Oracle® Health Sciences Identity and Access Management Service

Inbound User Provisioning Service API Guide

E56188-02

June 2017

ORACLE®

Oracle Health Sciences Identity and Access Management Service Inbound User Provisioning Service API Guide

E56188-02

Copyright © 2014, 2017, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface v

Audience v
Related Documents v
Documentation Accessibility v

1 Getting Started

1.1 Requirements for working with the API 1-1
1.2 User Capabilities 1-1
1.3 Stateless API 1-1
1.4 Encryption 1-1
1.5 Authentication 1-1
1.6 Terminology 1-1
1.7 Detailed API Specifications 1-2

2 Resources

2.1 URL Taxonomy 2-1
2.2 REST Resource Endpoints 2-1
2.2.1 Users 2-1
2.2.2 Groups 2-2
2.2.3 Bulk 2-2
2.3 Resource Schema 2-3
2.3.1 Users 2-3
2.3.2 Groups 2-6
2.3.3 Bulk 2-7
2.4 Return Codes 2-8

3 Inbound Provisioning Service APIs

3.1 User Management API 3-1
3.1.1 Resource-specific Headers 3-1
3.1.1.1 Accept & Content-Type 3-1
3.1.1.2 Authorization 3-1
3.1.2 Create User 3-1
3.1.2.1 Sample Message Exchange 3-2
3.1.3 Full Update User 3-3
3.1.3.1 Sample Message Exchange 3-4

3.1.4 Patch User 3-5
3.1.4.1 Sample Message Exchange 3-5
3.1.5 Retrieve User 3-6
3.1.5.1 Sample Message Exchange 3-6
3.1.6 Search User 3-7
3.1.6.1 Sample Message Exchange 3-8
3.1.7 Delete User 3-8
3.1.7.1 Sample Message Exchange 3-9
3.2 Group Management API 3-9
3.2.1 Resource-specific Headers 3-9
3.2.1.1 Accept & Content-Type 3-9
3.2.1.2 Authorization 3-9
3.2.2 List Groups 3-9
3.2.2.1 Sample Message Exchange 3-10
3.2.3 Retrieve a Group 3-10
3.2.3.1 Sample Message Exchange 3-11
3.2.4 Modify Group Membership 3-12
3.2.4.1 Sample Message Exchange — Add users to a group 3-12
3.2.4.2 Sample Message Exchange — Remove users from a group 3-13
3.2.4.3 Sample Message Exchange — Remove all users from a group 3-14
3.3 Bulk API 3-14
3.3.1 Bulk Request 3-14
3.3.2 Sample Message Exchange 3-15
3.3.3 Sample Message Exchange — Creating and adding the user to a group 3-17

Preface

The Oracle Health Sciences Identity and Access Management Service (OHSIAMS) Inbound User Provisioning Service is a REST web service that provides administrators with user and role management functionality. It is based on the SCIM (System for Cross-Domain Identity Management) REST protocol and built on Oracle Identity Manger (OIM), a console for administrators to manage users and assign appropriate business service authorizations.

Audience

This guide is intended for the development team of an application that uses the Inbound User Provisioning Service API to push data to the OHSIAMS user store. This guide describes the API web services, resources, and requests used to push new or updated user data or to record the removal of user data.

Related Documents

For more information, see the following documents on the `Oracle Help Center`:

- *Oracle Health Sciences Identity and Access Management Service Administrator Guide*
- *Oracle Health Sciences Identity and Access Management Services Secure Development Guide*

> **Note:** Always check the `Oracle Help Center` to ensure you have the latest documentation.

The following documents are available on My Oracle Support for authenticated users:

- *Oracle Health Sciences Identity and Access Management Service Release Notes*, ID 1964916.1
- *Oracle Health Sciences Identity and Access Management Service Known Issues*, ID 2020737.1

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1 Getting Started

The OHSIAMS Inbound User Provisioning Service API is a web services interface into the OHSIAMS application. It is an HTTP-based API that is technology and platform independent.

1.1 Requirements for working with the API

To use the OHSIAMS Inbound User Provisioning Service API, the client must be able to issue HTTP GET, POST, PUT, PATCH, and DELETE calls.

1.2 User Capabilities

The user specified in the call to the API must have appropriate OIM roles to perform the administration operations.

1.3 Stateless API

The OHSIAMS Inbound User Provisioning Service API that the application exposes is stateless. This means that each call is independent of the previous call, and the information conveyed by the client in the request must be sufficient for the server to understand and act on the request.

1.4 Encryption

All communication with the OHSIAMS Inbound User Provisioning Service API is encrypted and secured using HTTPS connections.

1.5 Authentication

The OHSIAMS Inbound User Provisioning Service API is protected by the Basic Authentication scheme. Basic authentication headers must be part of each request. The username must be tenant-qualified (<tenant>.username).

1.6 Terminology

The keywords *must*, *must not*, *required*, *shall*, *shall not*, *should*, *should not*, *recommended*, *may*, and *optional* in this document are to be interpreted as described in RF C 2119.

1.7 Detailed API Specifications

The following chapters describe the OHSIAMS Inbound User Provisioning Service API, grouped by OHSIAMS resources. In the URLs shown, values within braces {} are meant to be placeholders for the ID of a specific instance of the resource.

Each OHSIAMS API specification includes the following information:

- Purpose
- HTTP request method: GET, DELETE, PATCH, POST, PUT
- URL: the URL to which the call is made
- Request schema URI
- Response schema URI
- HTTP response codes
- Sample output in JSON.

