POLIZEI 20/20

Infrastructure Administrations

IGS SCIM Extension Operations

GEMEINSAM. DIGITAL. VERNETZT.

Infrastructure Administrations

1.0 Edition

Adrien Farkaš

Revision History

Revision	Date	Author	Reference
1.0	15.3.2024	A. Farkaš	First initial release
1.1	11.6.2024	A. Farkaš	Added /ApplicationAttributes endpoint description, other minor modifications

Table of Contents

Preface

Audience

This guide is intended for resource administrators and target system integration teams.

Reference Documents

For information about installing and using Oracle Identity and Access Management, visit the following Oracle Help Center page:

- *https://docs.oracle.com/en/middleware/idm/suite/12.2.1.3/index.html*

Confidentiality

The material contained in this documentation represents proprietary, confidential information pertaining to Oracle products and methods.

The audience agrees that the information in this documentation shall not be disclosed outside of Oracle, and shall not be duplicated, used, or disclosed for any purpose other than to evaluate this procedure.

Typographical Conventions

The following table describes the typographic changes that are used in this document.

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Symbol Conventions

The following table explains symbols that might be used in this document.

Symbol	Meaning
[ ]	Contains optional arguments and command options.
{ | }	Contains a set of choices for a required command option.

Symbol	Meaning
${ }	Indicates a variable reference.
-	Joins simultaneous multiple keystrokes.
+	Joins consecutive multiple keystrokes.
>	Indicates menu item selection in a graphical user interface.

About the Services

The IGS SCIM Extension represents SCIM interface for tenant integration. It is a (preferred) substitution to the existing LDAP interface allowing direct integration to tenants' IDM solutions and allows more fine-grained management of user's accounts.

This document assumes a working knowledge of SCIM 2.0 standards (defined in RFC7642, RFC7643 and RFC7644), terms defined in the specification documents will not be explained here.

The following sections contain description of available endpoints, examples of API requests and responses currently supported in the IGS SCIM Extension, along with important notes and constraints to consider in tenants' SCIM client design.

Endpoint /ResourceTypes

The `/ResourceTypes` endpoint can be used for GET method to retrieve supported resource types supported by this SCIM endpoint. The `/ResourceTypes` endpoint is read only.

The following API operations are supported by the IGS SCIM Extension `/ResourceTypes` endpoint implementation:

- List Resource Types

List available Resource Types

This endpoint provides the ability to list available resource types. Request supports filtering, sorting and limiting attributes to return, see the Query Parameters section for more information.

Request

> **Authorization**
>
> This end-point is available publicly and no authentication and/or authorization is required.

GET /ResourceTypes/

Request Header

Name	Type	Value
accept	string	application/scim+json
content-type	string	application/scim+json

Query Parameters

Name	Type	Required	Description
attributes	string	no	Comma separated list of attributes to return. Any resource type attributes can be listed (inclusing complex sub-attributes).
excludedAttributes	string	no	Comma separated list of attributes to exclude from the listing. Any top-level resource attributes can be listed.
filter	string	no	Specifies filtering of the entries to return. For general filtering information see Filters chapter.

Name	Type	Required	Description
sortBy	string	no	Attribute to use for output sorting.
sortOrder	string	no	Output sorting direction. Possible values are "ascending" and "descending".
startIndex	integer	no	The 1-based index of the first query result to return. A value less than 1 is interpreted as 1.
count	integer	no	Specifies the desired maximum number of query results per batch. A negative value is interpreted as 0. A value of 0 indicates that no resource results are to be returned.

Response

The list of resource types supported by this SCIM server as defined by the RFC7644.

Envelope

Name	Type	Required	Description
schemas	array of strings	yes	Schemas of the entry/entries returned.
totalResults	string	yes	Non-negative integer in string representation. Specifies the total number of results.
itemsPerPage	integer	no	Non-negative integer. Specifies the number of query results that are returned in a query response page.
startIndex	integer	no	The 0-based index of the first result in the current set of query results.
Resources	array of Resource objects	yes	The resource array of the populated result set.

Resource

Name	Type	Required	Description
schemas	array of strings	yes	Schemas of the entry/entries returned.
meta	Meta Information object	yes	Meta information for the resource.
name	string	yes	The name for this resource type.
endpoint	string	yes	The URI to access this resource type.
description	string	yes	The description of this resource type.
schemaExtensions	array of Extension objects	yes	The array of schemas extending this resource type.

Meta Information

Name	Type	Required	Description
resourceType	string	yes	The type of this resource.
location	string	yes	The URL for accessing this particular resource schema.

Extension

Name	Type	Required	Description
required	boolean	yes	Boolean flag indicating whether this schema is required.
schema	string	yes	The schema specification of this extension.

Example for listing resource types

GET /ResourceTypes

```
{
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:ListResponse"
    ],
    "totalResults": "2",
    "itemsPerPage": 0,
    "startIndex": 0,
    "Resources": [
        {
            "schemas": [
                "urn:ietf:params:scim:schemas:core:2.0:ResourceType"
            ],
            "meta": {
                "resourceType": "ResourceType",
                "location": "http://192.168.64.11:8005/igs/scim/v2/ResourceTypes"
            },
            "schema": "urn:ietf:params:scim:schemas:core:2.0:User",
            "name": "User",
            "endpoint": "/Users",
            "description": "Oracle User",
            "schemaExtensions": [
                {
                    "required": false,
                    "schema": "urn:ietf:params:scim:schemas:extension:oracle:2.0:IDM:User"
                },
                {
                    "required": false,
                    "schema": "urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:User"
                },
                {
                    "required": false,
                    "schema": "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"
                },
                {
                    "required": false,
                    "schema": "urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:UserApplication"
                }
            ]
        },
        {
            "schemas": [
                "urn:ietf:params:scim:schemas:core:2.0:ResourceType"
            ],
            "meta": {
                "resourceType": "ResourceType",
                "location": "http://192.168.64.11:8005/igs/scim/v2/ResourceTypes"
            },
            "schema": "urn:ietf:params:scim:schemas:oracle:core:2.0:IDM:ApplicationAccount",
            "name": "ApplicationAccount",
            "endpoint": "/Accounts",
            "description": "Oracle Account"
        }
    ]
}
```

Possible Errors

Error	Condition
401 Unauthorized	No or invalid authentication was provided.
403 Forbidden	Request was authenticated but authorization was not passed (authenticated user lacks role required to acces the resource).
503 Service Unavailable	Other processing error occured including invalid filter syntax. Response `description` attribute contains more details.

Endpoint /Schemas

The `/Schemas` endpoint can be used for `GET` method to retrieve supported SCIM schema. The schema provided consists of two parts:

- **Standard Oracle Identity Governance schema**, described at ht docs.oracle.com/cd/E52734_01/oim/OMDEV/scim.htm,
- **Custom SCIM schema extension**, described throughout this document.

The `/Schemas` endpoint is read only.

The following API operations are supported by the IGS SCIM Extension `/Schemas` endpoint implementation:

- List SCIM Schemas

List SCIM Schemas

This endpoint provides the ability to query SCIM resources. Request supports limiting attributes to return, see the Query Parameters section for more information.

Request

> **Authorization**
>
> This end-point is available publicly and no authentication and/or authorization is required.

GET /Schemas/

Request Header

Name	Type	Value
accept	string	application/scim+json
content-type	string	application/scim+json

Query Parameters

Name	Type	Required	Description
attributes	string	no	Comma separated list of attributes to return. Any top-level resource attributes can be listed.
excludedAttributes	string	no	Comma separated list of attributes to exclude from the listing. Any top-level resource attributes can be listed.

