InfoGlobalTech

Innovative Solutions for your Enterprise

CoSaCS

Administration Technical Document

Author: IGT PMO ● InfoGlobalTech ● Version 1.0

REVISION HISTORY

NOTE: The revision history cycle begins once changes or enhancements are requested after the initial version of the Technical Document has been completed.

Date	Version	Description	Author
16/12/2020	1.0	Initial	Kirti Vaishnavi M

TABLE OF CONTENTS

INDEX OF FIGURES

1 ADMINISTRATION MODULE OVERVIEW

All Administration of CoSaCS users is done from the CoSaCS Web Application. All options are available under the “Administration” menu. An administrative user can add or remove users, manage their roles and permissions, add/remove profiles, and monitor the application.

Figure 1 Administrator menu options

1.1 Users & Roles

Users are the people involved in using the CoSaCS application. Cashier, Supervisor, or Manager, etc. can each be considered as an individual user within the CoSaCS system. However, the roles and permissions shared can overlap.

Create User

- To add a new user, fill in all fields on the form and click "Submit"
- External Directory login refers to any other username that the user may have (Example: FACT login), that might need to be recorded.
- Passwords must comply with the complexity rule set up within the "Country Parameters" and "Security Section".
- Upon clicking on the "Create" button, the user will be created, and the page will redirect to the User Details page of the new user.

