

The system shall enable users (Passengers) to initiate the creation of new accounts.

UC Name	<i>User Account Creation UC-201</i>
Summary	<i>Enabling passengers to create new accounts within the system.</i>
Dependency	<i>None</i>
Actors	Primary Actor: User (Passenger) Secondary Actor: System
Preconditions	<i>1. The user attempts to sign up using personal information.</i> <i>2. The user's unique account identifiers (email) do not match with another user's in the system.</i> <i>3. The user agrees to the terms and conditions of service before proceeding with the sign-up process.</i> <i>4. The user provides all required information fields (such as name, email, password) during the sign-up attempt.</i>
Description of the Main Sequence	<i>Step 1: The user navigates to the sign-up page on the system.</i> <i>Step 2: The user fills in the required personal information such as name, email address, and password.</i> <i>Step 3: The system validates the entered information to ensure all required fields are filled correctly.</i> <i>Step 4: The system checks if the provided email address is unique and not already associated with an existing account.</i> <i>Step 5: If the email address is unique, the system sends a verification email to the provided address.</i> <i>Step 6: The user receives the verification email and clicks on the verification link to confirm their email address.</i> <i>Step 7: Upon email verification, the system creates a new account for the user.</i> <i>Step 8: The user receives a confirmation message indicating successful account creation.</i> <i>Step 9: The user can now log in to the system using their email address and password.</i>
Description of the Alternative Sequence	Alternative Sequence 1: If the email address provided is already associated with an existing account, the system prompts the user to choose a different email address or attempt to recover their existing account.

	Alternative Sequence 2: If any errors occur during the sign-up process, such as invalid information or technical issues, the system provides appropriate error messages and prompts the user to correct the issues and try again.
Non functional requirements	<p>Security: The security requirement for the sign-up process ensures the protection of user accounts and sensitive information from unauthorized access and potential breaches.</p> <p>Performance: The authentication process is expected to conclude within a specified duration of seconds.</p> <p>Scalability: The authentication database system should be capable of handling a large number of accounts.</p>
Postconditions	<ul style="list-style-type: none"> • If account creation is successful, user should be able to login with their registered information. • In case account creation fails, user shall not be able to login.

The system shall provide users (every level) with the ability to securely authenticate and access their accounts.

UC Name	<i>User Account Log-In UC-202</i>
Summary	<i>Enabling passengers to securely access their accounts within the system.</i>
Dependency	<i>User Account Creation (UC-201)</i>
Actors	Primary Actor: User Secondary Actor: System
Preconditions	<p><i>1.The user has already created an account (passenger) with the system or has been given one by the admin (privileged user).</i></p> <p><i>2.The user possesses valid login credentials, including a registered email address and password.</i></p> <p><i>3.The user has agreed to the terms and conditions of service before attempting to log in.</i></p> <p><i>4.The system is operational and accessible for user login.</i></p>

Description of the Main Sequence	<p><i>Step 1: The user enters their credentials to log in to the system.</i></p> <p><i>Step 2: The system verifies the provided credentials against the stored user data.</i></p> <p><i>Step 3: If the credentials match an existing user account, the system grants access to the user.</i></p>
Description of the Alternative Sequence	<p>Alternative Sequence 1: If the credentials do not match or are invalid, the system denies access and prompts the user to try again or reset their password.</p> <p>Alternative Sequence 2: If any errors occur during the log-in process, such as invalid information or technical issues, the system provides appropriate error messages and prompts the user to correct the issues and try again.</p>
Non functional requirements	<p>Security: The security requirement for the login process ensures the protection of user accounts and sensitive information from unauthorized access and potential breaches.</p> <p>Performance: The authentication process is expected to conclude within a specified duration of seconds.</p> <p>Scalability: The authentication database system should be capable of handling a large number of accounts.</p>
Postconditions	<ul style="list-style-type: none"> 1. If the user's credentials are validated successfully, the user gains access to their account. 2. Upon successful login, the system may redirect the user to their account dashboard or another designated landing page. 3. If the user's credentials are invalid, the system denies access and provides appropriate error messages. 4. After a specified number of unsuccessful login attempts, the system may lock the user's account for security purposes. 5. The system logs the login activity, recording successful and unsuccessful login attempts for security auditing purposes.

The system shall grant administrators the capability to create new specialized permission accounts, edit permissions, delete or reset password for users.

UC Name	<i>Admin Account Management UC-203</i>
Summary	<i>Enabling administrators to manage accounts (create, edit permissions, delete, password reset) for privileged users.</i>
Dependency	<i>None</i>
Actors	Primary Actor: User (Admin) Secondary Actor: System
Preconditions	<ol style="list-style-type: none"> <i>1. The administrator has appropriate access privileges and permissions to create, edit permissions, delete accounts or reset password for a specified account.</i> <i>2. The administrator is logged into the system.</i> <i>3. The system is operational and accessible.</i> <i>4. The administrator possesses all necessary information required to create , edit or delete the accounts, including user details and assigned permissions.</i>
Description of the Main Sequence	<p><i>Step 1: The administrator accesses the account management section of the system.</i></p> <p><i>Step 2: The administrator chooses the service he wants to do: create new account, edit an already existing account or delete an account.</i></p> <p><i>Step 3:</i></p> <p><i>*In case of account creation:</i></p> <p style="padding-left: 40px;"><i>--1: The administrator selects or defines the special permissions for the new account.</i></p> <p style="padding-left: 40px;"><i>--2: The system validates the entered information to ensure accuracy and completeness.</i></p> <p style="padding-left: 40px;"><i>--3: Upon successful validation, the administrator confirms the creation of the new account.</i></p> <p style="padding-left: 40px;"><i>--4: The system generates a confirmation message, indicating that the new account has been successfully created.</i></p> <p style="padding-left: 40px;"><i>--5: If applicable, the system sends a notification to the newly created account, providing login credentials and instructions.</i></p> <p><i>**In case of account permission edit:</i></p> <p style="padding-left: 40px;"><i>--1: The administrator modifies the permissions as</i></p>

	<p>required.</p> <p>--2: The system verifies the modified permissions and updates them for the selected account.</p> <p>--3: The system generates a confirmation message, indicating that the permissions have been successfully modified.</p> <p>***In case of account deletion:</p> <p>--1: The administrator navigates to the list of user accounts and selects the account to be deleted.</p> <p>--2: The system prompts the administrator to confirm the deletion action.</p> <p>--3: The administrator confirms the deletion of the selected account.</p> <p>--4: The system removes the selected account from the user database.</p> <p>--5: The system generates a confirmation message, indicating that the account has been successfully deleted.</p> <p>****In case of password reset:</p> <p>--1: The administrator navigates to the list of user accounts and selects the account for which the password needs to be reset.</p> <p>--2: The system prompts the administrator to enter a new password for the selected account.</p> <p>--3: The administrator enters the new password.</p> <p>--4: The system verifies the new password and updates it for the selected account.</p> <p>--5: The system generates a confirmation message, indicating that the password has been successfully reset.</p> <p>Step 4: The system logs the creation of the new account for auditing purposes</p> <p>Step 5: The administrator is returned to the main interface or account management section for further actions.</p>
Description of the Alternative Sequence	<p>Alternative Sequence 1: If during the account management process, the system encounters a critical error such as database connectivity issues or server malfunction, it halts the process, displays an error message informing the administrator of the technical issue, and advises them to attempt the process again later or contact technical support for assistance.</p>
Nonfunctional requirements	<p>-Reliability: The system should maintain consistent availability, minimizing downtime to ensure users can reliably</p>

	<p>access account management functionalities.</p> <ul style="list-style-type: none"> -Usability: The account management, interface should be intuitive and user-friendly, guiding administrators through the process with clear instructions and minimal complexity. -Scalability: The authentication database system should be capable of handling a large number of accounts. - Performance: The authentication process is expected to conclude within a specified duration of seconds. -Security: The security requirement for the account management process ensures the protection of user accounts and sensitive information from unauthorized access and potential breaches.
Postconditions	<ol style="list-style-type: none"> 1. Account is added/updated to the system's user database, allowing the administrator to manage its permissions and access rights. 2. The system generates a confirmation message, notifying the administrator of the successful account management. 3. If applicable, the system sends a notification to the account, providing login credentials and instructions on accessing the system if needed. 4. The account management event is logged in the system's audit trail, recording details such as the administrator responsible, timestamp, and any relevant metadata for auditing purposes. 5. The administrator is returned to the main interface or account management section, ready for further actions or tasks.