Administrative Guide
&
Daily Admin Activities

Ver 9.6

Dated Apr 10, 2023

SHE Technologies

Ph. 042 3740 1143

Table of Contents

Following are the Admin User Guide in sections and can implement by reading respective section.

1.1. IT - Administrator General Tasks

IT Administrator require to Manage & Perform the following task/Activities. IT Admin can take guidance from SHE Technologies Network and Support Team in this regard.

- Release Update (Update Exe / Queries)
- Read & Reply Emails
- Windows / Server Installation
- SQL Server Installation
- Server Preparation
- Client Machine Preparation
- Manual Database Backup
- Setting Auto database backup schedule
- Placing Database Backup on Safe Place
  (Externa Hard Drive / Separate Machine / Google Drive)
- Have a Testing Machine to Check release before update
- User Creation & Assigning Role / Rights
- Keep Software for installation
  - ALL DLLs
  - SQL Server Setup
  - Zoom , Any Desk ,Team Viewer

1.2. Sharing of Issues / Problems

Share your issues / problems and get fast feedback from our support team.

- Take **screen shot** of your Issues / Problem and send
  - Email support@shetechnologies.com
  - WhatsApp Group
- Take **about software** screenshot and send
- Take your **database backup** and send to email id backup4she@hotmail.com

1.3. End of Day / Close of Day

Perform the end of day activities

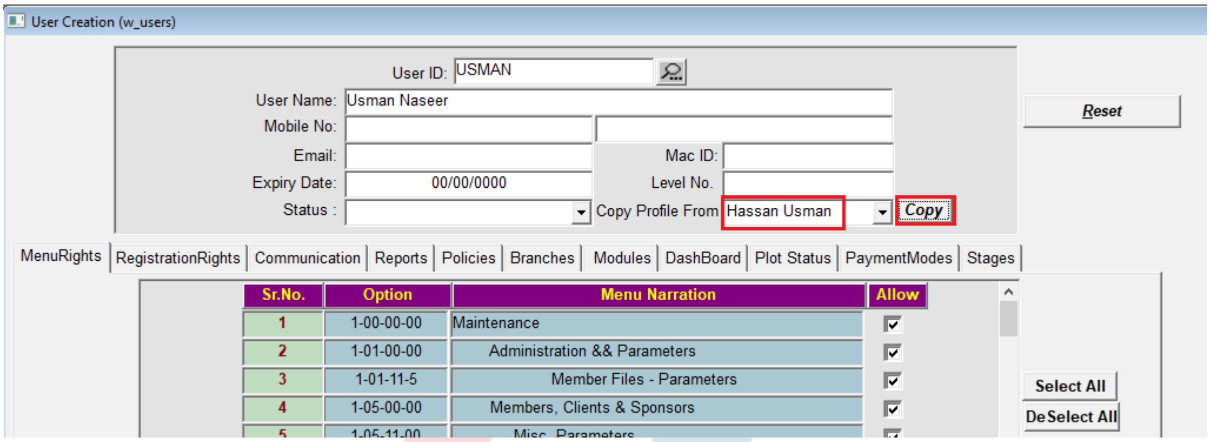
- Take Manual Database Backup + Check Auto Database Backup
- Copy Latest Today Backup at Safe Place

1.4. Create User

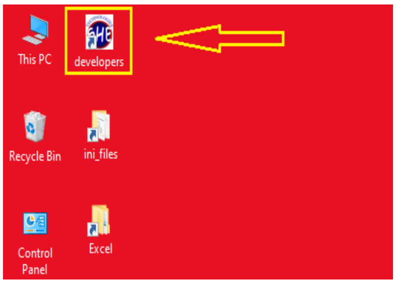
Maintenance → Misc. → User Parameters → User Creation

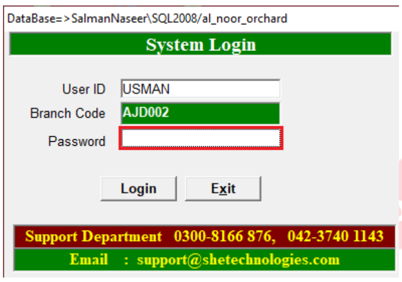
- Write User ID i.e USMAN
- Write User Name i.e Usman Naseer
- Level No. (1 to 51 for users, 52 to 999 for managers)
- Copy Profile From i.e. Hassan Usman
  (Select other user name and copy his rights to this user)
- Save

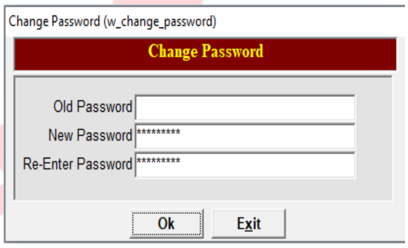
For how to assign user rights, Search and See **Section "**Assign User Rights**"**



- Open software + Login without Password + Set New Password
  (Leave old password blank for 1st time or if password is reset.
- It's done. Now User can Run software







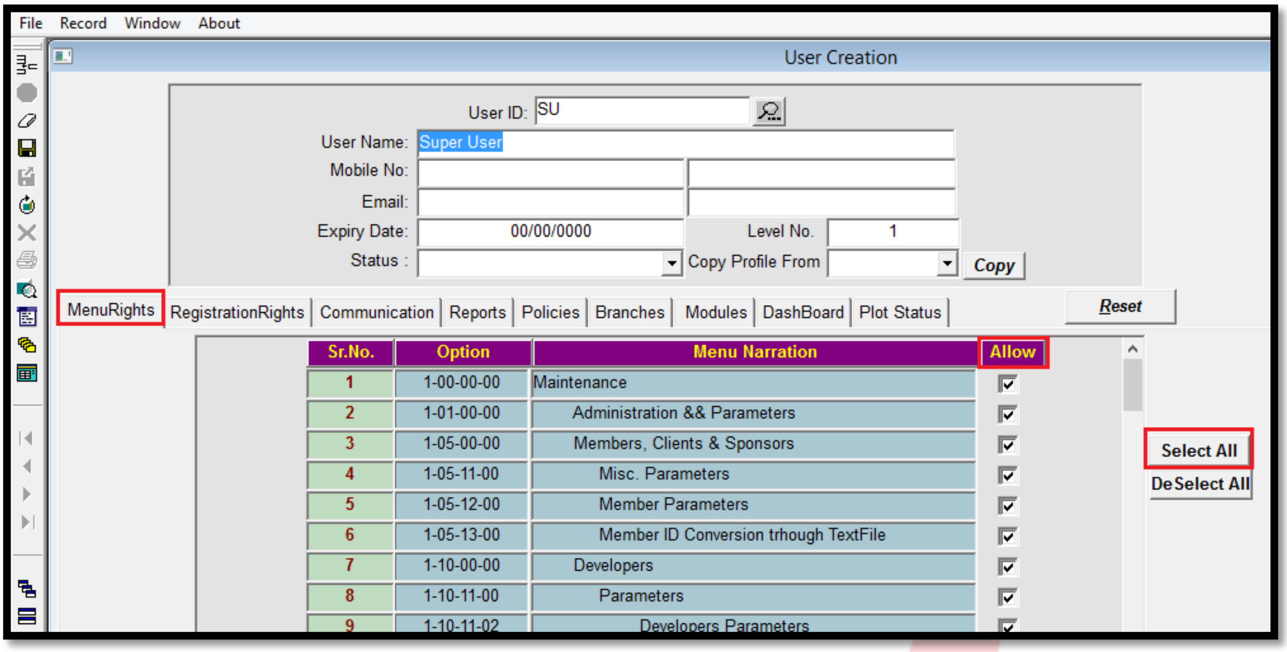
1.5. Assign User Rights

Maintenance → Misc. → User Parameters → User Creation

- Select User

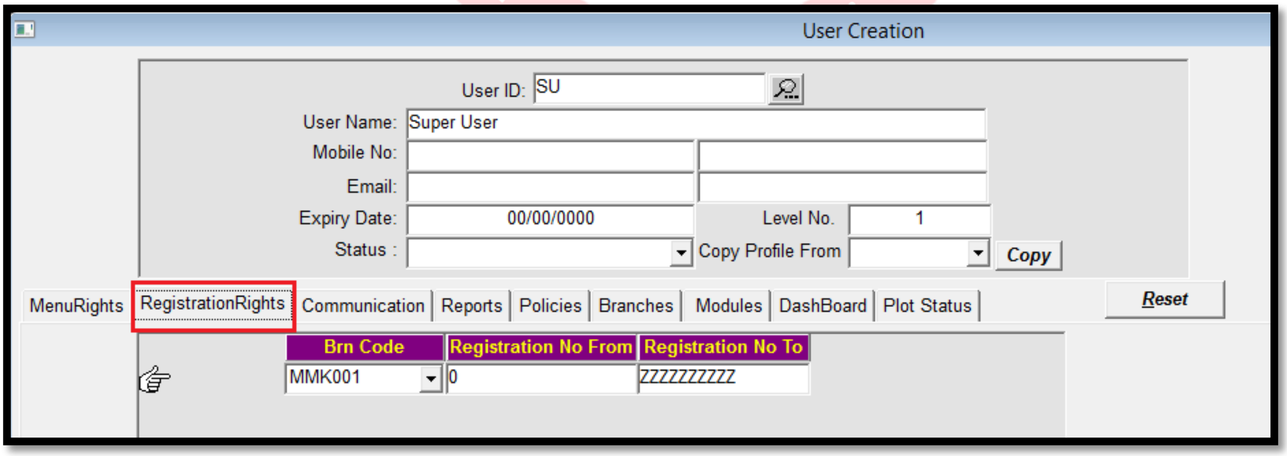
1.5.1. Menu Rights

- Click on the “MenuRights” tab.
- You can assign right by check/uncheck box against only particular Menus.

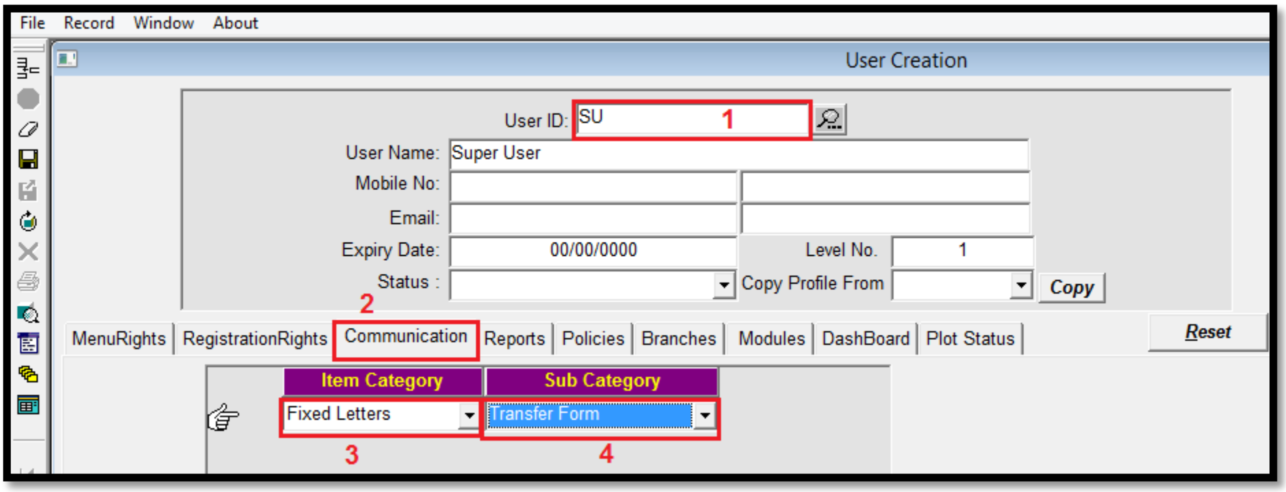


1.5.2. Rigistration Rights

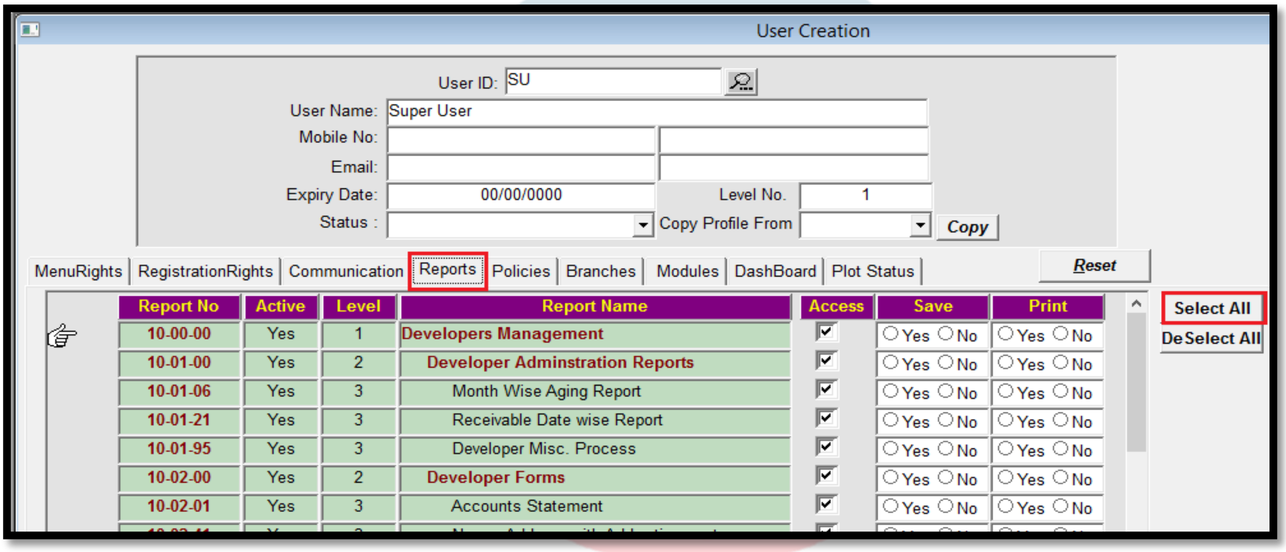
- Default Setting is 0 to zzzzz (This user can see this range of reg. nos.)



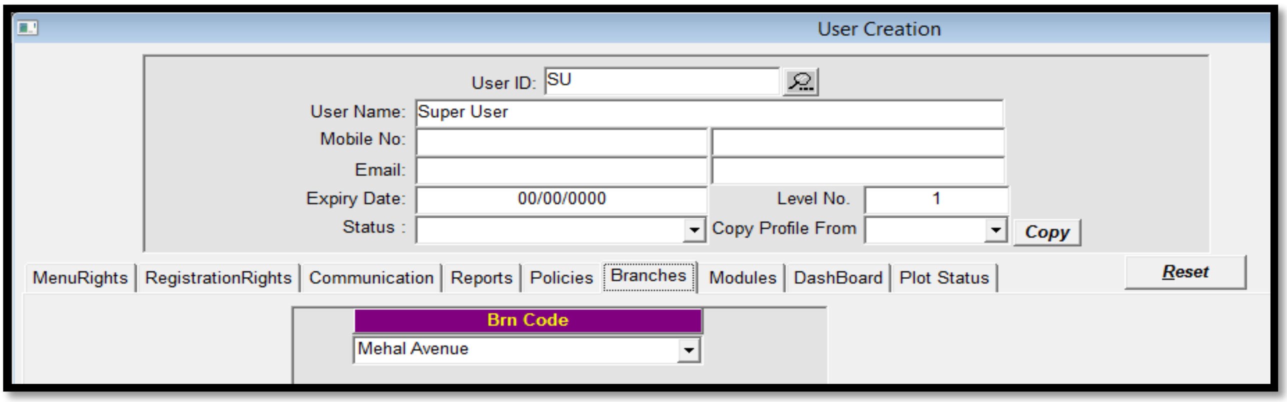
1.5.3. Letter Rights



1.5.4. Reports Rights

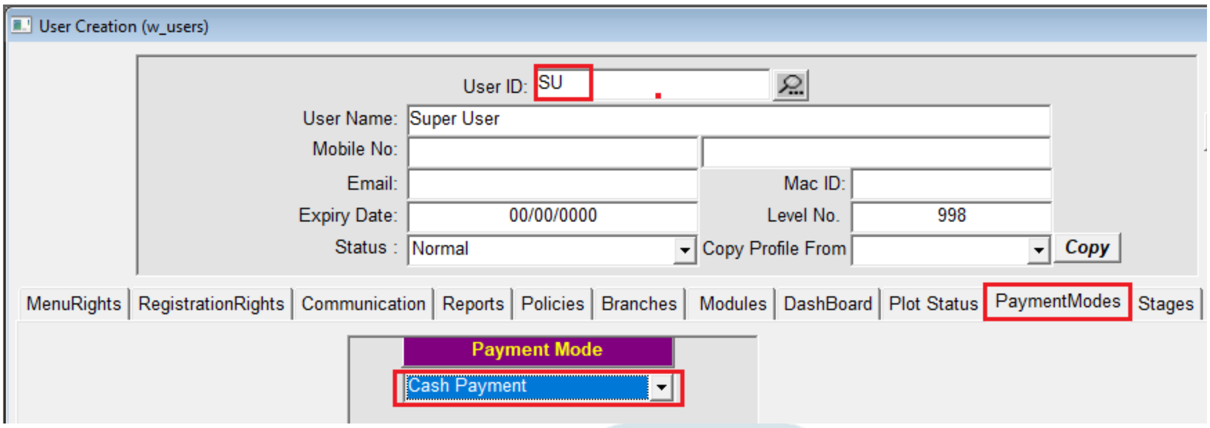


1.5.5. Branch Rights



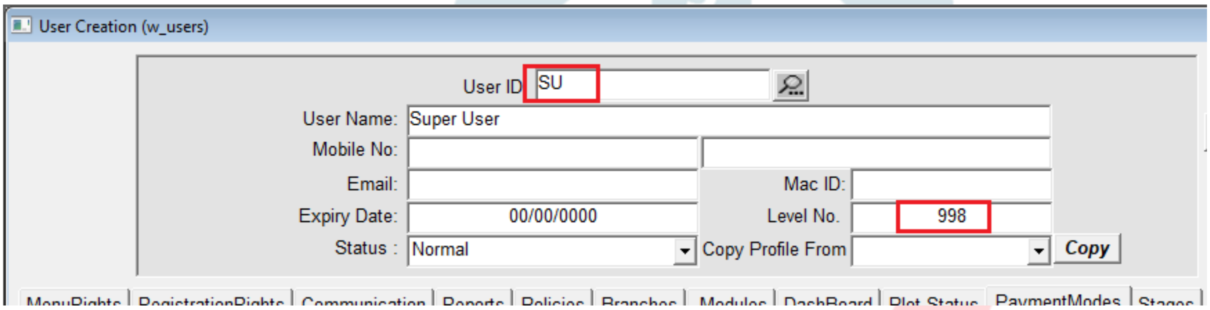
1.5.6. Payment Modes

- User can post receipts for any payment mode
- If you set “Cash Payment” means user can post only “Cash” mode receipts.
- You can assign multiple payment modes to any user.



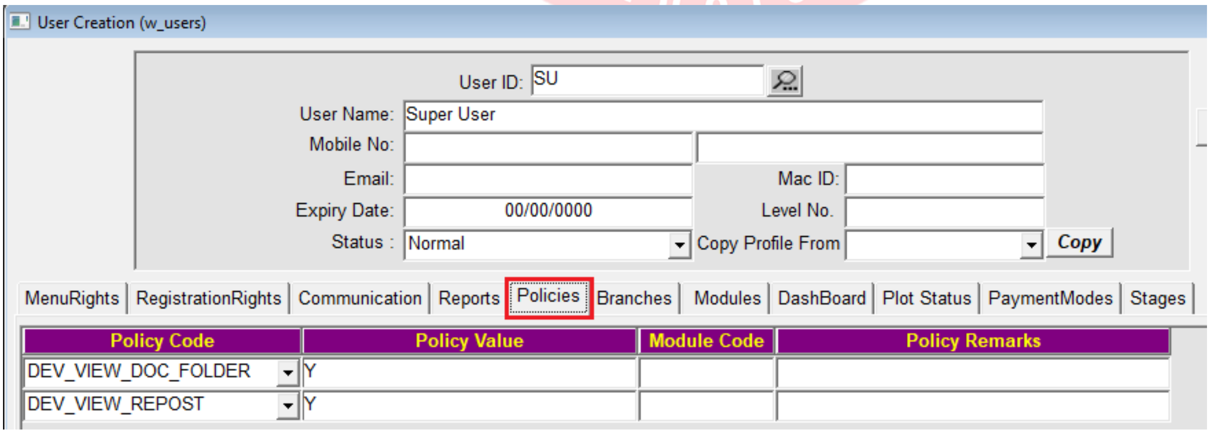
1.5.7. Level No

- User level from 52 and above can see Log of File in inquiry screen by Press (Alt + L).



1.5.8. User wise policies

- Select Policy Code
- Mark “Y” to Allow and “N” for restrict user.



1.6. Secure & Encrypt Users

Q1: What is secure user?

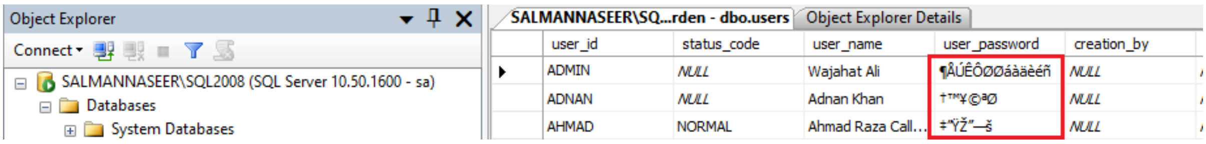
Ans: Secure User(s) means the SQL password of any user(s) is secret in SQL Logins

Q2: Purpose of secure user?

Ans: Secure from SQL Injection, Hacking, Etc.

Q3: What is Encryption?

Ans: Encryption means any she software user password is not visible at backend (SQL Database **Users** Table)

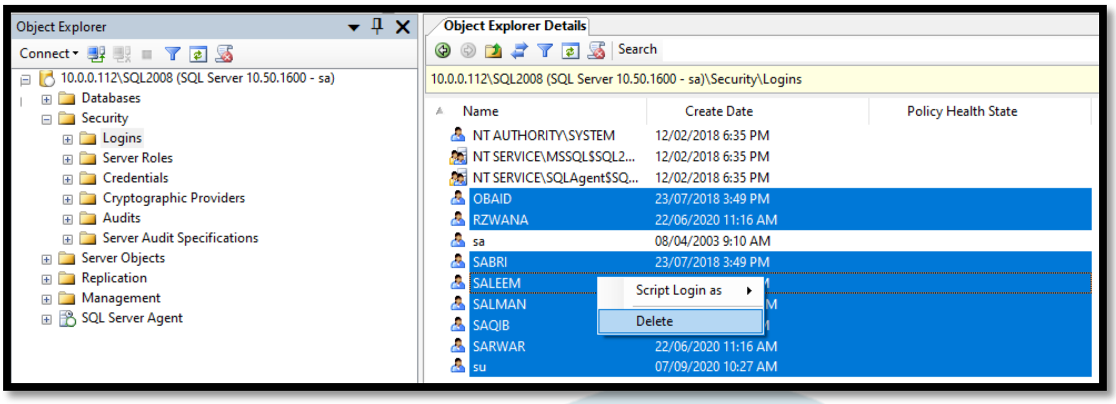


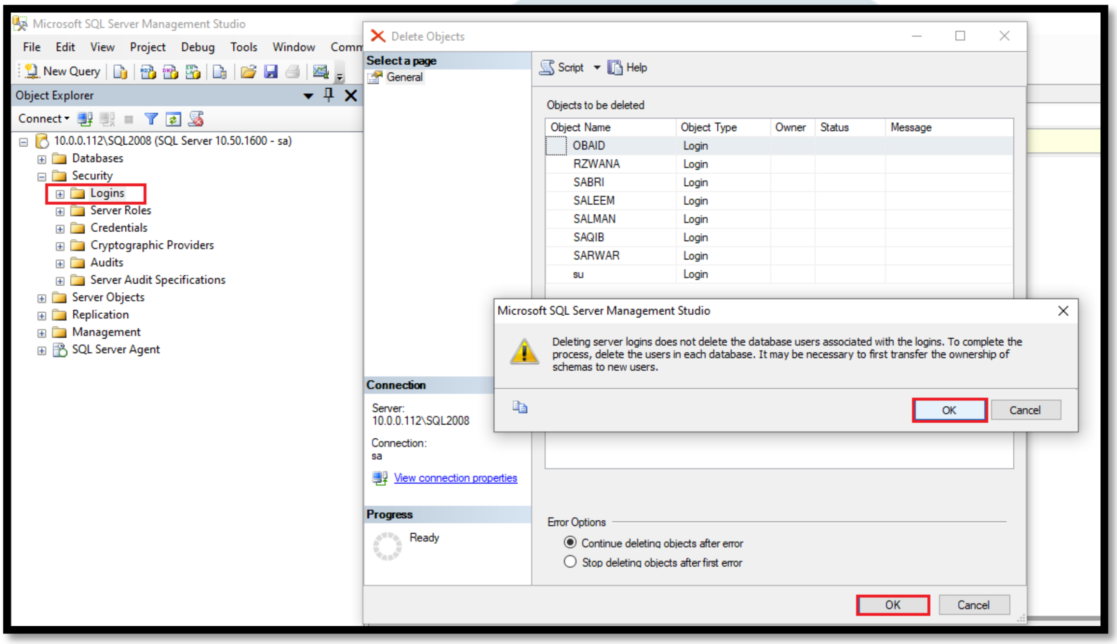
Q4: Purpose of Encryption?

Ans: Secure from SQL Injection, Hacking, Etc.

1.6.1. Before Make Secure Users – Delete SHE Software Users from SQL Logins

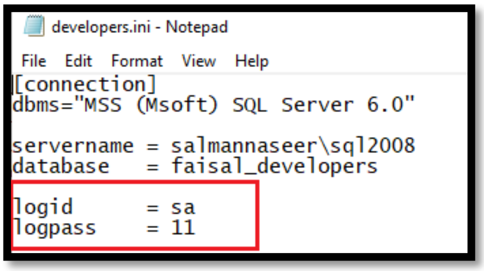
- Delete All SHE Software Users from SQL Security Logins (if already coming here)
  - Open SQL Server Management Studio
  - Security → Logins
  - Select SHE Users + Right Click + Delete + OK + OK



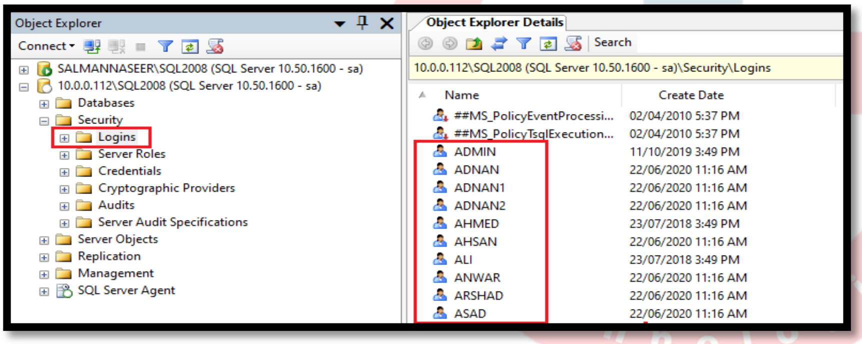


1.6.2. Secure & Encryption (Process)

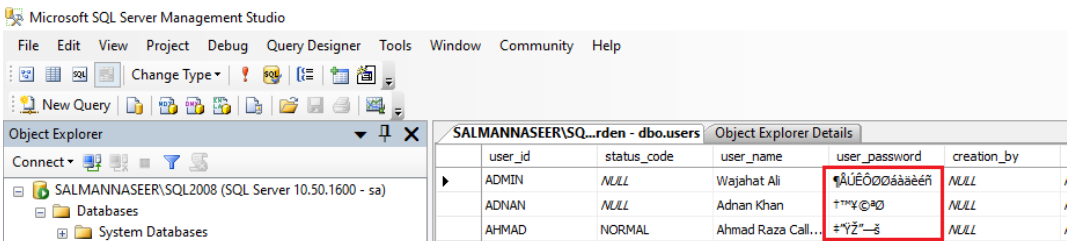
- Software Login with “**sa**” user
  (Use sa SQL password, See your sa password in developers.ini)



- Click Button “Secure Users” + OK (Now secureuid = Y)
  All SHE users will be re-created in SQL Logins



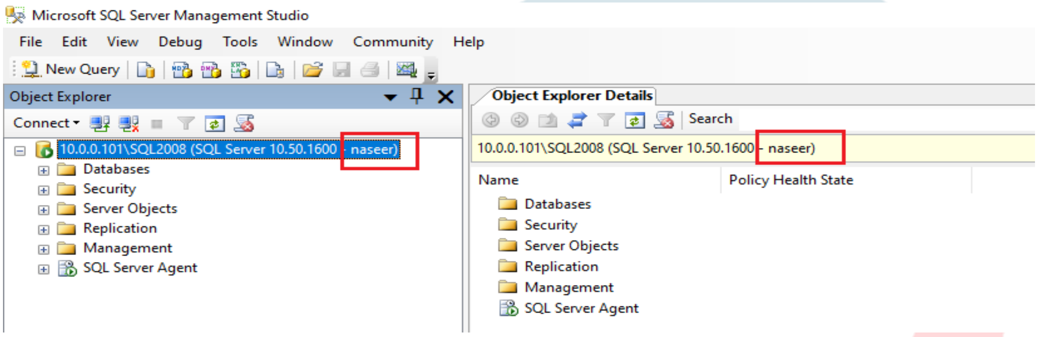
- Click Button “Encryption” + OK (Now encryption = Y)
  (This is one-time step, see in below screenshot password is not visible now)



1.6.3. How to Check Secure User (User is secure or Not?)

- Open SQL Server Management Studio
- Login Server with Secure User i.e. naseer (to check it is secure or not)
    - Login: Any she user i.e. naseer
    - Password: secret

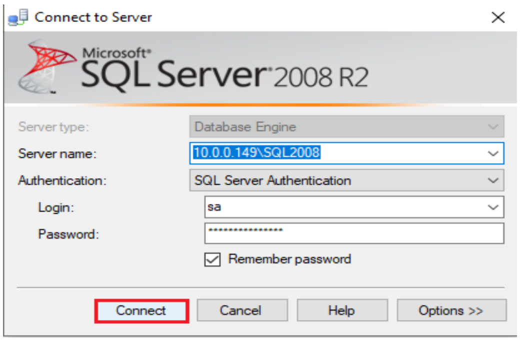
- If this is login by she user by fixed password "xxxxxxxx" then this is secure user. i.e. naseer in below screenshot



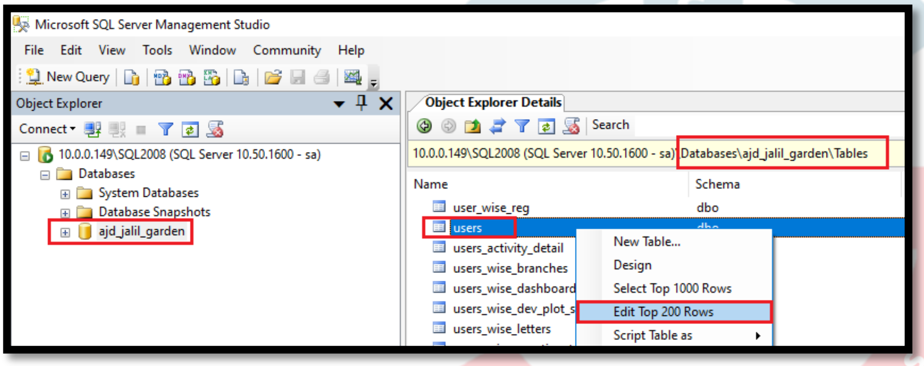
1.6.4. How to Check Encryption (User is Encrypted)

```
servername = salmannaseer\sql2008
database   = faisal_developers

logid      = sa
logpass    = 11
```

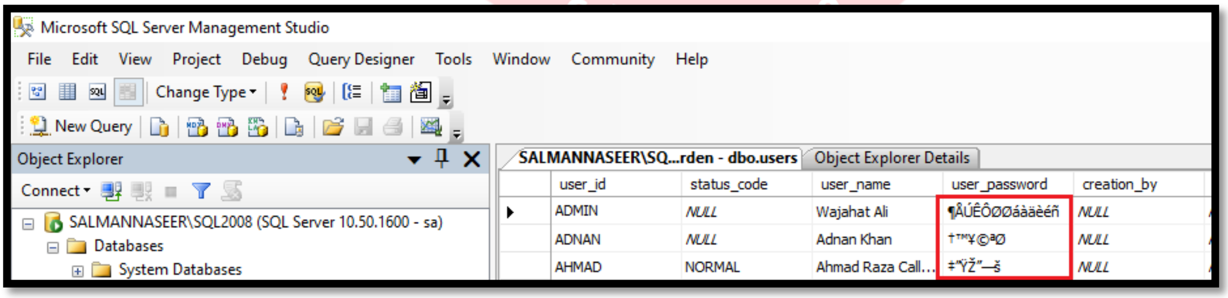
- Open SQL Server Management Studio
- Login Server
  - Login: sa
  - Password: 11 (see your sa password in developers.ini)



- Select Database + Press “F7”
- Open Tables + Right Click on **Users** Table
- Click “**Edit Top 200 Rows**”

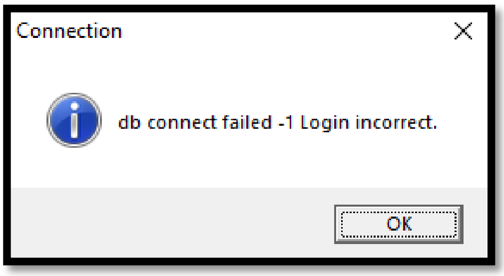


- See your users password are encrypted



1.6.5. User Login – Issues / Problems

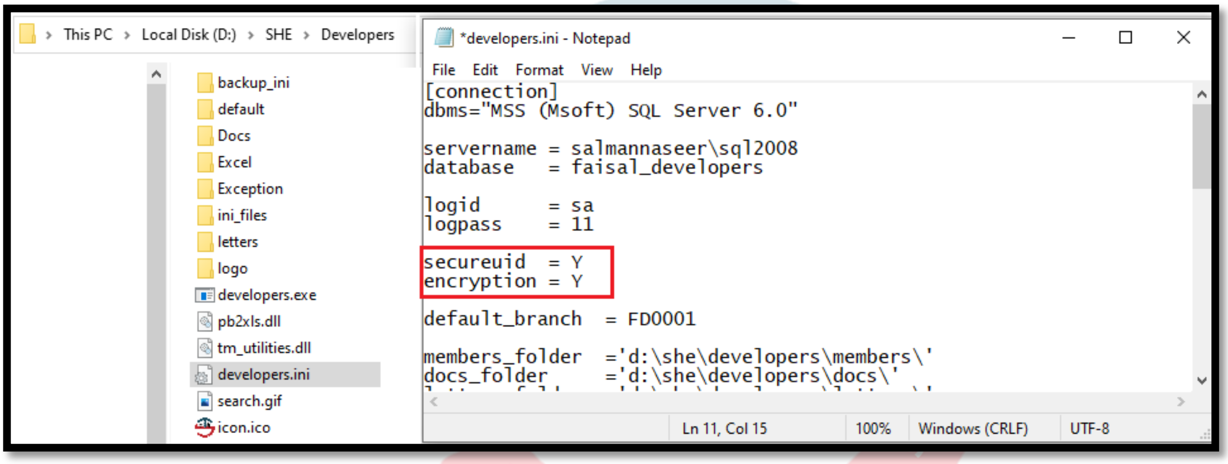
- If This message come when you login



You need to check your developers.ini settings (d:\SHE\developers\developers.ini)

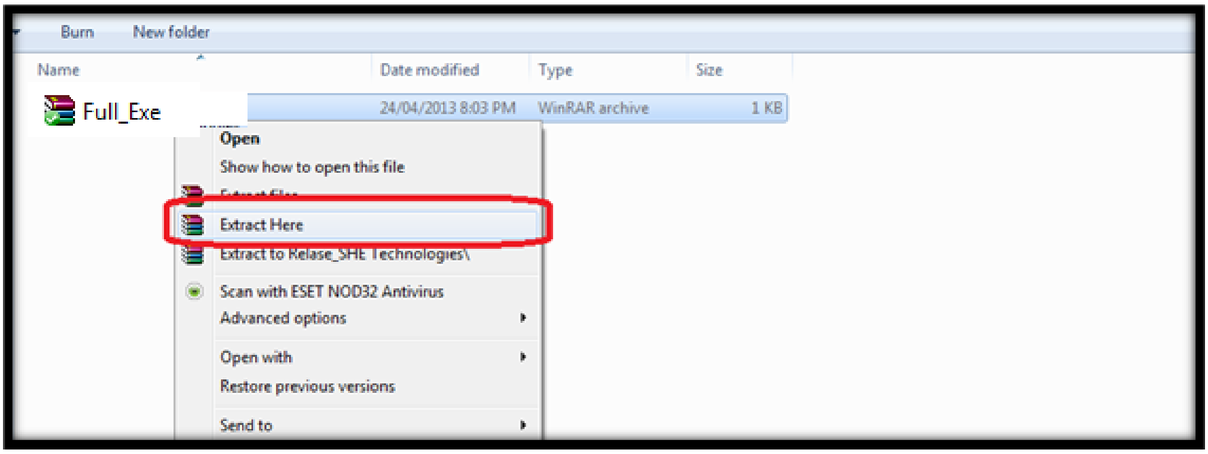
- **Check,** if your **user is secure user** then **secureuid = Y** otherwise **secureuid = N**
- **Check,** if your **users are encrypted** then **encryption = Y** otherwise **encryption = N**

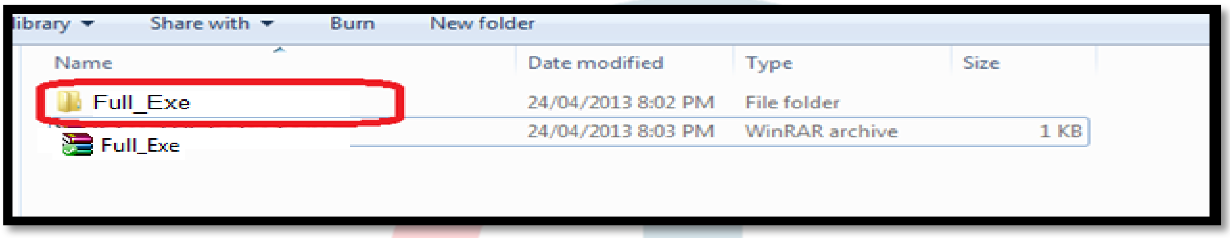
See section



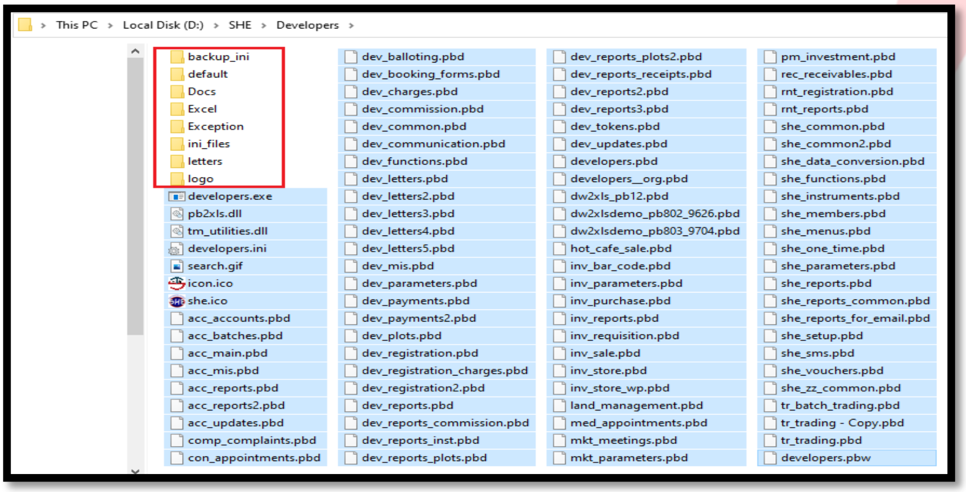
1.7. Software Installation

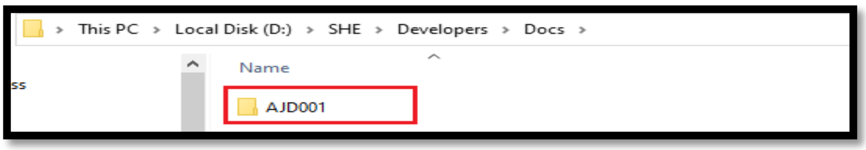
Get From Our Support Team the Full_Exe.rar and Extract It



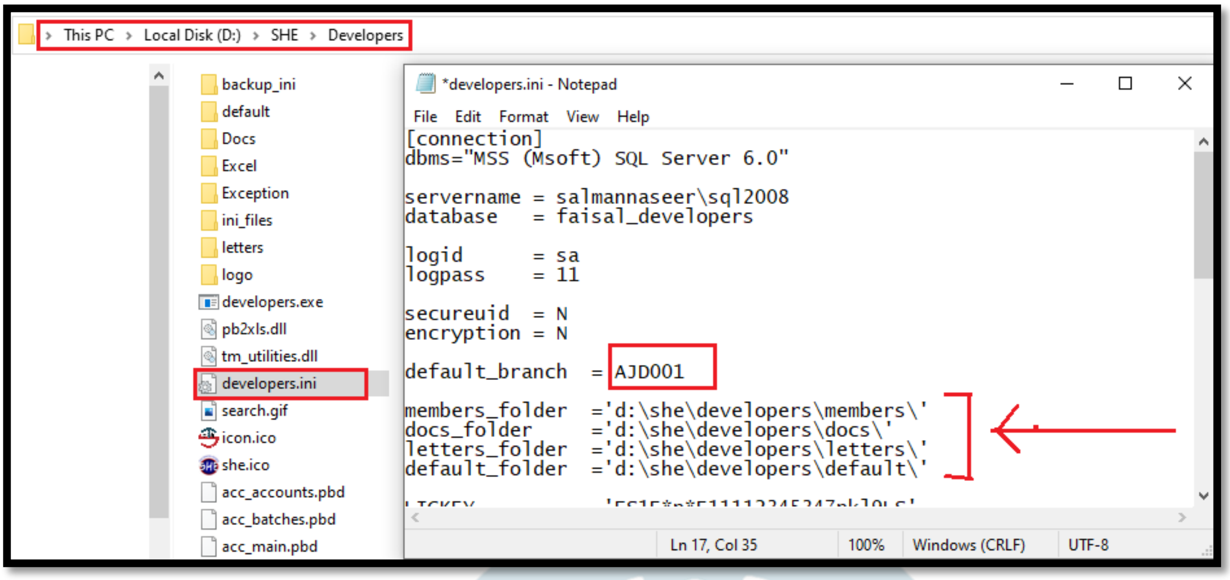


- From Full_Exe Folder, **Copy all files into d:\she\developers** (in server computer)
- **Make These Folders** in D:\SHE\Developers
  (Defualt, Docs, Excel, letters, logo, PDC)
- **Make Branch Code Folder** in All These Folders (Docs, Default, Letters, Excel, Etc)



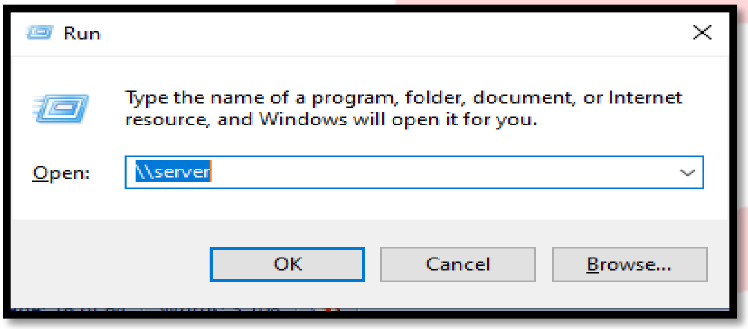


- **See your branch code** in your d:\she\developers\developers.ini File
- You can **set / change Path of Folders** (docs, letters, default and members)

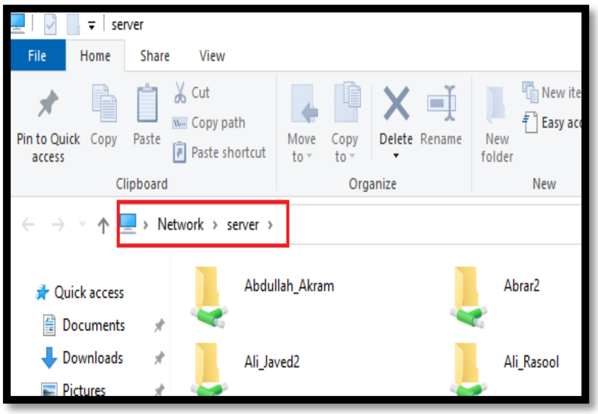


1.8. Network Connection Checking

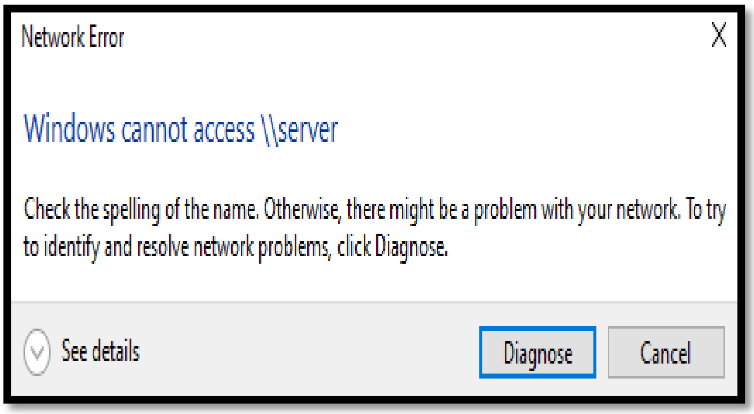
Check your server is connected, if **your server is not connected then contact your network admin** i.e. \\server



Connected



Not Connected



1.10. Prepare Client Machine

1.10.1. Prerequisites

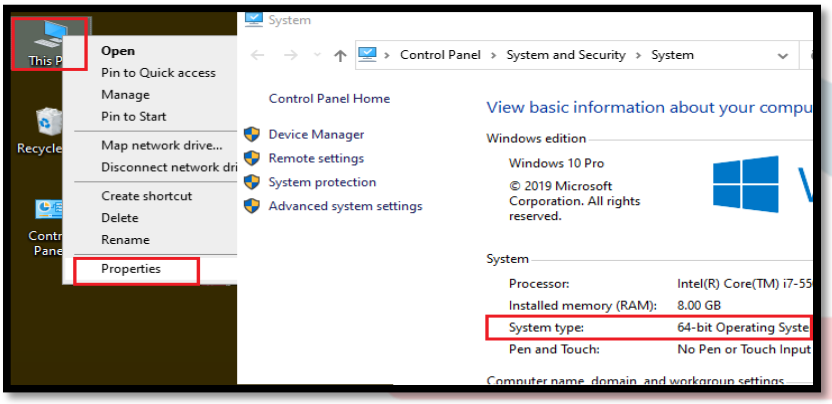
Following are prerequisites to make the client machine

- Client Computer/Laptop (Given specification & Fresh windows 7/8/10)
- DLLs Files
- Parameter File (i.e. developers.ini)
- Established Networking (Client machine should be on Network / LAN)

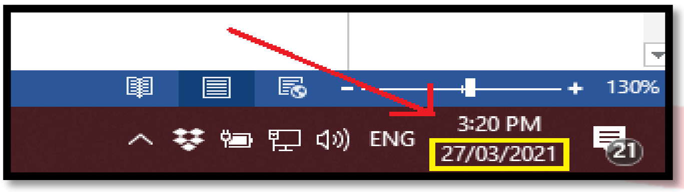
1.10.2. Procedure / Steps

To Make a Client machine following are steps

- Copy the All "DLLS Files" at the path
  - C:\Windows\System (For 64bit Windows)
  - C:\Windows\System32 (For 32bit Windows)

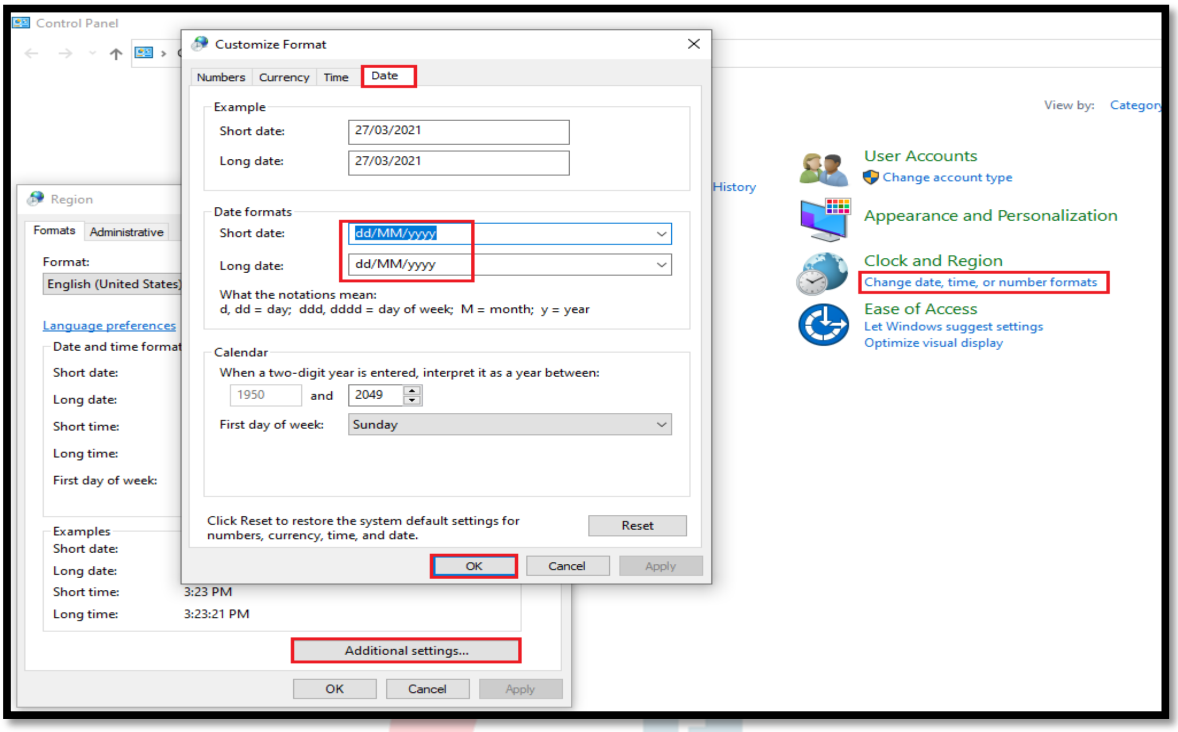


- Change Date Format of your Computer **dd/MM/yyyy** using Control Panel

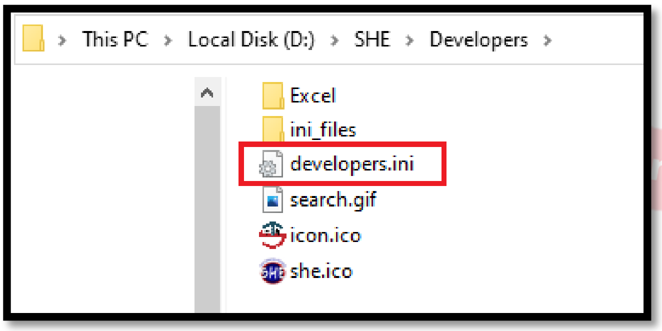


How to change computer date & time

- Control Panel→Change date, time, or number formats



- Create folders as (d:\she\developers)
- Place the developers.ini file in it as (d:\she\developers\developers.ini)
- Icon files, Excel folder, Etc. are **Optional**



1.10.3. Developers.ini (Confirguration)

Configure the developers.ini File in Any Client System

- Servername (Server Computer Name \ Instance Name)
- Database (i.e. SQL database Name)
- logpass (sa Password of sql server login)
- Default branch (Licensed branch code, given by SHE Technologies)
- Folders paths (docs, default, letters, members, backup_folder)

*developers.ini - Notepad

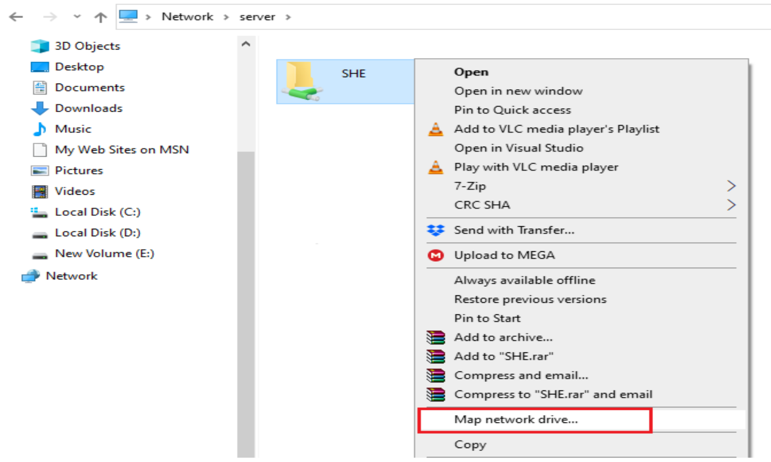
File Edit Format View Help

```
[connection]
dbms="MSS (Msoft) SQL Server 6.0"

servername = SalmanNaseer\SQL2008
database   = al_noor_orchard


logid      = sa
logpass    = Techno123

secureuid  = Y
encryption = Y

default_branch   = AJD002

members_folder   ='s:\developers\members\'
docs_folder      ='s:\developers\docs\'
letters_folder   ='s:\developers\letters\'
default_folder   ='s:\developers\default\'
backup_folder    ='s:\dbbackup\'

LICKEY           ='ASHV*n*F25222345347nkl9LS'
```

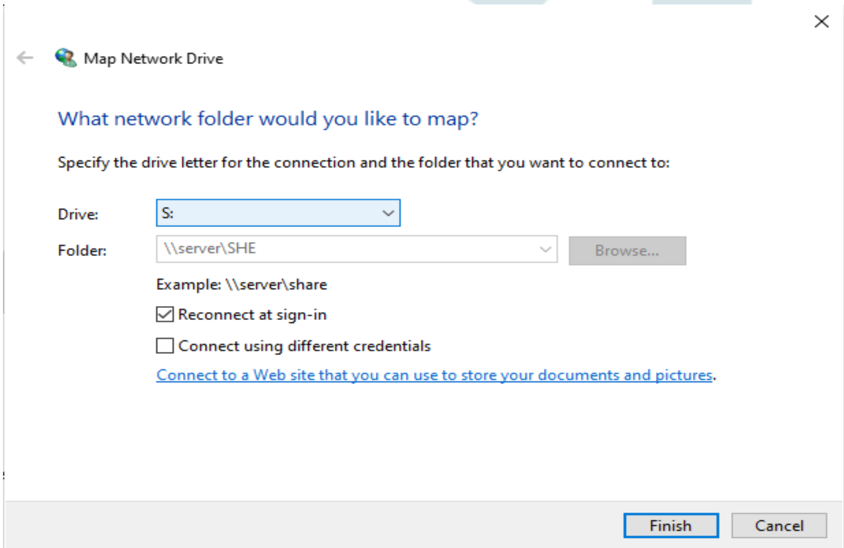
Ln 20, Col 19 | 100% | Windows (CRLF) | UTF-8

1.10.4. Map network drive from server SHE folder

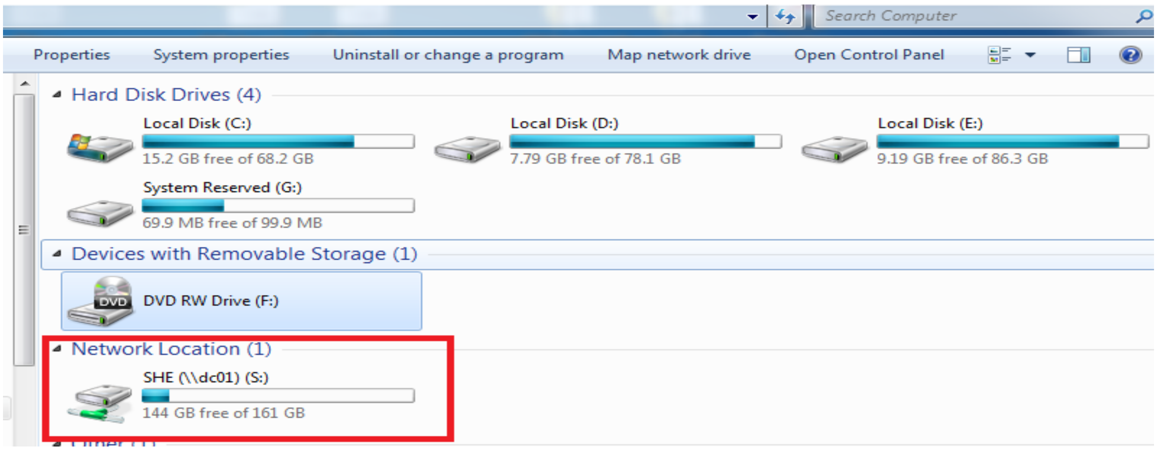
- Share **SHE** Folder on Server
- Access Server Computer from Client System
- Right Click on SHE Folder + Click "**Map Network Drive…**"



- Select Drive letter "**S:**"
- Click "**Finish**"

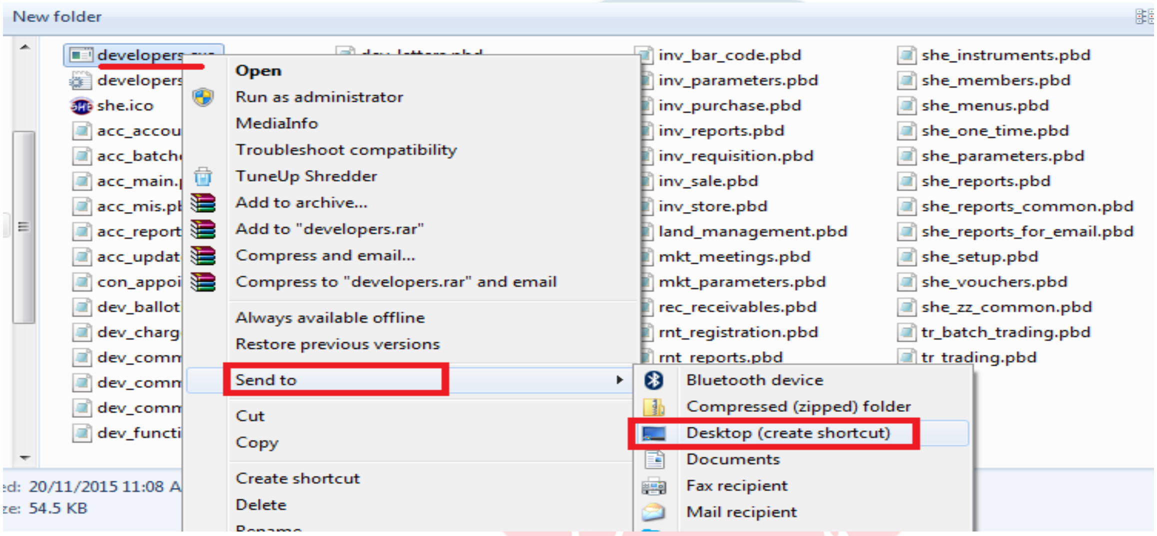


- Check your S: Drive as per below screenshot.

