representation

The following is a non-normative example of the fully populated SCIM representation in XML format.

```
<User xmlns="urn:scim:schemas:core:1.0">
  <id>2819c223-7f76-453a-919d-413861904646</id>
  <externalId>701984</externalId>
  <userName>bjensen@example.com</userName>
  <name>
    <formatted>Ms. Babs J Jensen III</formatted>
    <familyName>Jensen</familyName>
    <givenName>Barbara</givenName>
    <middleName>Jane</middleName>
    <honorificPrefix>Ms.</honorificPrefix>
    <honorificSuffix>III</honorificSuffix>
  </name>
  <displayName>Babs Jensen</displayName>
  <nickName>Babs</nickName>
  <profileUrl>https://login.example.com/bjensen</profileUrl>
  <emails>
    <email>
      <value>bjensen@example.com</value>
      <type>work</type>
      <primary>true</primary>
    </email>
    <email>
      <value>babs@jensen.com</value>
      <type>home</type>
    </email>
  </emails>
  <addresses>
    <address>
      <formatted>100 Universal City Plaza\nHollywood, CA 91608 USA</formatted>
      <streetAddress>100 Universal City Plaza</streetAddress>
      <locality>Hollywood</locality>
      <region>CA</region>
      <postalCode>91608</postalCode>
      <country>USA</country>
      <type>work</type>
      <primary>true</primary>
    </address>
    <address>
      <formatted>456 Hollywood Blvd\nHollywood, CA 91608 USA</formatted>
```





```
<streetAddress>456 Hollywood Blvd</streetAddress>
<locality>San Francisco</locality>
<region>CA</region>
<postalCode>91608</postalCode>
<country>USA</country>
<type>home</type>
</address>
</addresses>
<phoneNumbers>
  <phoneNumber>
    <value>555-555-5555</value>
    <type>work</type>
  </phoneNumber>
  <phoneNumber>
    <value>555-555-4444</value>
    <type>mobile</type>
  </phoneNumber>
</phoneNumbers>
<ims>
  <im>
    <value>someaimhandle</value>
    <type>aim</type>
  </im>
</ims>
<photos>
  <photo>
    <value>https://photos.example.com/profilephoto/72930000000Ccne/F</value>
    <type>photo</type>
  </photo>
  <photo>
    <value>https://photos.example.com/profilephoto/72930000000Ccne/T</value>
    <type>thumbnail</type>
  </photo>
</photos>
<userType>Employee</userType>
<title>Tour Guide</title>
<preferredLanguage>en_US</preferredLanguage>
<locale>en_US</locale>
<timezone>America/Los_Angeles</timezone>
<active>true</active>
<password>t1meMa$heen</password>
<groups>
  <group>
    <value>e9e30dba-f08f-4109-8486-d5c6a331660a</value>
    <display>Tour Guides</display>
  </group>
  <group>
    <value>6d1a1088-3a56-4371-8e3b-6d48d67493ec</value>
```



```
    <display>Employees</display>
  </group>
  <group>
    <value>5fd998b9-d2bd-479c-991b-6790537608dc</value>
    <display>US Employees</display>
  </group>
</groups>
<roles>
  <role>
    <value>administrator</value>
  </role>
</roles>
<entitlements>
  <entitlement>
    <value>delete users</value>
  </entitlement>
</entitlements>
<x509Certificates>
  <x509Certificate>
    <value>
      MIIDQZCCAqygAwIBAgICEAAwDQYJKoZIhvcNAQEFBQAwTjELMAkGA1UEBhMCVVMx
      EzARBgNVBAGMCKNhbgG1mb3JuaWExFDASBgNVBAoMC2V4YW1wbGUuY29tMRQwEgYD
      VQQDDAtleGtfcGx1LmNvbTAeFw0xMTEwMjIwMzFaFw0xMjEwMDQwNjI0MzFa
      MH8xCzAJBgNVBAYTA1VTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRQwEgYDVQQKDA1l
      eGtfcGx1LmNvbTEhMB8GA1UEAwwYTXMuIEJhcmJhcmEgSiBKZW5zZW4gSU1JMSIw
      IAYJKoZIhvcNAQkBFhNiamVuc2VuQGv4YW1wbGUuY29tMIIIBIjANBgkqhkiG9w0B
      AQEFAAOCAQ8AMIIBCgKCAQEa7Kr+Dcds/JQ5GwejJFcBIP682X3xpjis56AK02bc
      1FLgzdLI8auoR+cC9/Vrh5t66HkQIOdA4unHh0AaZ4xL5PhVbXIPMB5vAPKpzz5i
      PSi8x08SL7I7SDhcBVJhqVqr3Hg1LEG6UC1DdH07nkLuwXq8HcISKkbT5WFTVfFZ
      zidPl8HZ7DhXkZIRtJwBweq4bvm3hM10s7UQH05ZS6cVDgweKNwdLLrT51ikSQG3
      DYrl+ft781UQRIqxgwqCfXEuDiinPh0kkvIi5jivVu1Z9QiwlYEdRbLJ4zJQBmDr
      SGTMYn4lRc2HgH04DqB/bnMVorHB0CC6AV1QoFK4GPe1LwIDAQABo3sweTAJBgNV
      HRMEAjAAMCwGCWCGSAGG+EIBDQfFh1PcGVuU1NMIEdlbmVyYXRlZCBZJ0awZp
      Y2F0ZTAdbGNVHQ4EFgQU8pD0U0vsZIsaA16lL8En8bx0F/gwHwYDVR0jBBgwFoAU
      dGeKitcaF7gnzsNwDx708kqaVt0wDQYJKoZIhvcNAQEFBQADgYEA81SsFnOdYJt
      Ng5Tcq+/ByEDrBgnusx0jloUhByPMEVkoMZ3J7j1ZgI8rAb0kNngX8+pKfTiDz1R
      C4+dx8oU6Za+4NJXUjlL5CvV6BEYb1+QAEJwitTVvxB/A67g42/vzgAtoRUeDov1
      +GFibZ+GNF/cAYKcMtGcrs2i97ZkJMo=
    </value>
  </x509Certificate>
</x509Certificates>
<meta>
  <created>2010-01-23T04:56:22Z</created>
  <lastModified>2011-05-13T04:42:34Z</lastModified>
  <version>W/"a330bc54f0671c9"</version>
  <location>https://example.com/v1/Users/
  2819c223-7f76-453a-919d-413861904646</location>
</meta>
```

