

JiJi Password Reset Suite User Manual

JiJi Technologies

JiJi Password Reset Suite User Manual

JiJi Technologies

Table of Contents

1. OVERVIEW	1
Self Service	1
Help Desk	1
2. SYSTEM REQUIREMENTS	2
Windows Service	2
Web Client	2
3. INSTALLATION	3
Quick setup	3
Advanced setup	14
Installing windows service	14
Installing Web Client	18
4. FEATURES	23
Main Features	23
Additional Features	23
5. WORKING WITH ADMIN WEB	24
Home	24
User Status Statistics	24
AUDITS	24
Admin	25
Enable/Disable Feature	26
Language Settings	26
Notification Settings	27
Invite Users	28
Search User Settings	31
Agent Installation	32
Auto Unenroll Users	33
Mail Server Settings	35
Exclude AD Objects from Reports	35
Pass Through Authentication	36
SELF SERVICE POLICY SETTINGS	37
Creating and Deleting Policies	37
Ranking Policies	38
Export and Import	38
Enrollment Questions	38
Enrollment Settings	40
Security Settings	41
Password Reset Settings	41
Unlock Settings	42
Applies to Settings	43
Auto Enroll Users	43
Mobile Code Verification	45
Self-Update Policy	46
Help Desk	47
Help Desk Creation	47
Help Desk Settings	48
Reports	49
View Reports	49
Schedule reports	50
Add schedule	50
View Schedule	53
6. WORKING WITH SELF SERVICE WEB	54
USER DETAILS	54
ENROLLMENT	55
CHANGE PASSWORD	56
RESET PASSWORD	57

Reset Password using Mobile Code Verification	59
Unlock Account	60
7. WORKING WITH HELP DESK WEB	63
Reset Password	63
UNLOCK ACCOUNT	64
8. LICENSE REGISTRATION	66

List of Figures

1.1. JPRS setup	3
1.2. JPRS setup (a)	4
1.3.	4
1.4.	5
1.5.	6
1.6.	6
1.7.	7
1.8.	7
1.9.	8
1.10.	9
1.11.	10
1.12.	11
1.13.	12
1.14.	12
1.15.	13
1.16.	13
1.17.	14
1.18.	14
1.19.	15
1.20.	15
1.21.	16
1.22.	16
1.23.	17
1.24.	17
1.25.	18
1.26.	18
1.27.	19
1.28.	20
1.29.	20
1.30.	21
1.31.	21
1.32.	22
1.33.	22
1.34.	24
1.35.	25
1.36.	25
1.37.	26
1.38.	27
1.39.	28
1.40.	28
1.41.	29
1.42.	29
1.43.	30
1.44.	30
1.45.	31
1.46.	31
1.47.	32
1.48.	32
1.49.	33
1.50.	33
1.51.	34
1.52.	34
1.53.	35
1.54.	35
1.55.	36

1.56.	36
1.57.	37
1.58.	38
1.59.	39
1.60.	39
1.61.	40
1.62.	40
1.63.	41
1.64.	42
1.65.	43
1.66.	43
1.67.	44
1.68.	44
1.69.	45
1.70.	45
1.71.	46
1.72.	46
1.73.	47
1.74.	48
1.75.	49
1.76.	49
1.77.	50
1.78.	51
1.79.	52
1.80.	52
1.81.	53
1.82.	54
1.83.	55
1.84.	55
1.85.	56
1.86.	56
1.87.	57
1.88.	57
1.89.	58
1.90.	58
1.91.	59
1.92.	59
1.93.	60
1.94.	60
1.95.	61
1.96.	61
1.97.	62
1.98.	63
1.99.	64
1.100.	64
1.101.	65
1.102.	65

Chapter 1. OVERVIEW

JiJi Password Reset Suit is a web based password management system. JPRS is a compact pack which assists both self service and help desk management. Administrators can easily manage user passwords by delegating authority to help desk team or they can allow users to take care of their own password problems.

Self Service

Using Self Service Password Reset, Administrator can set some security policies to users with which the end user can reset their own Active Directory password securely without any kind of assistance from technical professionals. It reduces the number of password related Help Desk calls.

Help Desk

Administrators can create a group of users(Help Desk) with permissions to reset the password of end user. Dedicated help desk team will take care of password issues and reduce the security threats.

Chapter 2. SYSTEM REQUIREMENTS

Windows Service

- Dot Net Framework 3.5.
- Windows Active Directory Domain setup or machine should have added in active directory domain.

Web Client

- Dot Net Framework 3.5 with SP1.
- IIS 4.0 or higher with ASP.Net version 2.0.50727 enabled.

Chapter 3. INSTALLATION

There are two modes to install JiJi Password Reset Suit

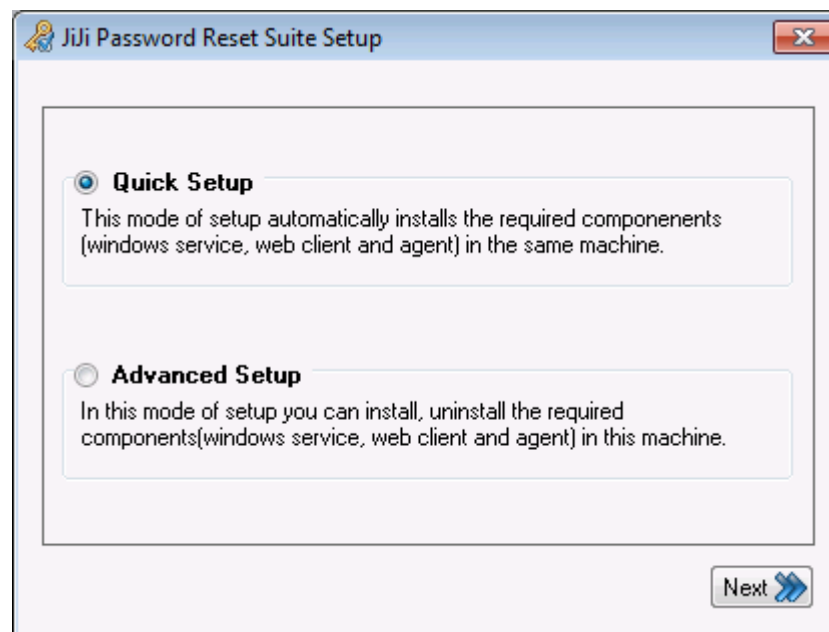
- Quick Setup
- Advanced Setup

Quick setup

In this mode, Web Client installation starts automatically after the completion of Windows Service installation. Follow the below given steps to install JiJi Password Reset Suit in quick setup mode.

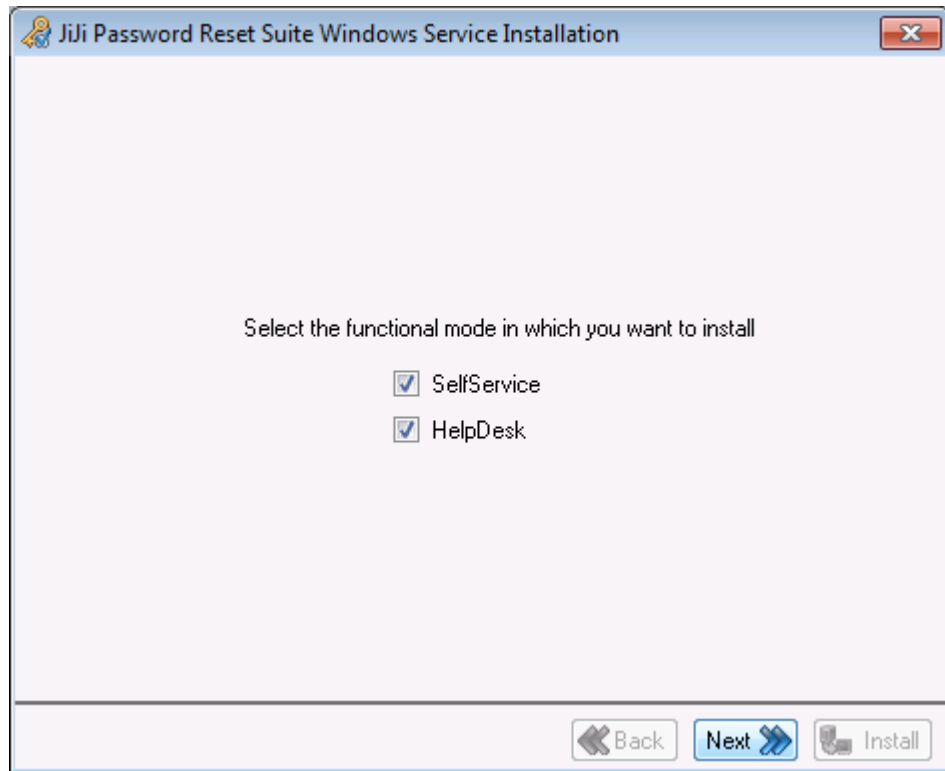
- Double click on the **JPRS setup**, a window will be opened. Click on '**Quick Setup**' and then click '**Next**'.

Figure 1.1. JPRS setup



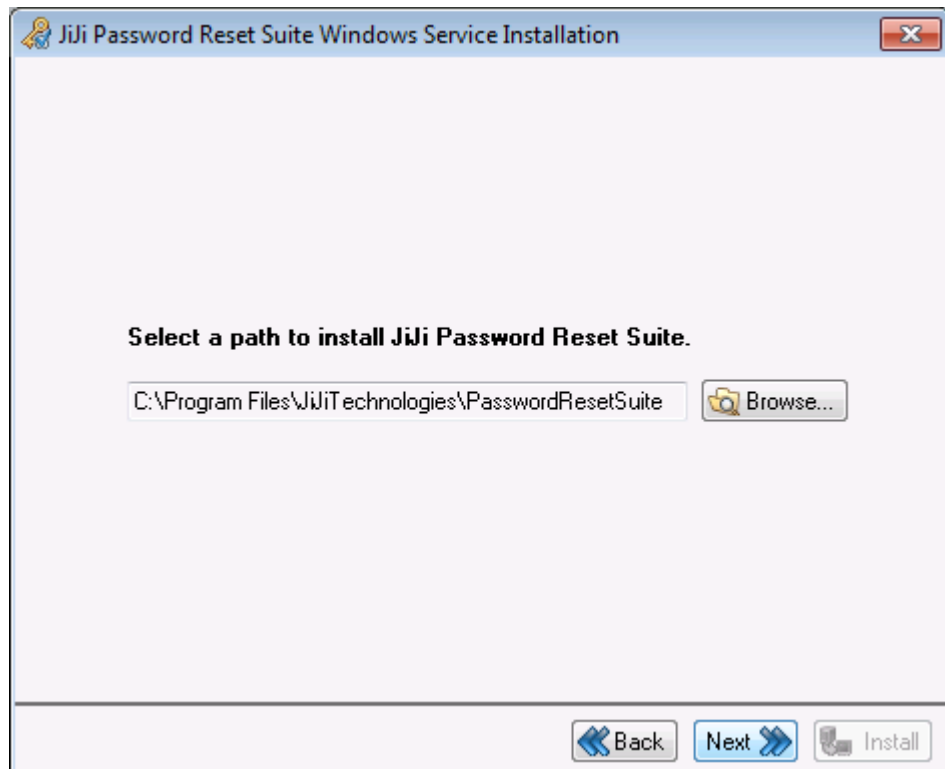
- You can install **Self Service** or **Help Desk** or **both**. Select as per your need and click '**Next**'.

Figure 1.2. JPRS setup (a)



- Browse the installation path.

Figure 1.3.

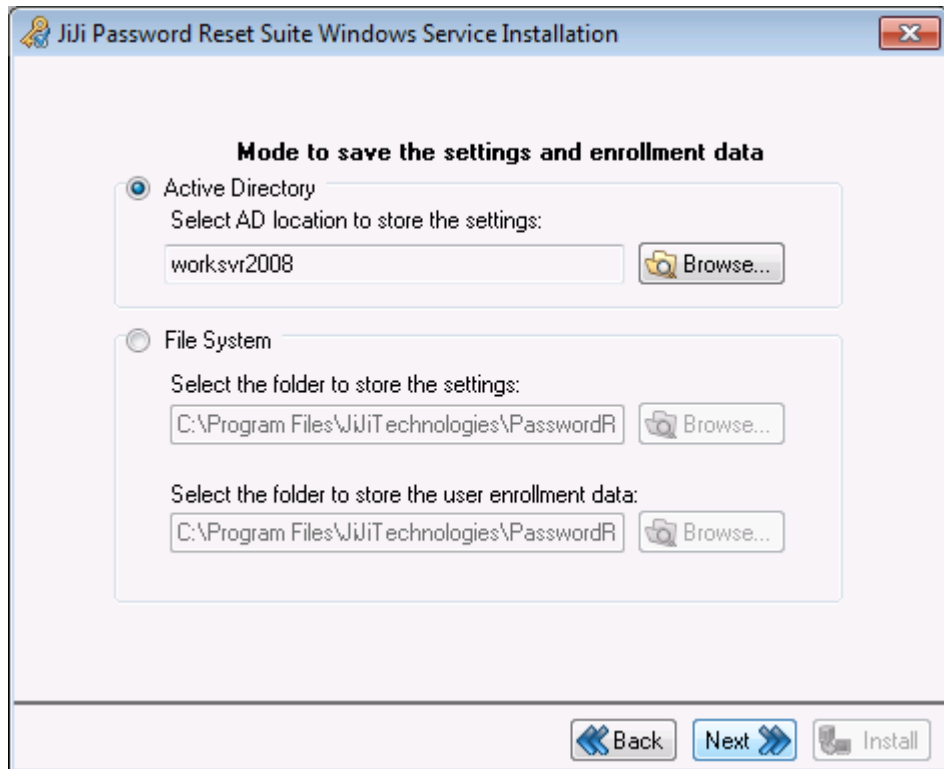


- Select the scope which has to be managed by Jiji Password Reset Suit.

