Login

This module requires system administrators to provide their username and associated password in order to access their accounts. The login process follows these key steps:

User Input

System Administrators needs to enter their username and associated password into the designated login fields on the platform’s login page.

Validation

The system verifies the entered username and password against the stored system administrator credentials.

Successful Validation

If the provided username and password are successfully validated, system administrators are granted access to navigate to their Dashboard screen.

Unverified Email Address

In the event that the email address is unverified, the system prompts system administrators to verify their email address.

The system administrator has the time frame of 24 hours to verify that email address. After that, the email would be expired. If system administrators have misplaced their verification link, they are given the option to request a new verification link to be sent to their registered email address. This ensures the security and accuracy of account information.

Failed Validation

If the entered username and password do not match the stored credentials. The system displays an appropriate error message to the system administrator. The error message clearly communicates the reason for the login failure, providing guidance on the necessary steps to rectify the issue.

Unmatched Email Address and Password

System Administrators are notified that the provided email address and password do not match. They are prompted to re-enter the correct credentials.

Missing Email Address or/and Password

System Administrators are notified that the email address or password field is missing. They are prompted to provide the necessary information in order to proceed with the login process.

“Remember Me” Feature

The "Remember Me" feature in the login screen is a functionality that allows users to opt for a convenient way to stay signed in to the CRM system without the need to manually enter their login credentials every time they access the application.

When users enable the "Remember Me" feature, the CRM system stores a persistent authentication token or cookie on their device.

This token is used to automatically authenticate the user upon subsequent visits to the login screen, bypassing the need to enter their username and password.

Doesn’t Have an Account

If a system administrator lands directly on the login page and it doesn’t have the account in the CRM then there is also an option of signup in the login screen.

When a user clicks on the "Signup" button, they are redirected to a registration form where they can enter details such as their name, email address, password, and any other required information.

Email Verification

Email verification is a crucial step in the signup process to ensure the validity and authenticity of the system administrator’s accounts. After they provide their email addresses during the signup form, the CRM system implements an email verification mechanism to validate the provided email address. The process of email verification typically involves the following steps:

Sending Verification Email

Upon completing the signup form, the CRM system generates and sends a verification email to the email address provided by the system administrator. This email contains a unique verification link.

User Notification

The system displays a confirmation message to the system administrator, informing them that a verification email has been sent to their provided email address OR verify your user through email before logging in.

The system administrator has the time frame of 24 hours to verify that email address. After that, the email would be expired.

This message typically includes instructions to check their inbox, including the spam or junk folder if necessary, for the verification email.

User Action

The system administrator is required to open the verification email and click on the provided verification link within a specified time frame. This action confirms that the email address belongs to the system administrator and enables the system to mark the email address as verified.

Verification Process

When the system administrator clicks the verification link, the CRM system verifies the authenticity of the email address. The system checks whether the provided information matches the records and confirms that the link is valid and has not expired.

Account Activation

Registration/Signup Module - User Flow Diagram

Once the email address is successfully verified, the system administrator can be redirected to the page where the platform display the message that “Your Email is successfully verified” and the CRM system activates the system administrator account, granting them access to the system’s features and functionalities.

Registration/Signup

To enhance user experience and provide system administrator with the convenience of self-registration, the platform offers a user-friendly interface that allows individuals to create their accounts easily. When the System Administrator creates a new account, the following fields will be available during the self-registration process:

(* indicates required fields)

First Name*

The System Administrator needs to enter their first name.

Validation

The name should contain only alphabetic characters (letters) from the alphabet.

Special characters, numbers, and symbols are not allowed in the "First Name" field.

The field should not be left blank or contain any spaces.

Last Name*

The System Administrator needs to enter their last name.

Validation

The name should contain only alphabetic characters (letters) from the alphabet.

Special characters, numbers, and symbols are not allowed in the "Last Name" field.

The field should not be left blank or contain any spaces.

Username*

This field requires the system admin to enter their username.

Validation

Username must be in the format of email (i.e. abc@company.com).

This format ensures compatibility and adherence to the specific validation standards.

Email*

It is mandatory for the system administrator to provide a valid and real email address during the account registration process.

The verification link is sent to the email address provided by the system admin during the registration process.

To complete the account verification process, the system administrator needs to click on the verification link received in their email.

Account verification ensures the security of the registration process and helps prevent the use of invalid or reauthorized email addresses.

Validation

The account remains inactive until system admin will verify their account through the provided email address.

Phone Number*

It is mandatory for the system administrator to provide a phone number during the account registration process.