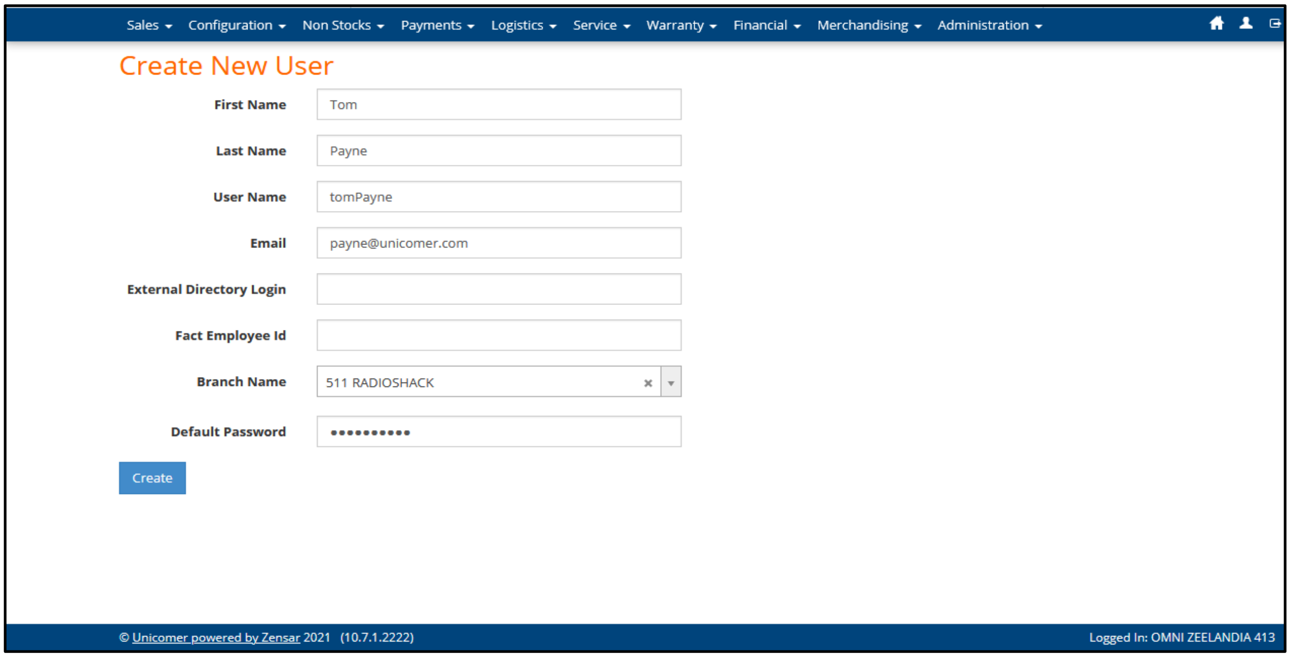


Figure 2 Create new user screen

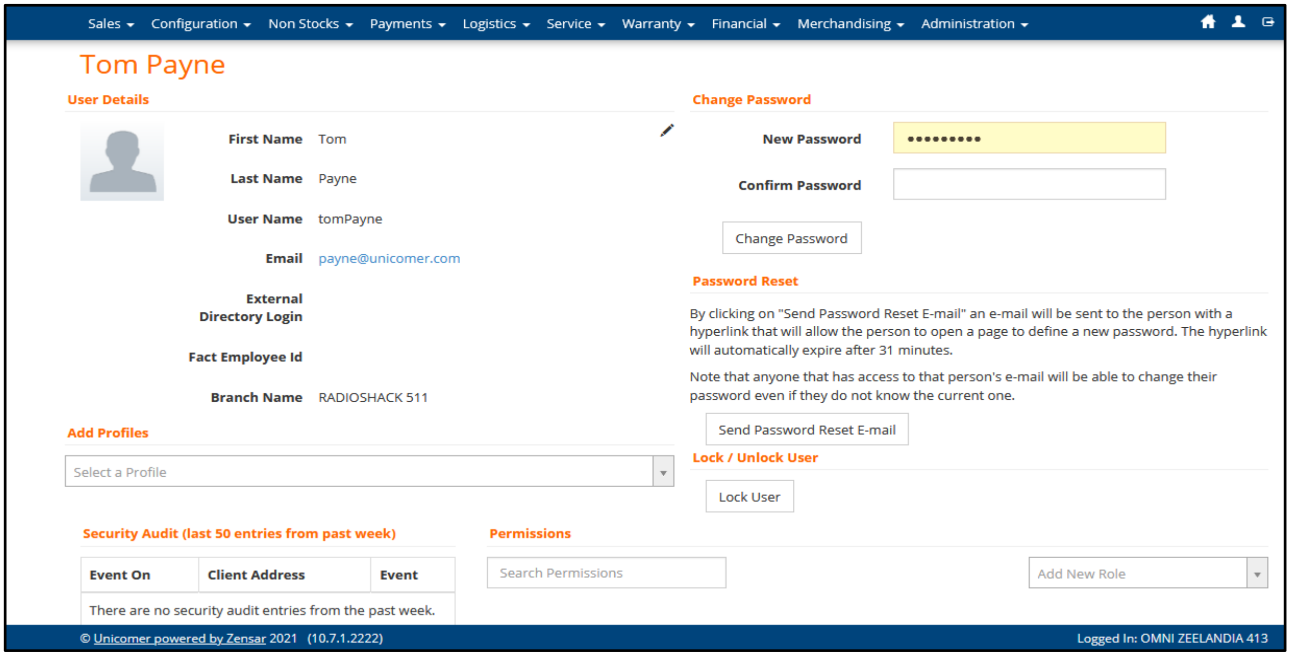


Figure 3: User screen after a new user is added

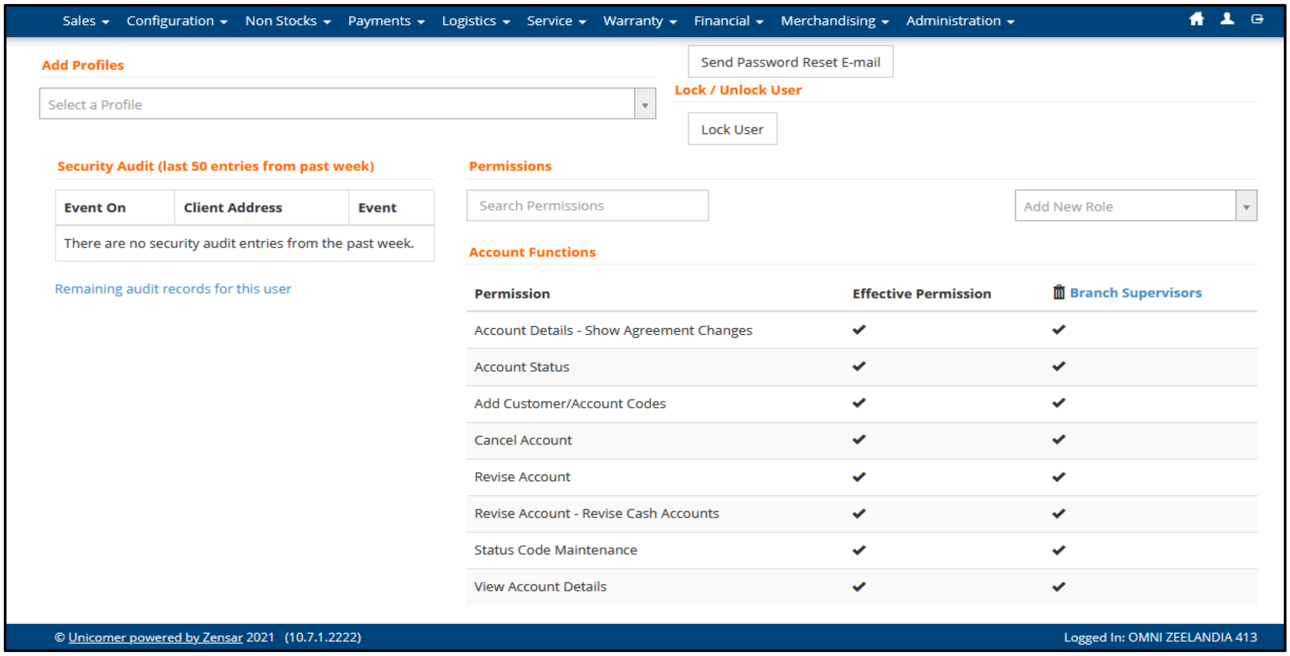


Figure 4:After a new role is added to a new user

Search User

The Search User screen is used to view and/or amend the details of a specific user. Users can be searched by entering details like ‘name’, ‘CoSaCS login’, etc. in the search box or by using any of the filter options available.

The search results will be displayed below the search filters. To view the individual user’s details, click on the respective user’s name. On the [page that is displayed](), one can view and edit (permission-dependent) specifics relating to that user.