Figure 1.4.

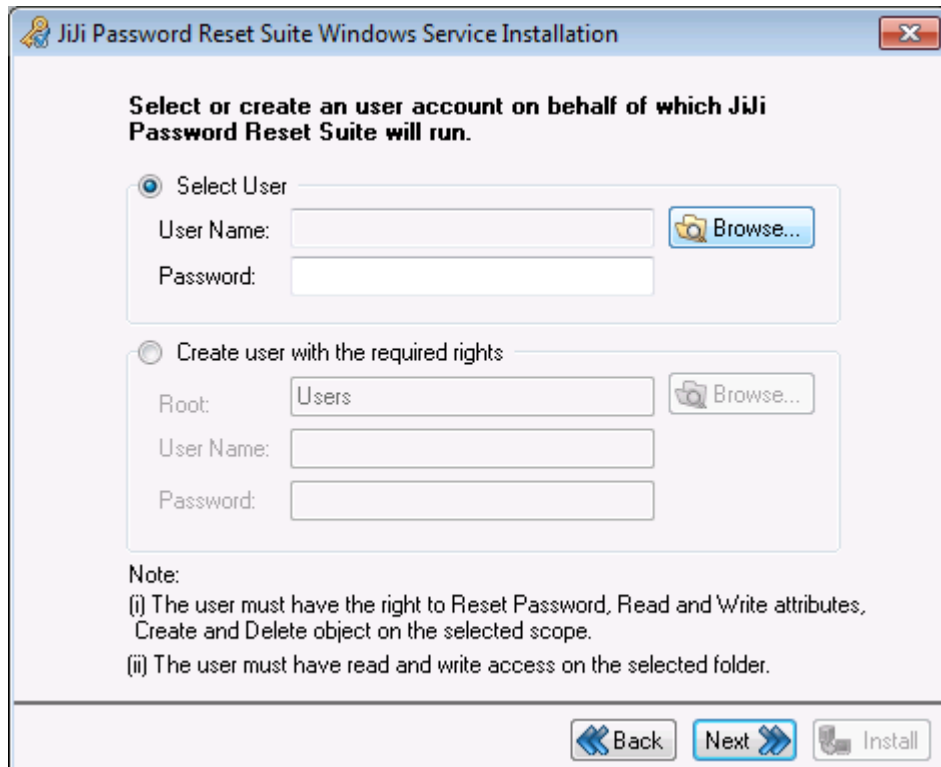
- Now select the mode to save the settings and enrollment data and click 'Next'.
- If you select Active Directory, then these datas will be stored in it.
- If you select File System, datas will be saved in folder in selected location in your computer.

Figure 1.5.



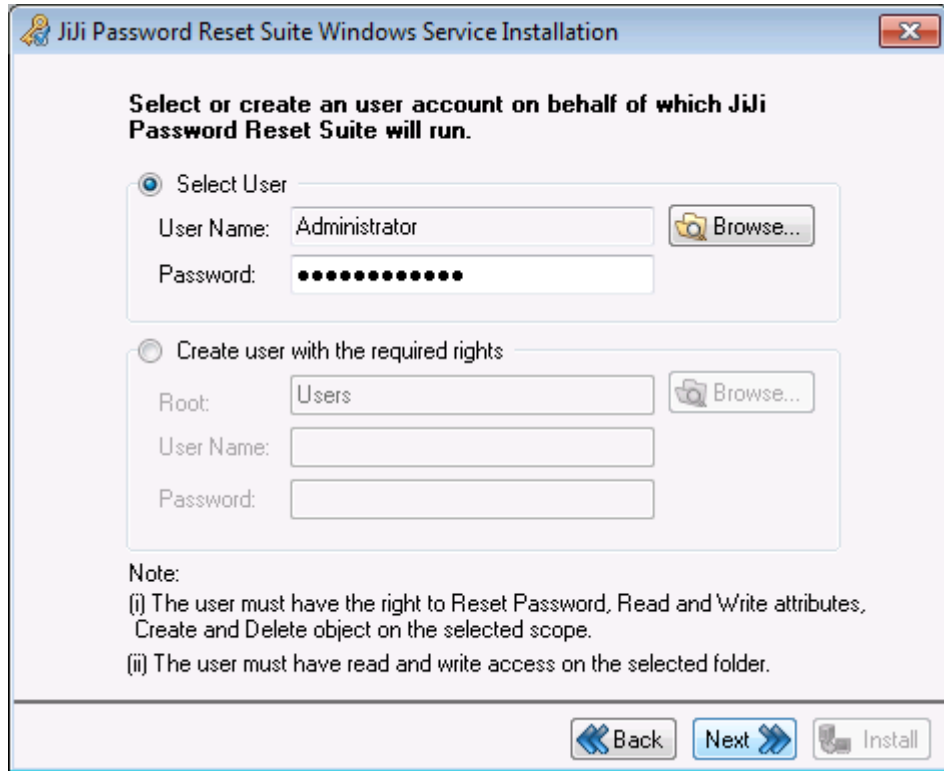
- Now you have to select or create an user, who must have the right to use this reset tool.
- Click 'Select User' and browse the already existing user.

Figure 1.6.



- A window will be opened. Use it to select the authorised user. User will be added as shown below.

Figure 1.7.



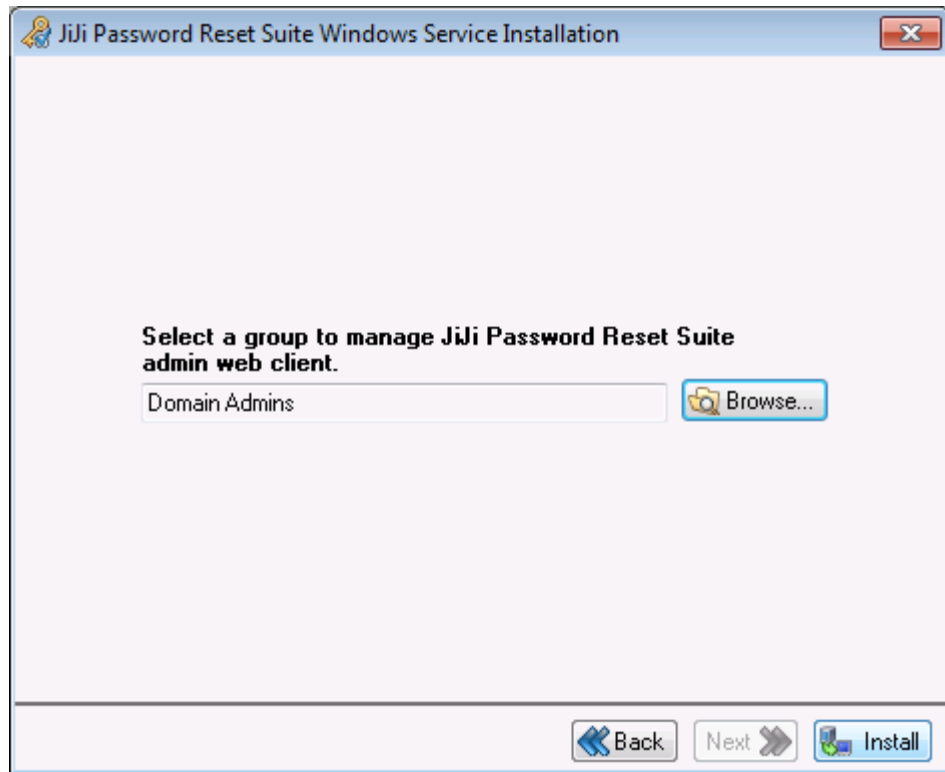
- To create new user you have to click '**Create user with Required rights**'. Select the root in which the particular user has to be added and then type the **user name** and **password**.

Figure 1.8.



- So in the previous step you have selected or created an user to manage user accounts and passwords. In this step you can select a particular **admin group** to manage **Admin Web Client**.

Figure 1.9.



- Now you can select '**Virtual Directory**' or '**Website**' to launch the Web Client.

Figure 1.10.

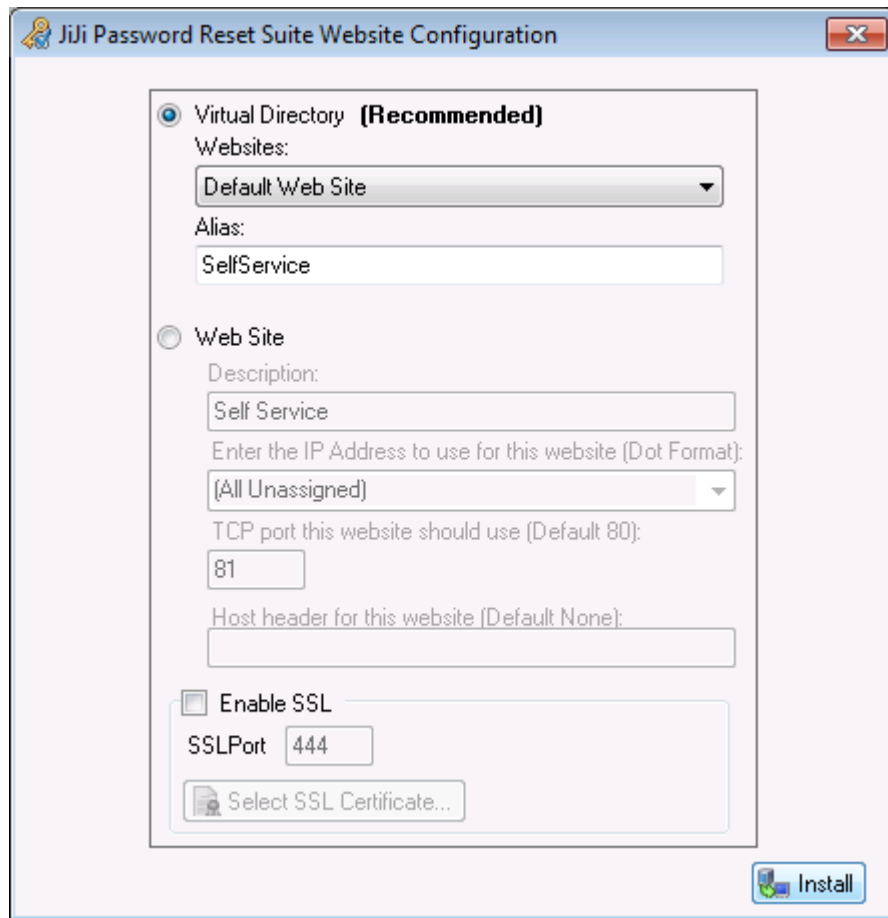
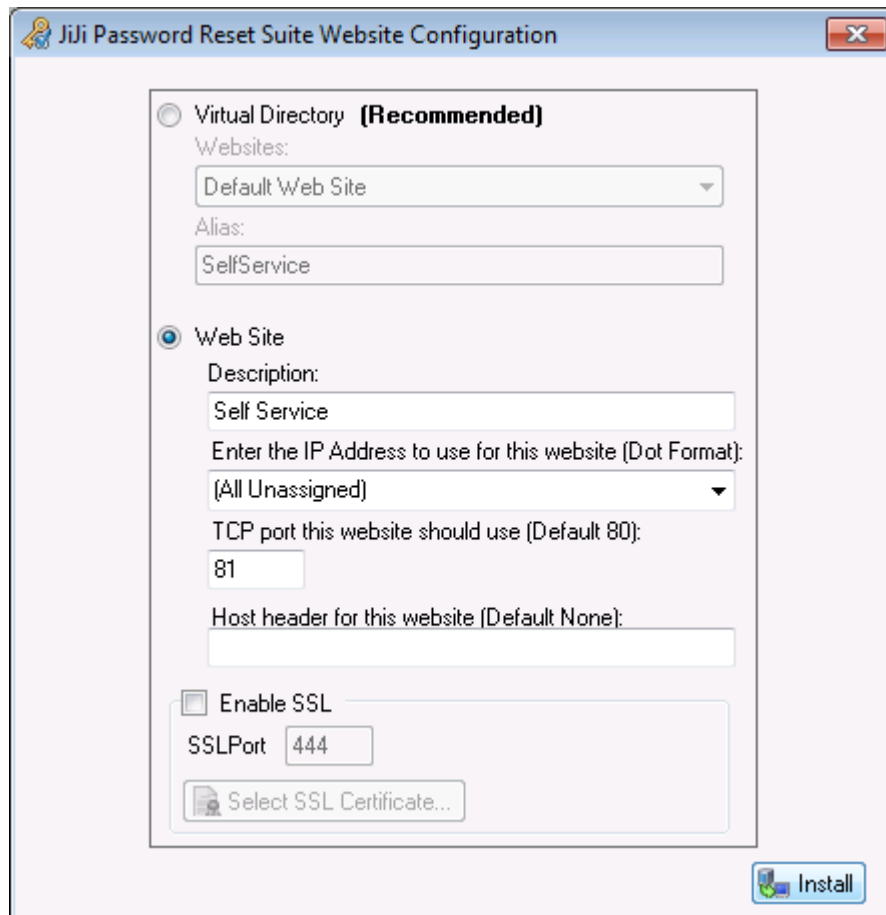
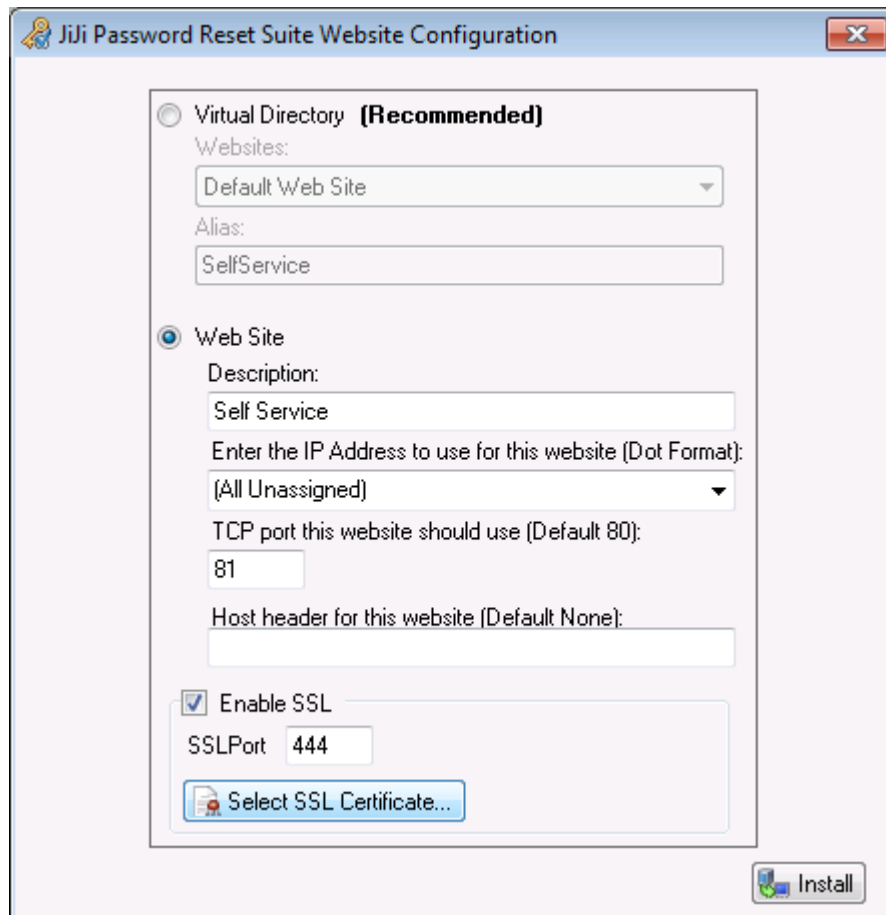