</User>

Mortimore, et al.

Expires February 28, 2013

[Page 35]

### **[12.3.](#) Enterprise User Extension Representation**

The following is a non-normative example of the fully populated User using the enterprise User extension in XML format.

```
<User xmlns="urn:scim:schemas:core:1.0"
xmlns:enterprise="urn:scim:schemas:extension:enterprise:1.0">
  <id>2819c223-7f76-453a-919d-413861904646</id>
  <externalId>701984</externalId>
  <userName>bjensen@example.com</userName>
  <name>
    <formatted>Ms. Babs J Jensen III</formatted>
    <familyName>Jensen</familyName>
    <givenName>Barbara</givenName>
    <middleName>Jane</middleName>
    <honorificPrefix>Ms.</honorificPrefix>
    <honorificSuffix>III</honorificSuffix>
  </name>
  <displayName>Babs Jensen</displayName>
  <nickName>Babs</nickName>
  <profileUrl>https://login.example.com/bjensen</profileUrl>
  <title>Tour Guide</title>
  <userType>Employee</userType>
  <preferredLanguage>en_US</preferredLanguage>
  <locale>en_US</locale>
  <timezone>America/Los_Angeles</timezone>
  <active>true</active>
  <password>t1meMa$h33n</password>
  <emails>
    <email>
      <value>bjensen@example.com</value>
      <type>work</type>
      <primary>true</primary>
    </email>
    <email>
      <value>babs@jensen.com</value>
      <type>home</type>
    </email>
  </emails>
  <addresses>
    <address>
      <formatted>100 Universal City Plaza\nHollywood, CA 91608 USA</formatted>
      <streetAddress>100 Universal City Plaza</streetAddress>
      <locality>Hollywood</locality>
      <region>CA</region>
      <postalCode>91608</postalCode>
      <country>USA</country>
```

<type>work</type>

Mortimore, et al.