2

Resources

The OHSIAMS Inbound User Provisioning Service API exposes resources through distinct URLs and the HTTP method calls dictate the action that is required to be performed on the identified resource. OHSIAMS resources include Users, Groups, and Bulk.

2.1 URL Taxonomy

The OHSIAMS Inbound User Provisioning Service API follows the URL taxonomy:

https://hs-identity-api.us.oracleindustry.com/scim/v1/<tenant>/<resource>

where

<tenant> determines the tenancy of the target resource. The OIM entitlements validate whether the authenticated user has the appropriate privileges to create or read resources in the specified tenant.

<resource> can be:

- /Users
- /Users/{id}
- /Groups
- /Groups/{groupname}
- /Bulk

2.2 REST Resource Endpoints

The resources component provides the REST resource endpoints as described in the SCIM specification.

2.2.1 Users

The */Users* resource endpoint handles user management operations.

Table 2–1 Using HTTP Methods with the Users Resource Endpoint

HTTP Method	Path	Description
GET	/Users/{id}	Given the ID of the user, returns the OIM user, if it exists.

Table 2–1 (Cont.) Using HTTP Methods with the Users Resource Endpoint

HTTP Method	Path	Description
GET	/Users?filter={filterName} eq "<username | externalId>"&attributes={comma separated attributes}	Searching for the user requires a filter. Supported filters are *userName* and *externalId*. The accepted operator is *eq*. *Attributes* is optional.
POST	/Users	Creates a user in OIM. Existing OHSIAMS validations apply while creating the user.
PUT	/Users/{id}	Replaces all the attributes of the user. If an attribute is not specified, the value is removed from the user in OIM.
PATCH	/Users/{id}	Updates only the specified attributes.
DELETE*	/Users/{id}	To maintain audit history, you cannot delete a user in the OHSIAMS application. Instead, the account is disabled and all the current roles and groups are revoked for this user account.

*After a user is deleted, when a new user request is received that matches the deleted (disabled) username in OIM, the application returns a 303 Redirect response with the location of the disabled user. You can either enable the user at this location or pick a new username and resubmit the request.

If the username in the new user request matches an active user, the application returns a 412 Precondition Failed with *username already exists* error message.

2.2.2 Groups

The */Groups* resource endpoint handles group management operations.

Table 2–2 Using HTTP Methods with the Groups Resource Endpoint

HTTP Method	Path	Description
GET	/Groups/{groupname}	Given the groupname, returns the group description and the list of OIM users currently assigned to the group.
GET	/Groups	Returns a list of groupnames under the given tenant.
PATCH	/Groups/groupname	Updates the group membership.

Note: Creation and deletion of a role in OIM is not supported for the tenant administrator role. Therefore, there is no support for the POST and DELETE operations.

2.2.3 Bulk

The */Bulk* resource endpoint handles bulk operations.

Table 2–3 Using HTTP Methods with the Bulk Resource Endpoint

HTTP Method	Path	Description
POST	/Bulk	Performs the bulk operations.

2.3 Resource Schema

The OHSIAMS Inbound User Provisioning Service API is a service provider implementation of the SCIM 2.0 specification. It uses the SCIM resource definition schema. Not all the SCIM schema attributes are required or supported. Below are the SCIM schema attributes supported by OHSIAMS.

2.3.1 Users

URI → **urn:scim:schemas:core:2.0:User**

Table 2–4 Supported SCIM Schema Attributes for Users

SCIM Attribute	Constraint: Mutability	Constraint: Uniqueness	Constraint: Required	Description
id	Read Only	Unique on the server across tenants.	True (generated by service provider).	32-character GUID generated by OHSIAMS. Example: `"id":"82be808061044f9e9cef4c8f08d53ef0"`
externalId	Read Write	Unique on the server within a tenant.	False	Generated by the client. Must be unique within a tenant. OHSIAMS internally stores the externalId with tenant prefix. The combination of tenant plus externalId must not exceed 255 characters. Example: `"externalId":"john.doe@customer.com"`

Table 2–4 (Cont.) Supported SCIM Schema Attributes for Users

SCIM Attribute	Constraint: Mutability	Constraint: Uniqueness	Constraint: Required	Description
username	Read Write	Unique on the server within a tenant.	True	The non-tenant-qualified username. OHSIAMS internally stores the username with tenant prefix. This username is used to log into OHSIAMS-protected applications. The tenancy of the user is derived from the request URL of the resource. Valid usernames are any combination of the following characters: [a-z], [A-Z], [0-9], space ( ), dash (-), and period (.). If the username is a valid email address, the at-sign (@) is permitted. The username must contain at least 4 characters. The combination of tenant plus username must not exceed 255 characters. Example: `"userName": "JOHN.DOE"`

name.givenName	Read
	Write
		None	True	User's first name.
				Length must be between 1 and 150 characters.
				Example:
				`"name":{`
				`"familyName":"Doe",`
				`"givenName":"John"`
				`}`

name.familyName	Read
	Write
		None	True	User's last name.
				Length must be between 1 and 150 characters.
				Example:
				`"name":{`
				`"familyName":"Doe",`
				`"givenName":"John"`
				`}`

emails [work]	Read
	Write
		None	True	OHSIAMS supports a single value of the *work* type.
				Example:
				`"emails":[{`
				`"value":"john.doe@customer.com",`
				`"type":"work"`
				`}]`