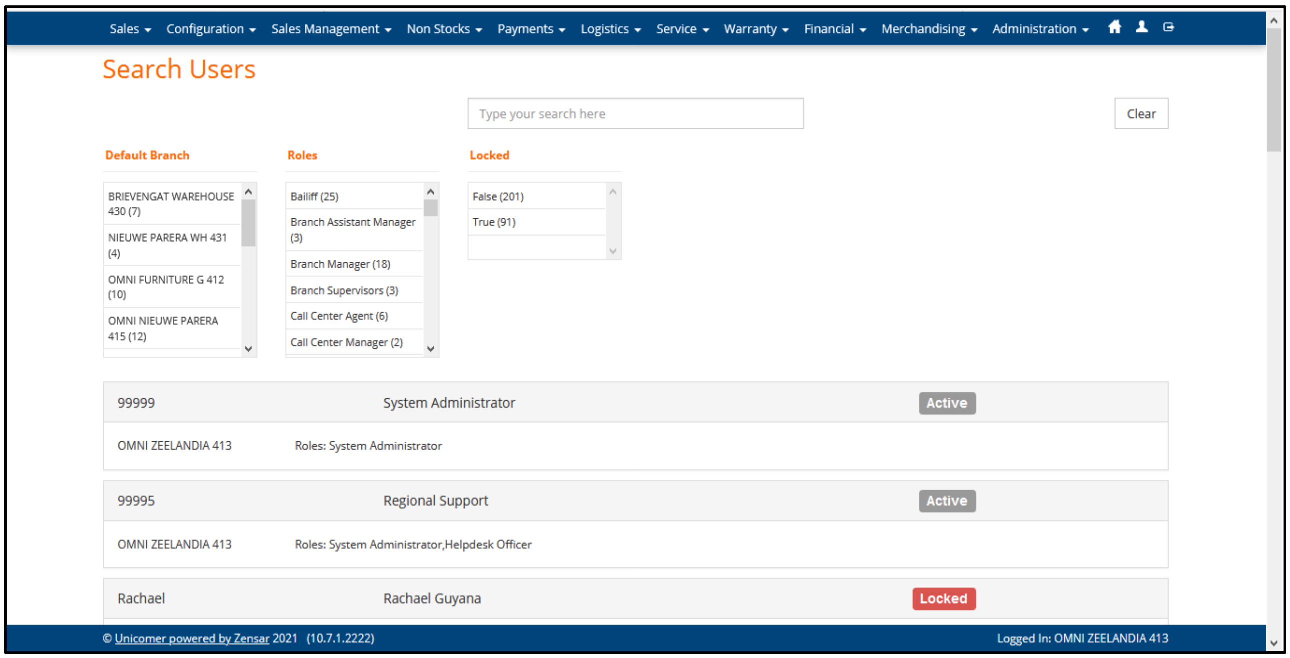


Figure 5 Search Users screen

Administrators can perform the following tasks on the [User Details page]():

View and edit user information

- All information is presented in a read-only format.
- If fields in the User Details section need to be edited, click the pencil icon in the top right-hand corner of that section.
- Edit and Save the necessary changes.

Change a user's password

- Use the Change Password section of the page to set a new password for the user.

Send a user a 'Set New Password' email

- This is dependent on the user having email access.
- The user then resets their password via a link in the email.

Lock or Unlock user

- If the user is locked, they can be unlocked by clicking the "Lock/Unlock" button and vice versa.
- Locking a user will prevent them from accessing CoSaCS.
- This function replaces the ex-employee's role.

Add Profiles

- This section will store additional information only relevant to a certain User Profile.
- Select from the available profiles in the drop-down list (now, Technician is the only option displayed).
- Any additional information associated with this profile will appear, to be populated.
- Select whether the Technician is 'Internal' or 'External'.
- Add the working hours (Start and End Time).
- Select the number of slots they can fit into the working hours.
- "Shift Length" and "Slot Size" will then be calculated and displayed.
- Add the categories in which this Technician can complete jobs.
- Delete categories from the list by clicking the bin icon next to the category.
- Save the details entered by clicking the disk icon in the Technician Profile section.

View and Search Permissions

- All permissions assigned to the user will be displayed under their respective Business Area heading.

- Use the “Search Permissions” box to find previously assigned permissions.
- The permissions page can be directly accessed by clicking on the role name.
  Note: Editing permissions on a role would also affect other users with the same role.
- If a user has two roles with conflicting permissions (i.e. permission is denied in one role but allowed in another), the permission will not be granted.

Superuser Permissions

- Few permissions, for specialized administrative changes, can only be assigned to or taken away from users by a ‘Super User’. The permissions that can only be assigned to a user by a Super User, are:
  - Scoring - Edit Scoreband Matrix.
  - Scoring - Edit Scoring Matrix.
- A Super User, in turn, requires special permission to makes them a Super. This permission is: “Assign Super User”.

Manage Roles

All Roles assigned to a user will be shown with their respective permissions ticked in the Account Functions grid. Roles can be removed by clicking on the BIN icon next to the Role Name. Add a role to the Account Functions grid by selecting it from the “Add New Role” drop-down list.

‘Effective Permission’ is overriding a permission if the user has more than one role assigned. Example: if a user has a role assigned that has permission actively denied and another role where the permission is allowed, the ‘Effective Permission’ will be denied.

Roles

On the Roles page, users with appropriate permissions can perform the following actions:

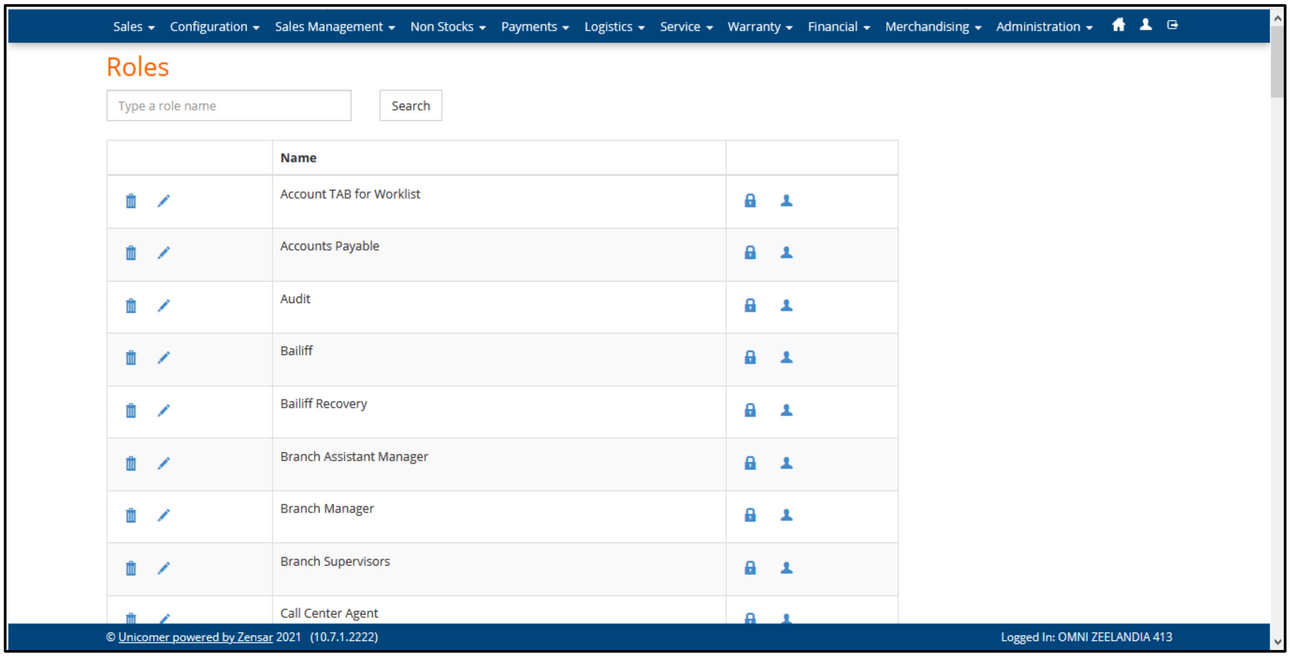


Figure 6 Roles screen

Search Roles

- A user can search for a particular role by entering the name or part of the name of the role.