Figure 1.11.



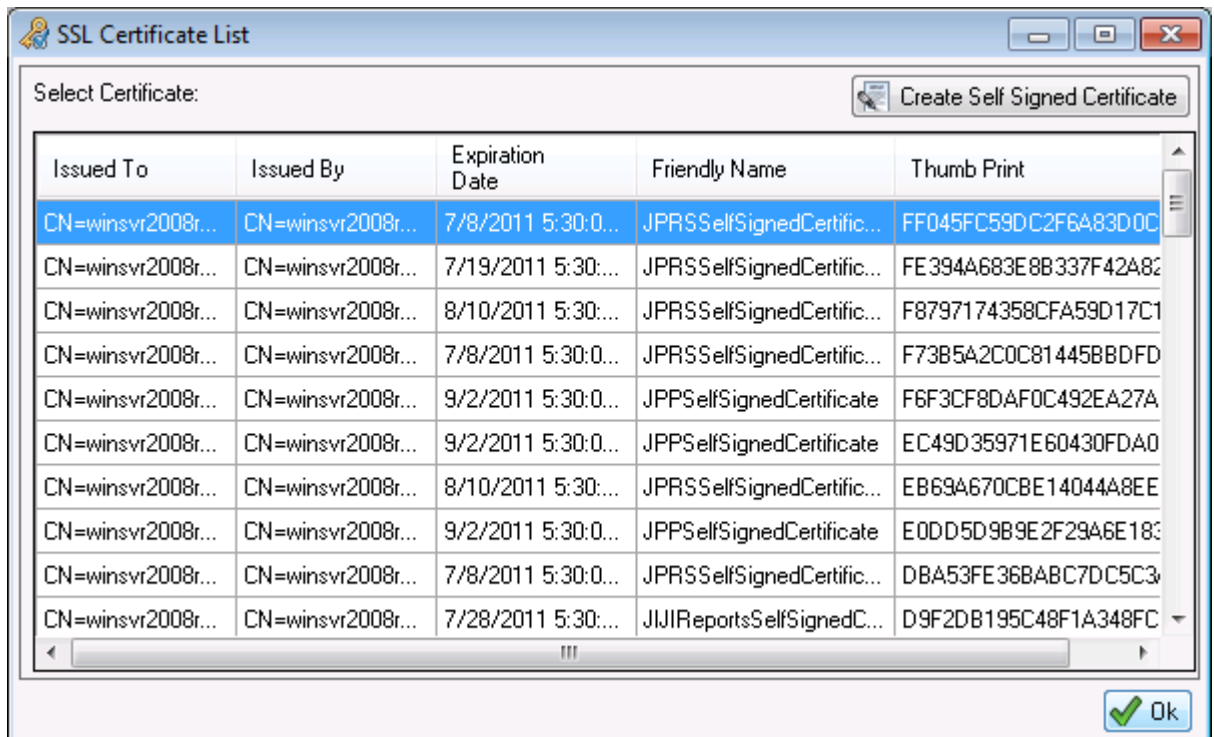
- You can enable SSL(Secure Socket Layer) to conduct secure operations on your website.
- Check the **'Enable SSL'** check box and give the valid **SSL port** number.

Figure 1.12.



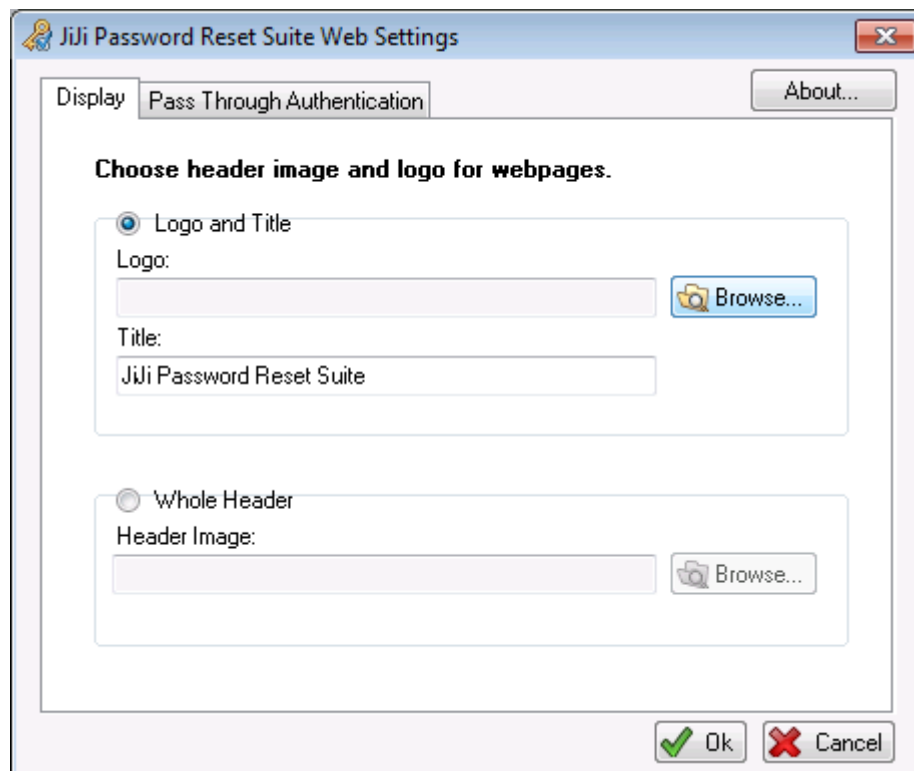
- Click on 'Select SSL Certificate button'. A window will be opened as shown below.
- You can either select the already existing certificate or create new by clicking '**Create Self Signed Certificate**'. Select it and click '**Ok**'.

Figure 1.13.



- Now **Web Settings** window will be opened. Select **Logo, Header image** and type the **Title** for your webpages.

Figure 1.14.



- Click on **Pass Through Authentication** tab. If you need to enable windows mode of authentication, check the check box and click 'Ok'.

Figure 1.15.




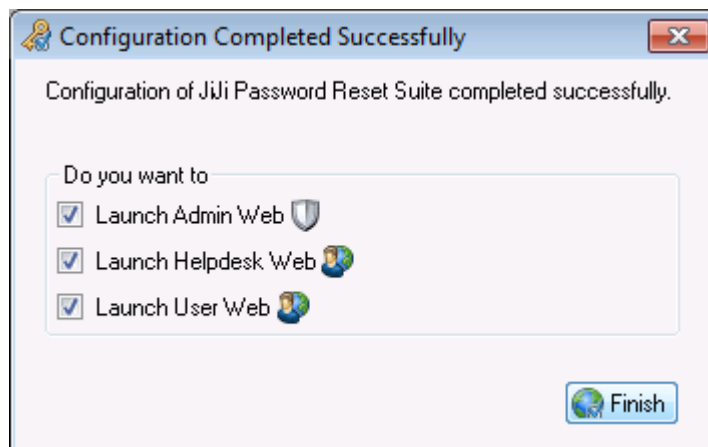
-  **Note**
To enable **windows mode of authentication**, follow the steps given in the **Pass through Authentication** tab.
- Finally a window will be opened, which asks whether to launch Admin, Helpdesk, User Web or not. Select any of the needed web and click '**Finish**'.

Figure 1.16.



Advanced setup

In this mode you can select **Windows Service** or **Web Client** to install or uninstall as per your need. You can also install **Logon client** which is used to reset password from the logon screen.

Installing windows service

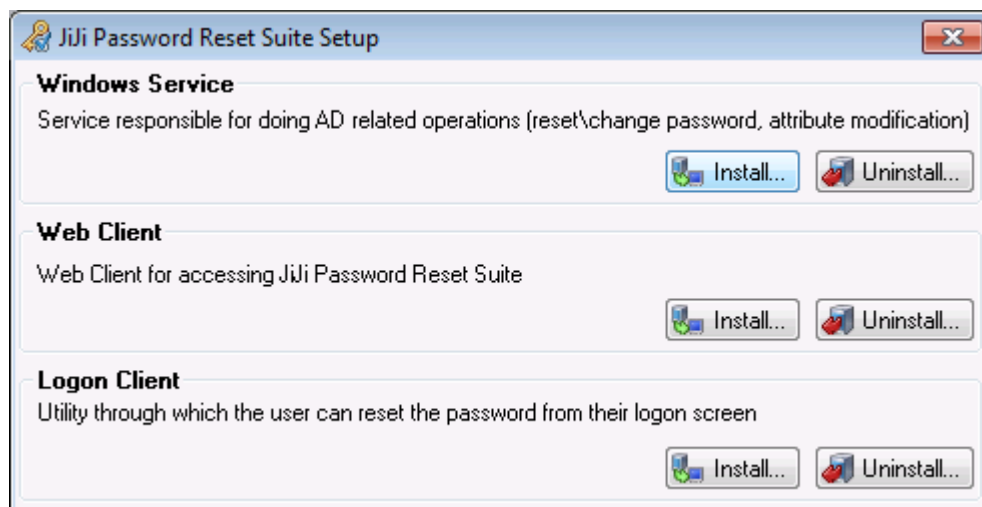
- Select '**Advanced Setup**' and click 'Next'.

Figure 1.17.