Table 2–4 (Cont.) Supported SCIM Schema Attributes for Users

SCIM Attribute	Constraint: Mutability	Constraint: Uniqueness	Constraint: Required	Description
phoneNumbers [work]	Read Write	None	False	OHSIAMS supports a single value of the *work* type. Example: `"phoneNumbers":[ { "value": "555-555-5555", "type":"work" }`
active	Read Write	None	False	Account Status. SCIM:TRUE → IAMS: Active, SCIM:FALSE → IAMS: Disable A user status can be Disabled in OHSIAMS if: ■ User has been disabled via a PATCH SCIM request. The user status is marked as disabled without removing any of the user's prior roles. ■ User has been issued a DELETE SCIM request. The user status is marked as disabled after removing any of the user's existing roles. You can only specify this attribute in a PATCH request. It must be specified alone (without any other user attributes). Example: `"active":true`
password	Write Only	None	False	Auto-generated if a value is not specified in the POST request. A password change is not allowed in a PUT request. A PATCH request must be specified alone (without any other user attributes). Updating the password (via PATCH) also unlocks the user account if it has been locked. Must adhere to OHSIAMS password policies. Example: `"password":"P@ssW0r3"`

Table 2–4 (Cont.) Supported SCIM Schema Attributes for Users

SCIM Attribute	Constraint: Mutability	Constraint: Uniqueness	Constraint: Required	Description
groups	Read Only	None	False	Lists the authorized business services of the current user. Example: `"groups":[ { "value": "<tenant>*.bizsvcrole", "display":"bizsvcrole" } ]` *<tenant> is the owner of the service.
meta	Read Only	None	False	Includes the user creation date, last update date, and location. Example: `"meta":{ "created": "2014-05-29T18:00:35Z", "lastModified": "2014-05-29T18:00:35Z", "location": "http://hs-identity-api.oracleindustry.com /scim/v1/mypharms/User/54dc4a653ee71a34e3a783883c744", "resourceType":"User" }`

2.3.2 Groups

URI → **urn:scim:schemas:core:2.0:Group**

Table 2–5 Supported SCIM Schema Attributes for Groups

SCIM Attribute	Constraint: Mutability	Constraint: Uniqueness	Constraint: Required	Description
Id	Read Only	Unique on the server across tenants.	True	SCIM group ID is a tenant-qualified business service name (OIM role) in OHSIAMS. Example: `"id":"<tenant>.pfst51trial"`
displayName	Read Only	None	False	Non-tenant-qualified business service name. Example: `"displayName":"pfst51trial"`
members	Read Write	None	False	Multivalued complex type.
members.value	Read Write	None	False	SCIM ID of the user.

Table 2–5 (Cont.) Supported SCIM Schema Attributes for Groups

SCIM Attribute	Constraint: Mutability	Constraint: Uniqueness	Constraint: Required	Description
members.display	Read Only	None	False	Non-tenant-qualified username.
members.$ref	Read Only	None	False	Location URI of the member. Example: `http://hs-identity-api.oci.com/scim/v1/<tenant>/Users/82be808061044f9e9cef4c8f08d53ef0`
members.type	Read Only	None	False	Of the type *User*. OHSIAMS does not support nested roles in OIM.
meta	Read Only	None	False	Group creation date and the last update date. Example: `"meta":{ "created": "2014-05-29T18:00:35Z", "lastModified": "2014-05-29T18:00:35Z", "resourceType":"Group" }`

2.3.3 Bulk

URI → **urn:scim:schemas:core:2.0:BulkRequest/BulkResponse**

Bulk requests and bulk responses share many attributes. Unless otherwise specified, each attribute below is present in both bulk requests and bulk responses.

Table 2–6 Supported SCIM Schema Attributes for Bulk

SCIM Attribute	Constraint: Uniqueness	Constraint: Required	Description
failOnErrors	None	False	An integer specifying the number of errors allowed before the operation is terminated and an error response is returned. Only the operations that are processed until the *failOnErrors* limit is reached are returned in the BulkResponse. The rest of the operations are ignored. Optional in a request. Not valid in a response.
Operations	None	True	Complex multivalued attribute.
Operations.method	None	True	The HTTP method of the current operation. Possible values are: ▪ POST, PUT, PATCH, or DELETE for User operations. ▪ PATCH for Group operations.

Table 2–6 (Cont.) Supported SCIM Schema Attributes for Bulk

SCIM Attribute	Constraint: Uniqueness	Constraint: Required	Description
Operations.bulkId	Must be unique within a bulk request.	False	The *bulkId* is a surrogate resource ID, enabling clients to uniquely identify newly created resources in the response and to cross-reference new resources in and across operations within a bulk request. Required when method is POST.
Operations.path	None	True	The relative path of the resource. If the method is POST, the value must specify a resource type endpoint (for example, */Users*). All other method values must specify the path to a specific resource (for example, */Users/2819c2237f76453a919d*)
Operations.data	None	True for all except the DELETE method.	The resource data for the bulk POST, PUT, or PATCH resource operation as a single request.
Operations.location	None	True for response.	The resource endpoint URL. Required in a response, except in the event of a POST failure.
Operations.status	None	True for response.	A complex type that contains information about the success or failure of one operation within the bulk request. Required in a response.
Operations.status.code	None	True for response.	The HTTP response code returned for the bulk operation as a single request. Required.
Operations.status.description	None	False	A human-readable error message. Required when an error occurs.