Delete Roles

- By clicking on the BIN icon, a user can delete a role.
- They will, however, need to confirm the deletion by clicking 'OK' on the confirmation pop-up.

Edit Roles

- The role name can be edited by clicking on the pencil icon. This allows the user to make the changes to the role.
- To save the changes the user needs to click on the disk icon.
- By clicking on the Cancel arrow, they can drop the changes.

Create a New Role

- Scroll to the bottom of the current list.
- Click the page icon at the bottom left corner of the table.
- Enter the name of the role to be created.
- Click the disk icon to save the new role.
- The role is created, now the user can add permissions and users to the role.

Permissions for Roles

- Click on the lock icon to view all permissions.
- The permissions page will open for that role.

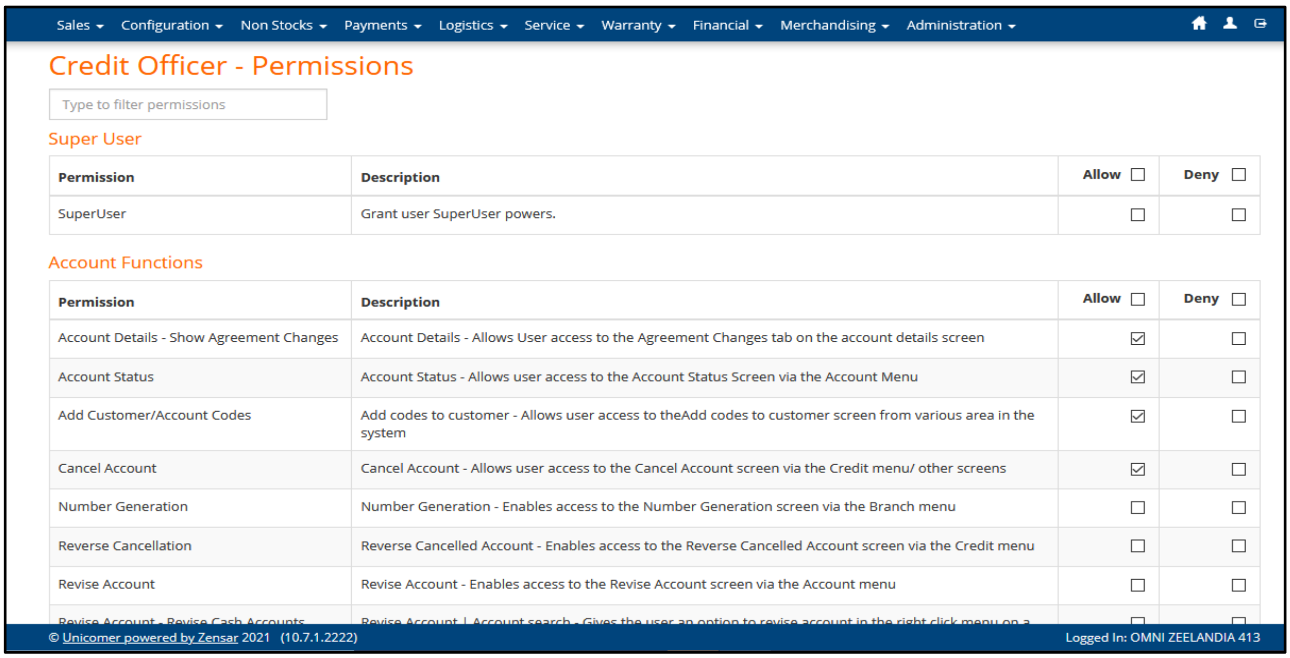


Figure 7: Role permissions page

- All permissions can be seen but only the ones with a tick under the "Allow" column are assigned to this role.
- Permissions are grouped by Business Area. Each area can be expanded or collapsed by clicking on the area name.
- Use the search box to find permissions, if required.

- To assign certain role permissions, select the respective checkbox in the “Allow” column.
- To remove certain permissions, select the respective checkbox under the “Deny” column.
- Clicking on the checkbox next to the “Allow” or” Deny” heading ensures that all permissions are assigned/denied to the user.
- Changes are automatically saved and will apply to all user accounts with that role.

View Users Assigned to a Role

- To view the list of users with a particular role, click on the PERSON Icon.
- All the users currently assigned to this role will be displayed.

