User Management (USM) - User Manual

*v. 1.0 – 2015-11-30*

Table of Contents

[Introduction 3](#_Toc436993350)

[Glossary 3](#_Toc436993351)

[Profile: Normal User 5](#_Toc436993352)

[How to change my security answers 5](#_Toc436993353)

[How to update my personal data 6](#_Toc436993354)

[How to change my password 7](#_Toc436993355)

[How to request a password 7](#_Toc436993356)

[How to know my different profiles 9](#_Toc436993357)

[How to log out from the system 9](#_Toc436993358)

[Profile: Administrator 10](#_Toc436993359)

[How to find back User information & Access Rights 10](#_Toc436993360)

[How to change a User password 11](#_Toc436993361)

[How to create a User 11](#_Toc436993362)

[How to give access rights to a User 13](#_Toc436993363)

[How to manage Organisations and related information 15](#_Toc436993364)

[Organisation 15](#_Toc436993365)

[Endpoint 17](#_Toc436993366)

[Communication Channel 18](#_Toc436993367)

[Endpoint contacts 19](#_Toc436993368)

[How to manage Policies 19](#_Toc436993369)

[How to manage Roles 21](#_Toc436993370)

[Features/Permissions 22](#_Toc436993371)

[Modify a role definition 23](#_Toc436993372)

[How to manage Scopes 24](#_Toc436993373)

[Datasets 25](#_Toc436993374)

[Modify a scope definition 26](#_Toc436993375)

[How to view Application information 28](#_Toc436993376)

[How to view data exposed by Applications 28](#_Toc436993377)

[How to validate user changes 30](#_Toc436993378)

# Introduction

This document is a basic user guide for the USM (User Security Management) application v1.7.1, called the User (Management) module when integrated under U-VMS.

Operations that can be performed in the user web interface are described in this document.

The main roles of USM cover the user authentication, user authorisation and the management of user data and related data. More precisely:

* to store data about users that might have access to applications, their access rights and information about organisations;
* to authenticate users;
* to verify or disseminate the user access rights;
* to disseminate information about organisations;

# Glossary

**Application**: it is a computer program designed to perform a group of coordinated functions, tasks, or activities. An application can be linked to USM. If so, it means that:

1. The application delegates the user authentication task to USM;
2. The application can request to get or to verify the access rights of a user;
3. The application exposes through a USM service a set of information used by USM to create user contexts;

**Communication channel**: A medium through which a message is transmitted to its intended audience. A communication channel in USM is attached to an endpoint and it specifies the type of messages that could be transmitted through.

**Context**: a context is always for a user but a user may have multiple ones. It is a container of three elements defining his framework for one or multiple applications. In basic terms, the container defines the WWH for each user: '**W**hat can he do', '**W**hat can he see', '**H**ow he wants to see data'. The three elements are:

1. Role: list of permissions to limit the actions of the user (The first W). It is the only mandatory element of a context;
2. Scope: list of datasets to limit the access to data for the user (the second W);
3. User preferences: list of options configured by the user (the H);

**Dataset**: it is a business information of an application that can be used to limit the access to data for a user, so a kind of filter. An application linked to USM may register in USM the list of his datasets that are used to create the context of a user;

**Endpoint**: it is a technical node in a network used for message exchanges. Technical information is stored in USM at the level of an organisation.

**Feature**: it is a function of an application. An application linked to USM must register in USM the list of his features that are used to give permissions to a user;

**IDM system:** Identity Management system used mainly to manage user data and credentials.

**LDAP:** Lightweight Directory Access Protocol system used to share corporate data like user information across an organisation or over internet.

**Module**: it is a synonym of "application" but this notion implies usually that a module is linked to a parent application.

**Option**: it is a parameter of an application that can be used by users to customize the layout (color of lines …) or the behaviour (refresh rate of a report …) of the application. An option has always a default value. When included in a user context, the option (with a specific value chosen by the user) becomes a user preference. An application linked to USM may register in USM the list of his options that are used to configure the context of a user;

**Permission**: it is a feature in a role affected to a user;

**Profile**: it is the set of all contexts attached to a user;

**Role**: it is a set of permissions on one or multiple applications;

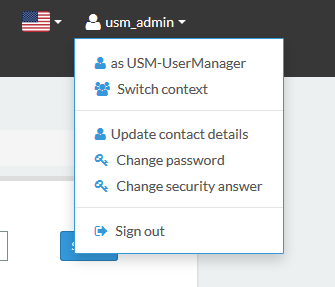
**Scope**: it is a set of datasets from one or multiple applications. The scope is defined to limit the access to data when used in a user context;

# Profile: Normal User

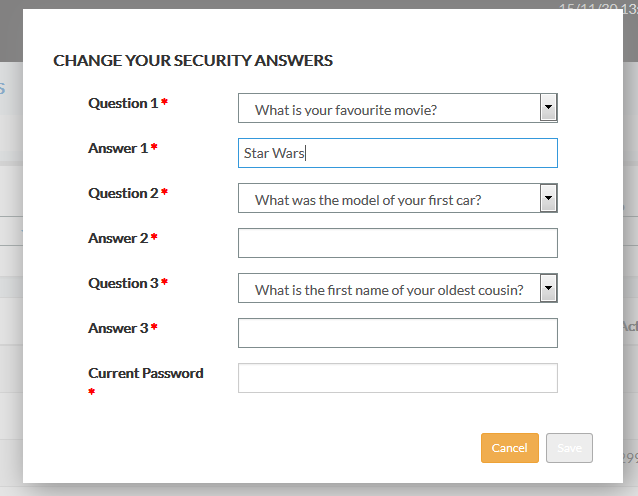
This list of actions may be triggered by any user of the U-VMS application.

## How to change my security answers

Option 'Change security answers' from the user contextual menu:



A pop-up displays a list of questions and answers (mandatory fields are marked with a red '\*'):



When activated for the first time, the list is empty. The user must choose a question in a list of predefined questions and provide an answer. The number of questions to be replied by the user is a parameter of the system (cfr Policies).

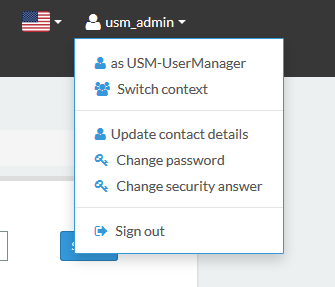
If it is not the first time, the list is filled with the previous answers of the user. The user may modify the reply and/or to change the question.

The system verifies that a question has not been selected more than once and that an answer has a minimum of three characters.

This list of security questions is used when the user has forgotten his password (cfr How to request a password).

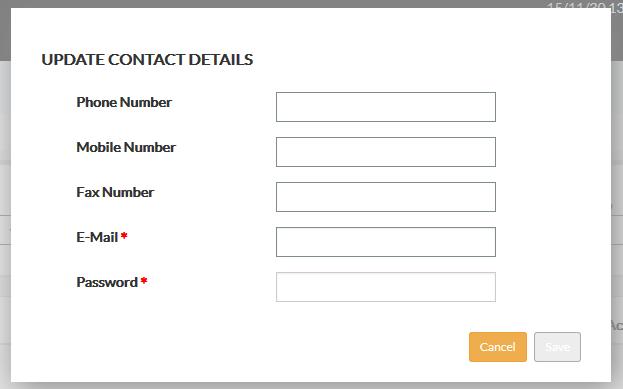
## How to update my personal data

Option 'Update contact details' from the user contextual menu (mandatory fields are marked by a '\*'):



A pop-up displays the following user information that may be modified (mandatory fields are marked with a red '\*'):

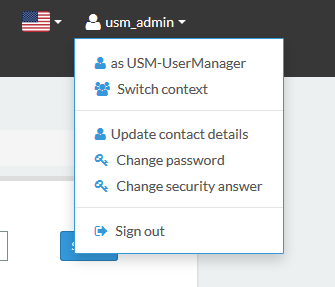
* Phone number
* Mobile number
* Fax number
* Email



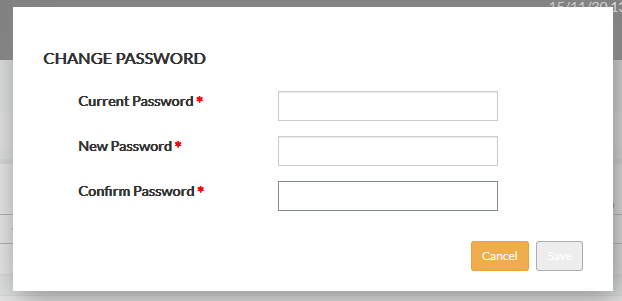
The "Password" field is not used to modify the password. It is a security channel to confirm the identity of the user. The 'save' button to commit changes is only active when the password has been filled in.

## How to change my password

Option 'Change password' from the user contextual menu:



A pop-up appears where the user must enter the current password and two times the new one (mandatory fields are marked with a red '\*'):



Depending on the password policies put in place in the system (cfr Policies), the system performs some controls based on: a minimum length, minimum number of digits, minimum number of special characters (!""£$%^&’\*(),./:@~<>+=-#), recent occurrence in the password history…

## How to request a password

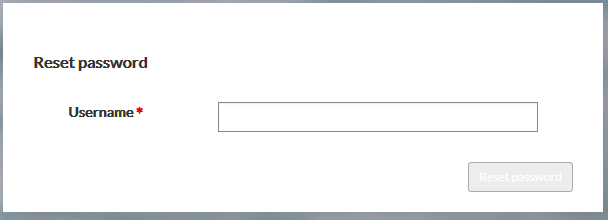
Two cases are possible:

1. The first time: the user must follow the procedure put in place by the organisation for such case. If there is no official procedure, the administrator of the system must be contacted.
2. Forgotten password:

In the login screen, the option 'Forgot your password?' can be activated:



A pop-up is displayed to request the username (mandatory fields are marked with a red '\*'):



Therefore, two cases are possible:

* 1. The user has already filled-in the security questions (cfr How to change my security answers): if so, the security question panel is displayed with the set of questions chosen by the user. The user must enter the answers and two times a new password. If no problem is detected (i.e. the answers are correct and the new password respects the password policies (cfr How to change my password), a successful message is displayed. The user can enter in the log in screen again with the new password.
  2. The user has no security questions (cfr How to change my security answers): the email address of the user registered in the system is used to send him an email with a temporary password. At first log in, the user must change it.

Example of email sent by the system:

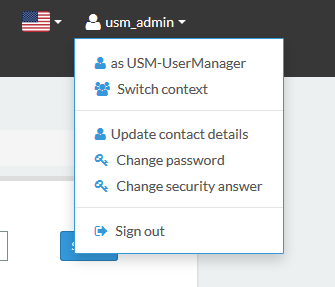
*Here is your new password:*

*u2y#rNs\*T8*

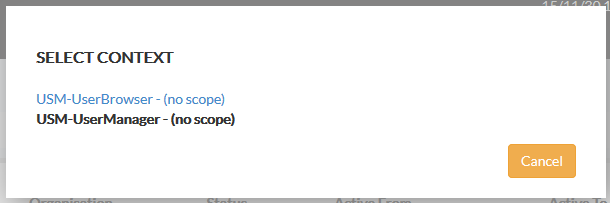
*Please login and change it.*

## How to know my different profiles

Option 'Switch context' from the user contextual menu:



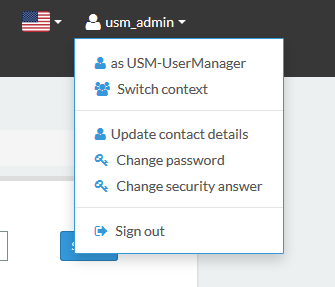
The list of contexts (role and scope) attached to the user is displayed:



The user may choose any context during his session. Depending on the selected context (and the permissions contained in), the web interface is automatically adapted to see only the options that the user may use.

## How to log out from the system

Option 'Sign out' from the user contextual menu:



# Profile: Administrator

This list of actions may be triggered by a user with special rights on the USM system.

## How to find back User information & Access Rights

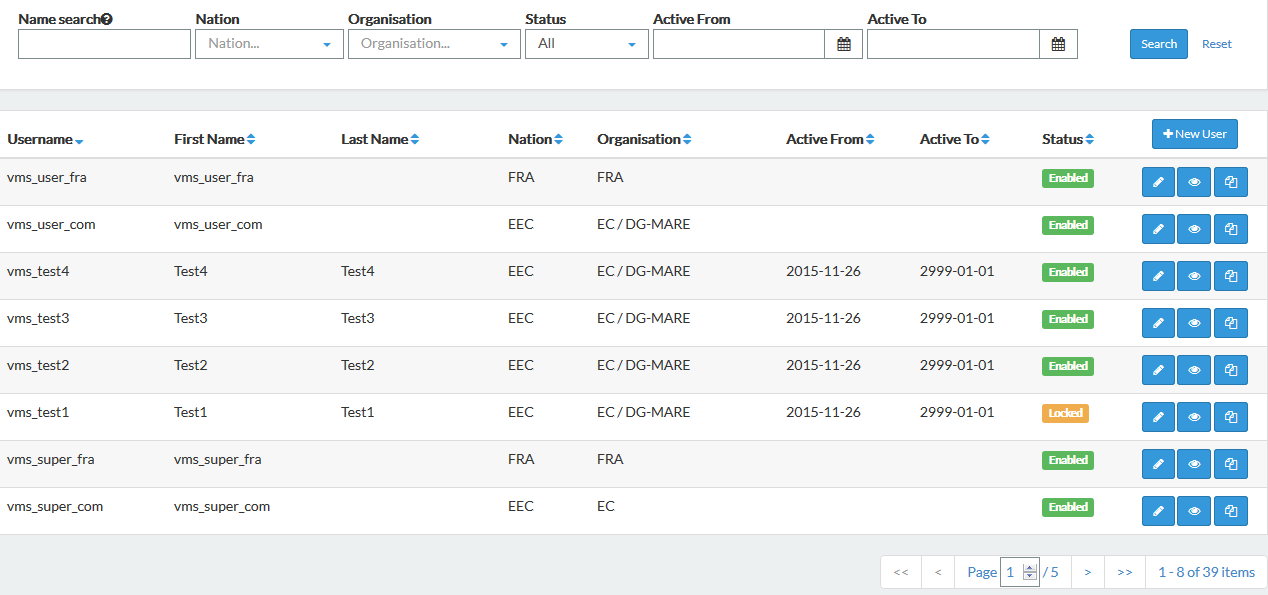
User information is accessible through the 'USERS' option from the main menu:



The web screen provides a set of filters to find back the users:

* Name search: a set of characters can be provided. The search is performed on the Username, First Name and Last Name. The position of the characters entered for the search in the data is not important;
* Nation: a selection of one entry in the list of countries registered in the system;
* Organisation: a selection of one entry in the list of organisations managed by the system;
* Status: a selection of one entry in the list of user statuses defined in the system;
* Active from: date from which users can be active in the system;
* Active to: date until when users can be active in the system;

The result of the search is displayed below the set of filters:



When there is no data corresponding to the search criteria, the message 'No result found.' is displayed.

If the search is successful, the list of users matching the criteria is displayed. For each user, the icon gives access to detailed user information in three tabs:

* Contact and Status Details: user information;
* Contexts: user rights (see context definition);
* Preferences: user preferences;

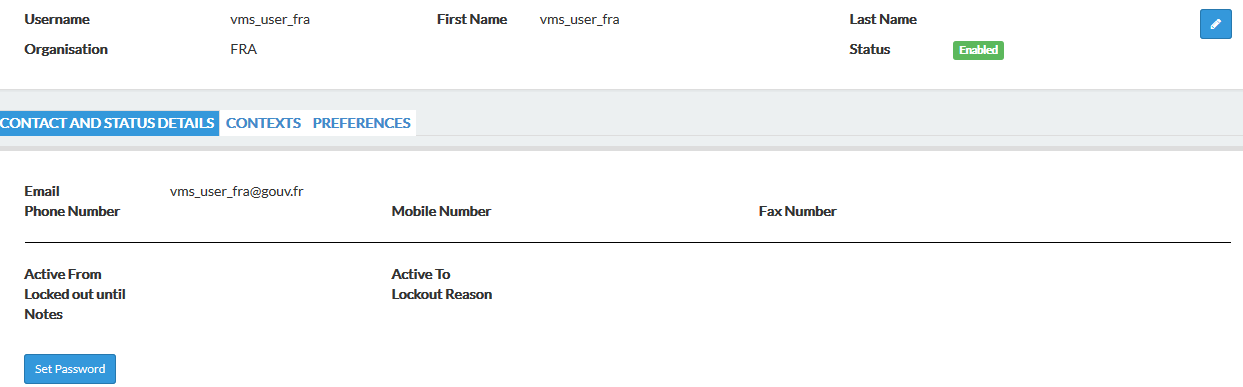
## How to change a User password

**This feature is not possible through USM if the system use an Identity Management (IDM) system.**

If so, the management of passwords must be done in that system and the corresponding option(s) in USM are not active.

If the management of passwords is delegated to USM, the following actions should be done:

1. To find back the user: cfr How to find back User information
2. For that user, to select the option for detailed user information. In the web screen, the option **'Set Password**' is visible.
3. The administrator may enter twice a new password for the user.



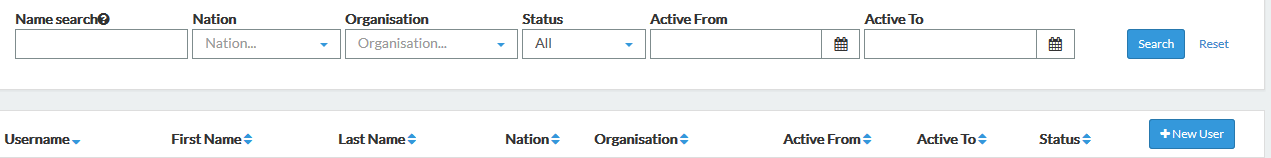
The communication of that new password to the user is not covered by the system.

## How to create a User

The following actions should be done:

1. To select the option 'USERS' in the main menu
2. In the web screen, the option '**New User**' is visible:





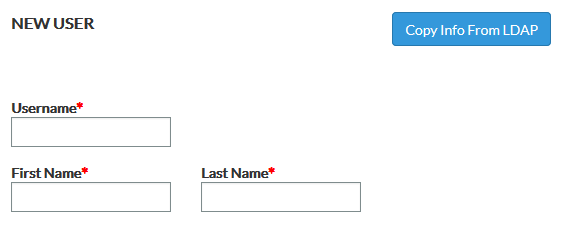
There are two ways of creating a user depending on the technical environment in place:

1. Using a IDM

The user interface allows a USM Administrator to pull (copy) information from an external Identity Management **(**IDM) system (e.g. LDAP, Active Directory) to complete the user information stored in USM.

With an IDM, some user information (depending on how USM is interfaced with: cfr the USM Admin guide & USM IDM setup guide) will be copied into USM. When imported, such information should not be updated anymore because the official source is considered to be the IDM. (a next version of USM will prevent that action)

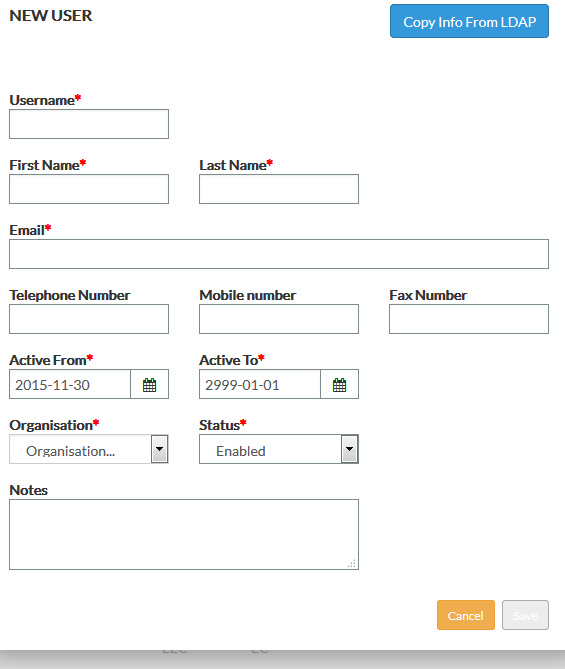
The procedure is the following: the username must be inserted first. Then the option **'Copy Info From LDAP**' is triggered. User information from the LDAP is copied in USM if the username entered in the web screen matches an existing username in the IDM. If not, an error message 'User not found' is displayed.



Some other user information needs to be filled in before finally saving the data (cfr next point).

1. Using USM as source for all user data

The following data should be provided (mandatory fields are marked by a red '\*'):

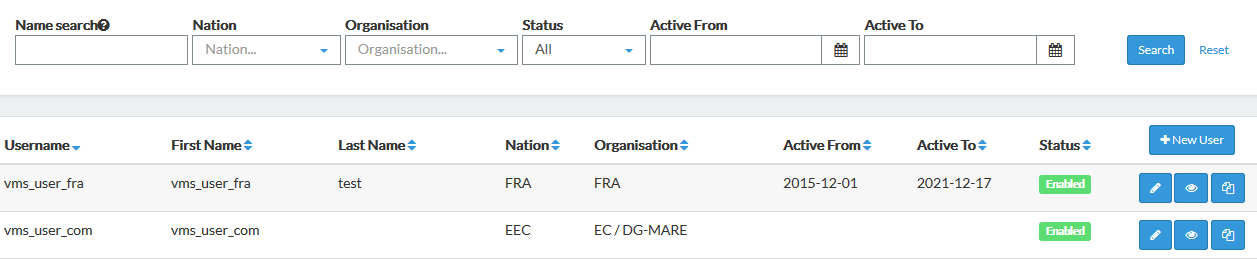


* Username: it must be unique. If not , an error 'User already exists' is generated when saving data;
* First name
* Last name
* Email: it must contain a '@' to be valid;
* Telephone number
* Mobile number
* Fax number
* Active from
* Active to
* Organisation: only the 'enable' organisation are proposed (cfr Organisation management)
* Status:
  + Enabled: the user is active. It is the default value.
  + Disabled: the user is no more active. He may not log-in in any UVMS module.
  + Locked: the user may not log-in in any UVMS module. This status is mainly managed by the system when the user access should be (temporarily) deactivated due to a violation of a security policy (wrong password entered multiple times …) cfr Policies management.
* A note

When data is saved, the user has still no password and no access right. Please see the corresponding entries in this document to complete the process.

## How to give access rights to a User

The first action is to find back the user: cfr How to find back User information.



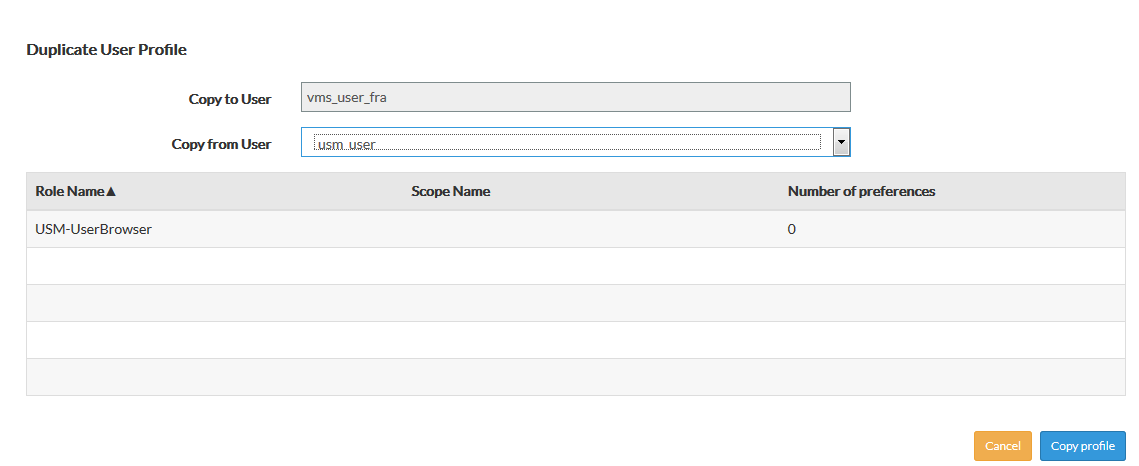
Then, two options are possible:

1. To clone an existing user profile

In such a case, all access rights (more precisely the contexts) from another user will be copied to this user. To do so, the action is triggered by clicking on the following icon at the level of the user entry in the user panel:

A pop-up is displayed where the administrator can pick-up a reference user from whom the contexts (role/scope/preferences) must be copied to the user. All the contexts of the reference user are displayed for information. When the '**Copy profile**' option is triggered, a message indicates that any previous access rights of the user receiving the new profile will be deleted.

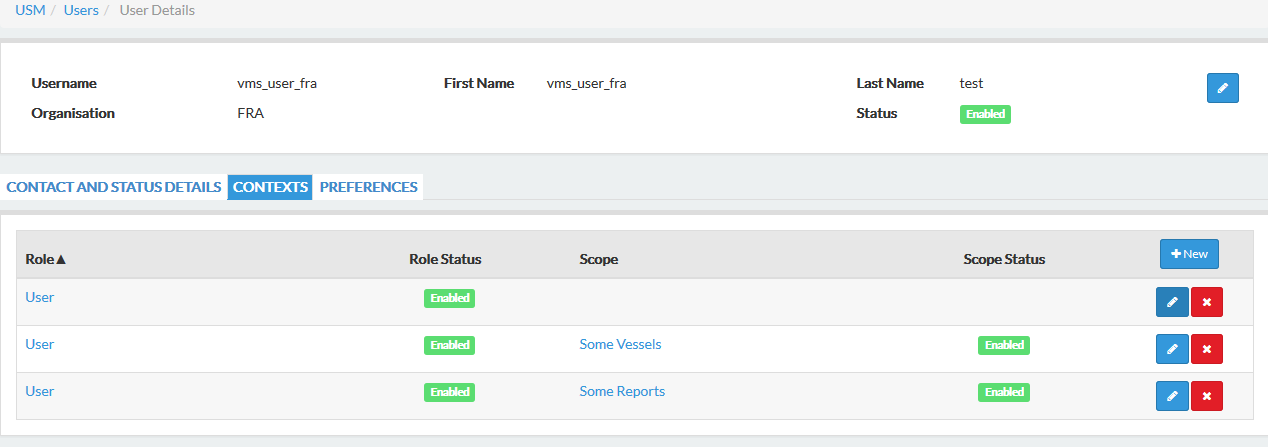
The new profile of the user can be later extended (cfr next option).



1. To create or change contexts

To do so, the action is triggered by clicking on the following icon at the level of the user entry in the user panel:

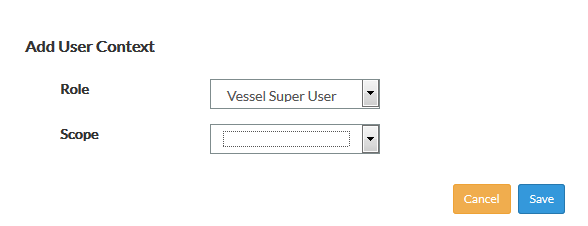
In the 'Contexts' tab, the permissions (if any) of the user are available:





A new context can be added to the profile of the user with the '**New**' option:

A pop-up is displayed where the administrator must choose a role and optionally a scope:



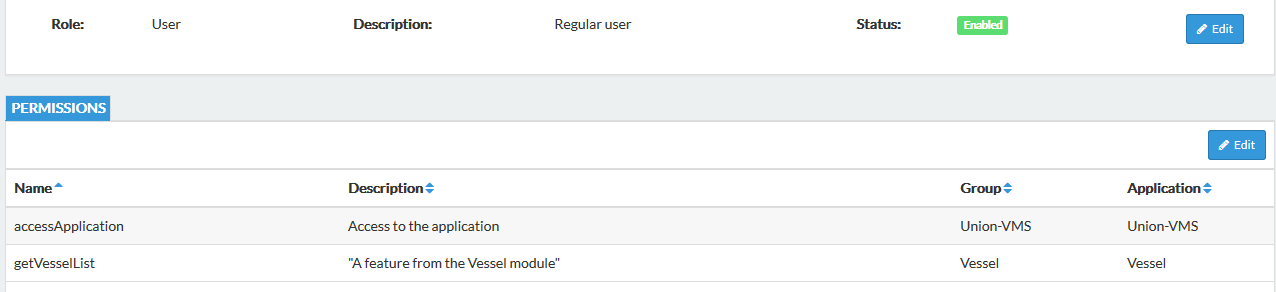
The system verifies if the context (role/scope) does not exist already for the user. If not, the profile of the user is modified. If the user is connected in U-VMS when the operation is performed, the impacts (new permissions …) will only take place at the next user session.

The same screen is proposed when updating a context with the icon:



Deletion of a context is also possible with the icon:

By clicking on the existing roles or scopes, the corresponding screens to view the content ( permissions or datasets) are displayed with options to manage them. It should be noted that in such case, the modifications done on a role or a scope affect all users having the element in their context(s) (Cfr How to manage Roles and How to manage Scopes).



## How to manage Organisations and related information

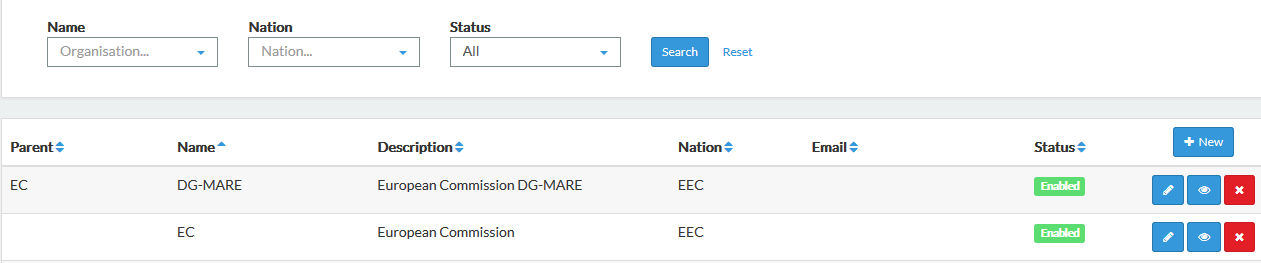
The option 'Organisations' in the main menu is the entry point:



An organisation may provide technical information for one or multiple endpoints. Each endpoint may have one or more communication channels and a list of contact people.

### Organisation

The web screen provides a set of filters to find back an existing organisation:



* Name search: a selection of one entry in the list of organisations created in the system;
* nation: a selection of one entry in the list of countries proposed by the system;
* Status: a selection of one entry in the list of organisation statuses defined in the system;

The result of the search is displayed below the set of filters.

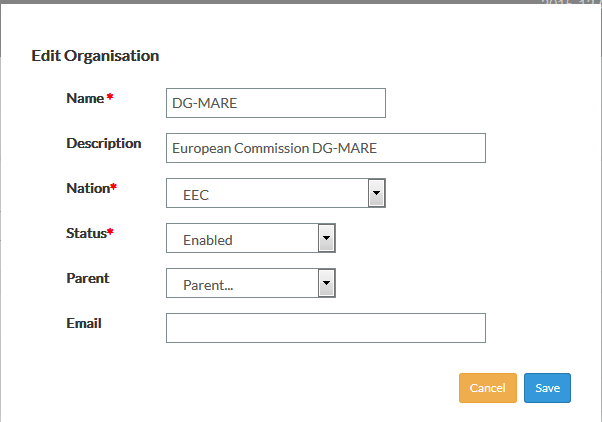
When there is no data corresponding to the search criteria, the message 'No result found.' is displayed.

If the search is successful, the list of organisations matching the criteria is displayed. For each entry in that list, the following actions are available:

The creation of an organisation is done by selection the '**New**' option:

The edition of an organisation is done with the icon closed to the organisation entry in the organisation panel :

For both options, the following pop-up is presented: (mandatory fields marked with a red '\*'):



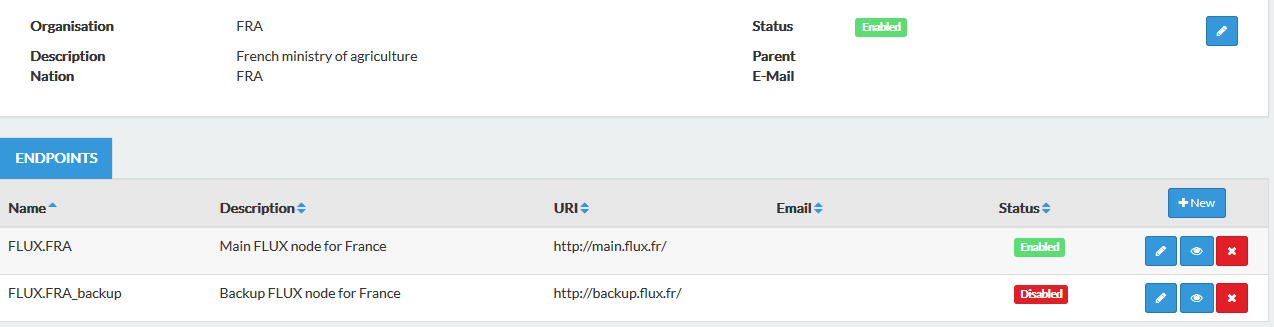
* Name
* Description
* Nation: to select one entry in the predefined list of countries
* Status:
  + Enabled: by default.
  + Disabled: with that status, the organisation cannot be selected anymore when creating/updating user information.
* Parent: a hierarchy of organisations can be registered. It can be used for defining a service under a certain department or a local organisation linked to an international headquarter.
* Email

The deletion of an organisation is done by the icon closed to the organisation entry in the organisation panel:

A deletion is only possible if there is no user belonging to that organisation. In case of deletion, all endpoints and communication channels associated with the organisation are deleted as well.

### Endpoint

The additional information attached to an organisation is visible when selecting the icon closed to the organisation entry in the organisation panel:

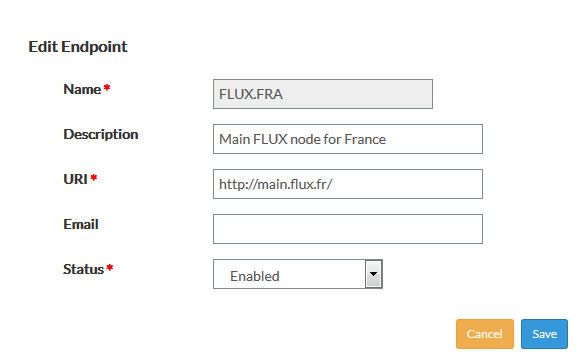




The creation of an endpoint of an organisation is done by selection the '**New**' option:

The edition of an endpoint is done with the icon closed to the endpoint entry in the endpoint panel:

For both options, the following pop-up is presented: (mandatory fields marked with a red '\*'):



* Name
* Description
* URI: Uniform Resource Identifier of the endpoint
* Email
* Status:
  + Enabled: by default.
  + Disabled: means that the endpoint cannot be used for electronic exchanges.

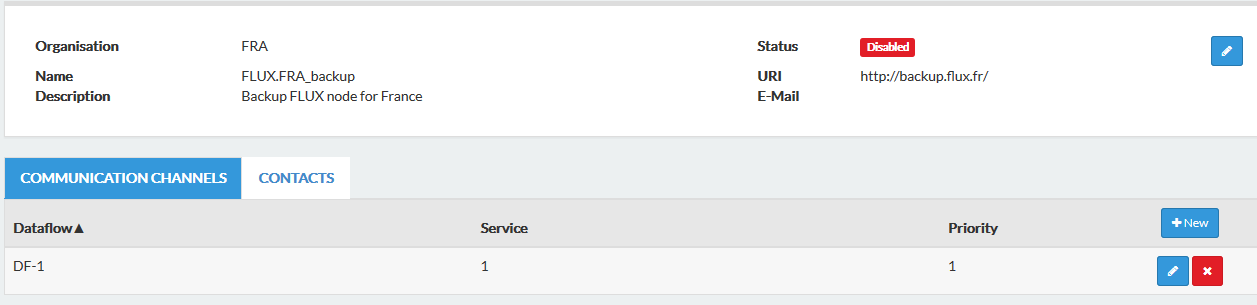


The deletion of an endpoint is done by the icon closed to the endpoint entry in the endpoint panel:

In case of deletion, all communication channels associated with the endpoint are deleted as well.

### Communication Channel

The additional information attached to an endpoint is visible when selecting the icon closed to the endpoint entry in the endpoint panel:

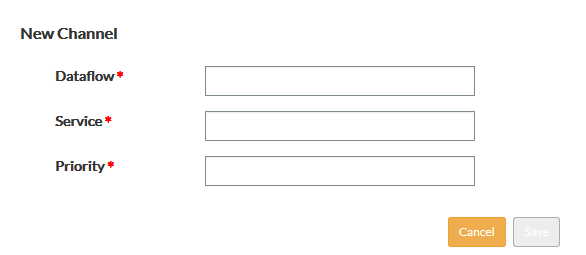




The creation of a communication channel of an endpoint is done by selection the '**New**' option:

The edition of communication channel is done with the icon closed to the entry in the communication channel panel:

For both options, the following pop-up is presented: (mandatory fields marked with a red '\*'):



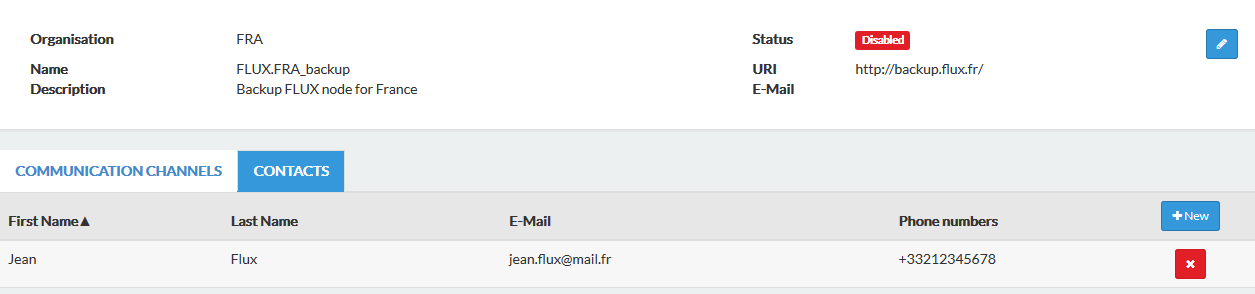
* Dataflow : name of the datawflow
* Service: service transiting through the dataflow
* Priority : value depending on the organisation policy for managing channels

The deletion of an organisation is done by the icon closed to the organisation entry in the organisation panel:

### Endpoint contacts

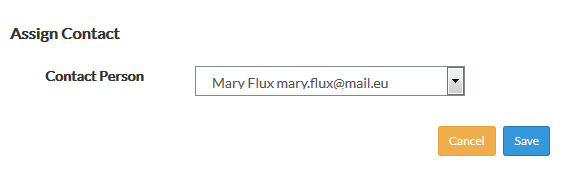
The web screen showing the detailed information of an endpoint is made of two tabs. The second tab is about contacts.

The contact panel shows (if any) all the contact points of an endpoint:



A new contact can be associated with an endpoint by selecting the '**New**' option:

A pop-up shows the list of all existing users with their first/last names and the email address. A selection of an entry creates a contact point:



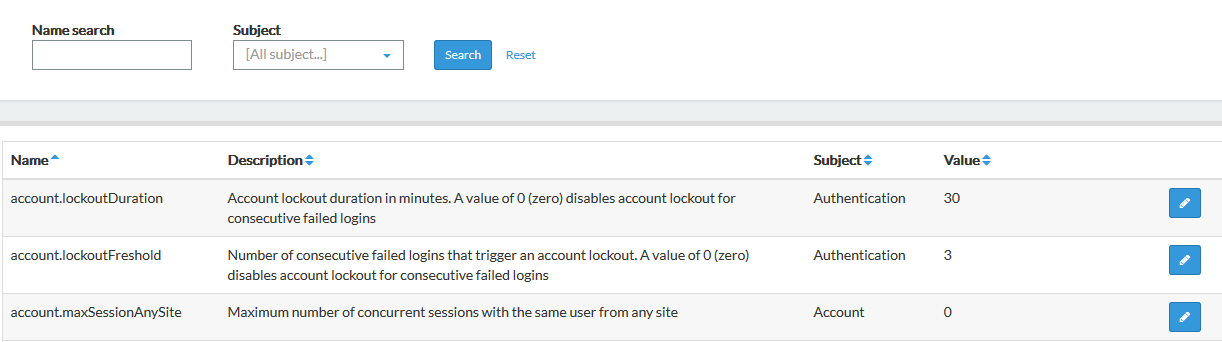
A contact point can be deleted by selecting the icon closed to the contact entry in the contact panel: In such case, only the reference to the user (contact role) is deleted, not the user itself.

## How to manage Policies

Policies are accessible through the 'Policies' option from the main menu:



The web screen provides a set of filters to find back the information:



* Name search: A set of characters can be provided. The search is performed on the policy names. The position in the data of the characters entered for the search is not important;
* Subject: a selection of an entry in a list of predefined subjects used to classify the policies;

The result of the search is displayed below the set of filters.

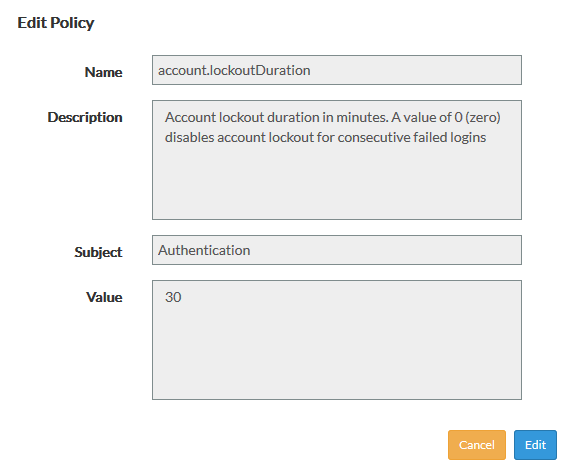
When there is no data corresponding to the search criteria, the message 'No results found.' is displayed.

If the search is successful, the list of policies matching the criteria is displayed. For each policy, the following data is available:

* Name
* Description
* Subject: used to classify the policy
* Value: cfr USM Admin guide

A policy can be modified by clicking on the icon closed to the entry in the policies panel.

A pop-up is displayed where the description and the value can be modified. A definition of each policy and information about possible values are given in the USM Admin guide:

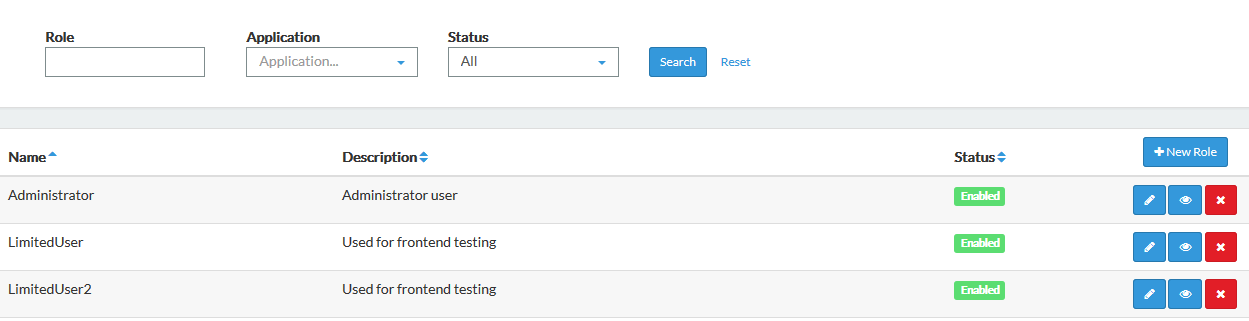


## How to manage Roles

Information about roles is accessible through the 'Roles' option from the main menu:



The web screen provides a set of filters to find back the roles:



* Role search: A set of characters can be provided. The search is performed on the role name. The position of the characters in the name is not important;
* Application: selection of an entry in the list of applications linked with USM;
* Status:
  + Enabled: valid/active role with a set of permissions
  + Disabled: inactive role

The result of the search is displayed below the set of filters.

When there is no data corresponding to the search criteria, the message 'No result found.' is displayed.

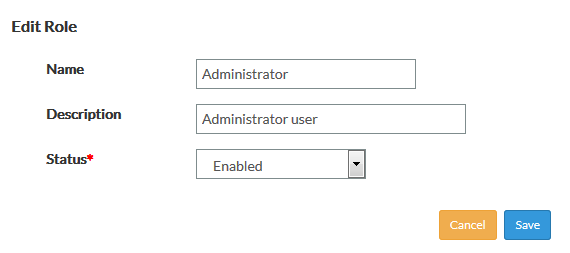
If the search is successful, the list of roles matching the criteria is displayed with the following information:

* Name:
* Description
* Status: enabled/disabled

The creation of a role is done by selection the '**New**' option:

The edition of a scope is done with the icon closed to the scope entry in the scope panel :

For both options, the following pop-up is presented: (mandatory fields marked with a red '\*'):



* Name: it must be unique.
* Description
* Status:
  + Enabled: by default.
  + Disabled: with that status, the role is not active (permissions not set).

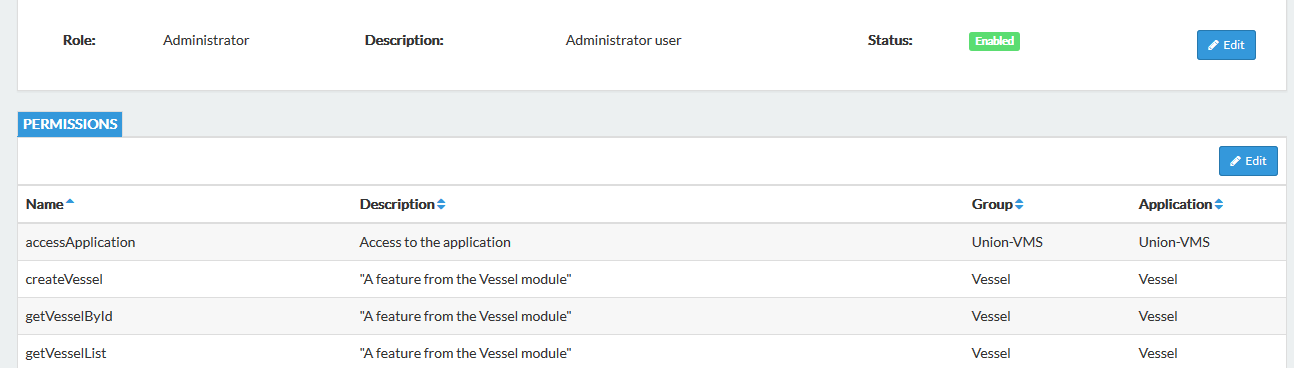


The deletion of a scope is done by the icon closed to the scope entry in the scope panel:

When deleting a role, the system raises a warning if the role is associated with a user context. The message mentions the number of users but it is not a blocking issue. It is possible to go forward. If so, there is a risk of having users without any access rights if they had only that role.

### Features/Permissions

The additional information attached to a role is visible when selecting the icon closed to the scope entry in the scope panel:



For each permission in the role, the following information is available:

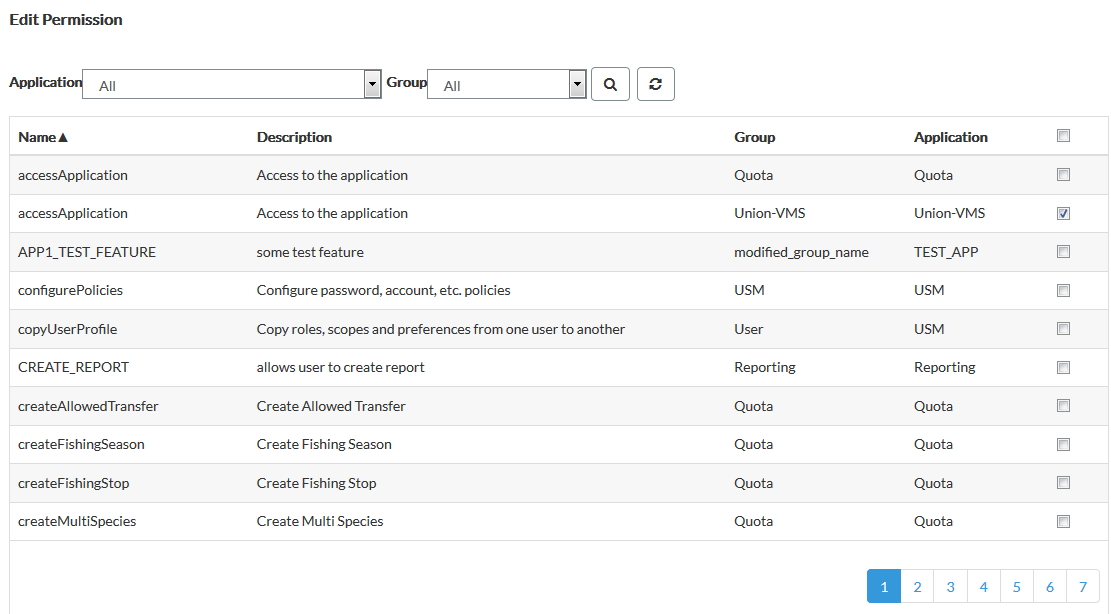
* Name of the feature
* Description of the feature
* Group: used to classify filters together when they are applied on a same business object
* Application: application exposing and using the feature

It should be noted that a role can be based on permissions coming from multiple applications.

### Modify a role definition

In the screen for consulting the datasets of a scope (cfr previous point), the following icon is available to modify the list:

A screen displays a set of filters to search for features proposed by all applications:



* Application: one entry in the list of applications linked to USM and providing permissions;
* Group: one entry in the list of groups defined in applications. A group is used to gather a list of permissions acting basically on a same functional object inside an application (ex: consulting, editing, deleting a vessel …)

The result of the search is displayed below the set of filters. The list of permissions is displayed with at the end of each entry of the list a check box which is ticked if the permission is already in the role being modified. The management of permissions of the role is done by selecting or deselecting the check boxes for permissions.

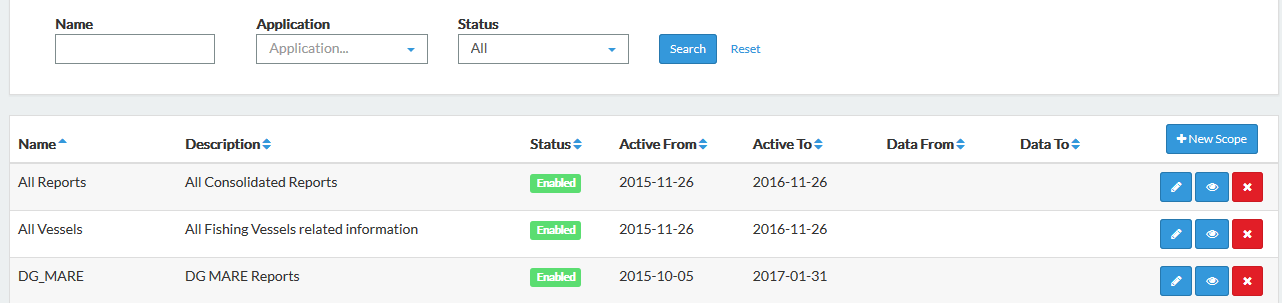
This process shows that a role can be based on permissions coming from multiple applications.

## How to manage Scopes

Information about scopes is accessible through the 'Scopes' option from the main menu:



The web screen provides a set of filters to find back the scopes:



* Name: A set of characters can be provided. The search is performed on the scope name. The position of the characters in the name is not important;
* Application: selection of an entry in the list of applications linked with USM;
* Status:
  + Enabled: valid/active scope with a set of filters
  + Disabled: inactive scope

The result of the search is displayed below the set of filters.

When there is no data corresponding to the search criteria, the message 'No result found.' is displayed.

If the search is successful, the list of scopes matching the criteria is displayed with the following information:

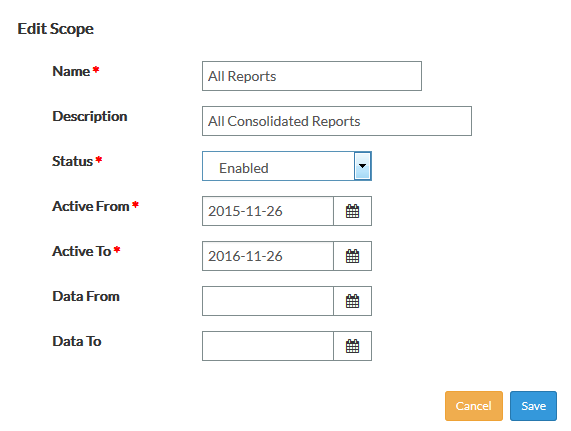
* Name
* Description
* Status
* Active from
* Active to
* Data From: when specified, date from which any data filtered by the scope will be selected
* Data To: when specified, date until which any data filtered by the scope will be selected

The data from/to is a general filter of the scope.

The creation of a scope is done by selection the '**New**' option:

The edition of a scope is done with the icon closed to the scope entry in the scope panel :

For both options, the following pop-up is presented: (mandatory fields marked with a red '\*'):



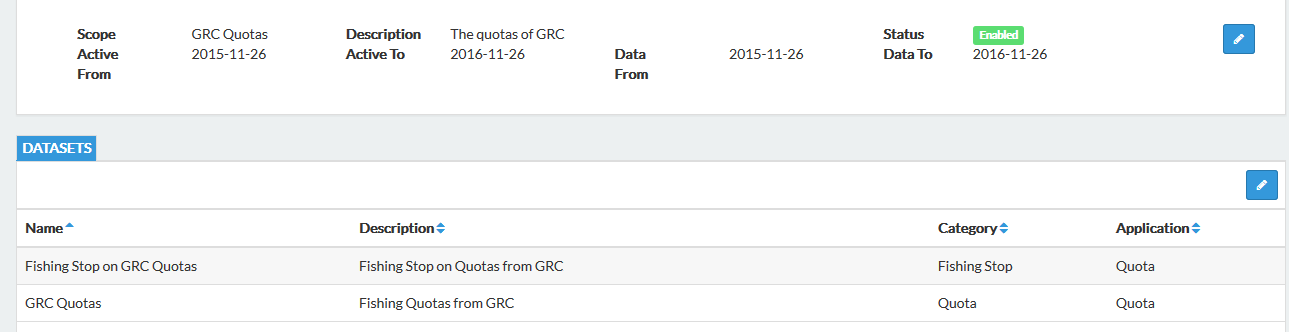
* Name: it must be unique.
* Description
* Status:
  + Enabled: by default.
  + Disabled: with that status, the scope is not active (filters not applied).
* Active from
* Active to
* Data From: when specified, date from which any data filtered by the scope will be selected
* Data To: when specified, date until which any data filtered by the scope will be selected



The deletion of a scope is done by the icon closed to the scope entry in the scope panel:

### Datasets

The additional information attached to a scope is visible when selecting the icon closed to the scope entry in the scope panel:



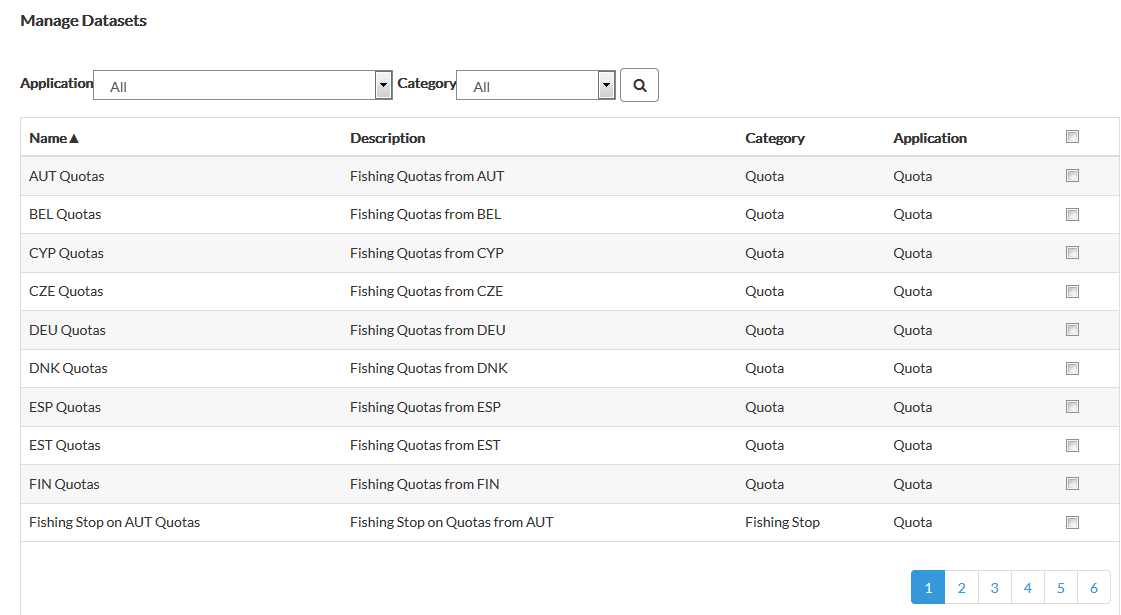
For each dataset in the scope, the following information is available:

* Name
* Description
* Category: used to group filters together when they are applied on a same business object
* Application: application exposing and using the filter

### Modify a scope definition

In the screen for consulting the datasets of a scope (cfr previous point), the following icon is available to modify the list:

A screen displays a set of filters to search for datasets proposed by all applications:



* Application: one entry in the list of applications linked to USM and providing datasets;
* Category: one entry in the list of categories defined in applications. A category is used to gather a list of datasets acting basically on a same object inside an application.

The result of the search is displayed below the set of filters. The list of datasets is displayed with at the end of each entry of the list a check box which is ticked if the datasets is already in the scope being modified. The management of datasets of the scope is done by selecting or deselecting the check boxes for datasets.

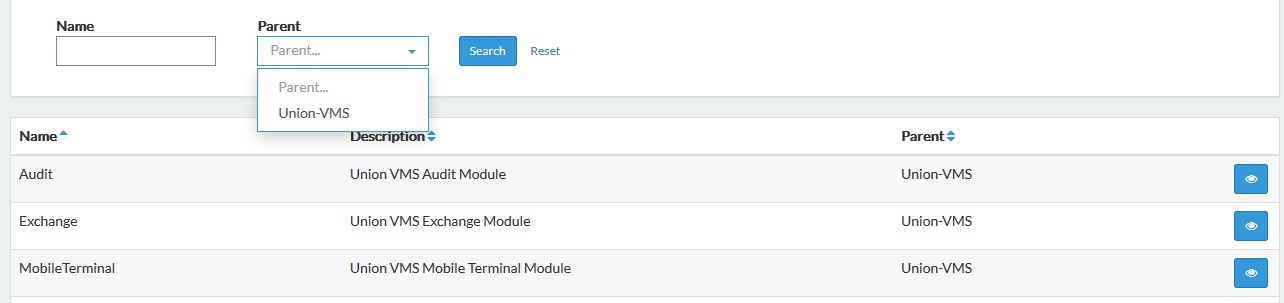
This process shows that a scope can be based on datasets coming from multiple applications.

## How to view Application information

Information about applications linked to USM is accessible through the 'Applications' option from the main menu:



The web screen provides a set of filters to find back the applications:



* Name search: A set of characters can be provided. The search is performed on the application name. The position of the characters in the name is not important;
* Parent: a hierarchy of applications can be registered in USM. For instance, USM module under U-VMS application. This filter is used to find the 'upper root' of applications;

The result of the search is displayed below the set of filters.

When there is no data corresponding to the search criteria, the message 'No result found.' is displayed.

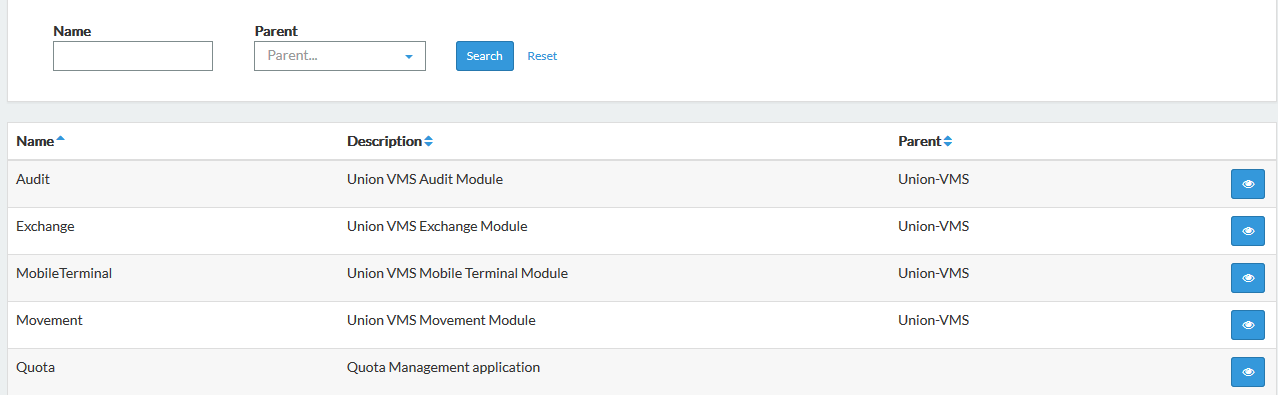
If the search is successful, the list of applications matching the criteria is displayed with the following information:

* Name
* Description
* Parent

## How to view data exposed by Applications

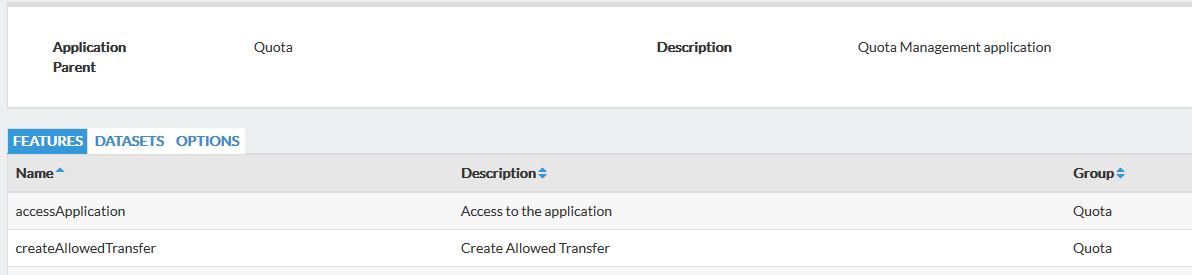
Information about applications linked to USM is accessible through the 'Applications' option from the main menu:



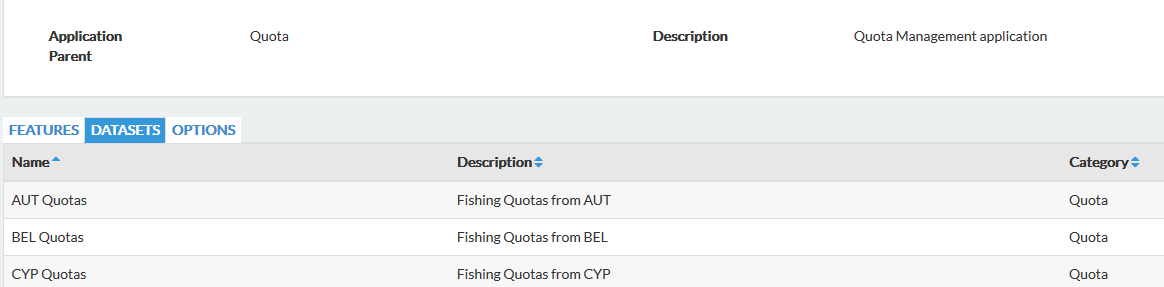


Data exposed by each application and registered in USM for defining roles and scopes, basis of the user contexts (access rights), are visible by selecting the icon closed to the entry in the organisation panel.

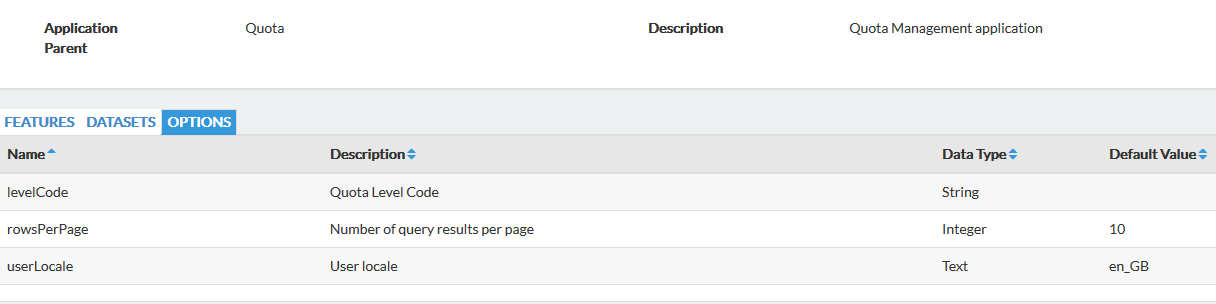
The web screen shows a tab by type of data exposed by an application:



* Features: functions of the application:
  + Name
  + Description
  + Group: used to classify the features



* Datasets
  + Name
  + Description
  + Category: used to classify the datasets



* Options:
  + Name
  + Description
  + Data type
  + Default value

## How to validate user changes

The system can be configured in such a way that any changes of personal data done by a user must be validated by a USM administrator before to be registered (cfr Policies).

If this setting is active, the option 'Changes' appears in the main menu:



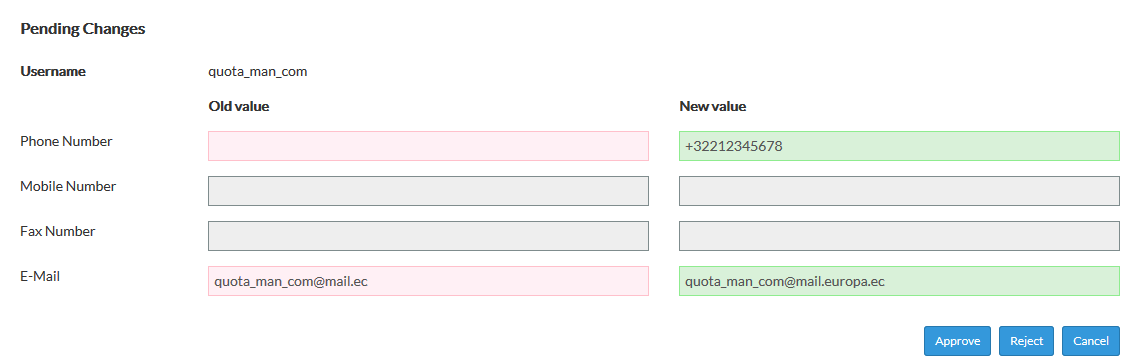
The list of following information is available when new changes to be validated are pending:



* Username: to identify the user
* Phone number: new value is any
* Mobile number: new value is any
* Fax number: new value is any
* Email: new value is any

The icon available in each entry of the list gives access to the validation screen.

The old and new values are displayed with options to reject, accept or cancel the operation:



If accepted, the user information is immediately updated in the system.

In this version of USM, the user is not notify of the decision of the administrator.