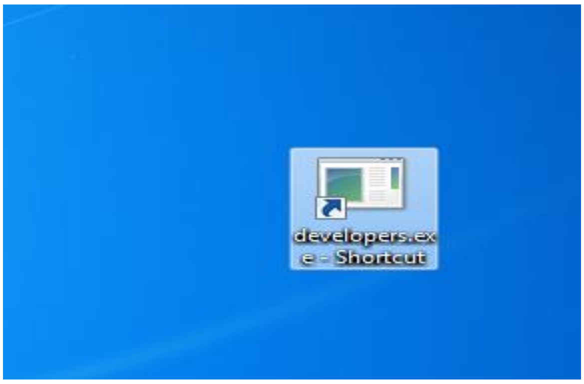


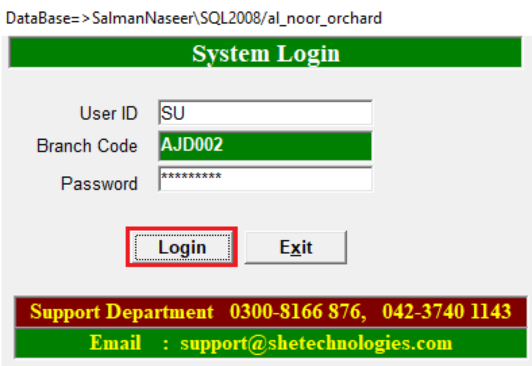
1.10.5. Create Exe Shortcut from Server

- Come at Exe Folder of server
- Right click developers.exe + Send to + Desktop (create shortcut)



- Software is ready
- Double click on Exe shortcut and run software



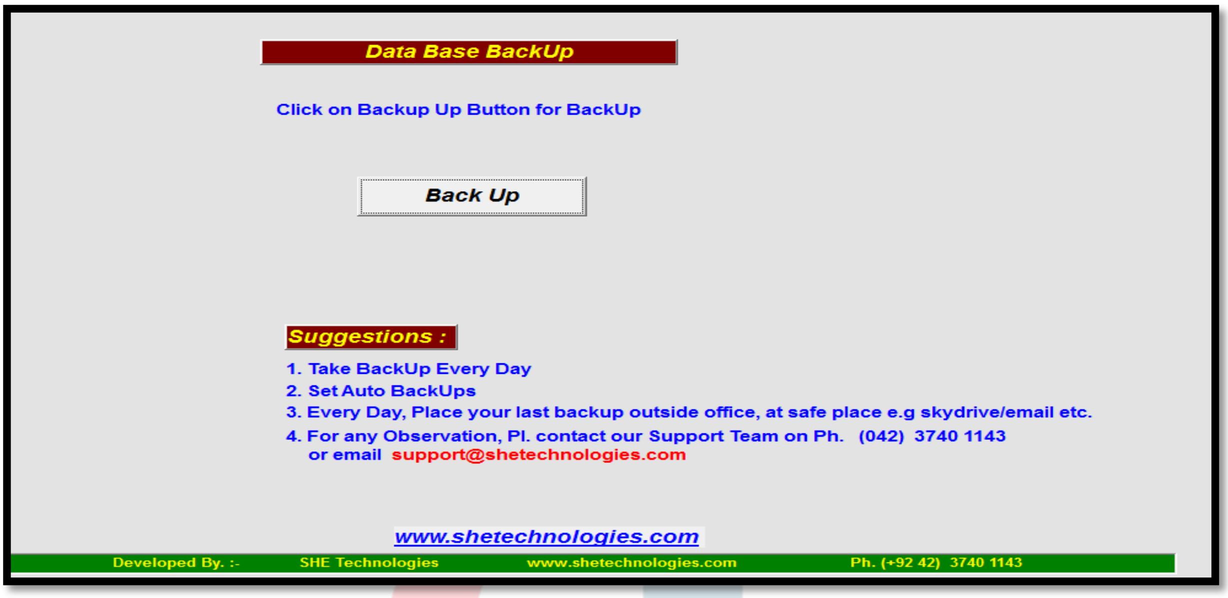


1.11. Take Backup of Database

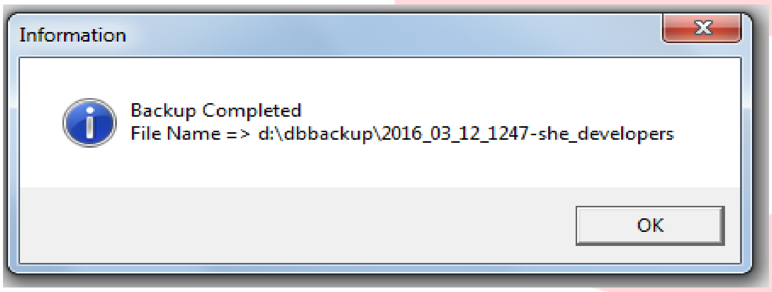
1.11.1. Data Base Backup

Maintenance → Misc. → Database Backup

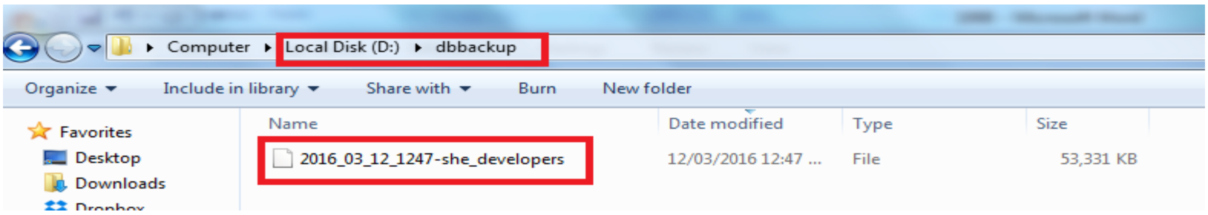
- Click Button "**Back Up**"



- It will take short time and will display below message after finishing backup



- Press OK button to close
- Verify backup file from the respective folder (i.e. d:\dbbackup)

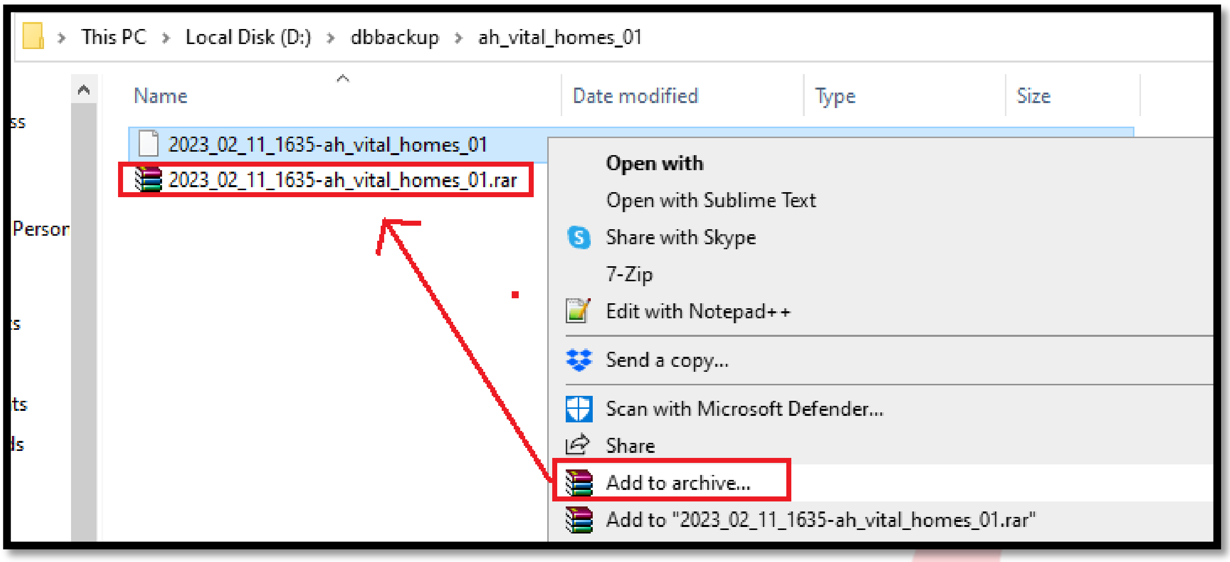


1.12. Backup Send to SHE Technologies (If Required)

- Take Database Backup (See point # 1.9)
- Restore database on testing server (See point # 1.18)
- Download Masking Query (See point # 1.13)
- Run **"Masking Query"** on testing server database (See point # 1.11.2)

Never Run Masking Query on Live Server

- Take Testing Server Database Backup (See point # 1.9)
- **Right click** on backup file
- Click "**Add to archive…**"



- Upload your **.rar** file to Google Drive, Etc.
- Send Google Drive link to our official email id backup4she@hotmail.com

Important Note:

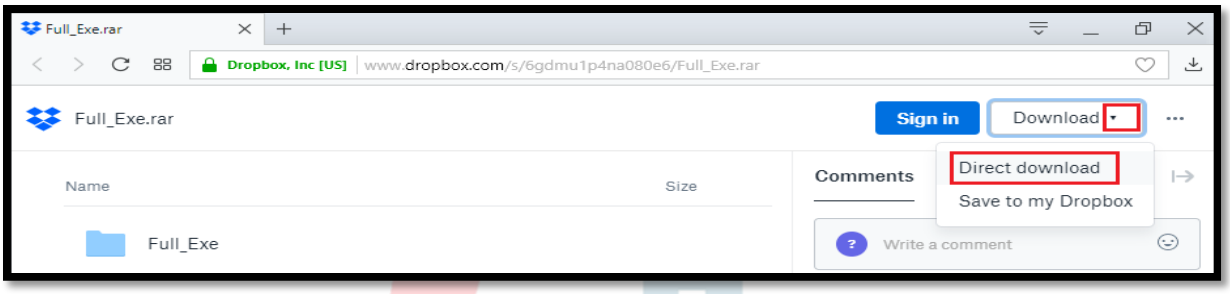
Please don't run masking query in live server database, otherwise we (SHE Technologies) are not responsible to recover your data.

1.13. Release Update

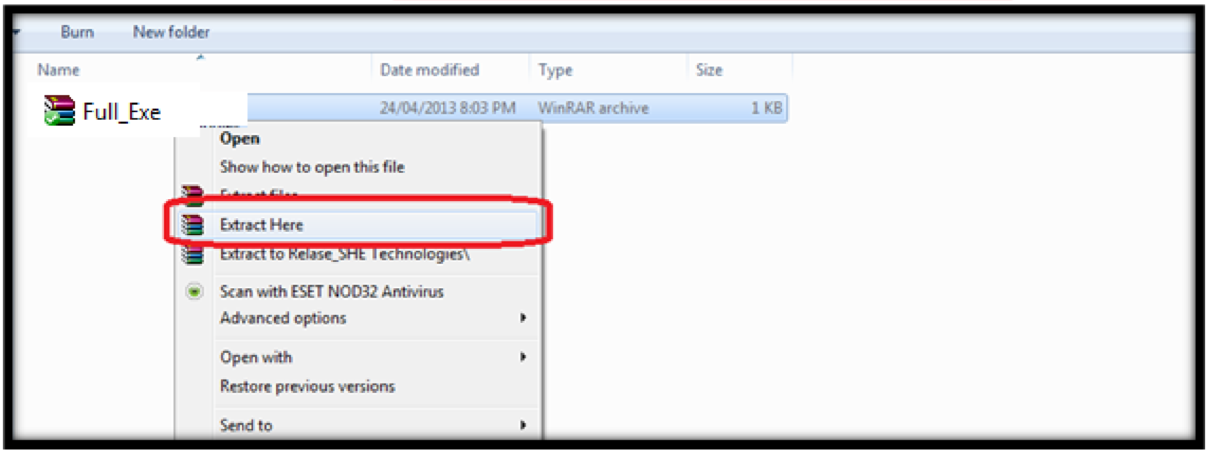
Release Update Include

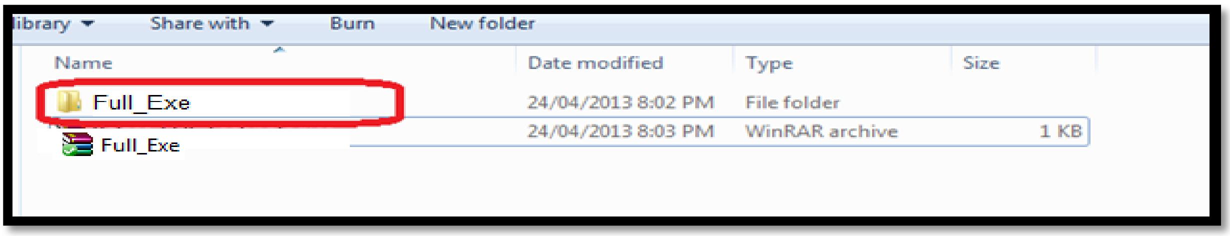
- Update Exe
- Run Query

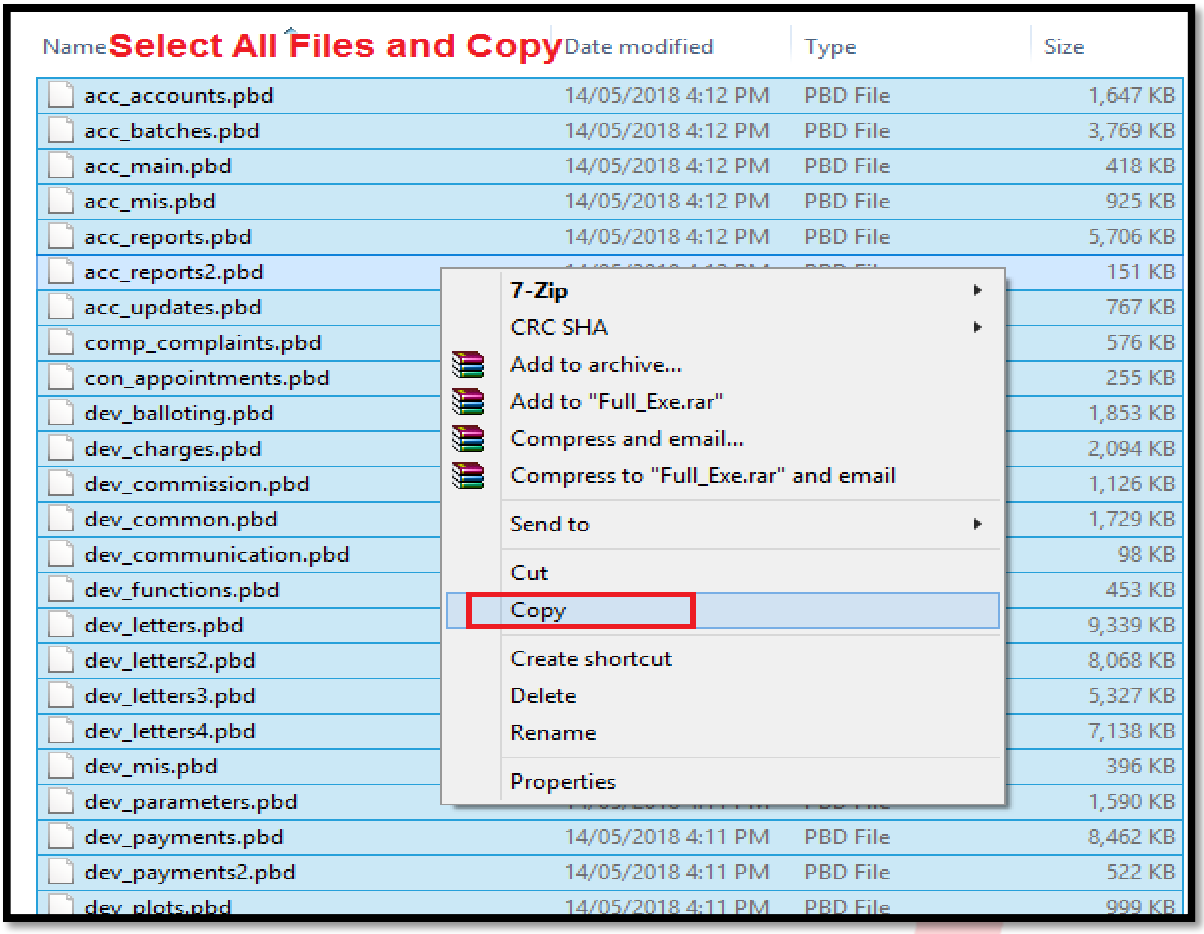
1.13.1. Update Exe.



Extract “Full_Exe.rar” to Folder “Full_Exe”

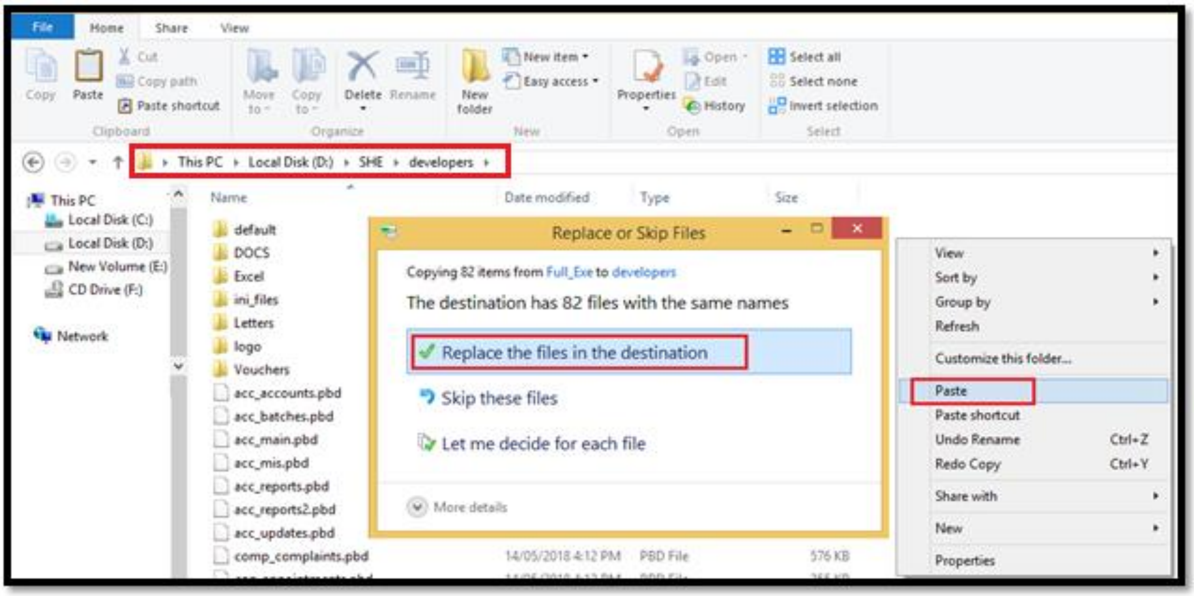






Replace all Files in Your Server (D:\SHE\Developers)

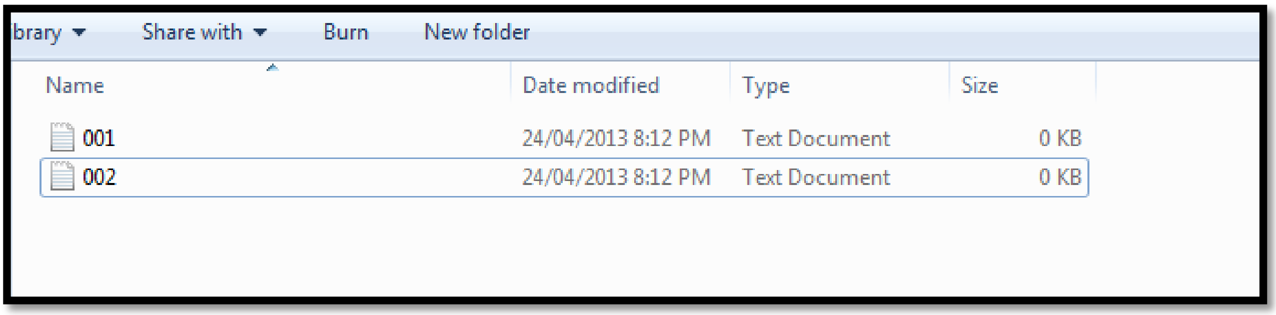
(All user should Run exe from server otherwise you need to replace on all places)



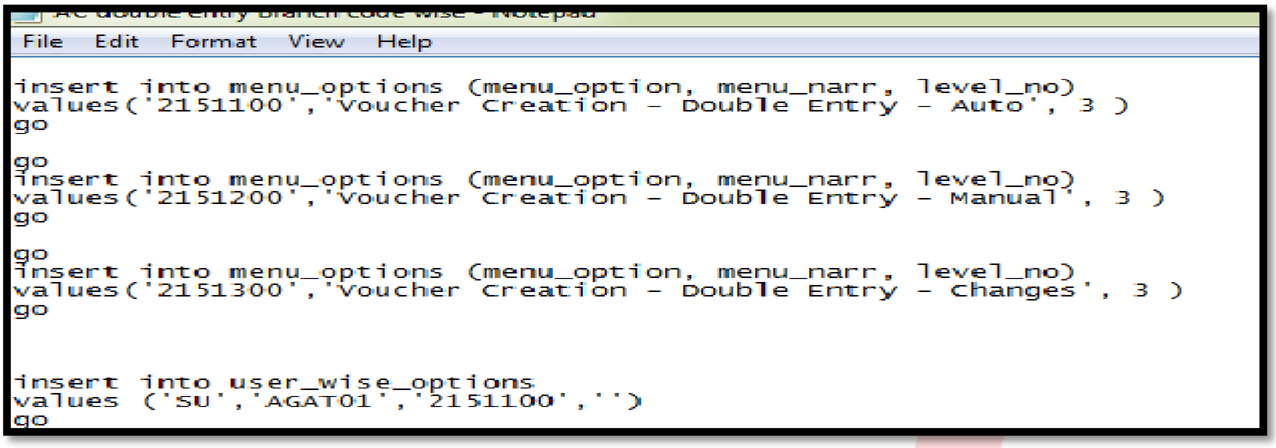
Part a is Done

1.13.2. Run Query (Take database Backup Before Run Any Query)

With Release E-Mail, you also find some Text Files

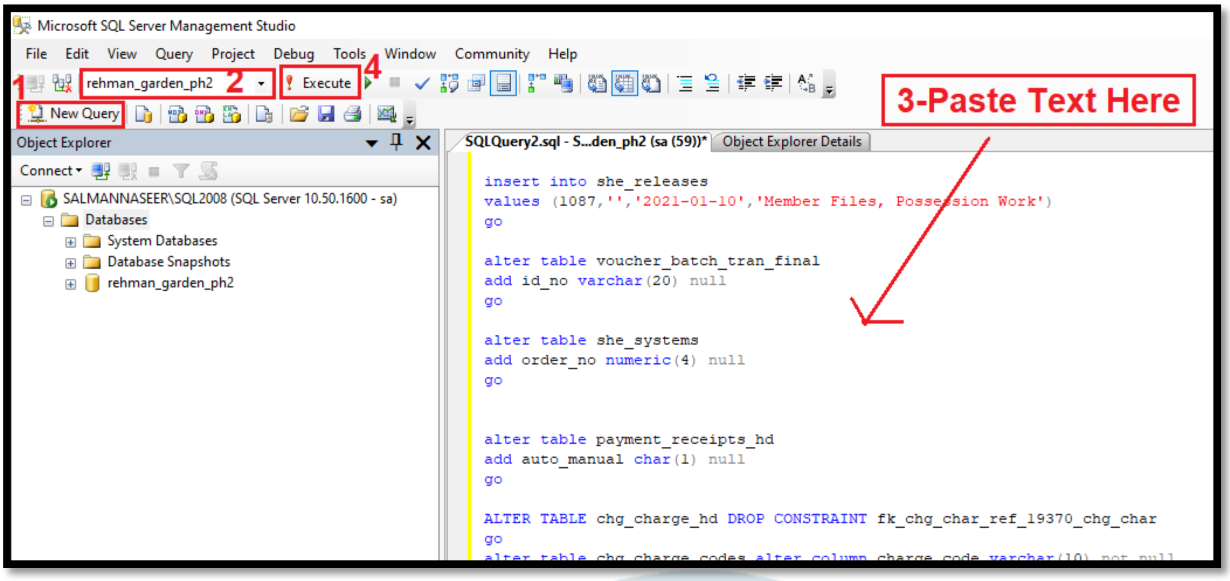


Open this Notepad file and Copy all the Text from it.



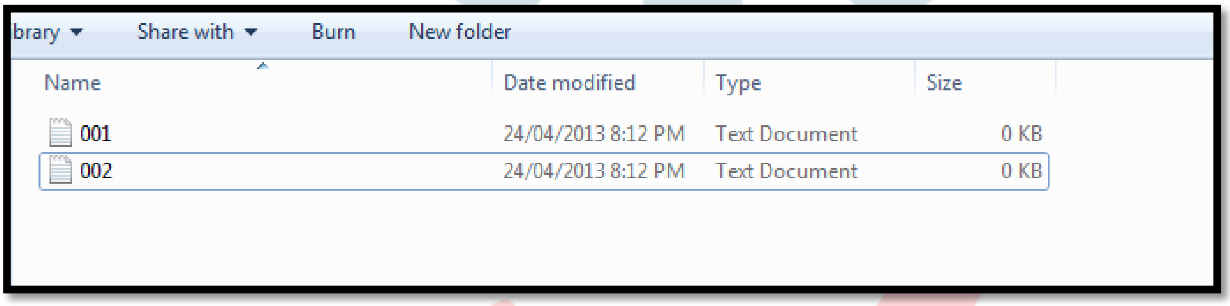
Open SQL Server Management Studio (Server Computer)

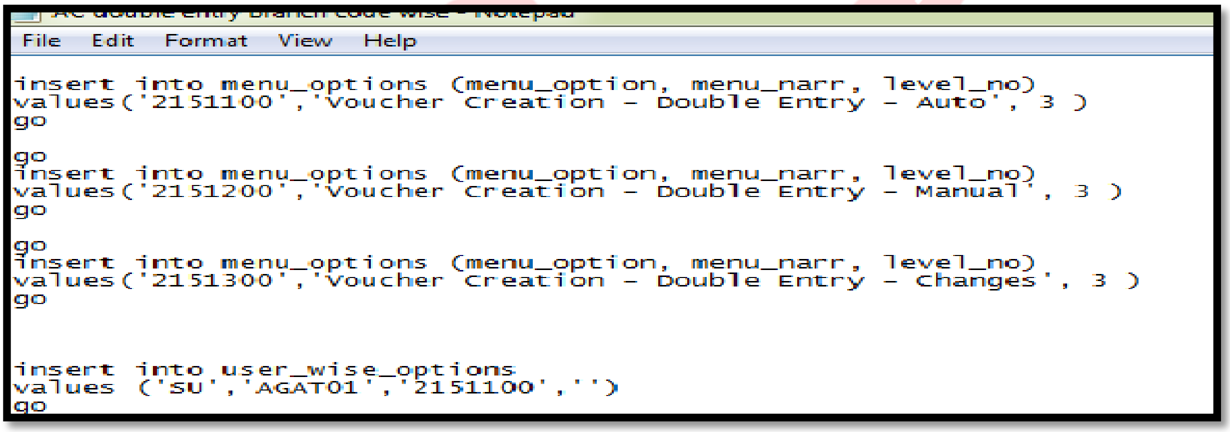
- Copy all text in new query as below screenshot
  (Verify as point # 2 that Query is running in your database, i.e. rehman garden_ph2

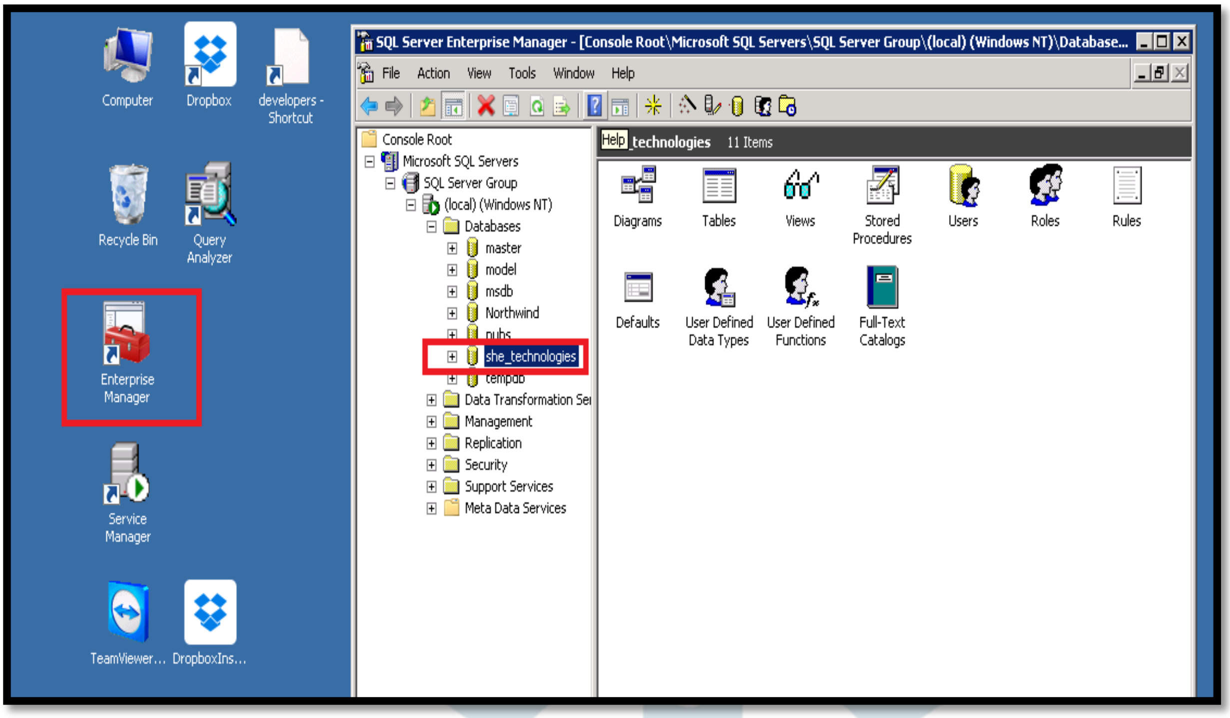


Part b is done.

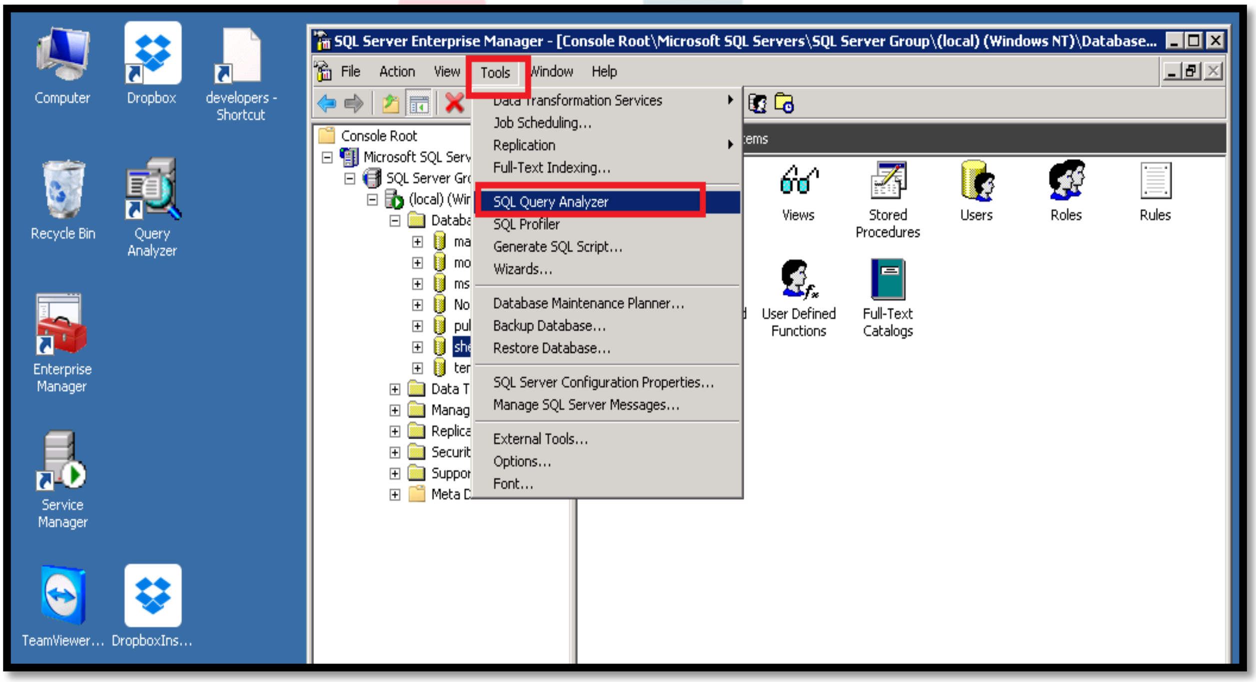
1.13.3. Run Query (For SQL-2000)

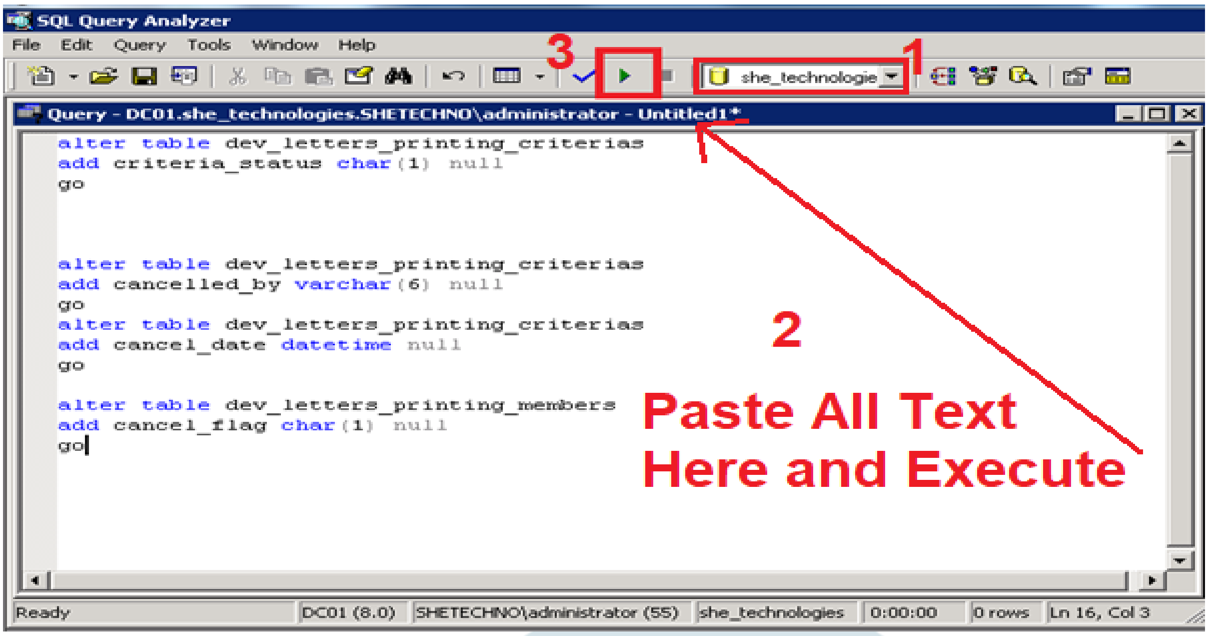






Click on Tools - > SQL Query Analyzer



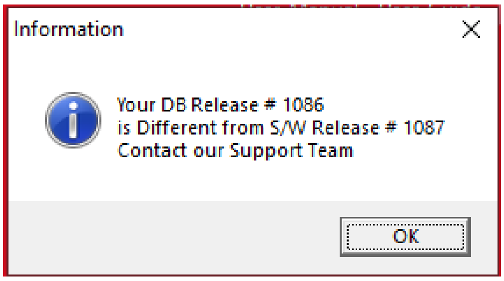


Part b is Done (for SQL2000)

1.14. Update Queries (Database Structure Update)

If you see this message when you login. Then download update query and run in your database.

(As per below message, download 1087 query and run in your software).



1.15. Download steps:

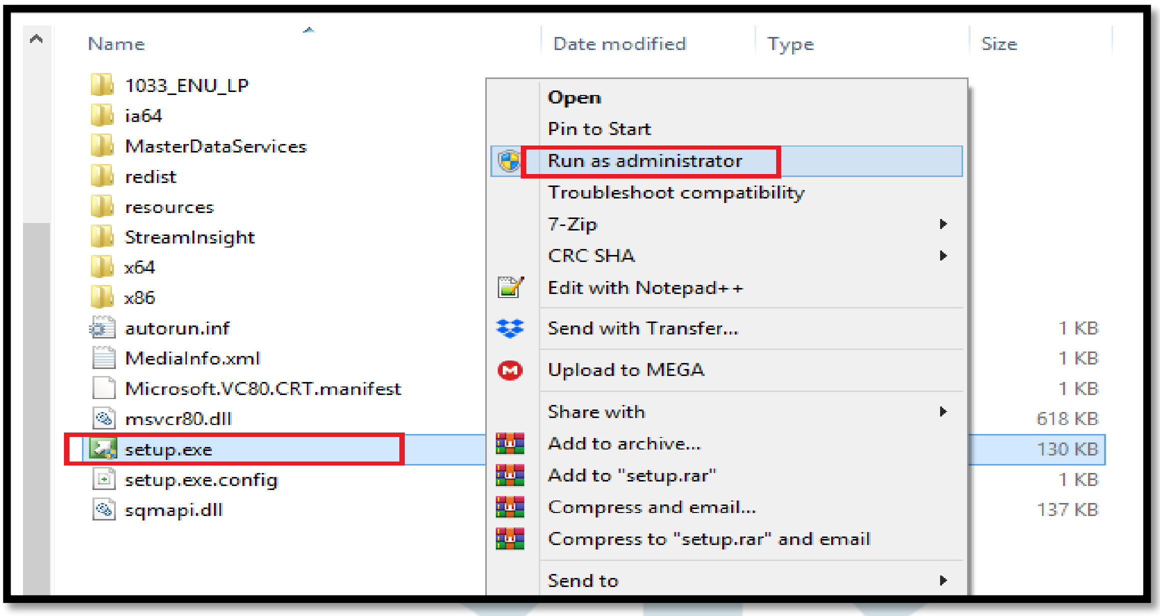
- Click this link: https://www.shetechnologies.com/
- Click "**Login**" at Top Right Corner
- User ID: she
- Password: shetec@123
- This is **download page** and you can download
  - SAMS Update Queries
  - Administrative Guide
  - User Guide(s) of any module i.e. SAMS Guide, Accounts Guide, Etc.
  - ALL DLLs
  - Masking Query
  - SQL Server 2008 Setup
- **See index page** to get your relevant section

Sr.No	Document Name	Updated Version	Links
1	Administrative Guide	10-02-2021	Download
2	Masking_Query	02-02-2021	Download
3	SQL 2000 for Window 10	02-02-2021	Download
4	SQL 2000 for Window 7 (Part 1)	02-02-2021	Download
5	SQL 2000 for Window 7 (Part 2)	02-02-2021	Download
6	SQL Server 2008 R2	02-02-2021	Download
7	ALL DLLs	02-02-2021	Download
8	SAMS User Manual	24-02-2021	Download
9	SAMS Update Queries	03-03-2021	GoTO Download

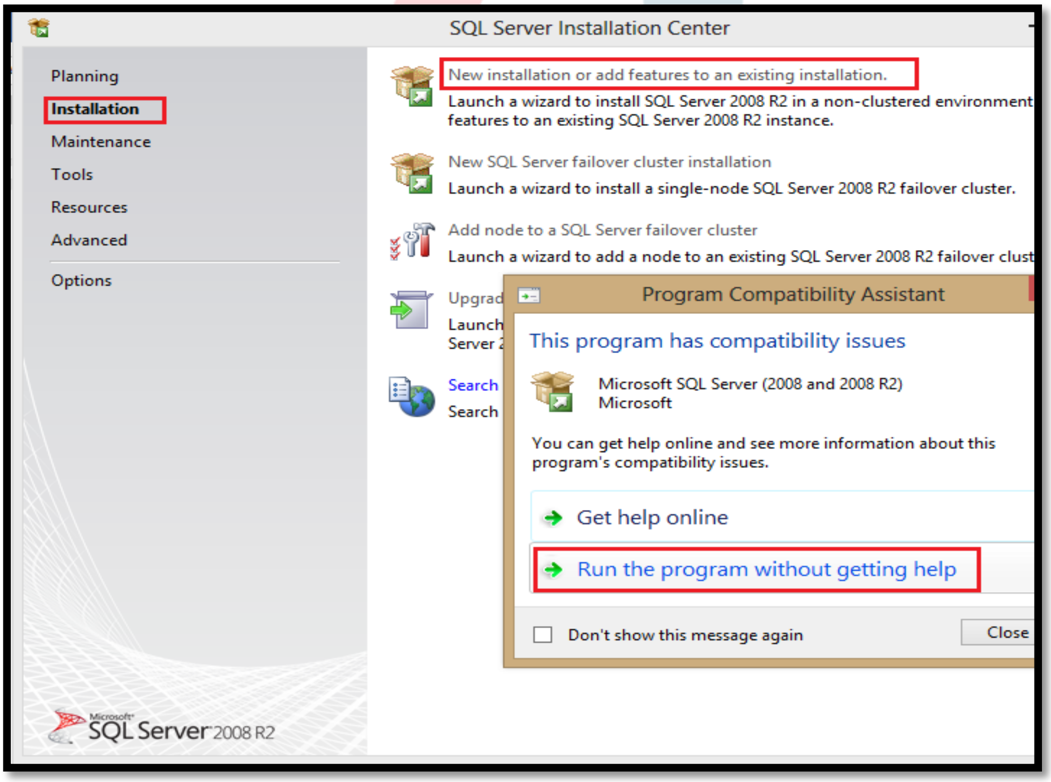
Sr.No	Query No	Links
1	1087	
2	1086	
3	1085	

1.16. SQL Server 2008 Installation

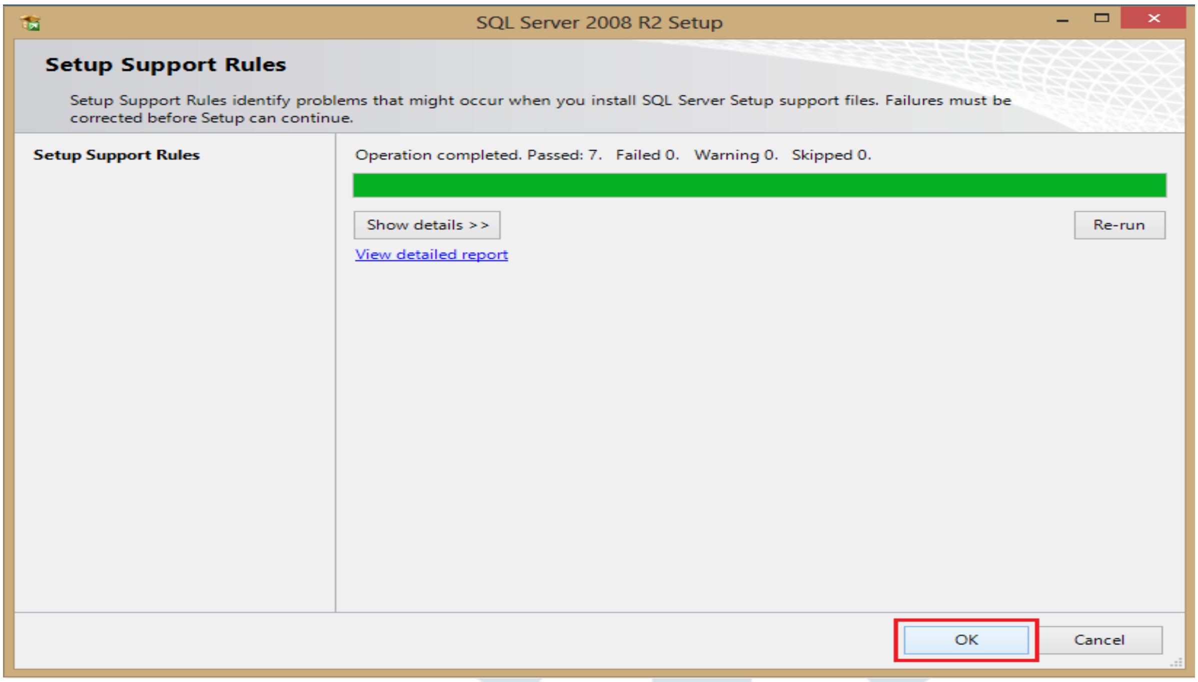
Go to Setup folder and Run Setup as Administrator



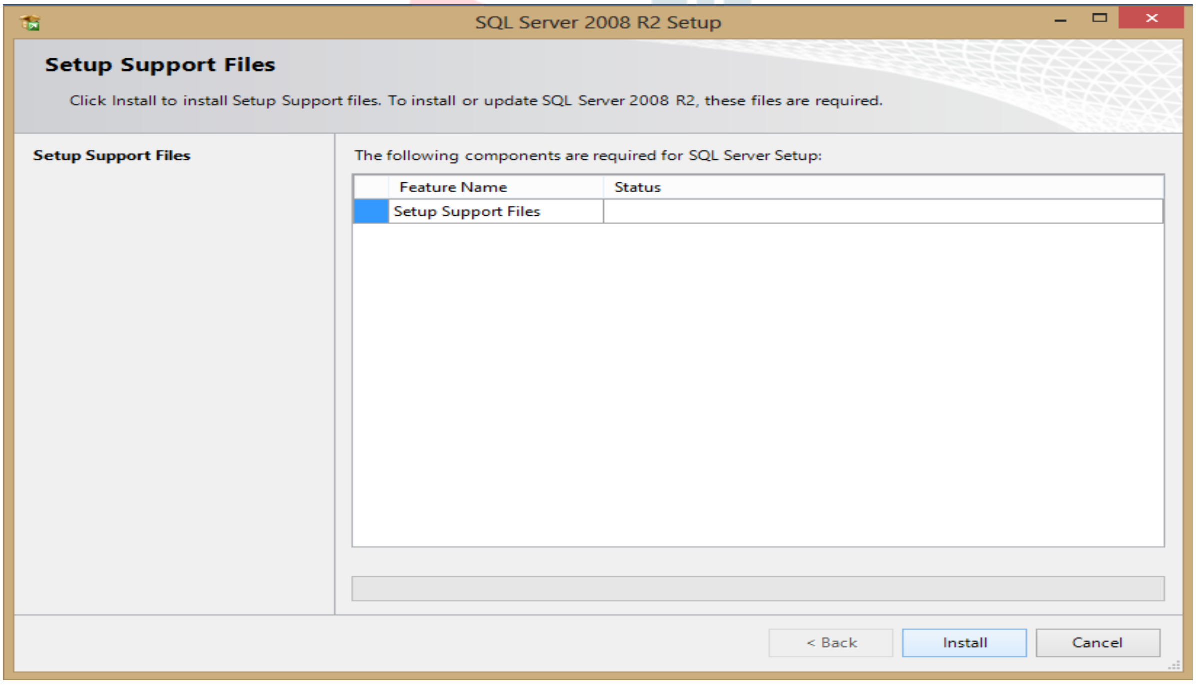
- Click installation + New Installation… + Run the program without getting help



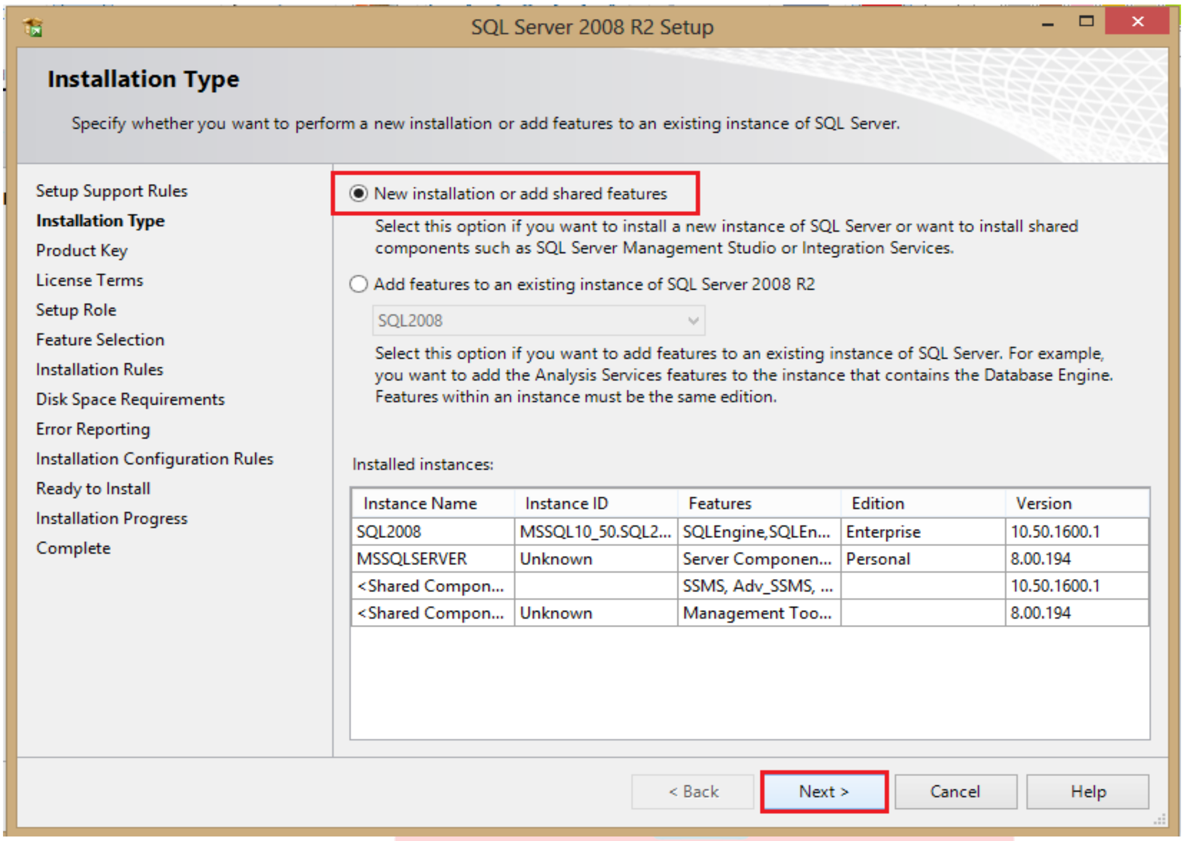
- Click OK



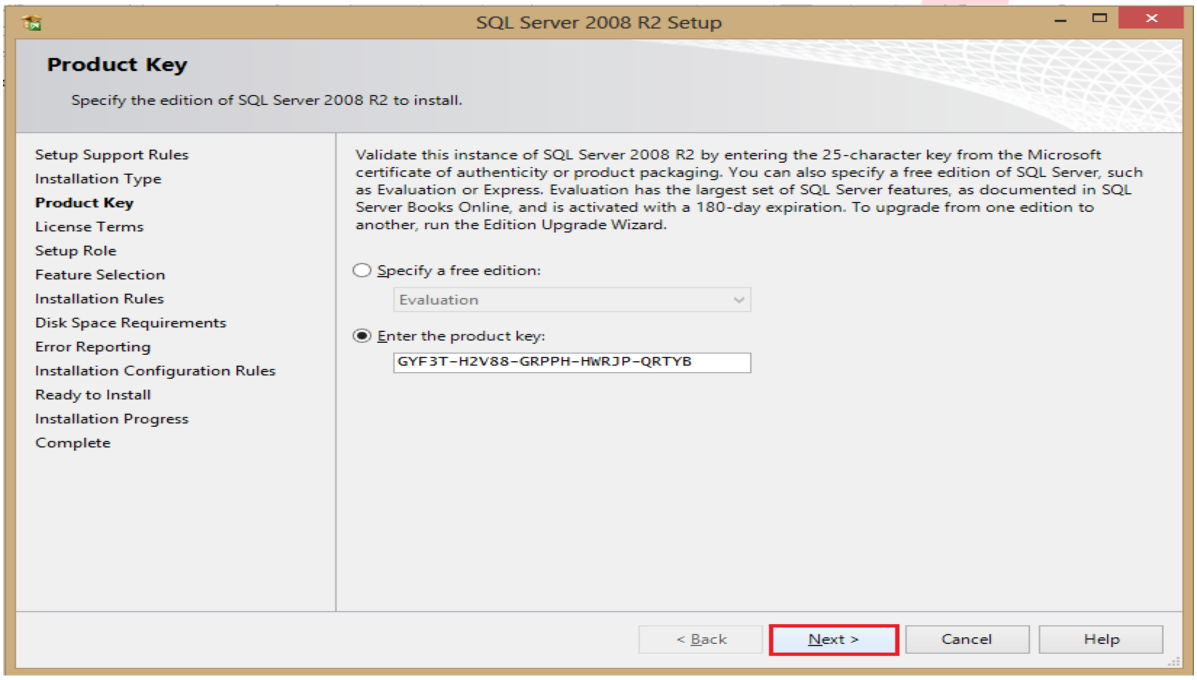
- Click Install (Setup Support Files)



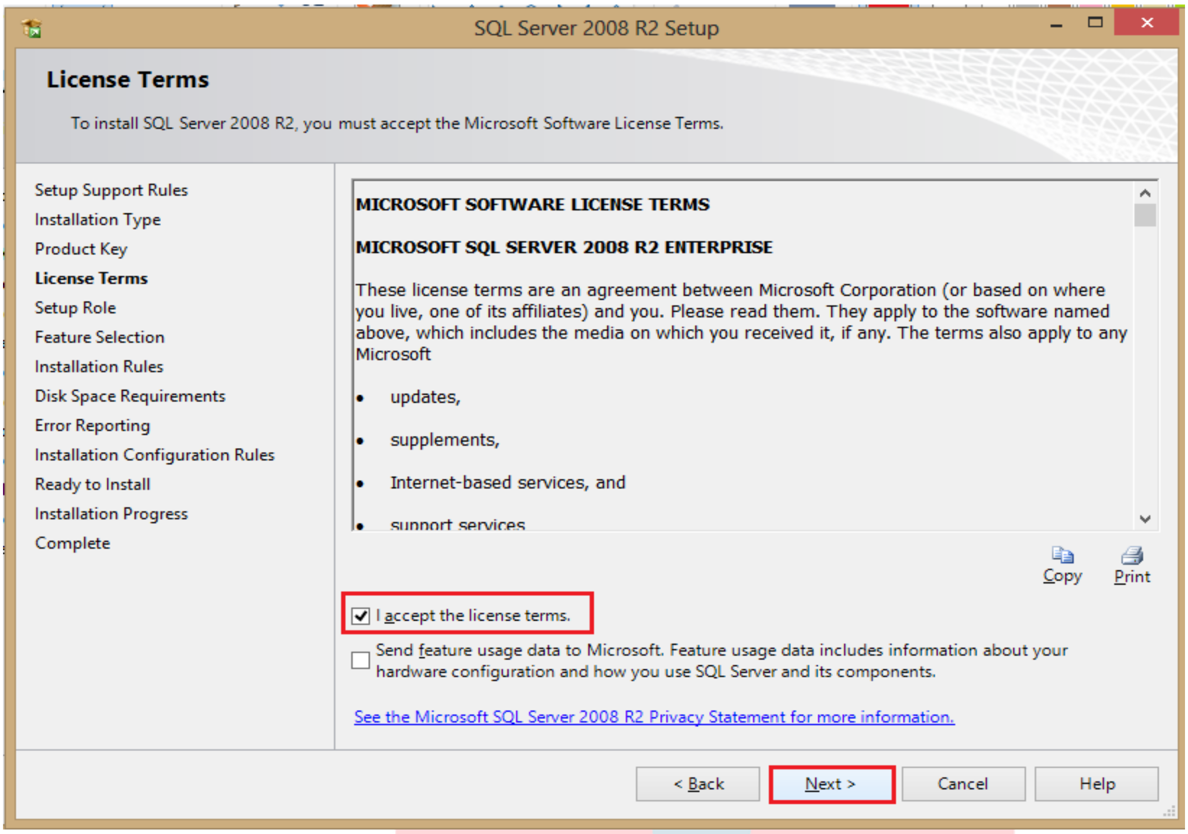
- Click New Installation or add shared features



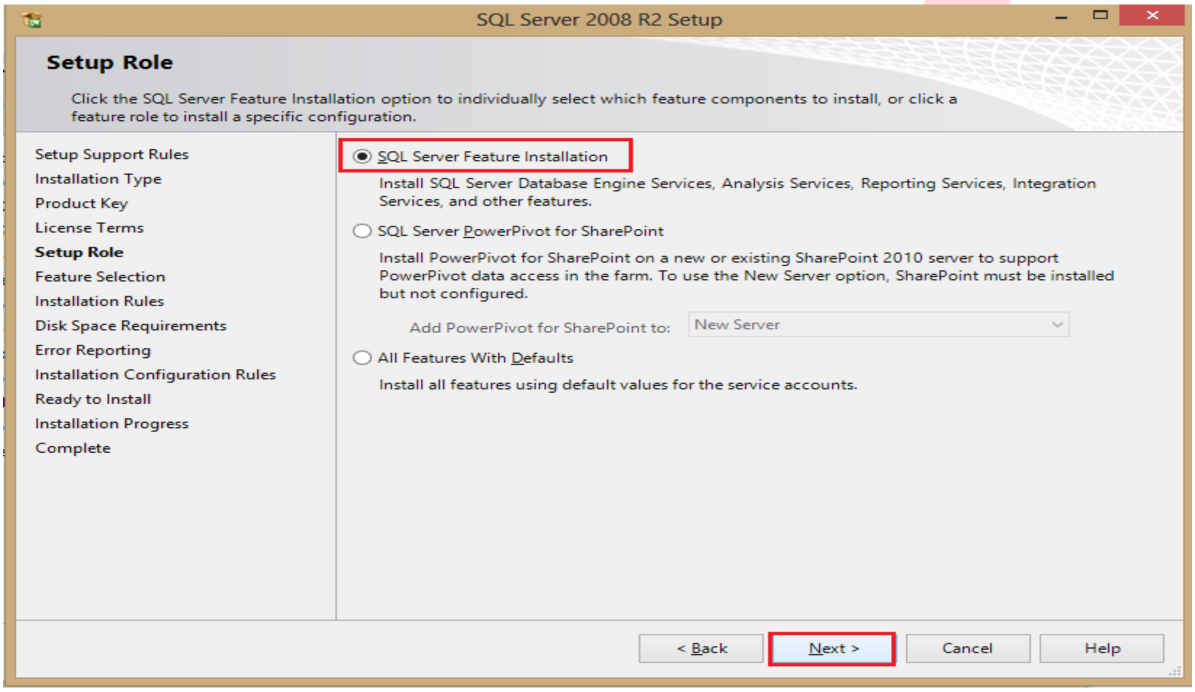
- Click Next (Product Key will be already here)



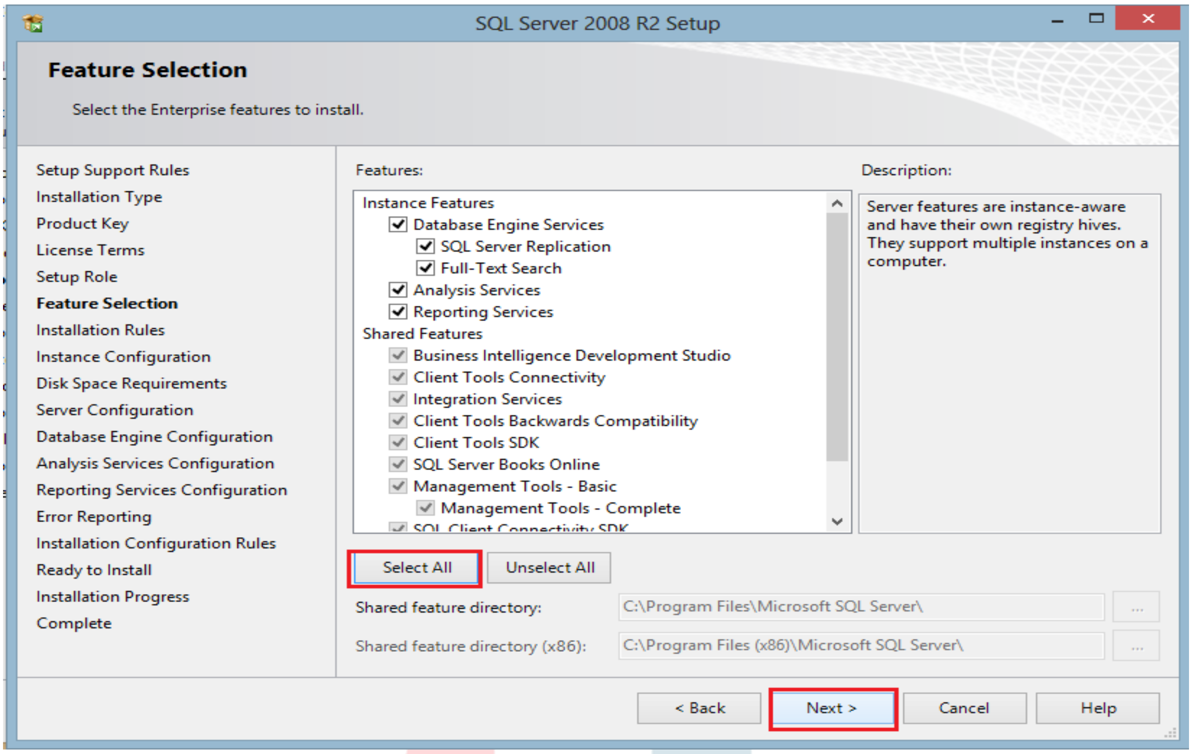
- Click (Accept Check box) + Next



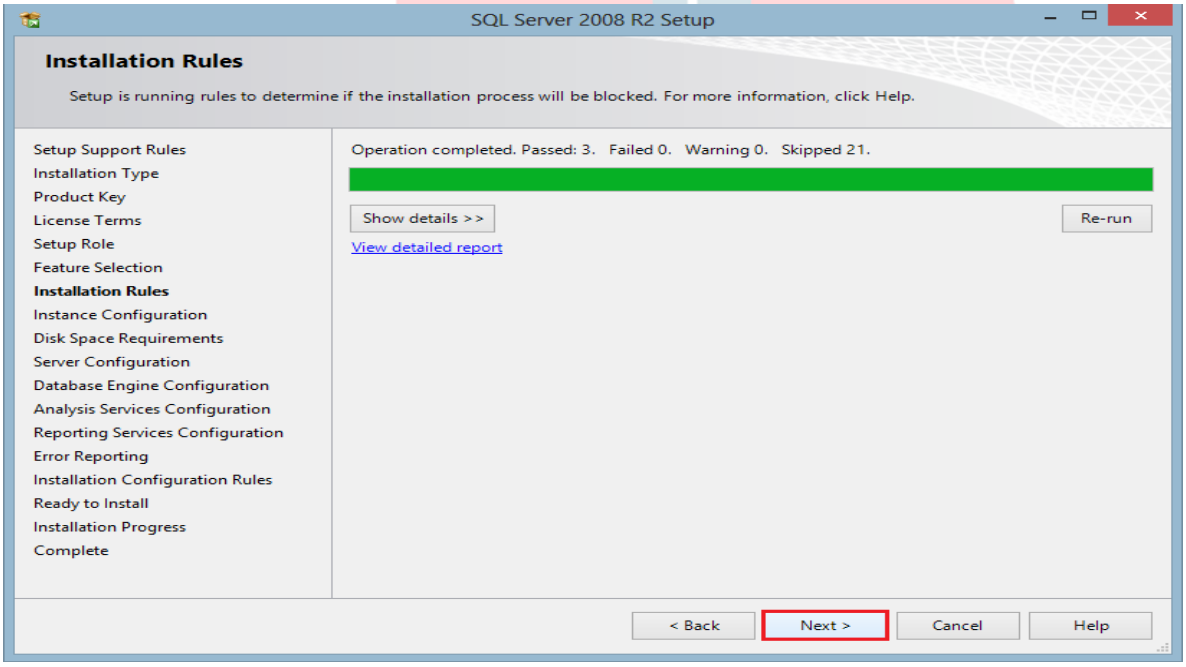
- Click SQL Server Feature Installation + Next



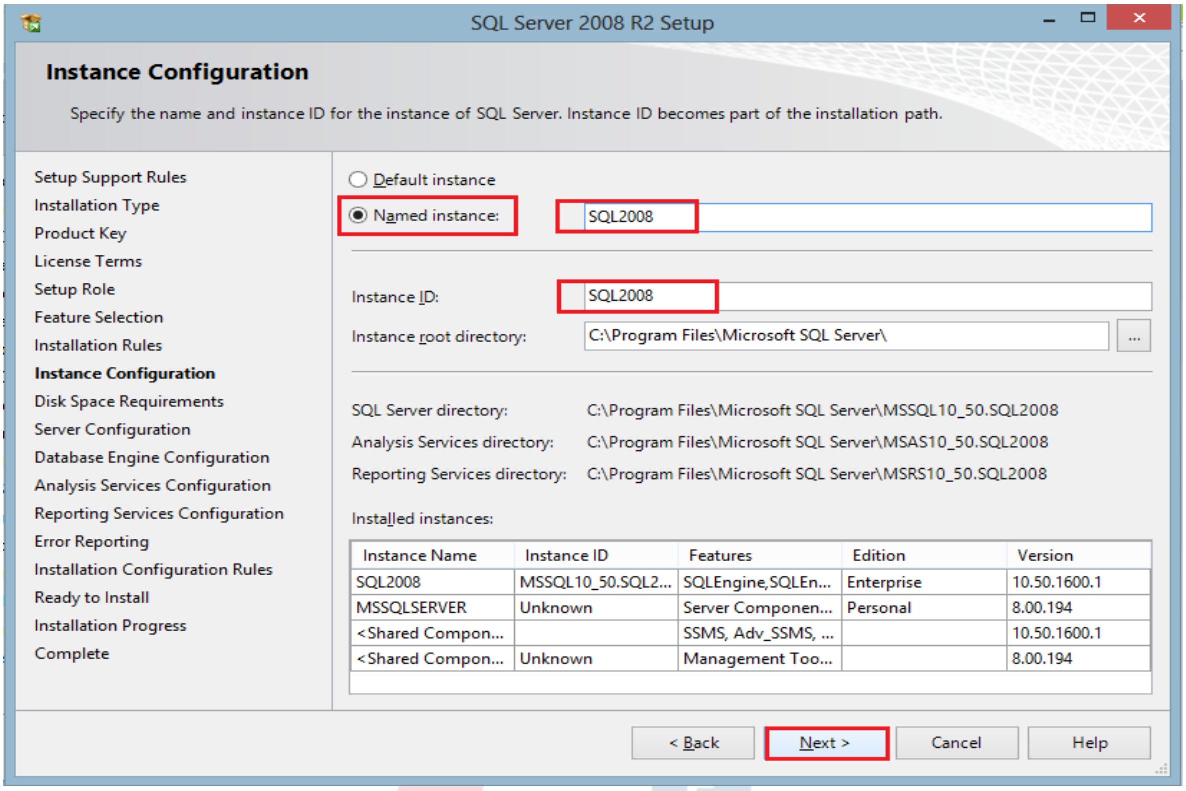
- Click Select All + Next



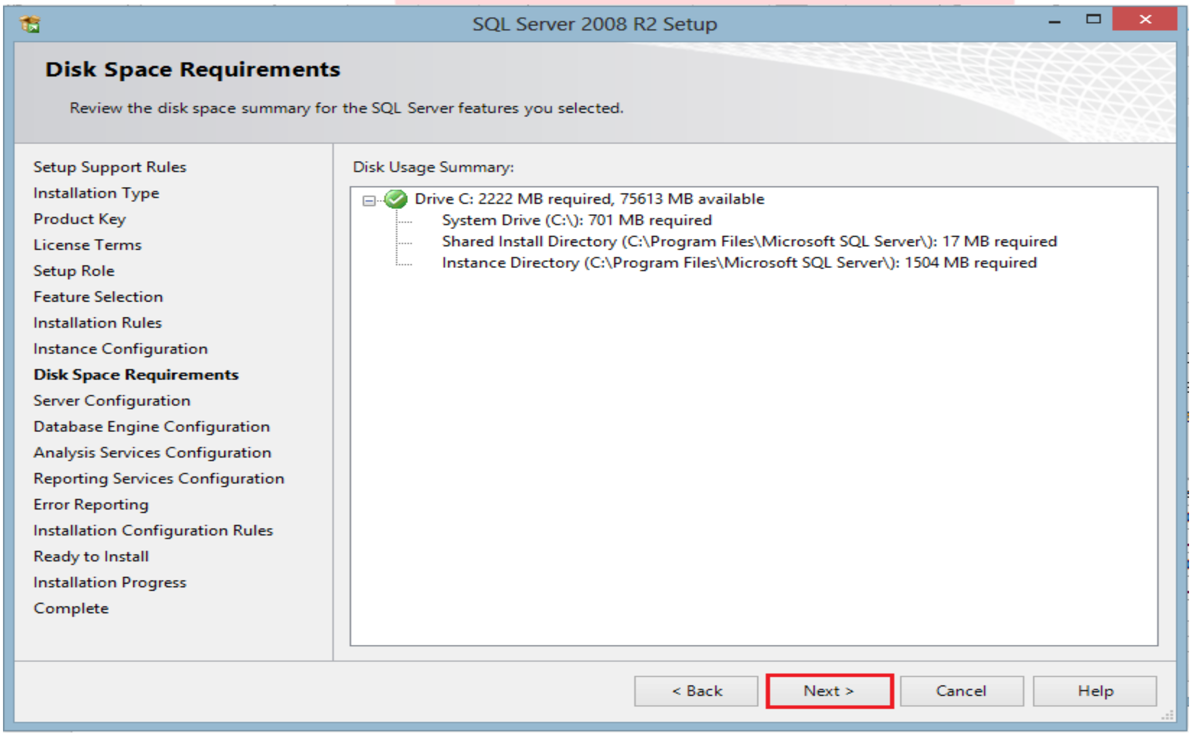
- Click Next



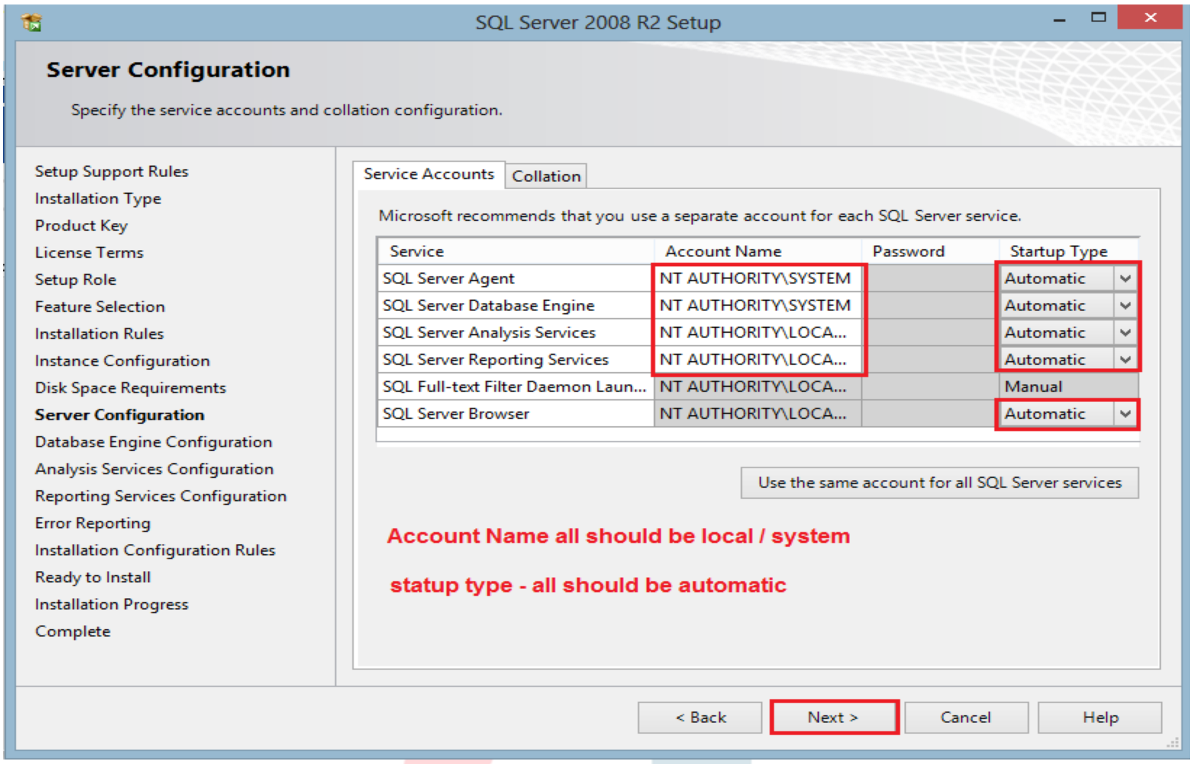
- Click Named instance + type "SQL2008" + Click Next



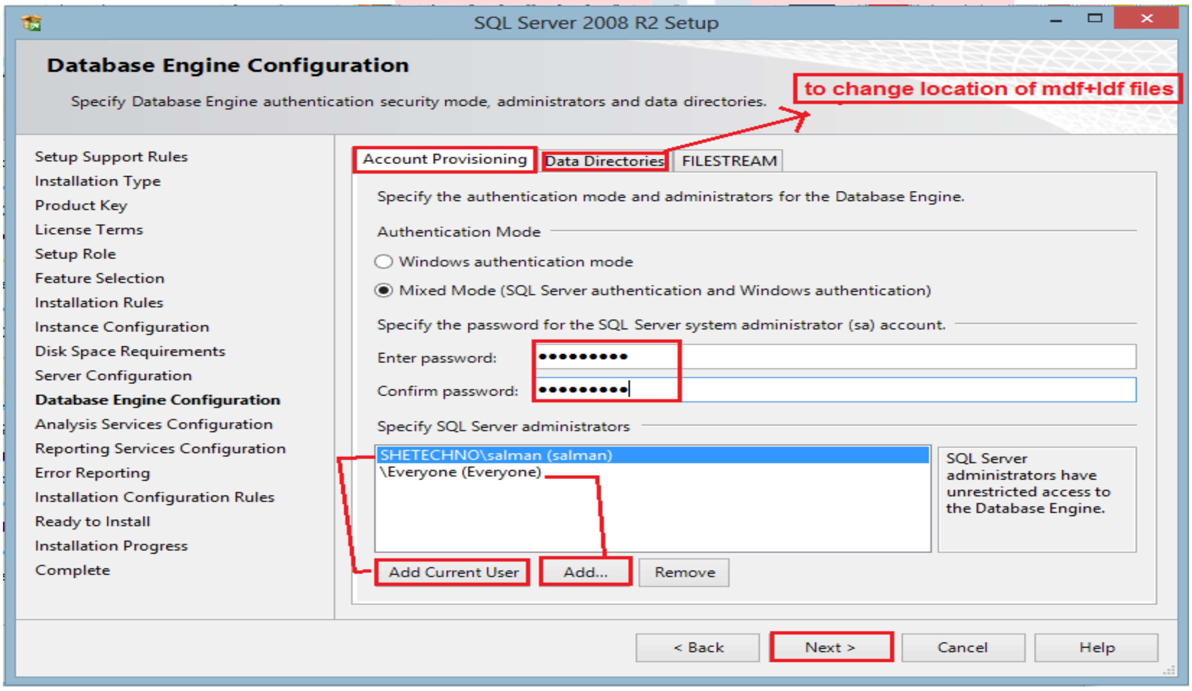
- Click Next



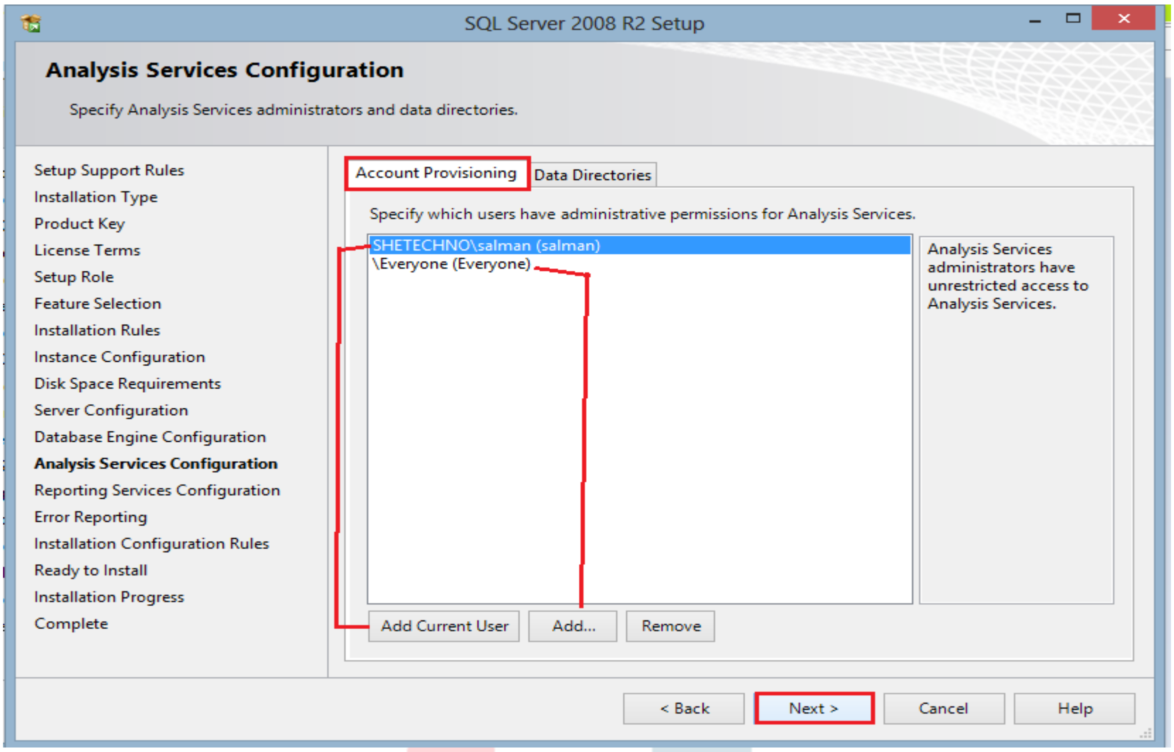
- Select all services as highlighted + automatic



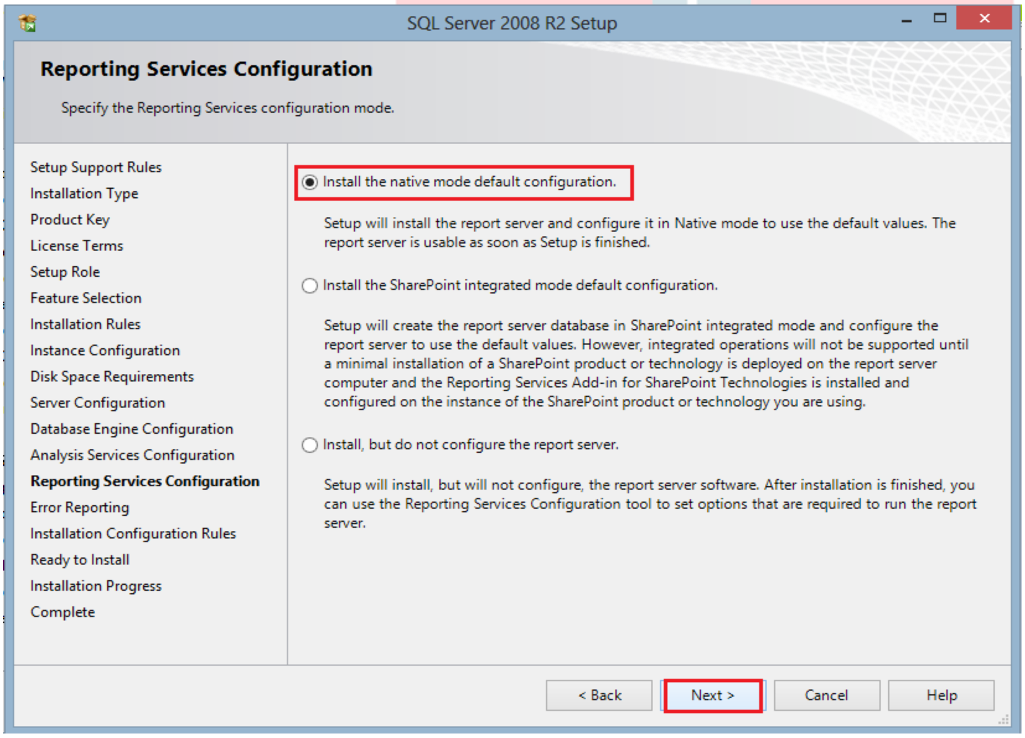
- Click Add Current User + Next



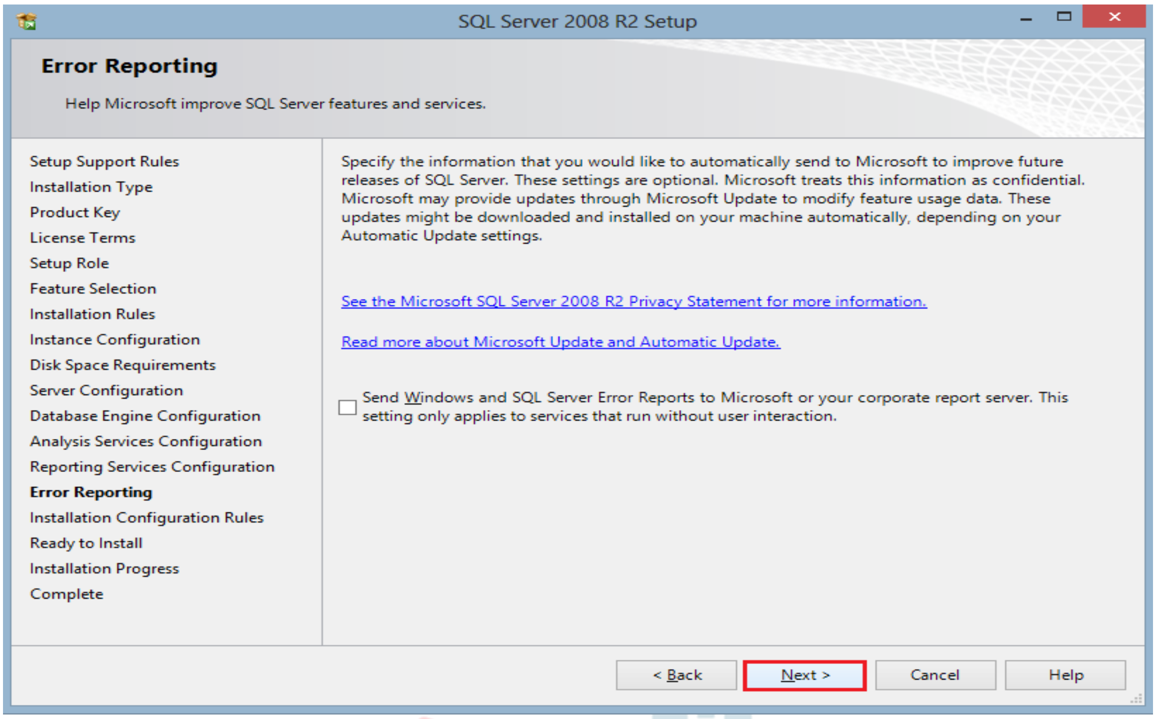
- Click Add Current User + Next



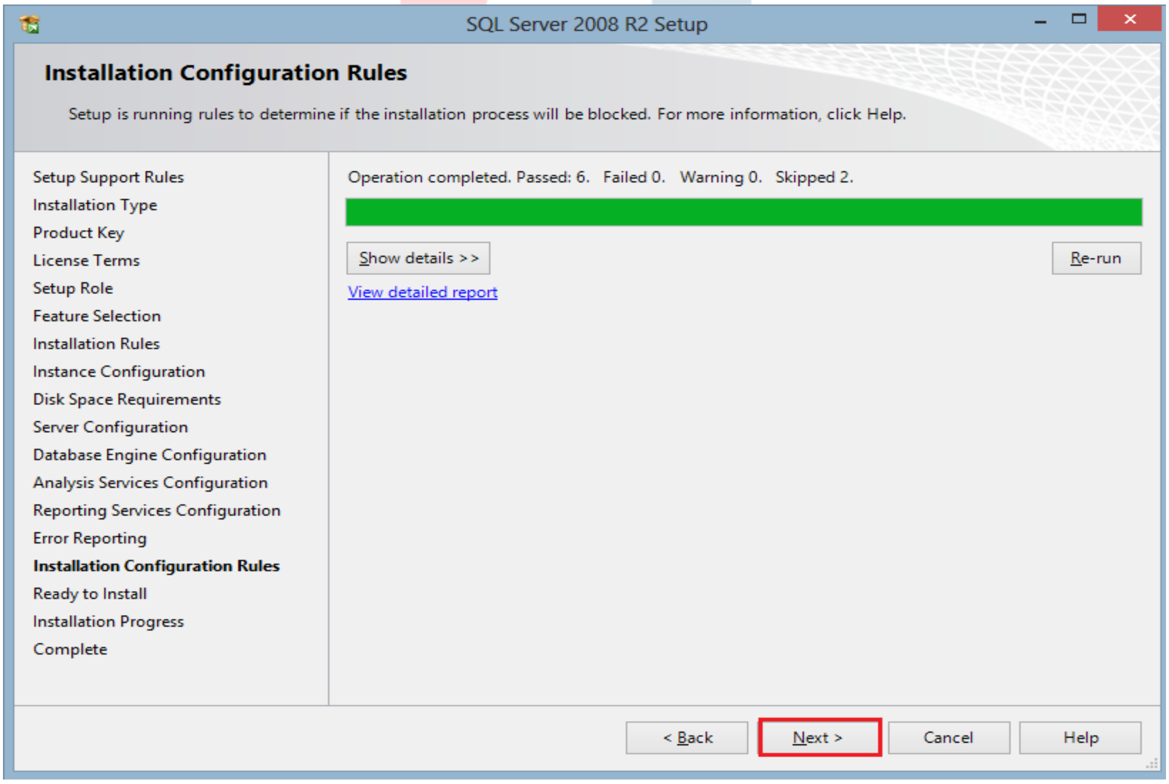
- Click “Install the native mode default configuration.” + Next



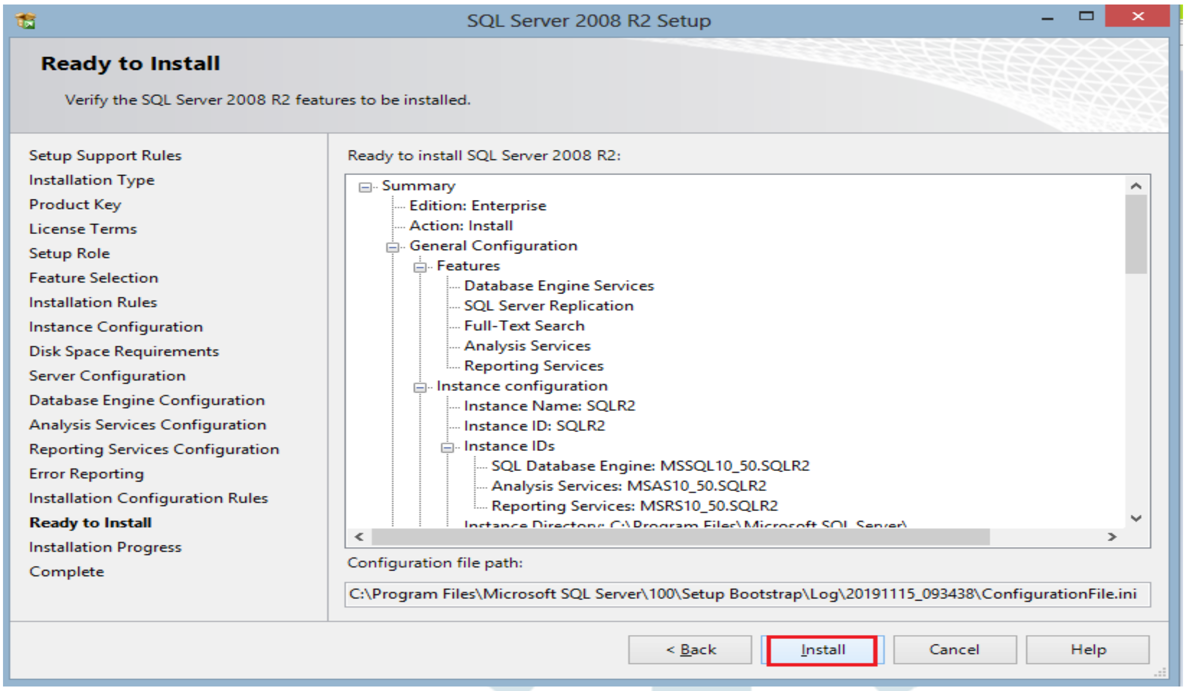
- Click Next



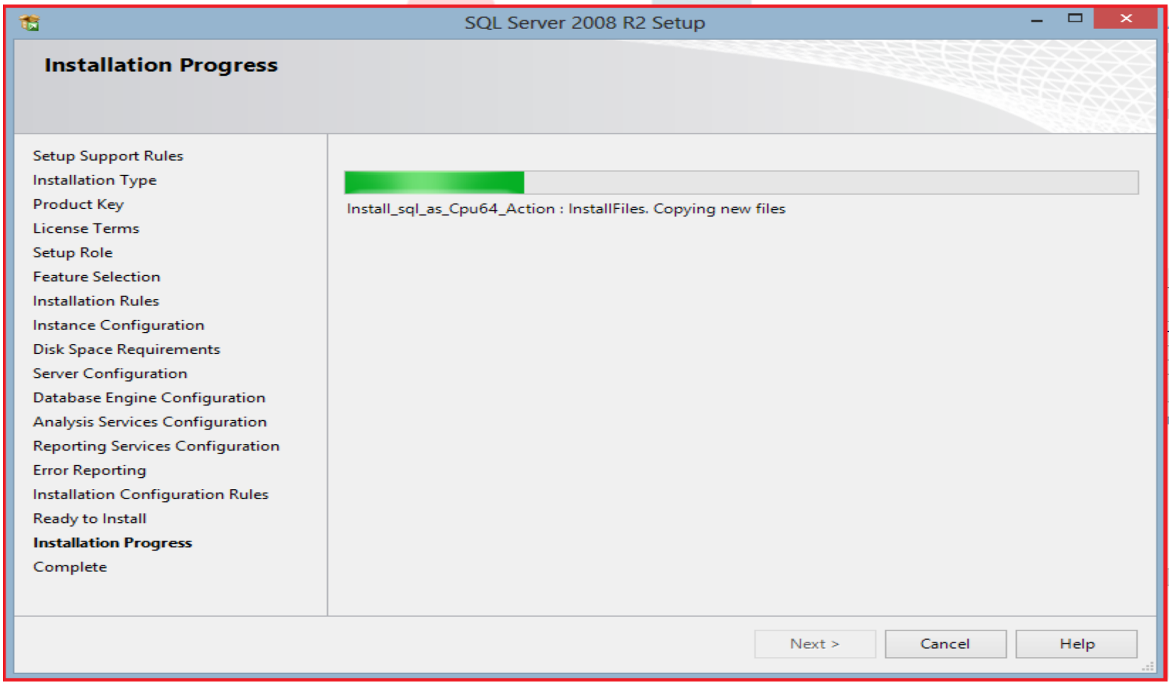
- Click Next



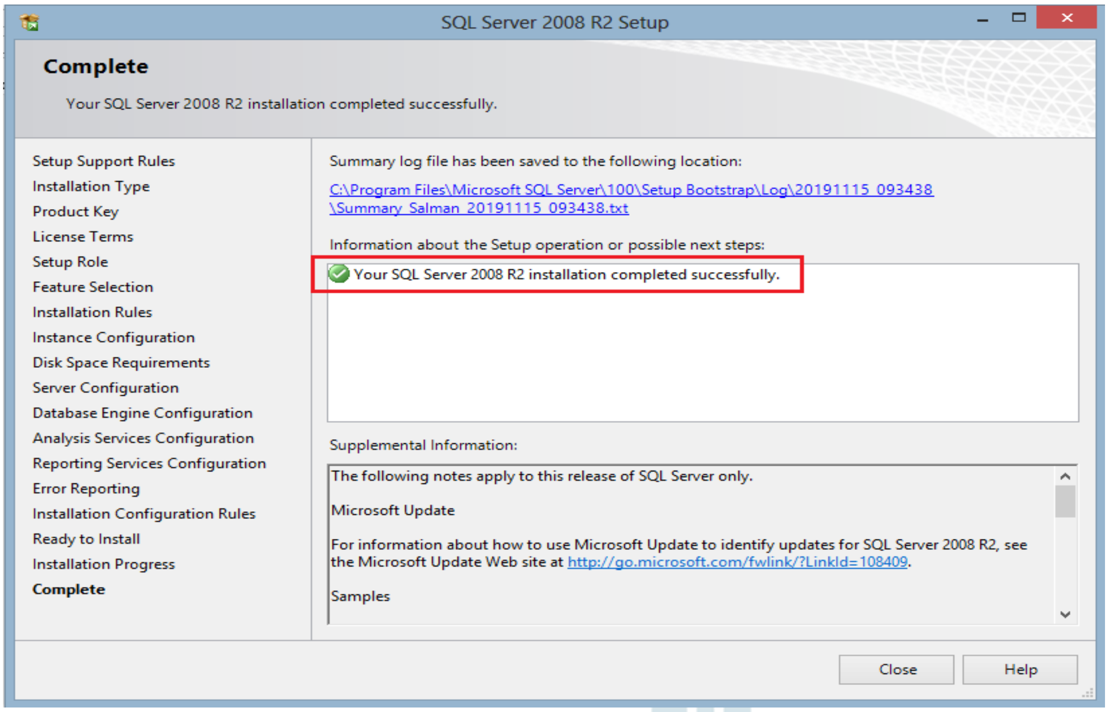
- Click Install



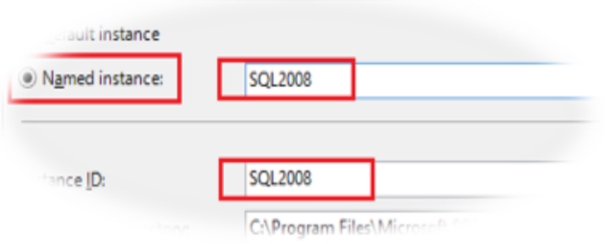
- See installation Progress

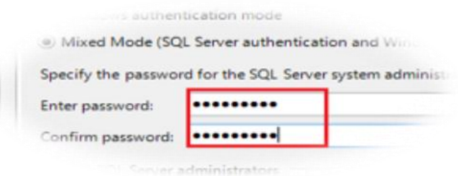


- See congratulation msg + Click Close



- Start SQL Server Management Studio





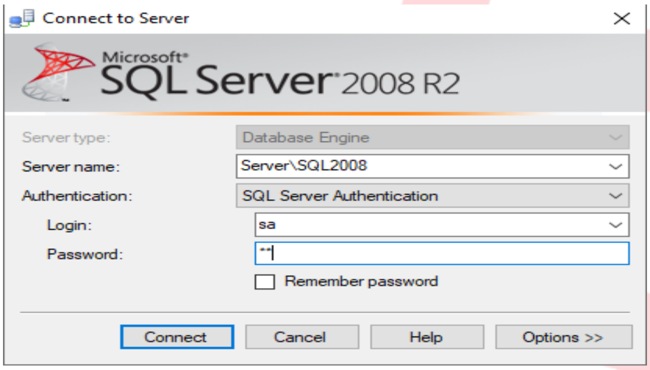
- Login the SQL Server 2008

  Server Name: Server\SQL2008 (Computer_Name\Instance Name)

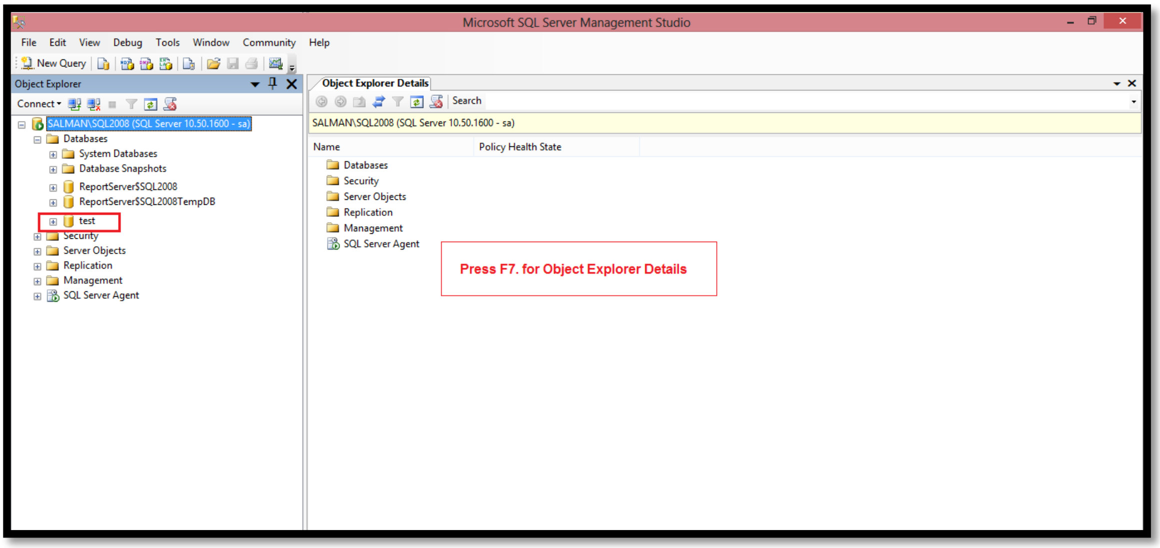
  Login: sa

  Password: Techno123 (use password set during installation)

  Click Connect (you can change password later)



- This is SQL Server 2008 Main Interface

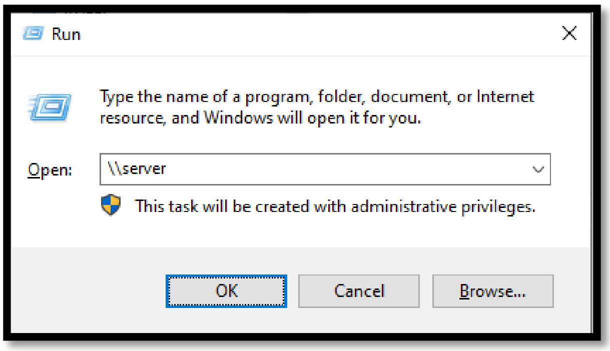


Your SQL Server 2008 is Successfully Installed.