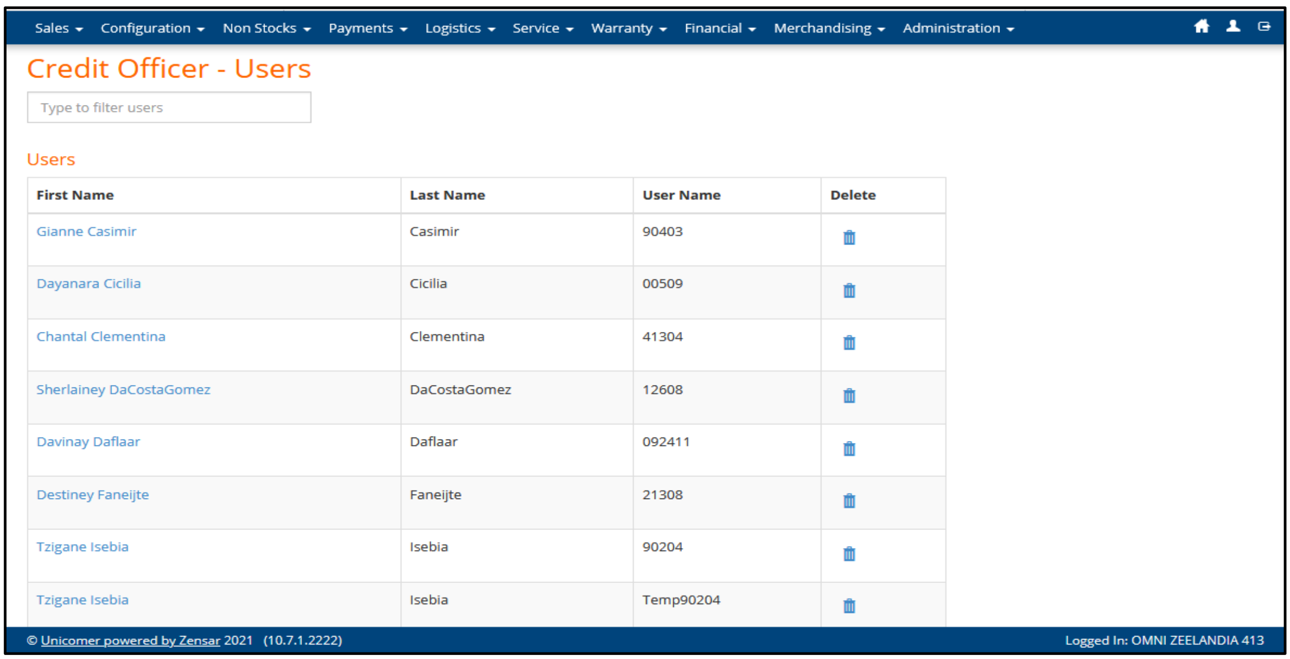
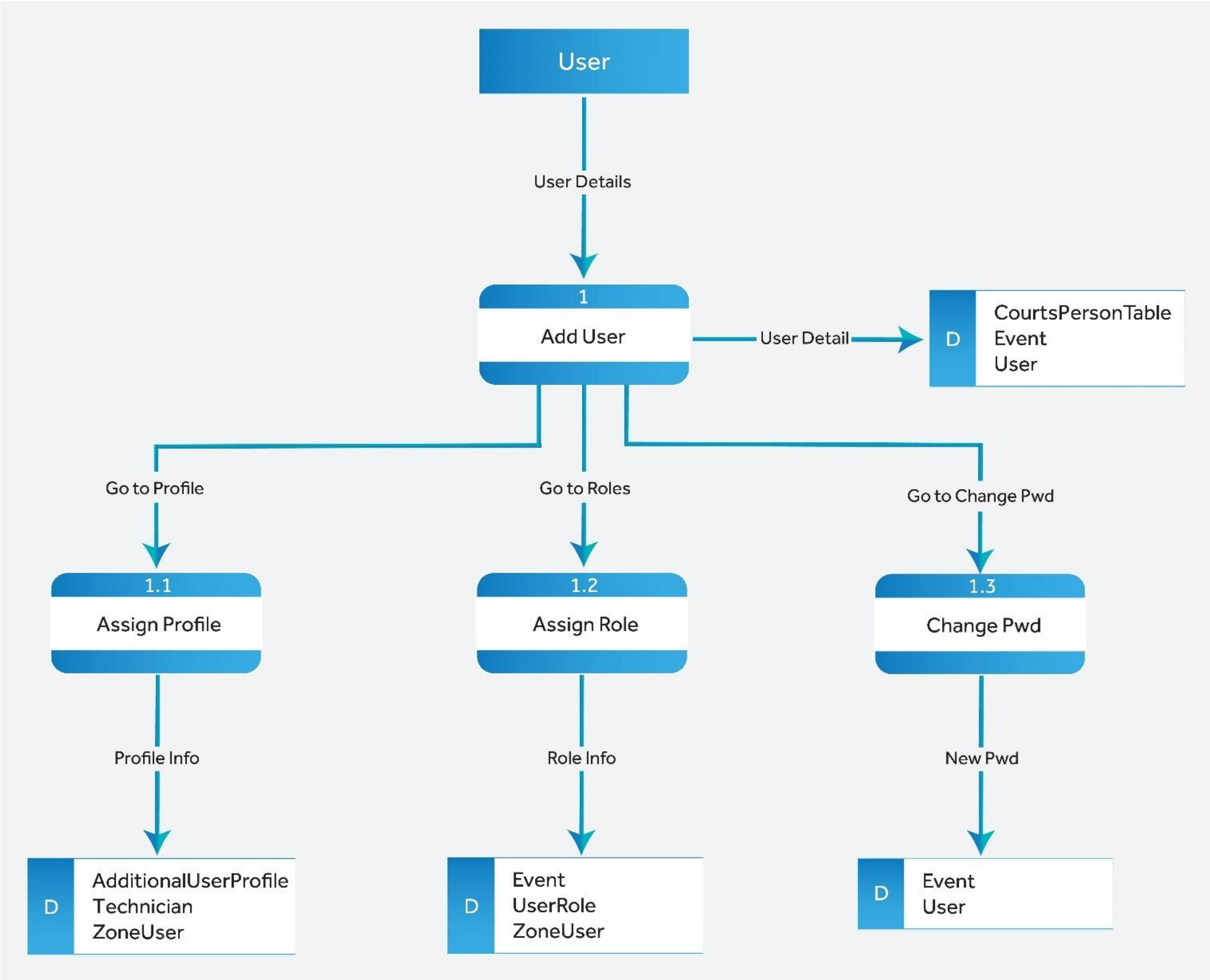


Figure 8: List of users assigned to a particular role

- A user from the list can be removed by clicking on the BIN icon.