Validation

There is a validation in place for phone numbers to ensure they do not exceed 15 digits. This validation serves to maintain data integrity and adhere to the standard format for phone numbers.

Password*

This platform maintains strict security measures, and thus, system administrators are required to create a password that meets specific complexity requirements.

Validation

The password validation includes a minimum of 8 characters, at least 1 uppercase letter, 1 lowercase letter, 1 number, and 1 special character.

Address*

The System Administrator needs to enter their postal address, which is useful for contact and correspondence.

Company*

The System Administrator needs to specify the name of the company or organization they are associated with.

Postal Code*

The System Administrator needs to provide the postal code or ZIP code associated with their address.

Country*

To enhance accuracy and ensure compatibility, the platform offers a user-friendly approach.

When the System Administrator enters the input field for the country. Instead of manually typing the country name, the system provides a convenient drop down menu that dynamically fetches a comprehensive list of countries using an API. So, The System admin can easily select their country of residence or operation from this list.

State*

Upon selecting the country, the platform dynamically fetches a list of states or regions specific to the chosen country. The system Administrator can select the appropriate state from this list.

City*

Similar to the state field, the city field presents a drop-down menu that dynamically populates the available cities based on the selected state. System Administrators can select their city from this list.

Roles*

During self-registration, System Administrators are asked to choose their roles from a drop-down menu that contains the predefined list of basic profiles. Selecting a role helps us better understand their professional position within their organization.

CEO
CTO
Administrator
IT Manager
Business Development Manager
Sales Manager

User Notification

After successful registration, Administrators will be presented with a popup message confirming the successful creation of their account. This popup serves as a notification that their account registration process has been completed successfully.

This popup includes essential details and instructions, such as a button labelled "Let’s Get Started." By clicking on this button, the system administrator will be seamlessly redirected to the login page of the CRM system.

Inactive User

In addition to the confirmation message, the platform sends a verification email to the provided email address. The verification email is an essential step in the registration process as it ensures the authenticity of the account and confirms the validity of the email address.

The accounts remains inactive until system admin will verify their account through the provided email address.

Two-Factor Authentication

By Implementing two-factor authentication (2FA) module using a QR code to log into a Customer Relationship Management (CRM) system is a security measure that adds an extra layer of protection to user accounts. Here’s how this process typically works:

Assign Two Factor Authentication

Login Module - User Flow Diagram

System Admin will be able to enable the Two-Factor Authentication against each pre-defined profiles within the CRM system by navigating to their security settings or preferences.

Username and Password

The user initiates the login process by entering their username and password on the CRM login page.

User Verification

The CRM system verifies the entered username and password against its database to ensure they are correct.

QR Code Request

After successfully verifying the username and password, the CRM system shows the unique QR code that is generated against the session and it will regenerate after each 15 seconds in case of timeout.

Scanning the QR Code

Using the 2FA authentication app, users scan the QR code displayed on the CRM login screen.

Code Generation

Once the QR code is scanned, the 2FA app links to the user’s CRM account and begins generating time-based one-time passwords (TOTPs).

Access Granted

If the TOTP provided by the user matches the one generated by the app at that moment, they gain access to their CRM account.

Forgot Password

This module allows system administrators to regain access to their accounts in the event of a forgotten password. The password recovery process follows these key steps:

Password Recovery Request

Navigate to the login screen and clicks on Forgot Password button that leads to page on the platform and initiate a password recovery request by providing their registered email address.

Email Verification

The system verifies the provided email address against the stored system administrator database to ensure its validity and association with an existing account.

Password Reset Link

Upon successful email verification, the system generates a unique password reset link and sends it to the system administrator’s registered email address. This link is time-limited up-to 15 minutes to ensure security and prevent unauthorized access.

Incorrect Email Address

In case of an incorrect email address that does not match any existing email addresses stored in the system, an error message will be displayed in the form of a popup. The error message will indicate that the email address entered is incorrect or not found. This notification serves to alert the system administrator that the provided email does not correspond to any registered accounts in the system.

User Notification

System Administrator receives an email containing the password reset link, along with instructions on how to proceed with resetting their password. The email also emphasizes the importance of keeping the password reset link confidential.

Password Reset Page

Clicking on the password reset link button redirects to a secure password reset page on the platform. This page prompts the system administrator to enter a new password.

New Password Creation

System Administrators are required to create a new password that meets the platform’s password complexity requirements. The password should typically include a minimum number of characters, a combination of uppercase and lowercase letters, numbers, and special characters.

Successful Password Reset

Once system administrators submit their new password, the system securely updates their account with the newly chosen password.

System Administrators are then notified of the successful password reset and prompted to log in using their updated credentials.

Personal Information

When the System Administrator successfully logs in to their designated dashboard, they will find an option in the top right corner. Under the profile menu, they will be able to manage the following things, Manage Profile: View and Edit Personal Details:

The "Personal Details" section of the platform empowers administrators to view and modify their personal information for accurate record-keeping and profile management.

Within this section, administrators can access and update the following fields such as:

First Name

Last Name

Username (Changes the process of updating username)

Email

Phone Number

Password

Address

Company

Postal Code

Country

State

City

Logout Feature:

The platform provides a Logout feature conveniently located under the profile menu. By selecting this option, the System Administrator can securely log out from their account, ensuring data privacy and enhancing the overall security of the CRM system.

This feature offers a simple and effective way for the administrator to end their session and protect sensitive information when necessary

Personal Information

When the System Administrator successfully logs in to their designated dashboard, they will find an option in the top right corner. Under the profile menu, they will be able to manage the following things,

Manage Profile: View and Edit Personal Details:

The "Personal Details" section of the platform empowers administrators to view and modify their personal information for accurate record-keeping and profile management.

Within this section, administrators can access and update the following fields such as:

First Name

Last Name

Username (Changes the process of updating username)

Email

Phone Number

Password

Address

Company

Postal Code

Country

State

City

Logout Feature:

The platform provides a Logout feature conveniently located under the profile menu. By selecting this option, the System Administrator can securely log out from their account, ensuring data privacy and enhancing the overall security of the CRM system.

This feature offers a simple and effective way for the administrator to end their session and protect sensitive information when necessary.

Profile Management

In the CRM system, the Profiles Management feature empowers system administrators to finely control access permissions related to apps, system configurations, and side menu settings. System administrators create profiles as templates, each pre-configured with specific permissions. These permissions dictate the extent of access and functionality granted to all users linked to these profiles. The Profiles Management module includes the following key functionalities:

Profile Creation

When adding a profile, the following steps and options are available:

Enter Profile Name:

To create a new profile in the CRM system, the System Administrator initiates the process by clicking on the ’Add Profile’ button.

This action triggers the appearance of a modal window, prompting the System Administrator to enter the desired profile name and then proceed with saving it.

Validation:

Profile name must be unique and profile does not create if the profile already exists with the same name. This serves as a label to identify and distinguish the profile from others within the CRM system.

If an system administrator attempts to create a profile with a name that already exists in the system, a validation error occurs, and a prompt displays an error message stating "Profile Name should be Unique."

Roles Management - User Flow Diagram

The profile name field must be completed and cannot be left empty. When a user attempts to proceed without filling in such a field, the system will prompt the user to provide the necessary information. For instance, if the field is left blank, the system will display a prompt urging the user to enter their name before proceeding.

Successful Profile Creation:

Upon successfully creating a profile, system administrator receive a confirmation message in the form of a popup, indicating that the profile has been successfully added to the system. This notification ensures that system administrator is aware of the successful profile creation and can proceed with further actions.

After the profile creation, the system automatically redirects the administrator to the detail page of the newly created profile.

From this detail page, he can manage following things,

App Settings - Permissions:

In this section, the System Administrator can assign specific apps to a profile. Once an app is assigned to a profile, all users associated with that profile gain access to various features, including app editing, module management, view customization, view type selection, section and field management, among others. In this section, the System Administrator can efficiently manage the following aspects:

Assigned Multiple Apps:

The Administrator navigates to the app assignment section. Within this section, he will find a list of available apps along with check boxes next to each app name. By selecting the check-boxes for the desired apps, the Administrator can assign those apps to the profile and that apps would be accessible to all the users that are lies under that profile.

By Default (Only One): By this Feature, Administrators can specify that only one default app is assigned to the profile, ensuring a focused user experience.

Visible (Multiple): Administrators can choose to make multiple apps visible to the profile, allowing users assigned to the profile to access and utilize those apps.

System Settings - Permissions:

In this section, administrators can configure various permissions related to system settings for the profile. These settings reflects the same to all the users that are associated with that profile. The following options are available within this section:

Allow two-Factor:

System Administrator can enable or disable the two-factor authentication for profiles by clicking the check box present next to “Allow Two Factor“ to enhanced security.

Enabling the checkbox triggers the display of a QR code.

Users will see this QR code on their screen after entering their username and password during their next login, once two factor authentication is enabled.

The QR code is regenerated automatically after a specific duration of time. This periodic regeneration enhances security by providing users with fresh QR codes at regular intervals.

Users need to install a 2FA authentication app (e.g., Google Authenticator, Authy, Microsoft Authenticator) on their trusted mobile device to scan the QR code.

Password expire in (Days):

This field display the drop-down menu with these options from which the System Administrator can set the minimum and maximum number of days for password expiration for a specific profile. This policy implements on all the users associated with the selected profiles on which the system administrator enables this feature:

30 days
60 days
90 days
180 days
One year
Never Expires

Password Expiration Policy: System Administrator can configure password expiration policies for different profiles. For instance, they can set a policy that requires users to change their passwords every 90 days.

User Login: Let’s say a user logs in for the first time with their initial password. The CRM system recognizes that this password has an expiration policy and calculates the date when it will expire based on the policy settings.

Notification Period: Salez.Ai typically provides users with a notification period before their password expires. This is often set a few days before the actual expiration date, for example, five days. During this notification period, if a user logs in (let’s say on the 85th day since their last password change), they will receive a notification.

Password Change Process: When the user follows the link or prompt, they are taken to a password change page. Here, they must enter their current password (the one that’s about to expire) and then create a new, secure password that meets the organization’s password policy requirements (e.g., a combination of letters, numbers, and special characters).

Successful Change: Once the user successfully changes their password, they can continue to access Salez.Ai as usual with the new password. The password expiration date is reset based on the policy settings, starting from the date of the password change.

Expired Password: If the user does not change their password during the notification period and the password expires, they will not be able to log in. They'll be locked out of their account until they follow a password reset process, they will see the modal at the time of the login to their account to setup your new password with the following fields,

Enter New Password

Confirm New Password

New Expiration Date: If password expiration policy is set for 90 days, and the user change his password on the 30th day, then new password's expiration date should be calculated from the date the user changed it. New password's expiration date would be 90 days from the date when user changed his password.

Invalid login attempt:

Administrators can define the minimum and maximum number of invalid login attempts allowed for each profile. These login attempts validation implements on all the users associated with that profile. After exceeding this limit, they may be locked out of their accounts temporarily and they needs to contact the administrator to regain the access again.

This field display the drop-down menu that contains the following number of attempts that are allowed to try. The invalid login attempts that are display in the drop-down menu are,

3

5

10

No Limits

Minimum password length:

Administrators can specify the minimum and maximum required length for passwords associated with the profile, ensuring adherence to password security best practices. The same validation implements on all the users associated with that profile.

The minimum and maximum required length for passwords are,

8 characters

12 characters

16 characters

Report create:

Administrators can grant or restrict the ability to create reports assigned to the profile by enabling or disabling this option.

Report run:

Administrators can determine whether profiles can run reports or not by enabling or disabling this option.

Edit Mode Access:

Administrators possess the capability to control access to the Edit Mode Screen for specific profiles by toggling a checkbox.

Enabling the checkbox grants the profile access to the Edit Mode Screen of the corresponding app, whereas disabling the checkbox restricts this access. When the checkbox is disabled, the toggle button for entering the Edit Mode Screen becomes unavailable for that particular profile.

Side Menu Settings (Assigned items in the side menu):

In profile management, administrator can access the Side Menu Settings section, where they will find a list of menu items corresponding to various functionalities and features.

The Administrator can easily restrict the users that are associated with the profiles to a certain level of permissions and visibility by using the check box that is shown against each menu item in the Side Menu Settings

When a checkbox is selected, it indicates that the corresponding menu item is visible and accessible to the user associated with that profile. Conversely, when a checkbox is deselected, it restricts the visibility and access of that menu item for all that users that belongs to that profile.

The menu items that can be managed in the Side Menu Settings section using the Checkbox includes:

Apps
Dashboard
User Management
User List
Profiles
Roles
Groups
Setting
App settings
Web to lead
Lead Mapping

List All Profiles

The CRM system provides a comprehensive feature to list all profiles within the platform. When accessing the "List All Profiles" section, system administrator is presented with a table or list displaying the profiles. The following information is typically included for each profile:

Date of Creation:

This column displays the date on which the profile was created by the system administrator. It provides them with a reference point for understanding the timeline of profile creation.

Name:

The name column showcases the unique identifier or label assigned to each profile. It helps system administrator quickly identify and differentiate between different profiles.

Action (Update & Modify Profile):

Under the action column, system administrator can perform various actions specific to each profile. These actions typically include options to update or modify settings associated with the profile. For each profile, The system administrator has the option to updates the following settings and permissions:

App Settings
Updated Assigned Apps
System Settings
Allow two-Factor
Password expire in (Days)
Invalid login attempt
Minimum password length
Report create
Report run
Edit Mode Access
Side Menu Settings

The menu items that can be managed in the Side Menu Settings section using checkboxes include:

Apps
Dashboard
User Management
User List
Profiles
Roles
Groups

Setting

App settings

Web to lead

Lead Mapping

Filters

Search Filters

The CRM system incorporates a powerful filtering feature that allows administrators to refine their search and retrieve specific profiles based on various criteria. The Filters functionality within the CRM system includes the following options:

Filter By Name

The System Administrator can apply a name filter to search for profiles by entering specific keywords or names associated with the profiles. This filter typically provides an input field where they can enter the desired name or keyword to narrow down the search results.

Filter By Date

The CRM system offers a date filter that allows administrators to filter profiles based on the date of creation. This filter is typically facilitated through a calendar interface where they can select a specific date or a range of dates to filter the profiles accordingly.

Reset Filter

To clear all applied filters and start a new search, Administrators can utilize the "Reset Filter" option. This function removes any previously set filters and resets the profile list to its original state, enabling them to perform a fresh search without any applied filters.

User List Management

User List Management in the CRM system refers to the functionality that allows administrators or authorized users to view, organize, and manage the list of users within the platform. It provides a centralized view of all users and their associated details, facilitating efficient user administration and access control. The User List Management typically includes the following features:

Search Filters

User List Management in the CRM system includes various filters and options to effectively manage and search for users. The following features are available:

Filter By Name:

Administrators can apply a name filter to search for specific users by entering specific keywords or names associated with the users. This filter typically provides an input field where users can enter the desired name or keyword to narrow down the search results.

Filter By Date:

The CRM system offers a date filter that allows users to filter users based on the date of creation. This filter is typically facilitated through a calendar interface where Admins can select a specific date or a range of dates to filter the profiles accordingly.

By All:

This option allows admin to view all user profiles without any specific filtering criteria. Within the "By All" filter option, users have additional sub-options to further refine their search:

All:

This option displays all user profiles, regardless of their verification status.

Verified:

This option shows only the user profiles that have been verified.

True:

This option filters the user profiles to display only those with a "true" status based on a specific attribute or condition.

False:

This option filters the user profiles to display only those with a "false" status based on a specific attribute or condition.

Reset Filter:

To clear all applied filters and start a new search, users can utilize the "Reset Filter" option. This function removes any previously set filters and resets the profile list to its original state, enabling users to perform a fresh search without any applied filters.

List All Users (Created By Admin)

The CRM system provides a comprehensive list of all users created by the administrator. This user list displays important details for each user profile, including

Name:

The name of the user, which could include the first name and last name.

Username:

The unique username associated with the user’s account. This is used for authentication and login purposes.

Email:

The email address registered for the user’s account. This serves as a primary contact method for communication.

Phone Number:

The phone number provided by the user during registration. This contact information allows for direct communication if required.

Date of Creation:

The specific date when the user profile was created in the CRM system. This information helps in tracking the timeline of user registrations.

Verified:

It indicates whether a user’s email address has been verified or not. This field serves as a status indicator to determine if the user has completed the email verification process.

Freeze:

There is a "Freeze" field that allows administrators to see the statuses of the user accounts whether they are frozen or not. If the user can exceed the number of the Invalid login attempts then their accounts would be temporarily frozen. The "Freeze" field serves as a control mechanism to temporarily restrict the functionality or access of a user account.

Actions:

View:

The "View" action allows administrators to access and view the details of a specific user account. By selecting the "View" option, administrators can retrieve information such as the user’s name, email address, phone number, role, and other relevant details.

Edit:

The "Edit" action enables administrators to modify and update the information associated with a user account. By selecting the "Edit" option, administrators gain access to an editable form or interface where they can make changes to fields such as the user’s name, email address, phone number, role, and other relevant details.

Add New User

To streamline the process of adding new users to the CRM system, an intuitive interface is provided. When adding a new user, the following fields are required to be completed:

First Name

Last Name

Username

Email

Phone Number

Password

Address Line

Company

Postal Code

Country

State

City

Role Type:

The assigned role for the user, chosen from a list of available roles fetched from the system.

Assign Profile:

The selected profile to assign to the user, chosen from a list of available profiles fetched from the system.