Expires February 28, 2013

[Page 36]

```
<primary>true</primary>
</address>
<address>
  <formatted>456 Hollywood Blvd\nHollywood, CA 91608 USA</formatted>
  <streetAddress>456 Hollywood Blvd</streetAddress>
  <locality>San Francisco</locality>
  <region>CA</region>
  <postalCode>91608</postalCode>
  <country>USA</country>
  <type="home">
</address>
</addresses>
<phoneNumbers>
  <phoneNumber>
    <value>555-555-5555</value>
    <type>work</type>
  </phoneNumber>
  <phoneNumber>
    <value>555-555-4444</value>
    <type>mobile</type>
  </phoneNumber>
</phoneNumbers>
<ims>
  <im>
    <value>someaimhandle</value>
    <type>aim</type>
  </im>
</ims>
<photos>
  <photo>
    <value>https://photos.example.com/profilephoto/72930000000Ccne/F</value>
    <type>photo</type>
  </photo>
  <photo>
    <value>https://photos.example.com/profilephoto/72930000000Ccne/T</value>
    <type>thumbnail</type>
  </photo>
</photos>
<groups>
  <group>
    <display>Tour Guides</display>
    <value>00300000005N2Y6AA</value>
  </group>
  <group>
    <display>Employees</display>
    <value>00300000005N34H78</value>
  </group>
  <group>
```





```
<display>US Employees</display>
<value>003000000005N98YT1</value>
</group>
</groups>
<roles>
  <role>
    <value>administrator</value>
  </role>
</roles>
<entitlements>
  <entitlement>
    <value>delete users</value>
  </entitlement>
</entitlements>
<x509Certificates>
  <x509Certificate>
    <value>
      MIIDQzCCAqygAwIBAgICEAAwDQYJKoZIhvcNAQEFBQAwtjELMAkGA1UEBhMCVVMx
      EzARBgNVBAgMCkNhbgG1mb3JuaWExFDASBgNVBAoMC2V4YW1wbGUuY29tMRQwEgYD
      VQQDDAtleGFtcGx1LmNvbTAeFw0xMTEwMjIwNjI0MzFaFw0xMjEwMDQwNjI0MzFa
      MH8xCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRQwEgYDVQQKDatl
      eGFtcGx1LmNvbTEhMB8GA1UEAwwYTXMuIEJhcmJhcmEgSiBKZW5zZW4gSU1JMSIw
      IAYJKoZIhvcNAQkBFhNiamVuc2VuQGv4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0B
      AQEFAAOCAQ8AMIIBCgKCAQEAE7Kr+Dcds/JQ5GwejJFcBIP682X3xpjis56AK02bc
      1FLgzdLI8auoR+cC9/Vrh5t66HkQI0dA4unHh0AaZ4xL5PhVbXIPMB5vAPKpzz5i
      PSi8x08SL7I7SDhcBVJhqVqr3Hg1lEG6UC1DdH07nkLuwXq8HcISKkbT5WFTVfFZ
      zidPl8HZ7DhXkZIRtJwBweq4bvm3hM10s7UQH05ZS6cVDgweKNwdLLrT51iksQG3
      DYrl+ft781UQRIqxgwqCfXEuDiinPh0kkvIi5jivVu1Z9QiwlyEdRbLJ4zJQBmDr
      SGTMYn4lRc2HgH04DqB/bnMvOrHB0CC6AV1QoFK4GPe1LwIDAQABo3sweTAJBgNV
      HRMEAjAAMCwGCWGSAGG+EIBDQqFFh1PcGVuU1NMIEdlbmVvYXRlZCBZJ0awZp
      Y2F0ZTAdBgNVHQ4EFgQU8pD0U0vsZISaA16lL8En8bx0F/gwHwYDVR0jBBgwFoAU
      dGeKitcaF7gnzsNwDx708kqaVt0wDQYJKoZIhvcNAQEFBQADgYEAA81SsFn0dYJt
      Ng5Tcq+/ByEDrBgnusx0jloUhByPMEVkoMZ3J7j1ZgI8rAb0kNngX8+pKfTiDz1R
      C4+dx8oU6Za+4NJXUj1L5CvV6BEYb1+QAEJwitTVvxB/A67g42/vzgAtoRUeDov1
      +GFibZ+GNF/cAYKcMtGcrs2i97ZkJMo=
    </value>
  </x509Certificate>
</x509Certificates>
<enterprise:employeeNumber>701984</enterprise:employeeNumber>
<enterprise:manager>
  <enterprise:managerId>902c246b-6245-4190-8e05-00816be7344a</
enterprise:managerId>
  <enterprise:displayName>Mandy Pepperidge</enterprise:displayName>
</enterprise:manager>
<enterprise:costCenter>4130</enterprise:costCenter>
<enterprise:organization>Universal Studios</enterprise:organization>
<enterprise:division>Theme Park</enterprise:division>
<enterprise:department>Tour Operations</enterprise:department>
```

<meta>

Mortimore, et al.

Expires February 28, 2013

[Page 38]

```
<created>2010-01-23T04:56:22Z</created>
<lastModified>2011-05-13T04:42:34Z</lastModified>
<version>W/"3694e05e9dff591"</version>
<location>https://example.com/v1/Users/
2819c223-7f76-453a-919d-413861904646</location>
</meta>
</User>
```

#### **[12.4.](#) Group Representation**

The following is a non-normative example of a SCIM Group representation in XML format.

```
<Group xmlns="urn:scim:schemas:core:1.0">
  <id>2819c223-7f76-453a-919d-413861904646</id>
  <displayName>Tour Guides</displayName>
  <members>
    <member>
      <value>902c246b-6245-4190-8e05-00816be7344a</value>
      <display>Babs Jensen</display>
    </member>
    <member>
      <value>902c246b-6245-4190-8e05-00816be7344a</value>
      <display>Mandy Pepperidge</display>
    </member>
  </members>
</Group>
```

### **[13.](#) Security Considerations**

The SCIM Core schema contains personally identifiable information as well as other sensitive data. Aside from prohibiting password values in a SCIM response this specification does not provide any means or guarantee of confidentiality.

#### **[Appendix A.](#) Contributors**

The SCIM Community would like to thank the following people for the work they've done in the research, formulation, drafting, editing, and support of this specification.

Morteza Ansari (morteza.ansari@cisco.com)



Sidharth Choudhury (schoudhury@salesforce.com)

Samuel Erdtman (samuel@erdtman.se)

Kelly Grizzle (kelly.grizzle@sailpoint.com)

Chris Phillips (cjphillips@gmail.com)

Erik Wahlstroem (erik.wahlstrom@nexussafe.com)

Special thanks to Joeseph Smarr, who's excellent work on the Portable Contacts Specification [[PortableContacts](#)] provided a basis for the SCIM schema structure and text.

## **14. Normative References**

[PortableContacts]

Smarr, J., "Portable Contacts 1.0 Draft C - Schema Only", August 2008.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[1] <<http://www.w3.org/TR/xmlschema-2/>>

[2] <<http://www.json.org/>>

[3] <<http://tools.ietf.org/html/rfc4512>>

[4] <[http://www.loc.gov/standards/iso639-2/php/code\\_list.php](http://www.loc.gov/standards/iso639-2/php/code_list.php)>

[5] <[http://www.iso.org/iso/country\\_codes/iso\\_3166\\_code\\_lists/country\\_names\\_and\\_code\\_elements.htm](http://www.iso.org/iso/country_codes/iso_3166_code_lists/country_names_and_code_elements.htm)>

[6] <<http://www.twinsun.com/tz/tz-link.htm>>

[7] <<http://tools.ietf.org/html/rfc3966>>

## Authors' Addresses

Chuck Mortimore (editor)  
Salesforce.com

Email: cmortimore@salesforce.com



Patrick Harding  
Ping Identity

Email: [pharding@pingidentity.com](mailto:pharding@pingidentity.com)

Paul Madsen  
Ping Identity

Email: [pmadsen@pingidentity.com](mailto:pmadsen@pingidentity.com)

Trey Drake  
UnboundID

Email: [trey.drake@unboundid.com](mailto:trey.drake@unboundid.com)