Employees

Overview

Admin app provides role based security system within the scope of accessible shops. Thus data federation mechanism i.e. what data business user has access to is determined by which shops and roles are assigned to their account.

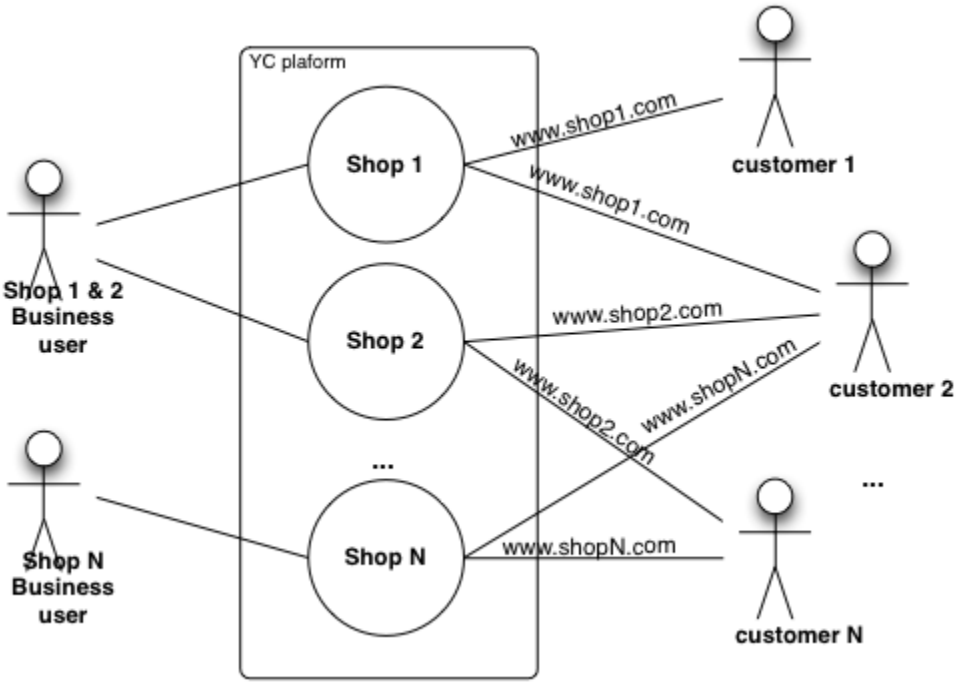
Each business user account has roles associated with it and each business user is assigned to one or more shops. When user logs into Admin app these roles and shop assignments are evaluated and held in session. Every request coming from this user is checked against what roles are applicable and what roles the user has as well as whether data viewed is available for specified shop assignments. If the user does not have the correct role a security exception is raised preventing access or modification of data.

For detailed description of roles refer to "Access rights" section below. Each role provides either read or write permissions. So it is possible to give read only rights to certain users as well. **Admin app adapts interface to the roles set for a particular user** and may remove some sections from the menu to which currently logged in user does not have access, thus keeping the UI clean and focused.

The out of the box roles scheme provides relatively fine grained access rights. However if more elaborate role hierarchy is required it is also possible via customisation which involves adjusting required roles on the Admin app controllers that expose business functions, which is a relatively simple customisation.

Data federation

Data federation refers to management of visibility of data. Sometimes it is desirable to limit access to certain data for certain users, organisation departments or different organisations (e.g. in marketplace environment).



Base unit of data federation in is a single shop. When business user is assigned to a shop they are granted access and will be able to view and manipulate data for that shop as authorised by the roles assigned to their account. This principle is followed throughout the platform whenever data is presented to the user in the Admin app.

> For users that are granted access to multiple shop if it is required to have different roles - then separate user accounts should be created with each assigned to a single shop thus enabling shop specific role set per user account.

Access rights

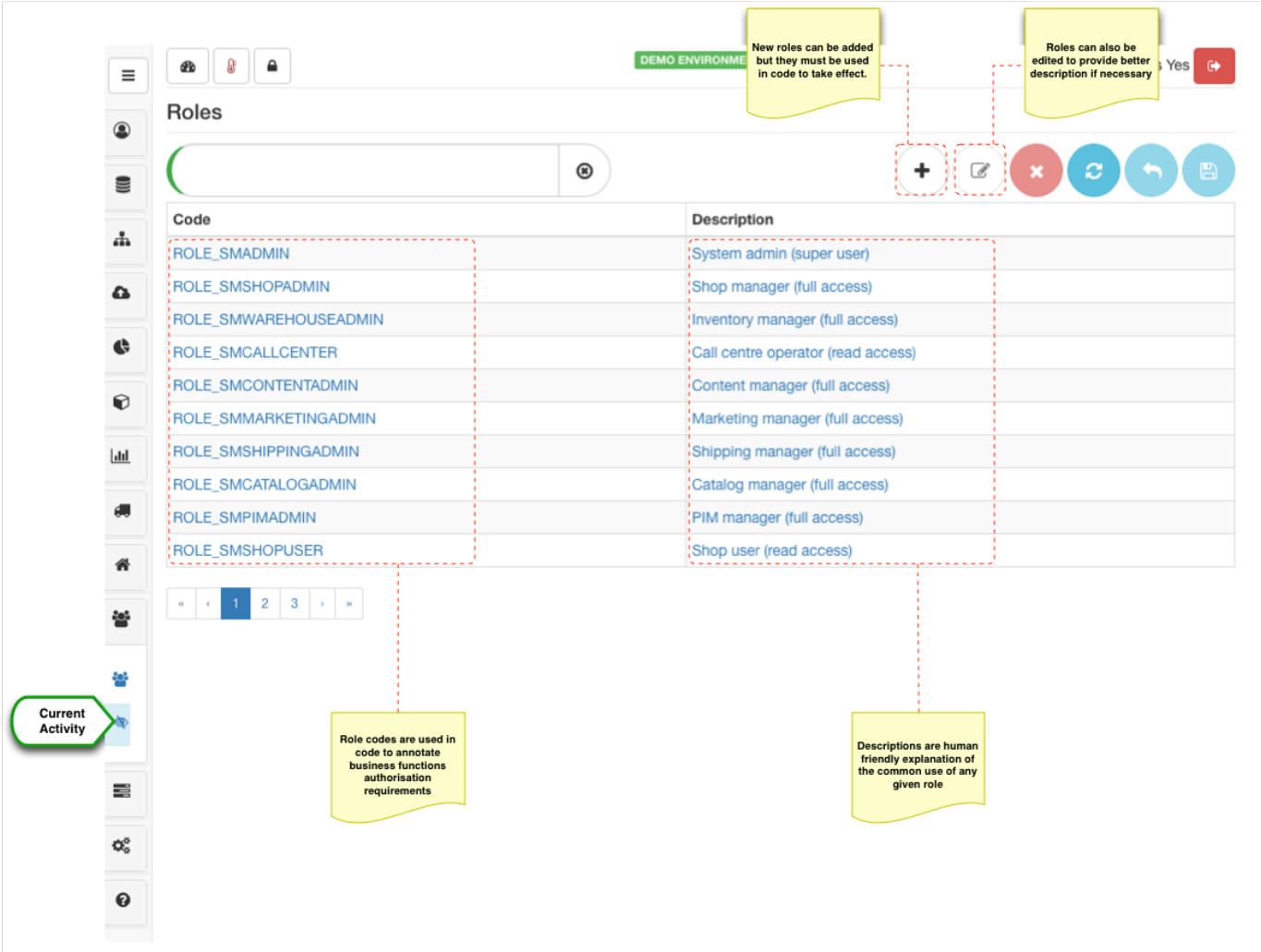
For version specific access right see:

- Business Functions 3.0.0
- Business Functions 3.5.0
- Business Functions 3.7.0

Roles

There is a number of predefined roles that are used to grant access to specific business function set. Most roles have either a read or write access so that it can be assigned independently.

New roles can be added but code changes need to be made to annotate business functions that will use these roles, which is a relatively simple change. For most use cases the roles provided out of the box are more than sufficient. Role description can be modified to provide better explanations of what they represent if the out of the box description does not provide enough details.



Employee management

It is perceived that the platform is managed by an organisation, regardless of whether this organisation is a single private person or a multinational the "organisation" in this context is the entity that owns the platform instance. Therefore in one way or another every business user that logs into the platform is an employee of the organisation.

From small businesses perspective this particular topic may not be of a high importance as it may be the case that the whole e-commerce operation is run by a single person or a team who have equal rights to access all data. However when we get into the realm of medium and large businesses whereby several departments collaborating in the e-commerce operation the separation of roles and limitation of data access become extremely important.

Regardless of the size each employee (business user) would need to be authorised for accessing one or more shops and they would need to be granted roles in order to fulfil their particular functions within the business.

Through data federation filters each business user will only see the data they are authorised to see.

Basic unit of data federation is a **shop**. Consider the following example. Platform with three shops A, B and C. Suppose shops A and B are under control of one department and we want to create Administrator that can manage both A and B. In such case a super Admin (ROLE_SMADMIN) would create a new user (say adminAB@myorg.com) and assign shops A and B and grant full access role (ROLE_SMSHOPADMIN). Now when adminAB@myorg.com logs in they are able to create additional users but will only be able to grant access to shop A and B, since it is the only ones they have access to. Suppose now we have two users that handle customer requests for each shop respectively. adminAB@myorg.com would create a user callcentreA@myorg.com and will assign only shop A and grant call centre role (ROLE_SMCALLCENTRE) and a second user callcentreB@myorg.com and will assign only shop B and grant call centre role. Both of these users will only have access to a single shop and only to the "Customer Service" section in Admin app. Now lets assume fulfilment centre is managed by another user ffAB@myorg.com, when creating this user we could grant call centre role as well as fulfilment centre access (ROLE_SMWAREHOUSEADMIN) which would allow this user to manage inventory and progress orders when "packing" and "preparing for shipment". As can be seen from this scenario and number of users with different roles and shop access right can be created to collaborate but not exceed their powers which is ensured by federation API.

3.7.0+ has additional data federation dimensions to fine tune access to master catalog and products. Single master catalog and PIM are shared resources it is important to manage it effectively however in a secure and controlled way. Notion of **supplier catalogs** and **master catalogs** allow to adjust data access rights to PIM and master catalog respectively.

Supplier catalog set as supplier catalog code property on the product allows to restrict access to PIM. Only managers that have supplier codes assigned will have access to restricted products. Note that if products do not specify a supplier catalog code - they are assumed to be publicly shared (i.e. for all shop managers who have access to the platform).

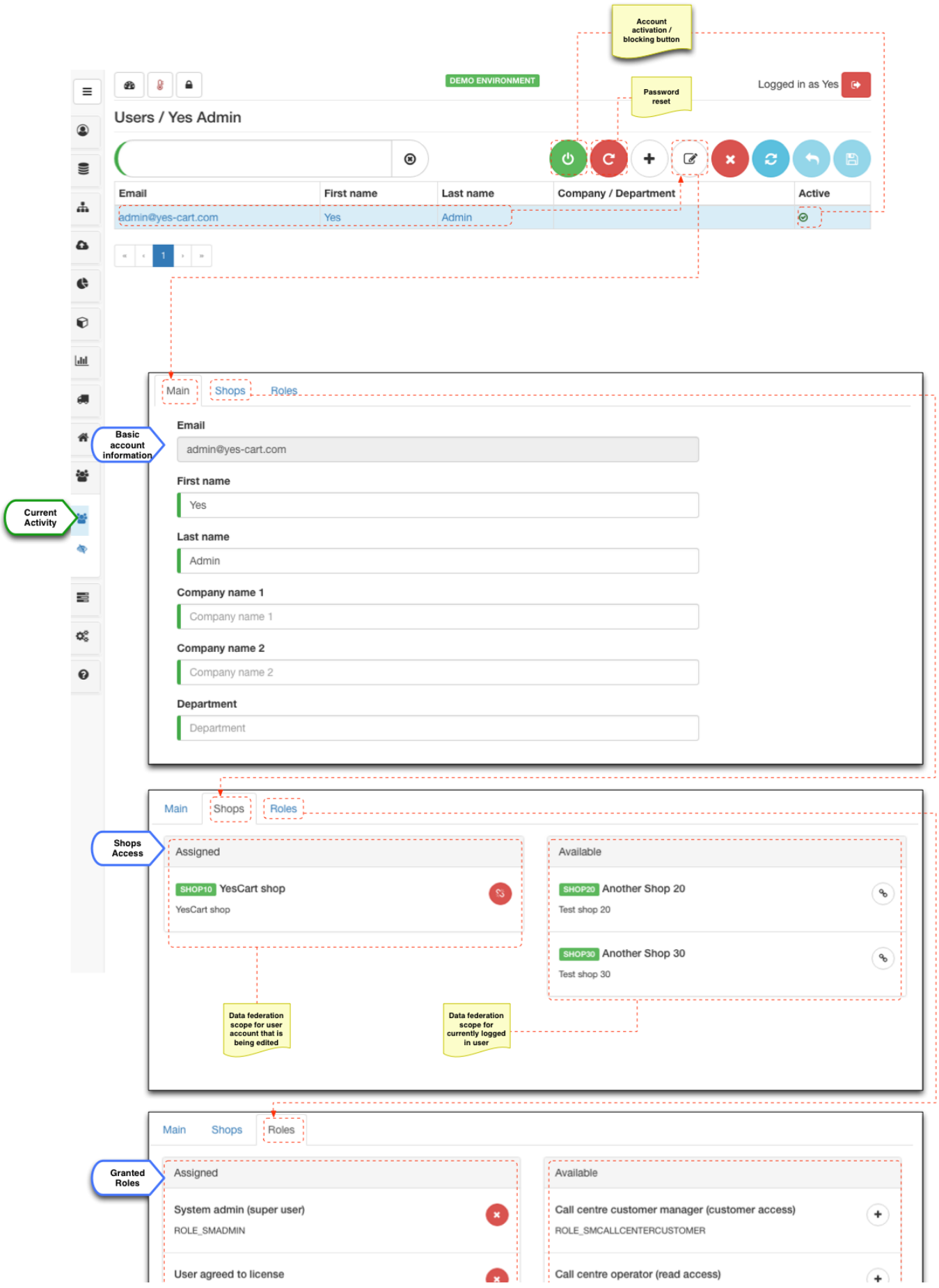
Master catalogs allow to define master catalog access which was historically implicitly set via shop catalog configurations. This is still the case and by default if master catalog configurations are not specified they are assumed from the shop configurations to which manager has access to. However as soon as catalog access is specified directly as manage record level is takes precedence. It is anticipated that this configuration provide more access (i.e. top level category) to allow better shop management access and flexibility in shop catalog configurations.

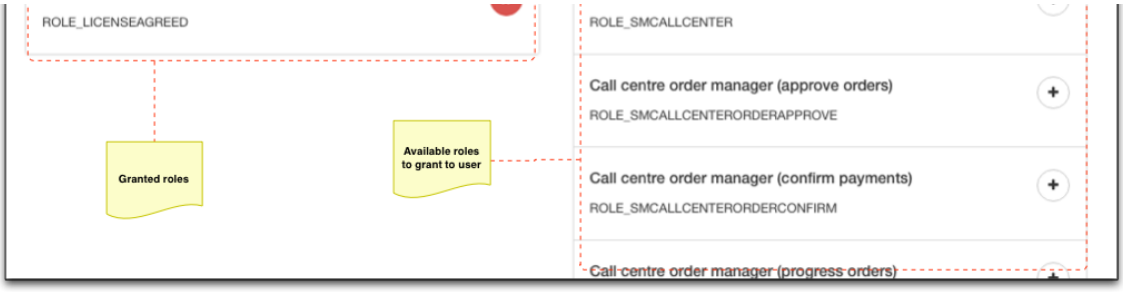
Managing accounts

When user accounts are created, activated / blocked, or their password is reset, **business user receives an email notification**. Account management is fairy simplistic and contains only basic information about the user and company/department they work for. The primary focus is data federation and authorisation management for given account.

> Note that all accounts are **disabled by default when created**, so administrator needs to click the activation button for the business user to start using it.

> Roles and Shop assignments data is kept in user session. Therefore any changes may not have any effect until user logs out of Admin app and then logs back in.


Account activation / blocking button
DEMO ENVIRONMENT
Password reset
Logged in as Yes
Users / Yes Admin
Email
First name
Last name
Company / Department
Active
admin@yes-cart.com
Yes
Admin
Main
Shops
Roles
Basic account information
Email
admin@yes-cart.com
First name
Yes
Last name
Admin
Company name 1
Company name 1
Company name 2
Company name 2
Department
Department
Current Activity
Shops Access
Assigned
SHOP10 YesCart shop
YesCart shop
Available
SHOP20 Another Shop 20
Test shop 20
SHOP30 Another Shop 30
Test shop 30
Data federation scope for user account that is being edited
Data federation scope for currently logged in user
Granted Roles
System admin (super user)
ROLE_SMADMIN
User agreed to license
Call centre customer manager (customer access)
ROLE_SMCALLCENTERCUSTOMER
Call centre operator (read access)

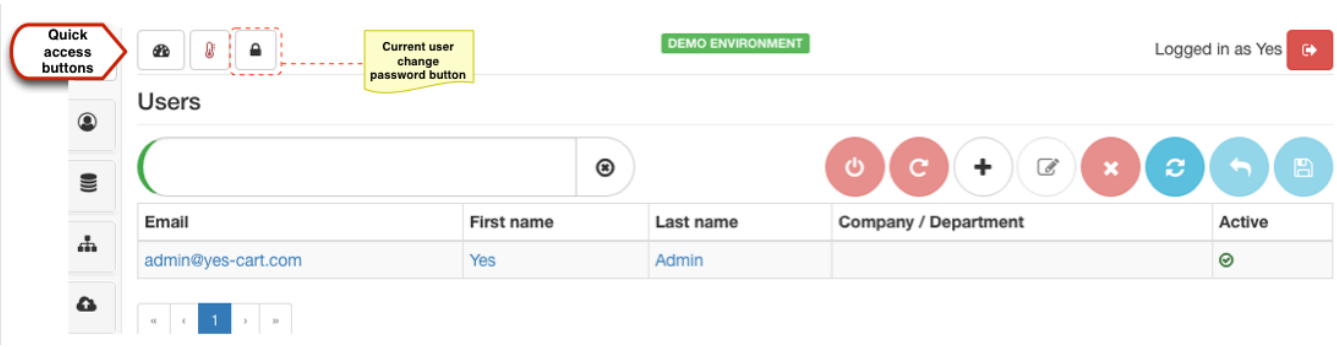


Password management

Administrator user has option to send a password reset notification for any business user account accessible by them. Email contains a link that business user can follow in order to set their new password and re-gain access to their account (Administrator would do this as least once after creating a new account).

For **security purpose the link has expiry time and if not used in time will become invalid**. In such case administrator user simply needs to reset password again. **Once reset password token is used is becomes invalid**, so you can only change password once using specific token.

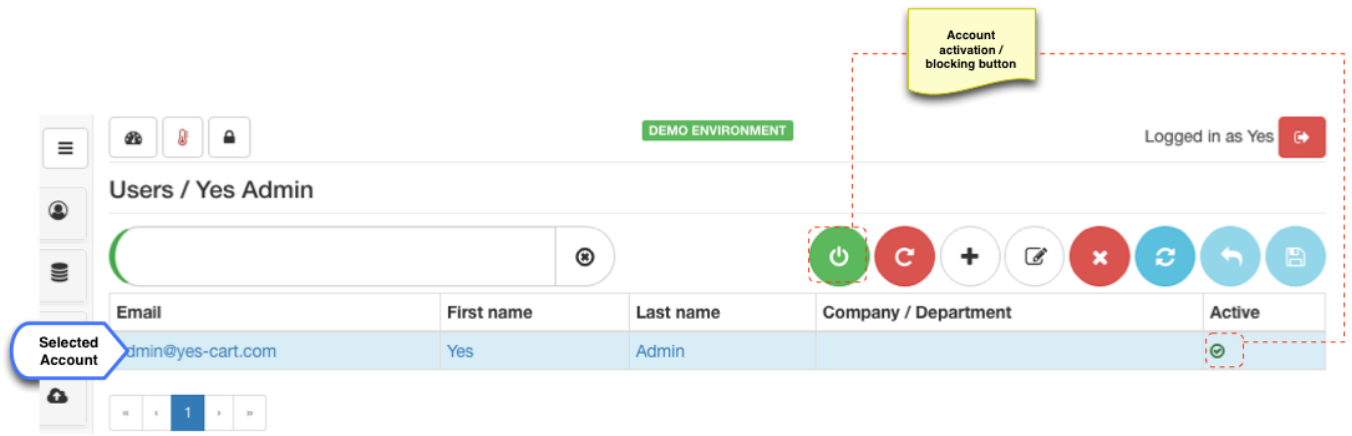
For business users that simply want to change their password they can do so by using the change password button on the quick access buttons toolbar.



Disabling accounts

There are several options how to prevent business user from accessing their account.

The simplest one is using account activation / blocking button which allows to either activate or block account depending on its current state. When account is disabled then button will be red indicating that it is inactive, clicking it will activate the account (after confirmation) and the button will change to green. The opposite will occur when active account is clicked to be disabled.



Blocking the account preserves all access rights and simply prevent user from logging in. When activated all old access right will be active again.

If it is desired to prevent this account from being used again (at least with an ease of just clicking activate button) an administrator in addition to blocking the account can also un-assign shops and roles. This way even if the account is activated by mistake the user will have no access rights.

Last resort is to delete the user account to remove their account information from the system. Audit information (created by, modified by) will still remain in the system, so there is no harm is deleting the accounts apart from the nuisance of having to re-enter them if they need to be re-activated.