Workspace ONE UEM SCIM Adapter

Authors:
Matt Williams, VMware EUC Customer Success Architect
Joe Rainone, VMware EUC Consulting Architect

Latest Version: 1906.ga

Validated through IdP's:

- Microsoft Azure Active Directory
- Okta (On Roadmap)

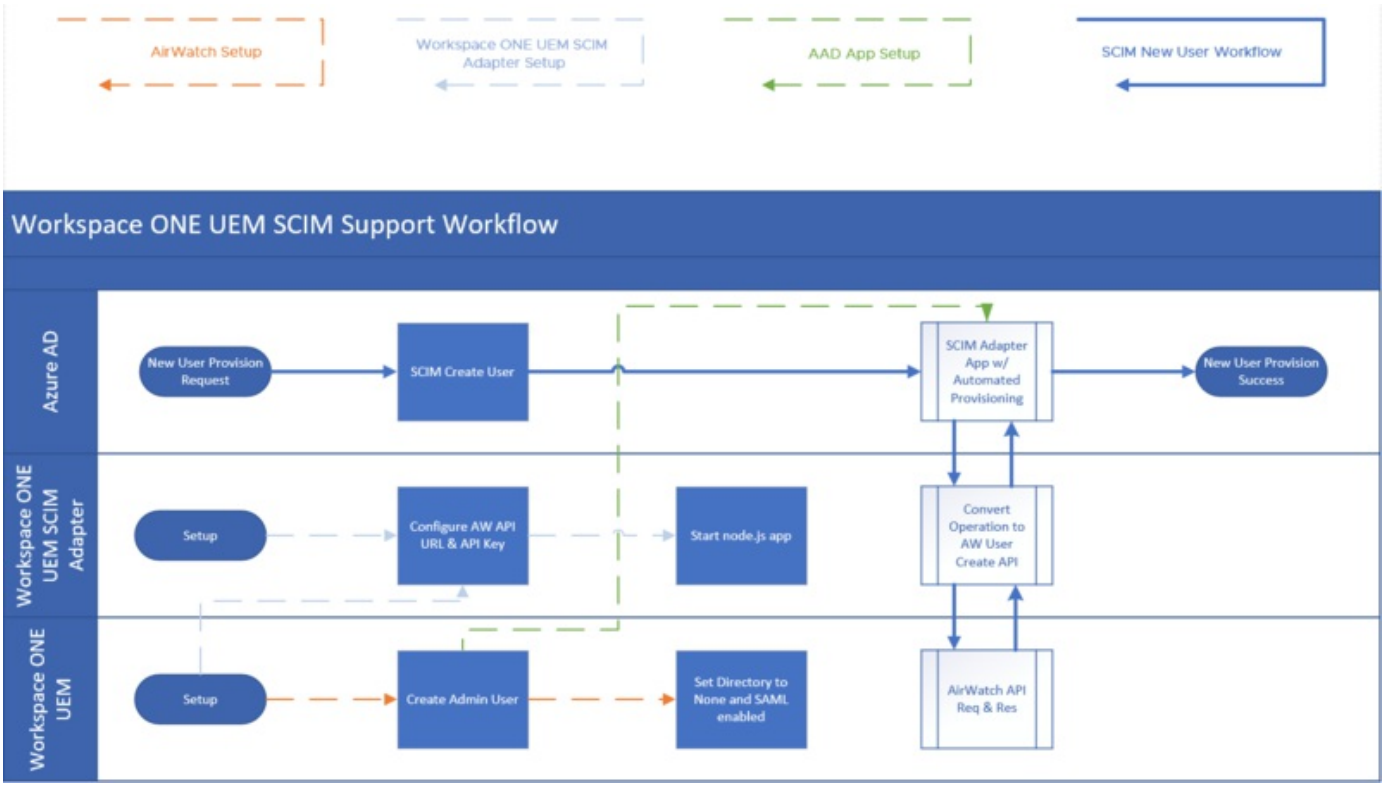
Latest news:

- Initial release now available for Azure AD provisioning

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 -> ExternalId = 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

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)
- Windows 10 OOBE Enrollment (On Roadmap)

2. Resource Attributes:

Identity Provider	**SCIM Adapter**	**Workspace ONE UEM**
UserName	UserName	UserName

ExternalId = ImmutableId	ExternalId	ExternalId
Emails type eq “Work”	Emails	EmailAddress
	Emails	EmailUser
GivenName	GivenName	FirstName
FamilyName	FamilyName	LastName
Formatted = {GivenName + FamilyName}	Formatted	DisplayName
Active = IsSfotDeleted	Active	Status

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 distirbution 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_1906
_beta.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`

```
{
    "scimgateway": {
      "scimversion": "2.0",
      "loglevel": "debug",
      "localhostonly": false,
      "port": 9000,
      "auth": {
        "basic": {
          "username": null,
          "password": null
        },
        "bearer": {
          "token": null,
          "jwt": {
            "azure": {
              "tenantIdGUID": null
            },
            "standard": {
              "secret": null,
              "publicKey": null,
              "options": {
                "issuer": null
              }
            }
          }
        }
      },
```

```
    "certificate": {
      "key": null,
      "cert": null,
      "ca": null,
      "pfx": {
        "bundle": null,
        "password": null
      }
    },
    "emailOnError": {
      "smtp": {
        "enabled": false,
        "host": null,
        "port": 587,
        "proxy": null,
        "authenticate": true,
        "username": null,
        "password": null,
        "sendInterval": 15,
        "to": null,
        "cc": null
      }
    }
  },
  "endpoint": {
    "entity": {
      "undefined": {
        "baseUrl": "https://your_api_server/api",
```

```
            "username": null,
            "password": null,
            "tenantCode": "your_aw-tentant-code"
          }
        }
      }
    }
```

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` 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`

<kbd>Ctrl</kbd>+<kbd>c</kbd> 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