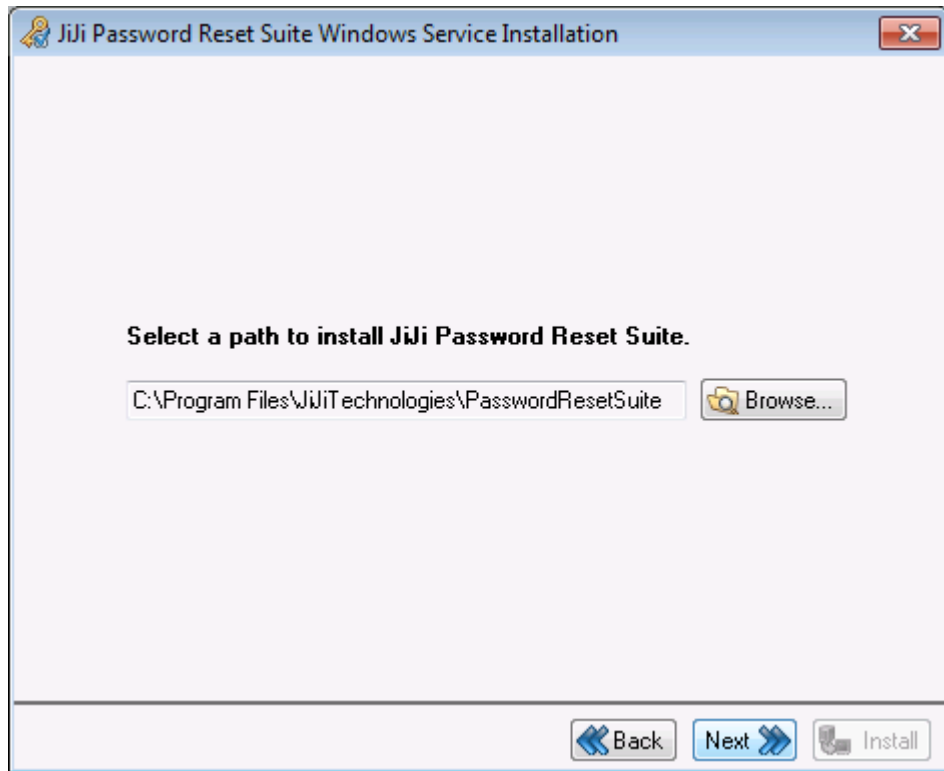
- Click '**Install**' button of Windows Service.

Figure 1.18.



- Then select a path to install.

Figure 1.19.



- Select the scope which has to be managed by JPRS.

Figure 1.20.



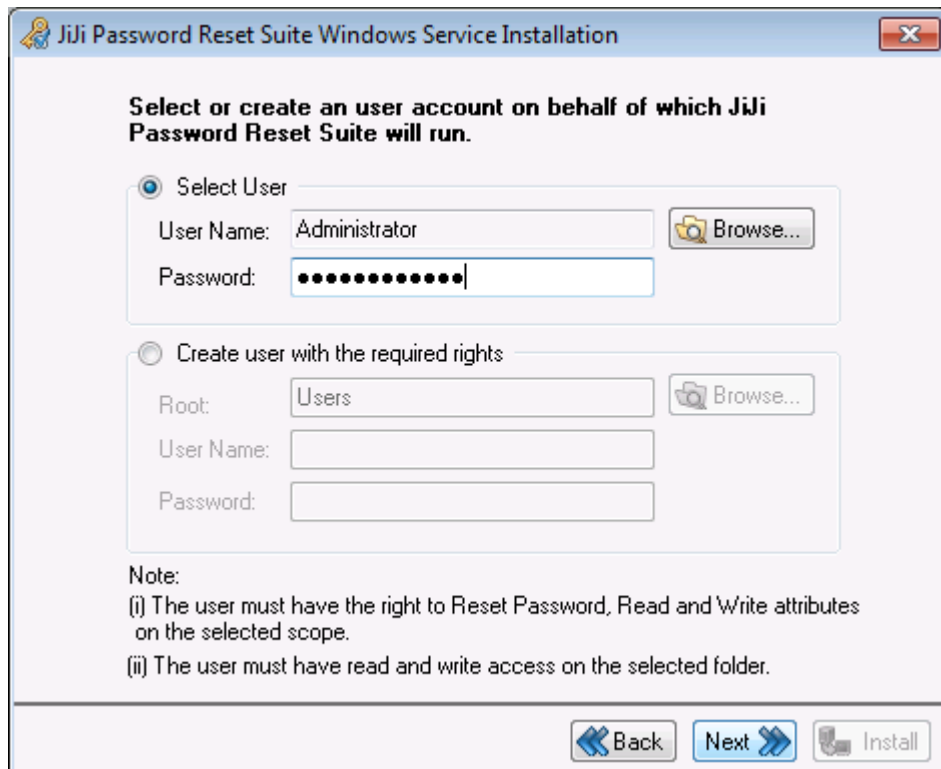
- Select **Active Directory** or **File System** to save the settings and enrollment datas.

Figure 1.21.



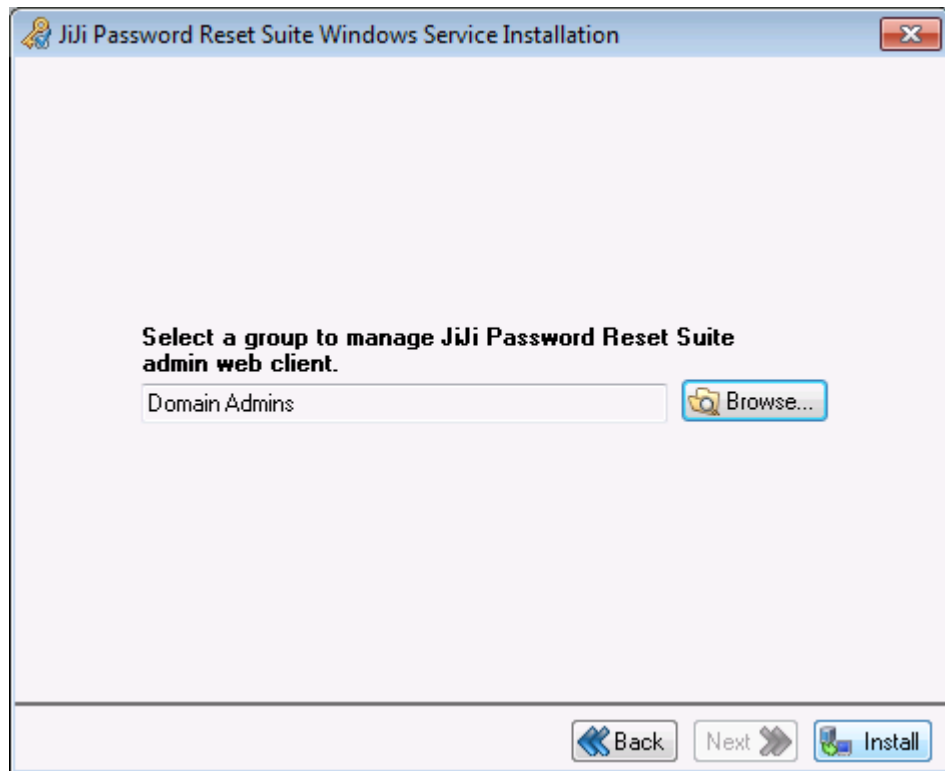
- Select or create authorised user who must have the right to reset passwords and unlock accounts.

Figure 1.22.



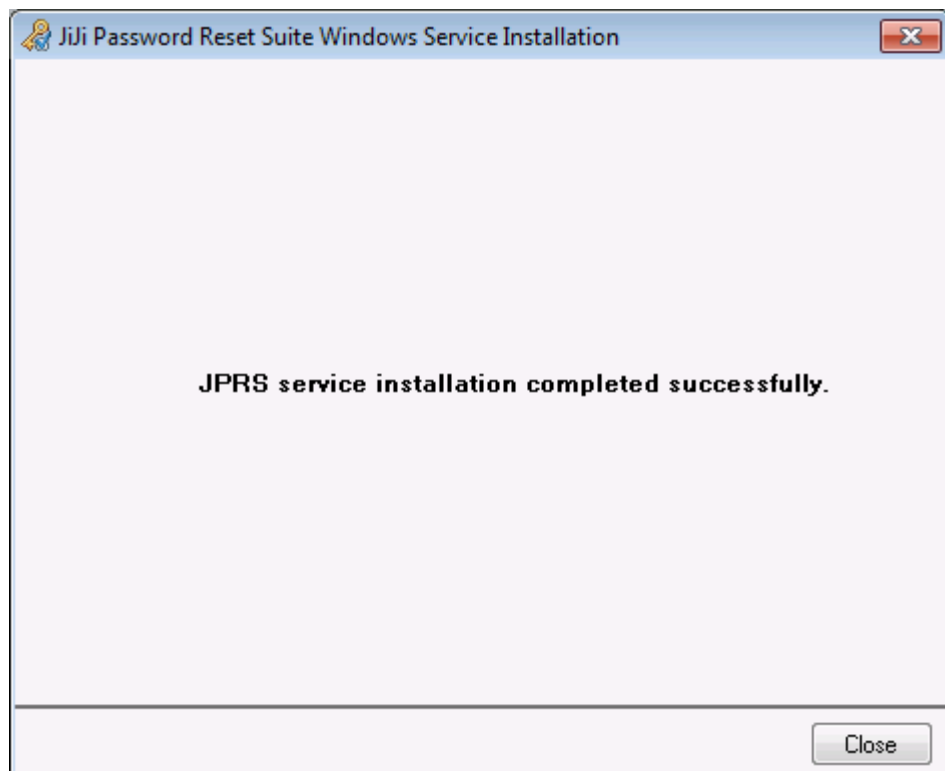
- Select a group to manage **Admin Web Client**.

Figure 1.23.



- Now **Windows Service** installation is completed successfully.

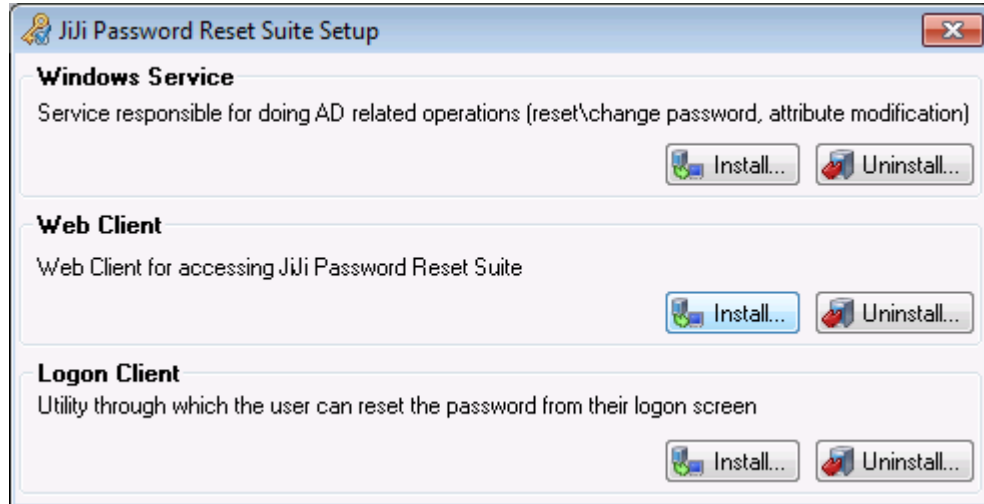
Figure 1.24.



Installing Web Client

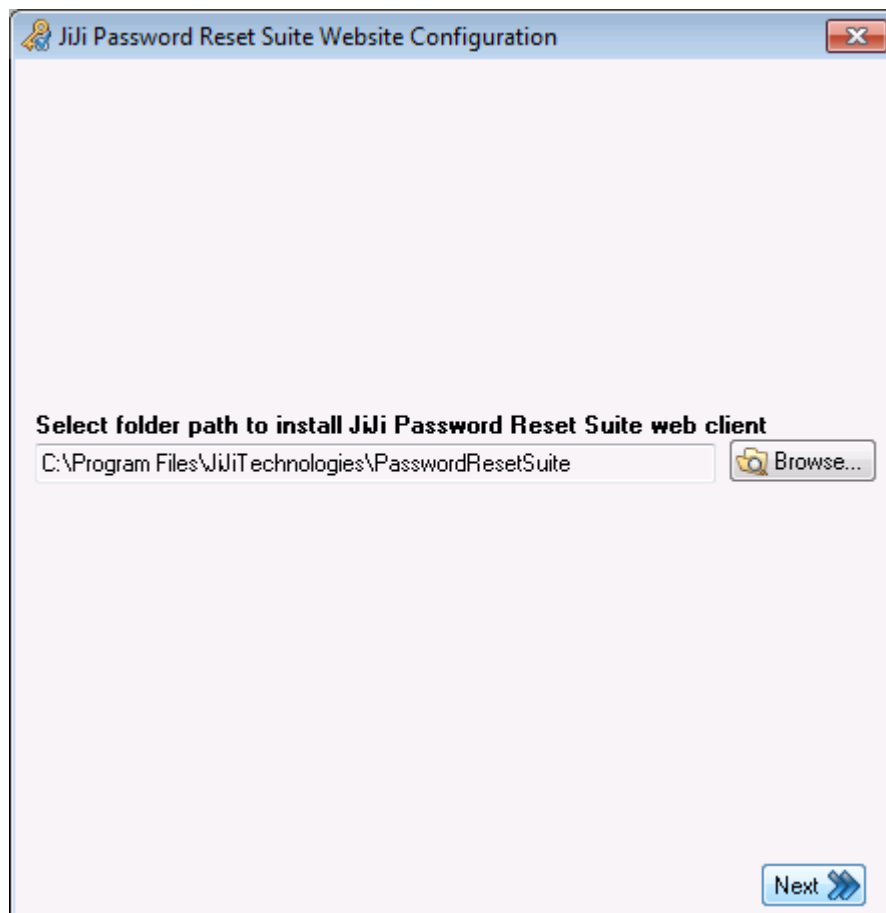
- Click **Install** button of **Web Client**.