Name	Type	Required	Description
filter	string	no	Specifies filtering of the entries to return. For general filtering information see Filters chapter.

Response

The list of schemas supported by this SCIM server as defined by the RFC7644.

Envelope

Name	Type	Required	Description
schemas	array of strings	yes	Schemas of the entry/entries returned.
totalResults	string	yes	Non-negative integer in string representation. Specifies the total number of results.
itemsPerPage	integer	no	Non-negative integer. Specifies the number of query results that are returned in a query response page.
startIndex	integer	no	The 0-based index of the first result in the current set of query results.
Resources	array of Resource objects	yes	The resource array of the populated result set.

Resource

Name	Type	Required	Description
id	string	yes	The unique URI of the schema.
schemas	array of strings	yes	Schemas of the entry/entries returned.
meta	Meta Information object	yes	Meta information for the resource.
name	string	yes	The schema's human-readable name.

Name	Type	Required	Description
attributes	array of Attributes objects	yes	The attributes supported by this resource.
description	string	yes	The schema's human-readable description.

Meta Information

Name	Type	Required	Description
resourceType	string	yes	The type of this resource.
location	string	yes	The URL for accessing this particular resource schema.

Attributes

Name	Type	Required	Description
name	string	yes	The attribute's name.
type	string	yes	The data type of this attribute. Possible values are "string", "boolean", "decimal", "integer", "dateTime", "reference" and "complex".
multiValued	boolean	yes	Indication whether the attribute can have multiple values.
description	string	yes	The attribute's human-readable description.
mutability	string	yes	The mutability of this attribute, i.e. whether this attribute value may be updated. Possible values are "readWrite", "readOnly", "writeOnly" and "immutable".
returned	string	yes	Indication when this attribute will be returned. Possible values are "never", "default", "always" and "request".
uniqueness	string	yes	A single keyword value that specifies how the service provider enforces uniqueness of attribute values. Possible values are "none", "server' and "global".

Name	Type	Required	Description
required	boolean	yes	Indication whether the attribute value is required.
caseExact	boolean	yes	Indication whether the attribute value is case-sensitive.
subAttributes	array of Attributes objects	no	For a "complex" type attribute, list of attribute sub-types.

Example for listing schemas

GET /Schemas

```
{
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:ListResponse"
    ],
    "totalResults": "9",
    "itemsPerPage": 0,
    "startIndex": 0,
    "Resources": [
        {
            "id": "urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:UserApplication",
            "schemas": [
                "urn:ietf:params:scim:schemas:core:2.0:Schema"
            ],
            "meta": {
                "resourceType": "Schema",
                "location": "http://192.168.64.11:8005/igs/scim/v2/Schemas/urn:ietf:params:scim:schemas:exte
            },
            "name": "UserApplication",
            "attributes": [
                {
                    "name": "applications",
                    "type": "complex",
                    "multiValued": true,
                    "description": "User's associated application instances",
                    "mutability": "readWrite",
                    "returned": "default",
                    "uniqueness": "none",
                    "required": false,
                    "caseExact": false,
                    "subAttributes": [
                        {
                            "name": "applicationName",
                            "type": "string",
                            "multiValued": false,
                            "description": "Name of the application instance",
                            "mutability": "readWrite",
                            "returned": "default",
                            "uniqueness": "none",
                            "required": false,
                            "caseExact": false
                        },
...
                        {
                            "name": "applicationAttributes",
                            "type": "complex",
                            "multiValued": true,
                            "description": "Attributes for the application instance account",
                            "mutability": "readWrite",
                            "returned": "default",
                            "uniqueness": "none",
                            "required": false,
                            "caseExact": false,
                            "subAttributes": [
                                {
                                    "name": "name",
                                    "type": "string",
                                    "multiValued": false,
                                    "description": "Attribute name (label from OIG)",
                                    "mutability": "readWrite",
                                    "returned": "default",
                                    "uniqueness": "none",
                                    "required": false,
                                    "caseExact": false
                                },
                                {
                                    "name": "value",
                                    "type": "string",
                                    "multiValued": false,
                                    "description": "Attribute value",
                                    "mutability": "readWrite",
                                    "returned": "default",
                                    "uniqueness": "none",
                                    "required": false,
                                    "caseExact": false
                                }
                            ]
                        },
                        {
                            "name": "entitlements",
                            "type": "complex",
                            "multiValued": true,
                            "description": "Entitlements associated with the application instance",
                            "mutability": "readWrite",
                            "returned": "default",
                            "uniqueness": "none",
                            "required": false,
                            "caseExact": false,
                            "subAttributes": [
                                {
                                    "name": "namespace",
                                    "type": "String",
                                    "multiValued": true,
                                    "description": "Namespace of the entitlement (e.g. UD_OUD_G)",
                                    "mutability": "readWrite",
                                    "returned": "default",
                                    "uniqueness": "none",
                                    "required": true,
                                    "caseExact": false
                                },
                                {
                                    "name": "entitlementValues",
                                    "type": "complex",
                                    "multiValued": true,
                                    "description": "Entitlements associated with the application instance",
                                    "mutability": "readWrite",
                                    "returned": "default",
                                    "uniqueness": "none",
                                    "required": false,
                                    "caseExact": false,
                                    "subAttributes": [
                                        {
                                            "name": "status",
                                            "type": "string",
                                            "multiValued": false,
                                            "description": "Status of the entitlement instance",
                                            "mutability": "read",
                                            "returned": "default",
                                            "uniqueness": "none",
                                            "required": false,
                                            "caseExact": false
                                        },
                                        {
                                            "name": "entitlement",
                                            "type": "complex",
                                            "multiValued": true,
                                            "description": "Attributes for the entitlement instance",
                                            "mutability": "readWrite",
                                            "returned": "default",
                                            "uniqueness": "none",
                                            "required": true,
                                            "caseExact": false,
                                            "subAttributes": [
                                                {
                                                    "name": "name",
                                                    "type": "string",
                                                    "multiValued": false,
                                                    "description": "Name of the entitlement",
                                                    "mutability": "readWrite",
                                                    "returned": "default",
                                                    "uniqueness": "none",
                                                    "required": true,
                                                    "caseExact": false
                                                },
                                                {
                                                    "name": "value",
                                                    "type": "string",
                                                    "multiValued": false,
                                                    "description": "Value of the entitlement",
                                                    "mutability": "readWrite",
                                                    "returned": "default",
                                                    "uniqueness": "none",
                                                    "required": true,
                                                    "caseExact": false
                                                }
                                            ]
                                        }
                                    ]
                                }
                            ]
                        }
                    ]
                }
            ],
            "description": "Schema extension for user application instances"
        },
        {
            "id": "urn:ietf:params:scim:schemas:oracle:core:2.0:IDM:ApplicationAccount",
            "schemas": [
                "urn:ietf:params:scim:schemas:core:2.0:Schema"
            ],
            "meta": {
                "resourceType": "Schema",
                "location": "http://192.168.64.11:8005/igs/scim/v2/Schemas/urn:ietf:params:scim:schemas:orac
            },
            "name": "ApplicationAccount",
            "attributes": [
                {
                    "name": "applicationName",
                    "type": "string",
                    "multiValued": false,
                    "description": "Name of the application instance",
                    "mutability": "read",
                    "returned": "default",
                    "uniqueness": "none",
                    "required": false,
                    "caseExact": false
                },
...
                {
                    "name": "entitlements",
                    "type": "complex",
                    "multiValued": true,
                    "description": "Entitlements associated with the account",
                    "mutability": "readWrite",
                    "returned": "default",
                    "uniqueness": "none",
                    "required": false,
                    "caseExact": false,
                    "subAttributes": [
                        {
                            "name": "namespace",
                            "type": "String",
                            "multiValued": true,
                            "description": "Namespace of the entitlement (e.g. UD_OUD_G)",
                            "mutability": "readWrite",
                            "returned": "default",
                            "uniqueness": "none",
                            "required": true,
                            "caseExact": false
                        },
                        {
                            "name": "entitlementValues",
                            "type": "complex",
                            "multiValued": true,
                            "description": "Entitlements associated with the application instance",
                            "mutability": "readWrite",
                            "returned": "default",
                            "uniqueness": "none",
                            "required": false,
                            "caseExact": false,
                            "subAttributes": [
                                {
                                    "name": "status",
                                    "type": "string",
                                    "multiValued": false,
                                    "description": "Status of the entitlement instance",
                                    "mutability": "read",
                                    "returned": "default",
                                    "uniqueness": "none",
                                    "required": false,
                                    "caseExact": false
                                },
                                {
                                    "name": "entitlement",
                                    "type": "complex",
                                    "multiValued": true,
                                    "description": "Attributes for the entitlement instance",
                                    "mutability": "readWrite",
                                    "returned": "default",
                                    "uniqueness": "none",
                                    "required": true,
                                    "caseExact": false,
                                    "subAttributes": [
                                        {
                                            "name": "name",
                                            "type": "string",
                                            "multiValued": false,
                                            "description": "Name of the entitlement",
                                            "mutability": "readWrite",
                                            "returned": "default",
                                            "uniqueness": "none",
                                            "required": true,
                                            "caseExact": false
                                        },
                                        {
                                            "name": "value",
                                            "type": "string",
                                            "multiValued": false,
                                            "description": "Value of the entitlement",
                                            "mutability": "readWrite",
                                            "returned": "default",
                                            "uniqueness": "none",
                                            "required": true,
                                            "caseExact": false
                                        }
                                    ]
                                }
                            ]
                        }
                    ]
                }
            ],
            "description": "Schema extension for application accounts"
        },
        ...
    ]
}
```

