User Manager

Manual for the User Manager Option v.3.0.6

Table of Contents

1 What is the User Manager?

Several different functions/profiles (roles) generally exist in a company. An accountant, for instance, will not perform the same operations as a payment encoder or a technical integrator. Logically, you will want to grant only the necessary access rights for each individual who will use your account, and on top of that, track which user has performed which operations.

The User Manager option allows you to assign a specific profile to each user to give him the access rights he needs to fulfil his function. The User Manager is an additional service available for all products.

1.1 Benefits

The User Manager allows you to:

- Configure several users under one account
- Manage the profile and access rights of each user
- Avoid critical mistakes by payment encoders
- Trace the actions of each user (e.g. number of transactions per day)
- Limit users to see only their transactions
- Easily manage access rights for temporary staff.

1.2 Access

You can access the User Manager via the “Users” link in your account menu.

1.3 Number of users

The number of available users depends on the exact User Manager option you select. User Managers are available for up to 5, 10, 20, 50, 100 or 200 users.

2 User Profiles and User Types

The main user profiles supported by the User Manager are: Viewer, Encoder, Super-encoder, Super-encoder without refund, Admin without user manager, and Admin.

Apart from that, there are two types of users: back-office users (ADM) and application users (API).

2.1 User profiles

2.1.1 Admin

An Admin user has full access rights.

Each time an account is created, a default user is automatically generated as well (the UserID of this default user is identical to the PSPID); this default user has an Admin profile. You can of course also create other Admin users.

An Admin user is the only user who has the permissions to change the account configuration.

2.1.2 Admin without user management

The Admin without user manager has the same access rights as the Admin, except he does not have access to the User Manager option.

2.1.3 Encoder

An Encoder can submit a new payment via the “New transaction” link in the account menu or via DirectLink.

2.1.4 Fraud analyst

A Fraud analyst can edit blacklists/whitelists, review the scoring of transactions, and dispute transactions.

> Note
>
> For this user profile to function properly, you have to tick "Fraud detection" in the user's access rights.

Click here for an overview of the different user permissions per user profile.

2.1.5 Fraud manager

A Fraud manager can edit all relevant fraud detection configuration pages, edit blacklists/whitelists, review and dispute transactions, etc.

> Note
>
> For this user profile to function properly, you have to tick "Fraud detection" in the user's access rights.

Click here for an overview of the different user permissions per user profile.

2.1.6 Fraud viewer

A Fraud viewer can view various Fraud detection configuration pages, but not edit anything.

Note

For this user profile to function properly, you have to tick "Fraud detection" in the user's access rights.

Click here for an overview of the different user permissions per user profile.

2.1.7 Super-encoder

A Super-encoder can not only submit new transactions, but also perform maintenance operations on existing transactions. He can also upload payment files and download transaction reports.

2.1.8 Super-encoder without refund

The Super-encoder without refund has the same access rights as the Super-encoder, except he is not able to perform refunds or cancel authorisations. This profile allows you to grant permission to perform data captures only, but not to perform refunds or delete payments.

2.1.9 Viewer

The viewer profile is an ideal profile for an accountant. A Viewer can display or query transaction statuses and reports, but cannot change or submit anything. This is a read-only access profile.

2.2 User Types

To be PCI compliant, our user management has to distinguish clearly between users (logins) who access the back-office module (website login) and users who access our platform automatically via an application.

We therefore have 2 types of users: the back-office user and the application user.

2.2.1 Back-office user (ADM user)

A back-office user (ADM user) is a user who has access to the ePDQ back office via the website.

A back-office user has to change his password every 90 days. He can do so via the “Password” link in the account menu.

2.2.2 Applicative user (API user)

An applicative user (API user) is a user specifically designed to be used by an application to make automatic requests to the payment platform (automatic file upload/download, direct payment requests, etc.).

Even though for an API user the various user profiles are available, we strongly recommend you to configure it with the "Admin" profile. This is unless eg. you wish to limit the rights for maintenance of transactions (refunds, cancellations etc.), in which case you can change the user profile to "Encoder". If you are not sure we recommend you to choose the "Admin" profile either way, otherwise please refer to the User profiles chapter for more information.

