SCIM Event Extension
draft-hunt-idevent-scim-00

Abstract

This specification profiles the Identity Event Token specification to define a set of identity events to be used with SCIM.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at 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 September 21, 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.
1. Introduction and Overview

This specification profiles the Identity Event Token [idevent-token] to define events for SCIM Protocol [RFC7644].

1.1. 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.

1.2. Definitions

This specification uses definitions from the specification [idevent-token].

2. SCIM Events

SCIM events JSON objects that are encoded in JWT form as per [idevent-token]. An event includes a eventUri which indicates the type of event and the event specific attributes. An event also includes standard JWT attributes "iss", "aud", "jti", and "iat" which indicates the event publisher (issuer), the the event feeds (audience), a token identifier, and the date of issue (iat).

2.1. Common Event Attributes

The following attributes are defined for all events defined in Section 2.3 or any schema defined within the uri namespace "urn:ietf:params:events:SCIM".

id
An optional multi-valued SCIM "id" value of the affected resource(s) as defined in Section 3.1 [RFC7643]. If provided the identifiers MUST correspond to the values referenced in "resourceUris".

attributes
A multi-valued list of affected SCIM attributes. Each attribute listed may be a fully-qualified attribute name or an attribute "path" as defined in Figure 7 of Section 3.3.2 of [RFC7644]

values
A JSON object structure containing the affected attributes and their associated values. If the "values" attribute is supplied, the event message MUST be encrypted. Service providers SHOULD take care to ensure that eligible subscribers are able to see attribute values. Alternatively, subscribers MAY use the resourceURIs to retrieve the final attribute values. When doing so, the SCIM service provider can then assess the subscribers right to obtain the actual attribute values.
For a password change event, in maximal disclosure mode (see Section 2.2), the clear text password attribute value MAY be included in the "values" attribute.

2.2. Disclosure Profiles

SCIM events are intended to disclose the minimum amount of information required to provide co-ordination between asynchronous systems. This has the effect of eliminating most error signaling conditions and simplifies privacy and security considerations.

For each event type, the following levels of disclosure are defined, for which different security considerations may apply:

Minimal
In general, the main information content is the event description itself. The event contents typically includes only REQUIRED attributes. Because no data content is exchanged, encryption of the event message is not required.

Default
In general the default information is exchanged. This includes the "sub" attribute and a list of affected SCIM attributes. Typically attribute values are not provided. Encryption of the event message is typically not required unless otherwise stated.

Maximal
In maximal mode, all data involved in the state change is exchanged. To prevent leakage of information, implementers SHOULD encrypt events that convey attributes about resources. This profile should typically be used when co-ordinating information between tightly-coupled systems that are part of a common administrative domain.

In the case of "minimal" and "default" disclosures, a subscriber MAY use a follow-up SCIM GET (see Section 3.4 [RFC7644]) to obtain the current state of the resource (sub) following the event. While this may be seen as costly (as a second call), using SCIM GET enables simpler error signalling, access control, distribution enforcement by the event publisher.

2.3. SCIM Events

2.3.1. urn:ietf:params:event:SCIM:add
The specified resource URI was added to the feed. An add does not indicate a resource is new or has been recently created. For example, an existing user has had a new role (e.g. CRM_User) added to their profile which has caused their resource to join a feed.
The following is an example of a minimal disclosure Add Event message (it has been modified for readability):

```json
{
    "jti": "6164f3bbf6ff41a88dc94f18cb0620e8",
    "eventUris": [
        "urn:ietf:params:event:SCIM:add"
    ],
    "iat": 1458505044,
    "iss": "https://scim.example.com",
    "aud": [
        "https://scim.example.com/Feeds/98d52461fa5bcb879593b7754",
        "https://scim.example.com/Users/2bf880af6674ac284bae9381673d462"
    ],
    "sub": "https://scim.example.com/Users/2bf880af6674ac284bae9381673d462"
}
```