Figure 1.25.



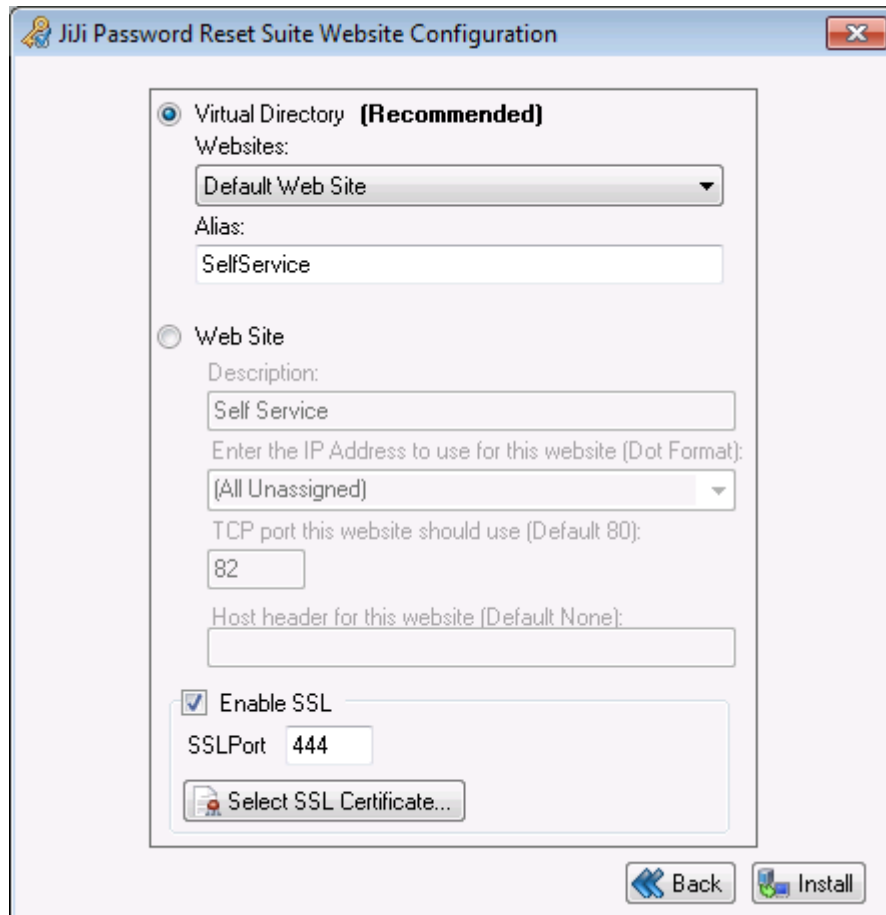
- Select the path to install and click **Next**.

Figure 1.26.



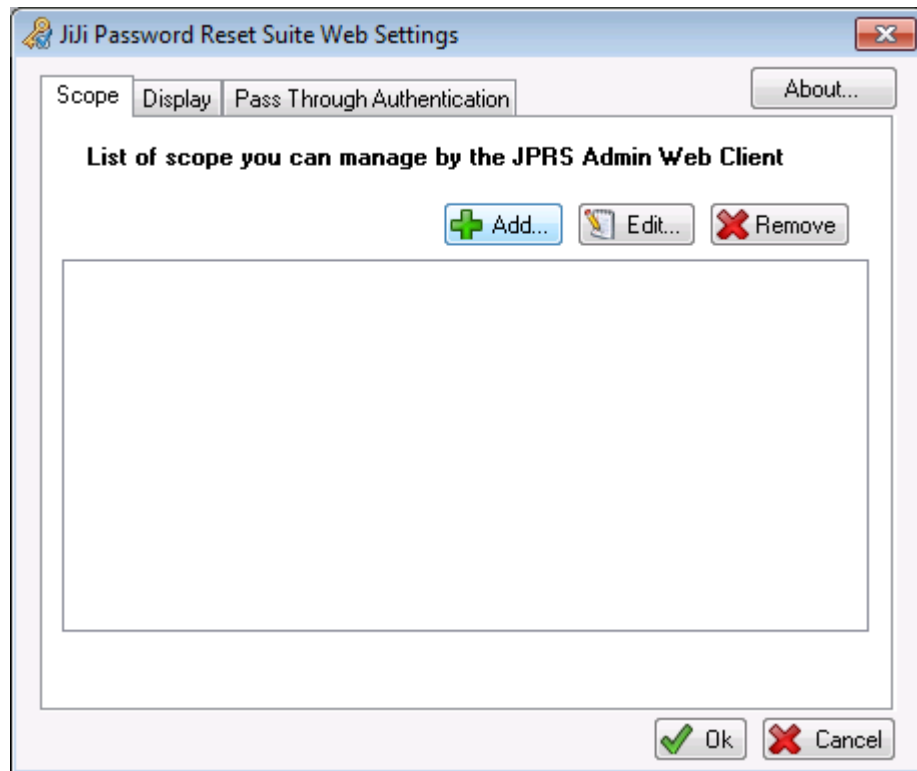
- Select **Virtual Directory** or **Website** to launch the Web Client. You can also enable **SSL certificate** to maintain security as shown in Quick setup.

Figure 1.27.



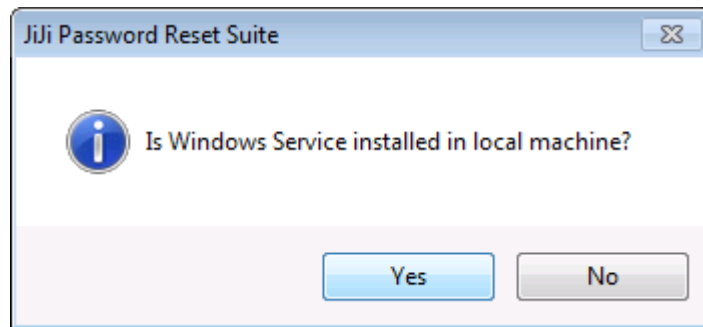
- **Display settings** and **Pass Through Authentication** are same as that seen in Windows Service.
- Now select scope which has to be managed by your Web Client by clicking 'Add' button.

Figure 1.28.



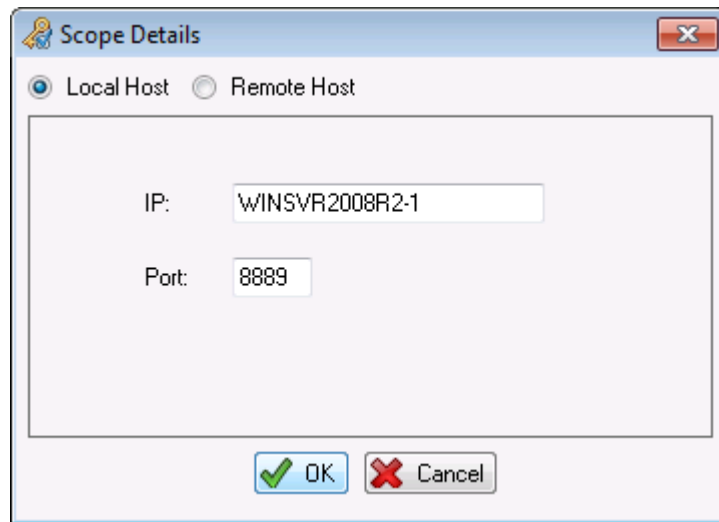
- If you install **Windows Service** in local machine click '**Yes**' otherwise click '**No**'.

Figure 1.29.



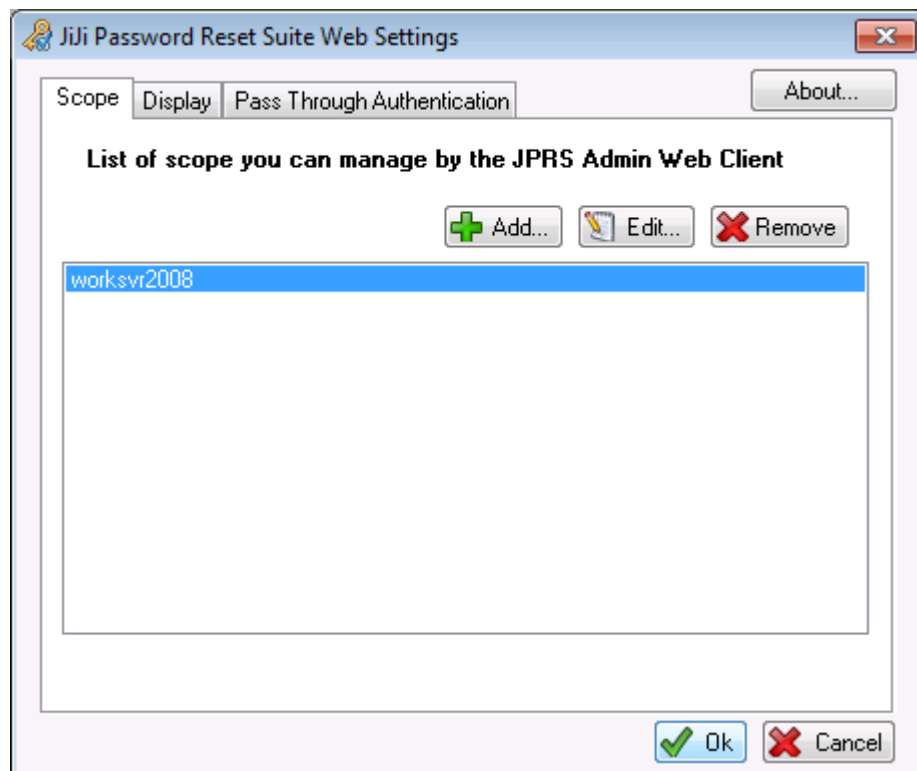
- **Scope Details** window will be opened. Enter local host IP and port number and click '**Ok**'.

Figure 1.30.



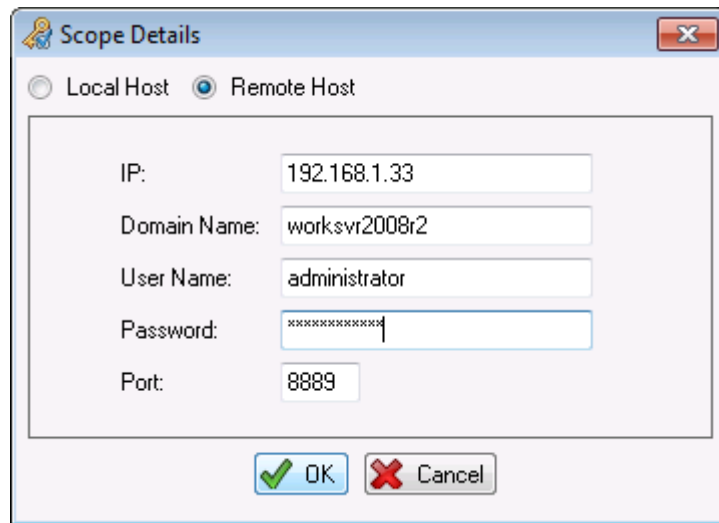
- **Scope** gets added as shown below.

Figure 1.31.



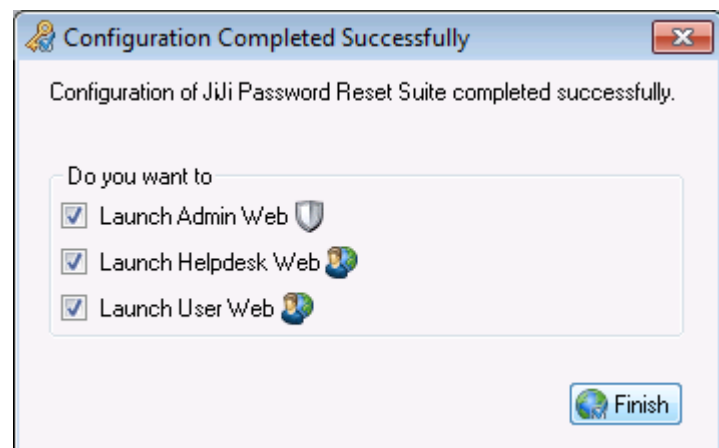
- If **Windows Service** is installed in remote machine, click '**Remote Host**' enter the details and click '**OK**' button.

Figure 1.32.



- Finally, check any of the checkbox which has to be launched and click '**Finish**'.

Figure 1.33.



Chapter 4. FEATURES

Main Features

End-users can perform following self service actions

- Self reset password
- Self change password
- Self unlock account
- Self update the Active Directory Attributes

Administrators can perform the following actions

- Configure self service policy settings for each Group/OU/Set of Users
- Configure email notifications for password soon to expire users/change password/reset password
- Can view general, Self Service, Help Desk reports.
- Can schedule reports.

Help desk can

- Reset passwords and unlock accounts of the users who request them.

Additional Features

- GINA Extension / Credential Provider.
- Two-way authentication before password reset by using Mobile Code Verification.
- Multilingual support in major European languages(French, German, Italian, Spanish and Russian).

Chapter 5. WORKING WITH ADMIN WEB

Administrator must have the full control over every password reset and change operations. They must delegate authority to the help desk using AdminWeb so that the help desk staffs can reset password to all users under the control of administrator. They can provide rights to users through Self Service settings so that every users can manage their own password problems without the help of help desk people. Both Self Service and Help Desk settings which can be made by administrators are explained below.

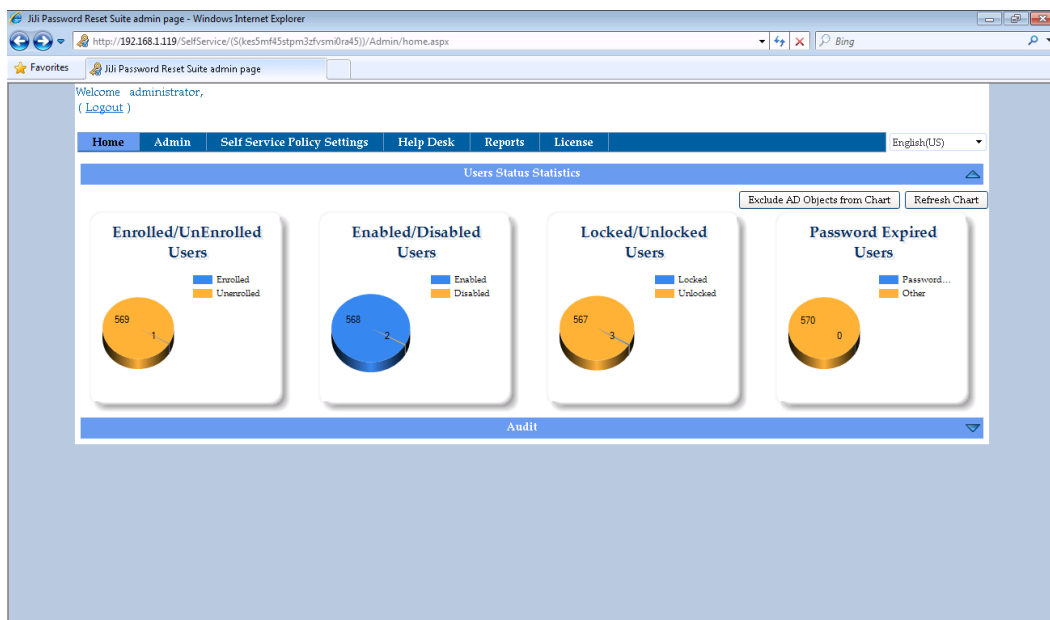
Home

Home page contains **User Statistics** and **User Audits**. You can click on the graph to view the corresponding reports.

User Status Statistics

- This is the graphical representation of Enrolled/Unenrolled, Enabled/Disabled, Locked/Unlocked, Password Expired Users.
- From this graph, you can easily find out number of users were locked, disabled and so on.
- If you do not need audits for certain AD Objects you can exclude it from the statistics chart by clicking '**Exclude AD Objects from Chart**' button.
- To view the updated report, click '**Refresh Chart**' button.

Figure 1.34.

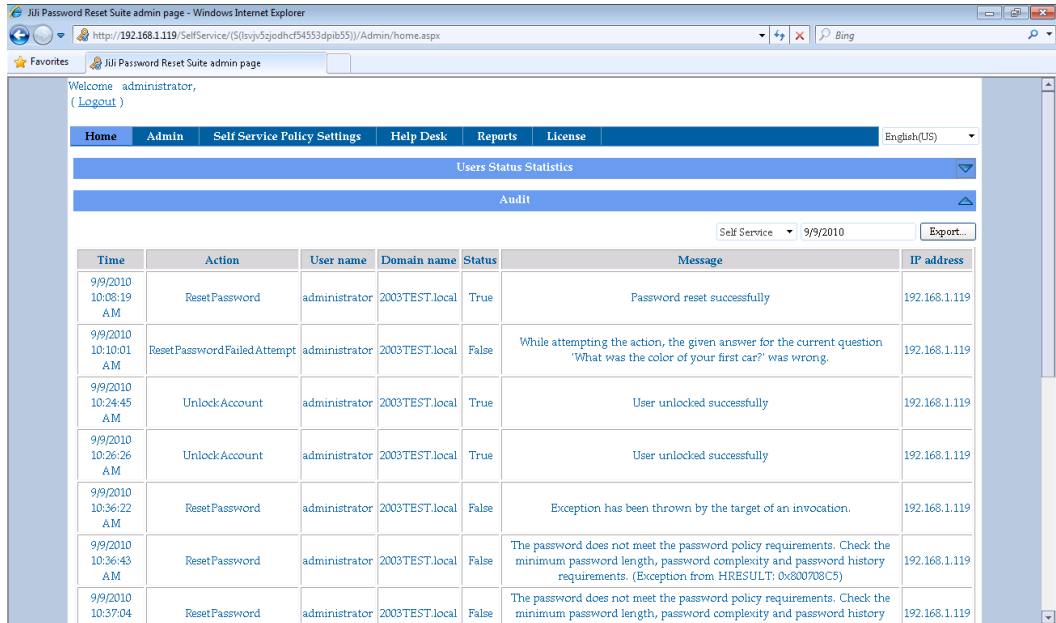


AUDITS

The changes made in passwords due to **Self Service** and **Help Desk** Password reset were displayed in Audit.

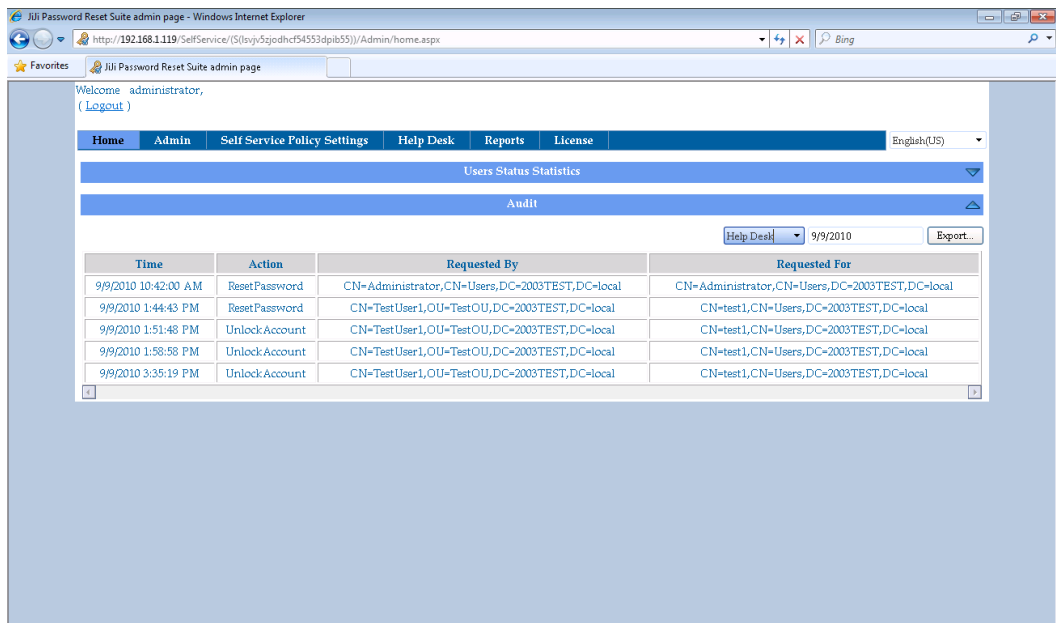
- You can view audit for the selected date.
- Generated report can be exported and stored in csv format.
- You can select **Self Service** from the combo box to view the change details related to it. Self Service audit is shown below.

Figure 1.35.



- Select **Help Desk** option from the combo box and view Help Desk audit.

Figure 1.36.



Admin

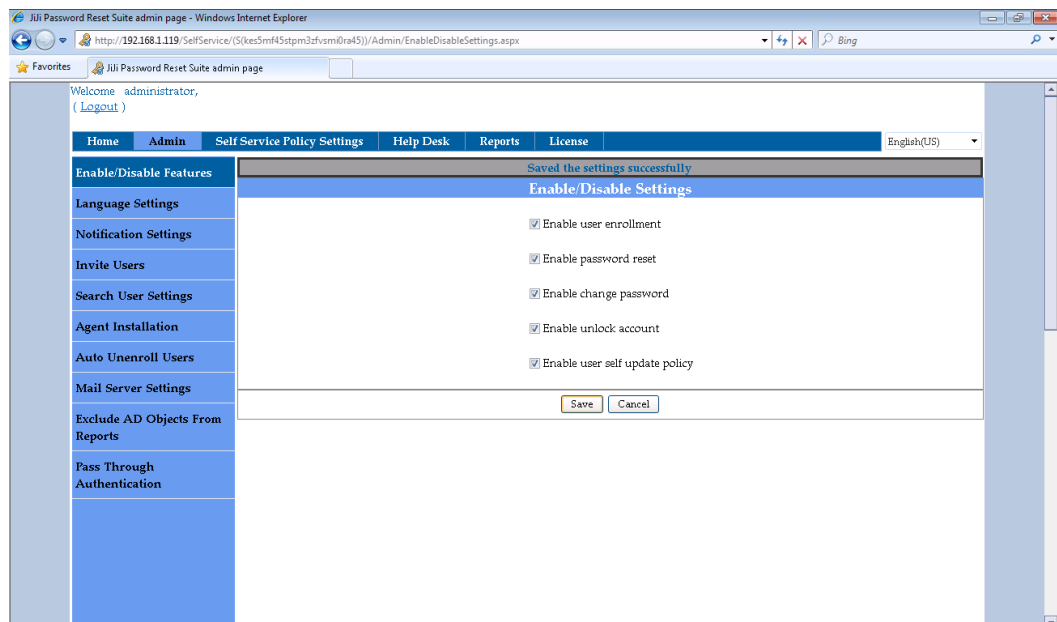
Here you can make all the general settings related to Self Service as well as Help Desk Password Reset.

Enable/Disable Feature

Administrator can disable certain features that should not be used by users. Features that can be enabled or disabled by admin are given below.

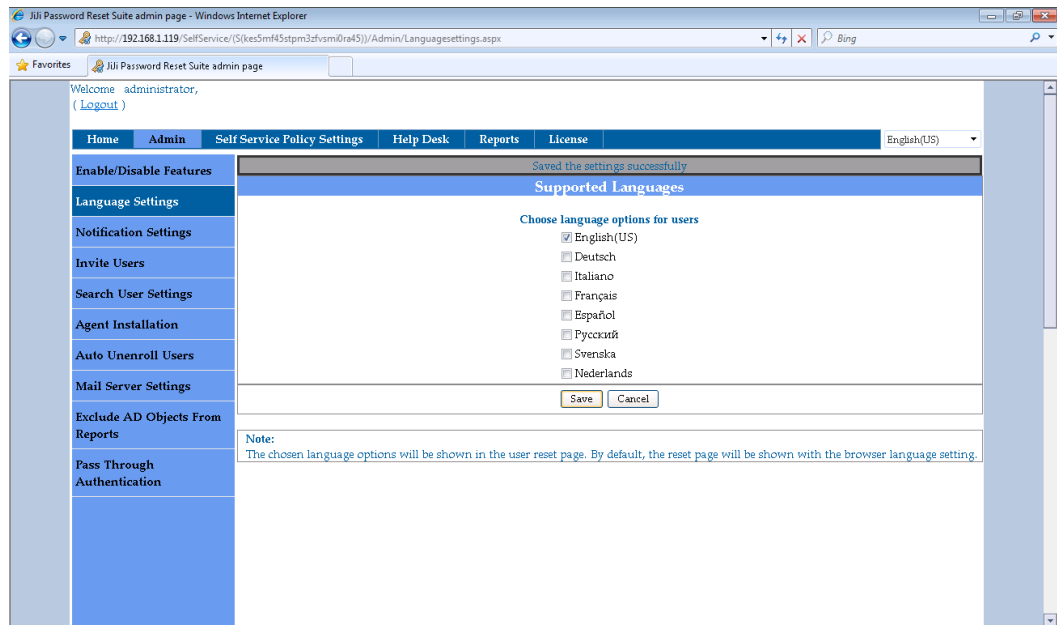
- User Enrollment
- Password Reset
- Change Password
- Unlock Account
- User Self Update Policy

Figure 1.37.



Language Settings

- You can choose the suitable language for users.

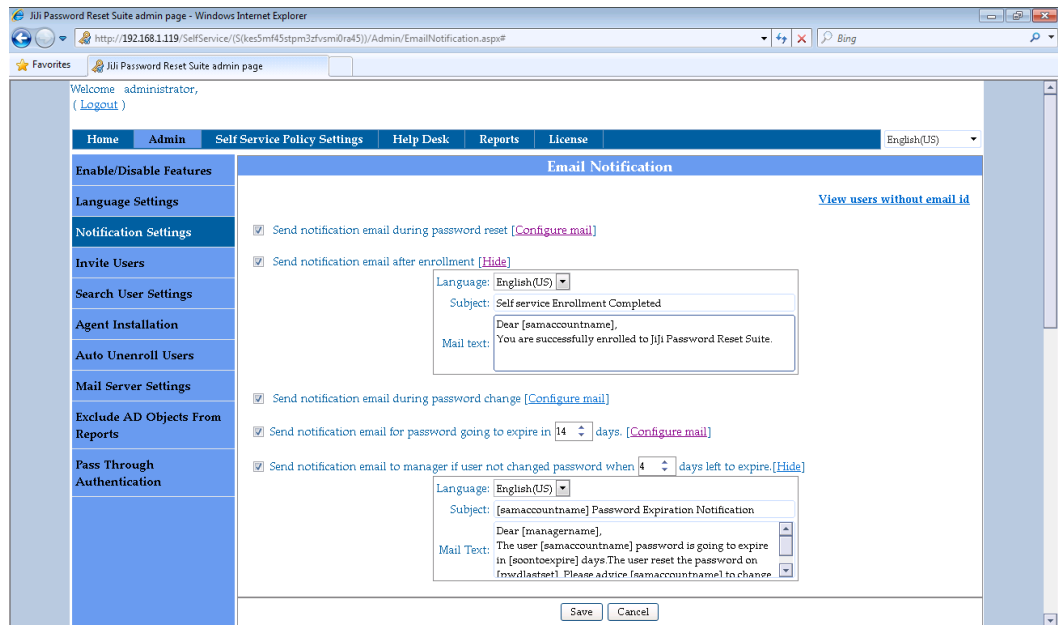
Figure 1.38.

Notification Settings

You can set the following notification settings to alert the users to reset their passwords or alert managers to advise them to reset.

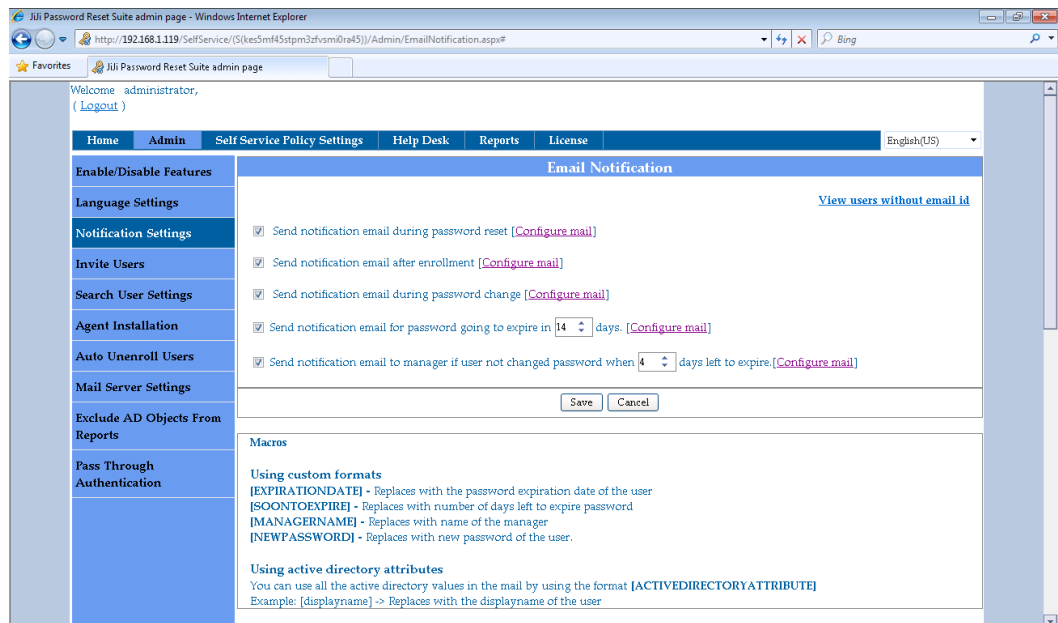
- Send notification during password reset
- Send notification email after enrollment
- Send notification during password change
- Send notification email for password going to expire in few days.
- Send notification email to manager if user not changed password when certain days left to expire.

Figure 1.39.



- You can use macros to replace the user name, manager name, password expiration date etc. As you enter the macros they get updated to the actual value automatically.
- You can also use Active Directory attributes.

Figure 1.40.



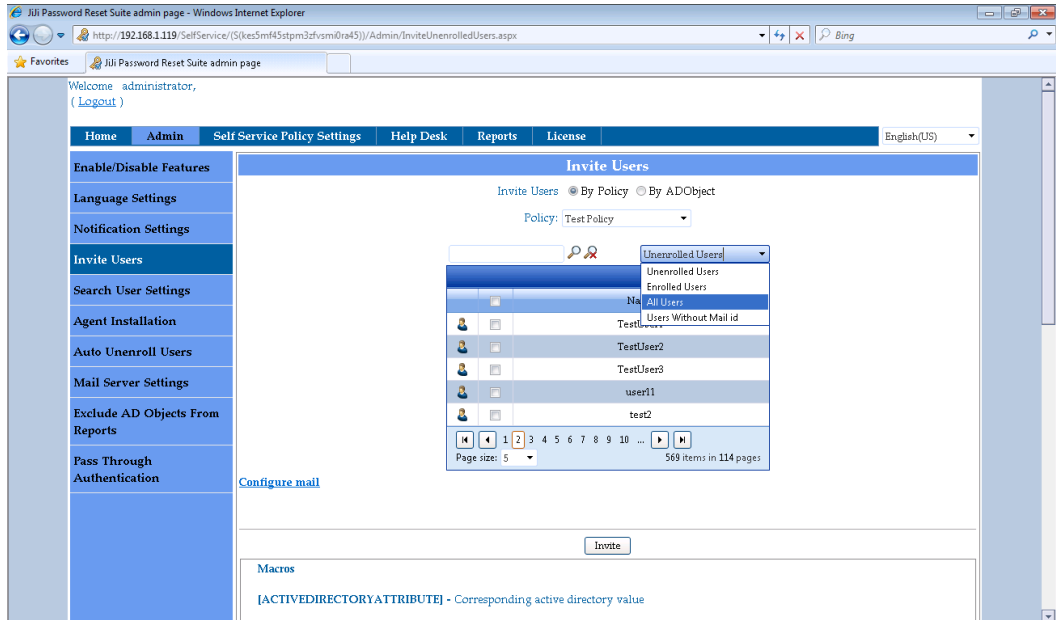
Invite Users

You can invite users under the certain policy or by Active Directory objects to enroll to Jiji Password Reset.

a) By Policy

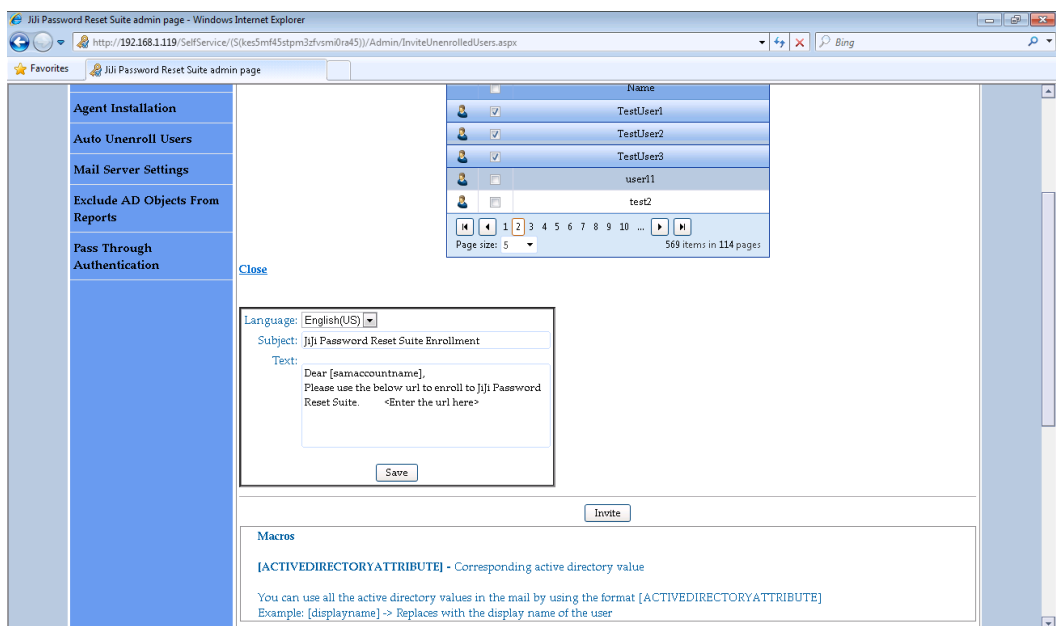
- To invite by Policy, click Invite Users **'By Policy'** then select Policy.

Figure 1.41.



- Select all users or unenrolled users or enrolled users or users without E-mail id from the combo box as shown below.
- Now users will be listed. Select the required users and click on Configure **mail** link label.
- Edit macros and enter the url which is to be used by users to enroll.

Figure 1.42.

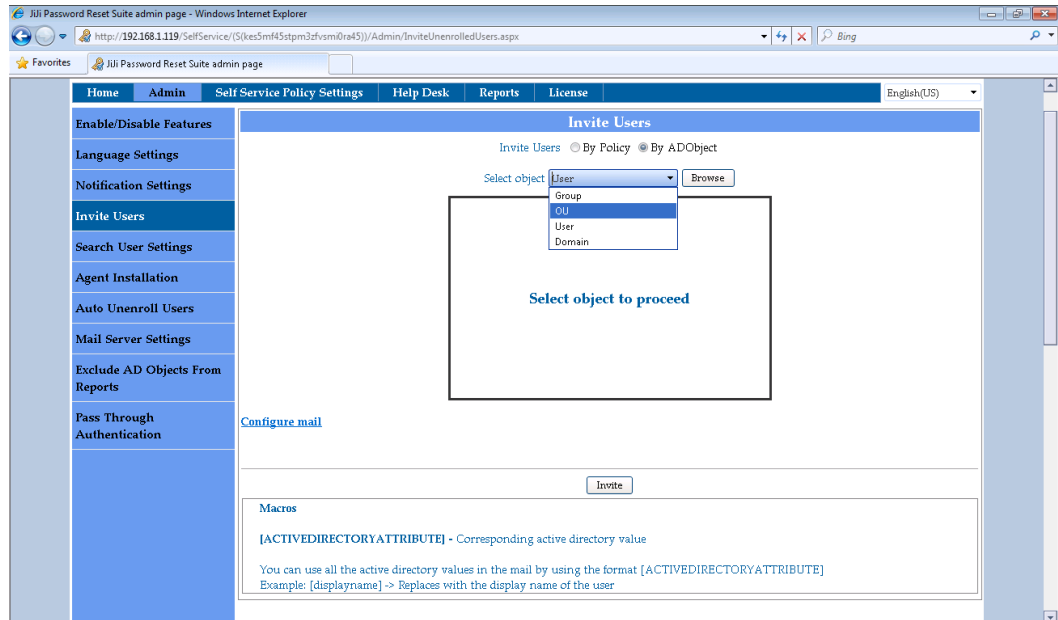


- Click Save button to save the settings and Invite button to send invite.

b) By AD Objects

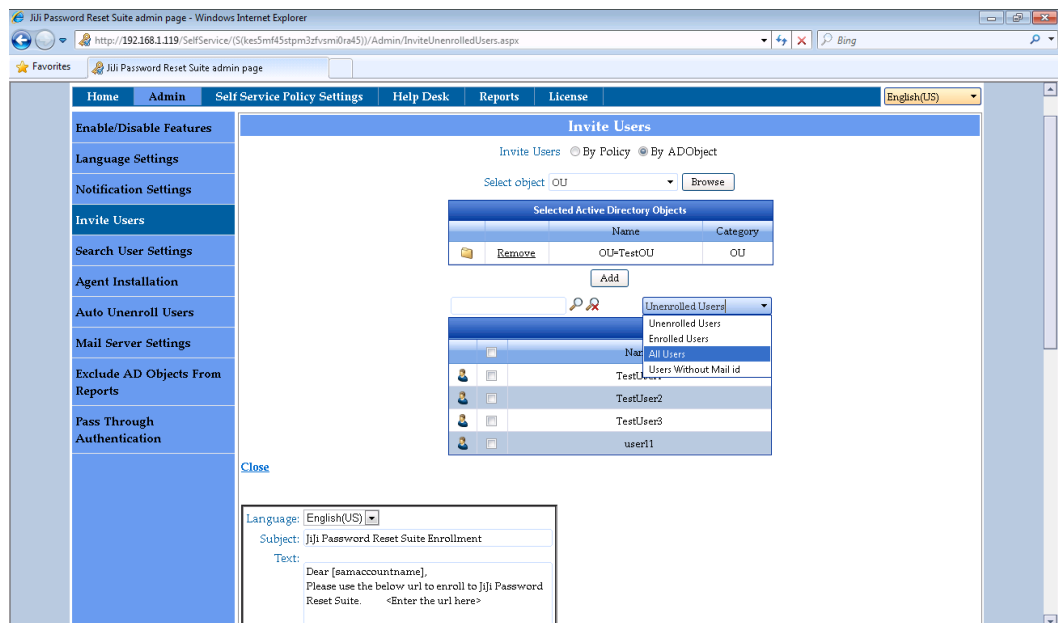
- To invite by AD Objects, Click Invite Users **'By AD Objects'**.
- Select Object such as User/Group/OU/Domain. Browse and add the object.