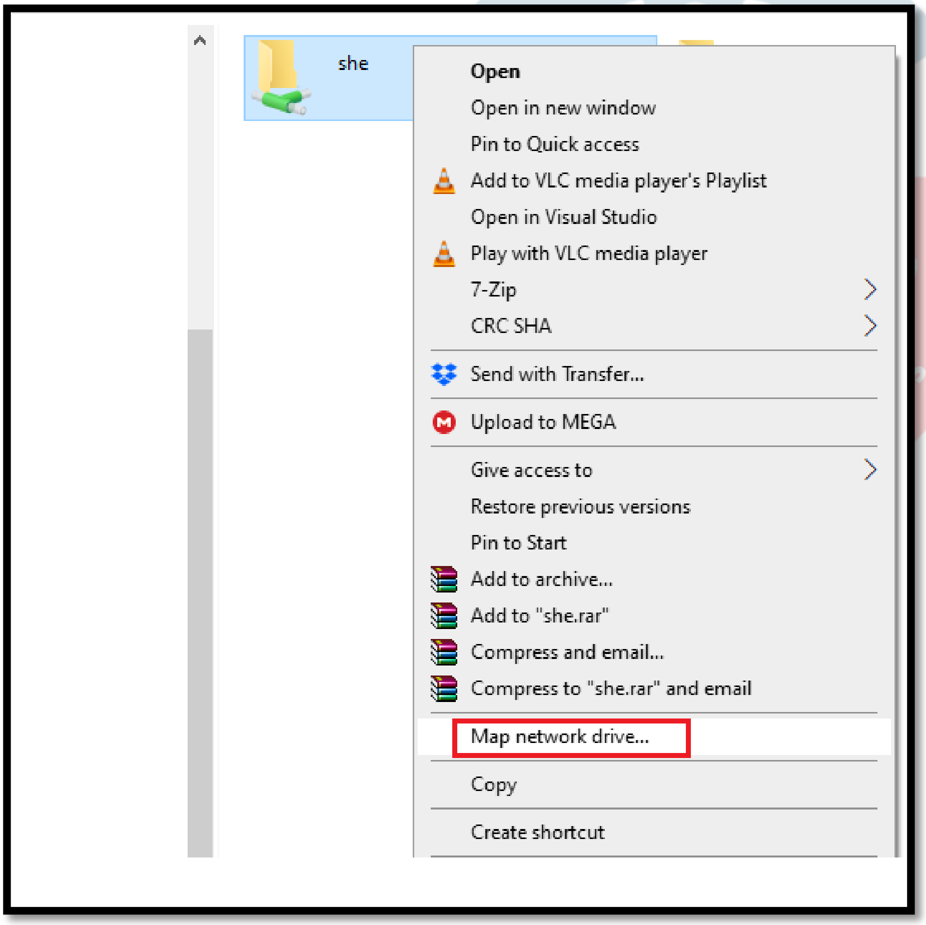
1.17. Thumb (Biometric) System Installation

1.17.1. Make S:\ Drive

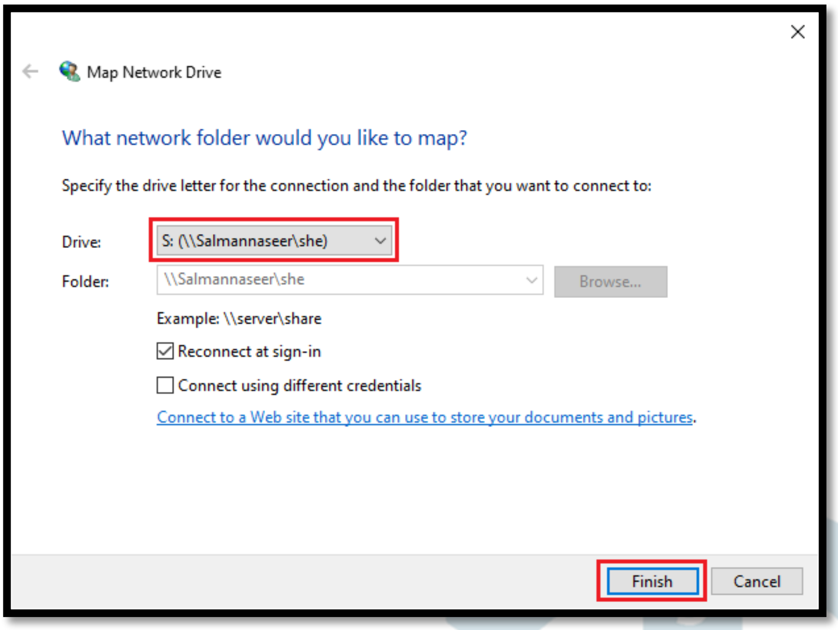
- Start “Run”
- Go to Your Server Computer



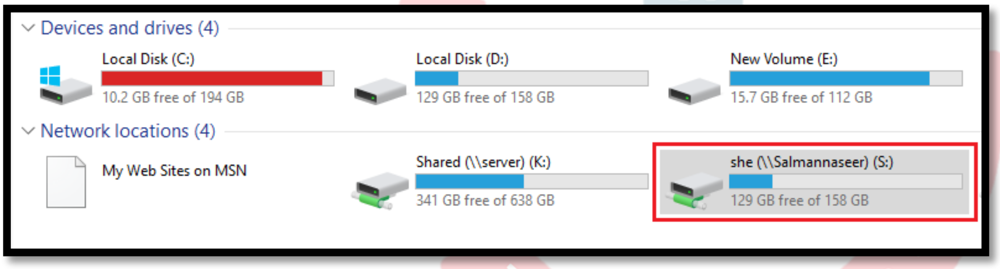
- Right click on “SHE” Folder
- Click “Map Network Drive”



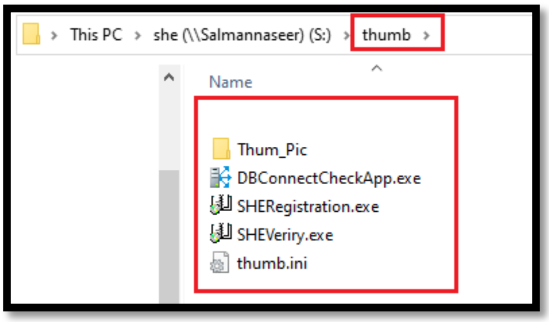
- Select Letter “S”
- Click “Finish”



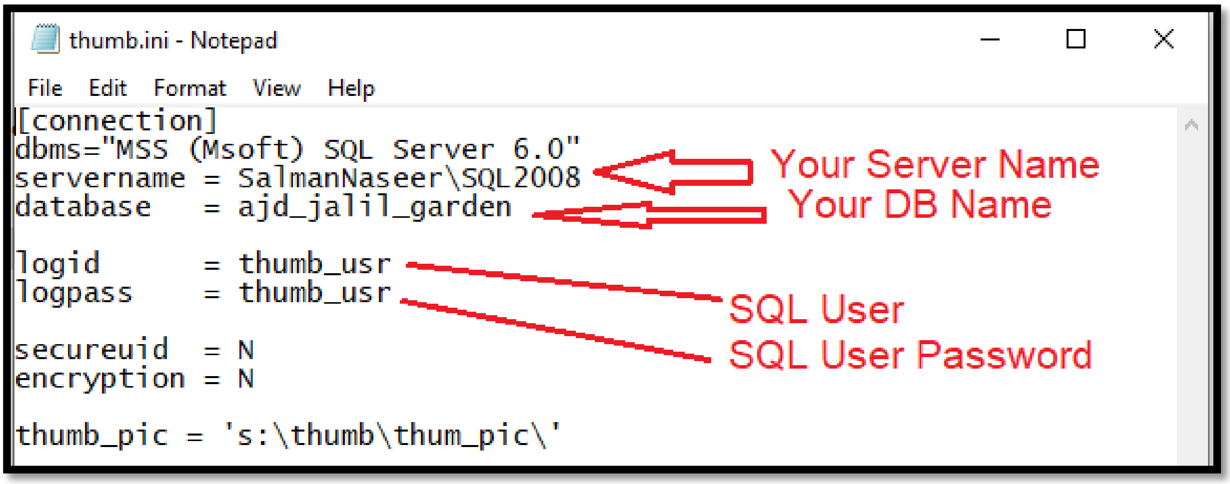
- See Map Drive Done as below



- Place Thumb Folder as **s:\thumb**
- Make sure folders and files in thumb folder
  - Thum_Pic
  - DBConnectCheckApp.exe
  - SHERegistration.exe
  - SHEVeriry
  - Thumb.ini

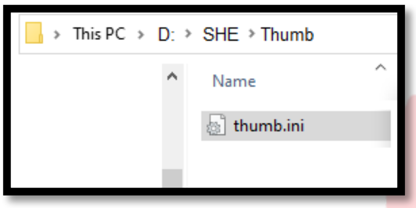


Thumb.ini File configuration



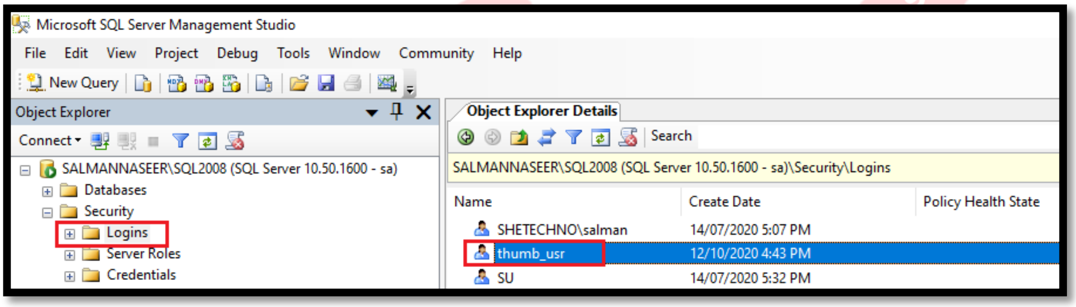
1.17.2. Client System Setting (if you have client systems)

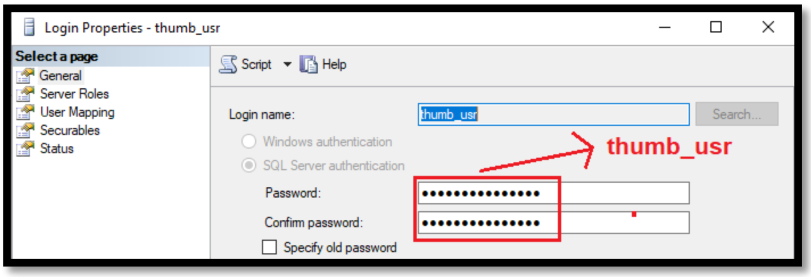
Place thumb.ini File in Client System as **d:\she\thumb\thumb.ini** & install SDK (1.15.4)



1.17.3. Make SQL User "thumb_usr"

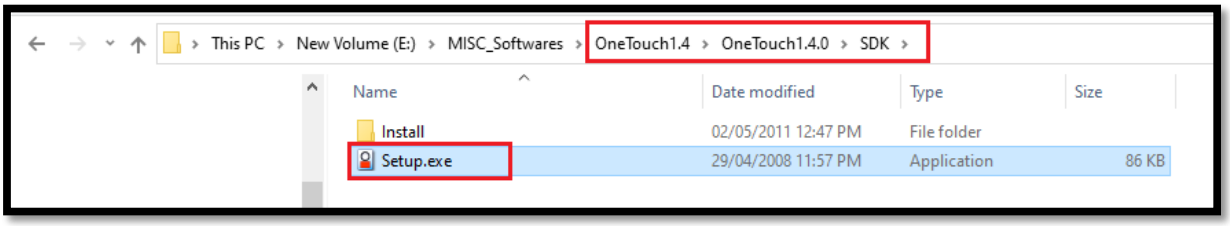
- Make user "thumb_usr"
- Password also set "thumb_usr"





1.17.4. SDK Installation (Thumb Device Software)

- Install this software for integrate thumb device
- Right Click "**Run as Administrator**"
- Next + Next + Install
- Finish



1.17.5. .Net Application case (This step is only do if you are using .Net Application

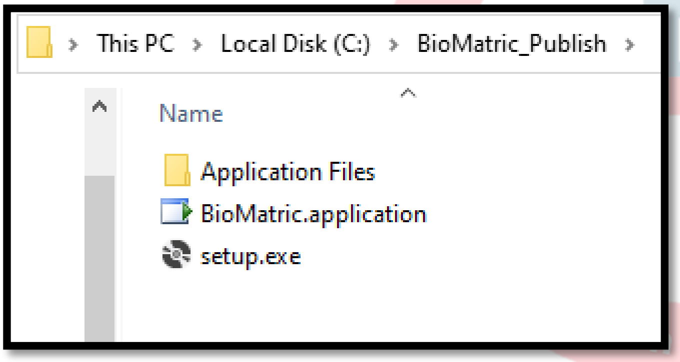
Place Files

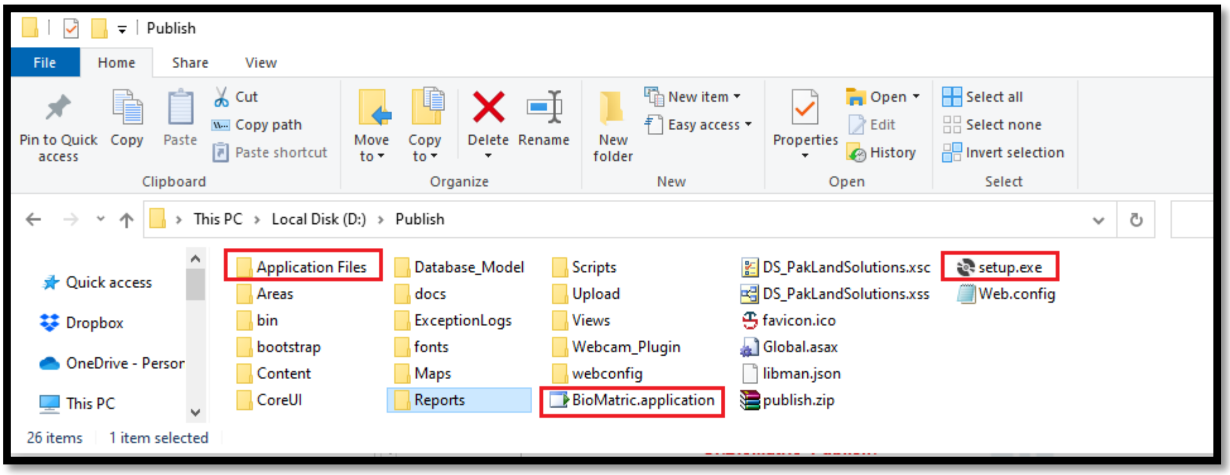
Application Files
BioMatric.application
setup.exe

at below 2 paths

C:\BioMatric_Publish

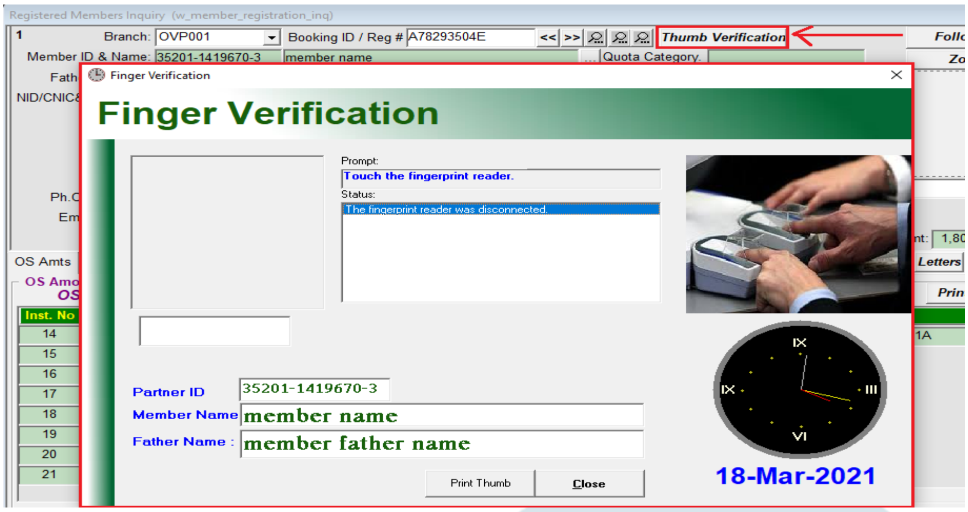
D:\Publish



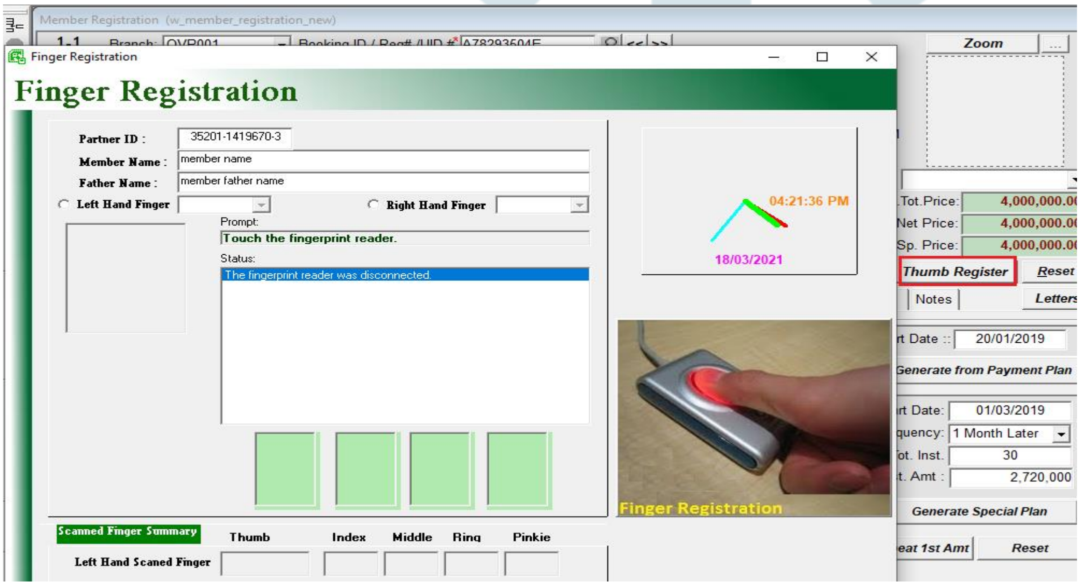


Now thumb system will run as below

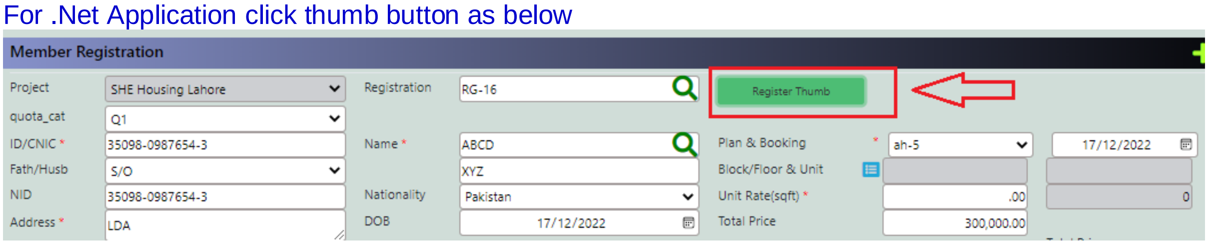
- Click Button “Thumb Verification”
- Finger Verification window will show



- Click “Thumb Register”
- See “Finger Registration” Popup as below screenshot



- For .Net Application click thumb button as below

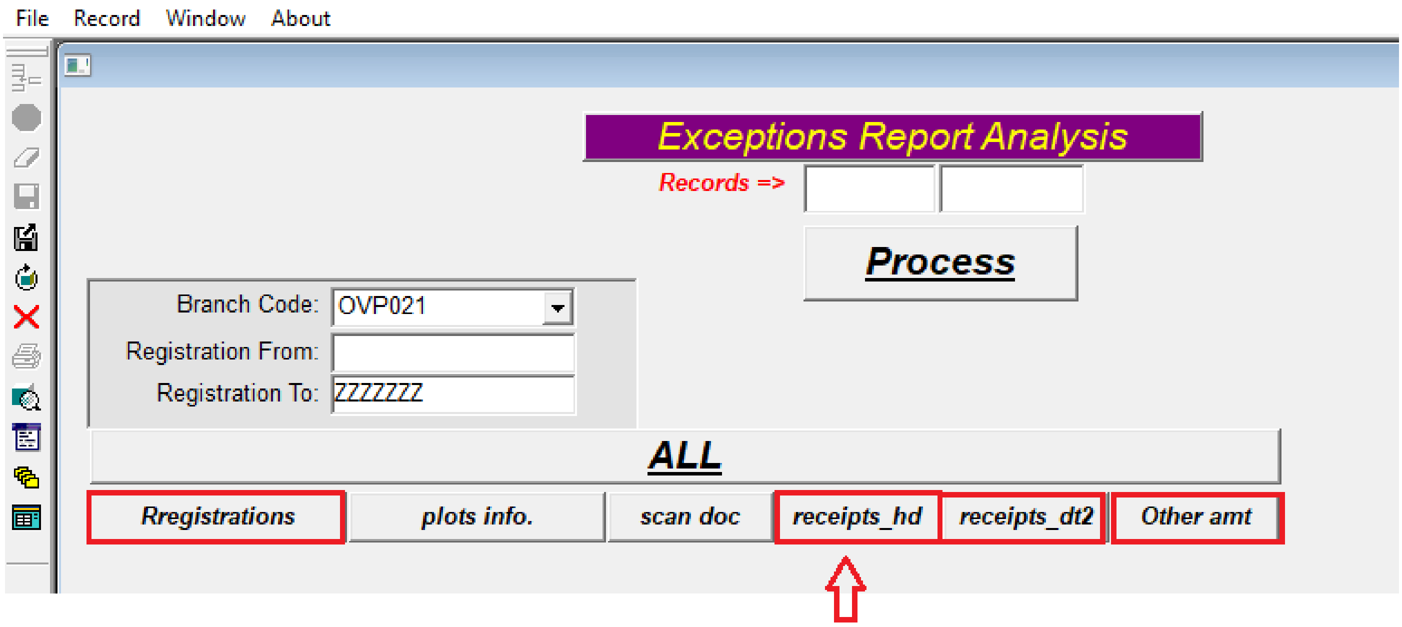


1.18. Exceptions (How to resolve exceptions)

There are some exception reports, that administrator should monitor and make arrangement to correct for smooth running of software and business.

Maintenance → Misc → Exception Information → Exceptions

- Click One by One
  - Registrations Button (exceptions in registrations)
  - Receipts_hd (exceptions in receipts)
  - Receipts_dt2 (exceptions in receipt detail)
  - Other amt (Exceptions in other payments)
- Highlighted buttons are related to SAMS

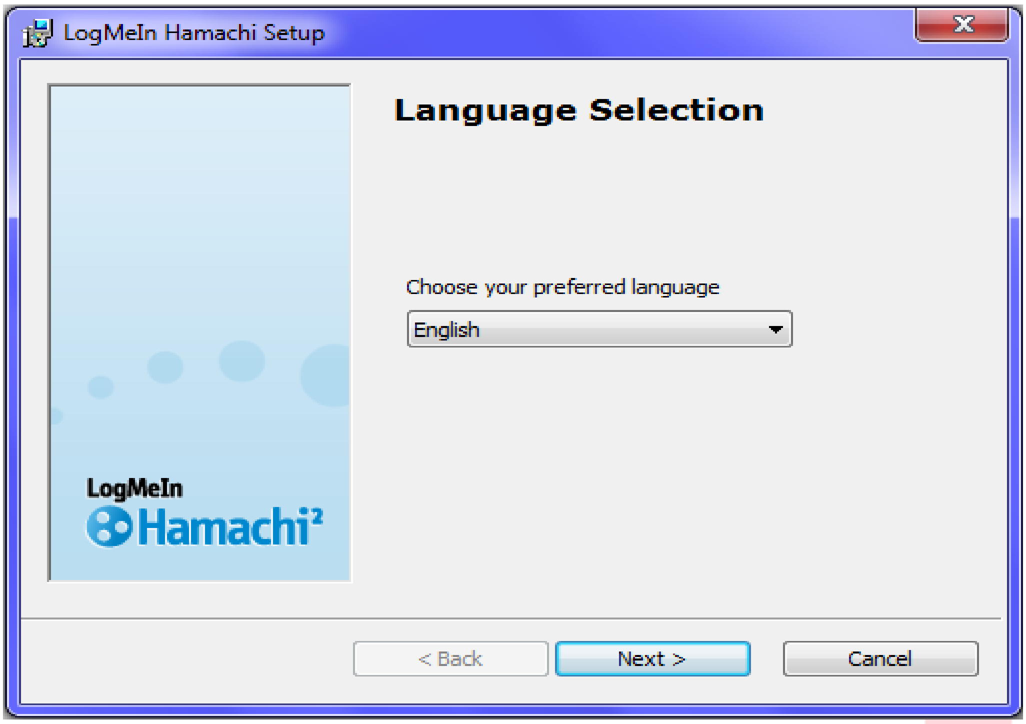


1.19. Wan Server with Hamachi

SHE Software on WAN (Wide Area Network)

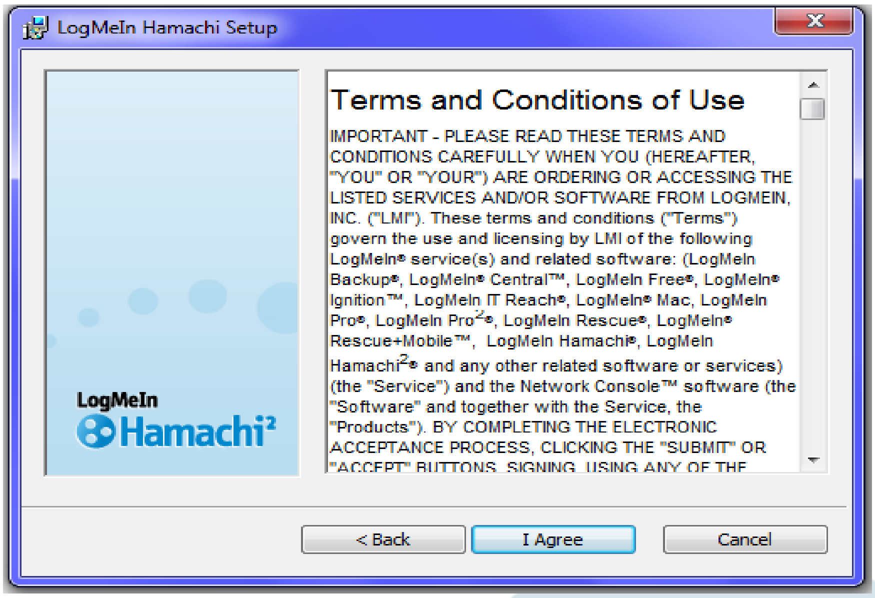
1.19.1. Server-Side Installation: -

- Double Click on Hamachi Installer Exe file. + Click **Next**



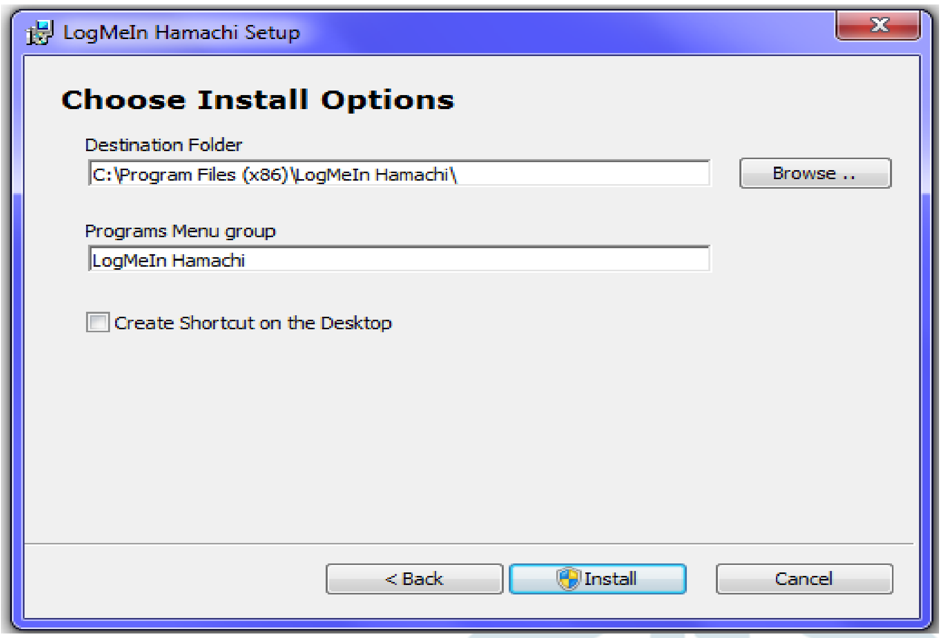
- Click on Next Button.

- Click on I Agree Button.

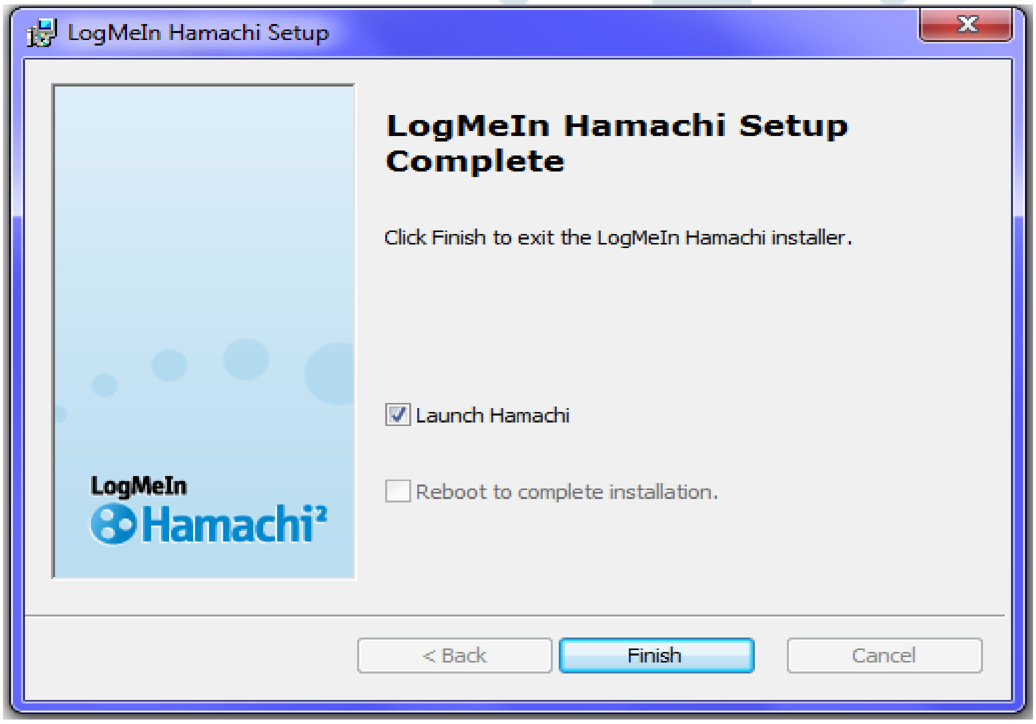


- Next

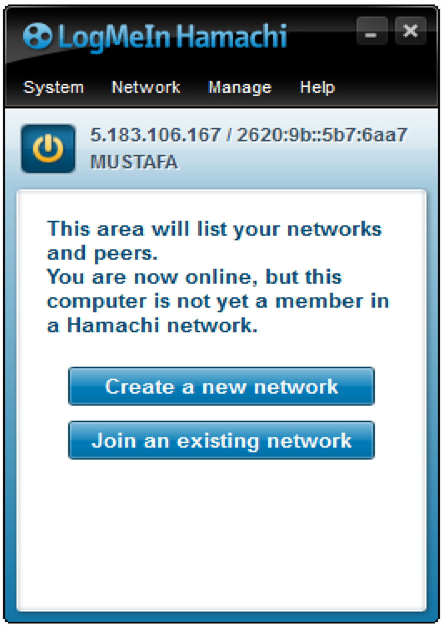
- Click “Install”



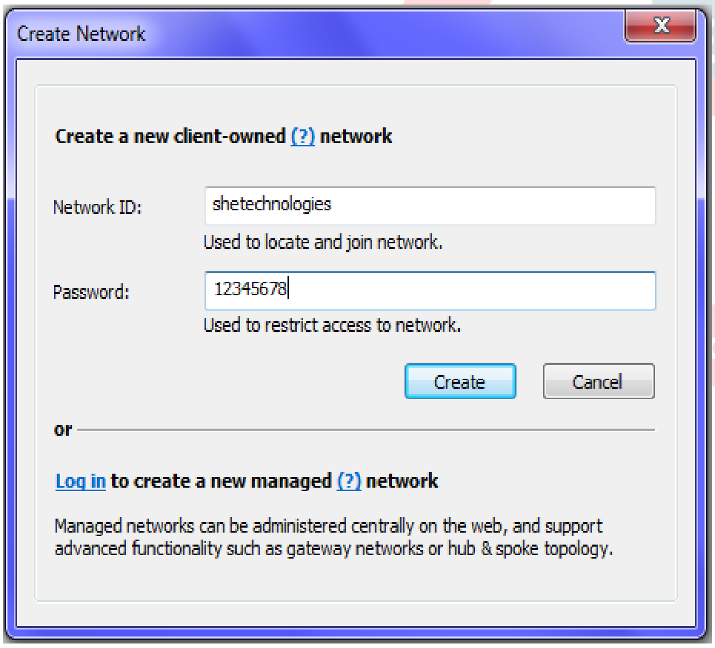
- Click on Finish Button.

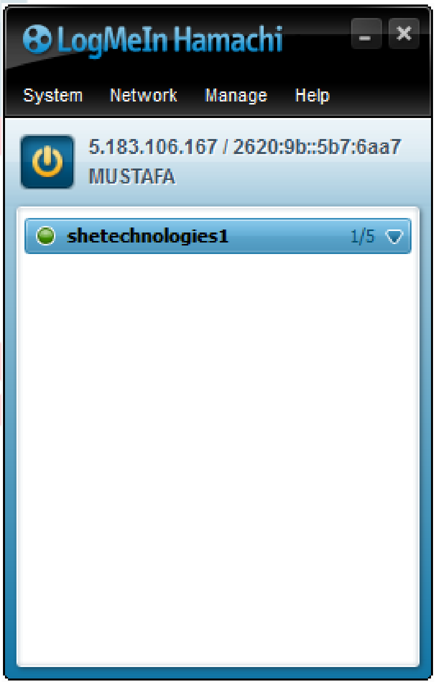


- Click on Create a new network.



- Set Network ID: server_name
- Password (to join network)

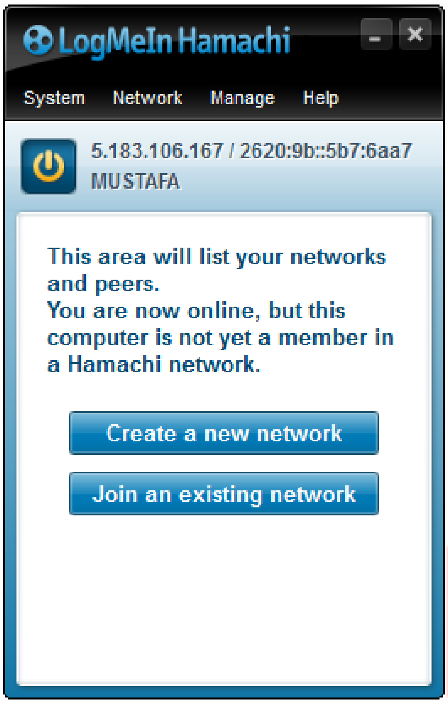


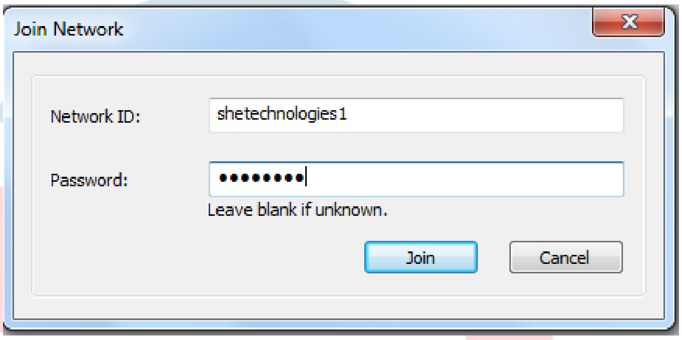


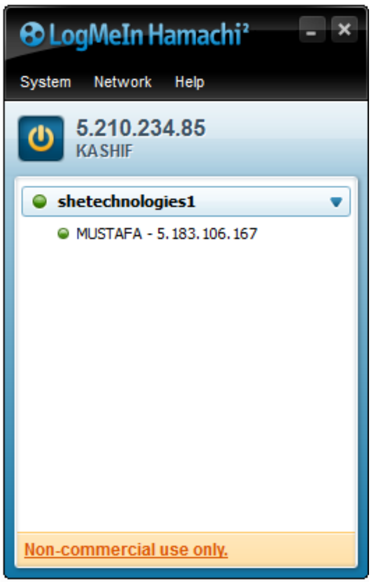
WAN Server Configuration Done Successfully.

1.19.2. Client Connectivity with Server: -

- Install Hamachi as installed on server
- Click "Join an Existing Network" (for client system)
  - Give network name i.e. defined during create network
  - Give password i.e. password of network defined
- Click on Join Button.





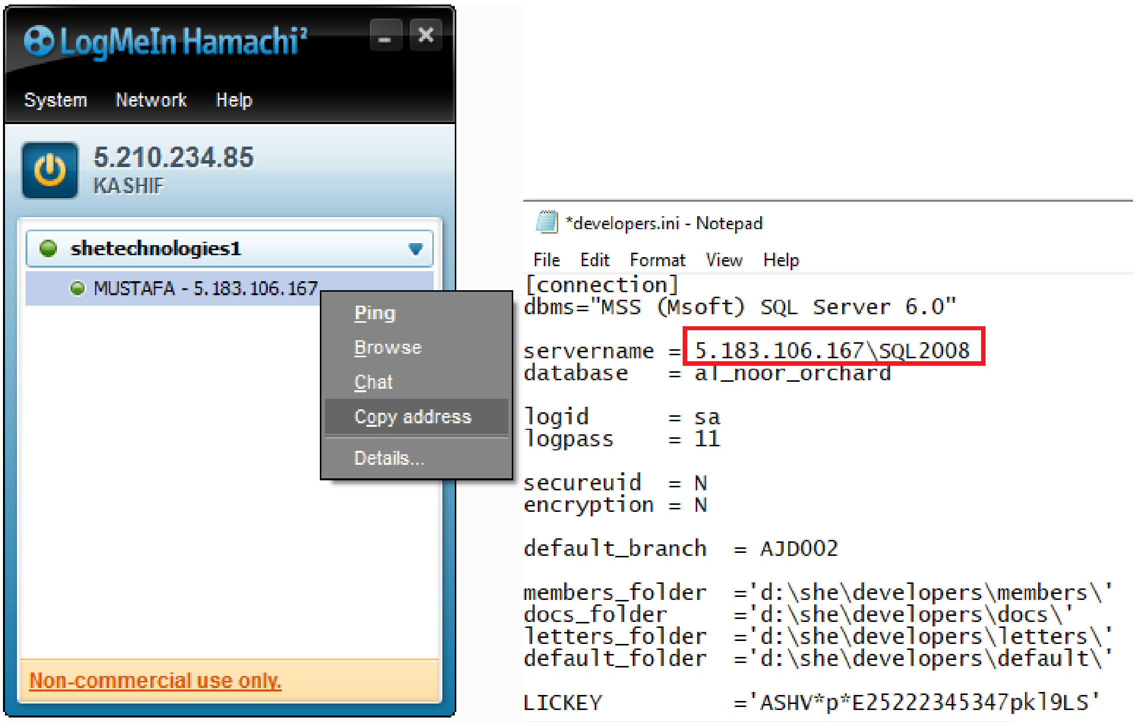


WAN Network Created and Joined Successfully
i.e. PC Name Mustafa with its Hamachi IP 5.183.106.167

SHE Technologies
A Software, Web Development & Consultant Co.

Server and Client are installed and Joined Successfully. Use its IP to access Server / PC and run software.

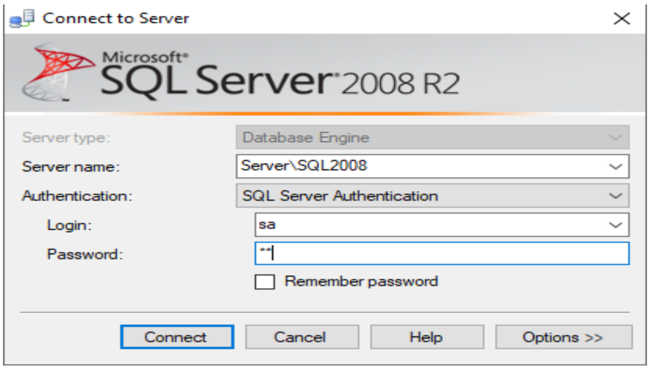
- Right click on Server name and click on Copy Address.
- Use This IP in developers.ini to run software using WAN



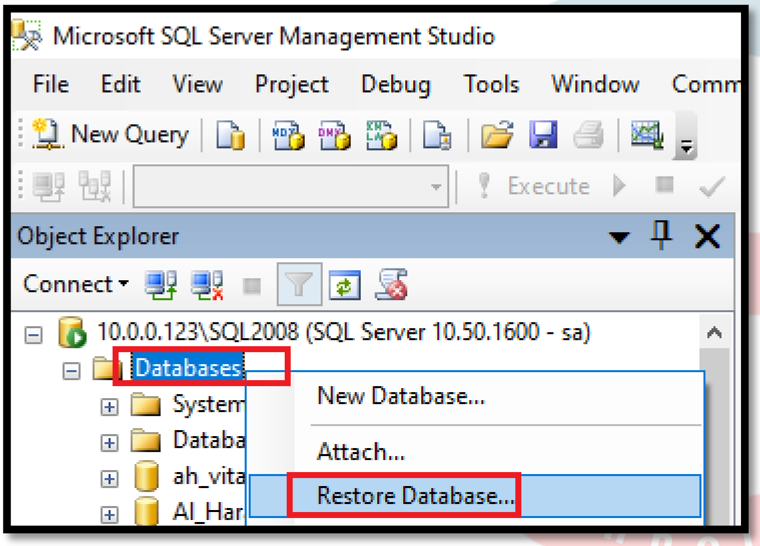
Note: - Minimum Internet speed 4MB required on both side.

1.20. Restore Database in SQL Server

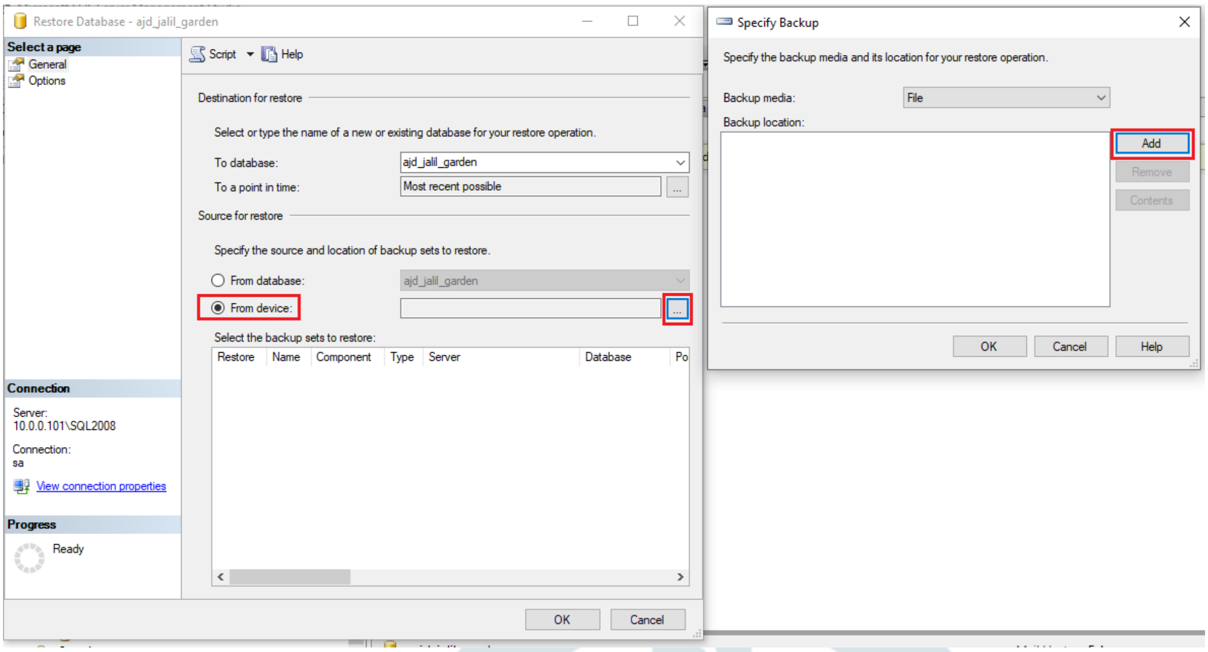
- Login to SQL Server Management Studio



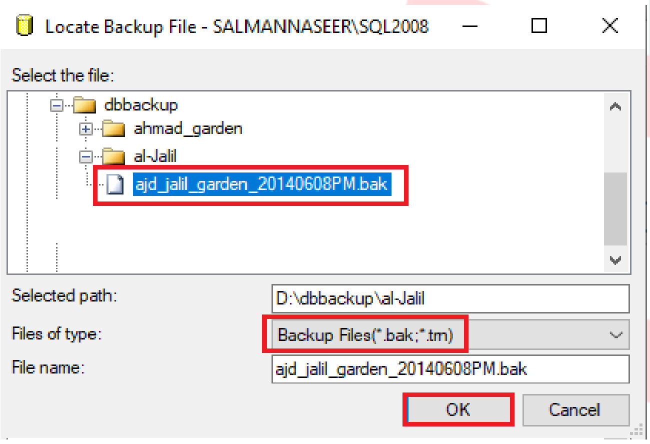
- Create your database if not in list (new SQL server is installed)
- Right click "**Databases**"
- Click "**New Database…**"



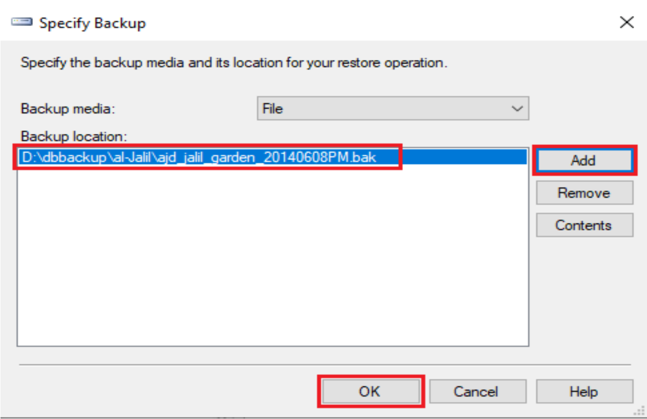
- Click “**From device**” → Click “…” → Add →



- Select **backup file** from your folder i.e. ajd_jalil_garden_20140608PM.bak
- Click “**OK**”

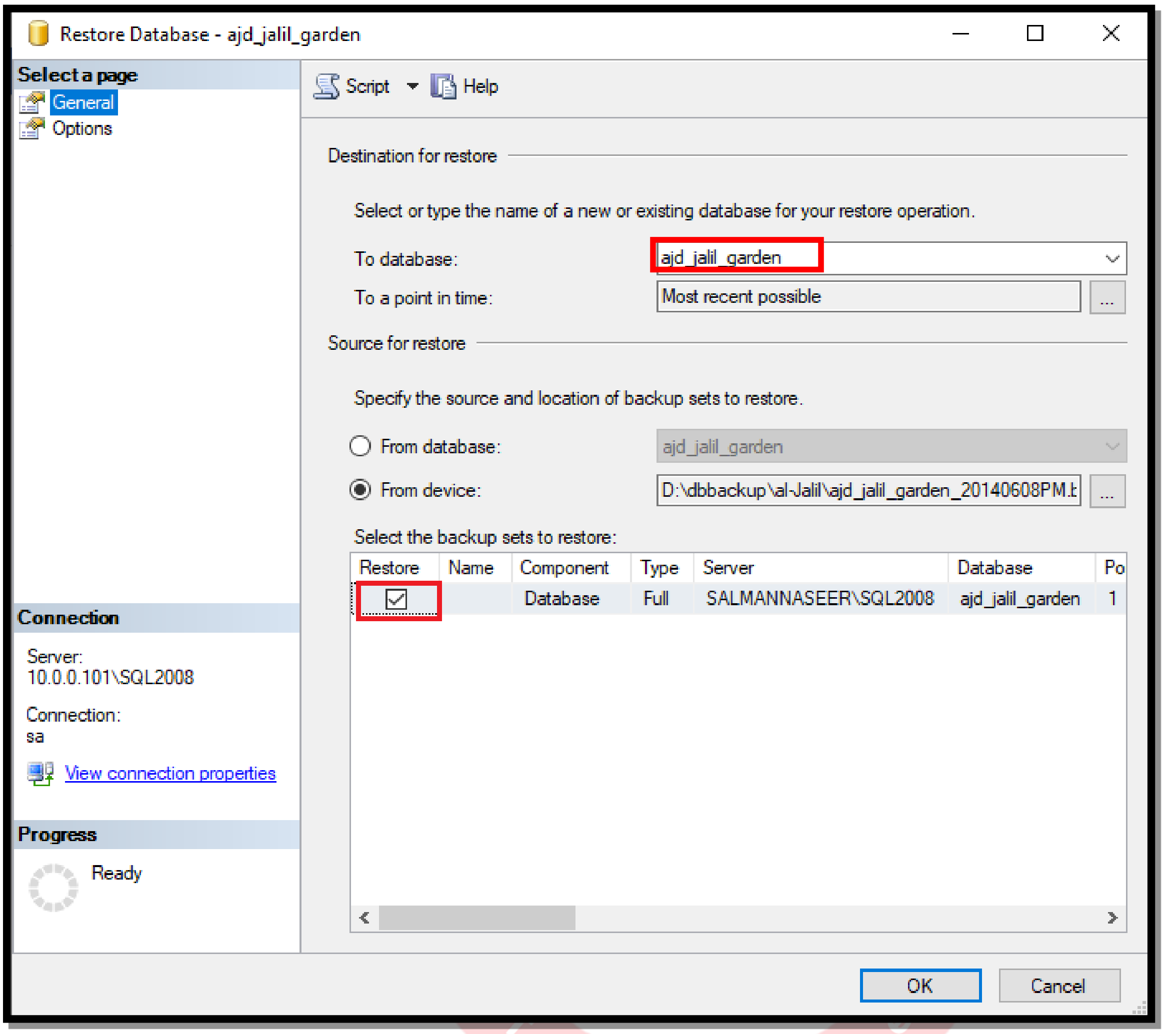


- Click “**OK**”

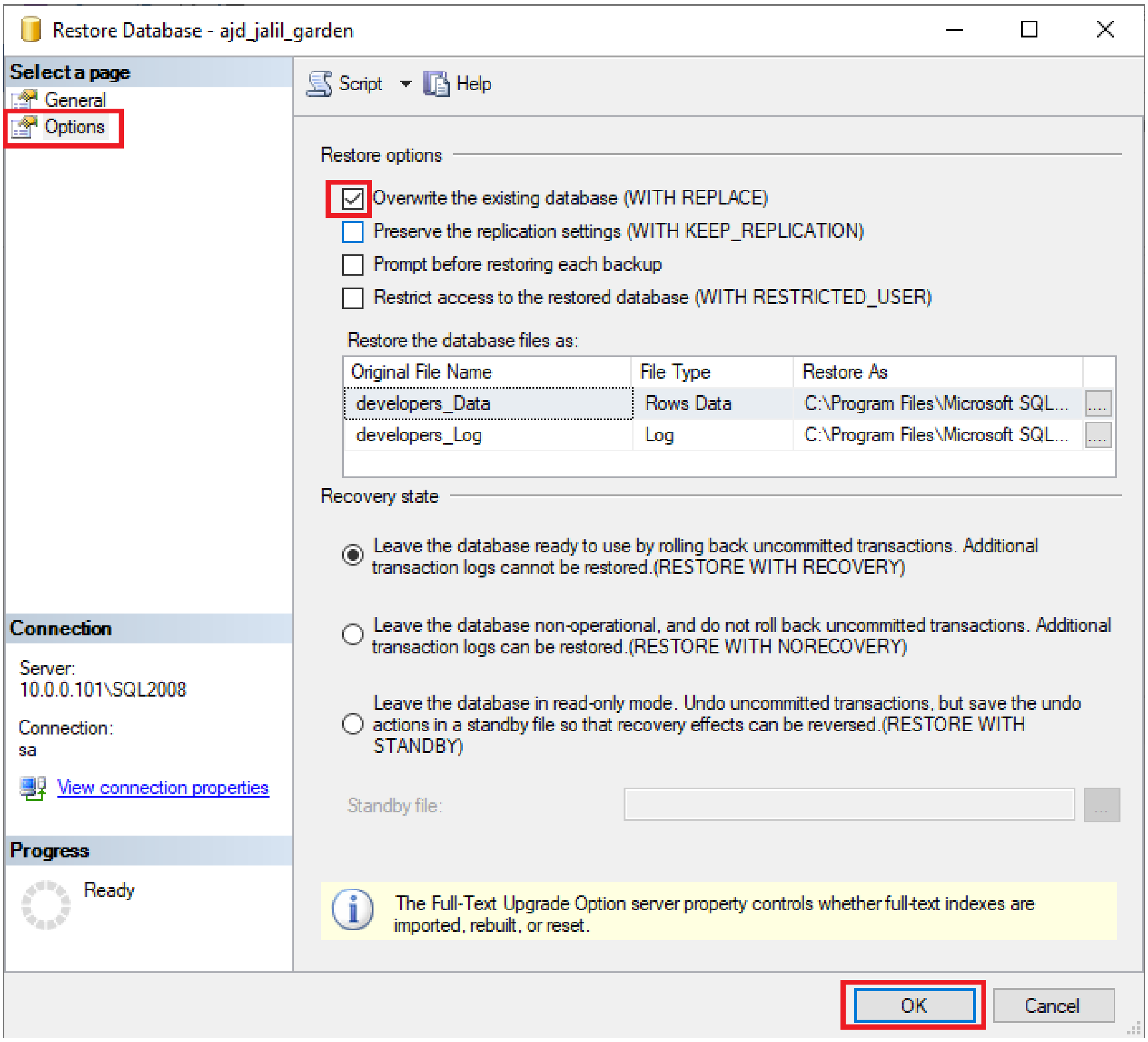


- **“Tick”** Restore

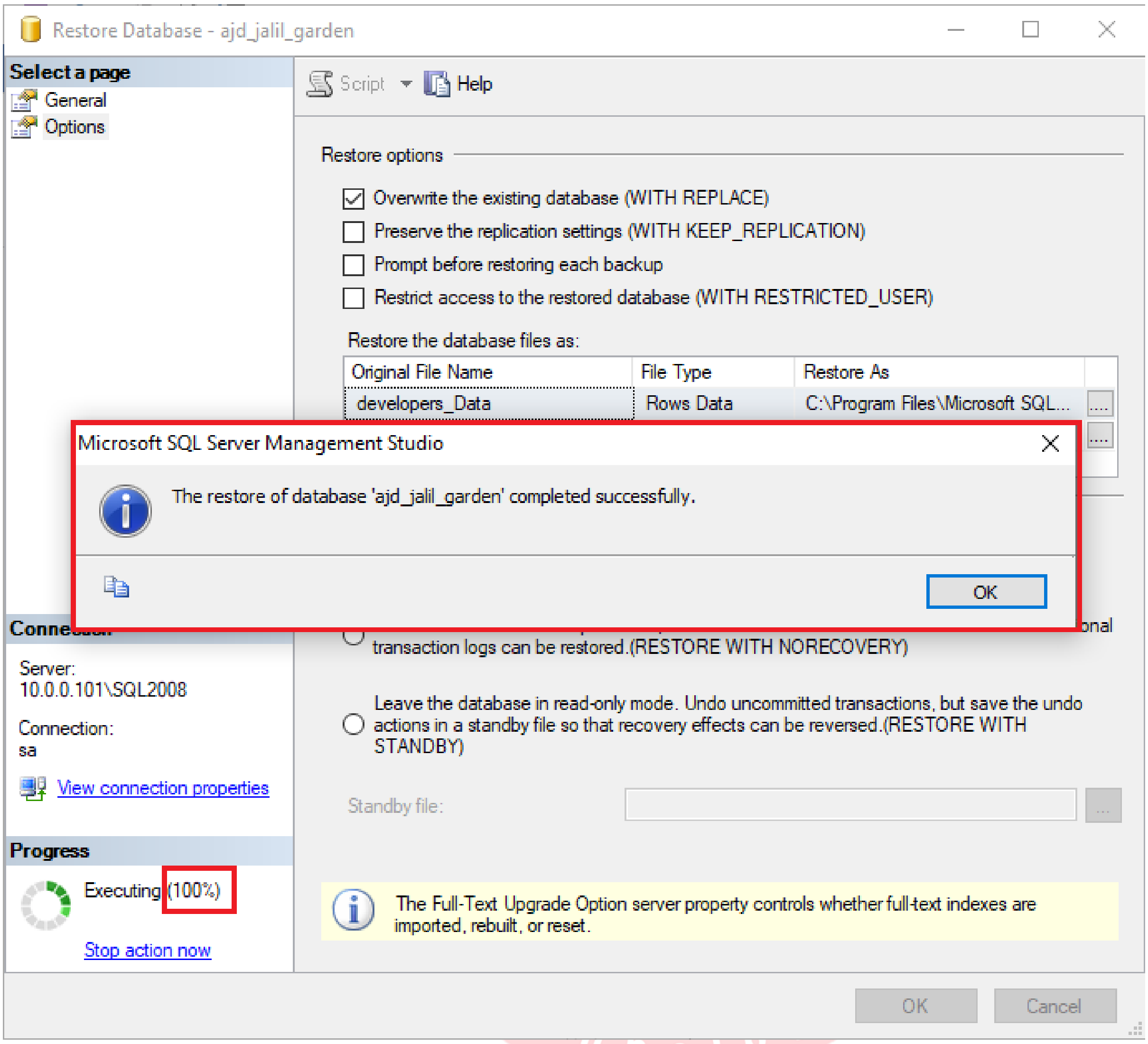
- Select **Database Name** i.e. ajd_jalil_garden



- Click "**Options**"
- "**Tick**" overwrite the exisiting databae (with replace)
- Click "**OK**"



- Database is restored successfully.



1.21. User Management

1.21.1. Introduction

Welcome to the User Management Module Guide.

This guide explains how to manage users within the ERP system. It covers user creation, updates, permission management, and password resets simply and practically.

User Management plays a key role in system security. It controls who can access the system and what actions they are allowed to perform.

1.21.2. Purpose of the Module

The User Management module is designed to create and manage user accounts, control ERP access, assign permissions based on job roles, improve system security, and maintain proper user records.

1.21.3. Before You Begin

Before creating or updating users, make sure all employee details, email addresses, mobile numbers, and required permissions are available and verified.

1.21.4. User Types

The ERP system supports Admin, Staff, and Client user types with different levels of system access.

1.21.5. Navigation Shortcuts

Use the following navigation paths for quick access to user management features.

Task	Navigation Path
Create User	Settings → Users → Create User
Update User	Settings → Users → View User → Edit
Reset Password	Settings → Users → Reset Password
Update Rights	Settings → Users → View User → Edit

1.21.6. Create User

This feature allows authorized users to create new system accounts.

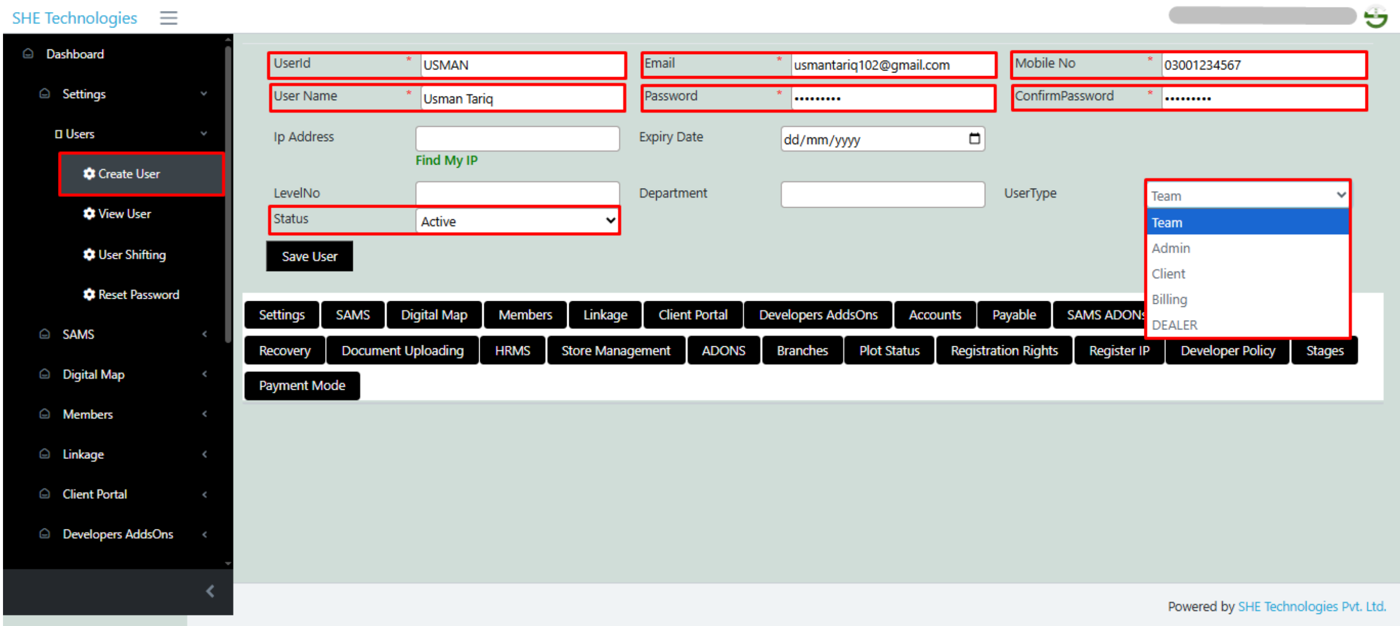
Required Fields

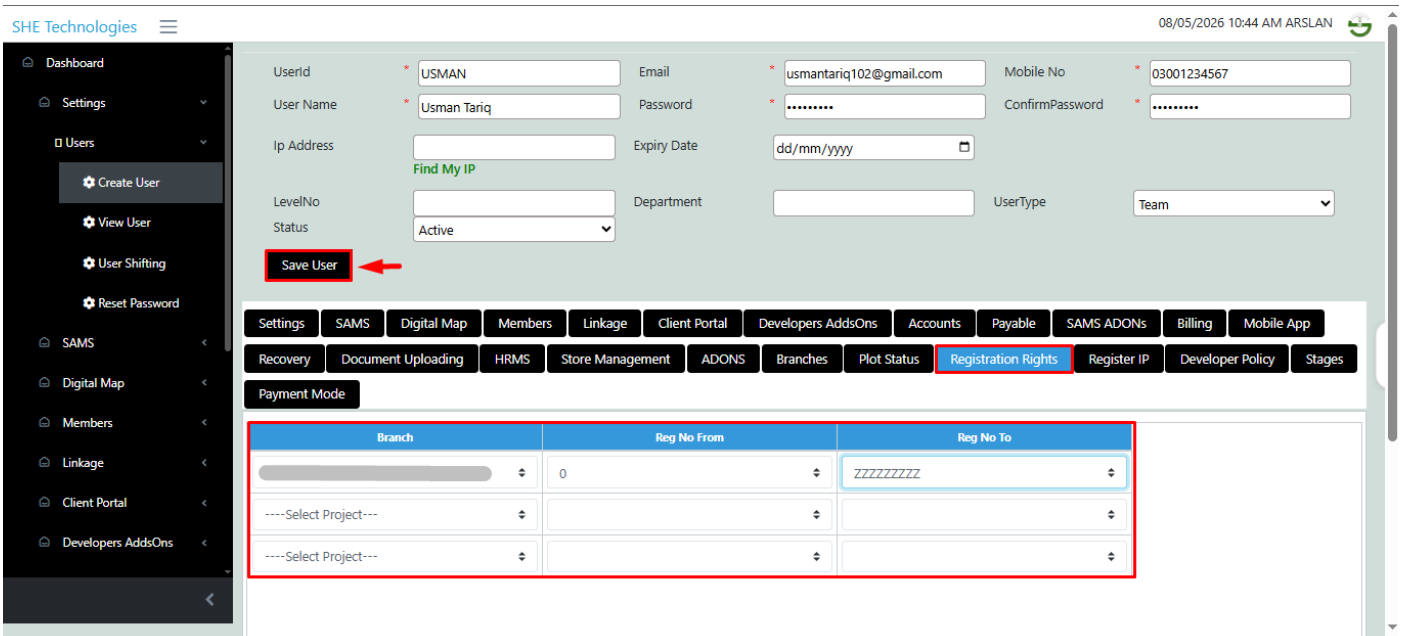
- User ID
- User Name
- Mobile Number

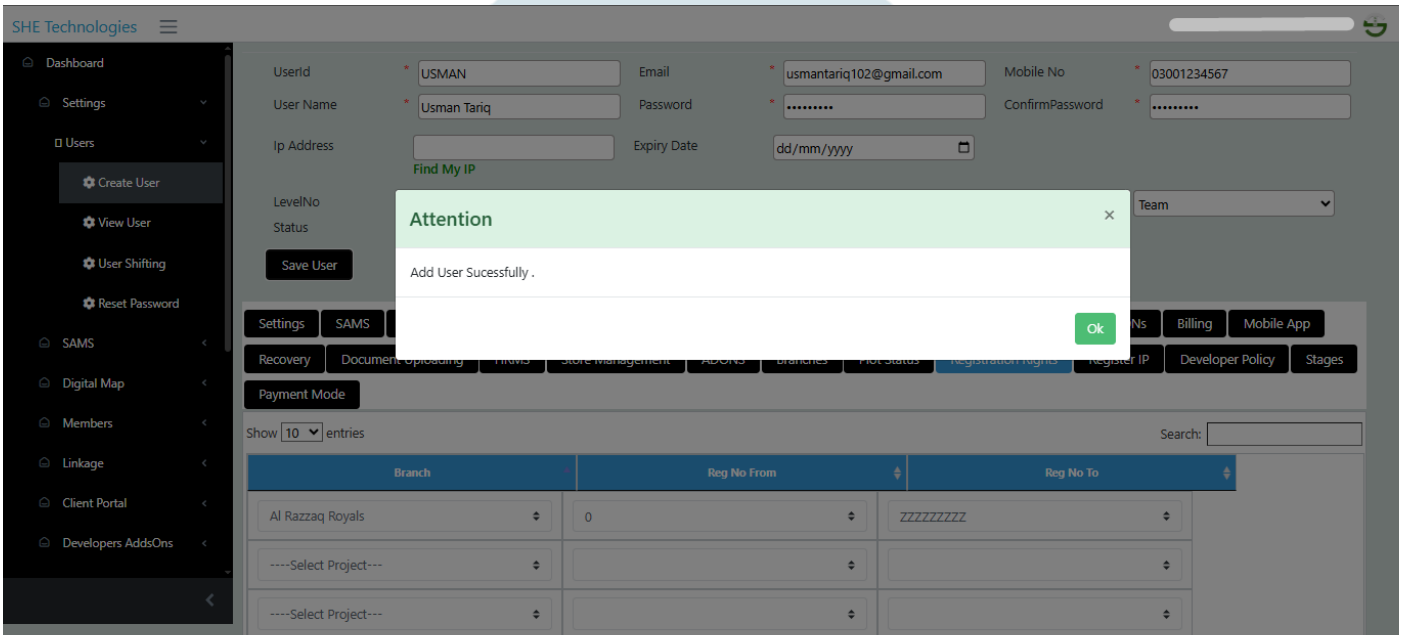
- Email ID
- Password

Steps to Create a User

1. Open Settings → Users → Create User
2. Enter all required user information
3. Select User Type and Status
4. Assign rights and permissions
5. Click the Save User button







User Fields

Field	Description
User ID	Unique identification code
User Name	Full user name
Mobile Number	Official contact number
Email ID	Valid email address
Password	Login password

User Type	Admin / Staff / Client
Status	Active / Inactive

User Rights/Permissions

Permission	Description
Add	Create records
Edit	Modify records
Delete	Remove records
View	Access and view screens
Can Values	Access configurable values/features

Tip: Assign only the permissions required for the user's role.

1.21.7. Update User

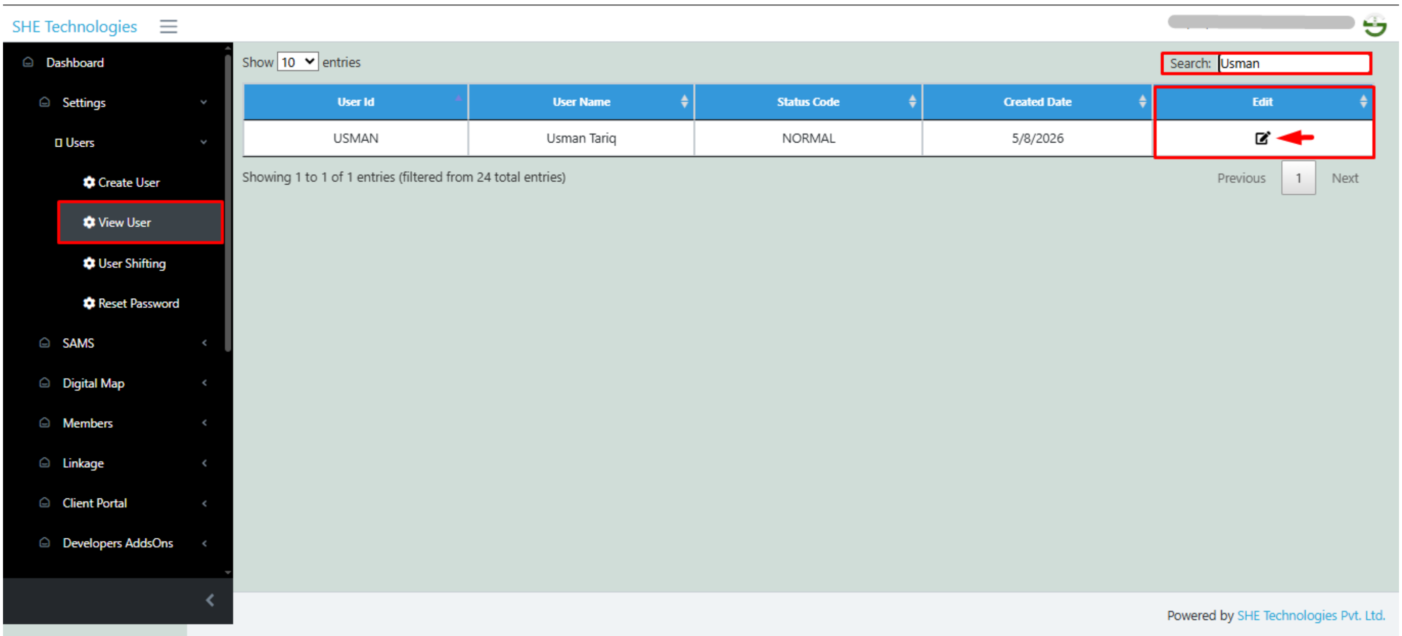
This feature allows authorized staff to update existing user information and permissions.

Information That Can Be Updated

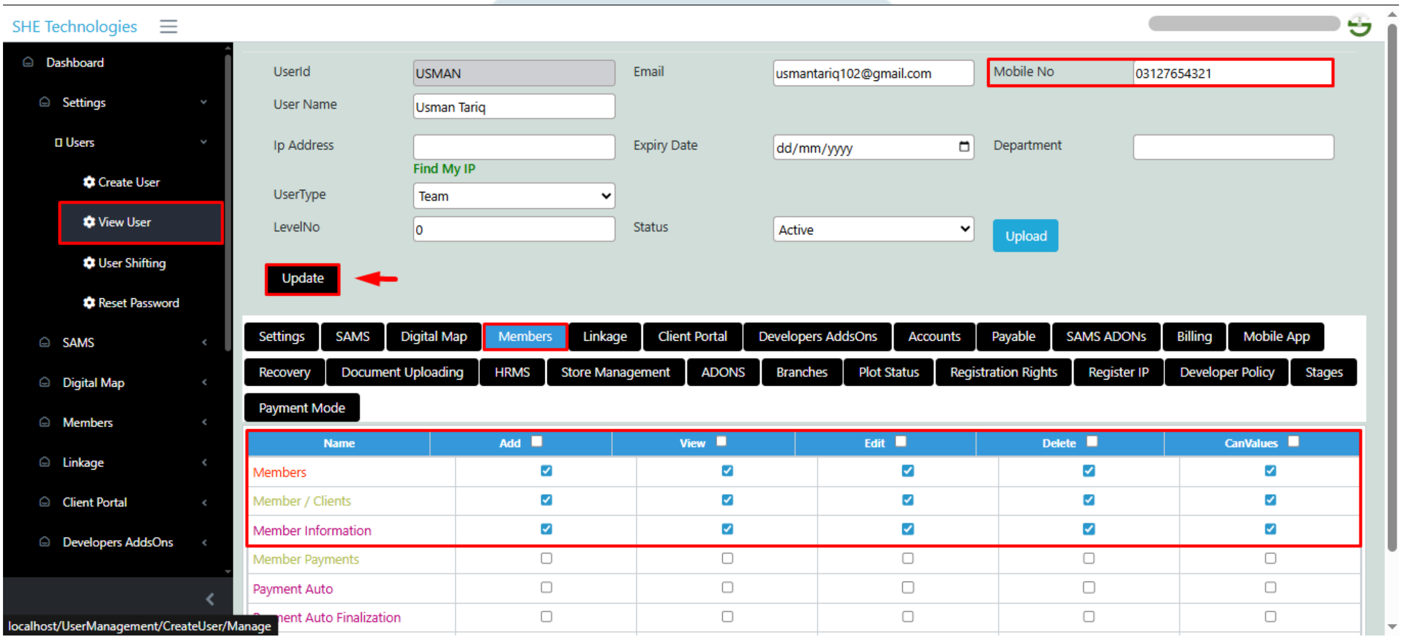
- Email ID
- Mobile Number
- User Name
- User Type
- User Status
- Module/Screen Rights

Steps to Update User

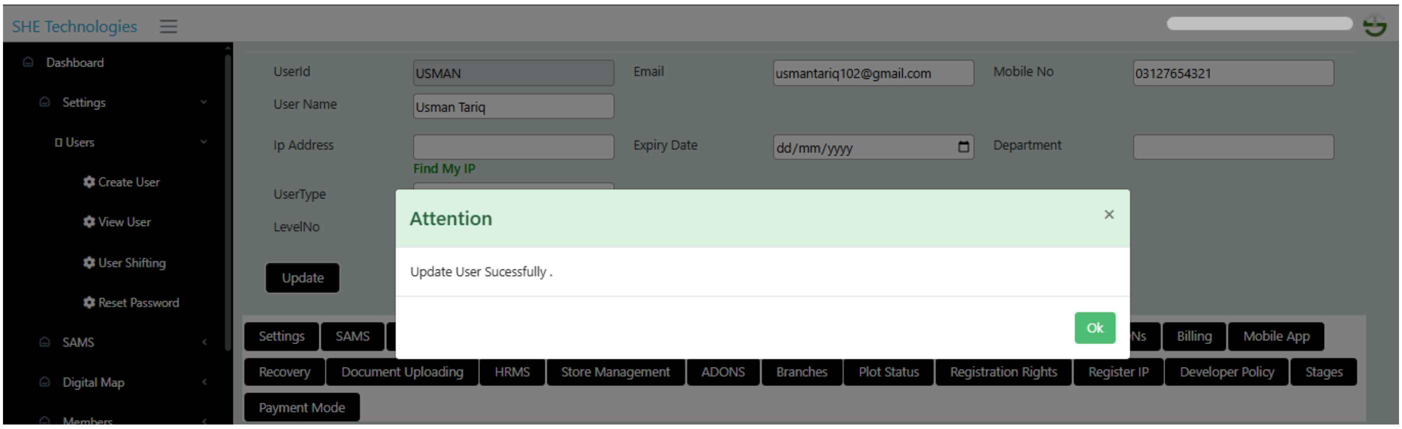
1. Open Settings → Users → View User
2. Search for the user using User ID or User Name
3. Click the Edit button
4. Modify the required information
5. Update permissions if needed
6. Click the **Update** button



SHE Technologies
Dashboard
Settings
Users
Create User
View User
User Shifting
Reset Password
SAMS
Digital Map
Members
Linkage
Client Portal
Developers AddsOns
Show 10 entries
Search: Usman
User Id
User Name
Status Code
Created Date
Edit
USMAN
Usman Tariq
NORMAL
5/8/2026
Showing 1 to 1 of 1 entries (filtered from 24 total entries)
Previous
1
Next
Powered by SHE Technologies Pvt. Ltd.



SHE Technologies
Dashboard
Settings
Users
Create User
View User
User Shifting
Reset Password
SAMS
Digital Map
Members
Linkage
Client Portal
Developers AddsOns
UserId
USMAN
Email
usmantariq102@gmail.com
Mobile No
03127654321
User Name
Usman Tariq
Ip Address
Expiry Date
dd/mm/yyyy
Department
Find My IP
UserType
Team
LevelNo
0
Status
Active
Upload
Update
Settings
SAMS
Digital Map
Members
Linkage
Client Portal
Developers AddsOns
Accounts
Payable
SAMS ADONS
Billing
Mobile App
Recovery
Document Uploading
HRMS
Store Management
ADONS
Branches
Plot Status
Registration Rights
Register IP
Developer Policy
Stages
Payment Mode
Name
Add
View
Edit
Delete
CanValues
Members
Member / Clients
Member Information
Member Payments
Payment Auto
Payment Auto Finalization
localhost/UserManagement/CreateUser/Manage



SHE Technologies
Dashboard
Settings
Users
Create User
View User
User Shifting
Reset Password
SAMS
Digital Map
UserId
USMAN
Email
usmantariq102@gmail.com
Mobile No
03127654321
User Name
Usman Tariq
Ip Address
Expiry Date
dd/mm/yyyy
Department
Find My IP
UserType
LevelNo
Update
Attention
Update User Sucessfully .
Ok
Settings
SAMS
Billing
Mobile App
Recovery
Document Uploading
HRMS
Store Management
ADONS
Branches
Plot Status
Registration Rights
Register IP
Developer Policy
Stages
Payment Mode

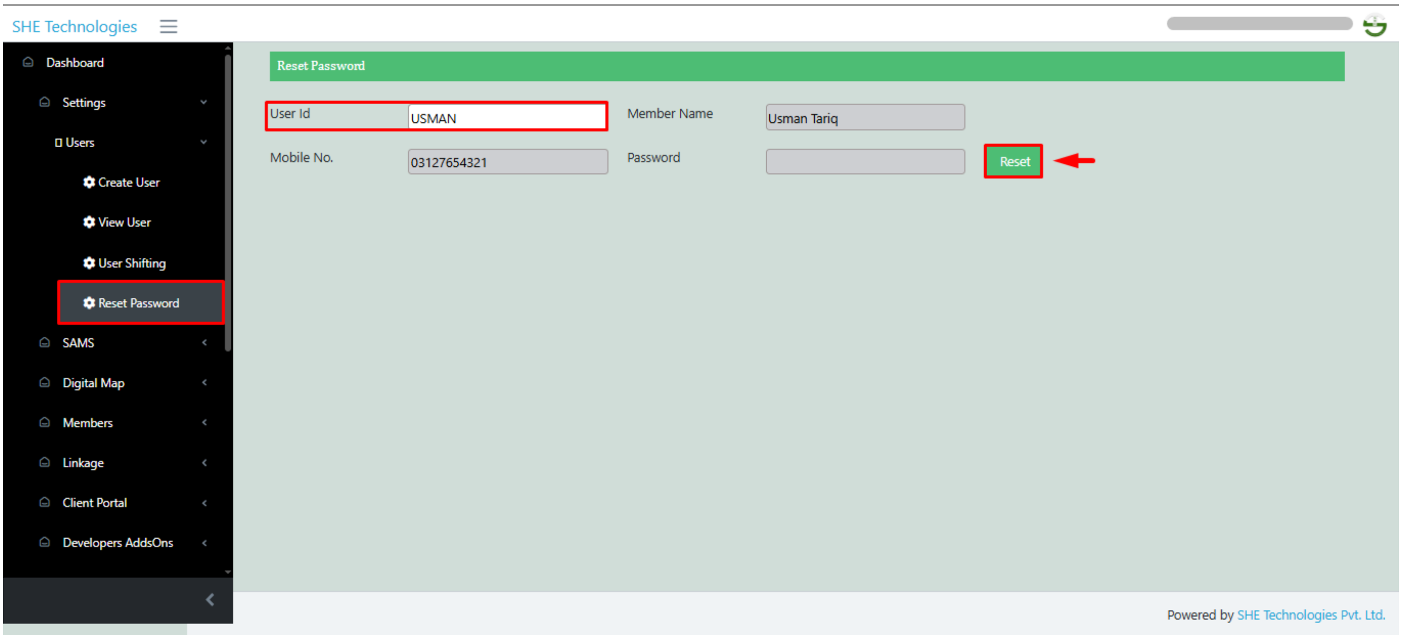
Tip: Ask users to log out and log back in after permission changes.

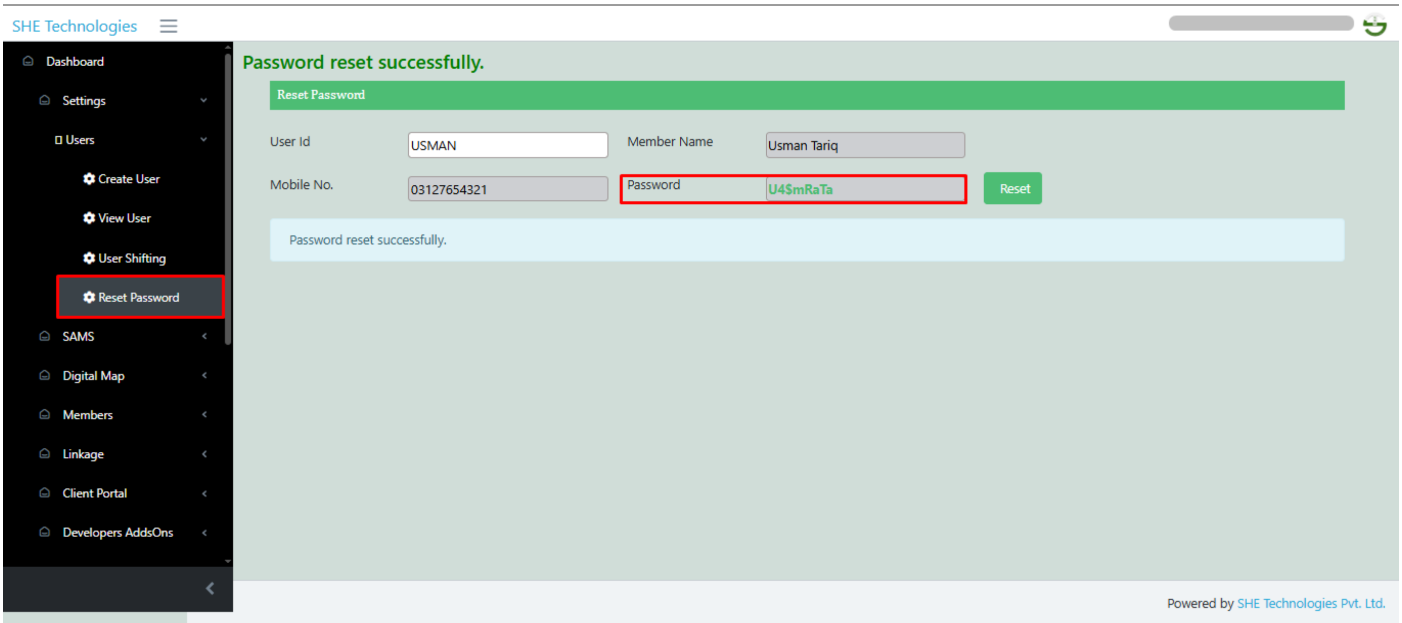
1.21.8. Reset Password

This feature allows authorized staff to reset passwords for existing users.

Steps to Reset Password

1. Open Settings → Users → Reset Password
2. Enter the correct User ID
3. Click Reset Password
4. Share the temporary password securely





Tip: Always verify the user's identity before resetting passwords.

1.21.9. User Rights Management

User rights control access to modules, screens, and actions.

Right	Description
View	User can view records/screens
Add	User can create records
Edit	User can update records
Delete	User can remove records
Can Values	User can access configurable values

Password Policy

Passwords must follow company security standards.

- ✓ Minimum 8 characters
- ✓ At least 1 uppercase letter
- ✓ At least 1 lowercase letter
- ✓ At least 1 number
- ✓ At least 1 special character

Example Password: Sams@2026

Tip: Avoid using mobile numbers, employee names, or simple passwords like Admin@123.

Validations and Error Messages

Validation	Error Message
User ID missing	User ID is required.
User Name missing	User Name is required.
Mobile Number missing	Mobile Number is required.
Email ID missing	Email ID is required.
Password missing	Password is required.
Duplicate User ID	User ID already taken.
Invalid email format	Please enter a valid email address.
Weak password	Password must be at least 8 characters, including uppercase, lowercase, a number, and a special character.

Common Mistakes to Avoid

- Assigning unnecessary Admin rights
- Forgetting to activate newly created users
- Resetting passwords for the wrong user
- Sharing login credentials

Tip: Before saving a user, carefully review the User Type, Status, and Assigned Rights.

1.21.10. Troubleshooting / FAQs

Q1. I cannot create a new user.

Check mandatory fields, duplicate records, and your Add permissions.

Q2. The user cannot log in after account creation.

Verify the account status, password, and assigned permissions.

Q3. I cannot edit user information.

Verify Edit rights or contact the system administrator.

Q4. Password reset is not working.

Verify the User ID and your password reset rights.

Q5. User cannot access a screen.

Verify View rights and assigned module permissions.

Dos and Don’ts

Dos

- ✓ Use unique User IDs
- ✓ Verify details before saving
- ✓ Use strong passwords
- ✓ Review permissions regularly
- ✓ Keep user information updated

Don'ts

- ✗ Do not share passwords openly
- ✗ Do not assign unnecessary Admin rights
- ✗ Do not keep inactive users active
- ✗ Do not reset passwords without verification

1.21.11. Security Recommendations

- Use strong passwords
- Change passwords periodically
- Avoid shared accounts
- Monitor unusual login activity

Tip: Password resets should only be performed for verified users.

Best Practices

- Follow role-based access control
- Assign minimum required permissions
- Maintain password confidentiality
- Keep employee records updated
- Review permissions regularly

1.21.12. Support Information

While reporting issues, provide the following details:

- User ID
- Screen name
- Error message
- Screenshot of the issue
- Date and time of occurrence

1.21.13. Final Notes

The User Management module is one of the most important parts of the ERP system. Accurate user management improves security, reduces operational issues, and ensures the right people have the correct access.

Before You Begin

Before using the Admin Panel, ensure the following:

• You have valid login credentials.

• You have a stable internet connection.

• Images or files prepared for upload meet system requirements.

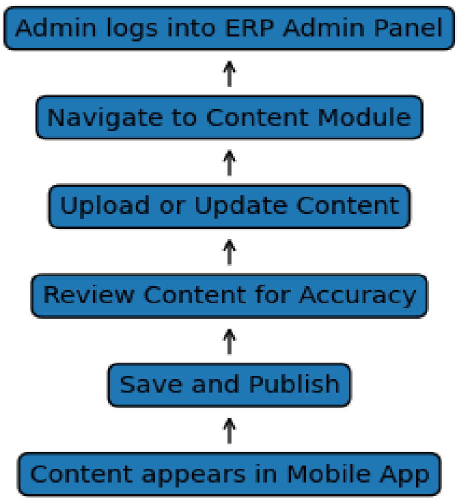
• You have appropriate access permissions.

1.22.1. Introduction

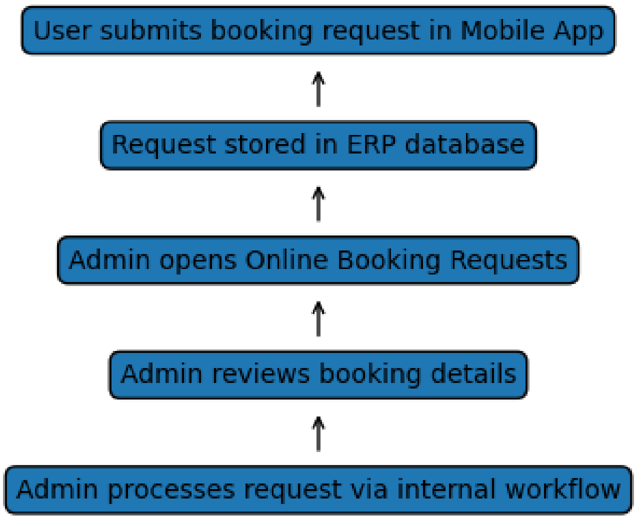
The SAMS ERP Mobile App Admin Panel enables authorized staff to manage and control the information displayed in the mobile application. Through this panel, administrators can update notifications, upload images, manage events, publish payment plans, monitor booking requests, and maintain company information.

1.22.2. Workflow Overview

Typical workflow for publishing mobile app content:



Typical workflow for handling booking requests:



1.22.3. Content Publishing Guidelines

- Ensure all uploaded content is accurate and verified before publishing.
- Avoid uploading duplicate or outdated information.
- Use clear, concise text for notifications and announcements.
- Upload good-quality images that represent the company professionally.
- Regularly review expiry dates for notifications and remove outdated content.
- Ensure project-specific content is uploaded under the correct project selection.

Image Size Standards

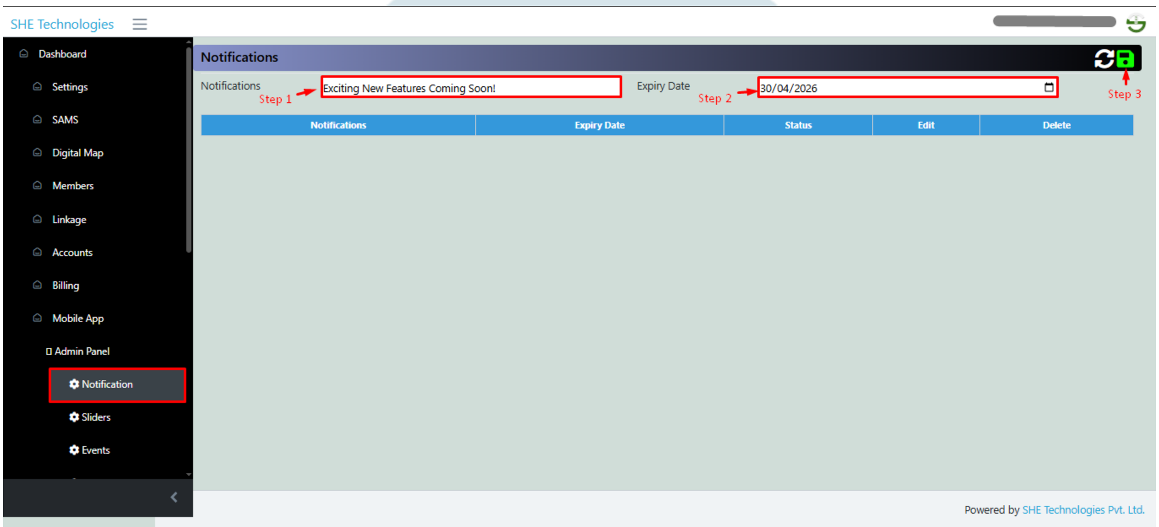
Module	Recommended Resolution	Maximum File Size
Sliders (Dashboard Banners)	1080 × 540 px	500 KB
Events Images	800 × 800 px	500 KB
Development Progress Images	800 × 800 px	500 KB
Payment Plan Images	800 × 800 px	500 KB

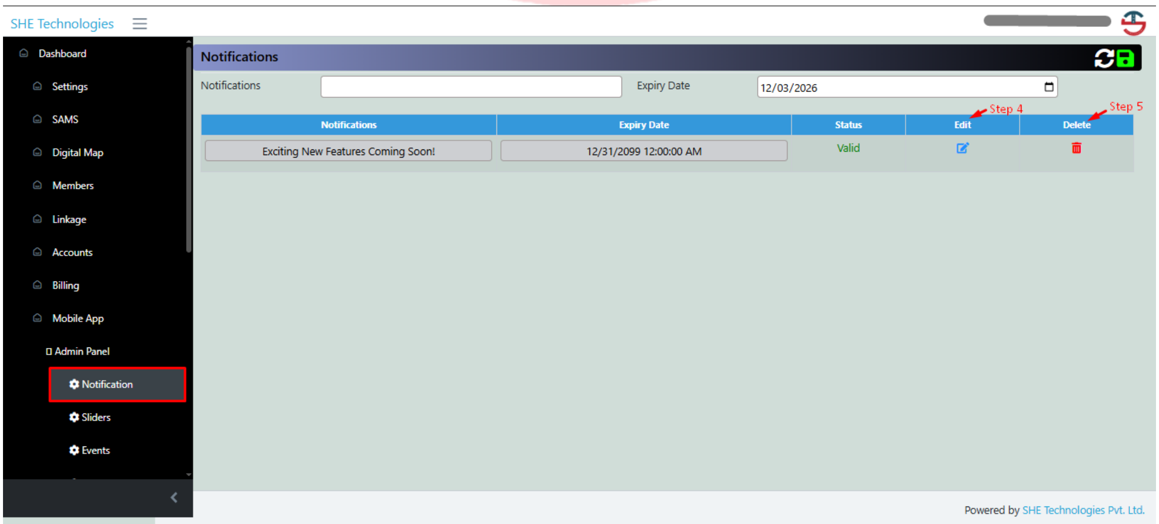
Social Media Logos	512 × 512 px	100 KB

1.22.4. Notifications

Used to publish announcements or important updates for mobile app users. Input fields include Notification Text and Expiry Date.

1. Enter the notification text.
2. Select the expiry date.
3. Click Save to publish.
4. Use Edit to modify existing notifications.
5. Use Delete to remove notifications.

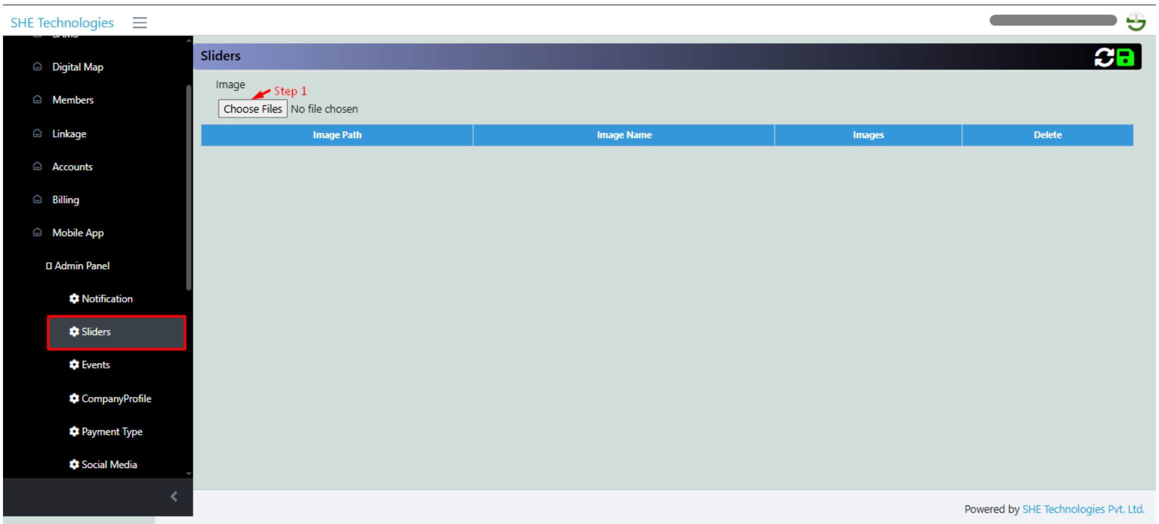


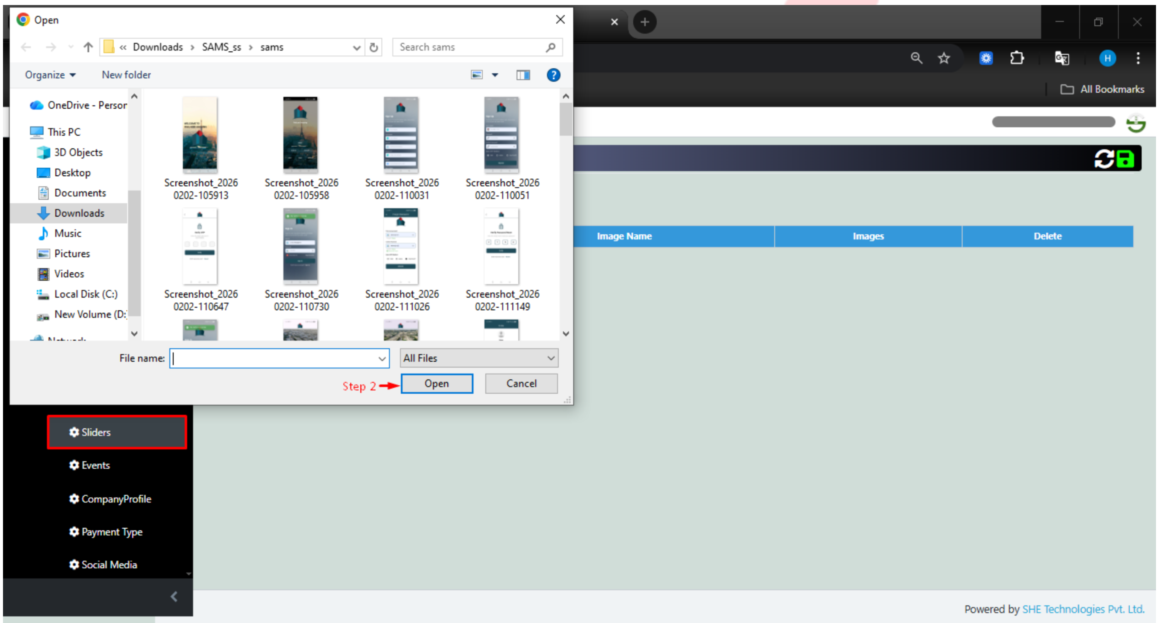


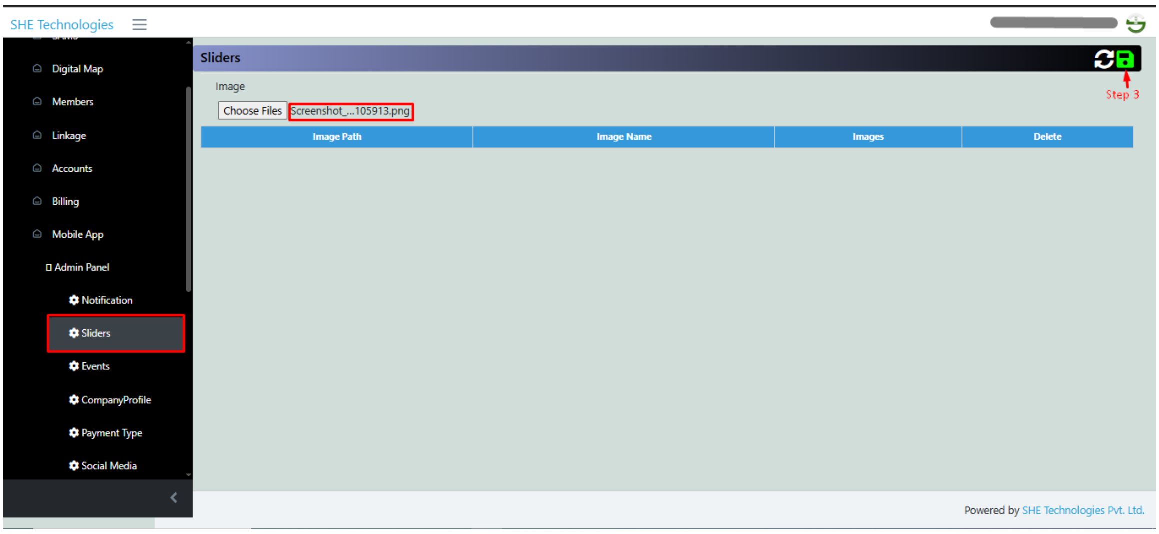
1.22.5. Sliders

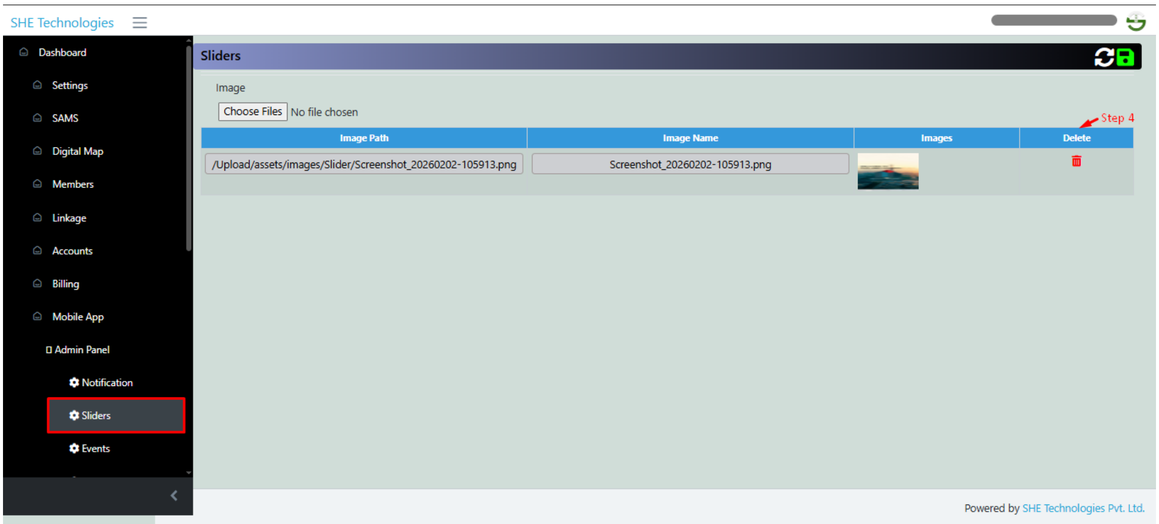
Used to upload dashboard banner images displayed in the mobile application.

1. Click Choose File to upload the slider image.
2. Select banner image from computer.
3. Save to publish the slider on the mobile dashboard.
4. Delete unwanted sliders if required.





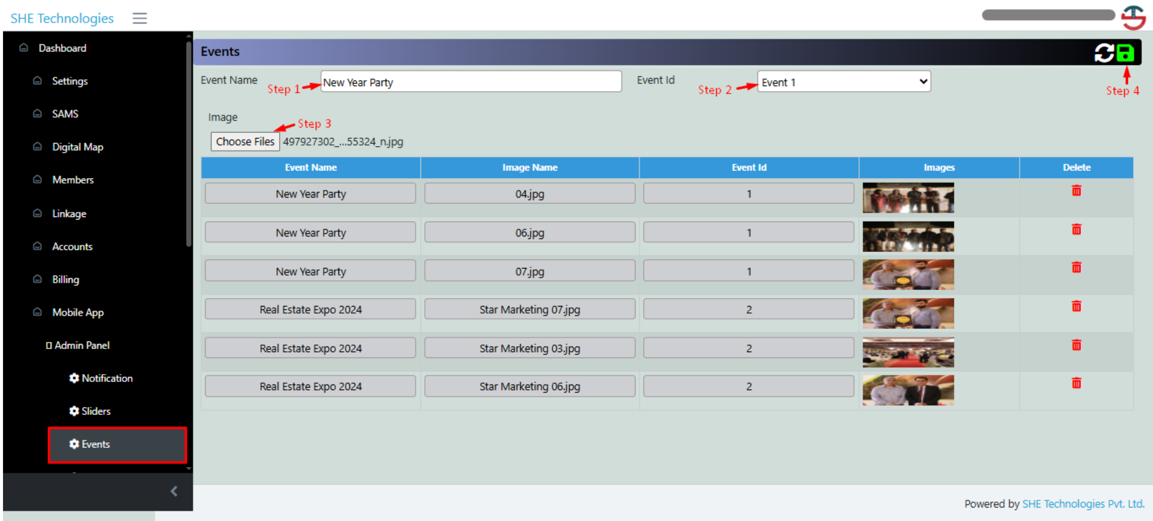




1.22.6. Events

Allows users to upload images related to company events. Input fields include Event Name, Event ID, and Image Upload.

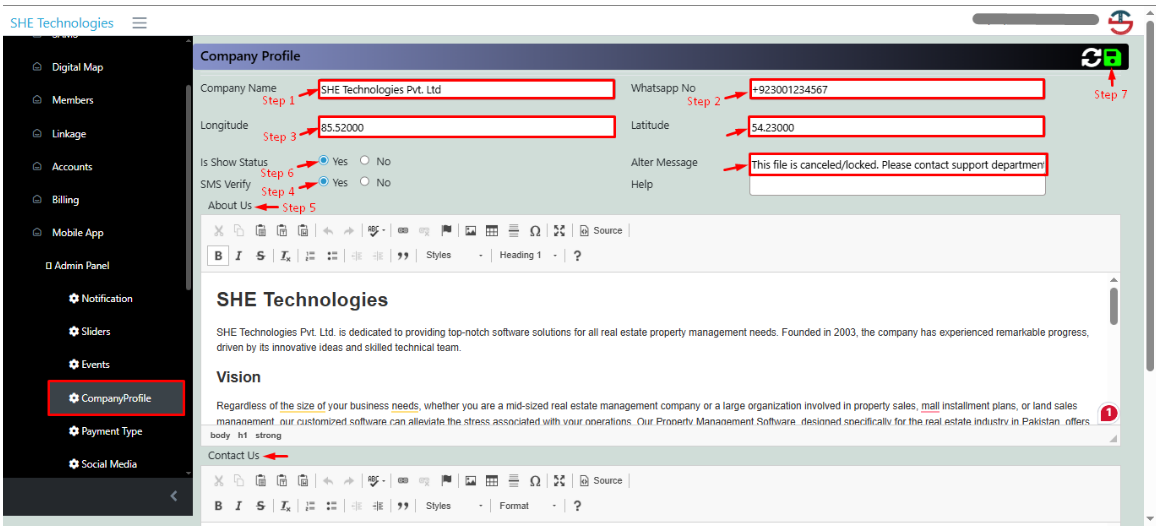
1. Enter Event Name.
2. Select Event ID from the dropdown.
3. Upload event image.
4. Click Save to publish event content.



1.22.7. Company Profile

Stores company information shown in the mobile application, such as name, WhatsApp number, coordinates, SMS verification option, warning messages, helpline number, About Us, and Contact Us details.

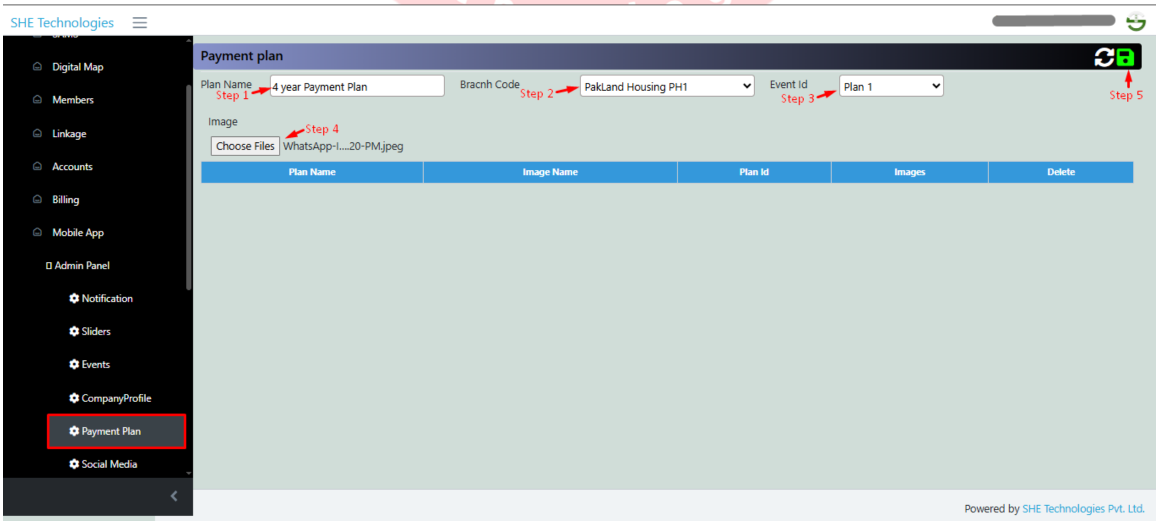
1. Update company name and contact details.
2. Enter WhatsApp number.
3. Provide latitude and longitude coordinates.
4. Enable or disable SMS verification.
5. Update About Us and Contact Us sections
6. Enable or Disable file status dialogue
7. Save to apply the updated company profile.

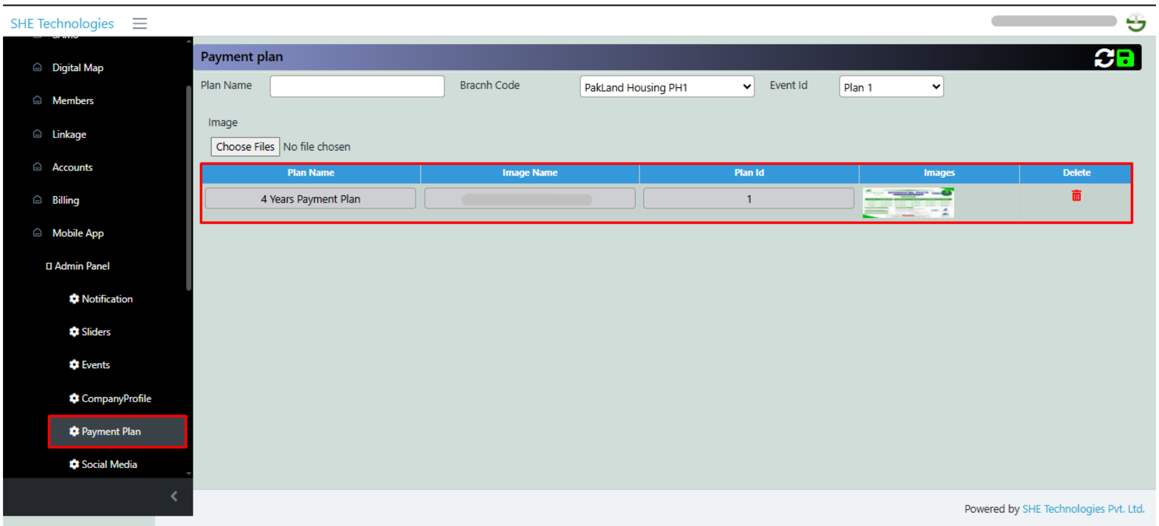


1.22.8. Payment Plans

Used to upload payment plan images for different projects. Fields include Payment Plan Name, Project Selection, and Payment Plan ID.

1. Enter payment plan name.
2. Select project.
3. Enter payment plan ID.
4. Upload payment plan image.
5. Save the record.





1.22.9. Social Links

Allows users to manage social media links visible in the mobile app, including platform, URL, and logo.

1. Select project.
2. Select social platform.
3. Enter URL.
4. Upload logo.
5. Save the record.

1.22.10. Development Progress

Used to upload images that show project construction or development progress.

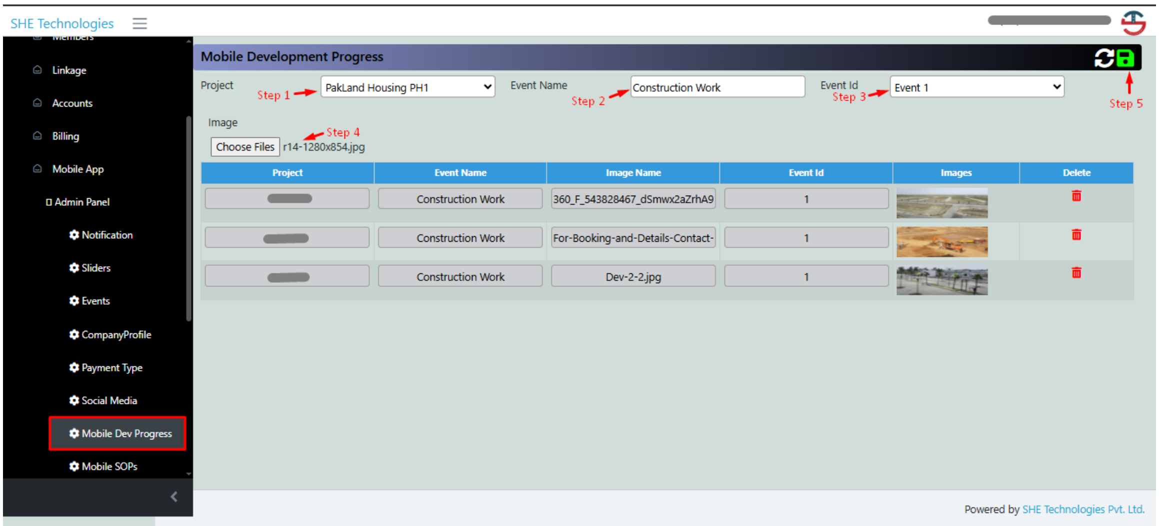
Select Project/Branch

Enter development Event Name.

Select Event ID.

Upload image.

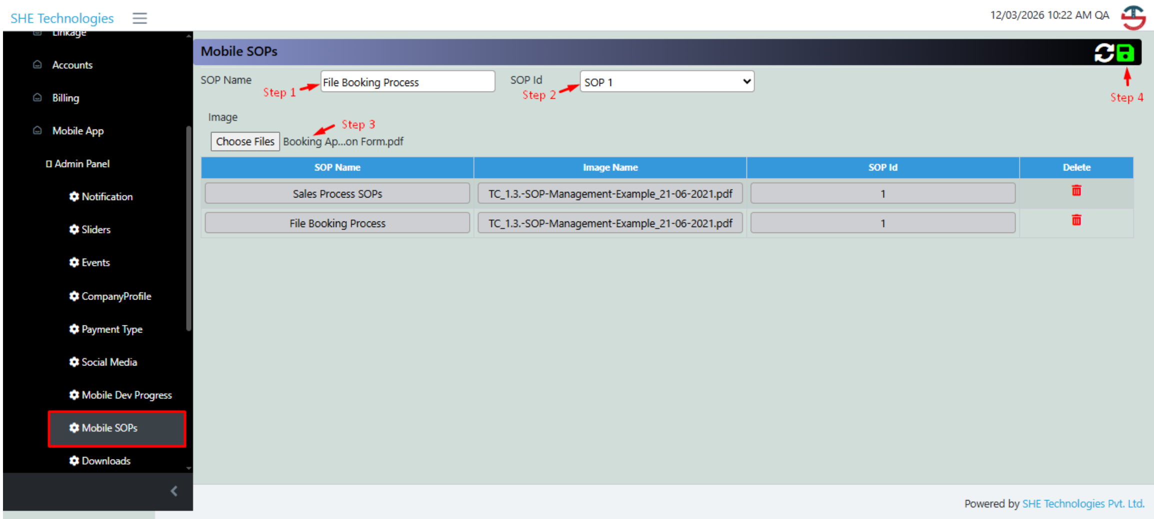
Save to publish update.



1.22.11. SOPs

Used to upload Standard Operating Procedure documents for reference.

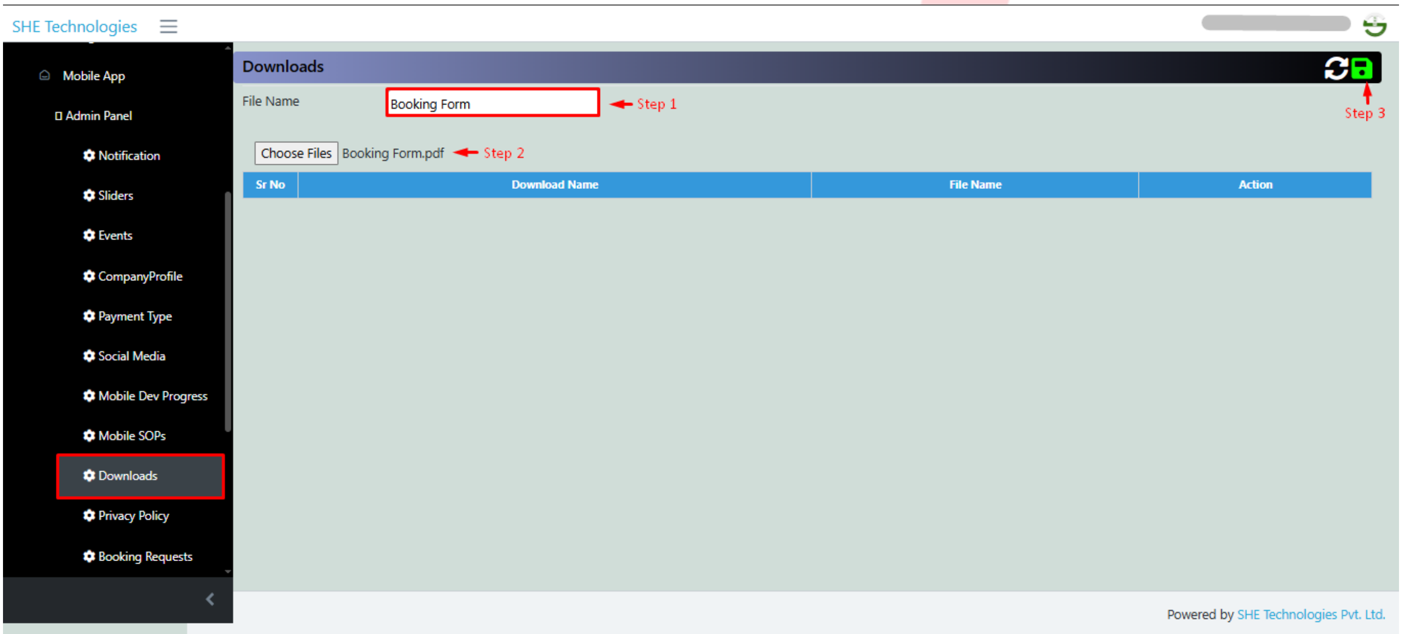
1. Enter SOP name.
2. Enter SOP ID.
3. Upload document.
4. Save to publish.

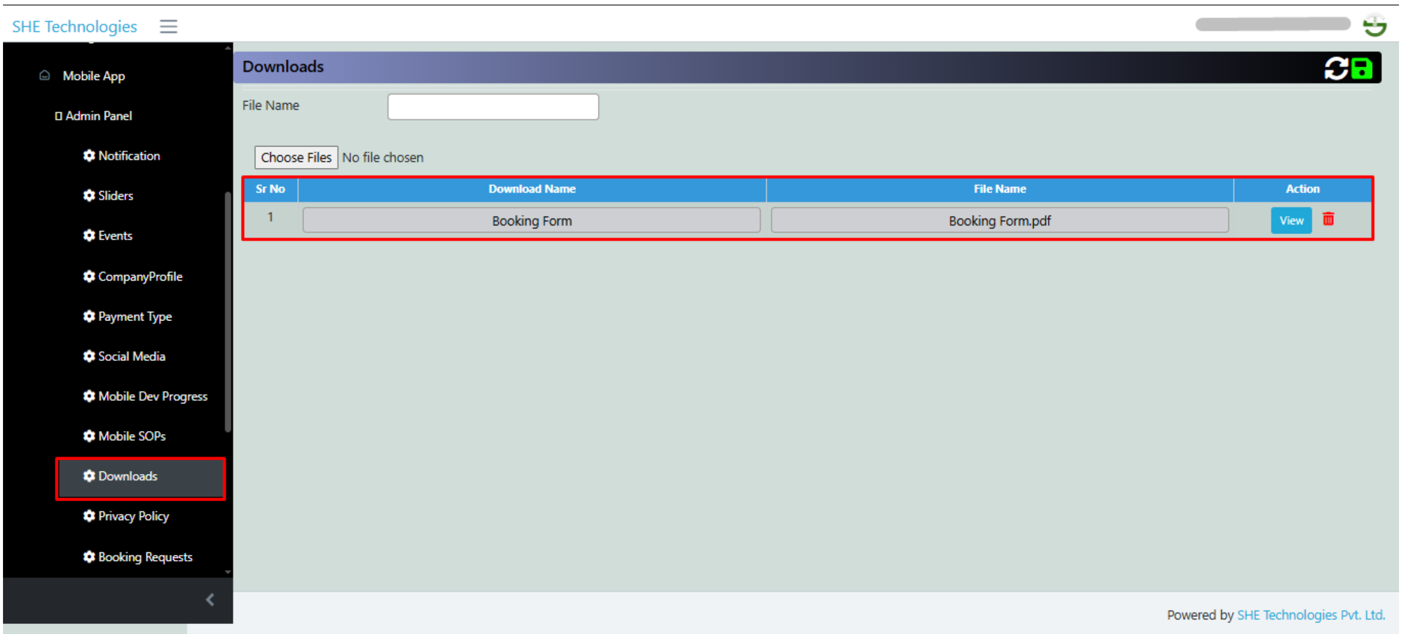


1.22.12. Downloads

Allows users to upload downloadable resources such as brochures or documents.

1. Enter file name.
2. Upload file.
3. Save to publish download.

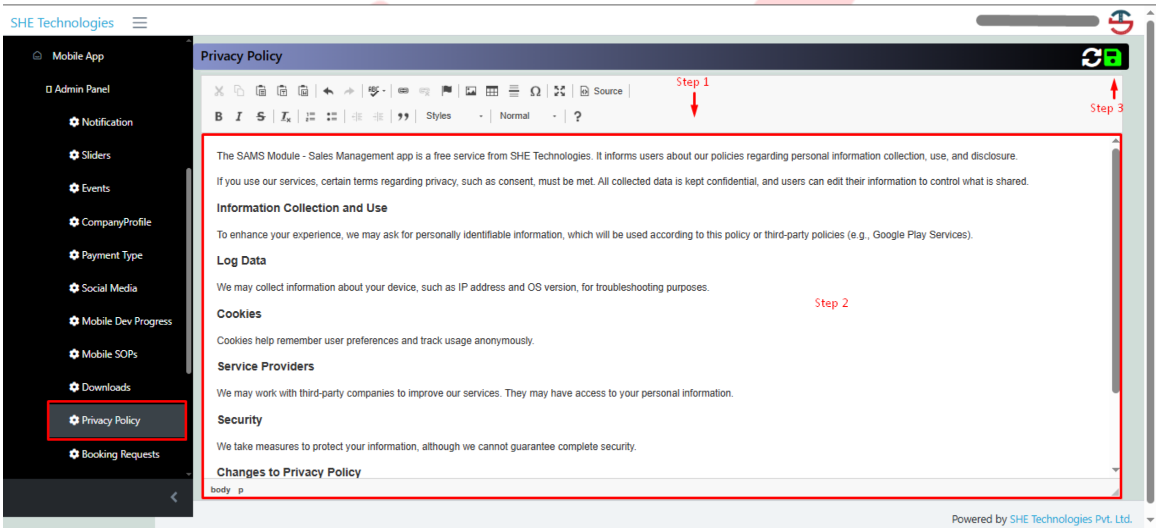




1.22.13. Privacy Policy

Used to maintain the privacy policy text displayed within the mobile application.

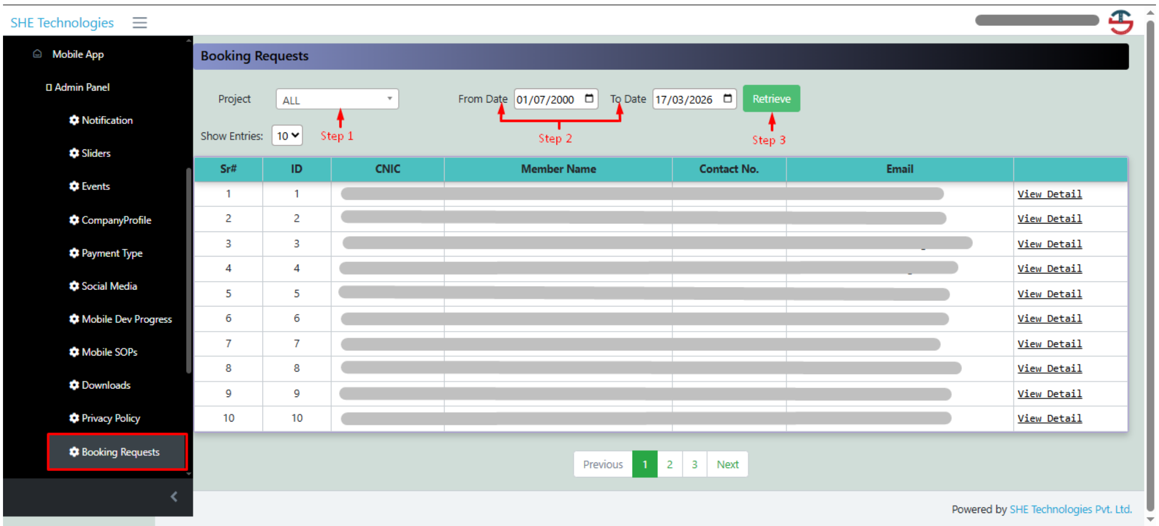
1. Enter or update privacy policy text.
2. Review the content.
3. Save changes.



1.22.14. Online Booking Requests

Displays booking requests submitted through the mobile application with filtering options by project and date range.

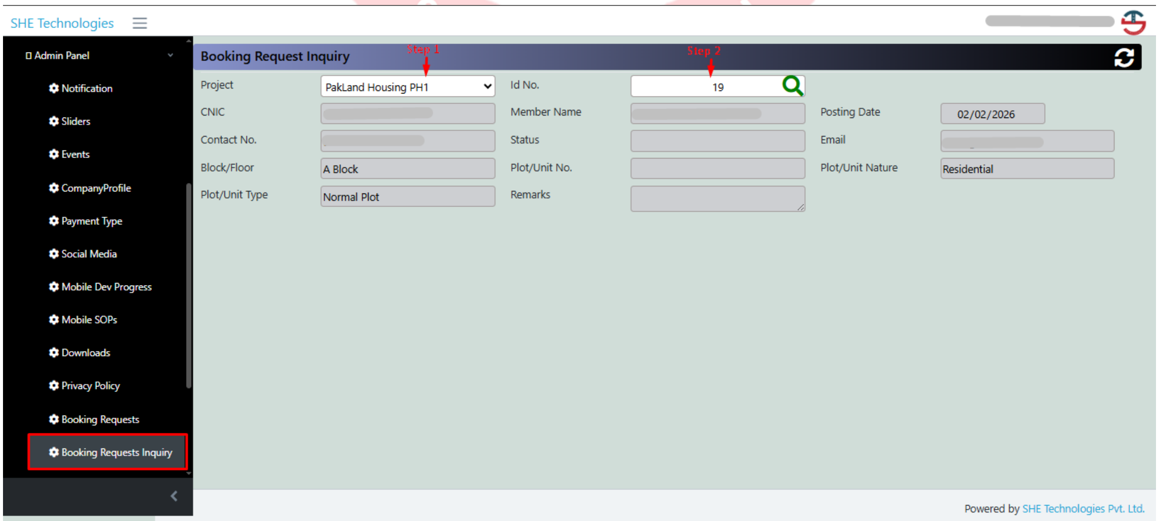
1. Select project.
2. Choose From and To date filters.
3. Click Retrieve to view booking records.



1.22.15. Booking Requests Inquiry

Provides detailed information about individual booking requests using project and booking ID filters.

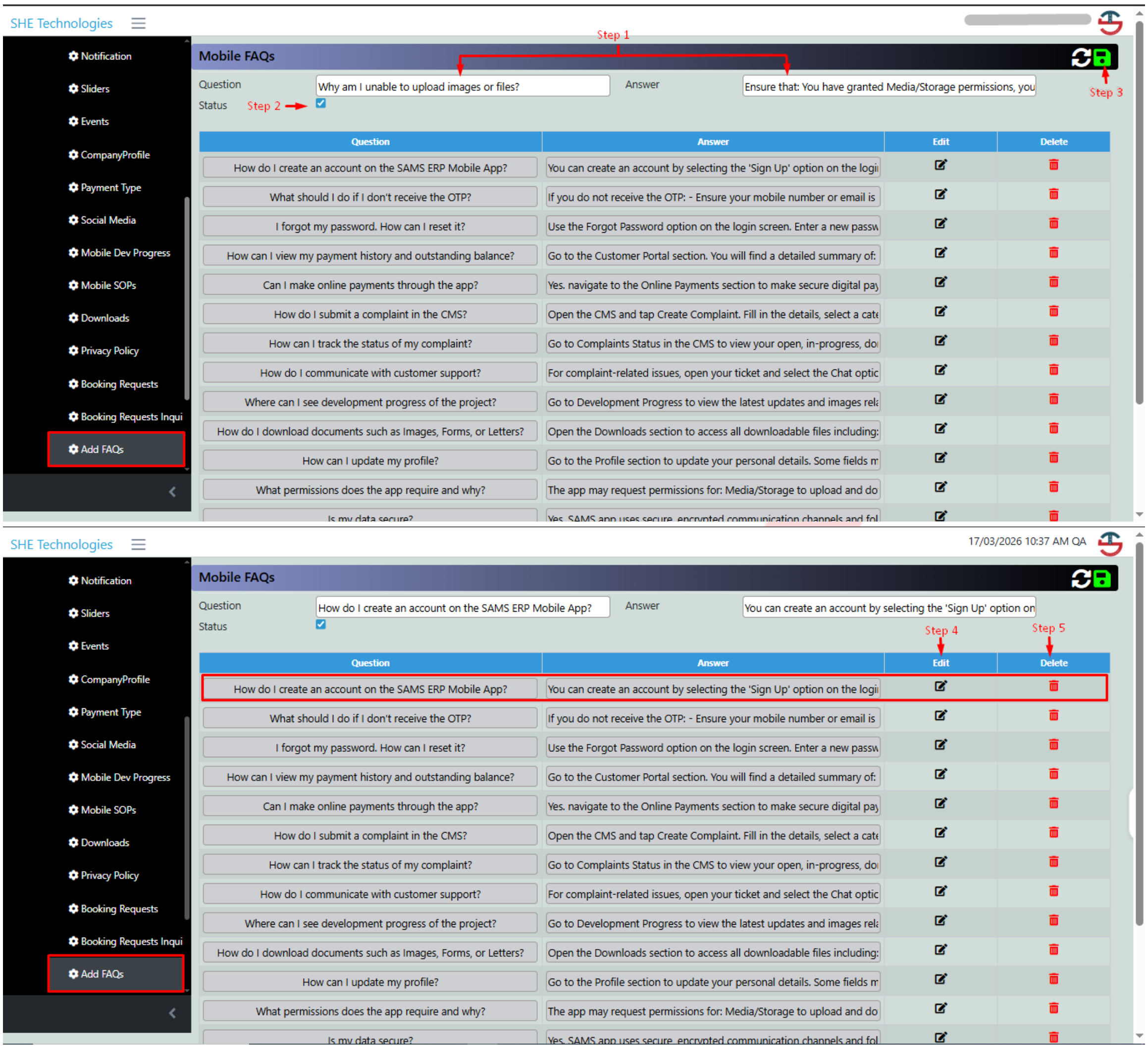
1. Select project.
2. Enter/Search booking ID number.



1.22.16. FAQs

Used to manage Frequently Asked Questions displayed in the mobile app.

1. Enter the FAQ question and answer.
2. Enable or disable status.
3. Save to publish.
4. Use Edit to modify existing FAQs.
5. Use Delete to remove unwanted FAQs.



1.22.17. Complaint Management System (CMS) Workflow

Department → Category → Role management Flow:

Step 1: Create Department

Step 2: Assign Department to Branch

Step 3: Create Categories under Department

Step 4: Assign Departments/Roles to Users

Step 5: CMS uses this mapping for complaint routing

1.22.18. Add Departments

Manage departments used in CMS.

1. Go to SAMS
2. Go to Parameters
3. Click Add Department
4. Enter Department ID
5. Enter Department Name
6. Click the Add button to save the records

Do's

- Use unique Department IDs
- No space and special characters in ID
- Keep naming consistent
- Review before deletion

Don'ts

- Do not duplicate Names
- Do not delete active departments

1.22.19. 2. Add Categories

Define categories under departments.

1. Go to SAMS
2. Go to Parameters
3. Click Add Categories

4. Select Branch
5. Select Department
6. Add categories
7. Click save to add/update records

Do's

- Use meaningful category names
- Map the correct department

Don'ts

- Avoid confused names
- Avoid wrong mapping

1.22.20. 3. Assign Department to Branch

Map departments to projects.

1. Go to SAMS
2. Go to Parameters
3. Click Assign Department to Branch
4. Select Branch
5. Select Department/s
6. Click the Assign button to save the records

Do's

- Verify mapping
- Review regularly

Don'ts

- Avoid wrong assignment
- Avoid removing active department/s

1.22.21. Assign Roles

Assign roles and departments to users.

1. Select Project
2. Select user id (Admin or Staff)
3. Select Department/s

4. Save to add/update records.

Do's

- Assign based on responsibility
- Limit admin rights

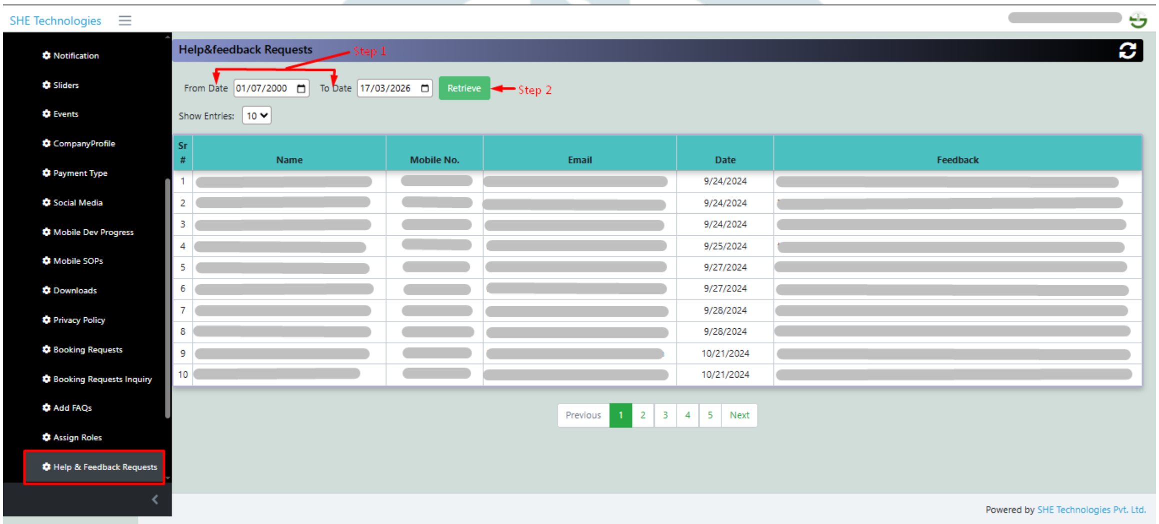
Don'ts

- Avoid excessive admin rights
- Avoid missing role mapping

1.22.22. Help & Feedback Requests

Displays queries and feedback submitted by mobile app users.

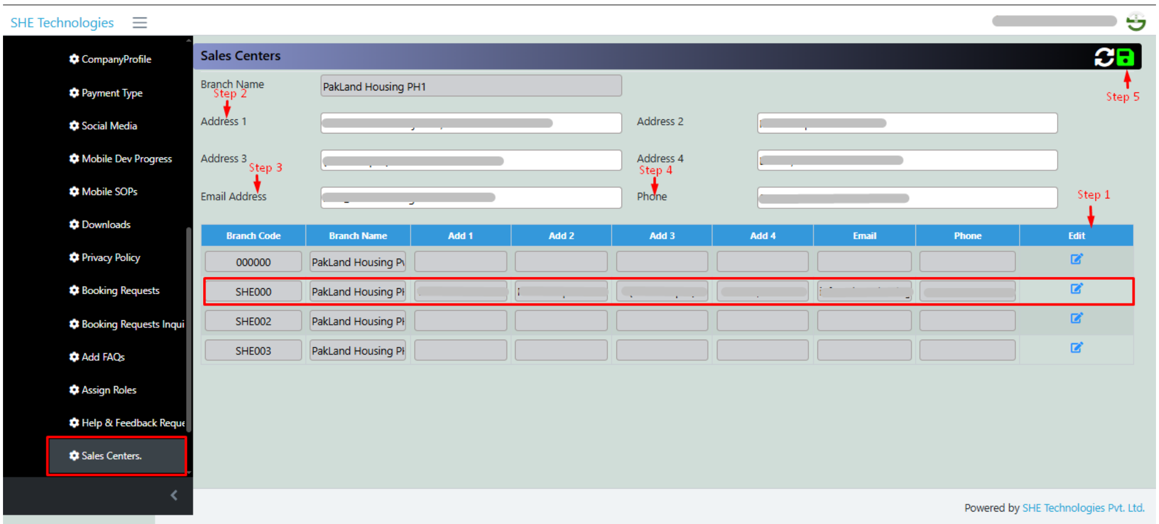
1. Select From and To dates.
2. Click Retrieve to view feedback.



1.22.23. Sales Centers

Used to manage addresses, email addresses, and contact numbers of company sales offices.

1. Click Edit
2. Enter office address.
3. Enter official email.
4. Enter contact number.
5. Save to update records.



1.22.24. Security

Access to the admin panel should be limited to authorized staff. Users must verify all content before publishing and follow internal change management procedures.

1.22.25. Troubleshooting

Common Issues and Solutions:

- Image not uploading – verify file size and format.
- Notification not appearing – check expiry date.
- Missing data – verify filter settings.

1.22.26. Support

For technical support, contact the support team.

1.23. SAMS ERP Mobile App User Guide

Before You Begin

Before using the SAMS ERP Mobile App, please ensure:
• You have an active internet connection
• Your registered mobile number or email is accessible for OTP verification
• Your device runs Android or iOS with the latest updates
• Notifications are enabled for timely alerts

Do's:
• Keep your login credentials secure
• Ensure correct personal information

Don'ts:
• Do not share OTPs or passwords
• Do not use public devices for login

1.23.1. Quick Start Guide

New to the SAMS ERP Mobile App? Follow these three simple steps to get started:

1. Download the SAMS ERP Mobile App from the Google Play Store or Apple App Store.

2. Sign up using your registered mobile number or email and verify via OTP.

3. Log in and access your dashboard to view payments, bookings, and updates.

1.23.2. Introduction

The SAMS (Sales Management System) ERP Mobile Application is designed to offer a seamless digital experience for managing bookings, processing payments, handling customer service interactions, tracking progress, and accessing official documentation. This comprehensive user guide includes detailed explanations, step-by-step instructions, helpful tips, and examples to help users maximize the benefits of all the app's features.

1.23.3. Getting Started

1.23.4. Installing the Application

The SAMS ERP Mobile App is available for both Android and iOS platforms.

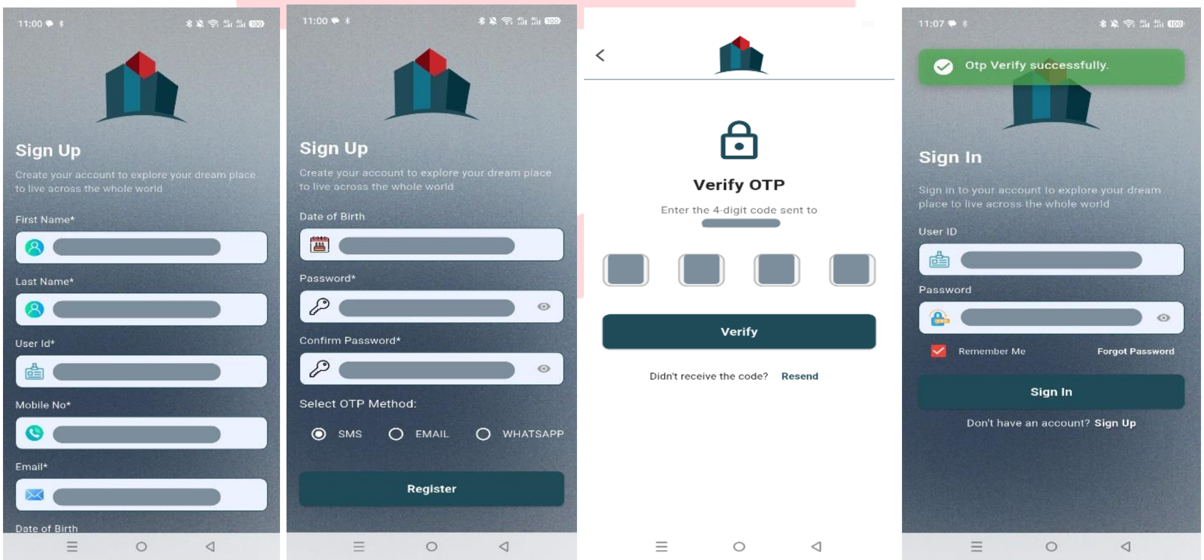
- Visit the Google Play Store on Android or the Apple App Store on iOS devices.
- Search for "SAMS ERP Mobile App".
- Tap **Install** and wait for the app to finish downloading.

- Allow required permissions when prompted (Notifications, Location Services, and Media/Files Access).

1.23.5. Creating an Account (Signup)

To ensure secure access, users must create an account. Here are the steps to register:

1. Open the SAMS Mobile App.
2. Tap the **"Signup"** option on the welcome screen.
3. Provide the necessary details: Full Name, User ID, Mobile Number, Email Address, and Date of Birth.
4. Choose your preferred method for receiving an **OTP** (One-Time Password):
   a. SMS
   b. Email
   c. WhatsApp
5. Enter the OTP you receive.
6. Create a password that meets the app's security requirements.
7. Tap **"Register"** to complete your registration.



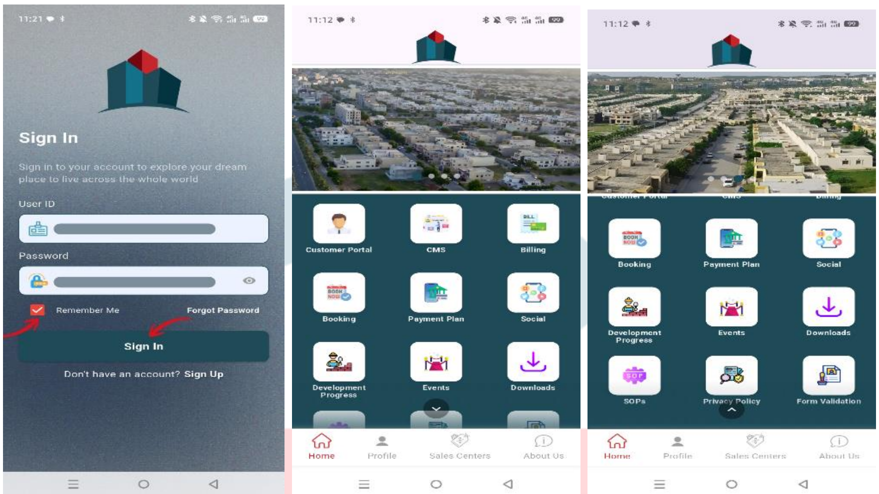
Tips:

- Please ensure your mobile number and email address are registered and active in our data center.
- If you don't receive the OTP, use the **Resend OTP** option or contact customer service.

1.23.6. First-Time Login Instructions

Once registered:

1. Open the app.
2. Enter your registered User ID and password.
3. Tap **Sign In**.
4. If prompted, please allow the necessary permissions for Notifications, Location Services, and Media/Files Access.



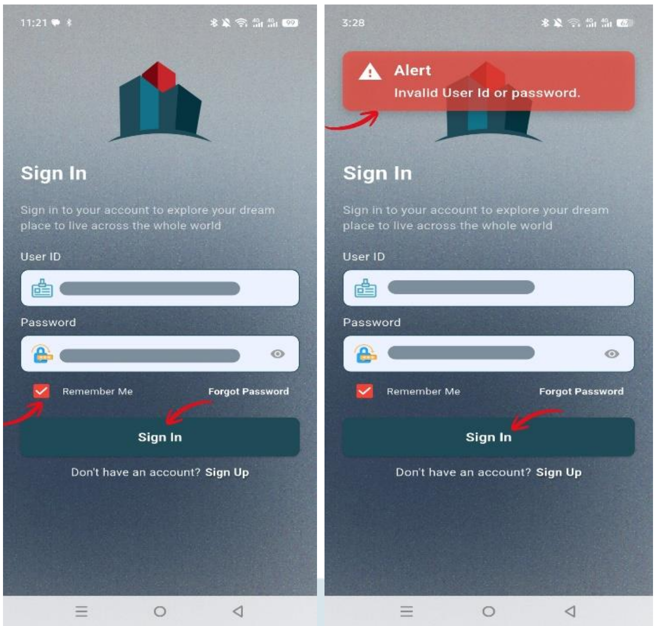
1.23.7. Login & Security Features

1.23.8. Standard Login

Users can log in using their registered credentials.

- Enter **User ID**.
- Enter **Password**.
- Tap **Sign In**.

If credentials are incorrect, the app will display an error message.



Do's:

- ✓ Use a strong password
- ✓ Log out after use

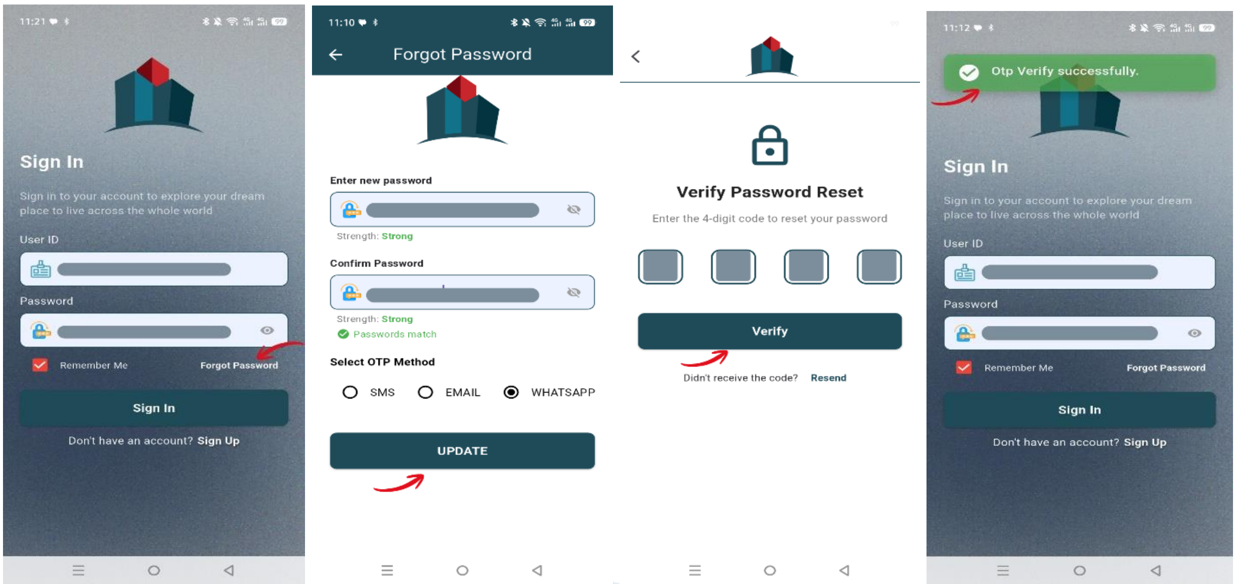
Don'ts:

- Avoid saving passwords on shared devices

1.23.9. Forgot Password

If you forget your password, follow these steps:

1. Tap **"Forgot Password?"**
2. Set and confirm your new password.
3. Choose your preferred **OTP** delivery method.
4. Enter the received OTP and tap **Verify**.



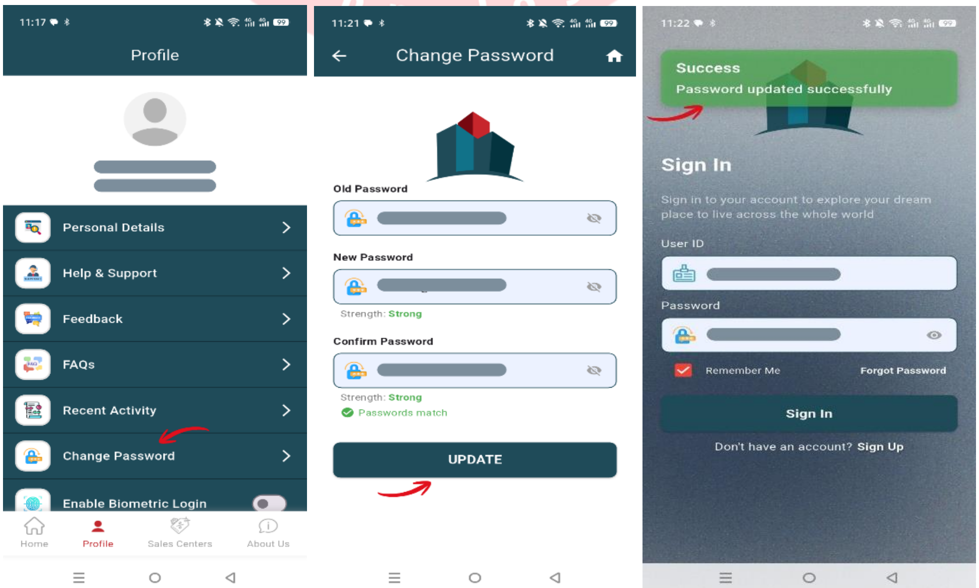
Tips:

- If you don't receive the OTP, use the **Resend OTP** option or contact customer service.

1.23.10. Change Password

To change your password in the app:

- Go to **Profile → Change Password**.
- Enter your current password.
- Enter and confirm your new password.



Security Recommendations

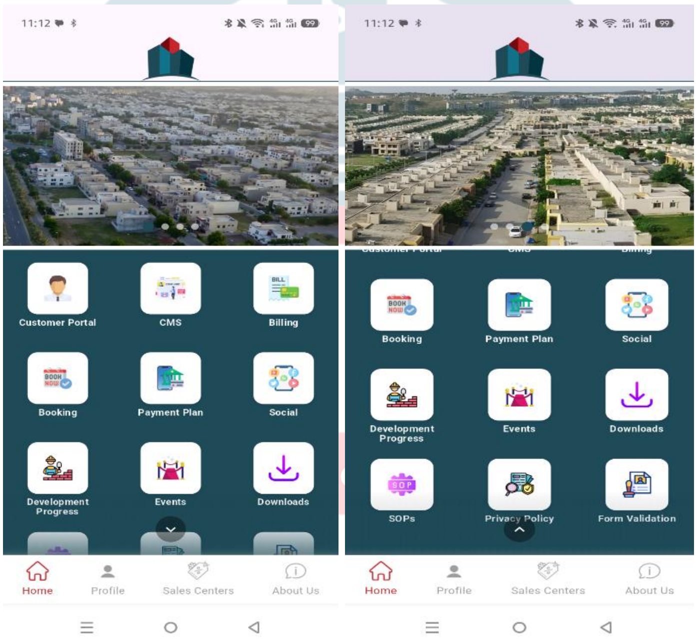
- Create strong passwords using a combination of letters, numbers, and symbols.
- Avoid sharing your passwords with others.
- Update your password every 90 days.
- Log out from public or shared devices after use.

1.23.11. Dashboard

The dashboard serves as the home screen and central hub of the app.

Key Components

- **Sliders:** Display the latest project or company updates.
- **Notifications:** Shows recent alerts.
- **Menu Buttons:** Fast access to all modules.
- **Summary Cards:** Quick stats for Payments, Bookings, and Complaints.



1.23.12. Customer Portal

The Customer Portal provides detailed information related to the user's personal information and booking summary.

Personal Information

Includes:

- Name

- CNIC
- Address

File/Unit Information

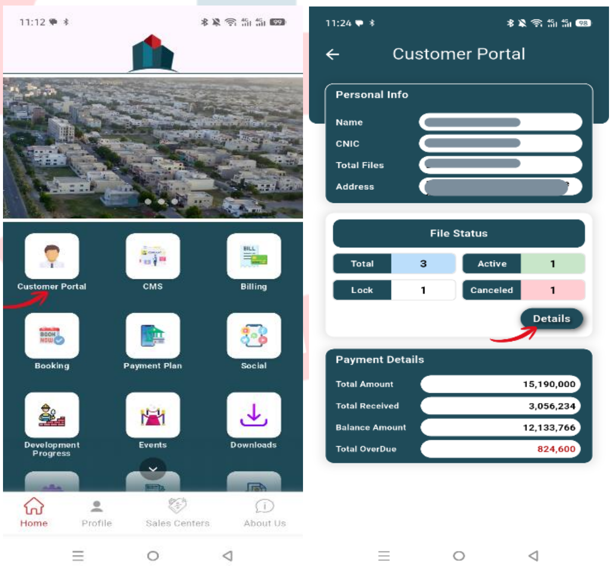
Displays:

- Total files
- Status

Financial Summary

Shows a complete breakdown:

- **Total Price** – Sum of all unit/s prices.
- **Total Received** – Sum of all verified payments.
- **Total Outstanding** – Sum of all remaining amounts.
- **Total Overdue** – Sum of all remaining amounts past their due date.



Tips:

- Users should verify their details and contact customer support if information appears incorrect.

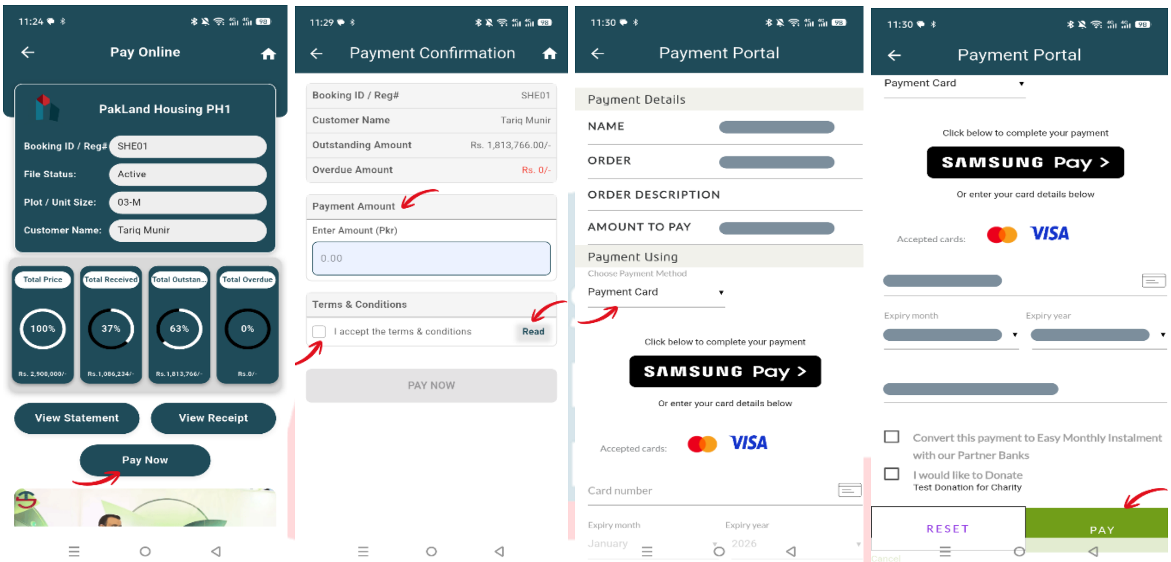
1.23.13. Online Payments

The Online Payments section allows you to manage all financial activities.

If you pay via bank transfer:

- Choose a file for which you want to make a payment
- Enter transaction amount
- Click the ‘Pay Now’ button
- Enter your debit/credit card details, i.e., card number, CVC, and proceed
- Enter the OTP received on your registered mobile number and submit
- You will get the digital receipt with the transaction’s details in case of a successful transaction.
- Take a screenshot and send it to the accounts department.

The finance team verifies this payment and updates your account.



Do’s:

- ✓ Confirm payment details before submitting
- ✓ Save digital receipts

Don’ts:

- Do not close the app during payment processing

1.23.14. CMS (Complaint Management System)

A full-featured module to submit and track customer complaints.

Overview

The Complaints Management System (CMS) in the SAMS ERP Mobile App allows users to report issues, track progress, and communicate with the resolution team. It ensures complaints are addressed efficiently and on time, providing users with status updates, issue details, and resolution timelines to keep them informed throughout the process.

- Client
- Staff
- Admin

Purpose

- Submit service-related issues directly through the app
- Track complaint progress in real time
- View complaint history and action logs
- Communicate with the concerned support team
- Improve accountability and complaint resolution efficiency

CMS Roles and Access Levels

The CMS is role-based. Access to complaint actions and screens depends on the logged-in user's type and role.

CMS for Client

Role of the Client

The Client is the end user who raises a complaint or service request using the mobile application.

- Submit complaints
- Track complaint progress
- Review complaint details
- Stay updated through chat and timeline history

Client Permissions

The Client can:

- Create a complaint ticket
- View ticket details
- View ticket timeline
- Communicate with Admin and Staff through in-app chat
- View complaint status overview from the dashboard

CMS Dashboard (Client)

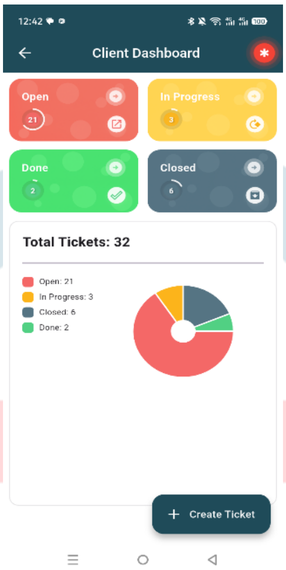
The **CMS Dashboard** provides the Client with a quick overview of all complaint tickets submitted through the app.

It displays:

- Open ticket count
- In Progress ticket count

- Done ticket count
- Closed ticket count
- Donut Chart showing complaint distribution by status

1. Open the CMS module.
2. The Dashboard will open by default or can be accessed from the menu.
3. Review the ticket status cards.
4. Use the chart for a quick visual understanding of complaint progress.



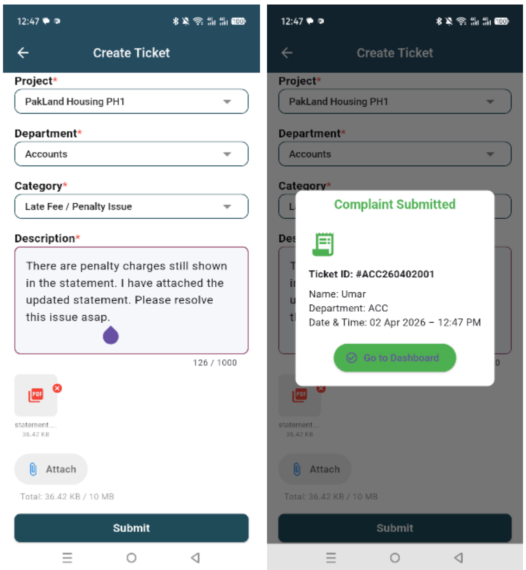
Create Ticket

The **Create Ticket** screen allows the Client to submit a complaint directly from the mobile application.

This is the starting point of the complaint lifecycle.

1. Open the CMS module.
2. Tap Create Ticket.
3. Select the Project.
4. Select the Department.
5. Select the Category.
6. Enter a clear and complete Description.
7. Upload supporting Attachments, if available.
8. Tap Submit.

Good Example: “Water leakage observed in the washroom area of Block C since last evening.”
Poor Example: “Problem here.”



Do’s

- ✓ Provide clear and accurate complaint information
- ✓ Attach evidence where possible
- ✓ Select the correct project, department, and category

Don’ts

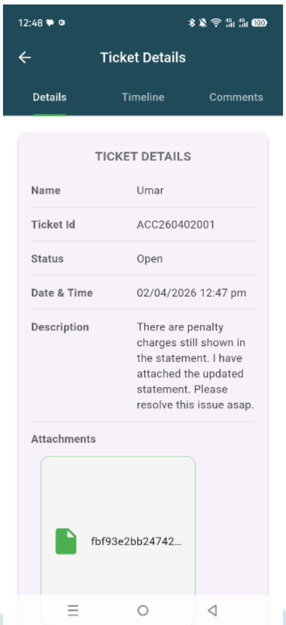
- Do not submit duplicate complaints for the same issue
- Do not leave the description vague or incomplete

Ticket Details (Client)

The **Ticket Details** screen provides complete information about a complaint submitted by the Client.

This screen displays:

- User Name
- Ticket ID
- Status
- Date & Time
- Description
- Attachments



Do's

- ✓ Always note the **Ticket ID** for reference
- ✓ Review details before following up on a complaint

Don'ts

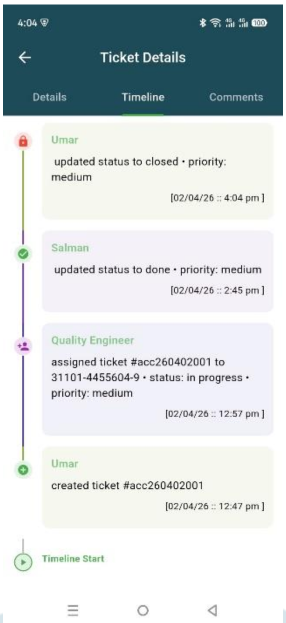
- Do not assume complaint progress without checking the latest status

Timeline (Client)

The **Timeline** screen shows the full complaint history and the actions taken on the ticket.

Typical timeline entries may include:

- Ticket created
- Ticket assigned
- Status changed
- Complaint resolved
- Complaint closed



Do's

- ✓ Check the timeline before requesting an update
- ✓ Use the timeline to understand the complaint stage

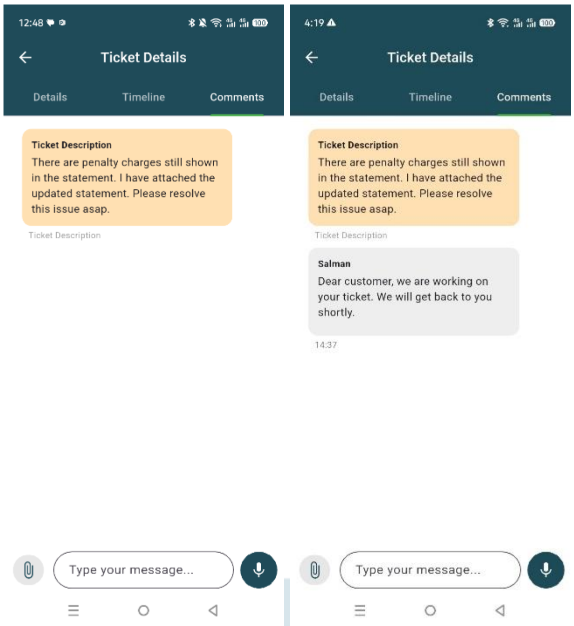
Don'ts

- Do not assume the complaint is delayed without checking recent actions

Comments / Chat (Client)

The **Comments** screen allows the Client to communicate directly with Admin and Staff through an in-app chat feature.

1. Open the ticket.
2. Tap Comments.
3. Enter your message in the chat field.
4. Tap Send.



Communication Best Practice

Messages should be:

- Clear
- Relevant
- Professional
- Complaint-specific

Good Example: “Please confirm whether the maintenance team has visited the site.”

Poor Example: “Any update???”

Do’s

- ✓ Keep messages relevant to the complaint
- ✓ Review previous messages before sending a new one

Don’ts

- Do not send repeated messages unnecessarily
- Do not use unclear or informal complaint communication

CMS for Staff

Role of Staff

The **Staff** user is responsible for handling and resolving complaints assigned by the Admin.

The Staff uses CMS to:

- Review complaint details
- Communicate with the Client and Admin
- Update progress
- Mark complaints as completed once resolved

Staff Permissions

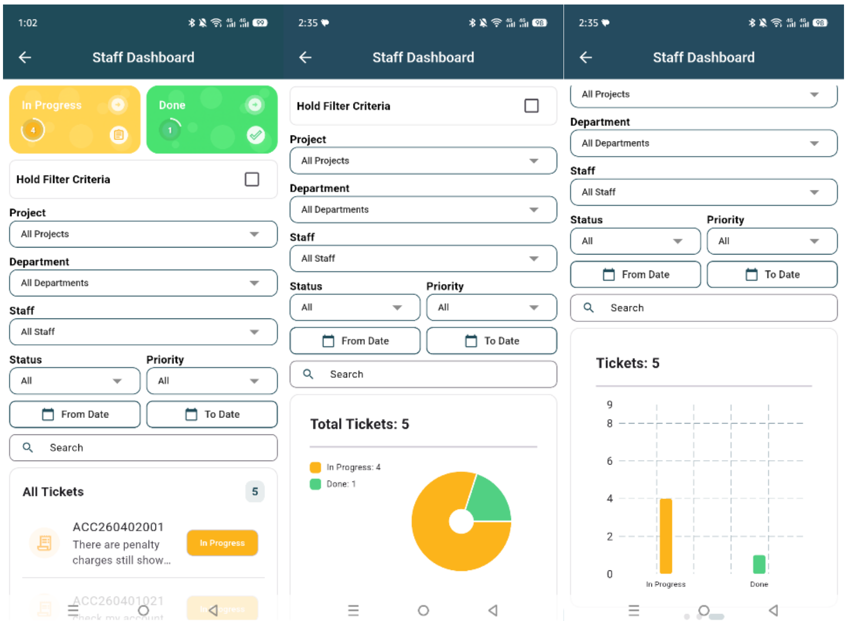
- View assigned complaints
- View ticket details
- View ticket timeline
- Communicate with Client and Admin
- Change ticket status to Done
- View complaints dashboard with filters and analytics

CMS Dashboard (Staff)

The Staff Dashboard provides a working overview of complaints assigned to or relevant to the staff member.

The dashboard displays:

- In Progress ticket count
- Done ticket count
- Project filter
- Department filter
- Ticket Status filter
- Priority filter
- Date-wise filters
- Donut Chart
- Graph for complaint activity analysis



Do’s

- ✓ Use filters to focus on active or urgent complaints
- ✓ Review dashboard data regularly

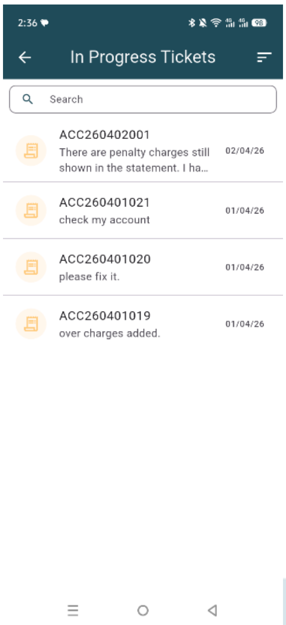
Don’ts

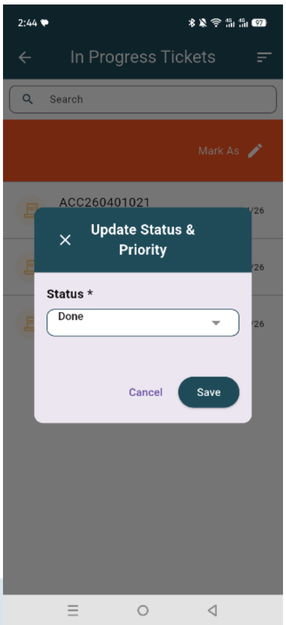
- Do not ignore high-priority complaints

In Progress (Staff)

The **In Progress** screen displays complaints that are currently assigned and being worked on.

1. Open the CMS Dashboard.
2. Tap In Progress.
3. Select the relevant complaint ticket.
4. Review the complaint details and attachments.
5. Take the required operational action.
6. Add comments if needed.
7. Swipe left and mark the ticket as Done once resolved.





Do's

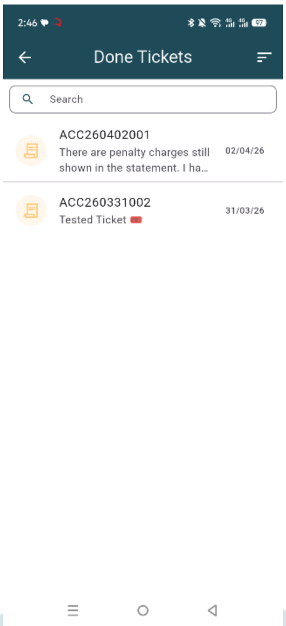
- ✓ Update status only after issue resolution
- ✓ Add meaningful progress notes where necessary

Don'ts

- Do not mark unresolved complaints as **Done**
- Do not skip reviewing attachments or prior updates

Done (Staff)

1. Open the CMS Dashboard.
2. Tap Done.
3. Select the relevant complaint ticket.
4. Review the complaint details and attachments.



CMS for Admin

Role of Admin

The **Admin** is responsible for managing the overall complaint handling process.

The Admin uses CMS to:

- Review complaints
- Assign correctly
- Prioritize appropriately
- Track until completion

Admin Permissions

- View all complaints
- Assign tickets to Staff
- Update ticket priority
- Update ticket status
- View dashboard analytics
- Review complaint timelines
- Communicate with Staff and Clients

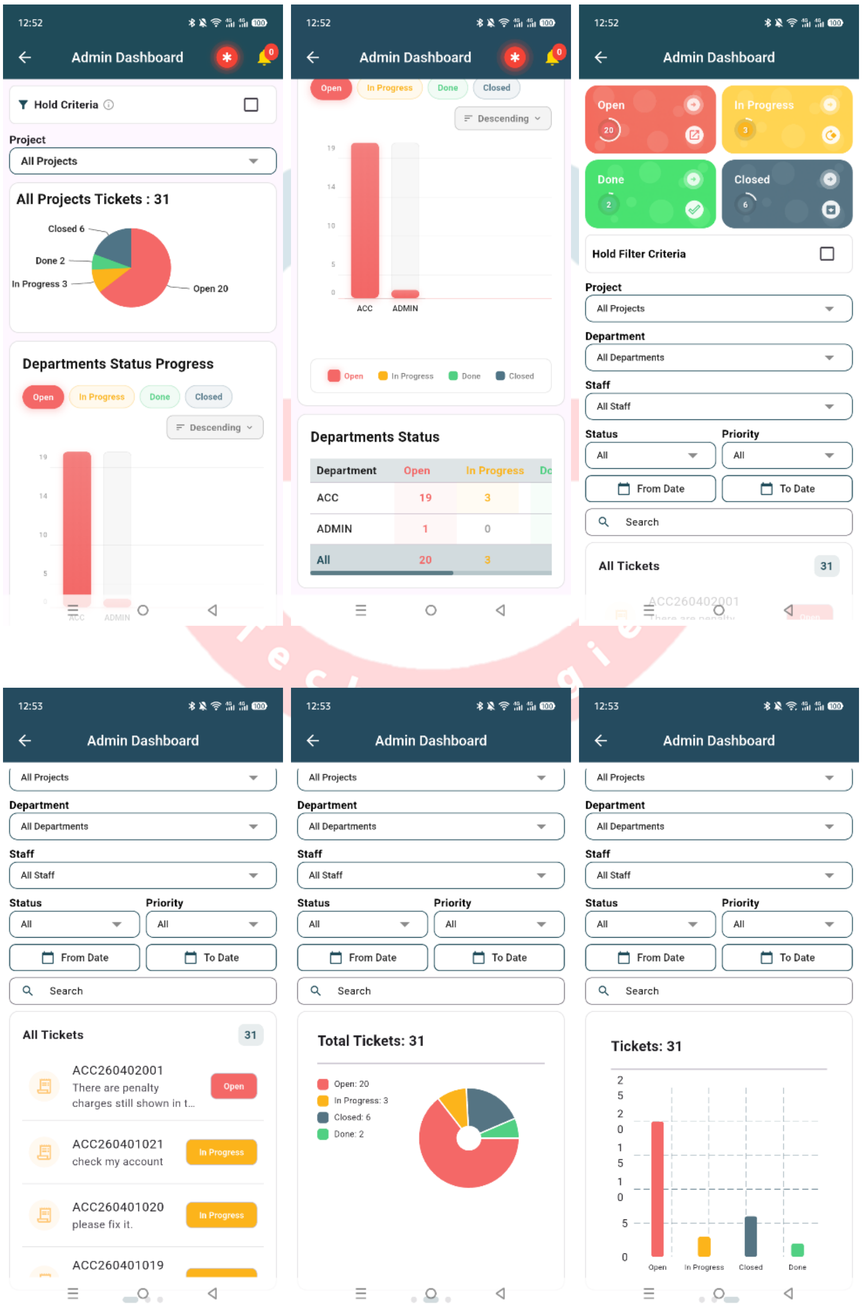
CMS Dashboard (Admin)

The Admin Dashboard provides complete complaint oversight and operational control.

The dashboard displays:

- Open ticket count
- In Progress ticket count
- Done ticket count

- Closed ticket count
- Project filter
- Department filter
- Staff filter
- Ticket Status filter
- Priority filter
- Date-wise filters
- Donut Chart
- Graphs for complaint analysis



Do's

- ✓ Review open complaints regularly
- ✓ Use filters to identify overdue or urgent complaints

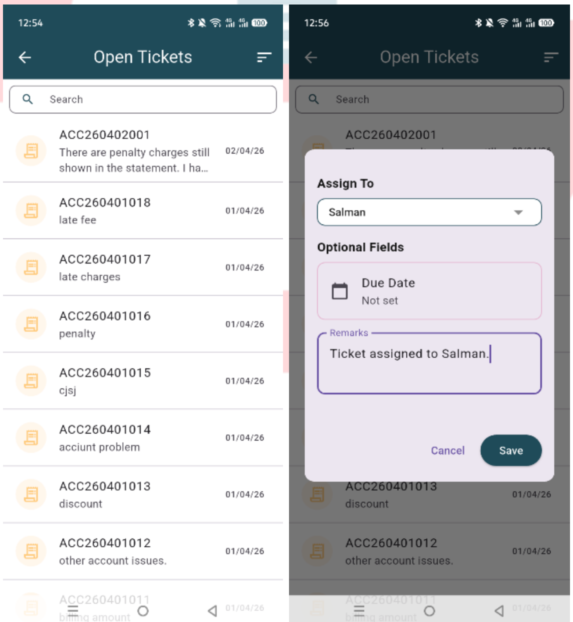
Don'ts

- Do not leave complaints unassigned
- Do not overlook repeated or high-priority complaint categories

Open Tickets (Admin)

The **Open Tickets** screen is used by the Admin to manage newly raised complaints.

1. Open the CMS Dashboard.
2. Tap Open.
3. Review the complaint details.
4. Swipe right to assign the ticket to the appropriate Staff member.
5. Swipe left to set the complaint Priority, if required.
6. Update the Status, if required.
7. Tap Save.



Priority Handling Guidance

Suggested priority usage:

- **High Priority** – urgent complaints requiring immediate action
- **Medium Priority** – standard complaints requiring routine handling
- **Low Priority** – non-critical issues with lower urgency

Do's

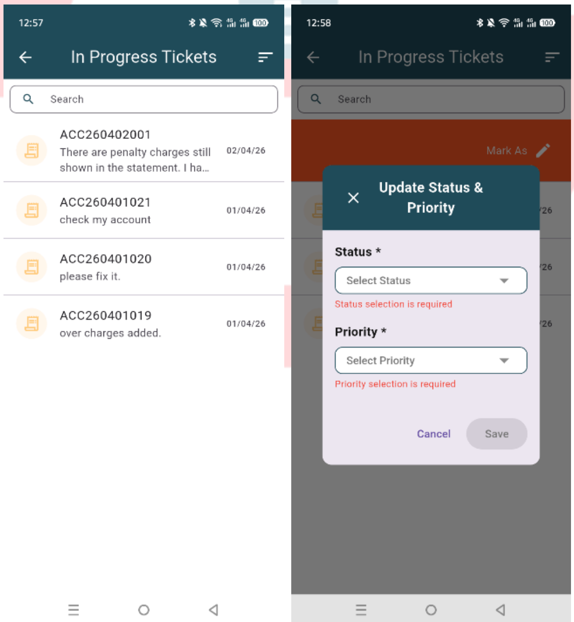
- ✓ Assign tickets promptly
- ✓ Match tickets with the correct department/staff
- ✓ Set priority based on actual urgency

Don'ts

- Do not assign tickets without reviewing complaint details
- Do not leave urgent complaints pending

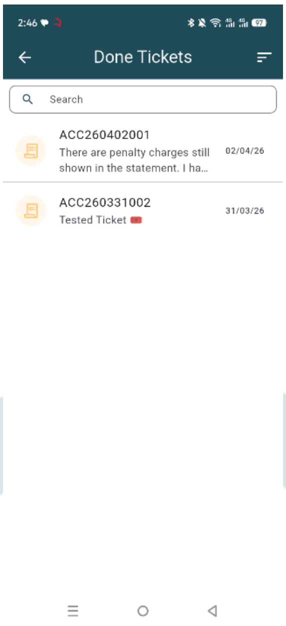
In Progress (Admin)

1. Open the CMS Dashboard.
2. Tap In Progress.
3. Review the complaint details.
4. Reassign the ticket to the new Staff member, if required
5. Set the complaint Priority, if required
6. Update the Status, if required.
7. Tap Save.



Done (Admin)

1. Open the CMS Dashboard.
2. Tap Done.
3. Review the done tickets.



Closed (Admin)

1. Open the CMS Dashboard.
2. Tap Closed.
3. Review the closed tickets.

Complaint Lifecycle

A complaint generally moves through the following stages:

- **Complaint Submitted** – The Client creates a complaint using Create Ticket.
- **Ticket Created as Open** – The complaint enters the system with Open status.
- **Admin Review and Assignment** – The Admin reviews the complaint and assigns it to the relevant Staff member.
- **Ticket Moved to In Progress** – Once work begins, the complaint status changes to In Progress.
- **Complaint Resolved** – The Staff resolves the issue and updates the complaint status to Done.
- **Complaint Closed** – The complaint may then be marked as Closed, depending on the workflow.

Suggested FAQs for CMS

Q1. How do I submit a complaint?

Go to CMS → Create Ticket, complete the required fields, and submit the complaint.

Q2. How can I track my complaint?

You can track it through the CMS Dashboard, Ticket Details, and Timeline.

Q3. Can I upload images or files with my complaint?

Yes, the Attachments field allows you to upload supporting files.

Q4. Who can assign my complaint to a staff member?

Only the Admin can assign complaint tickets to Staff.

Q5. How do I communicate about my complaint?

Use the Comments / Chat section within the ticket.

Q6. Who changes the complaint status?

The Admin manages complaint status updates, and the Staff can mark complaints as Done after resolution.

SOS / Emergency Alert Feature

Overview

The SOS / Emergency Alert feature in the SAMS ERP Mobile App is designed to provide immediate assistance during emergency situations. This feature allows users to instantly notify Admin and Staff members through the Complaint Management System (CMS) for urgent response and support.

The system automatically creates an SOS ticket, shares the user location (if enabled), and routes the alert to the assigned emergency response department.

SOS / Emergency Feature for Client

Client Permissions

- Trigger SOS alert
- View emergency ticket details
- Track emergency status
- Communicate with Admin and Staff
- View ticket timeline

SOS Screen

Purpose: This feature lets users quickly send out an emergency alert whenever they need to.

- Creates SOS ticket
- Sends emergency notifications to Admin and staff members
- Shares live location

Step-by-Step Instructions:

1. Open the SAMS Mobile App.
2. Go to CMS
3. Tap the SOS / Emergency button. (located at the top right on the screen)
4. Tap and hold the SOS button for 3 seconds.
5. Allow location permission if prompted.
6. Wait for the confirmation message.
7. Track updates through Ticket Timeline.

Do's:

- ✓ Use SOS only in real emergencies
- ✓ Keep GPS enabled
- ✓ Stay available for communication

Don'ts:

- × Do not misuse the SOS functionality
- × Do not disable GPS during emergencies

SOS Ticket Details

- Ticket ID
- Status
- Assigned Staff
- Timeline
- Location

Comments / Chat

1. Open SOS ticket.
2. Tap Comments.
3. Enter message.
4. Tap Send.

SOS / Emergency Feature for Staff

Staff Permissions

- Receive emergency alerts
- Accept emergency requests
- Track user location
- Update ticket status
- Communicate with Client and Admin

Emergency Alert Screen

Purpose: Displays incoming SOS alerts assigned to Staff users.

Step-by-Step Instructions:

1. Open emergency alert notification.
2. Review ticket details.
3. Tap Accept Response.
4. Navigate to user location.

5. Update ticket status.

Do's:

- ✓ Respond immediately
- ✓ Track user location carefully
- ✓ Update ticket regularly

Don'ts:

- × Do not delay emergency handling
- × Do not close unresolved tickets

Live Location Tracking

1. Open SOS ticket.
2. Go to Ticket Details.
3. Tap the location link.
4. Open map/navigation.
5. Track user location.

SOS / Emergency Feature for Admin

Admin Permissions

- Monitor SOS tickets
- Assign/reassign Staff
- Track emergency response
- View emergency analytics

SOS Dashboard

- Open emergency tickets
- Assigned responders

Ticket Management

1. Open emergency ticket.
2. Review details.
3. Assign or reassign Staff.
4. Monitor response progress.
5. Close the ticket after resolution. (Optional)

SOS Workflow Summary

1. User presses the SOS button
2. System validates the emergency department
3. SOS ticket is created
4. Alerts are sent to Admin & Staff
5. First Staff response is accepted
6. Other responses are ignored
7. User location is attached
8. Staff tracks the user on the map

Validation Rules

- SOS department must exist
- Location permission is required
- Internet connection is required
- Only the first response is accepted

Error Messages

- “This department is currently unavailable. Please contact support or administration.”
- “Location access is required.”
- “No internet connection.”
- “SOS/Emergency request already accepted.”

Role-Wise Access Summary

Feature	Client	Staff	Admin
Trigger SOS	Yes	Optional	Optional
View SOS Ticket	Yes	Yes	Yes
Accept Request	No	Yes	Yes
Track Location	No	Yes	Yes
Assign/Reassign	No	No	Yes
Close Ticket	Yes	No	Yes

Best Practices

For Clients

- Use SOS only during actual emergencies
- Keep GPS enabled

For Staff

- Respond immediately
- Maintain ticket updates

For Admin

- Monitor emergency responses
- Ensure emergency staff availability

SOS Workflow Diagram

1.23.15. Booking Form

Used to submit booking requests directly from the app.

Accessing the Booking Form

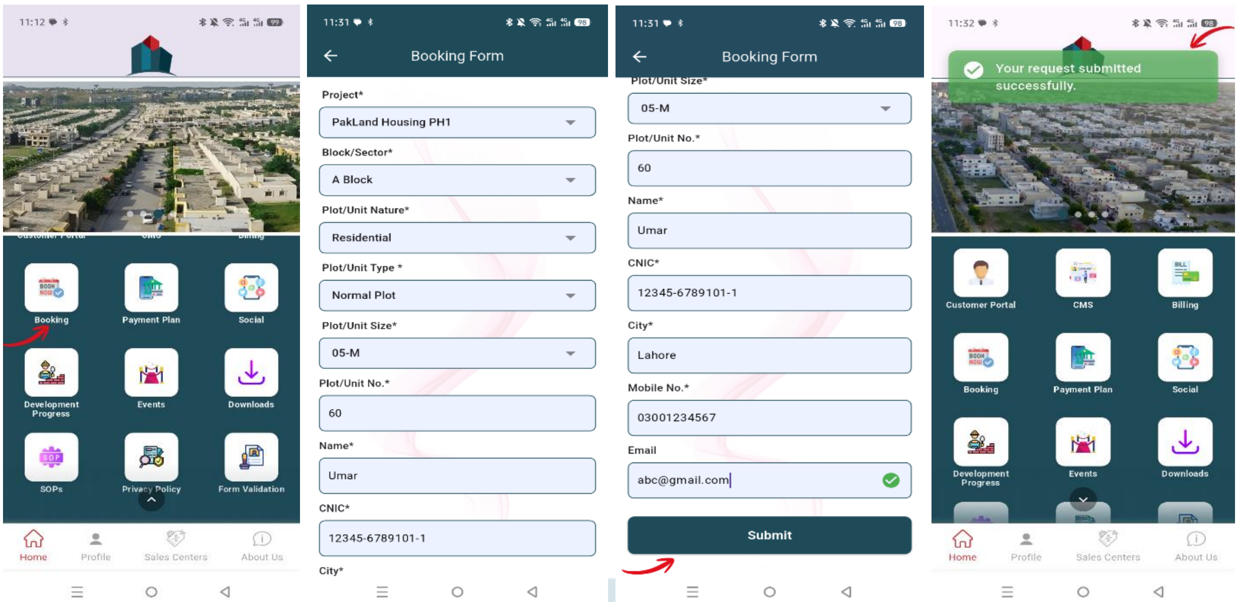
Navigate to the **Booking Form** from the main menu.

Required Information

- Project Selection
- Payment Plan & Unit Selection
- Personal Details (Name, CNIC, Mobile Number, Email, and City)

Example Submission

A user selects a unit in "Block A", enters personal details, and submits the booking form. The backend team verifies and confirms the booking.



1.23.16. Payment Plans

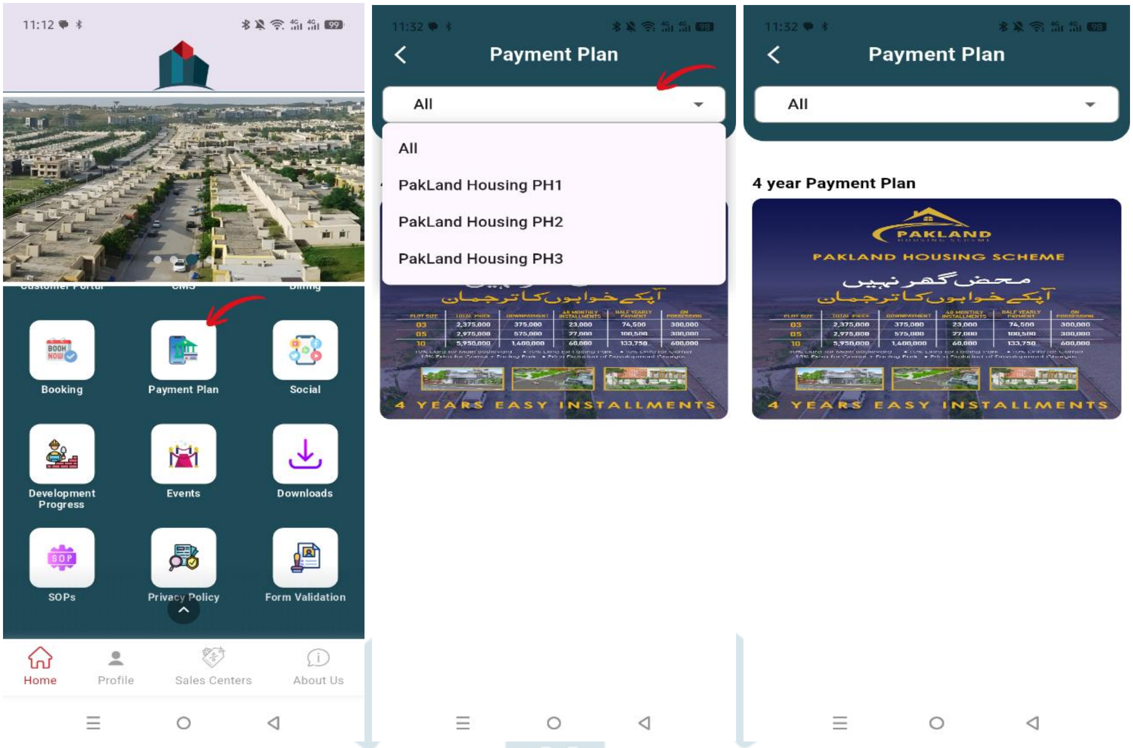
This screen displays all payment schedules for users' convenience.

Filtering Options

Users can filter plans by projects.

Example

If a user wants to view the plans for a specific project, they should select that project from the dropdown menu. To see all payment plans, they can choose "All."



1.23.17. Social Media Links

The Social Media Links screen provides users with quick access to the organization's official online platforms. This ensures they stay connected with the latest project updates, announcements, and media content.

Purpose

This section helps users follow the company's authentic social media profiles directly from within the app, improving communication and trust.

Features

- Displays a list of official social media platforms.
- Opens links in the device's browser or installed app.
- Ensures secure redirection with no data sharing.

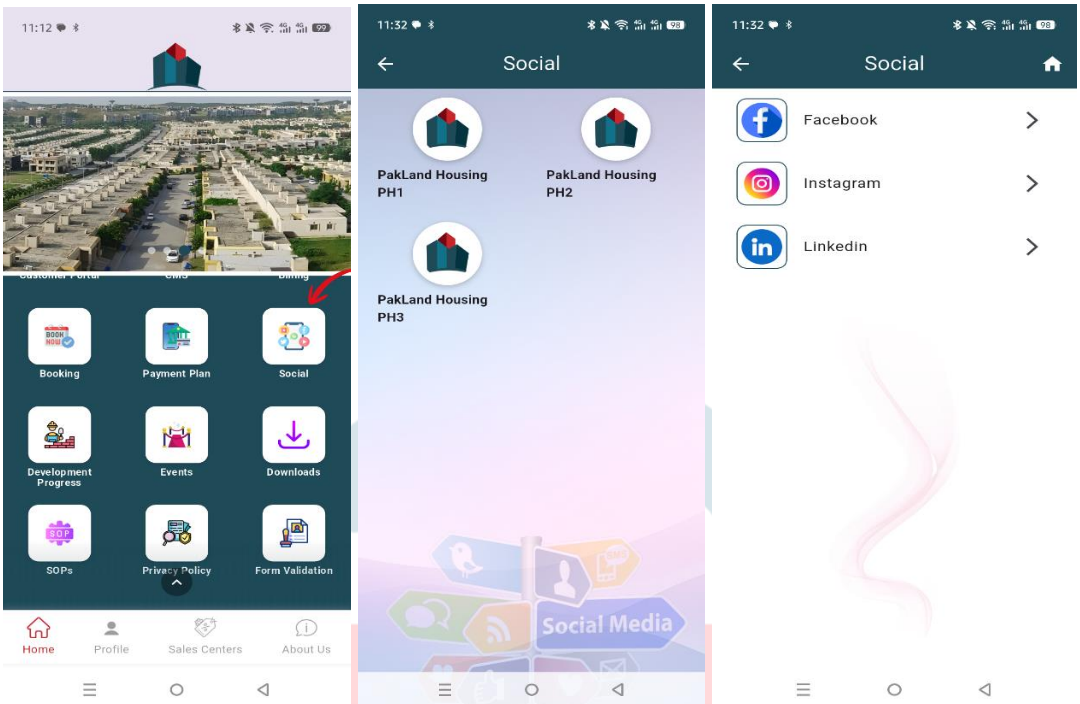
Available Social Media Platforms

Depending on the organization's online presence, the following links may appear:

- Facebook
- Instagram
- YouTube

- LinkedIn
- WhatsApp

etc.



1.23.18. Events

Event Listings

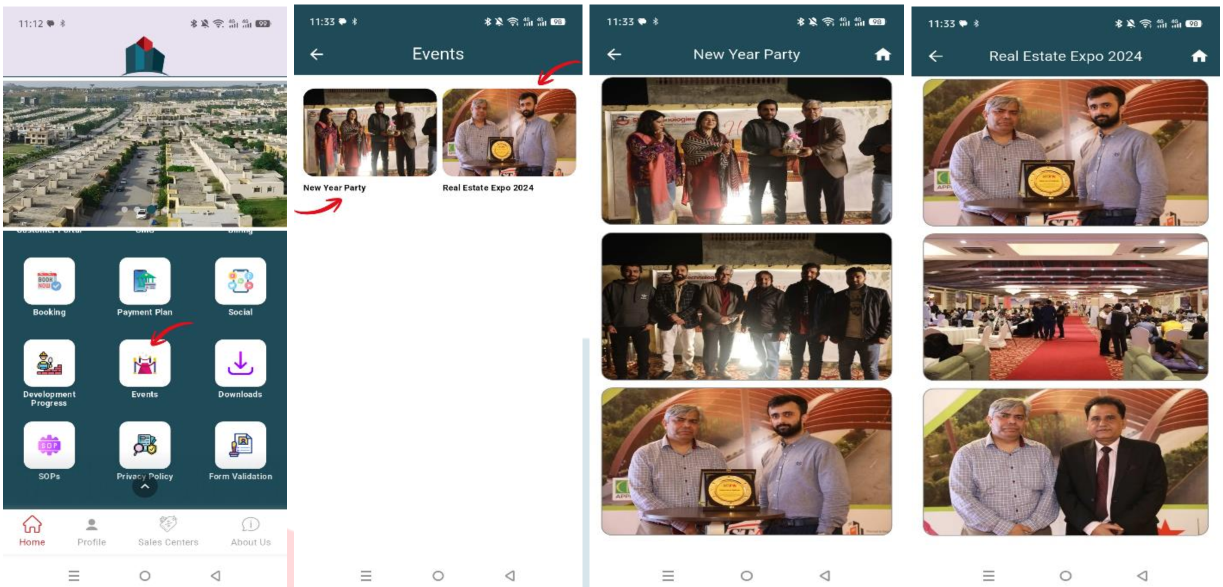
Shows upcoming and past events, including:

- Launch Events
- Customer Meetups
- Balloting
- Seminars

Event Details

Each event includes:

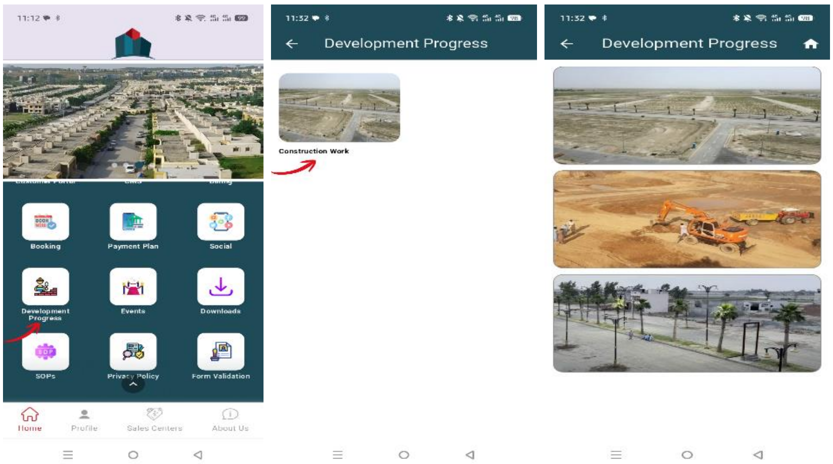
- Title
- Description
- Date



1.23.19. Development Progress

Provides real-time updates on project construction, including:

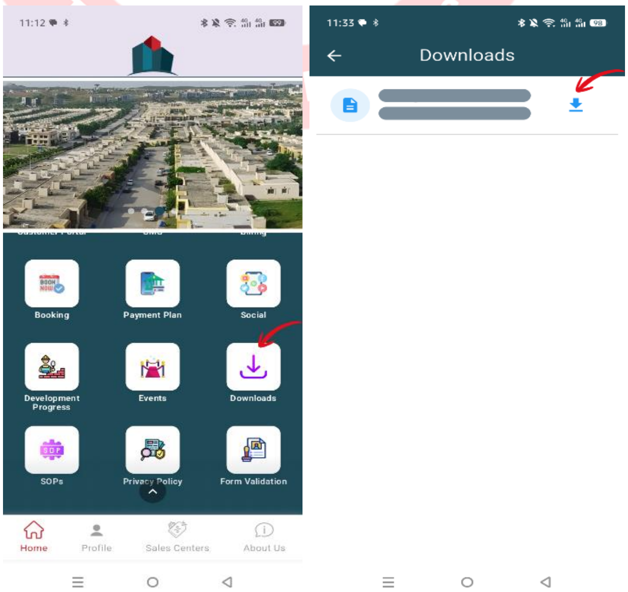
- Images
- Milestone achievements



1.23.20. Downloads

Contains digital resources such as:

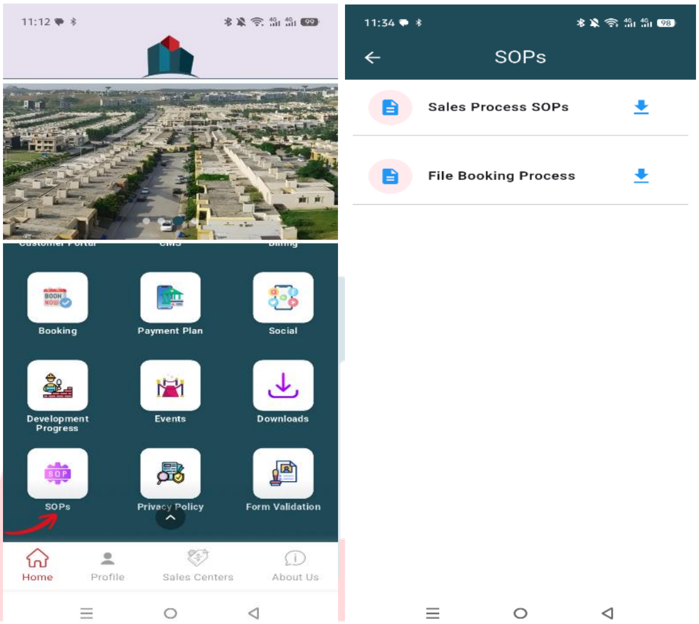
- Brochures
- Layout Plans
- Misc. Documents
- Notices
- Marketing Materials



1.23.21. SOPs (Standard Operating Procedures)

Users can review and download guidelines such as:

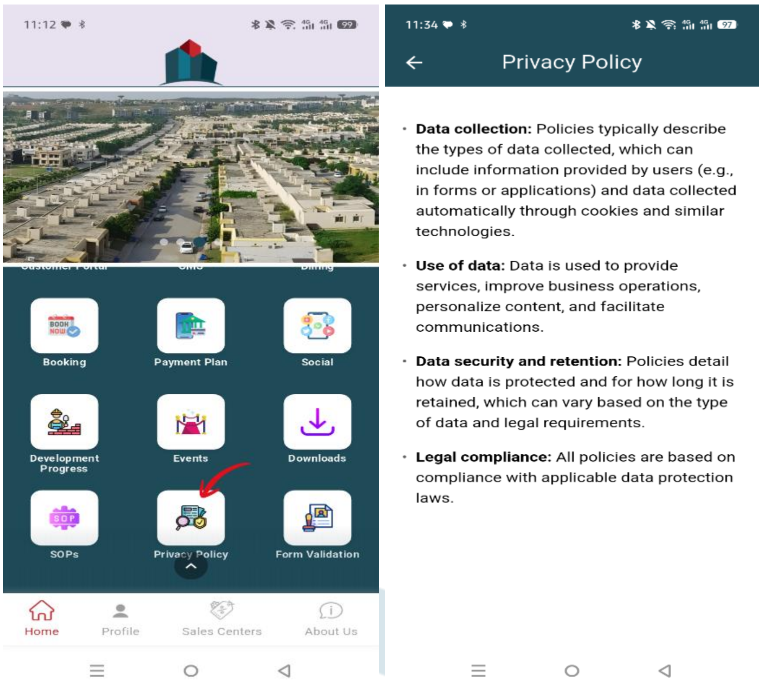
- Payment SOPs
- Complaint Handling SOPs
- Documentation SOPs



1.23.22. Privacy Policy

Explains:

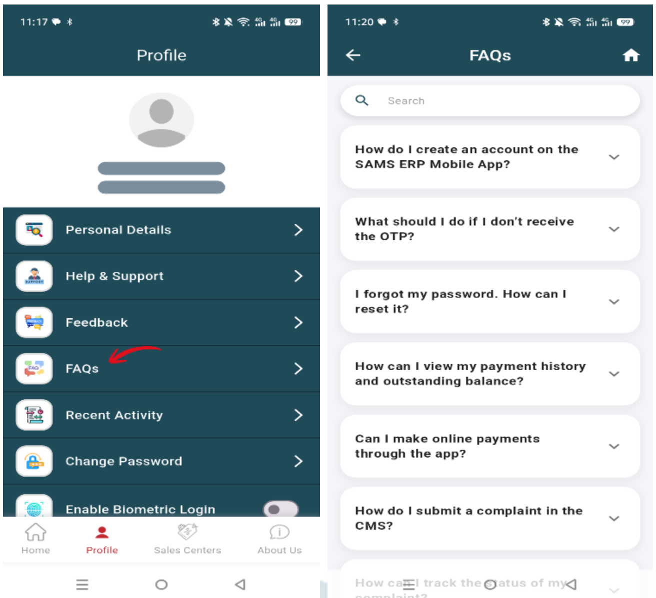
- How data is collected
- How your information is used
- User rights and responsibilities



1.23.23. FAQs

A detailed list of common questions related to:

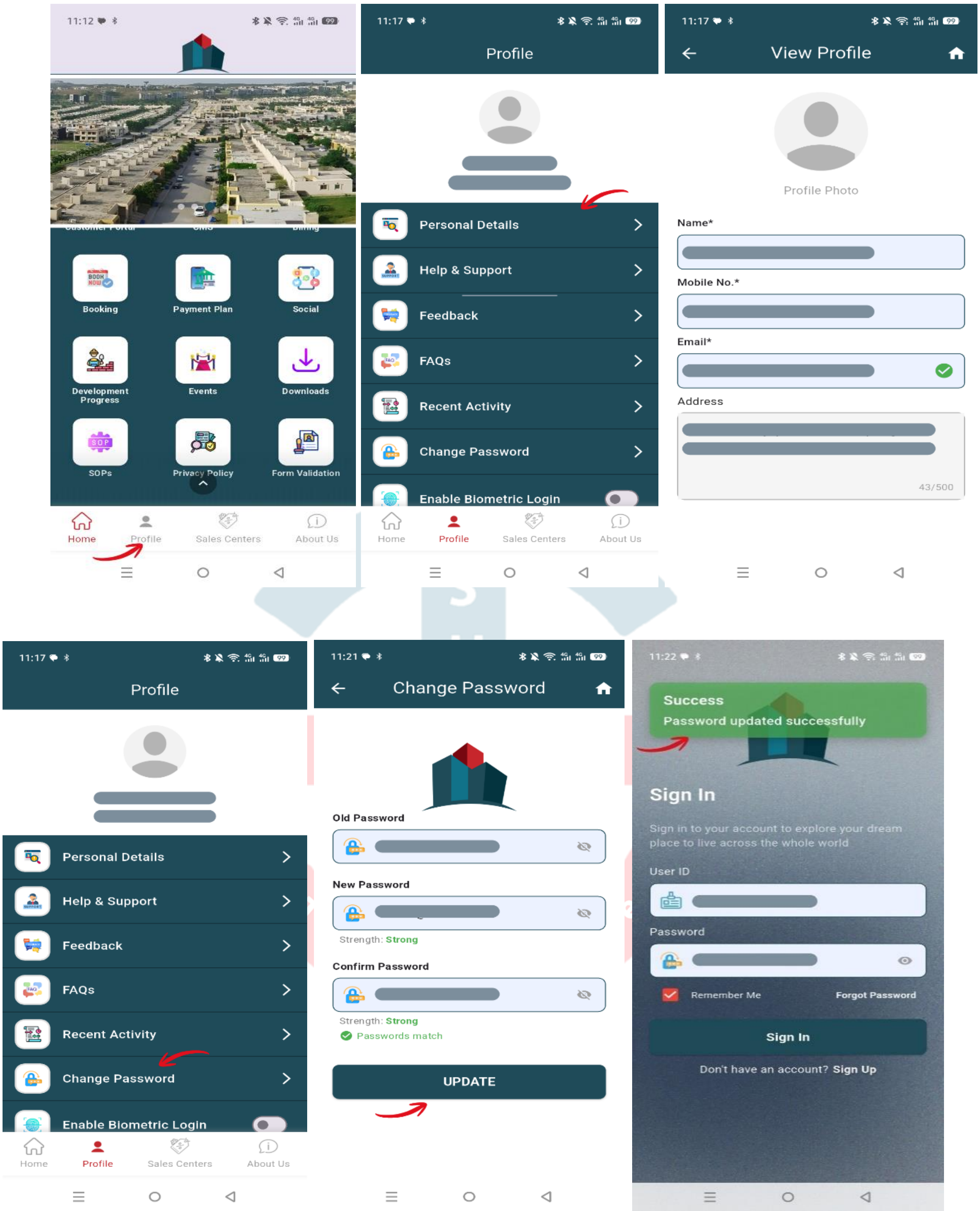
- Account
- Bookings
- Payments
- Complaints
- App Navigation

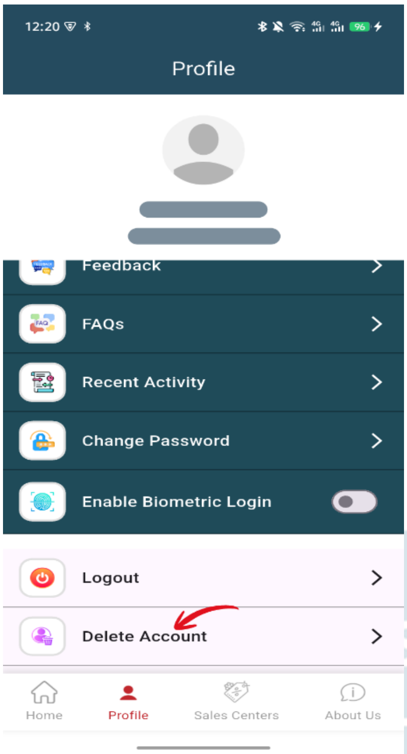


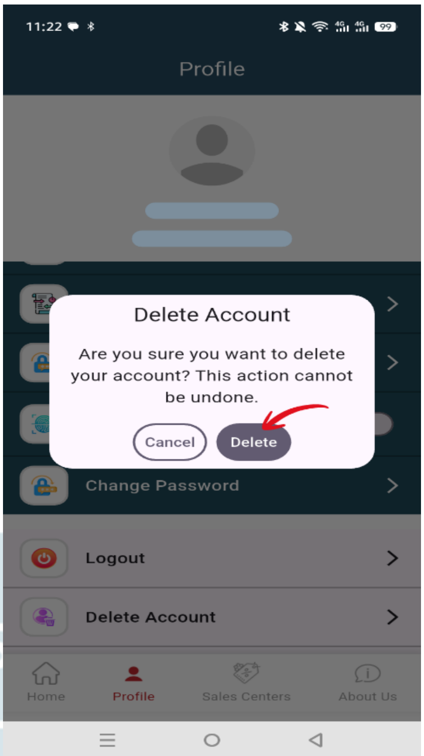
1.23.24. Profile

Allows users to:

- View Personal Information, i.e., name, mobile number, email address
- Get Help & Support
- Give Feedback
- Change Password
- Logout
- Delete Account


Booking
Payment Plan
Social
Development Progress
Events
Downloads
SOPs
Privacy Policy
Form Validation
Home
Profile
Sales Centers
About Us
Profile
Personal Details
Help & Support
Feedback
FAQs
Recent Activity
Change Password
Enable Biometric Login
View Profile
Profile Photo
Name*
Mobile No.*
Email*
Address
43/500
Change Password
Old Password
New Password
Strength: Strong
Confirm Password
Strength: Strong
Passwords match
UPDATE
Success
Password updated successfully
Sign In
Sign in to your account to explore your dream place to live across the whole world
User ID
Password
Remember Me
Forgot Password
Sign In
Don't have an account? Sign Up





1.23.25. Sales Centers

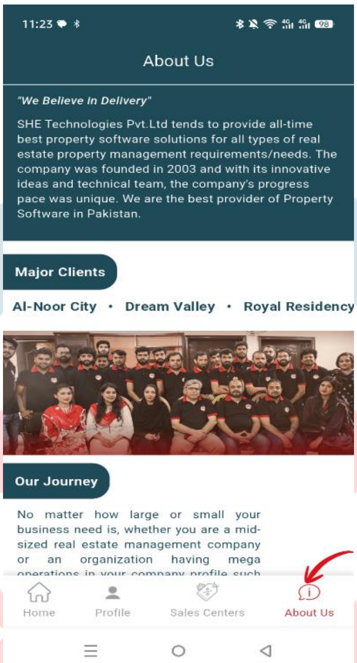
Displays:

- Sales Centers' Locations
- Contact Numbers
- Working Hours

1.23.26. About Us

Includes company:

- Overview
- Values
- Mission & Vision

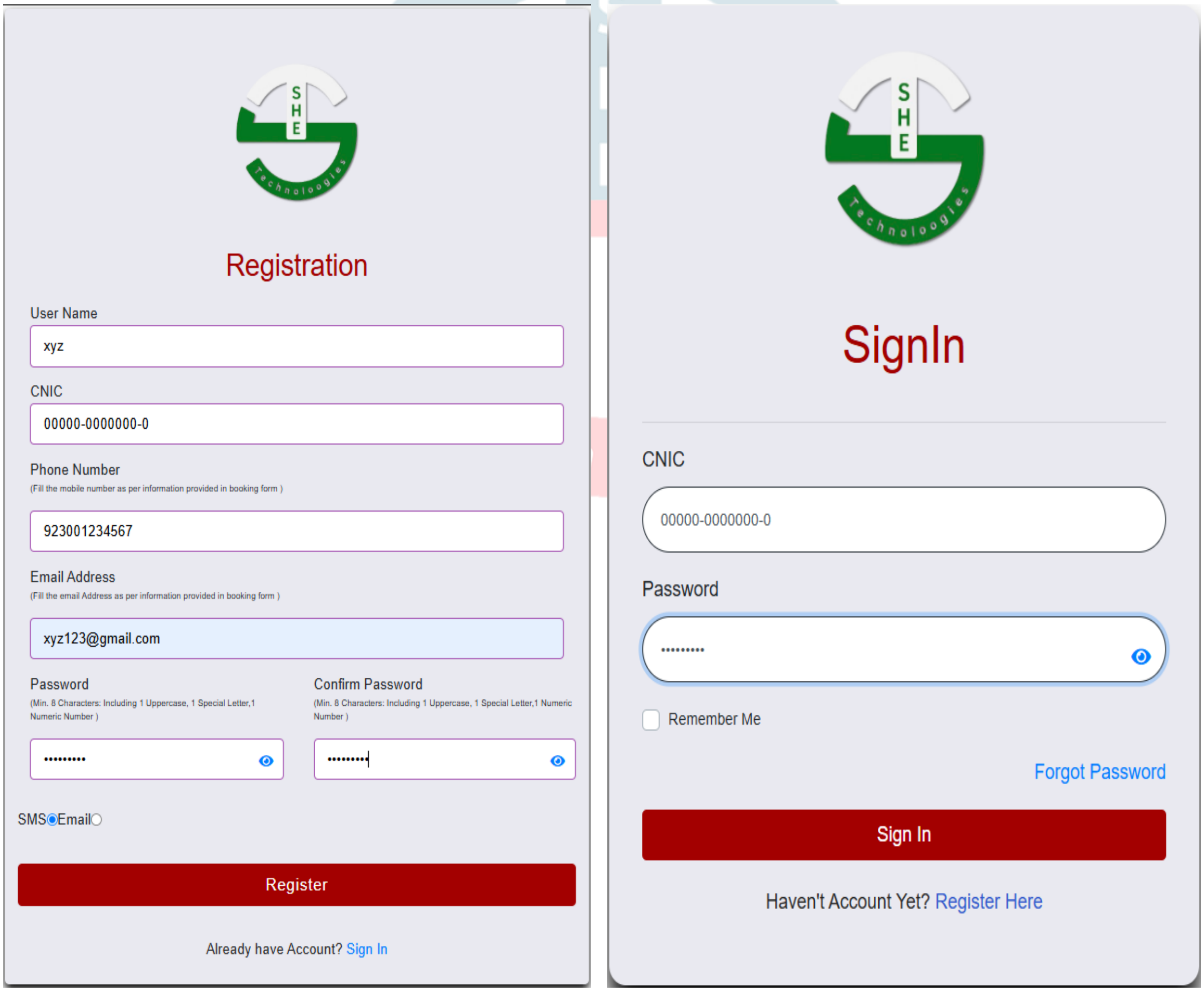


1.24. Client Portal

Your step-by-step guide to get booking details, receipts, making payments, checking account statements, and managing your real estate journey online.

1.24.1. Getting Started

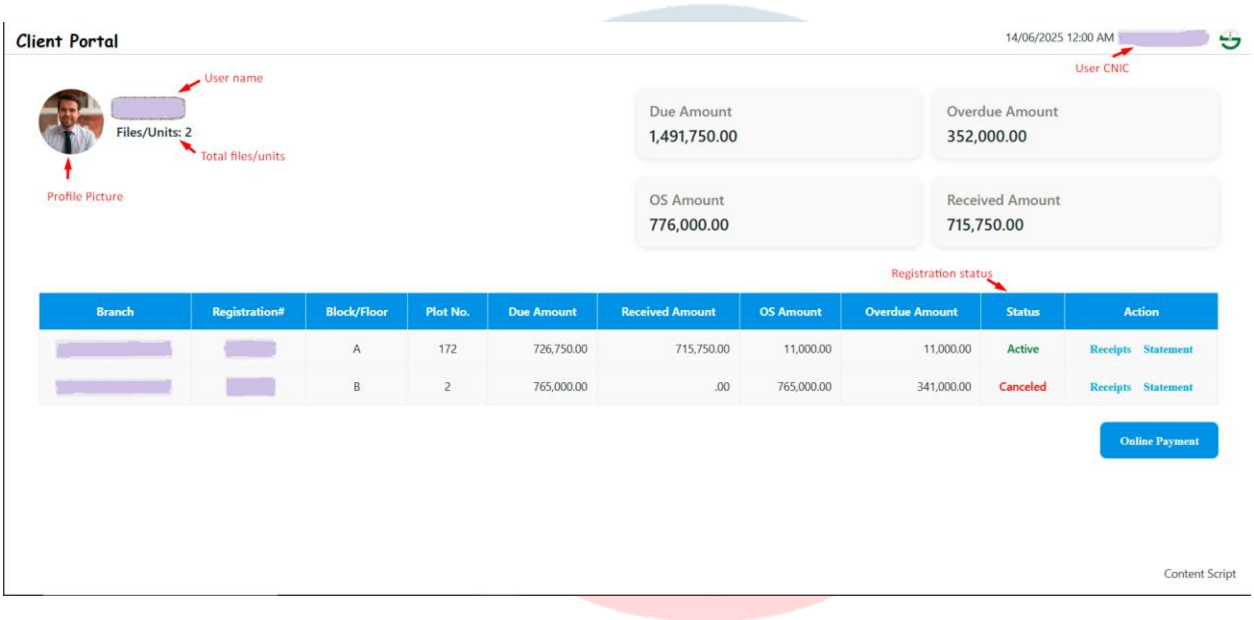
Step 1: Go to [portal URL]
Step 2: Click **Sign Up** if you're a new user, or **Sign in** if you already have an account
Step 3: Enter your basic details and verify your phone/email
Step 4: You'll land on your **Dashboard**, where everything starts



1.24.2. Dashboard

Users get the following information on their dashboard:

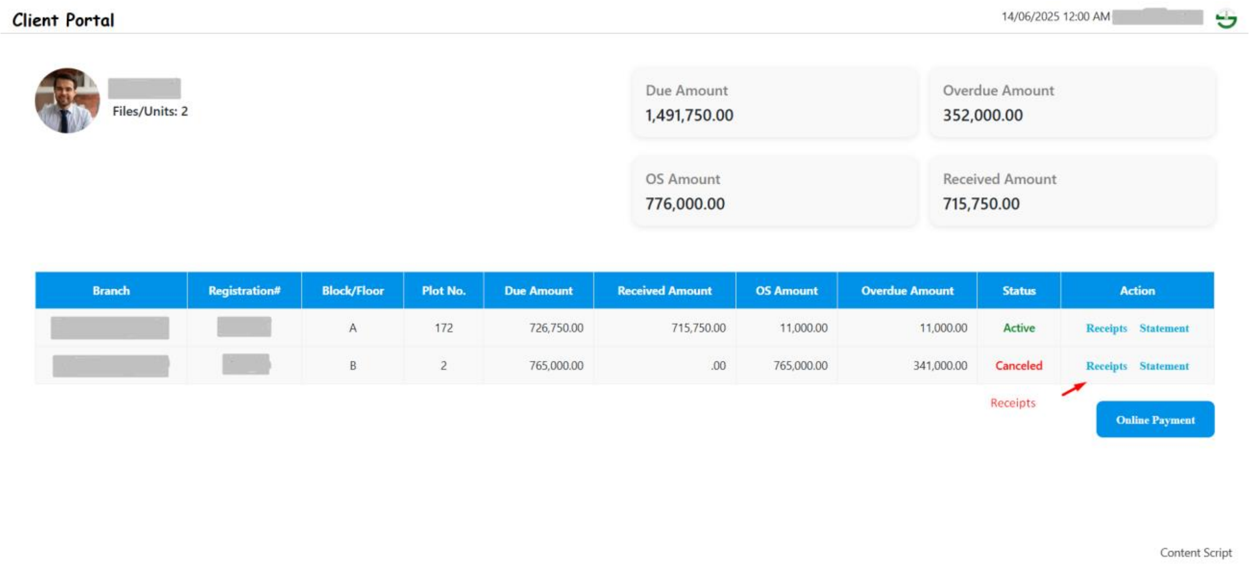
1. Personal information (Name, Profile picture, CNIC)
2. Booking details (Branch, Registration number, Block/Floor, Plot/Unit no.)
3. Registration status
4. Financial information (Due Amount, Received Amount, Outstanding Amount, Overdue Amount)
5. Receipts
6. Account statement

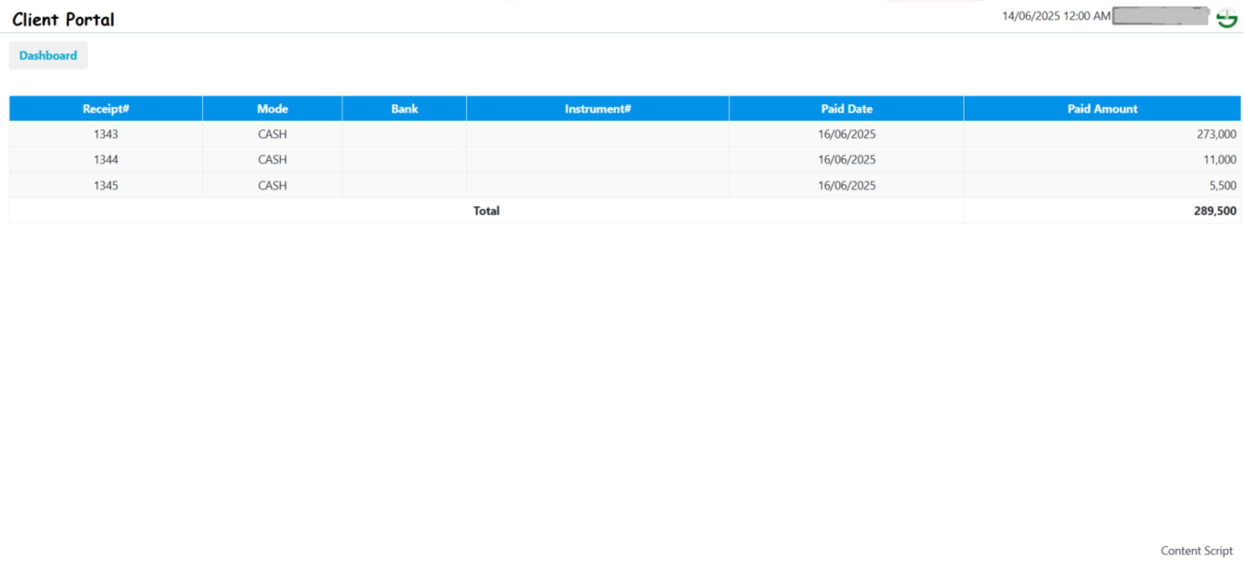


1.24.3. Viewing Receipts

Users can view their receipt details, e.g., receipt no., payment mode, bank name, instrument (cheque no.) no., etc., by following these steps:

1. Go to the **Dashboard**
2. Click on **Receipts**
3. Find the one you want

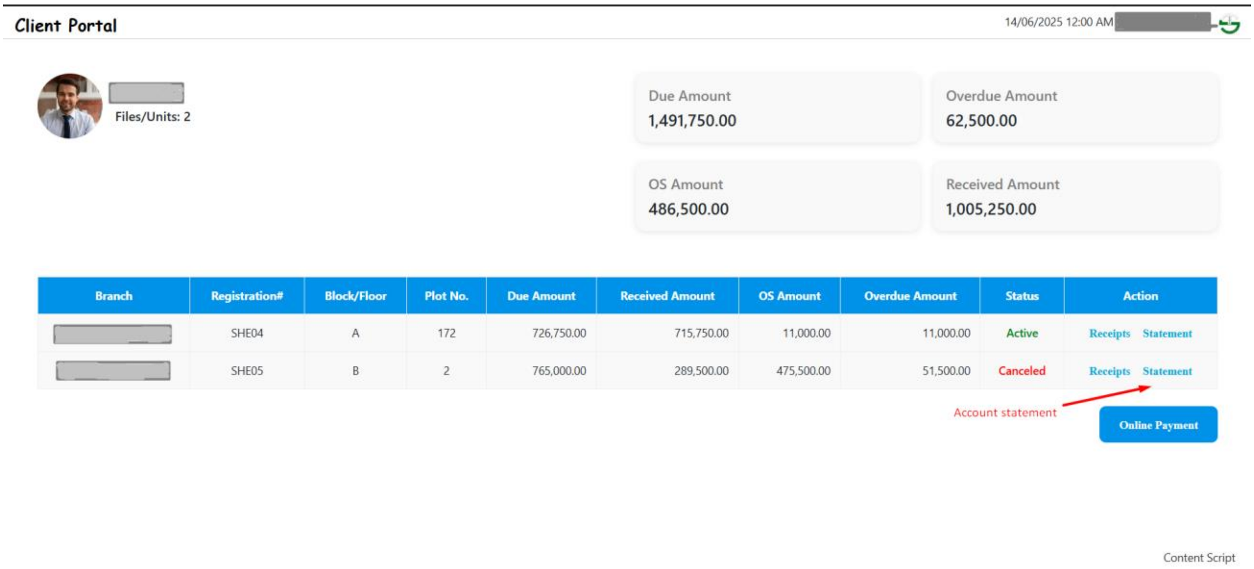


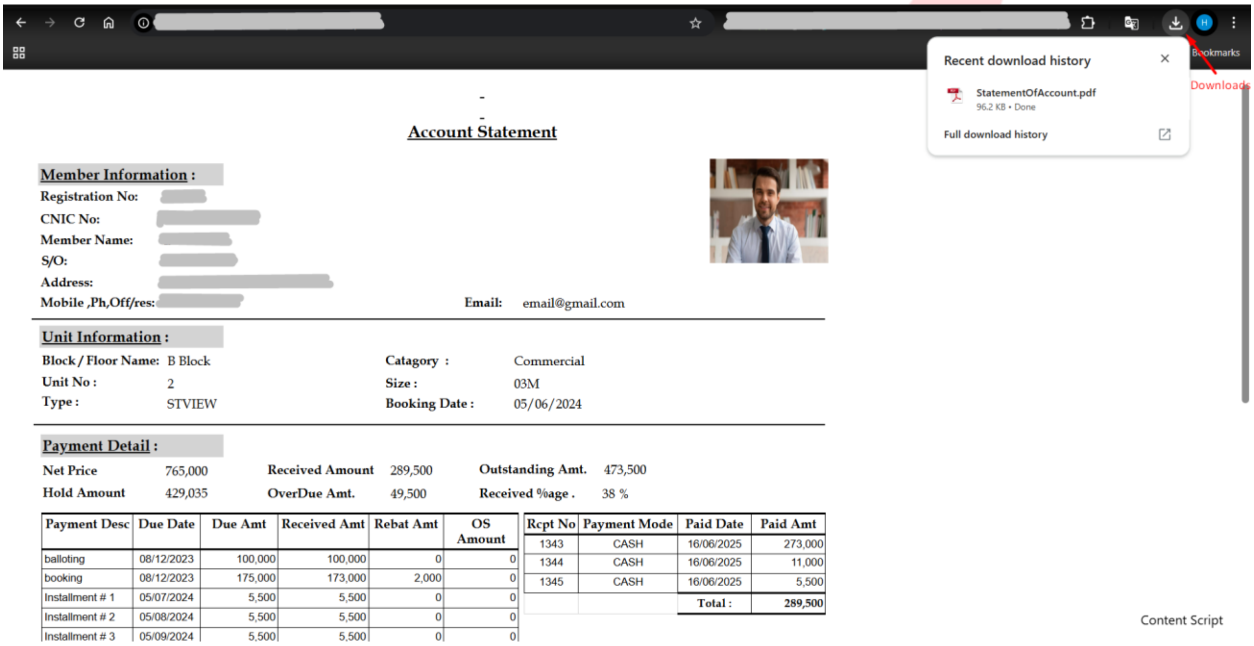


1.24.4. Checking Account Statement

1. Go to the **Dashboard**
2. Click on **Statement**

Note: The system will automatically download the account statement to the downloads.





Account Statement

Member Information :

Registration No:
CNIC No:
Member Name:
S/O:
Address:
Mobile ,Ph,Off/res:
Email: email@gmail.com

Unit Information :

Block / Floor Name: B Block
Catagory : Commercial
Unit No : 2
Size : 03M
Type : STVIEW
Booking Date : 05/06/2024

Payment Detail :

Net Price 765,000
Received Amount 289,500
Outstanding Amt. 473,500
Hold Amount 429,035
OverDue Amt. 49,500
Received %age . 38 %

Payment Desc	Due Date	Due Amt	Received Amt	Rebat Amt	OS Amount
balloting	08/12/2023	100,000	100,000	0	0
booking	08/12/2023	175,000	173,000	2,000	0
Installment # 1	05/07/2024	5,500	5,500	0	0
Installment # 2	05/08/2024	5,500	5,500	0	0
Installment # 3	05/09/2024	5,500	5,500	0	0

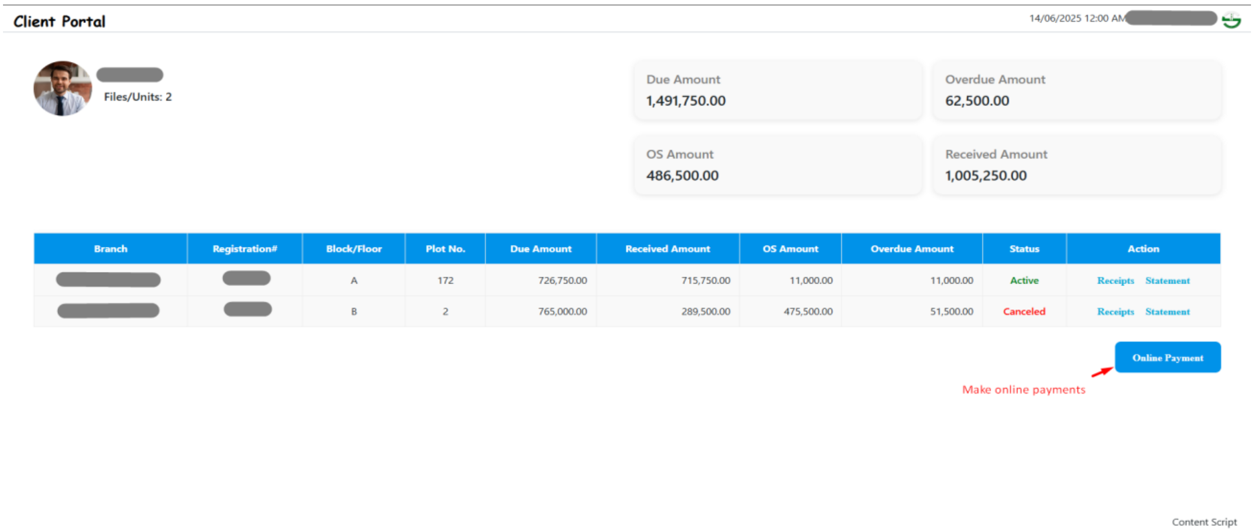
Rcpt No	Payment Mode	Paid Date	Paid Amt
1343	CASH	16/06/2025	273,000
1344	CASH	16/06/2025	11,000
1345	CASH	16/06/2025	5,500
		Total :	289,500

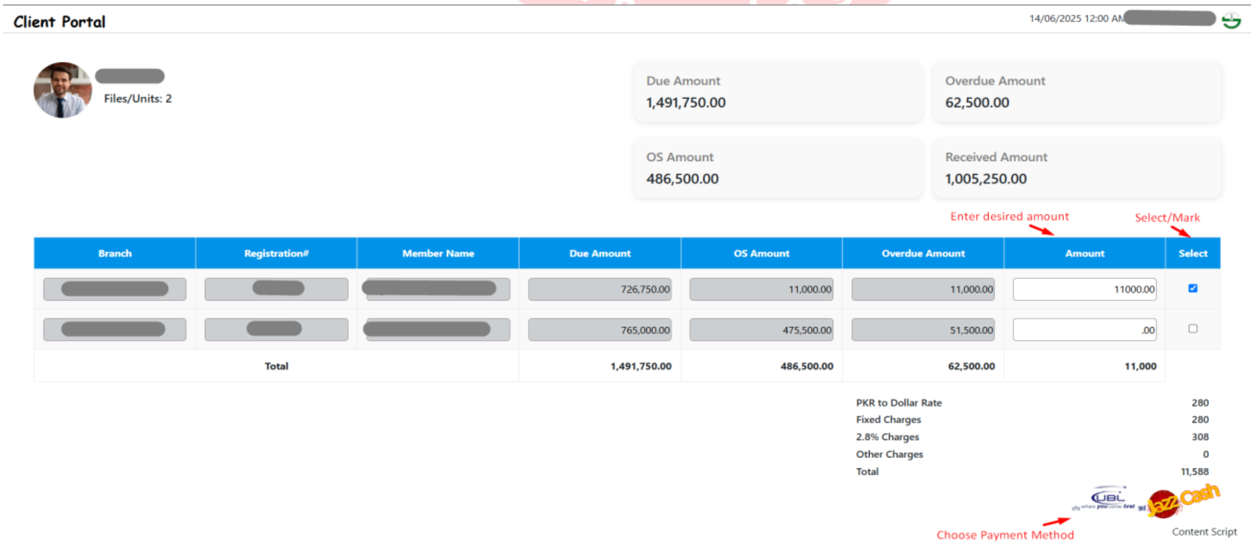
1.24.5. Making Online Payments

1. Go to the **Dashboard**
2. Review your due, overdue, or outstanding amounts
3. Click on **Online Payments**
4. Enter the desired amount in the **Amount** field
5. Select/Mark the entered amount
6. Choose your payment method (Debit/Credit Card, JazzCash, etc.)
7. Complete the payment

Note: Users will get a receipt once the transaction is complete.

Please contact customer support for an understanding of extra charges like currency exchange rate, fixed charges, 2.8% charges (may vary according to the terms & conditions), and other charges.





1.24.6. Help/Support

Support is available **[Day Start] to [Day End], [Scheduled Hrs.]**

Email us at: **[support email]**

Call Us at: **[support number]**

1.24.7. Frequently Asked Questions (FAQs)

Q: How do I reset my password?
A: Click "Forgot Password" on the Sign in screen and follow the steps.

Q: How do I change my password?
A: Click "Change Password" on the Profile section on the top right corner of the screen and follow the steps.

Q: Is my data secure?
A: Yes, your information is encrypted and safely stored.

1.25. Recovery Module

Recovery Module – Workflow

This document outlines the enhanced flow of the Recovery Module, highlighting key features and screen functionalities designed to streamline recovery operations and improve user efficiency in the SHE Technology "Recovery Module".

1.25.1. Client Assignment (Admin Role)

- Admins can assign Client IDs to users through the **"Assign User IDs"** screen.
- This centralized assignment functionality ensures accurate user-to-client mapping for recovery tracking.

1.25.2. Assigned Clients (Recovery Officer Role)

- Recovery Officers can view their allocated Client IDs via the **"Branch & ID Wise Overdue"** screen.
- This screen provides a comprehensive summary of each assigned client, including:
  - **ID Number**
  - **Member Name**
  - **Total Files**
  - **Due Amount**
  - **Received Amount**
  - **Outstanding Amount**
  - **Overdue Amount**

1.25.3. View Client Details

- Officers can access detailed client information by clicking the **"Details"** button on the Overdue screen.
- This section includes:
  - **Personal Information**
  - **Registration Inquiry**
  - **Receipt Inquiry**
  - **File Status Overview**
- It offers a complete 360-degree view of the client's history and current status.

1.25.4. Get Follow-up

- Officers can initiate or review follow-ups by selecting the **"Get Follow-up"** option.
- This feature allows them to:
  - Log new follow-up entries
  - View the **entire follow-up history** for the selected client ID
- Enables informed and consistent communication with clients.

1.25.5. Dashboard Overview

- The **Dashboard** provides a real-time view of all **pending follow-ups** up to the current date.
- The dashboard displays:
  - **Member ID**
  - **Member Name**
  - **Last Recorded Overdue Amount**
  - **Communication Type**
  - **Next Scheduled Follow-Up Date**
  - **Remarks / Additional Details**
- This ensures that no follow-up is missed and enables timely action.

1.25.6. Follow-Up List Management

- Users can manage and review actions taken for each assigned client based on:
  - **Date**
  - **Overdue Amount**
  - **Last Call to Action**
- The **Last Call Status** of any client can also be **updated** directly from this screen, facilitating better tracking and workflow continuity.

1.26. WhatsApp

Instructions for Clients WhatsApp Groups

Please be noted, we create THREE following WhatsApp groups for each client and every client must follow the given instructions for each group.

a) ERP (Software Related Issues/Matters/Requirements)
b) Accounts Group (Financial Matters)
c) Projects Group (New Features/Modules/Functionalities)

a) ERP Group (Software Related Issues/Matters/Requirements)

- This group is dedicated to discussing software-related issues, matters, and requirements for your organization's ERP system.
- Assign and designate a **Point of Contact (one or two)** through which the queries can be shared directly.
- Please use this group to ask questions about the ERP software, report any issues or bugs, and suggest new features or improvements that you think would be helpful for your organization.
- No ticket is required for the **Issue or Error**. They are to be asked directly in the group. For the requirements and amendments required in the installed ERP system, the client is **obligatory** to generate a ticket for that particular concern so that our support members of the group can understand the problem and provide useful solution accordingly.

b) Accounts Group (Financial Matters)

- This group is for discussing financial matters related to your organization, such as payments, invoices, and forecasting.
- Please use this group to ask questions about financial reports or procedures, share updates on financial performance, and discuss any financial challenges or opportunities.

c) Projects Group (New Features/Modules/Functionalities)

- This group is dedicated for discussing **new features, modules, and functionalities** that SHE Technologies introduce in its services or the services other than provided to the client.

NOTE:

- Do not ask questions that are not related to the group. The relevant group should be involved in every conversation.
- Please keep all discussions in above stated groups **professional and respectful**. Avoid sharing any **confidential or sensitive information** like credentials of any account or database backup.

1.27. Trusted/Registered IP Access

1.27.1. Overview

Trusted/Registered IP Access is a security feature in the ERP system that ensures only users logging in from approved IP addresses can access the software. This helps protect sensitive data by restricting access to secure and verified locations (e.g., office networks).

Think of it as a digital "entry gate" that only opens for known visitors.

1.27.2. Key Benefits

- Enhances system security by allowing only whitelisted IP addresses.
- Prevents unauthorized access from unknown networks.
- Helps meet compliance requirements for access control.

1.27.3. Who Can Use This Feature?

- **Administrators**: Can add or remove trusted IP addresses.
- **End Users**: Must log in from a registered/trusted IP to access the software.

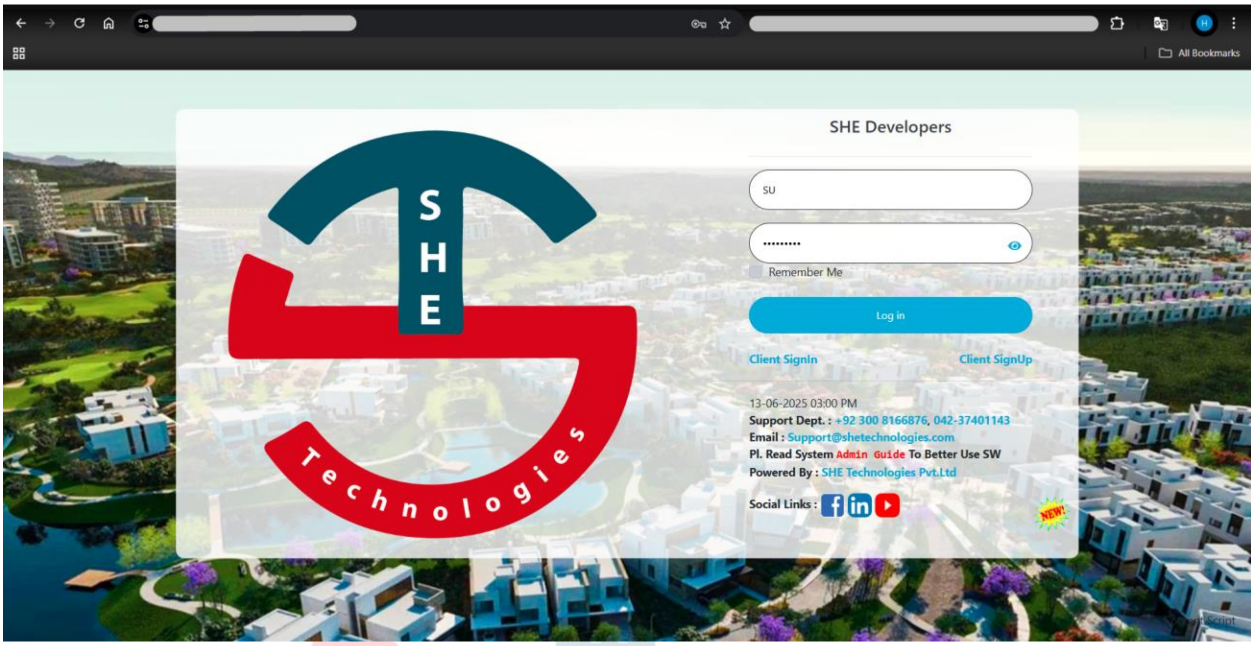
1.27.4. How It Works

When a user attempts to log in:

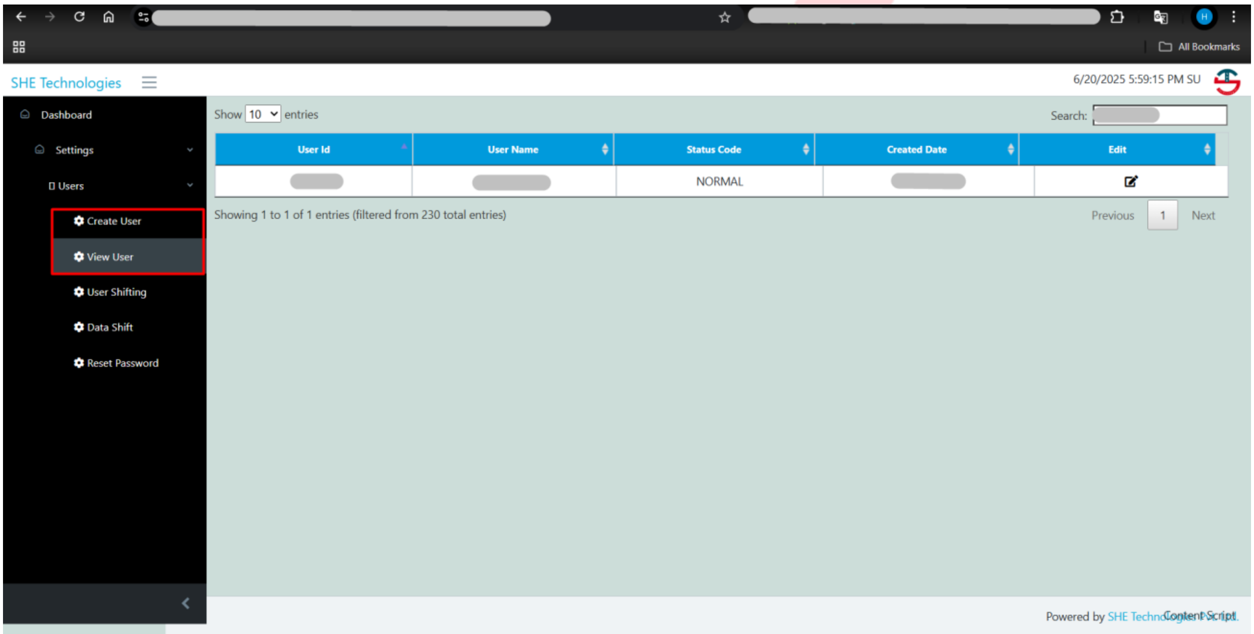
1. The system checks the user's current IP address.
2. If the IP is in the **Registered/Trusted IP list**, access is granted.
3. If not, the login is blocked, and a security notification may be triggered.

1.27.5. Accessing the Trusted IP Settings (For Admins)

1. **Log in** to the system as an Administrator.

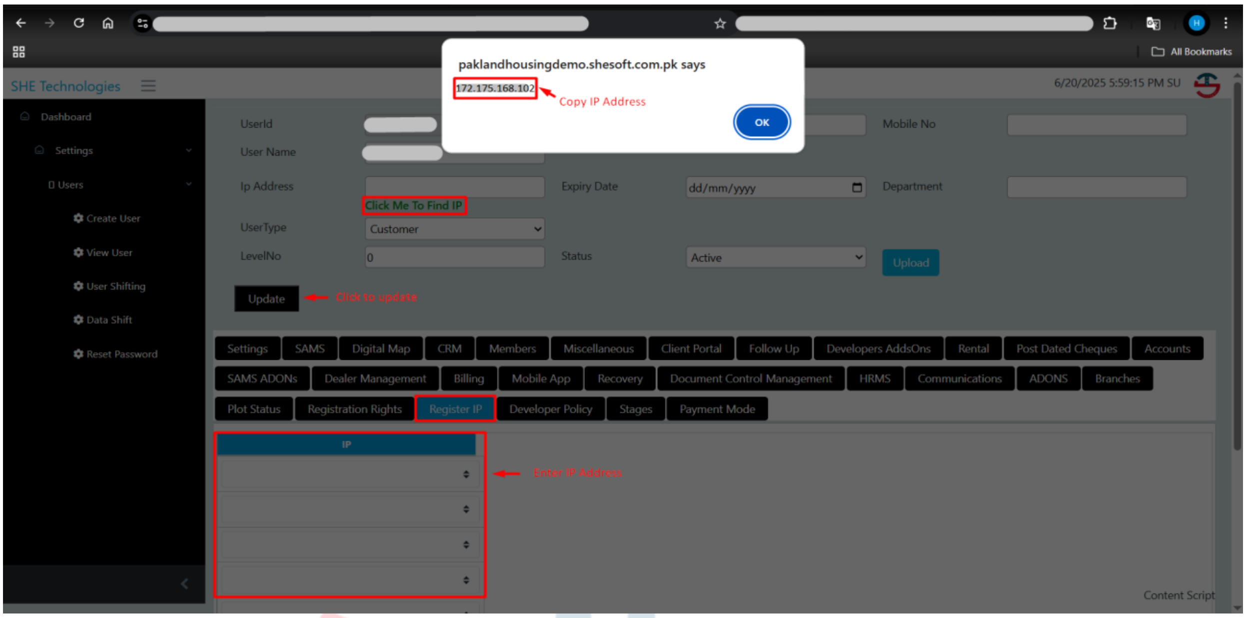


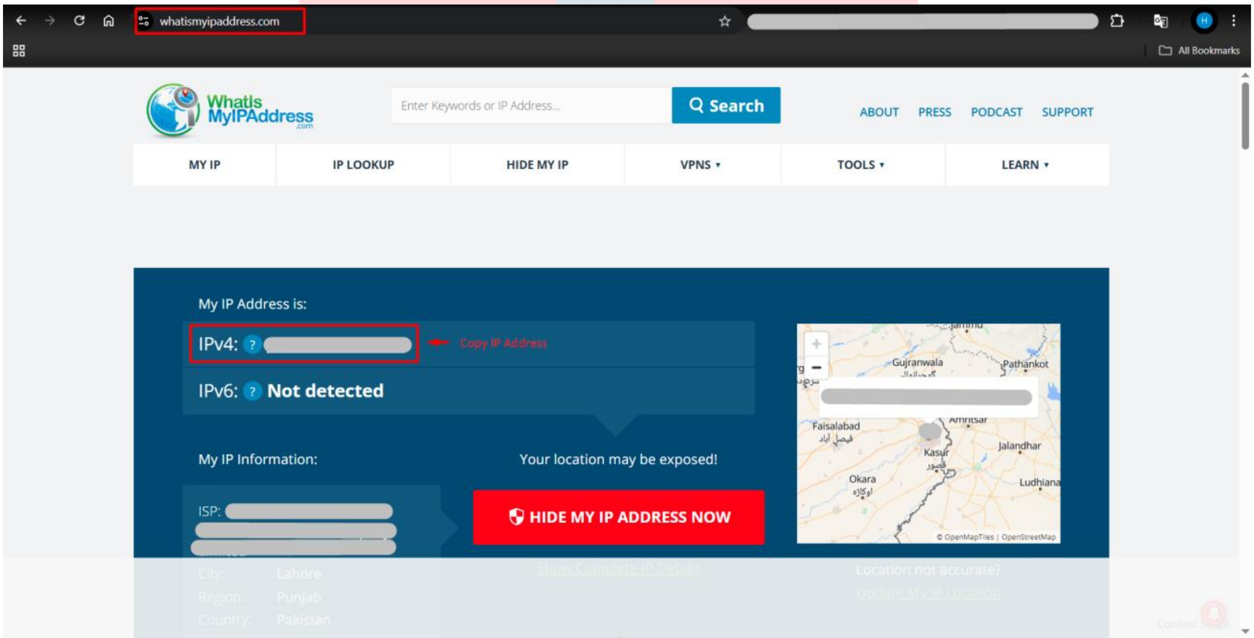
2. Navigate to:
   Settings → Users → Create/View User → Select User → Click Edit



3. Click on **"Find My IP"** or visit https://whatismyipaddress.com/
4. Copy IPv4 Address

5. Go to the **Register IP** tab.
6. Enter/Paste IP in the field.
7. Click **Save User/Update** to apply the settings.





Note: You can add multiple IP Addresses for a single user.

1.27.6. Managing Trusted/Registered IPs

Please follow these steps to update or remove IP Address.

1. Go to the **Registered IP** tab in **User Settings**.
2. Select IP to remove or update.

Note: Deleting or updating an IP currently in use may lock out active users.

1.27.7. Login Experience for Users

- If the user accesses from a **Trusted/Registered IP**, the login process continues normally.
- If the user accesses from an **Unregistered IP**, the system shows a warning:

"Access denied: Your current IP is not authorized."

Users should contact the administrator to request access.

1.27.8. Troubleshooting

Issue	Solution
1. Cannot log in from a new location	Contact your system admin to add the new IP.
2. IP added but still blocked	Ensure it is correctly formatted and enabled.
3. Admin locked out	Contact technical support.

1.27.9. Security Tips

- Use **Static IPs** where possible to prevent dynamic IP changes.
- Review and update the IP list regularly.

1.27.10. FAQs

Q1: Can I access the software from home?
A: Only if your home IP is added to the trusted list by your admin.

Q2: What happens if my IP address changes?
A: You will need to request access again from the new IP.

Q3: My IP keeps changing. What do I do?
A: Ask your internet provider for a static IP, or contact your admin when it changes.

1.28. Chrome Basic Troubleshooting

If Chrome is acting up slow, crashing, or just being weird, here's a user-friendly guide to help you fix it fast.

1.28.1. Restart Chrome

Why: Sometimes Chrome just needs a fresh start.
How:

- Click the **X** in the top-right (or red dot on Mac) to close all tabs.
- Reopen Chrome and see if the issue is gone.

1.28.2. Clear Cache

Why: Chrome stores a lot of temporary files. Over time, they can get corrupted.

How:

1. Click the **three dots** in the top-right corner → choose **Settings**.
2. Go to **Privacy and Security** → click **Clear browsing data**.
3. Select:
   - **Cached images and files**
   - **Cookies and other site data**
4. Set the time range to **All time**, then click **Clear data**.

1.28.3. Disable Extensions

Why: Extensions are helpful, but a buggy one can mess up everything.

How:

1. Click the **three dots** → **Extensions** → **Manage extensions**.
2. Toggle off all of them.
3. Refresh Chrome and check if the issue is gone.
4. Re-enable them one by one to find the troublemaker.

1.28.4. Update Chrome

Why: New versions fix bugs and speed things up.

How:

1. Click **three dots** → **Help** → **About Google Chrome**.
2. Chrome will automatically check and update if needed.
3. After it updates, **restart** Chrome.

1.28.5. Reset Chrome Settings

Why: If things are really off, resetting gives you a clean slate.

How:

1. Click **Settings** → scroll down to **Reset settings**.
2. Click **Restore settings to their original defaults**.
3. Confirm, and you're good!

1.28.6. Try Incognito Mode

Why: Incognito disables extensions temporarily.

How:

- Press **Ctrl + Shift + N** (Windows) or **Cmd + Shift + N** (Mac).
- See if Chrome behaves better in this mode. If it does, it's likely an extension issue.

1.28.7. Run Chrome's Built-in Malware Scanner

Why: It can scan your system for harmful software.

How:

1. Type `chrome://settings/cleanup` into the address bar.
2. Click **Find**, and let Chrome do its thing.

1.28.8. Turn Off Hardware Acceleration

Why: It offloads stuff to your graphics card, but sometimes it backfires.

How:

1. Go to **Settings** → **System**.
2. Turn off **Use hardware acceleration when available**.
3. Restart Chrome.

1.28.9. Check Your Internet

Why: Sometimes the problem isn't Chrome, it's your Wi-Fi.

How:

- Try another website or open Chrome on your phone.
- Still slow? Restart your router.

1.28.10. Create a New Chrome Profile

Why: Your profile might be corrupted.

How:

1. Click your profile icon (top right).
2. Choose **Add** → create a new user.

Sign in with your Google account.

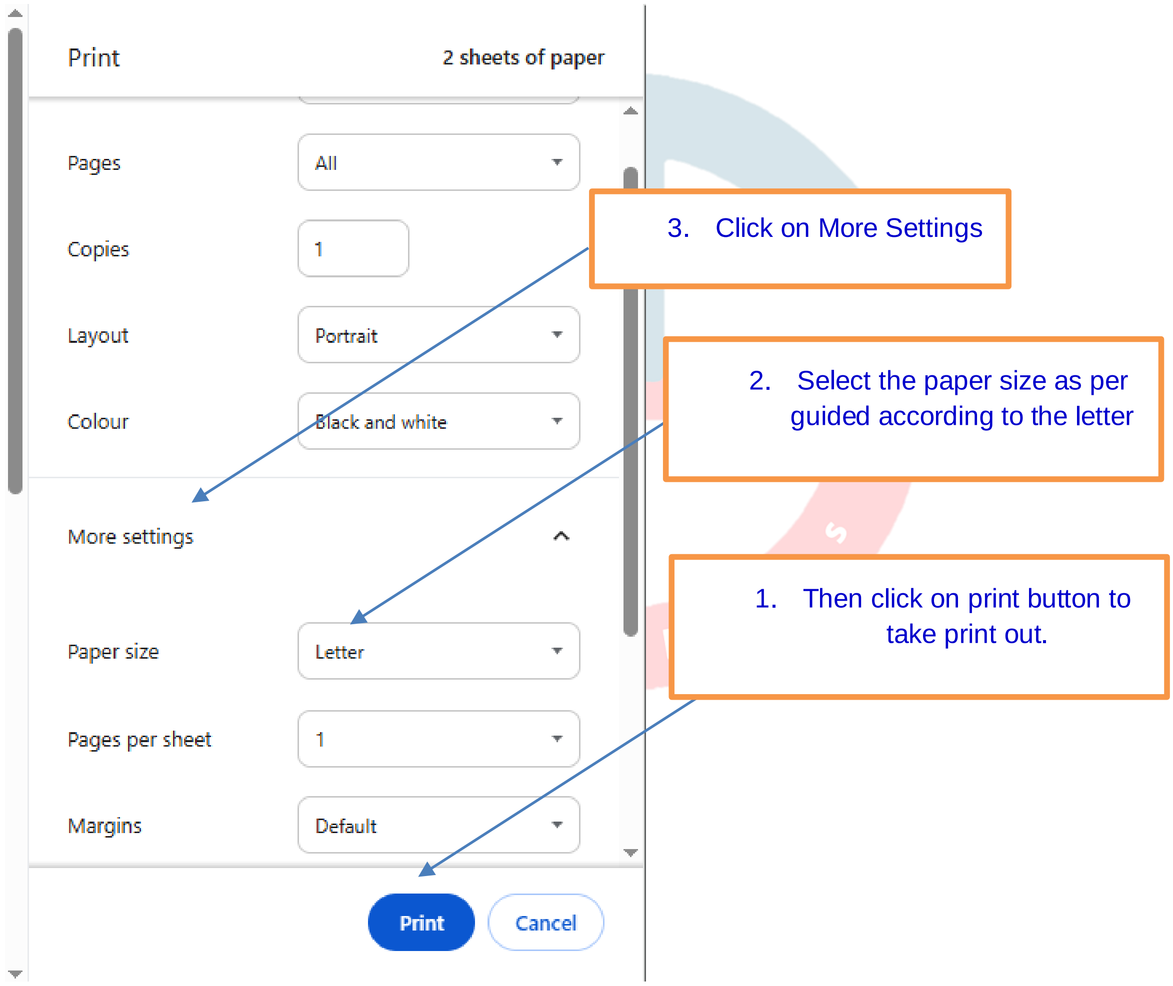
1.29. Ufone Mask Approval Procedure

Sr. No.	Task Detail	Responsibility	Status	Remarks
	Ufone Mask Approval Procedure			
1	Fill the documents on company letterhead that sent by SHE and send us back scanned copies. Manager / GM / Director / CEO any authority can fill the document	Client	Pending	
2	Required NTN certificate of company	Client	Pending	
3	Required CNIC copy of signed authority	Client	Pending	
4	Static IP Address required to use SMS portal on a specific computer	Client	Pending	
5	Masking will be 11 Characters max (including spaces)	Client	Pending	
6	For English messages, the Maximum length is 153 characters and the max is 765 (5 messages) at once	Client	Pending	
7	For Urdu messages maximum length is 67 characters and the max is 335 (5 messages) at once	Client	Pending	
8	Internet required for sending SMS (Internet Speed should be Minimum 50MB)	Client	Pending	
9	Telecom does not give any surety of SMS for converted numbers	Client	Pending	
10	Scan the following documents and send on to info@shetechnologies.com	Client	Pending	
11	It is normally takes a month to complete the process.	Client	Pending	
12	Per SMS cost Rs. 3.50/- **(Price can be increased in future as per company's rate increment)**	Client	Pending	
13	Minimum amount is Rs. 50,000/- after that you will recevie the monthly bill per SMS usage.	Client	Pending	
14	**Promotional Blocked Number Solution** - write unsub and send to 3627 For Mobilink/Warid - dial *3627# and choose 2nd option For Telenor - call on helpline and tell to operator to remove DNCR from his number For Ufone			
15	**Converted Number Solution** - Write MNP and send to 8331 For all network			

1.30. Printer Settings

Printer Settings for DotNet Letters/Reports

- Preferable browser is Google Chrome.
- Open any Letter/Report on your chrome browser.
- Press Ctrl + P and you will see the below screen.



1.31. Contact Us

We are here to serve & help you always and can contact with our respective teams.

Below are our contact numbers. Can co-ordinate accordingly from 10am ~ 6pm

Break time 1pm ~ 2:30pm

Support Team:

For any software related points / issues

PTCL 042 3740 1143
PTCL 042 3524 7773
Mobilink 0300 8166 876
Ufone 0333 408 2387
Telenor , 0345 766 5872
Email support@shetechnologies.com

Accounts Department:

For any financial, contract, invoice or Ledgers

PTCL 042 3740 2480
Ufone 0336 486 1154
Email accounts@shetechnologies.com
WhatsApp 0336 486 1154

General Inquires:

For any General Information

Ufone 0333 0444 777
Warid 0321 9999 444 , 0321 8166 876
Email info@shetechnologies.com
WhatsApp 0333 0444 777

*** End of Document ***