Abstract
The Simple Cloud Identity Management (SCIM) specification defines a simple, RESTful protocol for identity account management operations. SCIM’s model is based upon the experience of existing schemas and SaaS deployments, with specific emphasis on simplifying development and integration, and wherever possible, applying existing authentication, authorization, and privacy mechanisms.
Table of Contents

Abstract ................................................................. 1
Introduction ............................................................ 3
The SCIM Specification ............................................... 3
Use Cases ................................................................. 4
  Create User – Cloud to Cloud Multiplexing .................. 4
  Delete User – Enterprise to Cloud .............................. 5
  Create User – Just in Time ......................................... 6
Summary ................................................................. 7
References .............................................................. 7
Introduction

The 4 A’s of Identity Management are authentication, authorization, account management and audit logging. Currently, when enterprise employees access cloud applications, authentication is the only “A” with an accepted standard (SAML).

While SAML allows an enterprise to assert identities for employees as they access cloud-based applications relevant to their role, there are cases where the SaaS provider requires an existing account to be waiting for that employee. To date, there is no widely accepted standard protocol for the enterprise to manage (i.e., create, delete) these cloud identities. Consequently, various SaaS providers have defined their own proprietary interfaces, which means enterprise customers are forced to support a variety of logically similar but differently formatted interfaces.

More and more, SaaS applications are accessed through non-browser channels. Native mobile applications installed on mobile devices are a new key driver. Because enterprises cannot necessarily rely on SSO control for SaaS access control, they need active and explicit mechanisms to delete accounts from SaaS providers upon employee termination.

While the Services Provisioning Markup Language (SPML) specification addresses many of the use cases targeted by SCIM, SPML has not seen wide adoption within the enterprise, and none at all between the enterprise and the Cloud. SaaS providers generally opt for (arguably) simpler REST protocols rather than the SOAP stack associated with SPML, and the power of SPML is seen by many as overkill for basic cloud-based account management tasks.

The Simple Cloud Identity Management (SCIM) protocol defines a simple, RESTful protocol for identity account management operations. SCIM’s model is based on the experience of existing schemas and SaaS deployments, placing specific emphasis on simplicity of development and integration, and wherever possible, applying existing authentication, authorization, and privacy mechanisms.

The SCIM Specification

The SCIM specification has three major components:

1) The core schema provides an abstract schema and extension model for representing users and groups in the context of cloud applications. Standard serializations of that schema using JSON and XML are provided.
2) The SCIM protocol defines a REST API for exchanging user and user-related resources via JSON and/or XML.
3) Bindings define how to carry SCIM information on protocols other than the SCIM-defined REST API. An example is the SAML binding.

SCIM recommends using the OAuth protocol for SCIM API call authentication.
Use Cases

The following are representative SCIM use cases. The use cases are mapped onto the appropriate pieces of the SCIM specification set that support them.

Create User – Cloud to Cloud Multiplexing

An enterprise hires a new employee in a role that requires access to several different SaaS providers. The enterprise uses a SaaS provider for their HR functions. Upon the new employee being entered into the HR SaaS provider systems, the HR SaaS provider sends a SCIM message to the appropriate additional SaaS providers, indicating that a new account should be created. The sequence is shown below.

The SCIM REST API defines the form of the “create user” message sent from the HR SaaS provider. An example message is shown here:

```
POST /User  HTTP/1.1
Host: saas2.com
Content-Type: application/json
Authorization: Bearer h480djs93hd8
Content-Length: ...

{"schemas": ["urn:scim:schemas:core:1.0"],
 "userName": "bjensen@example.com",
 "name": {
  "familyName": "Jensen",
  "givenName": "Barbara"},
 "displayName": "Babs Jensen",
 "emails": {
  "value": "bjensen@example.com",
  "type": "work",
  "primary": true}}
```
The JSON object representing the new employee is sent as multiple HTTP POST messages from the HR SaaS provider to the other relevant SaaS providers. The OAuth access token delivered in the HTTP authorization header serves to authenticate the HR SaaS sender.

Delete User – Enterprise to Cloud
An employee leaves an enterprise. To prevent unauthorized access within a SaaS provider, the enterprise must terminate all established channel access—both browser-based and native mobile applications. Because the native application channel is authenticated and authorized through the issuance of a long-lived OAuth access token to the native application, revoking that channel requires that the enterprise actively push a SCIM “delete user” message to the SaaS provider, which will also revoke any outstanding OAuth access tokens. The sequence is show below:

After the enterprise sends the SCIM “delete user” message to the SaaS provider, the SaaS provider will de-authorize the already issued OAuth access tokens, thereby terminating the ex-employee’s mobile-channel access.

Below is a representative SCIM delete message and response.

DELETE /User/3f62ce30-dcd6-4dd7-abfe-2352a76f9978
Host: saas.com
Authorization: Bearer jy5dje99hd8
HTTP/1.1 200 OK

Unlike in the SOAP messaging model, the more RESTful SCIM uses the HTTP DELETE method to match the logical operation. As for the create call, the SCIM message is authenticated by including an OAuth access token.
Create User – Just in Time

An enterprise hires a new employee in a high turnover role that requires periodic and infrequent access to a given SaaS provider. Rather than creating a potentially unnecessary account upon hiring the new employee, the enterprise waits until the employee first accesses the SaaS application. As part of the web SSO operation from the enterprise to the SaaS application, an account is created “just-in-time”. The sequence is shown below:

The SAML SSO assertion carries sufficient information (encoded as SAML attributes) to allow the SaaS provider to create an account for the employee. The SCIM SAML binding defines how to carry the SCIM attributes in the SAML attributes. Below is a representative sample:

```xml
<saml:AttributeStatement xmlns:xs="http://www.w3.org/2001/XMLSchema"
                        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified" Name="SCIM.userName">
        <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">bjensen@example.com</saml:AttributeValue>
    </saml:Attribute>

    <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified" Name="SCIM.name.formatted">
    </saml:Attribute>

</saml:AttributeStatement>
```
The SaaS provider validates the SAML assertion, creates a local account based on the information in the attributes, and then initiates a session allowing the employee to start work. The next time the employee SSOs to the SaaS provider, the attributes would need not be sent (unless they had changed).

Summary

The Simple Cloud Identity Management (SCIM) specification is designed to simplify cloud-based identity management, making it more convenient and cost-effective for users to move into, out of and around the Cloud. Building upon SaaS provider and enterprise customer experience with existing proprietary mechanisms, SCIM places specific emphasis on simplicity of development and integration, while applying existing authentication, authorization, and privacy models. SCIM provides a common user schema and extension model, as well as binding documents to provide patterns for exchanging this schema using standard protocols.

References

5. OAuth - http://oauth.net/

About Ping Identity | The Cloud Identity Security Leader

Ping Identity provides cloud identity security solutions to the world’s foremost companies, government organizations and cloud businesses. For more information, dial U.S. toll-free 877.898.2905 or +1.303.468.2882, email sales@pingidentity.com or visit pingidentity.com.