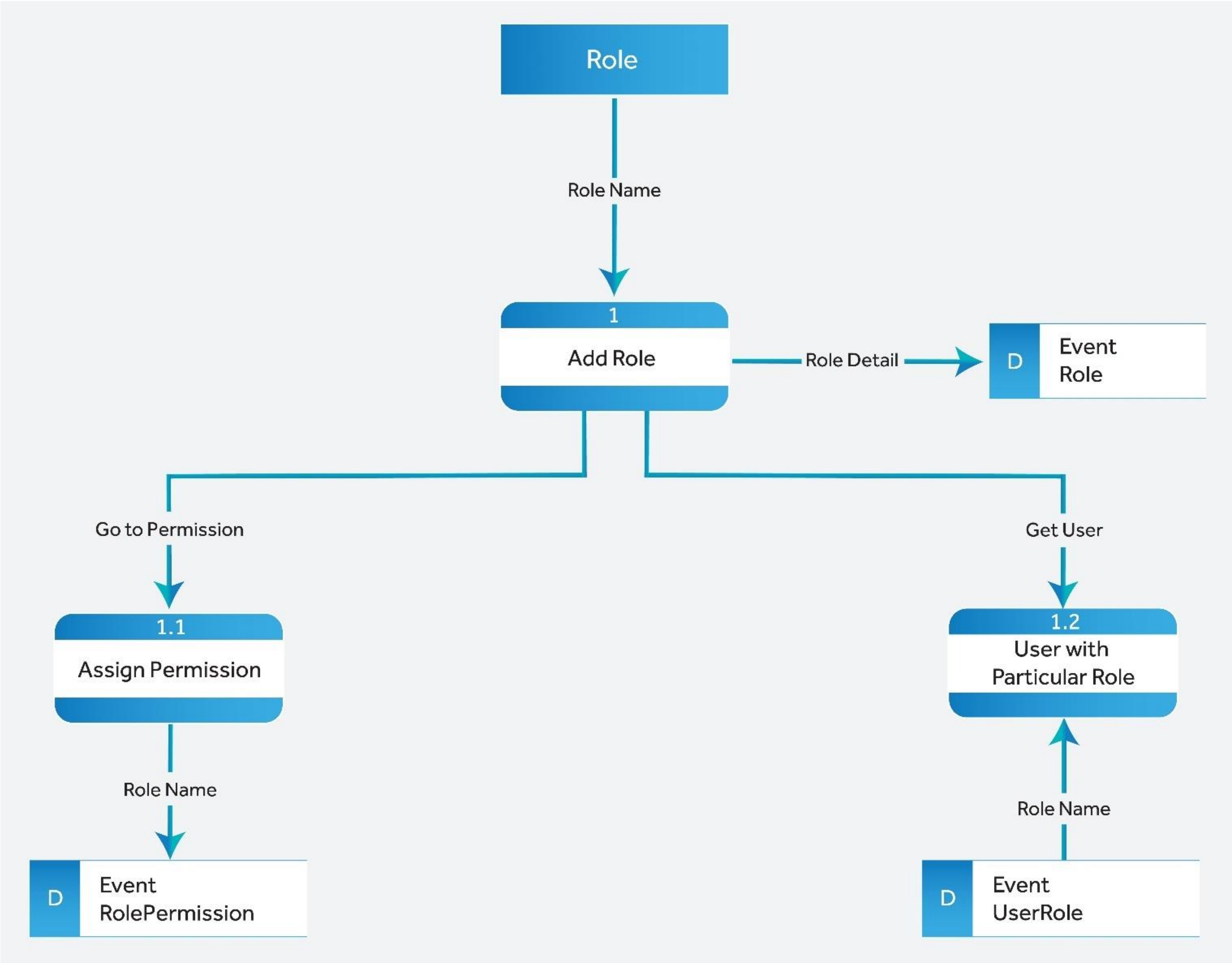
1.1.1 Data Flow Diagram – Users

The below Data Flow Diagram describes the data flow process involved in user maintenance:



1.1.2 Data Flow Diagram – Roles

The below Data Flow Diagram describes the data flow process involved in role maintenance:



1.2 Audit

This module acts as a system log and captures all actions performed in the system by any user. Using this module, the business can also link RF or Cash Loan accounts.

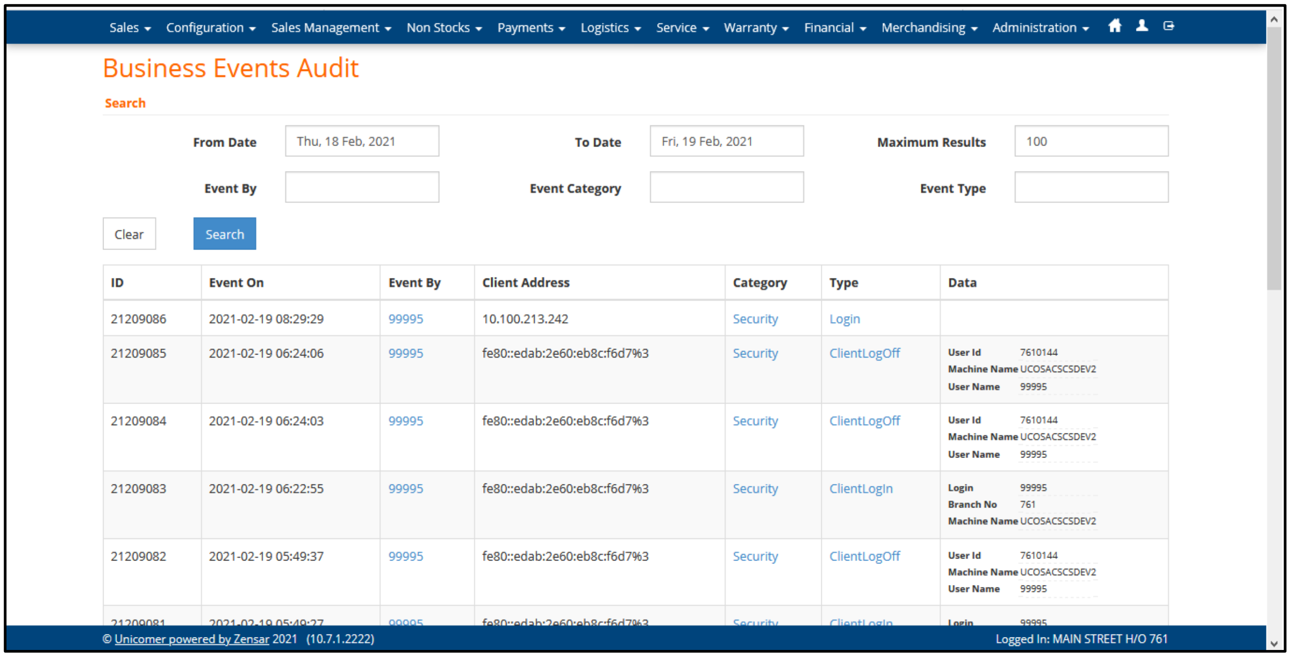


Figure 9 Audit screen

Audit trail on customer linking

Customer linking is a process where the RF or Cash Loan account created for one customer can be linked to another customer. After linking an account, the existing account will get linked to the new customer ID and will no longer have the old customer's ID and name.

Steps to link accounts:

- Open the customer screen into which the account needs to be transferred.
- From the menu option, select 'Link to Account'.
- The Link Customer to Account screen will be displayed.
- Enter the account number that needs to be linked.

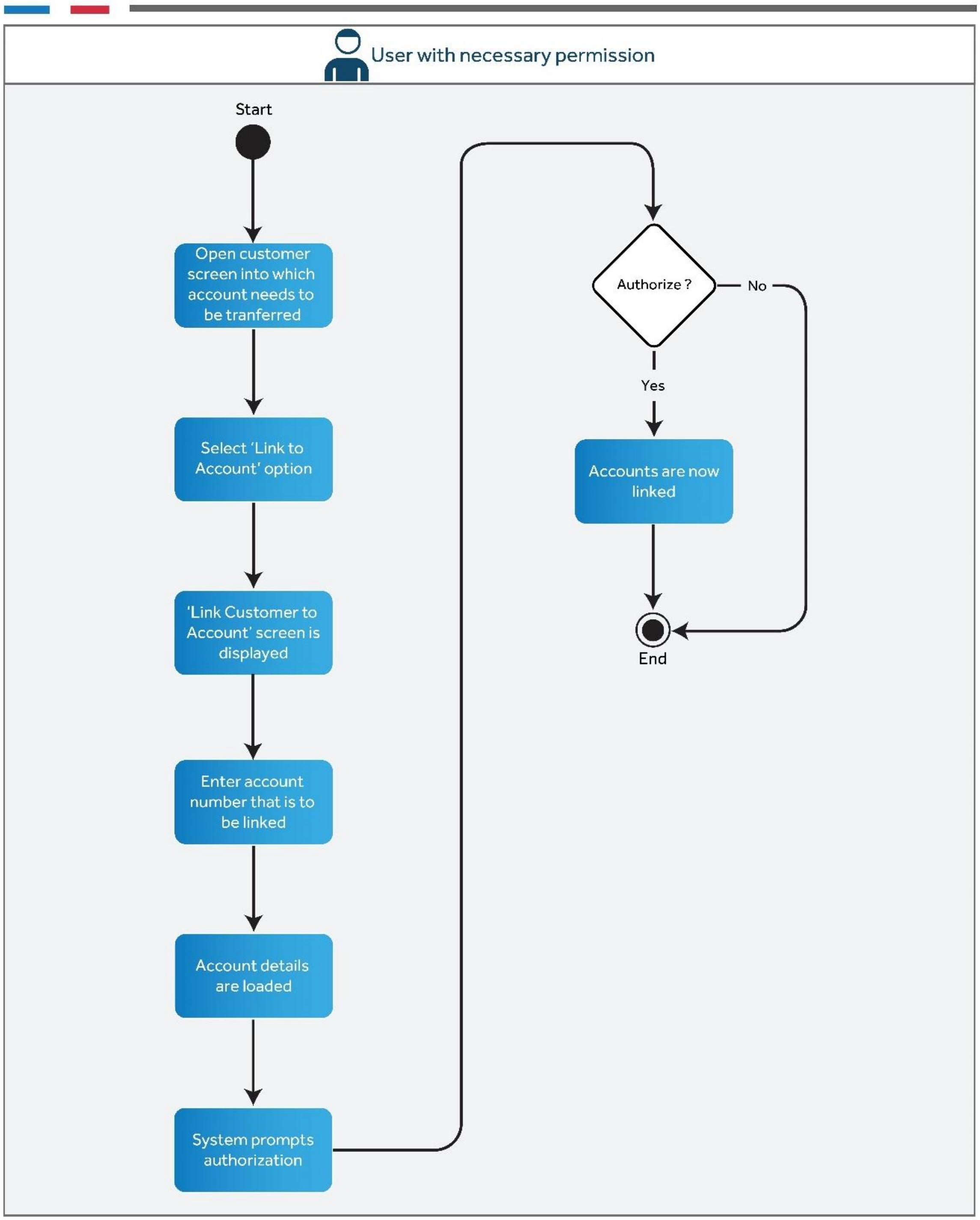
- After the account number is entered, the system will display the linking details.
- Then the system will prompt for authorization.
- If authorization is successful, then the account will get linked to the new customer.
- The new accounts created in the Windows Client will be updated to the web after the EOD process has been executed.
- The system will record the following details as part of the audit process:
    - Activity – Account Linking
    - Customer Code/Name Linked From
    - Customer Code/Name Account linked to
    - Account Number linked
    - Date/Time Account linked
    - Authorized user ID/Name

Benefits:

- ❖ Improve the process of account linking.
- ❖ Reports of all cases of account linkage.
- ❖ Audit process that protects all cases of fraudulent linkage.

1.2.1 Process flow

The below diagram depicts the steps involved when linking accounts:



1.3 Address Master

Address Master is a module introduced into the system as part of version 10.7. Here, the user can add new address details to the database. The address is added in three levels:

1. Region
2. Village
3. Zipcode

Only users with the permission “Address Master management” will be able to view the Address Master screen and can add/edit addresses within the system.

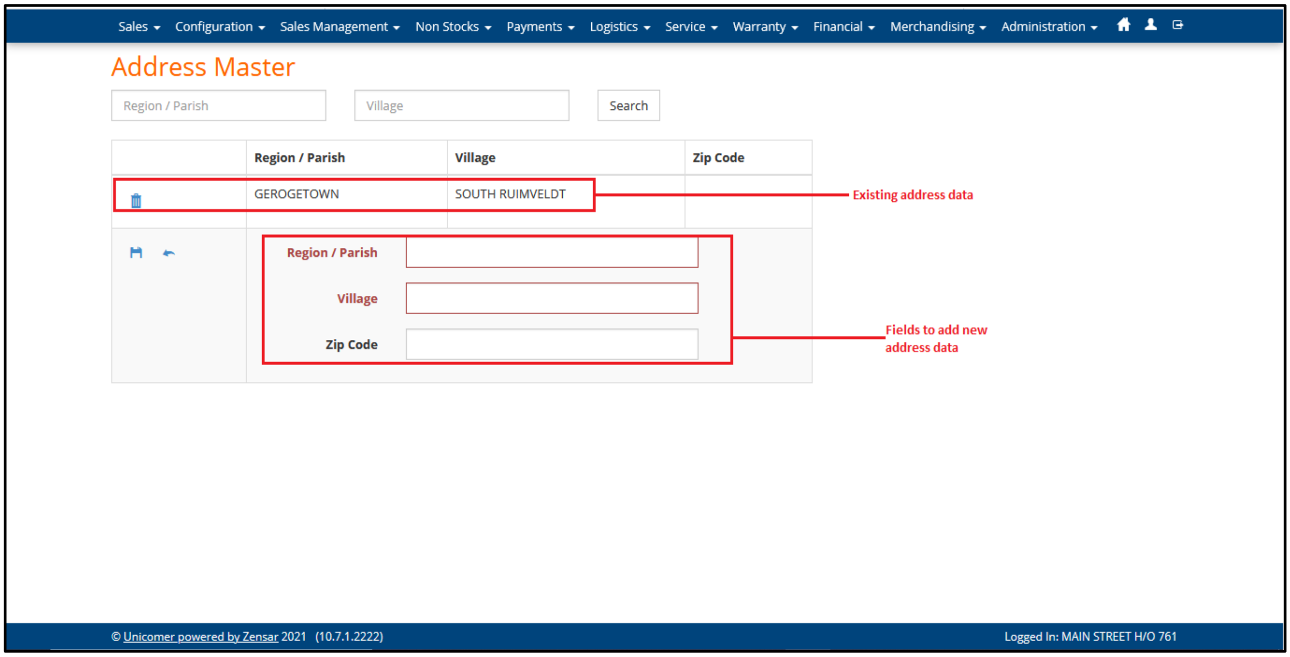
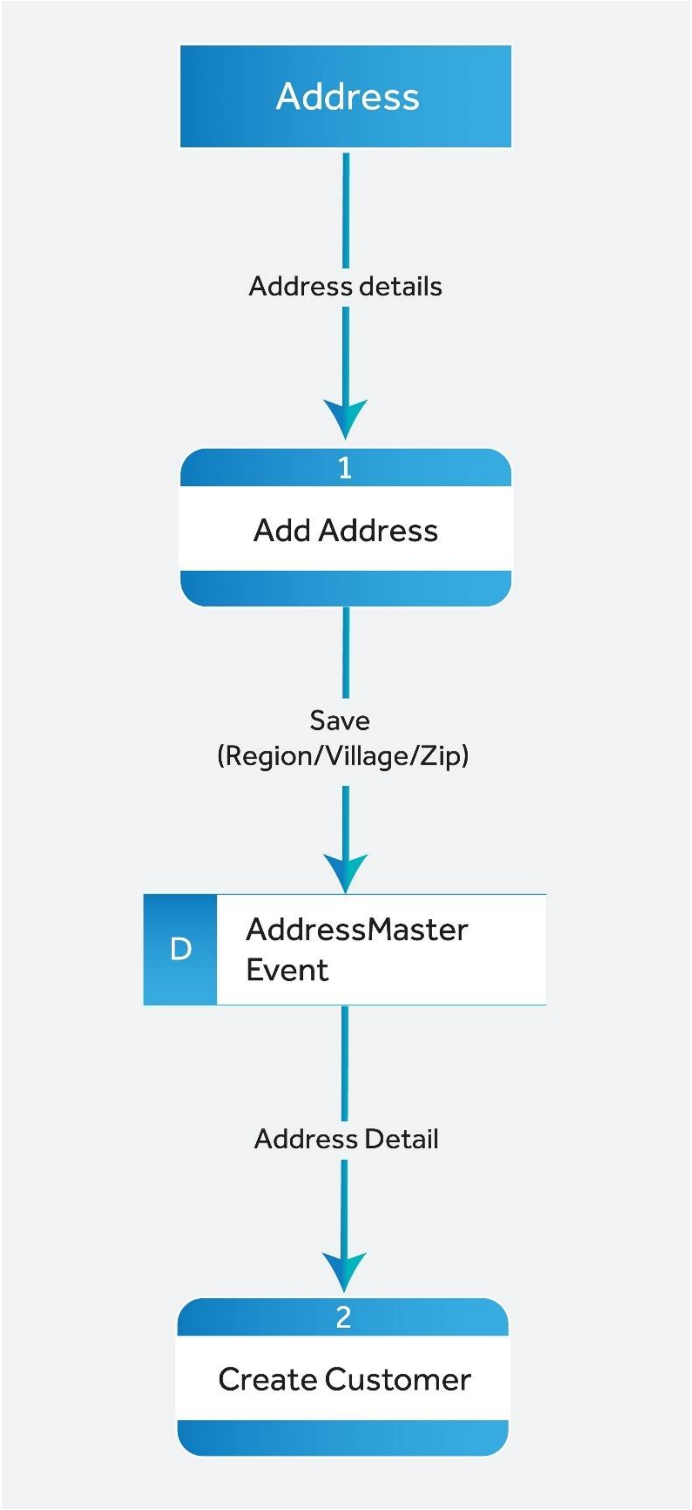


Figure 10 Address Master screen

1.3.1 Data Flow Diagram

The below diagram describes the data flow in the address master module:



1.3.2 Use case

The below diagram illustrates the users and processes involved with Address Master: