SCIM Specification for Archer SaaS

1. Introduction

SCIM stands for "System for Cross-domain Identity Management." It is an open standard protocol designed to simplify the management of user identities and resources across different systems and domains. With Archer's SCIM integration you can automate the process of user provisioning from your IDP systems, enabling seamless syncing of user information to Archer.

2. Supported Endpoints

Following end points are supported in Archer SCIM integration :

- createGroup
- getGroups
- getGroupById
- updateGroupById
- deleteGroup
- createUser
- getUsers
- getUserById
- updateUserById
- deleteUser

3. Configuration

SCIM Schema:

SCIM schema refers to the structure and definition of data that can be exchanged using the SCIM protocol. It outlines the format, attributes, and rules for representing user identities, groups, and other related information. Few Examples are :

- urn:ietf:params:scim:schemas:core:2.0:User: Defines attributes for representing user resources.
- urn:ietf:params:scim:schemas:core:2.0:Group: Defines attributes for representing group resources.
- urn:ietf:params:scim:schemas:extension:enterprise:2.0:User: Adds enterprise-specific attributes to user resources, like employee number, cost center, etc.
- urn:ietf:params:scim:schemas:extension:Archer:2.0:User: Archer schema that you can configure to add custom parameters that are also supported by Archer.

Subdomain for Each account

Your IDP systems can access SCIM Provisioner via their unique URL called the SCIM Base URL. This must be configured in the IDP's SCIM application. This URL will be provided by Archer to you.

3. Authentication

The SCIM provisioner uses an API key authentication per instance which is specifically defined for SCIM. This is a base 64 encoded string and needs to be configured in SCIM application within the IDP system.

4. Supported Operations

The SCIM API supports following CRUD operations:

- **Create**: POST
- **Read**: GET
- **Update**: PUT, PATCH
- **Delete**: DELETE

5. SCIM Resource Types

5.1. User Resource

A SCIM User resource represents an individual user and includes the following attributes:

- **id**: Unique identifier for the user (read-only).
- **userName**: Unique user identifier (required).
- **name**: Complex attribute containing givenName, familyName, and middleName.
- **emails**: List of email addresses.
- **phoneNumbers**: List of phone numbers.
- **active**: Boolean indicating if the user is active.
- **groups**: List of group memberships (read-only).

Sample User JSON:

This template is to define a JSON schema that represents an IDP user based on Archer's user requirements. This template will tell the IDP about how to provision user values to Archer.

```
{
    "schemas": [
        "urn:ietf:params:scim:schemas:core:2.0:User",
        "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
        "urn:ietf:params:scim:schemas:extension:Archer:2.0:User"
    ],
    "userName": "{$parameters.scimusername}",
    "name": {
        "givenName": "{$parameters.firstname}",
        "middleName": "{$parameters.familyname}",
        "familyName": "{$parameters.lastname}"
    },

    "title": "{$parameters.title}",
    "displayName": "{$parameters.firstname}",
    "profileUrl": "{$parameters.profile_url}",
```

```
    "userType": "{$parameters.user_type}",
    "preferredLanguage": "{$parameters.preferred_language}",
    "locale": "{$parameters.locale}",
    "timezone": "{$parameters.time_zone}",
    "emails": [
        {
            "value": "{$parameters.email}",
            "type": "Business",
            "primary": true
        }
    ],

    "phoneNumbers": [
        {
            "value": "{$parameters.phone}",
            "type": "Business",
            "primary": true
        }],
    "groups": [],
    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User": {
        "organization": "{$parameters.company}",
        "division": "{$parameters.division}",
        "department":        "{$parameters.department}"
    },

    "urn:ietf:params:scim:schemas:extension:Archer:2.0:User": {
        "domainId": null,
        "defaultHomeDashboardId": "{$parameters.default_home_dashboard_id}",
        "defaultHomeWorkspaceId": "{$parameters.default_home_workspace_id}",
        "enableApproveContentByEmail":
        "{$parameters.enable_approve_content_by_email}",
        "forcePasswordChange": "{$parameters.force_password_change}",
        "additionalNote": "{$parameters.additional_note}",
        "securityId": "{$parameters.security_id}"
    }
}
```

5.2. Group Resource

A SCIM Group resource represents a group of users and includes the following attributes:

- **id**: Unique identifier for the group (read-only).
- **displayName**: Human-readable name for the group (required).
- **members**: List of members (users).

Sample Group JSON:

```
{
  "schemas": ["urn:ietf:params:scim:schemas:core:2.0:Group"],
  "id": "e9e30dba-f08f-4109-8486-d5c6a331660a",
  "displayName": "Tour Guides",
  "members": [
    {
```

```
      "value": "2819c223-7f76-453a-919d-413861904646",
      "display": "Barbara Jensen"
    }
  ]
}}
```

6. Error Handling

The SCIM API uses standard HTTP status codes to indicate the success or failure of an API request. Common status codes include:

- **200 OK**: The request was successful.
- **201 Created**: The resource was successfully created.
- **204 No Content**: The resource was successfully deleted.
- **400 Bad Request**: The request was invalid or cannot be served.
- **401 Unauthorized**: Authentication failed or was not provided.
- **403 Forbidden**: The request is understood, but it has been refused or access is not allowed.
- **404 Not Found**: The resource could not be found.
- **409 Conflict**: The request could not be completed due to a conflict.

**Once a user is successfully provisioned, the user can login into Archer via SSO. *For manual login to Archer, System Administrator needs to reset the user password for Archer account.*