Possible Errors

Error	Condition
401 Unauthorized	No or invalid authentication was provided.
403 Forbidden	Request was authenticated but authorization was not passed (authenticated user lacks role required to acces the resource).
503 Service Unavailable	Other processing error occured including invalid filter syntax. Response `description` attribute contains more details.

Endpoint /Users

The `/Users` endpoint can be used for full user management, so `GET`, `POST`, `PUT` and `PATCH` methods are available to manipulate user entries.

> **Authorization**
>
> Any access to any method provided by this resource **MUST** be authorized by an access token.
>
> Accessing the endpoint requires valid user by providing Basic Authentication or Bearer/SAML/ OAuth token issued by BKA services, the authenticated user needs to be member of `viewer` or `administrator` Java(tm) Platform, Enterprise Edition (Java EE) roles.

The following API operations are supported by the IGS SCIM Extension `/Users` endpoint implementation:

- List Users
- Lookup User
- Create User
- Modify User
- Delete User

List Users

This endpoint provides the ability to query SCIM resources. Request supports limiting attributes to return, see the Query Parameters section for more information.

Request

> **Permission**
>
> Calling user must have administration capability for the organization where the user is located and capability to view users.

GET /Users/

Request Header

Name	Type	Value
accept	string	application/scim+json
content-type	string	application/scim+json

Query Parameters

Name	Type	Required	Description
attributes	string	no	Comma separated list of attributes to return.

Name	Type	Required	Description
			Any top-level resource attributes can be listed.
excludedAttributes	string	no	Comma separated list of attributes to exclude from the listing. Any top-level resource attributes can be listed.
filter	string	no	Specifies filtering of the entries to return. For general filtering information see Filters chapter.

Response

The list of identities visible to the requesting user, populated with attributes.

Envelope

Name	Type	Required	Description
schemas	array of strings	yes	Type(s) of the result(s) returned.
totalResults	string	yes	Non-negative integer in string representation. Specifies the total number of results.
itemsPerPage	integer	no	Non-negative integer. Specifies the number of query results that are returned in a query response page.
startIndex	integer	no	The 0-based index of the first result in the current set of query results.
Resources	array of identity objects	yes	The resource array of the populated result set.

Example for listing identities

GET /Users

```
{
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:ListResponse"
    ],
    "totalResults": "10",
    "itemsPerPage": 0,
    "startIndex": 0,
    "Resources": [
        {
            "id": "USER.1998",
            "schemas": [
                "urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:User",
                "urn:ietf:params:scim:schemas:extension:oracle:2.0:IDM:User",
                "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:oracle:2.0:OIG:UserApplication"
            ],
            "meta": {
                "resourceType": "User",
                "created": 1701185628000,
                "lastModified": 1707740291000,
                "location": "http://192.168.64.11:8005/igs/scim/v2/Users/1001"
            },
            "userType": "Intern",
            "userName": "USER.1998",
            "displayName": "Jozko Trtko",
...
        }
    ]
}
```

Possible Errors

Error	Condition
401 Unauthorized	No or invalid authentication was provided.
403 Forbidden	Request was authenticated but authorization was not passed (authenticated user lacks role required to acces the resource).
503 Service Unavailable	Other processing error occured including invalid filter syntax. Response `description` attribute contains more details.

Lookup User

This endpoint provides the ability to lookup existing application instance identified by a URN. Request does not support pagination and filtering.

Request

> **Permission**
>
> Calling user must have administration capability for the organization where the user is located and capability to view users.

GET /Users/{userName}

Request Header

Name	Type	Value
accept	string	application/scim+json
content-type	string	application/scim+json

Query Parameters

Name	Type	Required	Description
none			

Response

The representation of the user's (identified by the given **userName**) accounts and attributes.

Identities and Accounts Attributes

Name	Type	Required	Description
id	string	yes	The identifier of this user's identity, **value is OIM username**.
schemas	array of strings	yes	List of schema URNs referenced by this object.
meta	Meta Information object	yes	Meta information for this object.
array of attributes	varies	yes	List of attributes of the identity, e.g. **userType**, **userName** or **displayName**. The attributes are in the format **"Attribute Name": "Attribute value"** where the **attribute value** depends on the actual attribute - can be a string, a boolean, a number or an object.
Schema URNs	varies	yes	List of additional attributes of the identity identified by the Schema URN defining them. The attributes themselves are in the format **"Attribute Name": "Attribute value"** where the **attribute value** depends on the actual attribute - can be a string, a boolean, a number or an object. A specific URN (SCIM schema extension

Name	Type	Required	Description
			urn:ietf:params:scim:schemas:extension:oracle:2.0: is described below.

Meta Information

Name	Type	Required	Description
resourceType	string	yes	The type of this resource.
created	number	yes	The identity creation timestamp in the Java format (number of milliseconds since the epoch).
lastModified	number	yes	The identity last modifucation timestamp in the Java format (number of milliseconds since the epoch).

UserApplication SCIM Extension

Name	Type	Required	Description
applications	array of application objects	yes	List of application objects.

Application

Name	Type	Required	Description
applicationName	string	yes	Name of the application instance for this account.
status	string	yes	Status of the account.
applicationAttributes	array of application attributes objects	yes	List of application accounts and attributes.
entitlements	array of entitlements objects	yes	List of application entitlements.

Application Attributes

Name	Type	Required	Description
name	string	yes	Name of the application instance attribute.
value	string	yes	Value of the application instance attribute.

