Users & permissions

Read more on user roles and the functions available to them through the API.

New user accounts

Once your environment has been delivered it will be configured with an administrator who can assign new users their user accounts.

If you are the administrator, a link to reset the password will be sent to your email address. After setting your password, you can add user accounts to your organisation.

User accounts are present within the scope of an organisation. Depending on the organisation's hierarchy tree, a user can only see data present within the organisation their account resides in, and in that organisation's subsidiaries (i.e. "child organisations").

User roles and permissions

A user can be assigned one or more roles, which dictates the privileges available to that user in the UI, as well as the API privileges of any API keys created by that user. A user's roles may be assigned or revoked by a user within the same organisation who has an administrator role. The scope is limited according to the organisation that the user is assigned to, and its place in the organisation hierarchy. Note that user accounts are limited to one organisation, and have at least viewing permissions to all entities that are part of the child organisations.

Combining several roles for one user may be desirable to give a user the exact combination of permissions necessary to fulfill their role.

Provider roles

Provider roles are used to set up the most important parts of the environment that allow processing payments. This includes setting up accounts and processors.

- ProviderAdmin - This role gives the user permissions at the highest level, allowing them to view and administer nearly all aspects of the environment. This includes creating accounts and processors, and linking them.
- ProviderUser - This role has a top level view, but not the administrative rights as the ProviderAdmin role.

Merchant roles

Merchant roles are there to perform business as usual activities, such as administering users, creating and manipulating transactions - (e.g. refunds), and using rulesets to monitor and block transactions.

- MerchantAdmin - An administrative role that allows creating users within the same organisation, along with creating validation rulesets and tags.
- MerchantSupervisor - This is the only role that allows creating and manipulating transactions. This includes performing refunds, updating chargebacks, and performing credit funds transfers.
- MerchantUser - This role can be granted to users assigned to a merchant organisation, and has mostly read only rights.

	ProviderAdmin	ProviderUser	MerchantAdmin	MerchantSupervi	MerchantCashier	MerchantUser
Accounts	CRUD	R	R	R	R	R
Analytics	-	R	-	R	-	R
API Keys	-	-	-	CRUD	CRUD	-
Authenticators	CRUD	R	-	-	-	-

	ProviderAdmin	ProviderUser	MerchantAdmin	MerchantSupervi	MerchantCashier	MerchantUser
Bank account tokens	-	R	-	RU	RU	R
Chargebacks	R	R	-	CRU	R	R
Card tokens	-	R	-	RU	RU	R
Checkouts	R	R	-	CR	CR	R
CheckoutTemplates	CRU	R	CRUD	CR	R	R
Customers	R	R	-	-	CRU	R
Invoices	R	R	-	R	R	R
Logevents	R	-	R	-	-	-
Organisations	CRU	R	R	R	R	R
Processors	CRUD	-	-	-	-	-
Refunds	R	R	-	CRU	CRU	R
Tags	R	R	CRU	R	R	R
Transactions	R	R	-	CRU	CRU	R
ThreedAuthentications	-	R	-	R	-	R
Users	CRUD	RU	CRU	RU	RU	RU
UserAgents	R	R	-	R	R	R
ValidationRulesets	CRUD	-	CRUD	-	-	-
ValidationRulesetmatches	R	R	-	R	R	R

Creating a User

The following sample POST call to `/v1/user/` can be used to create a user:

```
{
"disabled": true,
```

```
"email": "user@example.com",
"name": "Jane Citizen",
"organisation": "c5d9d4b856f0faccc8446100",
"roles": [MerchantAdmin, MerchantSupervisor]
}
```

- `disabled` - If set to true, it prevents the user from performing any actions on this user record. Defaults to 'false'
- `email` - The user's email address.
- `name` - The name of the user.
- `organisation` - Users and all other entities belong to an "organisation".
- `roles` - A list of roles attached to the user. Available roles and permissions can be found on this page.

A sample 200 response:

```
{
"dashboard_widgets": [ ],
"disabled": true,
"email": "user@example.com",
"name": "Jane Citizen",
"organisation": "c5d9d4b856f0faccc8446100",
"roles": [ ],
"password_change_history": [ ],
"login_history": [ ]
}
```

- `dashboard_widgets` - An array containing the user's configuration for the dashboard.
- `password_change_history` - List of (attempts of) password changes of the user.
- `login_history` - List of login attempts made by the user.

Edit user accounts

By clicking on your own name in the UI, you will be able to edit your own user account. You will be able to edit name, email address and your password. Admin users will be able to change their roles, and those of others.

You can update a user account by requesting POST on `/user/{id}` (where {id} if the id of the existing user account):

```
{
"disabled": true,
"email": "user@example.com",
"name": "Jane Citizen",
"organisation": "c5d9d4b856f0faccc8446100",
"roles": [MerchantAdmin, MerchantSupervisor]
}
```

- `disabled` - If set to true, it prevents the user from performing any actions on this user record. Defaults to 'false'
- `email` - The user's email address.
- `name` - The name of the user.
- `organisation` - Users and all other entities belong to an "organisation".
- `roles` - A list of roles attached to the user. Available roles and permissions on this page.

Audit trail

A login history of a given user can be viewed in their user account page. This will specify the date and time of the login, the IP address and location, and whether the login was successful.

If a session already exists for the given user, upon login they will be prompted with a notification on which IP address they are already logged in.

Requesting the login history results in a response including an array of login attempts:

```
{
...
"login_history": [
{
"ip_address": "::ffff:127.0.0.1",
"success": true,
"time": "2017-10-11T11:49:46.610Z",
"user_agent": "",
"_id": "59de055af3a295574e288fac"
} ]
...
}
```

Passwords and account recovery

Password expiration

Your password will expire every 4 months. Once your password has expired, you will be notified the next time you login. You cannot reuse the same password that previously expired. When requesting a new password, you will receive a link in the email attached to the account.

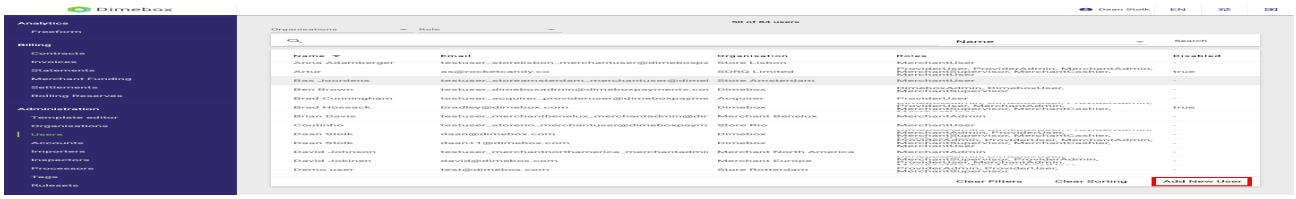
Disabled account

When your account has been disabled you will receive a notice in the UI or in an error message directly from the API. Please contact an administrator within or above your organisation to reenable your account. Disabled accounts also block the API-key. Take into account that a blocked API-key will also block transactions.

UI Guide

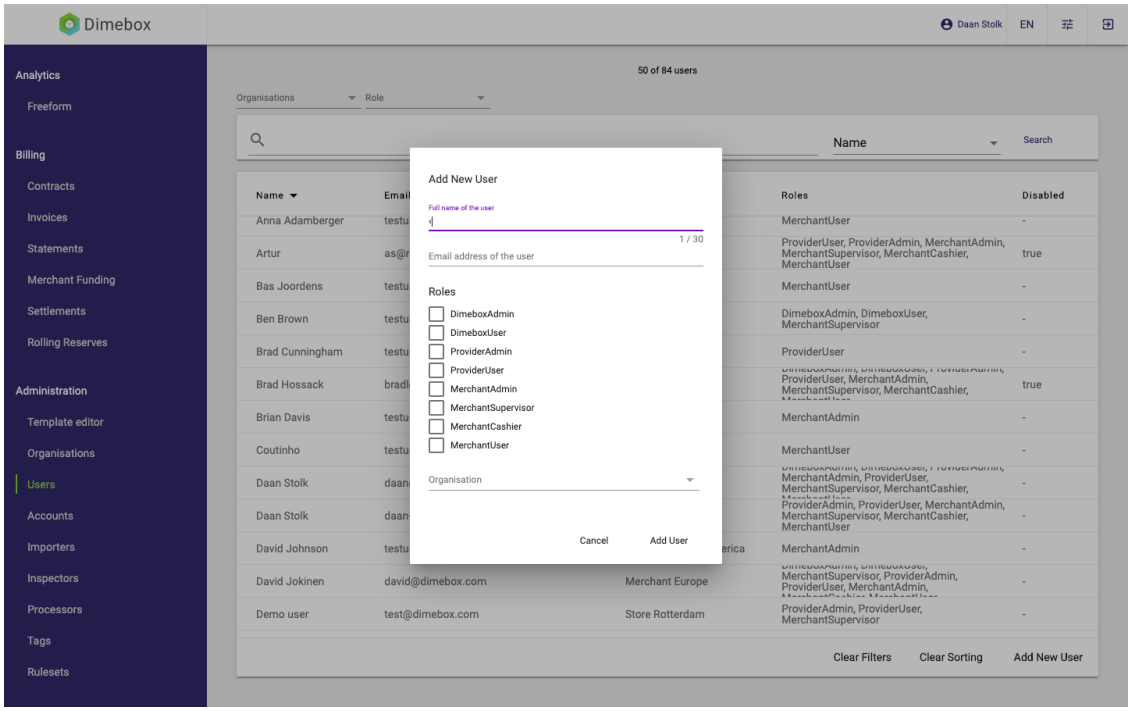
The following page describes how to create and edit a user. In order to create, edit or view a processor you will need the ProviderAdmin role.

1. Navigate to the Users tab. Click 'Add New User'

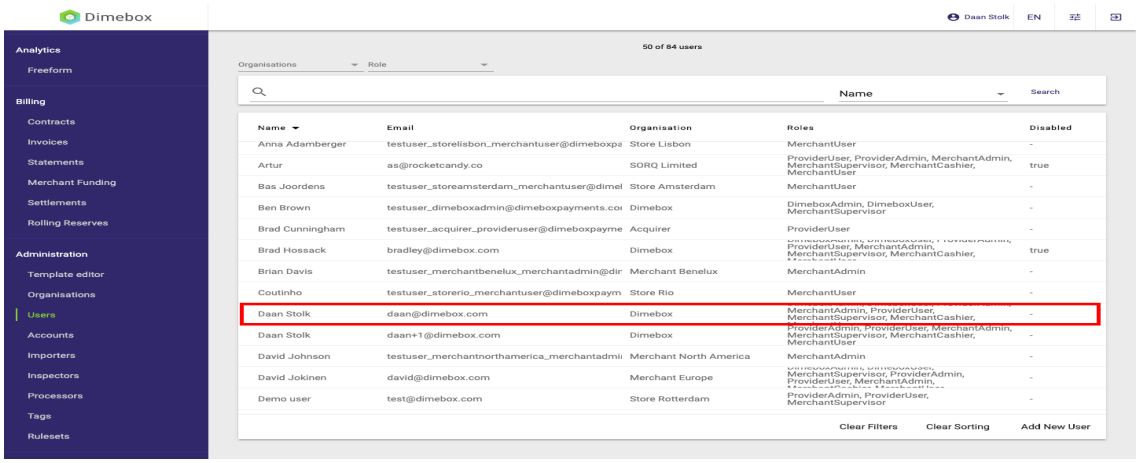


2. Every user will need to have roles assigned to it. Select the appropriate roles for this user and create them in the relevant organisation. More information on the scope of an user can be found here.

- `Full name of the user`: Can be changed later.
- `Roles`: Can be changed later. Find more information on the roles: here. Can be changed later.
- `Organisation`: The organisation the user belongs to. Make sure this is the same as the account you intend to use it for. More information with regard to relationships between organisations and accounts can be found here. Can be changed later.



3. After clicking save verify the user was created:



After creation of the user an email is sent to reset the password. Ask the user to check the spam folder if they do not see the email.