Figure 1: Example SCIM Add Event

### 2.3.2. urn:ietf:params:event:SCIM:create

The new resource URI has been created at the service provider and has been added to the feed. When a CREATE event is sent, a corresponding ADD event is not issued. In "minimal" disclosure mode, event specific data is returned. In "default" disclosure, the "attributes" attribute is returned disclosing what attributes were created at the publisher. In "maximal" disclosure mode, set of values reflecting the final state of the resource at the service provider are provided in the "values" attribute and MUST be encrypted as a JWE (see [idevent-token]).
The following is an example SCIM Create event message (it has been modified for readability) and uses maximal disclosure:

```json
{
   "jti": "4d3559ec67504aaba65d40b0363faad8",
   "eventUris": [
      "urn:ietf:params:event:SCIM:create"
   ],
   "iat": 1458496404,
   "iss": "https://scim.example.com",
   "aud": [
      "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754",
      "https://scim.example.com/Feeds/5d7604516b1d08641d7676ee7"
   ],
   "sub": "https://scim.example.com/Users/44f6142df96bd6ab61e7521d9",
   "urn:ietf:params:event:SCIM:create": {
      "attributes": ["id", "name", "userName", "password", "emails"],
      "values": {
         "emails": ["type": "work", "value": "jdoe@example.com"]
      },
      "password": "not4u2no",
      "userName": "jdoe",
      "id": "44f6142df96bd6ab61e7521d9",
      "name": {
         "givenName": "John",
         "familyName": "Doe"
      }
   }
}

Figure 2: Example SCIM Create Event (Maximal Disclosure)

In the above example, the user "jdoe" is created with values an email address, an initial password, and a name. Note that when raw data is sent, it is advisable to protect the event using JWE (see Section 2.2 [idevent-token]).
The following is an example SCIM Create event message (it has been modified for readability) and uses default disclosure:

```json
{
  "jti": "4d3559ec67504aaba65d40b0363faad8",
  "eventUris": [
    "urn:ietf:params:event:SCIM:create"
  ],
  "iat": 1458496404,
  "iss": "https://scim.example.com",
  "aud": [
    "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754",
    "https://scim.example.com/Feeds/5d7604516b1d08641d7676ee7"
  ],
  "sub": "https://scim.example.com/Users/44f6142df96bd6ab6e7521d9",
  "urn:ietf:params:event:SCIM:create": {
    "attributes": ["id", "name", "userName", "password", "emails"],
  }
}
```

The event above notifies the subscriber which attributes are available from the SCIM event publisher, but does not convey the actual information. The subscriber MAY retrieve that information by performing a SCIM GET to the "sub" value specified.

Figure 3: Example SCIM Create Event (Default Disclosure)

### 2.3.3. urn:ietf:params:event:SCIM:activate

The specified resource (e.g. User) has been activated. This optional event is used to indicate a high-level change in state as agreed between the publisher and subscriber. For example, an activated resource is one that can now have an active session (may log in) from a security perspective (may log in). Typically this event discloses only minimal information.
The following is an example of a minimal disclosure Activate Event message (it has been modified for readability):

```
{
    "jti": "6164f3bbf6ff41a88dc94f18cb0620e8",
    "eventUris": [
        "urn:ietf:params:event:SCIM:activate"
    ],
    "iat": 1458505044,
    "iss": "https://scim.example.com",
    "aud": [
        "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754",
        "https://scim.example.com/Users/2b2f880af6674ac284bae9381673d462"
    ],
    "sub": "https://scim.example.com/Users/2b2f880af6674ac284bae9381673d462"
}
```

Figure 4: Example SCIM Activate Event

2.3.4. urn:ietf:params:event:SCIM:modify

The specified resource has been updated (e.g. one or more attributes has changed). As with the create event, this event MAY be expressed in minimal, default, and maximal modes.

2.3.5. urn:ietf:params:event:SCIM:deactivate

The specified resource (e.g. User) has been deactivated and disabled. The exact meaning must be agreed to by a SCIM publisher and its corresponding subscriber. Typically this means the sub may no longer have an active security session. As with the activate event, this event has minimal disclosure requirements.

2.3.6. urn:ietf:params:event:SCIM:delete

The specified resource has been deleted from the SCIM publisher. The resource is also removed from the feed. When a DELETE is sent, a corresponding REMOVE is not issued. A delete event has minimal disclosure profile only.
The following is an example of a minimal disclosure Delete Event message (it has been modified for readability):

```
{
  "jti": "6164f3bbf6ff41a88dc94f18cb0620e8",
  "eventUris": [
    "urn:ietf:params:event:SCIM:delete"
  ],
  "iat": 1458505044,
  "iss": "https://scim.example.com",
  "aud": [
    "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754"
  ],
  "sub": "https://scim.example.com/Users/2b2f880af6674ac284bae9381673d462",
}
```

Figure 5: Example SCIM Delete Event

2.3.7. urn:ietf:params:event:SCIM:remove

The specified resource has been removed from the feed. Removal does not indicate that the resource was deleted or otherwise deactivated. This event has minimal disclosure.

The following is an example of a minimal disclosure Remove Event message (it has been modified for readability):

```
{
  "jti": "6164f3bbf6ff41a88dc94f18cb0620e8",
  "eventUris": [
    "urn:ietf:params:event:SCIM:remove"
  ],
  "iat": 1458505044,
  "iss": "https://scim.example.com",
  "aud": [
    "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754"
  ],
  "sub": "https://scim.example.com/Users/2b2f880af6674ac284bae9381673d462",
}
```

Figure 6: Example SCIM Remove Event

2.3.8. urn:ietf:params:event:SCIM:password

The specified resource (e.g. User) has changed its password or the password has been reset. When the password has changed, the "attributes" attribute is supplied with the value "password".
The following is a non-normative example showing a password change event using minimal disclosure:

```
{
    "jti": "3d0c3cf797584bd193bd0fb1bd4e7d30",
    "eventUris": [
        "urn:ietf:params:event:SCIM:password"
    ],
    "iat": 1458496025,
    "iss": "https://scim.example.com",
    "aud": [
        "https://jhub.example.com/Feeds/98d52461fa5bbc879593b7754",
        "https://jhub.example.com/Feeds/5d7604516b1d08641d7676ee7"
    ],
    "sub": "https://scim.example.com/Users/44f6142df96bd6ab61e7521d9",
}
```

Figure 7: Example SCIM Password Change Event

The password event MAY be extended to conveys a password reset, the event MAY include an additional eventUri value of "urn:ietf:params:event:extension:example.com:password" which includes the attribute "resetAttempts". "resetAttempts" indicates the current number of reset attempts since the last successful login by the subject.
The following is a non-normative example showing a password reset event:

```
{
    "jti": "3d0c3cf797584bd193bd0fb1bd4e7d30",
    "eventUris": [
        "urn:ietf:params:event:SCIM:password",
        "urn:ietf:params:event:extension:example.com:password"
    ],
    "iat": 1458496025,
    "iss": "https://scim.example.com",
    "aud": [
        "https://jhub.example.com/Feeds/98d52461fa5bbc879593b7754",
        "https://jhub.example.com/Feeds/5d7604516b1d08641d7676ee7"
    ],
    "sub":
        "https://scim.example.com/Users/44f6142df96bd6ab61e7521d9",
    "urn:ietf:params:event:SCIM:password":{
        "id":"44f6142df96bd6ab61e7521d9",
    },
    "urn:ietf:params:event:extension:example.com:password":{
        "resetAttempts":4
    }
}
```

Figure 8: Example SCIM Password Reset Event

3. Security Considerations

[[TO BE COMPLETED]]

4. IANA Considerations

This section registers the schema extensions found in Section 2.3 in the "Event" registry as per Section 4.2 [idevent-token].

Schema URI: See Section 2.3.

Schema Name: See corresponding names under Section 2.3.

Intended ResourceType: N/A. Events are not intended to be persisted in SCIM.

Purpose: See each description in Section 2.3.

Single-valued Attributes: None.
Multi-valued Attributes: All schemas in this specification share the same attributes. See Section 2.1.

Summary of schema URI registrations:

<table>
<thead>
<tr>
<th>Schema URI</th>
<th>Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:ietf:params:event:SCIM:add</td>
<td>Resource added to</td>
<td>Section 2.3</td>
</tr>
<tr>
<td></td>
<td>Feed Event</td>
<td></td>
</tr>
<tr>
<td>urn:ietf:params:event:SCIM:remove</td>
<td>Resource removed</td>
<td>Section 2.3</td>
</tr>
<tr>
<td></td>
<td>From Feed Event</td>
<td></td>
</tr>
<tr>
<td>urn:ietf:params:event:SCIM:create</td>
<td>New Resource Event</td>
<td>Section 2.3</td>
</tr>
<tr>
<td>urn:ietf:params:event:SCIM:modify</td>
<td>Resource modified</td>
<td>Section 2.3</td>
</tr>
<tr>
<td></td>
<td>Event</td>
<td></td>
</tr>
<tr>
<td>urn:ietf:params:event:SCIM:delete</td>
<td>Resource deleted</td>
<td>Section 2.3</td>
</tr>
<tr>
<td></td>
<td>Event</td>
<td></td>
</tr>
<tr>
<td>urn:ietf:params:event:SCIM:activate</td>
<td>Resource activated</td>
<td>Section 2.3</td>
</tr>
<tr>
<td></td>
<td>Event</td>
<td></td>
</tr>
<tr>
<td>urn:ietf:params:event:SCIM:deactivate</td>
<td>Resource deactivated</td>
<td>Section 2.3</td>
</tr>
<tr>
<td></td>
<td>Event</td>
<td></td>
</tr>
<tr>
<td>urn:ietf:params:event:SCIM:password</td>
<td>Password change</td>
<td>Section 2.3</td>
</tr>
<tr>
<td></td>
<td>Event</td>
<td></td>
</tr>
</tbody>
</table>

5. References

5.1. Normative References

[idevent-subscription]
Oracle Corporation, "Identity Event Subscription Protocol (work in progress)".

[idevent-token]
Oracle Corporation, "Identity Event Token (work in progress)".
5.2. Informative References


Appendix A. Contributors

Appendix B. Acknowledgments

The editor would like to thank the participants in the the SCIM working group and the id-event list for their support of this specification.

Appendix C. Change Log

Draft 00 - PH - First Draft

Authors’ Addresses

Phil Hunt (editor)
Oracle Corporation

Email: phil.hunt@yahoo.com

William Denniss
Salesforce.com

Email: wdenniss@google.com