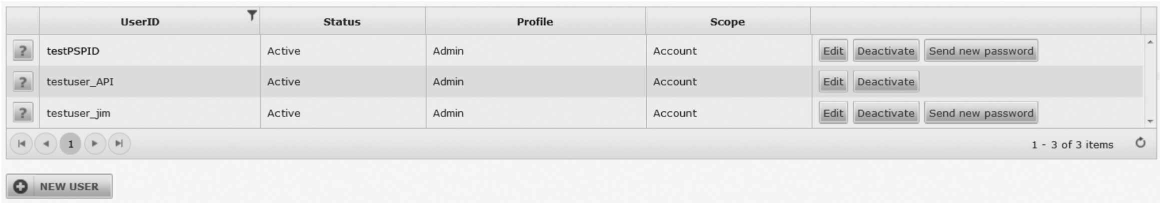
The password of an API user does not have to be changed on a regular basis. This is more convenient when the password has to be hard coded into your application. However, we recommend you change the password from time to time. To change an API user's password, select the “Users” link in your account menu, and use the "Change password" button for the applicable API user. You will be redirected to a page where you can change the password. Also, at the creation of a new API user you will have to configure the password on this page.

For security reasons, an API user is not granted access to the account administration module, i.e.

the user cannot log into the back office.

3 User Management

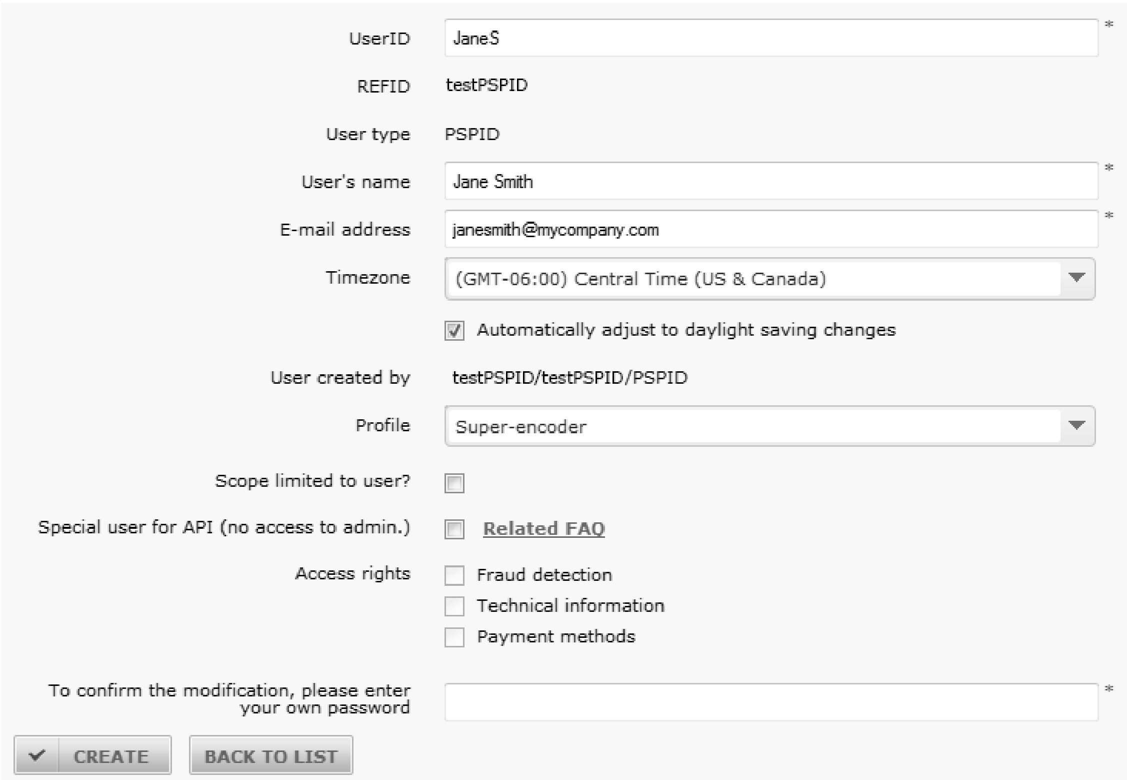
On the User Management page, you can create and new users, manage users' passwords, deactivate users that are no longer active in the company and edit user details.



The permitted number of users is displayed in the User Management menu page. Once the permitted number of users has been reached, the "New User" button will be disabled.

3.1 Create a new user

You can create a new user by clicking the "New User" button on the User Management page. The form that is displayed must be completed in order to submit a new user.



3.1.1 Pre-initialised details

The form contains three pre-initialised data fields:

- REFID: name of entity the UserID is linked to (e.g. for a merchant: his PSPID)
- User Type: type of entity the UserID is linked to (e.g. for a merchant: "PSPID")
- User created by: the UserID of the user creating this new user / his user type / his REFID.

3.1.2 User details

The user details that need to be completed are:

- USERID: the UserID (username) for the new user (min. 3 and max. 20 characters long, no spaces or special characters!)
- User's name: the new user's full name
- E-mail address: the new user's e-mail address (if in future a new password is triggered for this user, it will be sent to this e-mail address).

