Abstract

The System for Cross-Domain Identity Management (SCIM) specifications are designed to enable identity provisioning in cloud based applications and web services easier using HTTP protocol. This specification defines a method for discovering a SCIM service provider using the "/.well-known" mechanism and optional support for WebFinger queries.

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 August 6, 2016.

Copyright Notice

Copyright (c) 2016 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

1. Introduction and Overview .................................. 2
   1.1. Requirements Notation and Conventions ................. 2
   1.2. Definitions ........................................... 3
2. Discovery Using '/.well-known' .......................... 3
3. Discovery Using WebFinger ............................... 4
4. Security Considerations ................................. 5
   4.1. TLS Requirements .................................. 5
   4.2. Limited Information Disclosure ...................... 6
5. Privacy Considerations ................................... 6
6. IANA Considerations ...................................... 6
   6.1. Well-Known Registration ............................. 6
   6.2. Scim Link Relation Type .............................. 6
7. References ................................................ 7
   7.1. Normative References ................................ 7
   7.2. Informative References ............................... 8
Appendix A. Acknowledgements ............................... 8
Appendix B. Change Log ..................................... 8
Author’s Address ........................................... 8

1. Introduction and Overview

The System for Cross-Domain Identity Management (SCIM) protocol [RFC7644] is designed to enable identity provisioning in web applications using the HTTP protocol. This specification defines two methods for discovering a SCIM service provider using the "/.well-known" mechanism defined in [RFC5785] and an OPTIONAL WebFinger discovery as defined in [RFC7033] that allows the discovery of a specific SCIM service provider discovery based on a subject identifier.

1.1. 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 all figures may contain spaces and extra line-wrapping for readability and space reasons. Similarly, some URI’s contained within examples, have been shortened for space and readability reasons.
1.2. Definitions

Service Provider
An HTTP web application that provides identity information via the
SCIM protocol.

Client
A website or application that uses the SCIM protocol to manage
identity data maintained by the service provider. The client
initiates SCIM HTTP requests to a target service provider.

Endpoint
An endpoint for a service provider is a defined base path relative
to the service providers Base URI (see Sec 1.3 of [RFC7644]) over
which SCIM operations may be performed against SCIM resources.

2. Discovery Using ‘/.well-known’

In cases where a client would like to ask where the default SCIM
endpoint is, the "/.well-known/scim" discovery method MAY be used.
The discovery service MAY use the client’s security context to
determine the correct SCIM endpoint and MAY require authentication.
For example, a currently authenticated client may be assigned a
different SCIM endpoint than another subject as they may be members
of a different tenancy.

A SCIM service provider MAY be queried by issuing an HTTP GET request
at a previously known "/.well-known" discovery end-point [RFC5785]
using the URI suffix "scim".

The requesting client would make a request similar to the following
(with line wraps for display purposes only):

GET /.well-known/scim HTTP/1.1
HOST: example.com

If a SCIM service provider is known, a response is returned, encoded
in JSON with mime-type application/json

HTTP/1.1 200 OK
Content-Type: application/json

{
  "issuer":
    "https://example.com",
  "scim_base":
    "https://scim.example.com"
The response to a well-known endpoint with the URI suffix "scim" SHALL return a JSON structure consisting of the following attributes:

issuer  The issuer of the discovery information. The issuer MUST correspond to the URL of the discovery location.

scim_base  The base URL of a SCIM server as defined in Sec 1.3 of [RFC7644]. From this point, a client MAY query the SCIM service’s own configuration endpoints as documented in Section 4 [RFC7644].

When receiving a response, clients MUST confirm that the URI used to retrieve the well-known discovery information matches the returned "issuer" attribute.

If the service provider is able to detect a current security subject, the value of scim_base MAY change to match the authenticated subject. This may be useful in situations such as multi-tenancy where a specific SCIM service is defined for subjects that part of a specific security domain.

### 3. Discovery Using WebFinger

A SCIM service provider MAY offer WebFinger [RFC7033] discovery as a means of determining the base URL of a SCIM server (as defined in Section 1.3 [RFC7644]) assigned based upon a client’s knowledge of a subject or identifier or other unique account key that has been obtained through an out-of-band mechanism.

When making a WebFinger request, the client SHALL use the following parameters:

rel  Containing the value "scim"; and,

resource  With a value in the form of a URI whose scheme is "acct" as per [RFC7565] and whose suffix corresponds to an attribute of the subject which can either be mapped or searched in order to determine the appropriate SCIM base URL that corresponds to the identified account.

When the query is submitted, the WebFinger JRD response SHALL include an "href" value matching the SCIM base URL endpoint for the matched query resource. A match indicates where a resource MAY exist, it does not confirm that the matched resource exists. The actual account URI SHALL NOT be returned (see Section 4).
The following example uses the "rel" parameter to request links for a SCIM service provider (spaces and line-breaks added for readability):

GET /.well-known/webfinger?
resource=acct%3Abob%40example.com&
rel=scim HTTP/1.1
Host: example.com

The following example shows a corresponding response in JRD form (spaces and line-breaks added for readability):

HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Content-Type: application/jrd+json

{
  "subject" : "acct:bob@example.com",
  "links" : 
    [ 
      { 
        "rel" : "scim",
        "href" : "https://scim.example.com/tenant/b939a93/"
      }
    ]
}

Upon receiving the response, the client MAY query the discovered SCIM service’s own configuration endpoints as documented in Section 4 [RFC7644]. Using the href value provided, the client MAY do a SCIM Query to locate the actual URI of the account requested if one exists.

4. Security Considerations

4.1. TLS Requirements

This specification requires the use of transport-layer security when communicating with service providers. The service provider MUST support TLS 1.2 [RFC5246] and MAY support additional transport-layer security mechanisms meetings its security requirements. When using TLS, the client MUST perform a TLS/SSL server identity check as per [RFC6125]. Implementation security considerations for TLS can be found in [RFC7525].
4.2. Limited Information Disclosure

The intent of WebFinger discovery is to disclose only the correct SCIM endpoint for a potential account identifier. WebFinger is not intended be used to discover actual account URIs or to confirm their existence.

It is the intention of this specification that clients SHALL make a second query to the returned SCIM endpoint to discover the actual account URI if it exists. In the context of SCIM discovery, WebFinger is not intended as a secondary query protocol for SCIM due to the sensitive information contained in SCIM service providers (see Section 5).

5. Privacy Considerations

In cases where the WebFinger discovery method is used, it is important to consider that the account query contains personally identifiable information. Appropriate measure must be taken to keep this information confidential such as the use of Transport Layer Security.

Implementers SHOULD consider the privacy considerations outlined in Section 9.3 [RFC7643] when passing account query information.

6. IANA Considerations

6.1. Well-Known Registration

This section registers the well-known URI suffix "scim" as per Section 5.1 of [RFC5785].

URI suffix: The name requested for the well-known URI, relative to "/.well-known/" is "scim".

Change controller: IETF.

Specification document(s): This document.

6.2. Scim Link Relation Type

This section registers the link relation type "scim" as per Section 6.2.1 of [RFC5988].

Relation Name: scim

Description: Refers to a SCIM endpoint corresponding to a WebFinger query.
Reference: Section 3

7. References

7.1. Normative References


7.2. Informative References


Appendix A. Acknowledgements

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)
Oracle Corporation

Email: phil.hunt@yahoo.com