Workspace ONE UEM SCIM Adapter

Authors: Matt Williams, VMware EUC Staff Architect Joe Rainone, VMware EUC Consulting Architect

Latest Version: 2003.ga

Validated through IdP's:

- Microsoft Azure Active Directory
- Okta (On Roadmap)

20.03 Release Notes:

**Please Note:** If you have already setup WS1 SCIM Adapter, it is possible that moving to 20.03 will create new accounts. Please consider resetting Directory Services configuration for the OG you are connecting to.

New Features:

- Windows 10 OOBE Enrollment now supported
- Bitnami Node.js 12.16.1-0 now supported with embedded install
- Various Enterprise and Custom SCIM Schema attributes now supported (see below table)

Bugs Fixed:

- Resources with special characters in immutableId do not update

Overview

Workspace ONE UEM SCIM Adapter provides SCIM user/group management capabilities to Workspace ONE UEM. The middleware translates the System for Cross-Domain Identity Management, SCIM, to a CRUD REST framework that Workspace ONE UEM can interpret. This capability allows Workspace ONE UEM to synchronize cloud-based identity resources (users/groups/entitlements) without the need for an LDAP endpoint (service to service model). Examples include Azure AD, Okta, and Sailpoint.
Prerequisites

Requirements

1. Node.js v7.6+ persistent runtime environment
2. Reverse proxy with SSL certificate (i.e. Apache, NGINX, HAproxy, etc)
   - The service does not accept SSL certificates and must be secured thru an SSL reverse proxy
   - Consider 60 minute timeouts depending on directory size
3. Connectivity from directory source (Okta, Azure AD, etc) to service over HTTPS 443
4. Workspace ONE UEM API information:
   - Base API URL
   - Customer OG tenant code (REST API key)
5. Workspace ONE UEM 1810 or higher
6. Resource object source anchors:
   - User -> CustomAttribute1 = ImmutableId (objectGUID or Ms-Ds-Consistency-Guid)
   - Group -> ExternalId = displayName
7. Workspace ONE UEM Directory Services ->
   - 'Directory Type' must be set to 'None' at a minimum
   - 'Enable SAML Authentication For' set to 'Enrollment' at a minimum
   - Custom Attributes must be enabled, with "Custom Attribute 1" set to type 'String'

Functions and Attributes

1. Not Enabled:
- PATCH group modifications
- Multi-group query pagination
- Group membership query
- Administrator account provisioning (On Roadmap)
- Roles or Entitlements (On Roadmap)

2. Resource Attributes:

<table>
<thead>
<tr>
<th>Identity Provider</th>
<th>SCIM Adapter</th>
<th>Workspace ONE UEM</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserPrincipalName</td>
<td>UserName</td>
<td>UserName</td>
<td>Non-Modifiable</td>
</tr>
<tr>
<td>ObjectId</td>
<td>ExternalId</td>
<td>ExternalId</td>
<td>Non-Modifiable</td>
</tr>
<tr>
<td>ImmutableId</td>
<td>ImmutableId</td>
<td>CustomAttribute1</td>
<td>Non-Modifiable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>aadMappingAttribute</td>
<td>Non-Modifiable</td>
</tr>
<tr>
<td>Emails type eq &quot;Work&quot;</td>
<td>Emails</td>
<td>EmailAddress</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Emails</td>
<td>EmailUser</td>
<td></td>
</tr>
<tr>
<td>GivenName</td>
<td>GivenName</td>
<td>FirstName</td>
<td></td>
</tr>
<tr>
<td>FamilyName</td>
<td>FamilyName</td>
<td>LastName</td>
<td></td>
</tr>
<tr>
<td>Formatted = {GivenName + FamilyName}</td>
<td>Formatted</td>
<td>DisplayName</td>
<td></td>
</tr>
<tr>
<td>Active = IsSfotDeleted</td>
<td>Active</td>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>telephoneNumber</td>
<td>phoneNumbers.work</td>
<td>phoneNumber</td>
<td></td>
</tr>
<tr>
<td>department</td>
<td>department</td>
<td>department</td>
<td>Enterprise Schema</td>
</tr>
<tr>
<td>employeeId</td>
<td>employeeNumber</td>
<td>employeeldentifier</td>
<td>Enterprise Schema</td>
</tr>
<tr>
<td>{configurable}</td>
<td>customAttribute2</td>
<td>CustomAttribute2</td>
<td>Custom Schema/Non-Modifiable</td>
</tr>
<tr>
<td>{configurable}</td>
<td>customAttribute3</td>
<td>CustomAttribute3</td>
<td>Custom Schema/Non-Modifiable</td>
</tr>
<tr>
<td>{configurable}</td>
<td>customAttribute4</td>
<td>CustomAttribute4</td>
<td>Custom Schema/Non-Modifiable</td>
</tr>
<tr>
<td>{configurable}</td>
<td>customAttribute5</td>
<td>CustomAttribute5</td>
<td>Custom Schema/Non-Modifiable</td>
</tr>
</tbody>
</table>

Installation

**Install Node.js**

Node.js is a prerequisite and must be installed on the server. Consider using a one-click container deployment, such as Bitnami
Linux: Either build from source or download from your distribution repo Windows: Download the windows installer (.msi 64-bit) and install using default options.

**Install Workspace ONE UEM SCIM Adapter**

Create your own package directory e.g. /opt/ws1scim and copy the Adapter application within this `<package-root>`.

```
sudo mkdir /opt/ws1scim
cd /opt/ws1scim
sudo tar -zxvf <archivelocation>/ws1_uem_scim_adapter_2003_ga.tar.gz -C /opt/ws1scim/
```

**Startup and verification**

```
sudo node /opt/ws1scim/index.js
```

Start a web browser or use an appropriate CLI client (note, IE does not support JSON content)

```
curl -vv http://localhost:9000/ping
=> Health check with a "hello" response
"Ctrl + c" to stop the Adapter
```

You can use the `/ping` URI as a health check endpoint for load balancers and reverse proxies.

**Configuration**

Edit the `plugin-airwatch.json` configuration file according to your needs.

Below shows an example of `/opt/ws1scim/config/plugin-airwatch.json`

```json
{
  "scimgateway": {
    "scimversion": "2.0",
    "loglevel": "debug",
    "localhostonly": false,
    "port": 9000,
    "auth": {
      "basic": {
        "username": null,
        "password": null
      },
      "bearer": {
        "token": null,
        "jwt": {
          "azure": {
```
You should only need to edit the following configuration items within the `plugin-airwatch.json` file:

- **port** - The Adapter will listen on this port number.
- **loglevel** - error, info or debug. Output to logfile `/opt/ws1scim/logs/plugin-airwatch.log`
- **endpoint** - Contains endpoint specific configuration according to our plugin code. Place your Workspace ONE UEM API base URL i.e. [https://cn135.awmdm.com/api](https://cn135.awmdm.com/api) and UEM API Tenant Code Groups and Settings -> All Settings -> System -> Advanced -> API -> REST API -> API Key into the corresponding fields

## Manual startup

The Adapter can be started from a CLI running in administrative mode

```
sudo node /opt/ws1scim/index.js
```

Ctrl+c to stop

## Automatic startup - Persistent

There are various flavors of Node.js persistent service tools. For example, you can start the Adapter persistently with `forever`:

```
cd /opt/ws1scim/
sudo forever start ./index.js
netstat -an | grep 9000
```

## Other Installation Steps

Undocumented here; you will need to deploy a reverse proxy hosting SSL, and **ProxyPass** to `localhost:9000`. All connections from the source system will be on the public namespace, HTTPS.

## Deployment examples:

- **Bitnami** - Matt Williams
- **Photon** - Camille Debay