3.1.3 Time zone

With the creation of a user, automatically the time zone of the PSPID is applied. Afterwards, the user can configure the time zone of his choice.

The time zone that the user chooses is applicable for all the back-office pages where the time is relevant. This way the user can also also view and download transactions and files/reports in his own or preferred time zone.

Moreover the time can automatically be adjusted to daylight saving changes, by selecting the same option.

3.1.4 Profile

See User profiles

3.1.5 Scope limited to user

These options can only be configured for the following profiles: Encoder, Super-encoder and Super-encoder without refund.

If this box is enabled, Encoders will only be able to see and access transactions they have entered/initiated themselves. They will not be able to see/access any transactions entered by other users.

If this box is enabled, the Super-encoders will only be able to see, access and perform maintenance operations on transactions they have entered/initiated themselves (except for maintenance operations that are submitted via file upload). They will not be able to see/access/perform maintenance operations on any transactions that other users have entered.

3.1.6 Special user for API

If you want to create an application user, (cf. Applicative user (API user)) you have to enable this box. The user you create will only be permitted application access and not back-office access via the website.

3.1.7 Access rights

These options can only be configured for the following profiles: Viewer, Admin, Admin without user management.

The Viewer, Admin or Admin without user management will only have access to Reconciliation, Fraud detection, Payment methods and Technical information if you enable the respective boxes.

You can submit the user settings you entered by clicking the "Create" button. If any of the information has been incorrectly filled out, an error message will be displayed. Instead of the newly created user being sent his first password by e-mail, a screen will be displayed showing the password our system created for him. This password can then be communicated to the new user.

3.2 Password management

You can send a new password to a specific user by clicking the “Send new password” button. The new password will be sent to the e-mail address configured in the user’s details.

You cannot assign a new password to the user you logged in with yourself, or to the account’s default user. If the account’s default user has lost his password, he can only request a new password via the “Lost your password?” link on the login page. On the next page, he should complete the PSPID and click the “Submit” button. An e-mail containing a new password will be sent to the account's administrative e-mail address.

For API users there is no “Send new password” button. To change an API user's password, you have to use the "Change password" button. You will be redirected to a page where you can change the password manually.

3.3 Deactivate users

You can set a user to inactive by clicking the “Deactivate” button next to the user. When a user is inactive he is no longer allowed to log into the account and is no longer taken into account for the permitted number of users.

To display a full list of users (both active and inactive), you can click the “Show inactive users” button.

To be PCI compliant and for security reasons, you/we are not allowed to delete users.

3.4 Edit user details

To change a specific user’s details, you can click the “Edit” button next to that user. In the case of the default account user, only the name and e-mail address can be changed.

4 User Tracking for Transactions

The payment details of a transaction include an “Encoded by” field. This field contains the UserID/ PSPID/User type of the user who encoded the transaction. (This field is not visible for users who have been configured with a ‘scope limited to user’ in their user details.)

To display all the transactions encoded by a specific user, select the user from the 'Encoded by' drop-down list in the advanced selection criteria for “Financial history” and “View transactions”.

5 Appendix: User Permissions Overview

R = read (rights to view) W = write (rights to change/submit) **bold** = has to be configured in the user details						
	Viewer	Encoder	Super-encoder	Super-encoder without refund	Admin	Admin without user manager
Account Contact info languages/ URL/currencies	R	R	R	R	R W	R W
Account Subscription/option					R W	R W
Payment methods	R				R W	R W
Users					R W	
Support	R W	R W	R W	R W	R W	R W
Technical information	R				R W	R W
Error logs	R	R	R	R	R	R
Fraud Detection Module	R				R W	R W
Financial history	R	R	R W	R W	R W	R W
New transaction		R W	R W	R W	R W	R W
View transactions	R	R	R W	R W	R W	R W
New file			R W	R W	R W	R W
View files			R W	R W	R W	R W
Electronic reporting	R W	R W	R W	R W	R W	R W
Alias Manager	R	R	R	R	R W	R W

5.1 Fraud detection profiles

Note

For these user profiles to function properly, you have to tick "Fraud detection" in the user's access rights.

R = read (rights to view) W = write (rights to change/submit)			
	Fraud	Fraud	Fraud manager

R = read (rights to view) W = write (rights to change/submit)			
	viewer	analyst	
Fraud detection page	R	R	R W
Fraud detection page: FDMA configuration & risk lists	R	R	R W
Fraud detection page: 3-D Secure configuration	R	R	R W
Fraud detection page: Blacklists/Whitelists	R	R W	R W
Scoring details page (R only)	R	R	R
Scoring details page: fill dispute + Blacklists/Whitelists (RW only)	-	R W	R W
Score details page: review transactions (RW only)	-	R W	R W