User Microservice

The user microservice provides all of the tools for managing users access to their accounts and the wider TMF suite of applications and modules.

{{TODO: Generalised description of the user microservice}}

# Data Fields

## user.user\_id

Unique identifier for the user record, the ***user\_id*** is given as a MariaDB UUID.

## user.given\_name

The given name for the user record. For european and anglo-american names this can be considered as the forename or first name for a user record. However, for the purposes of internationalisation “given” is used in place of “first” or “fore” in the field name labelling schema. The ***given\_name*** field can be hyphenated but must not contain any white space characters

## user.middle\_name\_list

Comma separated list of users' middle names. This field can be NULL. For entered values, the system must make the following validations;

* Single white space characters must be used to separate each name word (U+0020 or ASCII 032).
* When storing the user supplied middle name list in the ***middle\_name\_list*** field, all separating (white space) characters must be replaced with a comma between each list item.
* When rendering the list as a returned set of items, all comma list item separators must be replaced with a single white space character.

## user.family\_name

The family name for the user record, family name is also termed as being the surname or last name for european and anglo-american names. As with ***given\_name***, the ***family\_name*** field can be hyphenated and must also not contain any white space characters. The word “family” is used in place of surname or lastname for the purposes of internationalisation.

## user.login\_username

***“login\_username”*** is a unique automatically generated string value used to identify the user account in addition to the ***user\_id***. The uniqueness of the username is ensured by being machine generated as a conflation of the users actual name fields and by attachment of a numeric reference as either a prefix or suffix if required.

The value for this field is set at account registration time when the user record is created and is unable to be user edited at any point later for the lifetime of the account record.

## user.login\_email

The ***“login\_email”*** field contains the user email address used for account authentication. This field is user editable.

## user.login\_password

User account password hash.

## user.login\_remembered

The “login\_remembered” field contains a JSON record that stores a token, an expiry datetime with a reference to the device that logged in. A record is created for each connected device. The record can be used for a user's connection history and is able to be cleaned (history deletion) by the user.

## user.user\_username

User specified username for the account. This field value is defined by the user. Even whilst the string value is user definable it still has to be unique within the system.

## user.account\_username

Flag to select what is publically displayed as the user account name. It can be either a concatenation of ***given\_name***, ***middle\_name\_list*** and ***family\_name***, or, ***given\_name*** and ***family\_name***, or, ***given\_name***, or ***login\_username*** (default), or, ***user\_username***.

## user.login\_password\_reset\_key

An auto generated activation key used by the application for automated password recovery and used in conjunction with an email verification.

## user.gmt\_timezone\_offset

Integer timezone offset code with reference to GMT having -12 to +12 where 0 is GMT:London.

## user.country\_code

Country code for user accounts set at the time of account registration (creation), can be updated.

## user.verified\_email

Flag to ensure the email account being used is real, available (active/live), and confirmed.

## user.registered\_at

Timestamp of when the user account was created is stored in MariaDB DATETIME format. This is a non editable field.

## user.last\_accessed

Timestamp of when the user account was last accessed stored in MariaDB DATETIME format

## user.active

Flag showing if the user account is active or disabled. A disabled account is still accessible by a user but has no publicly viewable identifying information.

## user.deleted

Marks a user account as deleted. This requires that all identifying account data is deleted.

## user.spam

Boolean flag to mark an account as spam.

## user.tenant\_id

TODO: {LONGTEXT JSON record} Needs definition – Multi-tenancy

## user.federated\_id\_user\_information

TODO: {LONGTEXT JSON record} Needs definition - List of all linked provider objects which contain "providerId" and "federatedId".

## user.token\_id

TODO: {LONGTEXT JSON record} Needs definition - New Identity Platform ID token for user.

## user.token\_refresh

TODO: {LONGTEXT JSON record} Needs definition - An Identity Platform refresh token.

## user.token\_valid\_since

TODO: {LONGTEXT JSON record} Needs definition - The timestamp, in seconds, which marks a boundary, before which Identity Platform ID tokens are considered revoked.

## user.token\_expires\_in

TODO: {LONGTEXT JSON record} Needs definition - The number of seconds in which the ID token expires.

## user.developer\_auth

TODO: {LONGTEXT JSON record} Needs definition - Whether the account is authenticated by the developer.

# Actions

Create new account

Login to existing account



Log out of an account

Reset existing account password

Forgotten email account recovery

Forgotten password account recovery

Forgotten username account recovery

Remember me

Update existing account details

Delete and account

# Metadata

# Processes

Data validation

Account activation

Password Reset

Details Update

Remember me

Issue recovery codes

## Recovery Modes

Forgotten email

Forgotten username

Forgotten password

Broken email (email no longer valid for any reason)

Use of recovery codes

# Microservice Endpoints

Get a single user profile

Get a set of users by associated group

Get all users

{{needs pagination for bulk reporting actions}}