2.4 Return Codes

In addition to returning an HTTP response code, the OHSIAMS Inbound User Provisioning Service API returns errors in the body of the response with error code and descriptions, as well as messages describing successful requests.

Table 2–7 HTTP Return Codes

HTTP Return Code	Description
200	Request processed successfully.
201	Request has been processed and a new resource has been created.
204	The server has fulfilled the request, but does not return a response (in a DELETE request).

Table 2–7 (Cont.) HTTP Return Codes

HTTP Return Code	Description
303	See Other redirect. (If a user with similar user name or externalId exists in a DISABLED state, the location of the user is sent in the response.)
401	Unauthorized. (User is not authenticated.)
403	Forbidden. (User is not authorized for the operation.)
404	Not found.
412	Precondition failed. (One or more validations failed. Refer to the error response for remediation.)
415	Client media type unsupported. (Only application/JSON is supported for all operations.)
500	Generic server failure.
501	Requested method or operation is not implemented.

3

Inbound Provisioning Service APIs

The APIs can be classified into three categories:

- **User Management**—Search, create, update, delete, disable, or change password for users.
- **Group Management**—List group members, add and remove members from the group.
- **Bulk**—Send a potentially large collection of resource operations in a single request.

3.1 User Management API

The SCIM */Users* resource endpoint is used for several user management operations.

3.1.1 Resource-specific Headers

Depending on the resource type, the following headers apply.

3.1.1.1 Accept & Content-Type

```
Accept: application/json
Content-Type: application/json;charset=UTF-8
```

3.1.1.2 Authorization

```
Authorization: Basic username: password
```

The username:password must be BASE64 encoded.

3.1.2 Create User

Table 3–1 Create User

HTTP Request Method	POST
URI	https://hs-identity-api.oracleindustry.com/scim/v1/<tenant>/Users
Request schema URI	urn:scim:schemas:core:2.0:User
Response schema URI	urn:scim:schemas:core:2.0:User

Table 3–1 (Cont.) Create User

HTTP Response Codes	The following response codes apply: ■ 201 ■ 303 ■ 400 ■ 401 ■ 403 ■ 404 ■ 412 For more information, see Section 2.4, "Return Codes".

3.1.2.1 Sample Message Exchange

Request

```
POST /scim/v1/mypharma/Users HTTP 1.1
Host: example.com
Authorization: Basic Y3VzdG9tZXIuYWRtaW51c2VyOnBhc3N3b3Jk=
Accept: application/json
Content-Type: application/json;charset=UTF-8
Content-Length: ...
{
    "schemas" : [
        "urn:scim:schemas:core:2.0:User"
    ],
    "externalId" : "john.doe@customer.com",
    "userName" : "john.doe",
    "name" : {
        "familyName" : "Doe",
        "givenName" : "John"
    },
    "emails" : [
        {
            "value" : "john.doe@mypharma.com",
            "type" : "work"
        }
    ],
    "phoneNumbers" : [
        {
            "value" : "555-555-5555",
            "type" : "work"
        }
    ],
    "password" : "S0M3P@ssw0rd"
}
```

Response

```
HTTP/1.1 201 Created
Content-Type: application/json
Content-Length: ...
Location https://hs-identity-api.oracleindustry.com/scim/v1/mypharma/
Users/5a5dc886031d49088cc01f723daa1f4e
{
    "schemas" : [
        "urn:scim:schemas:core:2.0:User"
    ],
```

```
    "id" : "5a5dc886031d49088cc01f723daa1f4e",
    "externalId" : "john.doe@mypharma.com",
    "userName" : "JOHN.DOE",
    "name" : {
        "familyName" : "Doe",
        "givenName" : "John"
    },
    "emails" : [
        {
            "value" : "john.doe@mypharma.com",
            "type" : "work"
        }
    ],
    "phoneNumbers" : [
        {
            "value" : "555-555-5555",
            "type" : "work"
        }
    ],
    "userType" : "LIVE",
    "active" : true,
    "meta" : {
        "created" : "2014-05-20T14:02:57Z ",
        "lastModified" : "2014-05-20T14:02:57Z ",
"location": "https://hs-identity-
api.oracleindustry.com/scim/v1/mypharma/Users/5a5dc886031d49088cc01f723daa1f4e",
        "resourceType": "User"
    }
}
```

3.1.3 Full Update User

Replaces the user attributes with the attributes specified in the request content. If an attribute is not specified, the value of that attribute is replaced as null.

If a password is not specified, the existing password is not altered.

Table 3–2 Replace User

HTTP Request Method	PUT
URI	https://hs-identity-api.oracleindustry.com/scim/v1/<tenant>/Users/{id}
Request schema URI	urn:scim:schemas:core:2.0:User
Response schema URI	urn:scim:schemas:core:2.0:User
HTTP Response Codes	The following response codes apply: ■ 200 ■ 400 ■ 401 ■ 403 ■ 404 ■ 412 For more information, see Section 2.4, "Return Codes".

3.1.3.1 Sample Message Exchange

Request

```
PUT /scim/v1/mypharma/Users/5a5dc886031d49088cc01f723daa1f4e HTTP 1.1
Host: example.com
Authorization: Basic Y3VzdG9tZXIuYWRtaW51c2VyOnBhc3N3b3Jk=
Accept: application/json
Content-Type: application/json;charset=UTF-8
Content-Length: ...
{
    "schemas" : [
        "urn:scim:schemas:core:2.0:User"
    ],
    "externalId" : "john.doe@mypharma.com",
    "userName" : "john.doe",
    "name" : {
        "familyName" : "Doe",
        "givenName" : "John"
    },
    "emails" : [
        {
            "value" : "john.doe@mypharma.com",
            "type" : "work"
        }
    ]
}
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: ...
Location https://hs-identity-api.oracleindustry.com/scim/v1/mypharma/
Users/5a5dc886031d49088cc01f723daa1f4e
{
    "schemas" : [
        "urn:scim:schemas:core:2.0:User"
    ],
    "id" : "5a5dc886031d49088cc01f723daa1f4e",
    "externalId" : "john.doe@mypharma.com",
    "userName" : "JOHN.DOE",
    "name" : {
        "familyName" : "Doe",
        "givenName" : "John"
    },
    "emails" : [
        {
            "value" : "john.doe@mypharma.com",
            "type" : "work"
        }
    ],
    "userType" : "LIVE",
    "active" : true,
    "meta" : {
        "created" : "2014-05-20T14:02:57Z",
        "lastModified" : "2014-06-06T13:48:48Z",
"location": "https://hs-identity-
api.oracleindustry.com/scim/v1/mypharma/Users/5a5dc886031d49088cc01f723daa1f4e",
        "resourceType": "User"
    }
```

```
}
```

3.1.4 Patch User

Use HTTP PATCH when only a portion of the user attributes are required to be changed.

Table 3–3 Patch User

HTTP Request Method	PATCH
URI	https://hs-identity-api.oracleindustry.com/scim/v1/<tenant>/Users/{id}
Request schema URI	JSON Patch format (Refer to SCIM specification)
Response schema URI	urn:scim:schemas:core:2.0:User
HTTP Response Codes	The following response codes apply: ■ 200 ■ 400 ■ 401 ■ 403 ■ 404 ■ 412 For more information, see Section 2.4, "Return Codes".

3.1.4.1 Sample Message Exchange

Request

```
PATCH /scim/v1/customer/Users/5a5dc886031d49088cc01f723daa1f4e HTTP 1.1
Host: example.com
Authorization: Basic Y3VzdG9tZXIuYWRtaW51c2VyOnBhc3N3b3Jk=
Accept: application/json
Content-Type: application/json;charset=UTF-8
Content-Length: ...
{
  "op":"replace",
  "path":"name",
  "value":{
    "familyName":"Does",
    "givenName":"Johnathan"
  }
}
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: ...
Location https://hs-identity-api.oracleindustry.com/scim/v1/mypharma/
Users/5a5dc886031d49088cc01f723daa1f4e
{
    "schemas" : [
        "urn:scim:schemas:core:2.0:User"
    ],
    "id" : "5a5dc886031d49088cc01f723daa1f4e",
```

```
    "externalId" : "john.doe@mypharma.com",
    "userName" : "JOHN.DOE",
    "name" : {
        "familyName" : "Does",
        "givenName" : " Johnathan "
    },
    "emails" : [
        {
            "value" : "john.doe@mypharma.com",
            "type" : "work"
        }
    ],
    "phoneNumbers" : [
        {
            "value" : "555-555-5555",
            "type" : "work"
        }
    ],
    "userType" : "LIVE",
    "active" : true,
    "meta" : {
         "created" : "2014-05-20T14:02:57Z",
        "lastModified" : "2014-06-06T13:48:48Z",
"location": "https://hs-identity-
api.oracleindustry.com/scim/v1/mypharma/Users/5a5dc886031d49088cc01f723daa1f4e",
        "resourceType": "User"
    }
}
```

3.1.5 Retrieve User

Table 3–4 Retrieve User

HTTP Request Method	GET
URI	https://hs-identity-api.oracleindustry.com/scim/v1/<tenant>/Users/{id}
Request schema URI	NA
Response schema URI	urn:scim:schemas:core:2.0:User
HTTP Response Codes	The following response codes apply: ■ 200 ■ 401 ■ 403 ■ 404 For more information, see Section 2.4, "Return Codes".

3.1.5.1 Sample Message Exchange

Request

```
GET /scim/v1/mypharma/Users/5a5dc886031d49088cc01f723daa1f4e HTTP 1.1
Host: example.com
Authorization: Basic Y3VzdG9tZXIuYWRtaW51c2VyOnBhc3N3b3Jk=
Accept: application/json
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: ...
Location https://hs-identity-api.oracleindustry.com/scim/v1/mypharma/
Users/5a5dc886031d49088cc01f723daa1f4e
{
    "schemas" : [
        "urn:scim:schemas:core:2.0:User"
    ],
    "id" : "5a5dc886031d49088cc01f723daa1f4e",
    "externalId" : "john.doe@mypharma.com",
    "userName" : "JOHN.DOE",
    "name" : {
        "familyName" : "Doe",
        "givenName" : "John"
    },
    "emails" : [
        {
            "value" : "john.doe@mypharma.com",
            "type" : "work"
        }
    ],
    "phoneNumbers" : [
        {
            "value" : "555-555-5555",
            "type" : "work"
        }
    ],
    "userType" : "LIVE",
    "active" : true,
    "meta" : {
        "created" : "2014-02-30T14:02:57Z",
        "lastModified" : "2014-02-30T14:02:57Z",
"location": "https://hs-identity-
api.oracleindustry.com/scim/v1/mypharma/Users/5a5dc886031d49088cc01f723daa1f4e",
        "resourceType": "User"
    }
}
```

3.1.6 Search User

The HTTP GET method searches for a user based on the filter query parameter. Wildcard characters are not allowed in the filter value. If a user is found, GET returns only one result object.

The result set returns the entire user object. This can be restricted to return only the attributes specified in the attributes query parameter

Allowed filters: *userName*, *externalId*.

Sample: /Users?filter=userName+Eq+"john.doe"&attributes=id,externalId

Table 3–5 Search User

HTTP Request Method	GET
URI	https://hs-identity-api.oracleindustry.com/scim/v1/<tenant>/Users

Table 3–5 (Cont.) Search User

Query Parameters	filter={filterName} A filter is required. The allowed filter names are *externalId* and *userName*.
Request schema URI	NA
Response schema URI	urn:scim:schemas:core:2.0:ListResponse
HTTP Response Codes	The following response codes apply: ■ 200 ■ 401 ■ 403 ■ 404 For more information, see Section 2.4, "Return Codes".

3.1.6.1 Sample Message Exchange

Request

```
GET
/scim/v1/mypharma/Users?filter=externalId+Eq+"john.doe@mypharma.com"&attributes=id
,externalId HTTP 1.1
Host: example.com
Authorization: Basic Y3VzdG9tZXIuYWRtaW51c2VyOnBhc3N3b3Jk=
Accept: application/json
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: ...
{
    "schemas" : [
        "urn:scim:schemas:core:2.0:ListResponse"
    ],
    "totalResults" : 1,
     "Resources" : [
          {
              "schemas" : [
                "urn:scim:schemas:core:2.0:User"
            ],
            "id" : "82be808061044f9e9cef4c8f08d53ef0",
            "externalId" : "john.doe@mypharma.com"
      }
    ]
}
```

3.1.7 Delete User

To maintain an audit history, a user cannot be deleted from the OHSIAMS application. Instead, the account is disabled and all the current roles or groups are revoked for this user account.

For more details on user resources related to DELETE, see Section 2.2.1, "Users".

Table 3–6 Delete User

HTTP Request Method	DELETE
URI	https://hs-identity-api.oracleindustry.com/scim/v1/<tenant>/Users
Request schema URI	NA
Response schema URI	NA
HTTP Response Codes	The following response codes apply: ■ 204 ■ 401 ■ 403 ■ 404 For more information, see Section 2.4, "Return Codes".

3.1.7.1 Sample Message Exchange

Request

```
DELETE /scim/v1/mypharma/Users/cb72d08d626041dfbec77014dbe35861
HTTP 1.1
Host: example.com
Authorization: Basic Y3VzdG9tZXIuYWRtaW51c2VyOnBhc3N3b3Jk=
Accept: application/json
```

Response

```
HTTP/1.1 204 No Content
```

3.2 Group Management API

The SCIM */Groups* resource endpoint assigns and revokes users from an OHSIAMS group. Only the operations listed below are supported.

3.2.1 Resource-specific Headers

Depending on the resource type, the following headers apply.

3.2.1.1 Accept & Content-Type

```
Accept: application/json
Content-Type: application/json;charset=UTF-8
```

3.2.1.2 Authorization

```
Authorization: Basic username: password
```

The username:password must be BASE64 encoded.

3.2.2 List Groups

Table 3–7 List Groups

HTTP Request Method	GET

Table 3–7 (Cont.) List Groups

URI	https://hs-identity-api.oracleindustry.com/scim/v1/<tenant>/Groups
Request schema URI	NA
Response schema URI	urn:scim:schemas:core:2.0:ListResponse
HTTP Response Codes	The following response codes apply: ■ 200 ■ 401 ■ 403 ■ 404 For more information, see Section 2.4, "Return Codes".

3.2.2.1 Sample Message Exchange

Request

```
GET /scim/v1/mypharma/Groups HTTP 1.1
Host: example.com
Authorization: Basic Y3VzdG9tZXIuYWRtaW51c2VyOnBhc3N3b3Jk=
Accept: application/json
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: ...
{
    "schemas" : [
        "urn:scim:schemas:core:2.0:ListResponse"
    ],
    "totalResults" : 3,
    "Resources" : [
        {
            "id" : "mypharma.lshdme"
        },
        {
            "id" : "mypharma.pfst50"
        },
        {
            "id" : "mypharma.argussafety"
        }
    ]
}
```

3.2.3 Retrieve a Group

Table 3–8 Retrieve a Group

HTTP Request Method	GET
URI	https://hs-identity-api.oracleindustry.com/scim/v1/<tenant>/Groups/{groupname}
Request schema URI	NA

Table 3–8 (Cont.) Retrieve a Group

Response schema URI	urn:scim:schemas:core:2.0:Group
HTTP Response Codes	The following response codes apply: ■ 200 ■ 401 ■ 403 ■ 404 For more information, see Section 2.4, "Return Codes".

3.2.3.1 Sample Message Exchange

Request

```
GET /scim/v1/mypharma/Groups/mypharma.lhsdme HTTP 1.1
Host: example.com
Authorization: Basic Y3VzdG9tZXIuYWRtaW51c2VyOnBhc3N3b3Jk=
Accept: application/json
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: ...
{
    "schemas" : [
        "urn:scim:schemas:core:2.0:Group"
    ],
    "id" : "mypharma.lshdme",
    "displayName" : "lshdme",
    "members" : [
        {
            "value" : "82be808061044f9e9cef4c8f08d53ef0",
            "display" : "tony.stark",
            "$ref" :
"https://hs-identity-api.oracleindustry.com/scim/v1/mypharma/Users/82be808061044f9
e9cef4c8f08d53ef0"
        },


        {
            "value" : "8a0722126d914a5faa3d18ab806d2310",
            "display" : "mjack635375460126150000",
            "$ref" :
"https://hs-identity-api.oracleindustry.com/scim/v1/mypharma/Users/8a0722126d914a5
faa3d18ab806d2310"
        },

        {
            "value" : "47af6c8070c54eb4bfcf60554e582ac1",
            "display" : "user123abc456id",
            "$ref" :
"https://hs-identity-api.oracleindustry.com/scim/v1/mypharma/Users/47af6c8070c54eb
4bfcf60554e582ac1"
        }
    ],
    "meta" : {
        "created" : "2014-06-01T14:22:38Z",
```

```
        "resourceType" : "Group"
    }
}
```

3.2.4 Modify Group Membership

Table 3–9 Modify Group Membership

HTTP Request Method	PATCH
URI	https://hs-identity-api.oracleindustry.com/scim/v1/<tenant>/Groups/{groupname}
Request schema URI	JSON PATCH format
Response schema URI	urn:scim:schemas:core:2.0:Group
HTTP Response Codes	The following response codes apply: ■ 200 ■ 401 ■ 403 ■ 404 ■ 412 For more information, see Section 2.4, "Return Codes".

3.2.4.1 Sample Message Exchange — Add users to a group

Request

```
PATCH /scim/v1/mypharma/Groups/mypharma.lhsdme HTTP 1.1
Host: example.com
Authorization: Basic Y3VzdG9tZXIuYWRtaW51c2VyOnBhc3N3b3Jk=
Accept: application/json
Content-Type: application/json
Content-Length: ...
{
   "op":"add",
   "path":"members",
    "value":[
        {  "value": "2819c2237f76453a919d413861904646" },
        {  "value": "c68580ea3b82486a969b2b801ffd2aa8" }
    ]
}
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: ...
{
    "schemas" : [
        "urn:scim:schemas:core:2.0:Group"
    ],
    "id" : "mypharma.lshdme",
    "displayName" : "lshdme",
    "members" : [
        {
```

```
            "value" : "82be808061044f9e9cef4c8f08d53ef0",
            "display" : "tony.stark",
            "$ref" :
"https://hs-identity-api.oracleindustry.com/scim/v1/mypharma/Users/82be808061044f9
e9cef4c8f08d53ef0"
        },
        {
            "value" : "2819c2237f76453a919d413861904646",
            "display" : "mjack635375460126150000",
            "$ref" :
"https://hs-identity-api.oracleindustry.com/scim/v1/mypharma/Users/8a0722126d914a5
faa3d18ab806d2310"
        },
        {
            "value" : " c68580ea3b82486a969b2b801ffd2aa8",
            "display" : "user123abc456id",
            "$ref" :
"https://hs-identity-api.oracleindustry.com/scim/v1/mypharma/Users/47af6c8070c54eb
4bfcf60554e582ac1"
        }
    ],
    "meta" : {
        "created" : "2014-06-01T14:22:38Z",
        "resourceType" : "Group"
    }
}
```

3.2.4.2 Sample Message Exchange — Remove users from a group

Request

```
PATCH /scim/v1/mypharma/Groups/mypharma.lhsdme HTTP 1.1
Host: example.com
Authorization: Basic Y3VzdG9tZXIuYWRtaW51c2VyOnBhc3N3b3Jk=
Accept: application/json
Content-Type: application/json
Content-Length: ...
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: ...
{
    "schemas" : [
        "urn:scim:schemas:core:2.0:Group"
    ],
    "id" : "mypharma.lshdme",
    "displayName" : "lshdme",
    "members" : [
        {
            "value" : "82be808061044f9e9cef4c8f08d53ef0",
            "display" : "tony.stark",
            "$ref" :
"https://hs-identity-api.oracleindustry.com/scim/v1/mypharma/Users/82be808061044f9
e9cef4c8f08d53ef0"
        }
    ],
    "meta" : {
        "created" : "2014-06-01T14:22:38Z",
        "resourceType" : "Group"
```

```
    }
}
```

3.2.4.3 Sample Message Exchange — Remove all users from a group

Request

```
PATCH /scim/v1/mypharma/Groups/mypharma.lhsdme HTTP 1.1
Host: example.com
Authorization: Basic Y3VzdG9tZXIuYWRtaW51c2VyOnBhc3N3b3Jk=
Accept: application/json
Content-Type: application/json
Content-Length: ...
{
   "op":"remove",
   "path":"members"
}
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: ...
{
    "schemas" : [
        "urn:scim:schemas:core:2.0:Group"
    ],
    "id" : "mypharma.lshdme",
    "displayName" : "lshdme",
    "members" : [  ],
    "meta" : {
        "created" : "2014-06-01T14:22:38Z",
        "resourceType" : "Group"
    }
}
```

3.3 Bulk API

The SCIM */Bulk* resource endpoint sends a potentially large collection of resource operations in a single request.

Bulk operations are handled in the order they appear in the POST content. When using the surrogate bulkId, you must ensure that the POST operation that generates the ID for the bulkId occurs before any update operations are performed for that bulkId.

3.3.1 Bulk Request

Table 3–10 Bulk Request

HTTP Request Method	POST
URI	https://hs-identity-api.oracleindustry.com/scim/v1/<tenant>/Bulk
Request schema URI	urn:scim:schemas:core:2.0:BulkRequest
Response schema URI	urn:scim:schemas:core:2.0:BulkResponse

Table 3–10 (Cont.) Bulk Request

HTTP Response Codes	The following response codes apply: ■ 200 ■ 401 ■ 403 ■ 412 ■ 413 For more information, see Section 2.5, Return Codes.

Note: A successful POST on Bulk might not mean that the entire set of operations is successful. The client must iterate the BulkResponse to validate the status of each operation.

3.3.2 Sample Message Exchange

Request

```
POST /scim/v1/mypharma/Bulk HTTP 1.1
Host: example.com
Authorization: Basic Y3VzdG9tZXIuYWRtaW51c2VyOnBhc3N3b3Jk=
Accept: application/json
Content-Type: application/json
Content-Length: ...
{
  "schemas": ["urn:scim:schemas:core:2.0:BulkRequest"],
  "failOnErrors":1,
  "Operations":[
    {
      "method":"POST",
      "path":"/Users",
      "bulkId":"qwerty",
      "data":{
        "schemas": ["urn:scim:schemas:core:2.0:User"],
        "userName":"Alice"
      }
    },
    {
      "method":"PUT",
      "path":"/Users/b7c14771-226c-4d05-8860-134711653041",
      "data":{
        "schemas": ["urn:scim:schemas:core:2.0:User"],
        "id":"b7c14771134711653041",
        "userName":"Bob"
      }
    },
    {
      "method": "PATCH",
      "path": "/Users/5d8d29d3a3cb6763ffcc",
      "data": [
        {
            "op": "remove",
            "path": "phoneNumbers"
        },
        {
            "op": "replace",
```

```
            "path": "userName",
            "value": "Jonh.doe@mypharma.com"
        }
      ]
    },
    {
      "method":"DELETE",
      "path":"/Users/e90253151e07454e468b"
    }
  ]
}
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: ...
{
    "schemas": ["urn:scim:schemas:core:2.0:BulkResponse"],
    "Operations": [
        {
            "location":
"https://hs-identity-api.oracleindustry.com/scim/v1/mypharma/Users/92b725cd01f8e14
6b87a",
            "method": "POST",
            "bulkId": "qwerty",
            "status": {
                "code": "201"
            }
        },
        {
            "location":
"https://hs-identity-api.oracleindustry.com/scim/v1/mypharma/Users/b7c147711347116
53041",
            "method": "PUT",
            "status": {
                "code": "200"
            }
        },
        {
            "location":
"https://hs-identity-api.oracleindustry.com/scim/v1/mypharma/Users/5d8d29d3a3cb676
3ffcc",
            "method": "PATCH",
            "status": {
                "code": "200"
            }
        },
        {
            "location":
"https://hs-identity-api.oracleindustry.com/scim/v1/mypharma/Users/e90253151e07454
e468b",
            "method": "DELETE",
            "status": {
                "code": "204"
            }
        }
    ]
}
```

3.3.3 Sample Message Exchange — Creating and adding the user to a group

Request

```
POST /scim/v1/mypharma/Bulk HTTP 1.1
Host: example.com
Authorization: Basic Y3VzdG9tZXIuYWRtaW51c2VyOnBhc3N3b3Jk=
Accept: application/json
Content-Type: application/json
Content-Length: ...
{
    "schemas" : [
        "urn:scim:schemas:core:2.0:BulkRequest"
    ],
    "failOnErrors" : 1,
    "Operations" : [
        {
            "method" : "POST",
            "path" : "/Users",
            "bulkId" : "qwerty",
            "data" : {
                "schemas" : [
                    "urn:scim:schemas:core:2.0:User"
                ],
                "externalId" : "bulk.user@mypharma.com",
                "userName" : "bulk.user@mypharma.com",
                "name" : {
                    "familyName" : "User",
                    "givenName" : "Bulk"
                },
                "emails" : [
                    {
                        "value" : "bulk.user@mypharma.com",
                        "type" : "work"
                    }
                ],
                "password" : "Welcome1"
            }
        },
        {
            "method" : "PATCH",
            "path" : "/Groups/mypharma.lshdme",
            "data" : {
                "op" : "add",
                "path" : "members",
                "value" : [
                    {
                        "value" : "bulkId:qwerty"
                    }
                ]
            }
        }
    ]
}
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: ...
{
```

```
    "schemas" : [
        "urn:scim:schemas:core:2.0:BulkResponse"
    ],
    "Operations" : [
        {
            "location" :
"http://hs-identity-api.oracleindustry.com/scim/v1/mypharma/Users/c1f6f0df5e80498b
b0d34c62b27694c9",
            "method" : "POST",
            "bulkId" : "qwerty",
            "path" : "/Users",
            "status" : {
                "code" : "201"
            }
        },
        {
            "method" : "PATCH",
            "path" : "/Groups/mypharma.lshdme",
             "status" : {
                "code" : "200"
            }
        }
    ]
}
```