Entitlements

Name	Type	Required	Description
namespace	string	yes	Namespace specific for the entitlements listed. An application may support multiple entitlement namespaces (e.g. **LDAP Roles** and **LDAP Groups** are two independent entitlement types each identified by an appropriate namespace).
entitlementValues	array of entitlement values objects	yes	Value of the application instance entitlement.

Entitlement Values Object

Name	Type	Required	Description
status	string	yes	Status of this entitlement instance, possible values are "Provisioned", "Requested".
entitlement	array of entitlement objects	yes	Value of the application instance attribute.

Entitlement

Name	Type	Required	Description
name	string	yes	Identity account attribute (containing this entitlement) name.
value	string	yes	Name of the entitlement.

Example for looking up a particular identity

GET /Users/AFARKAS

```
{
    "id": "AFARKAS",
    "schemas": [
        "urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:User",
        "urn:ietf:params:scim:schemas:extension:oracle:2.0:IDM:User",
        "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:oracle:2.0:OIG:UserApplication"
    ],
    "meta": {
        "resourceType": "User",
        "created": 1707744800000,
        "lastModified": 1707744800000,
        "location": "http://192.168.64.11:8005/igs/scim/v2/Users/AFARKAS"
    },
    "userType": "EMP",
    "userName": "AFARKAS",
    "displayName": "Adrien Farkas",
    "name": {
        "honorificSuffix": "afarkas@vm.oracle.com",
        "familyName": "Farkas",
        "givenName": "Adrien"
    },
...
    "urn:ietf:params:scim:schemas:extension:oracle:2.0:IDM:User": {
        "createBy": {
            "value": "1",
            "$ref": "http://192.168.64.11:8005/igs/scim/v2/Users/1"
        },
        "passwordExpireDate": 1718109201000,
        "updateBy": {
            "value": "1",
            "$ref": "http://192.168.64.11:8005/igs/scim/v2/Users/1"
        },
        "locked": {
            "duration": 0,
            "value": "0"
        }
    },
...
    "urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:UserApplication": {
        "applications": [
            {
                "applicationName": "IDSAccount",
                "status": "Provisioned",
                "applicationAttributes": [
                    {
                        "name": "NsuniqueID",
                        "value": "5B1C8425B2F44BFF8E62047518B47385"
                    },
                    {
                        "name": "User ID",
                        "value": "afarkas"
                    },
...
                },
                "entitlements": [
                    {
                        "namespace": "UD_IDS_GRP",
                        "entitlementValues": [
                            {
                                "status": "Provisioned",
                                "entitlement": [
                                    {
                                        "name": "Group Name",
                                        "value": "AM.IDS Endpoint~orclUserWritePrivilegeGroup"
                                    }
                                ]
                            },
                            {
                                "status": "Provisioned",
                                "entitlement": [
                                    {
                                        "name": "Group Name",
                                        "value": "AM.IDS Endpoint~orclGroupWritePrivilegeGroup"
                                    }
                                ]
                            }
                        ]
                    }
                ]
            }
        ]
    }
}
```

Possible Errors

Error	Condition
401 Unauthorized	No or invalid authentication was provided.
403 Forbidden	Request was authenticated but authorization was not passed (authenticated user lacks role required to acces the resource).
404 Not Found	Requested application instance was not found.
503 Service Unavailable	Other processing error occured including invalid filter syntax. Response `description` attribute contains more details.

Create User

This endpoint provides the ability to create a new identity and, optionally, request accounts and supply account attributes.

Request

> **Permission**
>
> Calling user must have administration capability for the organization where the user is created and capability to create users.

POST /Users

Request Header

Name	Type	Value
accept	string	application/scim+json
content-type	string	application/scim+json

Query Parameters

Name	Type	Required	Description
none			

Request Body

Standard SCIM POST operation request as defined in RFC7644. The example for creating user with minimal set of attributes is shown in the Example section.

Input body is in form of:

Envelope

Name	Type	Required	Description
schemas	array of strings	yes	Schema list contained in the request.
array of attributes	varies	yes	List of attributes of the identity, e.g. **userType**, **userName** or **displayName**. The attributes are in the format **"Attribute Name": "Attribute value"** where the **attribute value** depends on the actual attribute - can be a string, a boolean, a number or an object.

Response

The full user entry is returned by this operation described here.

Example for creating an identity

POST /Users

```
{
    "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:oracle:2.0:OIG:User",
        "urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:UserApplication"
    ],
    "userName": "AFARKAS",
    "name": {
        "givenName": "Adrien",
        "familyName": "Farkas"
    },
    "emails": [
        {
            "value": "adrien.farkas@example.com",
            "type": "work"
        }
    ],
    "phoneNumbers": [
        {
            "value": "555-555-5555",
            "type": "work"
        }
    ],
    "userType": "EMP",
    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User": {
        "employeeNumber": "123456"
    },
    "urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:User": {
        "homeOrganization": {
            "value": "5",
            "$ref": "http://HOST_NAME:PORT/iam/governance/scim/v1/Organizations/5"
        }
    }
}
```

Possible Errors

Error	Condition
401 Unauthorized	No or invalid authentication was provided.
403 Forbidden	Request was authenticated but authorization was not passed (authenticated user lacks role required to acces the resource).
404 Not Found	Requested application instance was not found.
503 Service Unavailable	Other processing error occured including invalid filter syntax. Response `description` attribute contains more details.

Modify User

This endpoint provides the ability to lookup existing application instance identified by a URN. Request does not support pagination and filtering.

Request

> **Permission**
>
> Calling user must have administration capability for the organization where the user is located and capability to modify users.

PATCH /Users/{userName}

Request Header

Name	Type	Value
accept	string	application/scim+json
content-type	string	application/scim+json

Query Parameters

Name	Type	Required	Description
none			

Request Body

Standard SCIM patch operation request as defined in chapter 3.5.2 of RFC7644. Multiple operations can be included in a single request.

Using this method only **BKA OIM basic attributes** (called **profile attributes**, belonging to schemas `urn:ietf:params:scim:schemas:core:2.0:User"`, `urn:ietf:params:scim:schemas:extension:oracle:2.0:IDM:User`, `urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:User` and `urn:ietf:params:scim:schemas:extension:enterprise:2.0:User`) can be altered, account attributes (including entitlements) are only returned by GET method for convenience and cannot be modified using this endpoint.

Input body is in form of:

Envelope

Name	Type	Required	Description
schemas	array of strings	yes	Schema identifier for the operation.
Operations	array of Operations objects	yes	The name for this application instance.

Operations

Name	Type	Required	Description
op	string	yes	Identifier of the operation. Possible values are "add", "remove" and "replace".
path	string	yes	Path of the attribute being modified, may contain schema reference URI.
value	string or array of objects	yes	Value for the attribute being modified, exact syntax depends on the actual attribute.

Response

The full user entry is returned by this operation described here.

> **Asynchronous Requests**
>
> As all the modification requests are performed asynchronously (as they might be subject of approval) the returned user entry will not yet reflect the changes requested.

Example for identity profile attribute modification

PATCH /Users/AFARKAS

This example modifies attribute **Initials** profile attribute by setting its value to **A.**

```
{
  "schemas":
  [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations":
  [
    {
        "op": "replace",
        "path": "urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:User:initials",
        "value": "A."
    }
  ]
}
```

Possible Errors

Error	Condition
401 Unauthorized	No or invalid authentication was provided.
403 Forbidden	Request was authenticated but authorization was not passed (authenticated user lacks role required to acces the resource).
404 Not Found	Requested application instance was not found.
503 Service Unavailable	Other processing error occured including invalid filter syntax. Response `description` attribute contains more details.

Delete User

This endpoint provides the ability to delete users in BKA OIM via SCIM interface.

Request

> **Permission**
>
> Calling user must have administration capability for the organization where the user is modified and capability to delete users.

DELETE /Users/{userName}

Request Header

Name	Type	Value
accept	string	application/scim+json
content-type	string	application/scim+json

Query Parameters

Name	Type	Required	Description
none			

Response

Upon successful deletion a 204 response is returned with no body

Possible Errors

Error	Condition
401 Unauthorized	No or invalid authentication was provided.
403 Forbidden	Request was authenticated but authorization was not passed (authenticated user lacks role required to acces the resource).
503 Service Unavailable	Other processing error occured including invalid filter syntax. Response `description` attribute contains more details.

Endpoint /Applications

The `/Applications` endpoint can be used retrieving list of available applications (alongside with all namespaces, entitlements and members), for listing available entitlement namespaces (alongside with all entitlements and members) for a specific application, for listing available entitlements (alongside with all members) for a specific application namespace, for listing assigned members for a specific per-application entitlement and modify entitlement assignmentfor entitlement membership management using PATCH operation.

> **Authorization**
>
> Any access to any method provided by this resource **MUST** be authorized by an access token.
>
> Accessing the endpoint requires valid user by providing Basic Authentication or Bearer/SAML/ OAuth token issued by BKA services, the authenticated user needs to be member of `viewer` or `administrator` Java(tm) Platform, Enterprise Edition (Java EE) roles.

The following API operations are supported by the IGS SCIM Extension `/Users` endpoint implementation:

- List Applications
- List Per-Application Namespaces
- List Per-Namespace Entitlements
- List Per-Entitlement Members
- Modify Per-Entitlement Members

List Applications

This endpoint provides the ability to list available applications. In the result also list of namespaces and entitlements alongside with members are returned. Request supports limiting attributes to return, see the Query Parameters section for more information.

Request

> **Permission**
>
> Calling user must have administration capability for the organization where the user is modified and capability to list applications.

GET /Applications/

Request Header

Name	Type	Value
accept	string	application/scim+json
content-type	string	application/scim+json

Query Parameters

Name	Type	Required	Description
attributes	string	no	Comma separated list of attributes to return. Any top-level resource attributes can be listed.
excludedAttributes	string	no	Comma separated list of attributes to exclude from the listing. Any top-level resource attributes can be listed.
filter	string	no	Specifies filtering of the entries to return. For general filtering information see Filters chapter.

Response

The list of identities visible to the requesting user, populated with attributes.

Envelope

Name	Type	Required	Description
schemas	array of strings	yes	Type(s) of the result(s) returned.
totalResults	string	yes	Non-negative integer in string representation. Specifies the total number of results.
itemsPerPage	integer	no	Non-negative integer. Specifies the number of query results that are returned in a query response page.
startIndex	integer	no	The 0-based index of the first result in the current set of query results.
Resources	array of application objects	yes	The resource array of the populated result set.

Application

Name	Type	Required	Description
applicationName	string	yes	Name of the application.
namespaces	array of namespace objects	yes	List of entitlements.

Example for listing applications

GET /Applications

```
{
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:ListResponse"
    ],
    "totalResults": "2",
    "itemsPerPage": 2,
    "startIndex": 0,
    "Resources": [
        {
            "applicationName": "IDSAccount",
            "schemas": [
                "urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:Applications"
            ],
            "namespaces": [
                {
                    "namespace": "UD_IDS_GRP",
                    "entitlements": [
                        {
                            "entitlementName": "AM.IDS Endpoint~orclUserWritePrivilegeGroup",
                            "attributeValues": [
                                {
                                    "attributes": [
                                        {
                                            "name": "Group Name",
                                            "value": "AM.IDS Endpoint~orclUserWritePrivilegeGroup"
                                        }
                                    ],
                                    "members": [
                                        "AFARKAS"
                                    ]
                                }
                            ]
                        },
                        {
                            "entitlementName": "AM.IDS Endpoint~orclUserReadPrivilegeGroup",
                            "attributeValues": [
                                {
                                    "attributes": [
                                        {
                                            "name": "Group Name",
                                            "value": "AM.IDS Endpoint~orclUserReadPrivilegeGroup"
                                        }
                                    ],
                                    "members": [
                                        "AFARKAS",
                                        "JLAKIC"
                                    ]
                                }
                            ]
                        }
                    ]
                }
            ]
        },
        {
            "applicationName": "AJSAccount",
            "schemas": [
                "urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:Applications"
            ],
            "namespaces": [
                {
                    "namespace": "UD_AJS_PRJ",
                    "entitlements": [
                        {
                            "entitlementName": "AJS.Endpoint~AJS Test Project 22",
                            "entitlementId": "Project",
                            "attributeValues": [
                                {
                                    "attributes": [
                                        {
                                            "name": "Project",
                                            "value": "AJS.Endpoint~AJS Test Project 22"
                                        },
                                        {
                                            "name": "Role",
                                            "value": "IDM Test Role 02"
                                        }
                                    ],
                                    "members": [
                                        "AFARKAS"
                                    ]
                                },
                                {
                                    "attributes": [
                                        {
                                            "name": "Project",
                                            "value": "AJS.Endpoint~AJS Test Project 22"
                                        },
                                        {
                                            "name": "Role",
                                            "value": "IDM Test Role 05"
                                        }
                                    ],
                                    "members": [
                                        "JLAKIC"
                                    ]
                                }
                            ]
                        },
                        {
                            "entitlementName": "AJS.Endpoint~AJS Test Project 23",
                            "attributeValues": [
                                {
                                    "attributes": [
                                        {
                                            "name": "Project",
                                            "value": "AJS.Endpoint~AJS Test Project 22"
                                        },
                                        {
                                            "name": "Role",
                                            "value": "IDM Test Role 02"
                                        }
                                    ],
                                    "members": [
                                        "JLAKIC"
                                    ]
                                },
                                {
                                    "attributes": [
                                        {
                                            "name": "Project",
                                            "value": "AJS.Endpoint~AJS Test Project 22"
                                        },
                                        {
                                            "name": "Role",
                                            "value": "IDM Test Role 05"
                                        }
                                    ],
                                    "members": [
                                        "AFARKAS"
                                    ]
                                }
                            ]
                        }
                    ]
                },
                {
                    "namespace": "UD_AJS_GRP",
                    "entitlements": [
                        {
                            "entitlementName": "AJS.Endpoint~idm-test-group-01",
                            "attributeValues": [
                                {
                                    "attributes": [
                                        {
                                            "name": "Group",
                                            "value": "AJS.Endpoint~idm-test-group-01"
                                        }
                                    ],
                                    "members": [
                                        "AFARKAS"
                                    ]
                                }
                            ]
                        },
                        {
                            "entitlementName": "AJS.Endpoint~idm-test-group-02",
                            "attributeValues": [
                                {
                                    "attributes": [
                                        {
                                            "name": "Group",
                                            "value": "AJS.Endpoint~idm-test-group-02"
                                        }
                                    ],
                                    "members": [
                                        "JLAKIC"
                                    ]
                                }
                            ]
                        }
                    ]
                }
            ]
        }
    ]
}
```

Possible Errors

Error	Condition
401 Unauthorized	No or invalid authentication was provided.
403 Forbidden	Request was authenticated but authorization was not passed (authenticated user lacks role required to acces the resource).

Error	Condition
503 Service Unavailable	Other processing error occured including invalid filter syntax. Response `description` attribute contains more details.

List Per-Application Namespaces

This endpoint provides the ability to list entitlement namespaces available in a applications. In the result also list of entitlements alongside with members are returned. Request supports limiting attributes to return, see the Query Parameters section for more information.

Request

> **Permission**
>
> Calling user must have administration capability for the organization where the user is modified and capability to list applications.

GET /Applications/{application}

Request Header

Name	Type	Value
accept	string	application/scim+json
content-type	string	application/scim+json

Query Parameters

Name	Type	Required	Description
attributes	string	no	Comma separated list of attributes to return. Any top-level resource attributes can be listed.
excludedAttributes	string	no	Comma separated list of attributes to exclude from the listing. Any top-level resource attributes can be listed.
filter	string	no	Specifies filtering of the entries to return. For general filtering information see Filters chapter.

Response

The list of identities visible to the requesting user, populated with attributes.

Envelope

Name	Type	Required	Description
schemas	array of strings	yes	Type(s) of the result(s) returned.
totalResults	string	yes	Non-negative integer in string representation. Specifies the total number of results.
itemsPerPage	integer	no	Non-negative integer. Specifies the number of query results that are returned in a query response page.
startIndex	integer	no	The 0-based index of the first result in the current set of query results.
Resources	array of namespace objects	yes	The resource array of the populated result set.

Namespace

Name	Type	Required	Description
namespace	string	yes	Name of the application.
entitlements	array of entitlement objects	yes	List of entitlements.

Example for listing namespaces

GET /Applications/AJSAccount

```
{
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:ListResponse"
    ],
    "totalResults": "2",
    "itemsPerPage": 2,
    "startIndex": 0,
    "Resources": [
        {
            "namespace": "UD_AJS_PRJ",
            "entitlements": [
                {
                    "entitlementName": "AJS.Endpoint~AJS Test Project 22",
                    "entitlementId": "Project",
                    "attributeValues": [
                        {
                            "attributes": [
                                {
                                    "name": "Project",
                                    "value": "AJS.Endpoint~AJS Test Project 22"
                                },
                                {
                                    "name": "Role",
                                    "value": "IDM Test Role 02"
                                }
                            ],
                            "members": [
                                "AFARKAS"
                            ]
                        },
                        {
                            "attributes": [
                                {
                                    "name": "Project",
                                    "value": "AJS.Endpoint~AJS Test Project 22"
                                },
                                {
                                    "name": "Role",
                                    "value": "IDM Test Role 05"
                                }
                            ],
                            "members": [
                                "JLAKIC"
                            ]
                        }
                    ]
                },
                {
                    "entitlementName": "AJS.Endpoint~AJS Test Project 23",
                    "attributeValues": [
                        {
                            "attributes": [
                                {
                                    "name": "Project",
                                    "value": "AJS.Endpoint~AJS Test Project 22"
                                },
                                {
                                    "name": "Role",
                                    "value": "IDM Test Role 02"
                                }
                            ],
                            "members": [
                                "JLAKIC"
                            ]
                        },
                        {
                            "attributes": [
                                {
                                    "name": "Project",
                                    "value": "AJS.Endpoint~AJS Test Project 22"
                                },
                                {
                                    "name": "Role",
                                    "value": "IDM Test Role 05"
                                }
                            ],
                            "members": [
                                "AFARKAS"
                            ]
                        }
                    ]
                }
            ]
        },
        {
            "namespace": "UD_AJS_GRP",
            "entitlements": [
                {
                    "entitlementName": "AJS.Endpoint~idm-test-group-01",
                    "attributeValues": [
                        {
                            "attributes": [
                                {
                                    "name": "Group",
                                    "value": "AJS.Endpoint~idm-test-group-01"
                                }
                            ],
                            "members": [
                                "AFARKAS"
                            ]
                        }
                    ]
                },
                {
                    "entitlementName": "AJS.Endpoint~idm-test-group-02",
                    "attributeValues": [
                        {
                            "attributes": [
                                {
                                    "name": "Group",
                                    "value": "AJS.Endpoint~idm-test-group-02"
                                }
                            ],
                            "members": [
                                "JLAKIC"
                            ]
                        }
                    ]
                }
            ]
        }
    ]
}
```

Possible Errors

Error	Condition
401 Unauthorized	No or invalid authentication was provided.
403 Forbidden	Request was authenticated but authorization was not passed (authenticated user lacks role required to acces the resource).
503 Service Unavailable	Other processing error occured including invalid filter syntax. Response `description` attribute contains more details.

List Per-Namespace Entitlements

This endpoint provides the ability to list members for a particular entitlement. Since a single entitlement can contain multiple attributes (at least the entitlement attribute itself) all available attribute name-value pairs are returned alongside with members for each attribute name-value pair assigned.

Request

> **Permission**
>
> Calling user must have administration capability for the organization where the user is modified and capability to list entitlements.

GET /Applications/{application}/{namespace}

Request Header

Name	Type	Value
accept	string	application/scim+json
content-type	string	application/scim+json

Query Parameters

Name	Type	Required	Description
none			

Response

The list of attribute name-value pairs and member account names for each combination.

Envelope

Name	Type	Required	Description
schemas	array of strings	yes	Type(s) of the result(s) returned.
totalResults	string	yes	Non-negative integer in string representation. Specifies the total number of results.
itemsPerPage	integer	no	Non-negative integer. Specifies the number of query results that are returned in a query response page.
startIndex	integer	no	The 1-based index of the first result in the current set of query results.
Resources	array of entitlement objects	yes	The resource array of the populated result set.

Example for listing entitlements

GET /Applications/AJSAccount/UD_AJS_PRJ

```
{
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:ListResponse"
    ],
    "totalResults": "2",
    "itemsPerPage": 2,
    "startIndex": 0,
    "Resources": [
        {
            "entitlementName": "AJS.Endpoint~AJS Test Project 22",
            "entitlementId": "Project",
            "attributeValues": [
                {
                    "attributes": [
                        {
                            "name": "Project",
                            "value": "AJS.Endpoint~AJS Test Project 22"
                        },
                        {
                            "name": "Role",
                            "value": "IDM Test Role 02"
                        }
                    ],
                    "members": [
                        "AFARKAS"
                    ]
                },
                {
                    "attributes": [
                        {
                            "name": "Project",
                            "value": "AJS.Endpoint~AJS Test Project 22"
                        },
                        {
                            "name": "Role",
                            "value": "IDM Test Role 05"
                        }
                    ],
                    "members": [
                        "JLAKIC"
                    ]
                }
            ]
        },
        {
            "entitlementName": "AJS.Endpoint~AJS Test Project 23",
            "attributeValues": [
                {
                    "attributes": [
                        {
                            "name": "Project",
                            "value": "AJS.Endpoint~AJS Test Project 22"
                        },
                        {
                            "name": "Role",
                            "value": "IDM Test Role 02"
                        }
                    ],
                    "members": [
                        "JLAKIC"
                    ]
                },
                {
                    "attributes": [
                        {
                            "name": "Project",
                            "value": "AJS.Endpoint~AJS Test Project 22"
                        },
                        {
                            "name": "Role",
                            "value": "IDM Test Role 05"
                        }
                    ],
                    "members": [
                        "AFARKAS"
                    ]
                }
            ]
        }
    ]
}
```

Possible Errors

Error	Condition
401 Unauthorized	No or invalid authentication was provided.
403 Forbidden	Request was authenticated but authorization was not passed (authenticated user lacks role required to acces the resource).
503 Service Unavailable	Other processing error occured including invalid filter syntax. Response `description` attribute contains more details.

List Per-Entitlement Members

This endpoint provides the ability to list members for a particular entitlement. Since a single entitlement can contain multiple attribute (at least the entitlement attributs itself) all available attribute name-value pairs are returned alongside with members for each attribute name-value pair assigned.

Request

> **Permission**
>
> Calling user must have administration capability for the organization where the user is modified and capability to view identities.

GET /Applications/{application}/{namespace}/{entitlement}

Request Header

Name	Type	Value
accept	string	application/scim+json
content-type	string	application/scim+json

Query Parameters

Name	Type	Required	Description
none			

Response

The list of attribute name-value pairs and member account names for each combination.

Entitlement

Name	Type	Required	Description
entitlementName	string	yes	Name of the entitlement.
entitlementId	string	no	Name name of the entitlement attribute. Can be omitted for single-attribute entitlements
attributeValues	array of attribute value objects	yes	For a single entitlement, list of possible attribute values (including the entitlement attribute itself).

Attribute Value

Name	Type	Required	Description
attributes	array of attributes objects	yes	List of name-value pairs for account attribute values.
members	array of strings	yes	List of member account names.

Attributes

Name	Type	Required	Description
id	string	yes	Name of the attribute.
value	string	yes	Value of the attribut.

Example for listing single-attribute entitlement members

GET /Applications/IDSAccount/UD_IDS_GRP/AM.IDS

Endpoint~orclUserWritePrivilegeGroup

```
{
    "entitlementName": "AM.IDS Endpoint~orclUserWritePrivilegeGroup",
    "attributeValues": [
        {
            "attributes": [
                {
                    "name": "Group Name",
                    "value": "AM.IDS Endpoint~orclUserWritePrivilegeGroup"
                }
            ],
            "members": [
                "AFARKAS"
            ]
        }
    ]
}
```

Example for listing multi-attribute entitlement members

GET /Applications/AJSAccount/UD_AJS_PRJ/AJS.Endpoint~AJS Test Project 22

```
{
    "entitlementName": "AJS.Endpoint~AJS Test Project 22",
    "entitlementId": "Project",
    "attributeValues": [
        {
            "attributes": [
                {
                    "name": "Project",
                    "value": "AJS.Endpoint~AJS Test Project 22"
                },
                {
                    "name": "Role",
                    "value": "IDM Test Role 02"
                }
            ],
            "members": [
                "AFARKAS"
            ]
        },
        {
            "attributes": [
                {
                    "name": "Project",
                    "value": "AJS.Endpoint~AJS Test Project 22"
                },
                {
                    "name": "Role",
                    "value": "IDM Test Role 05"
                }
            ],
            "members": [
                "JLAKIC"
            ]
        }
    ]
}
```

Possible Errors

Error	Condition
401 Unauthorized	No or invalid authentication was provided.

Error	Condition
403 Forbidden	Request was authenticated but authorization was not passed (authenticated user lacks role required to acces the resource).
503 Service Unavailable	Other processing error occured including invalid filter syntax. Response `description` attribute contains more details.

Modify Entitlement Members

This endpoint provides the ability to assign or revoke members by modifying entitlement.

Request

> **Permission**
>
> Calling user must have administration capability for the organization where the user is modified and capability to modify identities.

PATCH /Applications/{application}/{namespace}/{entitlement}

Request Header

Name	Type	Value
accept	string	application/scim+json
content-type	string	application/scim+json

Query Parameters

Name	Type	Required	Description
none			

Request Body

Standard SCIM patch operation request as defined in chapter 3.5.2 of RFC7644. Multiple operations can be included in a single request.

Input body is in form of:

Envelope

Name	Type	Required	Description
schemas	array of strings	yes	Schema identifier for the operation.

Name	Type	Required	Description
Operations	array of Operations objects	yes	The name for this application instance.

<u>**Operations**</u>

Name	Type	Required	Description
op	string	yes	Identifier of the operation. Possible values are "add", "remove" and "replace".
path	string	yes	Path of the entitlement attribute being modified.
value	array of objects	no	Value for the attribute being modified, exact syntax depends on the actual attribute.

Response

The full entitlement entry is returned by this operation described here.

> **Asynchronous Requests**
>
> As all the modification requests are performed asynchronously (as they might be subject of approval) the returned user entry will not yet reflect the changes requested.

Example for requesting a single-attribute entitlement to be assigned to an account

PATCH /Applications/IDSAccount/UD_IDS_GRP/AM.IDS

Endpoint~orclUserWritePrivilegeGroup

This example modifies the entitlement by adding a new **members** value. To fully identify the the membership also **attributes** array is supplied (there are no new "additional" attributes in this case but to make the PATCH operation unified it part of the operation as well).

```
{
  "schemas":
  [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations":
  [
    {
      "op": "add",
      "path": "attributeValues",
      "value": {
        "attributes": [
          {
            "name": "Group Name",
      "value": "AM.IDS Endpoint~orclUserWritePrivilegeGroup"
     }
    ],
    "members": [
      "JLAKIC",
      "AFARKAS"
    ]
   }
  }
 ]
}
```

Example for requesting a multi-attribute entitlement to be assigned to an account

PATCH /Applications/AJSAccount/UD_AJS_PRJ/AJS.Endpoint~AJS Test Project 22

This example modifies the entitlement by adding a new **members** value. In this case this is multi-attribute entitlement and in order to fully identify where to add the member to also **attributes** array is supplied.

```
{
 "schemas":
 [
  "urn:ietf:params:scim:api:messages:2.0:PatchOp"
 ],
 "Operations":
 [
  {
   "op": "add",
   "path": "attributeValues",
   "value": {
    "attributes": [
     {
      "name": "Project",
      "value": "AJS.Endpoint~AJS Test Project 22"
     },
     {
      "name": "Role",
      "value": "IDM Test Role 02"
     }
    ],
    "members": [
     "JLAKIC",
     "AFARKAS"
    ]
   }
  }
 ]
}
```

Example for removing a single-attribute entitlement member

PATCH /Applications/IDSAccount/UD_IDS_GRP/AM.IDS Endpoint~orclUserWritePrivilegeGroup

This example modifies the entitlement by removing a **members** value from a specific attribute name-value pair.

```
{
  "schemas":
  [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations":
  [
    {
      "op": "remove",
      "path": "attributeValues.attributes[
            ( name eq \"Group Name\" AND
             value eq \"AM.IDS Endpoint~orclUserWritePrivilegeGroup\")
          ].members",
      "value": [
          "JLAKIC",
          "AFARKAS"
      ]
    }
  ]
}
```

Example for removing a multi-attribute entitlement member

PATCH /Applications/AJSAccount/UD_AJS_PRJ/AJS.Endpoint~AJS Test Project 22

This example modifies the entitlement by removing a **members** value from a specific multi-attribute attribute name-value pairs.

Please note the name-value pairs coupled together using parenthesis and AND-ed together, alongside with the actual **members** value to be removed. As the schema is generic parenthesis are required to prioritize individual name-value attributes.

```
{
  "schemas":
  [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations":
  [
    {
      "op": "remove",
      "path": "attributeValues.attributes[
            ( name eq \"Project\" AND
             value eq \"AJS.Endpoint~AJS Test Project 22\")
            AND
            ( name eq \"Role\" AND
             value eq \"IDM Test Role 02\")
          ].members",
      "value": [
          "JLAKIC",
          "AFARKAS"
      ]
    }
  ]
}
```

Possible Errors

Error	Condition
401 Unauthorized	No or invalid authentication was provided.

Error	Condition
403 Forbidden	Request was authenticated but authorization was not passed (authenticated user lacks role required to acces the resource).
404 Not Found	Requested application instance was not found.
503 Service Unavailable	Other processing error occured including invalid filter syntax. Response `description` attribute contains more details.

Endpoint /ApplicationAttributes

The `/ApplicationAttributes` endpoint can be used for retrieving schema attribute information for one particular application instance using the GET method.

> **Authorization**
>
> Any access to any method provided by this resource **MUST** be authorized by an access token.
>
> Accessing the endpoint requires valid user by providing Basic Authentication or Bearer/SAML/OAuth token issued by BKA services, the authenticated user needs to be member of `viewer` or `administrator` Java(tm) Platform, Enterprise Edition (Java EE) roles.

The following API operations are supported by the IGS ZeRo Services `/accounts` endpoint implementation:

- Lookup Application Attributes

Lookup Application Attributes

This endpoint provides the ability to retrieve application attributes using a standard SCIM GET operations.

Request

> **Permission**
>
> Calling user must have administration capability to list the application.

GET /ApplicationAttributes/{application}

Request Header

Name	Type	Value
accept	string	application/scim+json
content-type	string	application/scim+json

Query Parameters

Name	Type	Required	Description
none			

Response

Output data is in form of:

Envelope

Name	Type	Required	Description
totalResults	string	yes	Non-negative integer in string representation. Specifies the total number of results.
itemsPerPage	integer	no	Non-negative integer. Specifies the number of query results that are returned in a query response page.
startIndex	integer	no	The 0-based index of the first result in the current set of query results.
Resources	array of resources objects	yes	The resource array of the populated result set.

Application Attributes Resource

Name	Type	Required	Description
name	string	yes	Attribute namespace (for complex attributes) or the actual technical name of the schema attribute (for non-complex attributes) as it needs to be supplied during provisioning.
label	string	yes	The human readable name for this application instance suitable for GUI displaying purpose.
type	string	yes	Schema attribute content type suitable for GUI displaying purpose.
variantType	string	yes	Technical schema attribute content type (e.g. for syntax checking).
length	integer	yes	Maximum content length for string variants (or "0" for number type or "1" for boolean type)
required	boolean	no	Boolean flag indicating whether this is a required schema attribute for provisioning.
entitlement	boolean	no	Boolean flag indicating whether this schema attribute represents an entitlement.

Name	Type	Required	Description
lookupName	string	no	If schema attribute is a list-of-values (exactly one value from a fixed list) this is the reference to appropriate lookup.
lookupValues	array of lookup values objects	no	Lookup Values array for non-entitlement attributes.
attributeReference	array of attributes objects	no	References for attributes constituing complex attributes.

Lookup Values

Name	Type	Required	Description
key	string	yes	The code for this lookup value as it needs to be supplied during provisioning.
decode	string	yes	The human readable key name suitable for GUI displaying purpose.

Example for identity account attribute modification

GET /ApplicationAttributes/AJSAccount

This example lists attributes for the AJSAccount (Atlassian Jira) application and shows both simple and complex attributes.

```
{
    "totalResults": 7,
    "itemsPerPage": 0,
    "startIndex": 0,
    "Resources": [
        {
            "name": "UD_AJS_USR_UID",
            "label": "User Name",
            "required": true,
            "entitlement": false,
            "type": "TextField",
            "variantType": "String",
            "length": 255
        },
        {
            "name": "UD_AJS_USR_PWD",
            "label": "Password",
            "entitlement": false,
            "type": "PasswordField",
            "variantType": "String",
            "length": 255
        },
        {
            "name": "UD_AJS_USR_DISPLAY_NAME",
            "label": "Display Name",
            "required": true,
            "entitlement": false,
            "type": "TextField",
            "variantType": "String",
            "length": 255
        },
        ...
        {
            "name": "UD_AJS_PRJ",
            "attributeReference": [
                {
                    "name": "UD_AJS_PRJ_PID",
                    "label": "Project",
                    "required": true,
                    "entitlement": true,
                    "type": "LookupField",
                    "variantType": "String",
                    "length": 255,
                    "lookupName": "AJS.Project"
                },
                {
                    "name": "UD_AJS_PRJ_RID",
                    "label": "Role",
                    "required": false,
                    "entitlement": false,
                    "type": "LookupField",
                    "variantType": "String",
                    "length": 255,
                    "lookupName": "AJS.Role",
                    "lookupValues": [
                        {
                            "decode": "TP1 role 3",
                            "key": "10102"
                        },
                        {
                            "decode": "TP2 role 1",
                            "key": "10103"
                        },
                        ...
                    ]
                }
            ]
        },
        {
            "name": "UD_AJS_GRP",
            "attributeReference": [
                {
                    "name": "UD_AJS_GRP_GID",
                    "label": "Group",
                    "required": true,
                    "entitlement": true,
                    "type": "LookupField",
                    "variantType": "String",
                    "length": 255,
                    "lookupName": "AJS.Group"
                }
            ]
        }
    ]
}
```

Possible Errors

Error	Condition
401 Unauthorized	No or invalid authentication was provided.

Error	Condition
403 Forbidden	Request was authenticated but authorization was not passed (authenticated user lacks role required to acces the resource).
404 Not Found	Requested application instance was not found.
503 Service Unavailable	Other processing error occured including invalid filter syntax. Response `description` attribute contains more details.

Using Filters

The following chapter describer filtering facilities used through all **search** operations where filtering is referenced.

Filtering is employed by providing left-hand-side (LHS) **attribute**, comparison **operator** followed by right-hand-side (RHS) **value**. It is invoked by supplying the optional *filter* query parameter as follows: `filter=<LHS> <OP> <RHS>`.

LHS - Attributes

List of available attributes differs per-operation and will be listed there. In general, LHS attributes correspond to object attribute names (**case-insensitive**) as received in response JSON.

Operators

Unless specified otherwise for individual operations the following operators are available:

- **eq** (equals) for text, boolean, temporal and numerical values
- **sw** (starts with) for text values
- **eq** (ends with) for text values
- **co** (contains) for text values
- **gt** (greater than) for numerical and temporal values
- **ge** (greater than or equal) for numerical and temporal values
- **lt** (less than) for numerical and temporal values
- **le** (less than or equal) for numerical and temporal values

RHS - Values

The values are supplied in one of the following formats:

- **"string"** literal string value enclosed in double quotes
- **number** literal numerical value not enclosed in double quotes
- **"date"** literal temporal value in the format "yyyy-MM-dd", e.g. "2023-03-15
- **"date time"** literal temporal value in the format "yyyy-MM-dd HH:mm:ss "2023-03-15 12:34:56"
- **"boolean"** boolean value in the format "0" (false) or "1" (true)

Simple filters

The following are examples of valid simple filters:

- **key eq 3**
- **name sw "GDPD SZ2 End"**
- **itResourceName co "SZ2"**
- **updateDate gt "2023-02-22"**
- **createDate le "2023-02-22 13:43:46"**

Multiple filters

Simple filters can chained using **AND** and **OR** operators, or inverted using **NOT** operator. In the last case the sub-filter must be enclosed in round brackets:

- **name sw "GDPD SZ2 Endpoint" AND key eq 2**

- **name co "SZ2" OR name co "SZ3"**
- **appInstanceName co "SZ2" AND createDate gt "2022-02-12"**
- **NOT (appInstanceName co "SZ2")**
- **NOT (name co "NSIS" OR key eq 3)**

Attributes and the opeaSimple filters can chained using **AND** and **OR** operators, or inverted using **NOT** operator. In the last case the sub-filter must be enclosed in round brackets: