Identity Manager GE - Keyrock Specification

DATE: 19 September 2016

This version:

http://ging.github.io/fiware-idm/api-spec/v3

Latest version:

http://ging.github.io/fiware-idm/api-spec/latest

Editors

- Álvaro Alonso González
- Enrique García Navalón
- Federico A. Fernández Moreno

Copyright

Abstract

Identity Manager (IdM) GE API specifications comply with existing standards for authentication and user and provide access information. The following sections provide pointers to those standards and, when applicable, details about how the RESTful binding work.

This specification is intended for Service Consumers (with developement skills) and Cloud Providers. For the former, this document provides a full specification of how to interoperate with the Identity Management Service API. For the latter, this specification indicates the interface to be provided to the client application developers to provide the described functionalities. To use this information, the reader should first have a general understanding of the Generic Enabler service.

The API user should be familiar with:

- RESTful web services
- HTTP/1.1
- JSON and/or XML data serialization formats.
- SCIM 2.0
- OAuth 2.0

Preface

Status of this document

This is a work in progress and is changing on a daily basis. Please send your comments to FIWARE IdM Github Project.

Table of Contents

API Summary

        - DELETE - Disable two factor authentication [/v3/users/{user_id}/OS-TWO-FACTOR/two_factor_auth]
    - Two Factor Authentication Security Questions
        - GET - Retrieve non-sensitive data [/v3/users/{user_id}/OS-TWO-FACTOR/two_factor_data]
        - HEAD - Check security question [/v3/users/{user_id}/OS-TWO-FACTOR/sec_question?security_answer={security_answer}]
    - Two Factor Authentication Devices
        - POST - Remember new device or get new token [/v3/OS-TWO-FACTOR/devices?user_id={user_id}&user_name={user_name}&domain_name={domain_name}&device_id={device_id}&device_token={device_token}]
        - HEAD - Check for device [/v3/OS-TWO-FACTOR/devices?device_id={device_id}&device_token={device_token}&user_id={user_id}&user_name={user_name}&domain_name={domain_name}]
        - DELETE - Forget all devices [/v3/users/{user_id}/OS-TWO-FACTOR/devices]
- SCIM 2.0
    - Users
        - GET - List Users [/v3/OS-SCIM/v2/Users/]
        - POST - Create a User [/v3/OS-SCIM/v2/Users/]
    - User
        - GET - Read info about a User [/v3/OS-SCIM/v2/Users/{user_id}]
        - PUT - Update a User [/v3/OS-SCIM/v2/Users/{user_id}]
        - DELETE - Delete a User [/v3/OS-SCIM/v2/Users/{user_id}]
    - Organizations
        - GET - List Organizations [/v3/OS-SCIM/v2/Organizations]
        - POST - Create an Organization [/v3/OS-SCIM/v2/Organizations]
    - Organization
        - GET - Read info about an Organization [/v3/OS-SCIM/v2/Organizations/{organization_id}]
        - PUT - Update an Organization [/v3/OS-SCIM/v2/Organizations/{organization_id}]
        - DELETE - Delete an Organization [/v3/OS-SCIM/v2/Organizations/{organization_id}]
    - Service Provider
        - GET - Read Service Provider Configuration [/v3/OS-SCIM/v2/ServiceProviderConfigs]

License

API Specification

Keystone extensions

As Keyrock backend is based on Openstack Keystone, it fully implement its APIs. You can check them in OpenStack Identity API v3 specification. Openstack also provides some Identity API curl examples in order to understand how the API works.

In order to manage other entities that only Keyrock offers, you have to use the extensions APIs, explained bellow. These APIs are exposed by the back-end NOT the front-end.

Consumers [/v3/OS-OAUTH2/consumers]

Consumers are the Applications registered in Keyrock to consume OAuth2 resources.

List Consumers

GET /v3/OS-OAUTH2/consumers

Create a Consumer

POST /v3/OS-OAUTH2/consumers

Consumer [/v3/OS-OAUTH2/consumers/{consumer_id}]

Parameters

consumer_id (required)
Id of the consumer.

Read Consumer details

GET /v3/OS-OAUTH2/consumers/{consumer_id}

Update a Consumer

PATCH /v3/OS-OAUTH2/consumers/{consumer_id}

Delete a Consumer

DELETE /v3/OS-OAUTH2/consumers/{consumer_id}

Roles [/v3/OS-ROLES/roles]

List Roles

GET /v3/OS-ROLES/roles

Create a Role

POST /v3/OS-ROLES/roles

Role [/v3/OS-ROLES/roles/{role_id}]

Parameters

role_id (required)
Id of the role.

Read Role details

GET /v3/OS-ROLES/roles/{role_id}

Update a Role

PATCH /v3/OS-ROLES/roles/{role_id}

Delete a Role

DELETE /v3/OS-ROLES/roles/{role_id}

Permissions [/v3/OS-ROLES/permissions]

List Permissions

GET /v3/OS-ROLES/permissions

Create a Permission

POST /v3/OS-ROLES/permissions

Permission [/v3/OS-ROLES/permissions/{permission_id}]

Parameters

permission_id (required)
Id of the permission.

Read Permission details

GET /v3/OS-ROLES/permissions/{permission_id}

Update a Permission

PATCH /v3/OS-ROLES/permissions/{permission_id}

Delete a Permission

DELETE /v3/OS-ROLES/permissions/{permission_id}

Role - Permission Relationships [/v3/OS-ROLES/roles/{role_id}/permissions]

Parameters

role_id (required)
Id of the role.

List permissions associated to a role

GET /v3/OS-ROLES/roles/{role_id}/permissions

Role - Permission Relationship

[/v3/OS-ROLES/roles/{role_id}/permissions/{permission_id}]

Parameters

permission_id (required)
Id of the permission.
role_id (required)
Id of the role.

Assign a permission to a role

PUT /v3/OS-ROLES/roles/{role_id}/permissions/{permission_id}

Remove a permission from a role

DELETE /v3/OS-ROLES/roles/{role_id}/permissions/{permission_id}

Role - User Relationships [/v3/OS-ROLES/users/role_assignments]

List users role assignments

GET /v3/OS-ROLES/users/role_assignments

Role - User Relationship

[/v3/OS-ROLES/users/{user_id}/applications/{application_id}/roles/{role_id}]

Parameters

application_id (required)
Id of the application.
role_id (required)
Id of the role.
user_id (required)
Id of the user.

Assign a role to a user

PUT /v3/OS-ROLES/users/{user_id}/applications/{application_id}/roles/{role_id}

Remove a role assignment from a user

DELETE /v3/OS-ROLES/users/{user_id}/applications/{application_id}/roles/{role_id}

Role - User Relationship inside an organization

[/v3/OS-ROLES/users/{user_id}/organizations/{organization_id}/applications/{application_id}/roles/{role_id}]

Parameters

application_id (required)
Id of the application.
organization_id (required)
Id of the organization.
role_id (required)
Id of the role.
user_id (required)
Id of the user

Assign a role to a user inside an organization

PUT /v3/OS-ROLES/users/{user_id}/organizations/{organization_id}/applications/{application_id}/roles/{role_id}

Remove a role assignment from a user inside an organization

DELETE /v3/OS-ROLES/users/{user_id}/organizations/{organization_id}/applications/{application_id}/roles/{role_id}

Role - Organization Relationships **[/v3/OS-ROLES/organizations/role_assignments]**

List organizations role assignments

GET /v3/OS-ROLES/organizations/role_assignments

Role - Organization Relationship

[/v3/OS-ROLES/organizations/{organization_id}/applications/{application_id}/roles/{role_id}]

Parameters

application_id (required)
Id of the application.

organization_id (required)
Id of the organization.

role_id (required)
Id of the role.

Assign a rol to an organization

PUT /v3/OS-ROLES/organizations/{organization_id}/applications/{application_id}/roles/{role_id}

Remove a role assignment from an organization

DELETE /v3/OS-ROLES/organizations/{organization_id}/applications/{application_id}/roles/{role_id}

Two Factor Authentication

[/v3/OS-TWO-FACTOR/two_factor_auth?user_id={user_id}&user_name={user_name}&domain_id={domain_id}&domain_name={domain_name}]

Check if two factor authentication is enabled for a certain user

HEAD /v3/OS-TWO-FACTOR/two_factor_auth?user_id={user_id}&user_name={user_name}&domain_id={domain_id}&domain_name={domain_name}

Either user_id or user_name (along with domain_id or domain_name) must be provided.

Parameters

domain_id (optional)
ID of the domain that the user belongs to.

domain_name (optional)
Name of the domain that the user belongs to.

user_id (optional)
ID of the user to be checked.

user_name (optional)
Name of the user to be checked.

Two Factor Authentication Keys [/v3/users/{user_id}/OS-TWO-FACTOR/two_factor_auth]

Parameters

user_id (required)
ID of the user.

Enable two factor authentication / Get new key

POST /v3/users/{user_id}/OS-TWO-FACTOR/two_factor_auth

Disable two factor authentication

DELETE /v3/users/{user_id}/OS-TWO-FACTOR/two_factor_auth

Two Factor Authentication Security Questions [/v3/users/{user_id}/OS-TWO-FACTOR/]

Parameters

user_id (required)
ID of the user.

Retrieve non-sensitive data

GET /v3/users/{user_id}/OS-TWO-FACTOR/two_factor_data

Check security question

HEAD /v3/users/{user_id}/OS-TWO-FACTOR/sec_question?security_answer={security_answer}

Parameters

security_answer (required)
Answer to be checked.

Two Factor Authentication Devices [/v3/OS-TWO-FACTOR/devices]

Remember new device or get new token

POST /v3/OS-TWO-FACTOR/devices?user_id={user_id}&user_name={user_name}&domain_name={domain_name}&device_id={device_id}&device_token={device_token}

Either user_id or user_name and domain_name must be provided. The parameter device_token is required when providing device_id.

Parameters

device_id (optional)
ID of the device to be remembered, none if new one.
device_token (optional)
Current token of the device, none if new one.
domain_name (optional)
Name of the domain that the user belongs to.
user_id (optional)
ID of the user.
user_name (optional)
Name of the user.

Check for device

HEAD /v3/OS-TWO-FACTOR/devices?device_id={device_id}&device_token={device_token}&user_id={user_id}&user_name={user_name}&domain_name={domain_name}

Either user_id or user_name and domain_name must be provided.

Parameters

device_id (required)
ID of the device to be checked.
device_token (required)
Current token of the device to be checked.
domain_name (optional)
Name of the domain that the user belongs to.
user_id (optional)
ID of the user.
user_name (optional)
Name of the user.

Forget all devices

DELETE /v3/users/{user_id}/OS-TWO-FACTOR/devices

Parameters

user_id (required)
ID of the user.

SCIM 2.0

The IDM provides several authentication mechanisms. Any of them is valid to access the SCIM 2.0 API.

The access to the SCIM 2.0 API (except ServiceProvider calls) is only allowed for administrators, access attempts performed by non-admin users will be answered with HTTP 401 (Unauthorized).

In this case, we will be using version 2.0 of the API, but version 1.1 is compatible. To use version 1.1, replace in the examples below v2 with v1. In the case of the organizations, only v2 is available.

Just like Keystone extensions, these APIs are exposed by the back-end NOT the front-end.

Users [/v3/OS-SCIM/v2/Users/]

List Users

GET /v3/OS-SCIM/v2/Users/

Create a User

POST /v3/OS-SCIM/v2/Users/

User [/v3/OS-SCIM/v2/Users/{user_id}]

Parameters

user_id (required)
Id of the user.

Read info about a User

GET /v3/OS-SCIM/v2/Users/{user_id}

Update a User

PUT /v3/OS-SCIM/v2/Users/{user_id}

Delete a User

DELETE /v3/OS-SCIM/v2/Users/{user_id}

Organizations [/v3/OS-SCIM/v2/Organizations]

List Organizations

GET /v3/OS-SCIM/v2/Organizations

Create an Organization

POST /v3/OS-SCIM/v2/Organizations

Organization [/v3/OS-SCIM/v2/Organizations/{organization_id}]

Parameters

organization_id (required)
Id of the organization.

Read info about an Organization

GET /v3/OS-SCIM/v2/Organizations/{organization_id}

Update an Organization

PUT /v3/OS-SCIM/v2/Organizations/{organization_id}

Delete an Organization

DELETE /v3/OS-SCIM/v2/Organizations/{organization_id}

Service Provider [/v3/OS-SCIM/v2/ServiceProviderConfigs]

Read Service Provider Configuration

GET /v3/OS-SCIM/v2/ServiceProviderConfigs

"Information" provides the number of total users, total organizations (not counting the default organizations), cloud organizations, and the number of each type of user (basic, trial and community).

Examples

Keystone extensions

Consumers

[/v3/OS-OAUTH2/consumers]

List Consumers

GET /v3/OS-OAUTH2/consumers

Request /v3/OS-OAUTH2/consumers

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body


```
{
  "links": {
    "self": "http://host/v3/OS-OAUTH2/consumers",
    "previous": null,
    "next": null
  },
  "consumers": [
    {
      "scopes": [
        "all_info"
      ],
      "redirect_uris": [
        "http://my_app/login"
      ],
      "img_small": "ApplicationAvatar/small/asdasdasdasdasdad",
      "name": "App test",
      "links": {
        "self": "http://host/v3/OS-OAUTH2/consumers/asdasdasdasdasdad"
      },
      "extra": {
        "url": "http://app.com",
        "img_original": "ApplicationAvatar/original/asdasdasdasdasdad",
        "img_small": "ApplicationAvatar/small/asdasdasdasdasdad",
        "img_medium": "ApplicationAvatar/medium/asdasdasdasdasdad"
      },
      "url": "http://app.com",
      "img_original": "ApplicationAvatar/original/asdasdasdasdasdad",
      "client_type": "confidential",
      "response_type": "code",
      "img_medium": "ApplicationAvatar/medium/asdasdasdasdasdad",
      "grant_type": "authorization_code",
      "id": "asdasdasdasdasdad",
      "description": "App test"
    }
  ]
}
```


Create a Consumer

POST /v3/OS-OAUTH2/consumers

Request /v3/OS-OAUTH2/consumers (application/json)

Headers

```
Content-Type: application/json
X-Auth-token: token
```

Body


```
{
  "consumer": {
    "name": "test_consumer",
    "description": "my test consumer",
    "client_type": "confidential",
    "redirect_uris": [
      "http://localhost/login"
    ],
    "grant_type": "authorization_code",
    "scopes": [
      "all_info"
    ]
  }
```

```
}
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body


```
{
  "consumer": {
    "scopes": [
      "all_info"
    ],
    "redirect_uris": [
      "http://localhost/login"
    ],
    "description": "my test consumer",
    "links": {
      "self": "http://host/v3/OS-OAUTH2/consumers/308423904823490234923"
    },
    "extra": {},
    "secret": "3534535345345",
    "client_type": "confidential",
    "response_type": "code",
    "grant_type": "authorization_code",
    "id": "308423904823490234923",
    "name": "test_consumer"
  }
}
```


Consumer

[/v3/OS-OAUTH2/consumers/{consumer_id}]

Read Consumer details

GET /v3/OS-OAUTH2/consumers/{consumer_id}

Request /v3/OS-OAUTH2/consumers/{consumer_id}

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body


```
    {
      "consumer": {
        "scopes": [
          "all_info"
        ],
        "redirect_uris": [
          "http://app.com/v1/login_fiware"
```

```
        ],
        "img_small": "ApplicationAvatar/small/dddjajdsajd23234232342",
        "name": "App test",
        "links": {
          "self": "http://host/v3/OS-OAUTH2/consumers/dddjajdsajd23234232342"
        },
        "extra": {
          "url": "http://app.com/v1",
          "img_original": "ApplicationAvatar/original/dddjajdsajd23234232342",
          "img_small": "ApplicationAvatar/small/dddjajdsajd23234232342",
          "img_medium": "ApplicationAvatar/medium/dddjajdsajd23234232342"
        },
        "url": "http://app.com/v1",
        "img_original": "ApplicationAvatar/original/dddjajdsajd23234232342",
        "description": "App test",
        "secret": "43534534535345345345345",
        "client_type": "confidential",
        "response_type": "code",
        "grant_type": "authorization_code",
        "id": "dddjajdsajd23234232342",
        "img_medium": "ApplicationAvatar/medium/dddjajdsajd23234232342"
      }
    }
```


Update a Consumer

PATCH /v3/OS-OAUTH2/consumers/{consumer_id}

Request /v3/OS-OAUTH2/consumers/{consumer_id} (application/json)

Headers

```
Content-Type: application/json
X-Auth-token: token
```

Body

```
{
  "consumer": {
    "field_to_update": "value",
    "antoher_field_to_update": [
      "another_value"
    ]
  }
}
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Delete a Consumer

DELETE /v3/OS-OAUTH2/consumers/{consumer_id}

Request /v3/OS-OAUTH2/consumers/{consumer_id}

Headers

```
X-Auth-token: token
```

Response 204 (application/json)

Headers

```
Content-Type: application/json
```

Roles

[/v3/OS-ROLES/roles]

List Roles

GET /v3/OS-ROLES/roles

Request /v3/OS-ROLES/roles

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body


```
{
  "links": {
    "self": "http://host/v3/OS-ROLES/roles",
    "previous": null,
    "next": null
  },
  "roles": [
    {
      "is_internal": false,
      "application_id": "3123123131fg12f3g1f23g1jjjhg123h",
      "id": "3123123845782311312gff2h3782318",
      "links": {
        "self": "http://host/v3/OS-ROLES/roles/3123123845782311312gff2h3782318"
      },
      "name": "admin1"
    },
    {
      "is_internal": false,
      "application_id": "2312389718290371289371 2h3dh1031sd3",
      "id": "90834823948209f0sdf8jf'82kr820384",
      "links": {
        "self": "http://host/v3/OS-ROLES/roles/90834823948209f0sdf8jf82kr820384"
      },
      "name": "test"
    }
  ]
}
```

Create a Role

POST /v3/OS-ROLES/roles

Request /v3/OS-ROLES/roles (application/json)

Headers

```
Content-Type: application/json
X-Auth-token: token
```

Body

```
{
  "role": {
    "name": "test_role",
    "application_id": "2222"
  }
}
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body

```
{
  "role": {
    "is_internal": false,
    "application_id": "2222",
    "id": "308423904823490234923",
    "links": {
      "self": "http://host/v3/OS-ROLES/roles/308423904823490234923"
    },
    "name": "test_consumer"
  }
}
```

Role

[/v3/OS-ROLES/roles/{role_id}]

Read Role details

GET /v3/OS-ROLES/roles/{role_id}

Request /v3/OS-ROLES/roles/{role_id}

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body


```
{
  "role": {
    "is_internal": false,
    "application_id": "3893298128973173d9173712d3",
    "id": "213412312jsd3jsj3812s3123",
    "links": {
      "self": "http://host/v3/OS-ROLES/roles/213412312jsd3jsj3812s3123"
    },
    "name": "physician"
  }
}
```


Update a Role

PATCH /v3/OS-ROLES/roles/{role_id}

Request /v3/OS-ROLES/roles/{role_id} (application/json)

Headers

```
Content-Type: application/json
X-Auth-token: token
```

Body


```
{
  "role": {
    "name": "test_role_new",
    "application_id": "2222"
  }
}
```


Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Delete a Role

DELETE /v3/OS-ROLES/roles/{role_id}

Request /v3/OS-ROLES/roles/{role_id}

Headers

```
X-Auth-token: token
```

Response 204 (application/json)

Headers

```
Content-Type: application/json
```

Permissions

[/v3/OS-ROLES/permissions]

List Permissions

GET /v3/OS-ROLES/permissions

Request /v3/OS-ROLES/permissions

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body


```
{
  "links": {
    "self": "http://host/v3/OS-ROLES/permissions",
    "previous": null,
    "next": null
  },
  "permissions": [
    {
      "xml": "",
      "resource": "radio",
      "name": "Access",
      "links": {
        "self": "http://host/v3/OS-ROLES/permissions/72389398893218371743 4rhejas"
      },
      "is_internal": false,
      "action": "GET",
      "application_id": "3423423424c234cx2342c",
      "id": "72389398893218371743 4rhejas"
    },
    {
      "xml": "",
      "resource": "/ui/resource1",
      "name": "identify resource1",
      "links": {
        "self": "http://host/v3/OS-ROLES/permissions/3987429348'3239234234"
      },
      "is_internal": false,
      "action": "POST",
      "application_id": "234234xc43242c",
      "id": "3987429348'3239234234"
    }
  ]
}
```


Create a Permission

POST /v3/OS-ROLES/permissions

Request /v3/OS-ROLES/permissions (application/json)

Headers

```
Content-Type: application/json
X-Auth-token: token
```

Body

```
{
  "permission": {
    "name": "test_permission",
    "application_id": "2222"
  }
}
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body


```
{
  "permission": {
    "xml": null,
    "resource": null,
    "name": "test_consumer",
    "links": {
      "self": "http://host/v3/OS-ROLES/permissions/128379817348973489273498 3"
    },
    "is_internal": false,
    "action": null,
    "application_id": "2222",
    "id": "128379817348973489273498 3"
  }
}
```


Permission

[/v3/OS-ROLES/permissions/{permission_id}]

Read Permission details

GET /v3/OS-ROLES/permissions/{permission_id}

Request /v3/OS-ROLES/permissions/{permission_id}

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body


```
    {
      "permission": {
```

```
        "xml": "",
        "resource": "/enterprise/edit",
        "name": "Enterprise",
        "links": {
          "self": "http://host/v3/OS-ROLES/permissions/21897318273128937sh12a1"
        },
        "is_internal": false,
        "action": "GET",
        "application_id": "23129371237917f17fd07102d7",
        "id": "21897318273128937sh12a1"
      }
    }
```


Update a Permission

PATCH /v3/OS-ROLES/permissions/{permission_id}

Request /v3/OS-ROLES/permissions/{permission_id} (application/json)

Headers

```
Content-Type: application/json
X-Auth-token: token
```

Body

```
{
  "permission": {
    "name": "test_permission",
    "application_id": "2222"
  }
}
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Delete a Permission

DELETE /v3/OS-ROLES/permissions/{permission_id}

Request /v3/OS-ROLES/permissions/{permission_id}

Headers

```
X-Auth-token: token
```

Response 204 (application/json)

Headers

```
Content-Type: application/json
```

Role - Permission Relationships

[/v3/OS-ROLES/roles/{role_id}/permissions]

List permissions associated to a role

GET /v3/OS-ROLES/roles/{role_id}/permissions

Request /v3/OS-ROLES/roles/{role_id}/permissions

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body


```
{
  "links": {
    "self": "http://host/v3/OS-ROLES/permissions",
    "previous": null,
    "next": null
  },
  "permissions": [
    {
      "xml": null,
      "resource": "res2",
      "name": "getInfo",
      "links": {
        "self": "http://host/v3/OS-ROLES/permissions/237801283712837012387123 07"
      },
      "is_internal": false,
      "action": "GET",
      "application_id": "asdasdasd12313213123",
      "id": "237801283712837012387123 07"
    }
  ]
}
```


Role - Permission Relationship

[/v3/OS-ROLES/roles/{role_id}/permissions/{permission_id}]

Assign a permission to a role

PUT /v3/OS-ROLES/roles/{role_id}/permissions/{permission_id}

Request /v3/OS-ROLES/roles/{role_id}/permissions/{permission_id}

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Remove a permission from a role

DELETE /v3/OS-ROLES/roles/{role_id}/permissions/{permission_id}

Request /v3/OS-ROLES/roles/{role_id}/permissions/{permission_id}

Headers

```
X-Auth-token: token
```

Response 204 (application/json)

Headers

```
Content-Type: application/json
```

Role - User Relationships

[/v3/OS-ROLES/users/role_assignments]

List users role assignments

GET /v3/OS-ROLES/users/role_assignments

Request /v3/OS-ROLES/users/role_assignments

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body

```
{
  "role_assignments": [
    {
      "organization_id": "32163781263892173912312",
      "application_id": "12312301293-80181902380",
      "user_id": "30891239081038123",
      "role_id": "12331234"
    },
    {
      "organization_id": "00000000000000000000000000000frb",
      "application_id": "645765889gsdfadsasd",
      "user_id": "4341234213423234234",
      "role_id": "4324234"
    }
  ]
}
```

Role - User Relationship

[/v3/OS-ROLES/users/{user_id}/applications/{application_id}/roles/{role_id}]

Assign a role to a user

PUT /v3/OS-ROLES/users/{user_id}/applications/{application_id}/roles/{role_id}

Request /v3/OS-ROLES/users/{user_id}/applications/{application_id}/roles/{role_id}

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Role - User Relationship inside an organization

[/v3/OS-ROLES/users/{user_id}/organizations/{organization_id}/applications/{application_id}/roles/{role_id}]

Assign a role to a user inside an organization

PUT /v3/OS-ROLES/users/{user_id}/organizations/{organization_id}/applications/{application_id}/roles/{role_id}

Request /v3/OS-ROLES/users/{user_id}/organizations/{organization_id}/applications/{application_id}/roles/{role_id}

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Remove a role assignment from a user inside an organization

DELETE /v3/OS-ROLES/users/{user_id}/organizations/{organization_id}/applications/{application_id}/roles/{role_id}

Request /v3/OS-ROLES/users/{user_id}/organizations/{organization_id}/applications/{application_id}/roles/{role_id}

Headers

```
X-Auth-token: token
```

Response 204 (application/json)

Headers

```
Content-Type: application/json
```

Role - Organization Relationship

[/v3/OS-ROLES/organizations/{organization_id}/applications/{application_id}/roles/{role_id}]

Assign a rol to an organization

PUT /v3/OS-ROLES/organizations/{organization_id}/applications/{application_id}/roles/{role_id}

Request /v3/OS-ROLES/organizations/{organization_id}/applications/{application_id}/roles/{role_id}

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Remove a role assignment from an organization

DELETE /v3/OS-ROLES/organizations/{organization_id}/applications/{application_id}/roles/{role_id}

Request /v3/OS-ROLES/organizations/{organization_id}/applications/{application_id}/roles/{role_id}

Headers

```
X-Auth-token: token
```

Response 204 (application/json)

Headers

```
Content-Type: application/json
```

Two Factor Authentication

[/v3/OS-TWO-FACTOR/two_factor_auth?user_id={user_id}&user_name={user_name}&domain_id={domain_id}&domain_name={domain_name}]

Check if two factor authentication is enabled for a certain user

HEAD /v3/OS-TWO-FACTOR/two_factor_auth?user_id={user_id}&user_name={user_name}&domain_id={domain_id}&domain_name={domain_name}

Request /v3/OS-TWO-FACTOR/two_factor_auth?domain_id={domain_id}&domain_name={domain_name}&user_id={user_id}&user_name={user_name}

Headers

```
X-Auth-token: token
```

Response 204

Two Factor Authentication Keys

[/v3/users/{user_id}/OS-TWO-FACTOR/two_factor_auth]

Enable two factor authentication / Get new key

POST /v3/users/{user_id}/OS-TWO-FACTOR/two_factor_auth

Request /v3/users/{user_id}/OS-TWO-FACTOR/two_factor_auth (application/json)

Headers

```
Content-Type: application/json
X-Auth-token: token
```

Body

```
{
    "two_factor_auth": {
        "security_question":"sample question",
        "security_answer":"sample answer"
    }
}
```

Response 201 (application/json)

Headers

```
Content-Type: application/json
```

Body

```
{
    "two_factor_auth": {
        "two_factor_key": "TSLX244ZPTDFTF43",
        "user_id": "user0",
        "links": {
            "self": "http://localhost:5000/v3/OS-TWOFACTOR/two_factor_auth"
        },
        "uri": "otpauth://totp/FIWARE%20Lab%20Accounts:user0@test.com?secret=TSLX244ZPTDFTF43&
issuer=FIWARE%20Lab%20Accounts",
        "security_answer": "sample question",
        "security_question": "sample answer"
    }
}
```

Request /v3/users/{user_id}/OS-TWO-FACTOR/two_factor_auth (application/json)

Headers

```
Content-Type: application/json
X-Auth-token: token
```

Response 201 (application/json)

Headers

```
Content-Type: application/json
```

Body


```
{
    "two_factor_auth": {
        "two_factor_key": "O3JGFSSJZHQL24Q6",
        "user_id": "user_0",
        "links": {
            "self": "http://localhost:5000/v3/OS-TWOFACTOR/two_factor_auth"
        },
        "uri": "otpauth://totp/FIWARE%20Lab%20Accounts:user0@test.com?secret=O3JGFSSJZHQL24Q6&
issuer=FIWARE%20Lab%20Accounts",
        "security_answer": "sample question",
        "security_question": "sample answer"
    }
}
```


Disable two factor authentication

DELETE /v3/users/{user_id}/OS-TWO-FACTOR/two_factor_auth

Request /v3/users/{user_id}/OS-TWO-FACTOR/two_factor_auth

Headers

```
X-Auth-token: token
```

Response 204

Two Factor Authentication Security Questions

[/v3/users/{user_id}/OS-TWO-FACTOR/]

Retrieve non-sensitive data

GET /v3/users/{user_id}/OS-TWO-FACTOR/two_factor_data

Request /v3/users/{user_id}/OS-TWO-FACTOR/two_factor_data

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body

```
{
    "two_factor_auth": {
        "security_question": "sample question",
        "user_id": "user0",
        "links": {
            "self": "http://localhost:5000/v3/OS-TWOFACTOR/two_factor_auth"
        }
    }
}
```

Check security question

HEAD /v3/users/{user_id}/OS-TWO-FACTOR/sec_question?security_answer={security_answer}

Request /v3/users/{user_id}/OS-TWO-FACTOR/sec_question?security_answer={security_answer} (application/json)

Headers

```
Content-Type: application/json
X-Auth-token: token
```

Response 204

Two Factor Authentication Devices

[/v3/OS-TWO-FACTOR/devices]

Remember new device or get new token

POST /v3/OS-TWO-FACTOR/devices?user_id={user_id}&user_name={user_name}&domain_name={domain_name}&device_id={device_id}&device_token={device_token}

Request /v3/OS-TWO-FACTOR/devices?device_id={device_id}&device_token={device_token}&domain_name={domain_name}&user_id={user_id}&user_name={user_name}

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body

```
{
    "two_factor_auth": {
        "device_token": "7525dc5bc8134b4a97526bcd7e45175e",
        "links": {
            "self": "http://localhost:5000/v3/OS-TWOFACTOR/two_factor_auth"
```

```
        },
        "device_id": "815dfb0790934775bc8dac15f197a1f0"
    }
}
```

Check for device

HEAD /v3/OS-TWO-FACTOR/devices?device_id={device_id}&device_token={device_token}&user_id={user_id}&user_name={user_name}&domain_name={domain_name}

Request /v3/OS-TWO-FACTOR/devices?device_id={device_id}&device_token={device_token}&domain_name={domain_name}&user_id={user_id}&user_name={user_name}

Headers

```
X-Auth-token: token
```

Response 204

SCIM 2.0

Users

[/v3/OS-SCIM/v2/Users/]

List Users

GET /v3/OS-SCIM/v2/Users/

Request /v3/OS-SCIM/v2/Users/

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body

```
{
  "totalResults": 12,
  "Resources": [...],
  "schemas": [
    "urn:scim:schemas:core:2.0",
    "urn:scim:schemas:extension:keystone:2.0"
  ]
}
```

Create a User

POST /v3/OS-SCIM/v2/Users/

Request /v3/OS-SCIM/v2/Users/ (application/json)

Headers

```
Content-Type: application/json
X-Auth-token: token
```

Body

```
{
  "userName": "alice",
  "displayName": "Alice",
  "password": "passw0rd",
  "emails": [
    {
      "value": "alice@mailhost.com"
    }
  ]
}
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

User

[/v3/OS-SCIM/v2/Users/{user_id}]

Read info about a User

GET /v3/OS-SCIM/v2/Users/{user_id}

Request /v3/OS-SCIM/v2/Users/{user_id}

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body

```
{
  "userName": "user1@user.com",
  "urn:scim:schemas:extension:keystone:2.0": {
    "domain_id": "default"
  },
  "active": true,
  "id": "user1",
```

```
  "schemas": [
    "urn:scim:schemas:core:2.0",
    "urn:scim:schemas:extension:keystone:2.0"
  ]
}
```

Update a User

PUT /v3/OS-SCIM/v2/Users/{user_id}

Request /v3/OS-SCIM/v2/Users/{user_id} (application/json)

Headers

```
Content-Type: application/json
X-Auth-token: token
```

Body

```
{
  "userName": "alice",
  "displayName": "Alice",
  "password": "passw0rd_new",
  "emails": [
    {
      "value": "alice@mailhost.com"
    }
  ]
}
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Delete a User

DELETE /v3/OS-SCIM/v2/Users/{user_id}

Request /v3/OS-SCIM/v2/Users/{user_id}

Headers

```
X-Auth-token: token
```

Response 204 (application/json)

Headers

```
Content-Type: application/json
```

Organizations

[/v3/OS-SCIM/v2/Organizations]

List Organizations

GET /v3/OS-SCIM/v2/Organizations

Request /v3/OS-SCIM/v2/Organizations

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body

```
{
  "totalResults": 24,
  "Resources": [...],
  "schemas": [
    "urn:scim:schemas:core:2.0",
    "urn:scim:schemas:extension:keystone:2.0"
  ]
}
```

Create an Organization

POST /v3/OS-SCIM/v2/Organizations

Request /v3/OS-SCIM/v2/Organizations (application/json)

Headers

```
Content-Type: application/json
X-Auth-token: token
```

Body

```
{
  "name": "Name of organization",
  "is_default": true,
  "domain_id": "domain",
  "active": true,
  "id": "ID"
}
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Organization

[/v3/OS-SCIM/v2/Organizations/{organization_id}]

Read info about an Organization

GET /v3/OS-SCIM/v2/Organizations/{organization_id}

Request /v3/OS-SCIM/v2/Organizations/{organization_id}

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body

```
{
  "name": "org1",
  "is_default": true,
  "urn:scim:schemas:extension:keystone:2.0": {
    "domain_id": "default"
  },
  "active": true,
  "id": "22928e07c0bd4063a7f0bb8c826b0a18",
  "schemas": [
    "urn:scim:schemas:core:2.0",
    "urn:scim:schemas:extension:keystone:2.0"
  ]
}
```

Update an Organization

PUT /v3/OS-SCIM/v2/Organizations/{organization_id}

Request /v3/OS-SCIM/v2/Organizations/{organization_id} (application/json)

Headers

```
Content-Type: application/json
X-Auth-token: token
```

Body

```
{
    "name": "New name of organization",
    "is_default": true,
    "domain_id": "domain",
    "active": true,
    "id": "ID"
}
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Service Provider

[/v3/OS-SCIM/v2/ServiceProviderConfigs]

Read Service Provider Configuration

GET /v3/OS-SCIM/v2/ServiceProviderConfigs

Request /v3/OS-SCIM/v2/ServiceProviderConfigs

Headers

```
X-Auth-token: token
```

Response 200 (application/json)

Headers

```
Content-Type: application/json
```

Body


```
{
  "sort": {
    "supported": false
  },
  "bulk": {
    "maxPayloadSize": 0,
    "supported": false,
    "maxOperations": 0
  },
  "changePassword": {
    "supported": true
  },
  "xmlDataFormat": {
    "supported": false
  },
  "information": {
    "basicUsers": 1,
    "totalCloudOrganizations": 12,
    "totalUserOrganizations": 24,
    "communityUsers": 0,
    "totalUsers": 12,
    "trialUsers": 0,
    "totalResources": 48
  },
  "documentationUrl": "https://github.com/ging/fi-ware-idm/wiki/SCIM-2.0-API",
  "patch": {
    "supported": true
  },
  "filter": {
    "supported": true,
    "maxResults": 9223372036854775807
  },
  "etag": {
    "supported": false
  },
  "schemas": [
    "urn:scim:schemas:core:2.0:ServiceProviderConfig"
  ],
  "authenticationSchemes": [
    {
```

```
      "name": "Keytone Authentication",
      "documentationUrl": "http://keystone.openstack.org/",
      "primary": true,
      "specUrl": "http://specs.openstack.org/openstack/keystone-specs",
      "type": "keystonetoken",
      "description": "Authentication using Keystone"
    }
  ]
}
```

Acknowledgements

The editors would like to express their gratitude to all the people that have contributed to this specification.

References

- Apiary project (http://docs.keyrock.apiary.io/#reference)
- Github source (https://github.com/ging/fiware-idm)
- Generic Enabler service (https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE.ArchitectureDescription.Security.IdentityManagement)
- UPM (https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/UPM)
- FIWARE Open Specification License (implicit patent license) (http://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FI-WARE_Open_Specification_Legal_Notice_%28implicit_patents_license%29)
- FIWARE IdM Github Project (https://github.com/ging/fiware-idm/issues)
- OpenStack Identity API v3 specification (http://developer.openstack.org/api-ref-identity-v3.html)
- Identity API curl examples (http://docs.openstack.org/developer/keystone/api_curl_examples.html)