Figure 1.43.



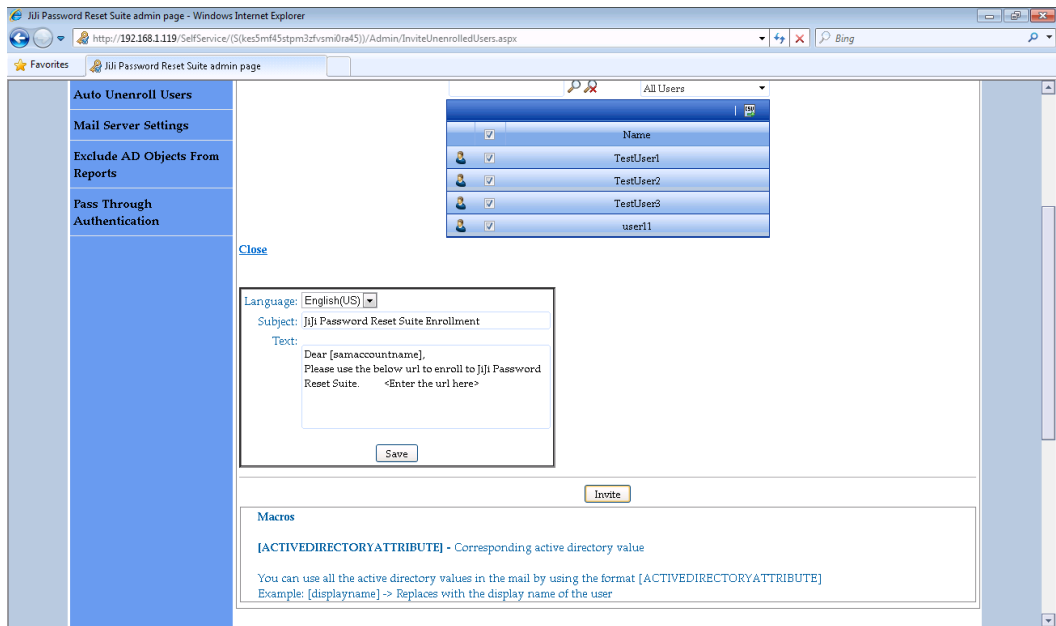
- Select all users or unenrolled users or enrolled users or users without E-mail id from the combo box.

Figure 1.44.



- Edit and save the mail configuration. Click **'Invite'** button to send invite.

Figure 1.45.

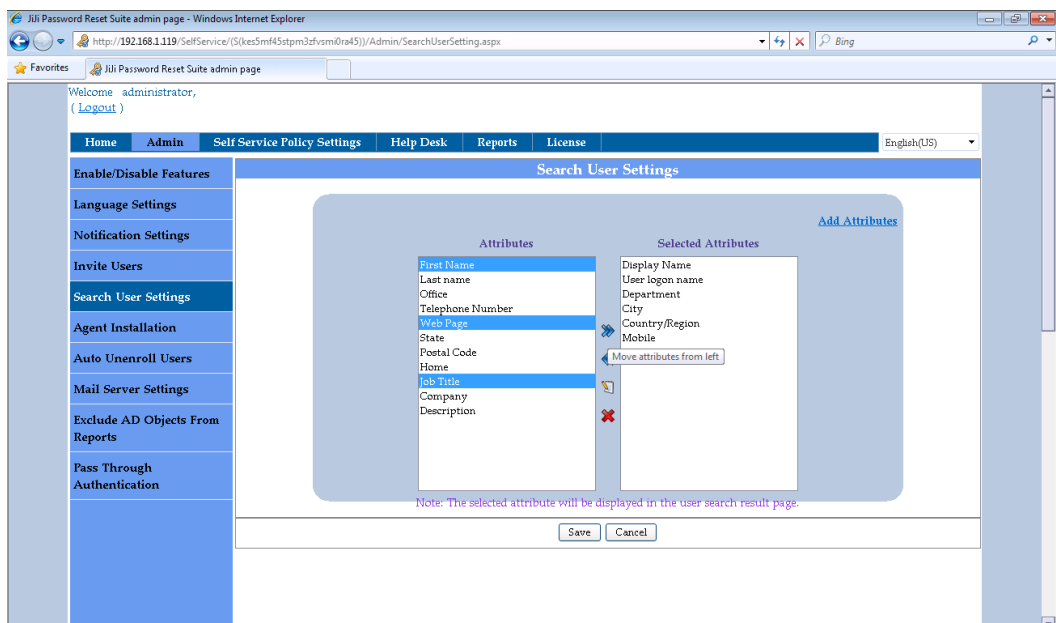


Search User Settings

These settings were used to display the selected attributes while searching users. For example, if First Name, Mobile, City were the attributes selected in Search User Settings then while searching users only those attributes of the user will be displayed.

- Select the necessary attributes.
- Shift them to the right.
- Save the settings.

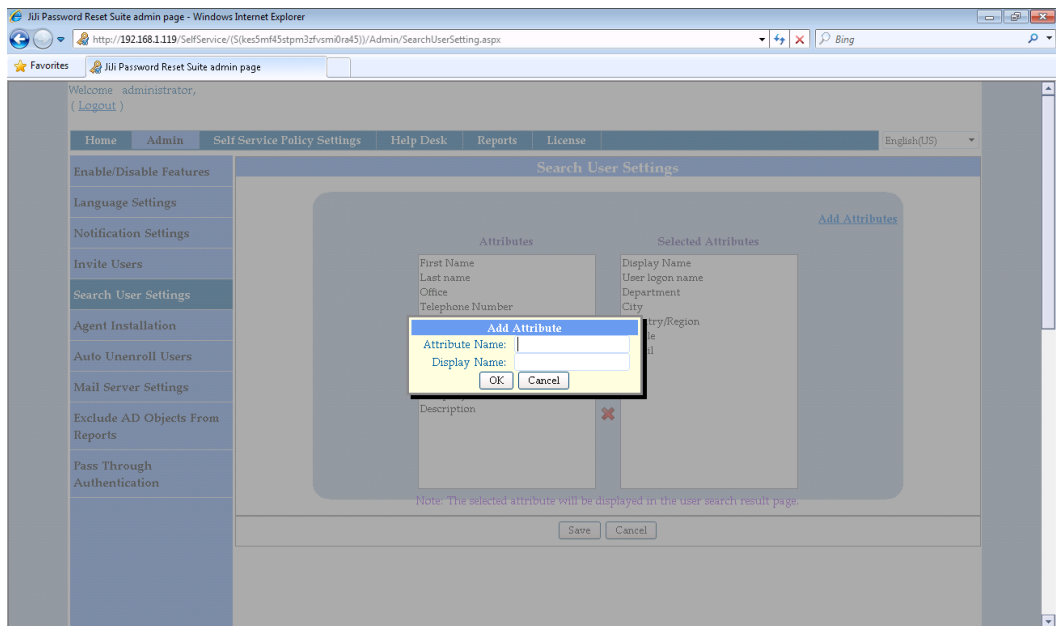
Figure 1.46.



If you need extra attributes you can add it as follows.

- Click on **Add Attributes** link label.
- A window will be opened. Enter the attribute name, display name and click ok button.

Figure 1.47.



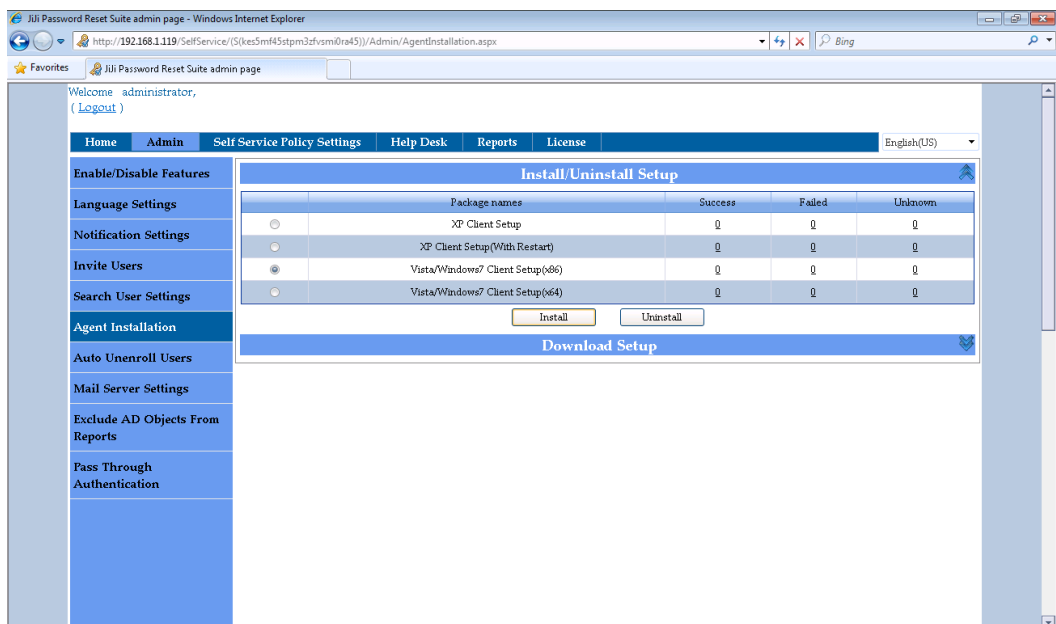
- To edit or delete, select the attribute and click on the corresponding image shown at the center.

Agent Installation

This is to reset password from the windows logon screen.

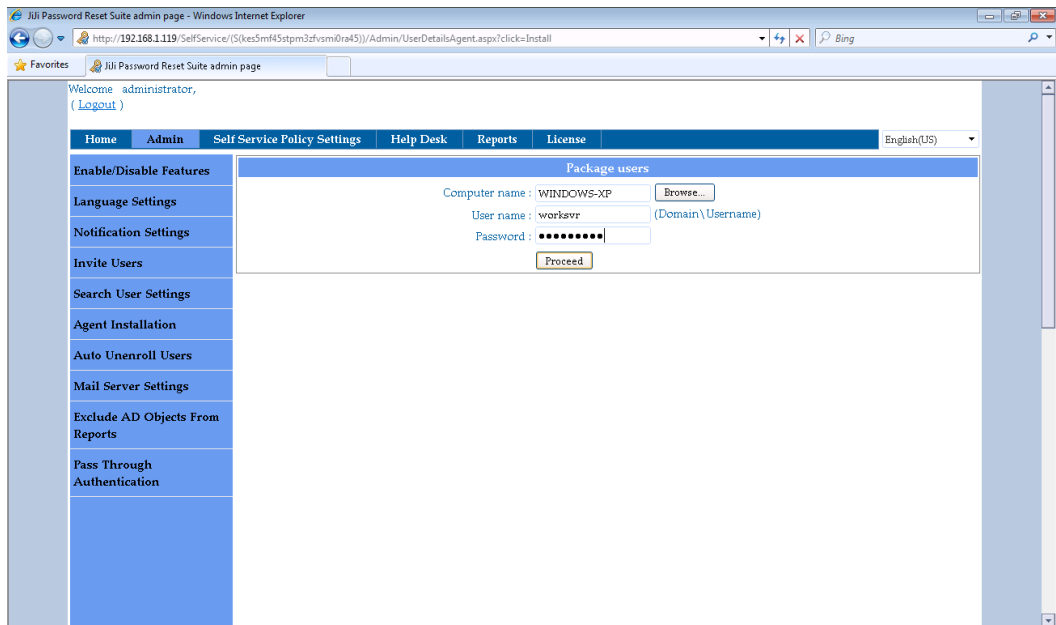
- Select any one of the packages and click install button.

Figure 1.48.



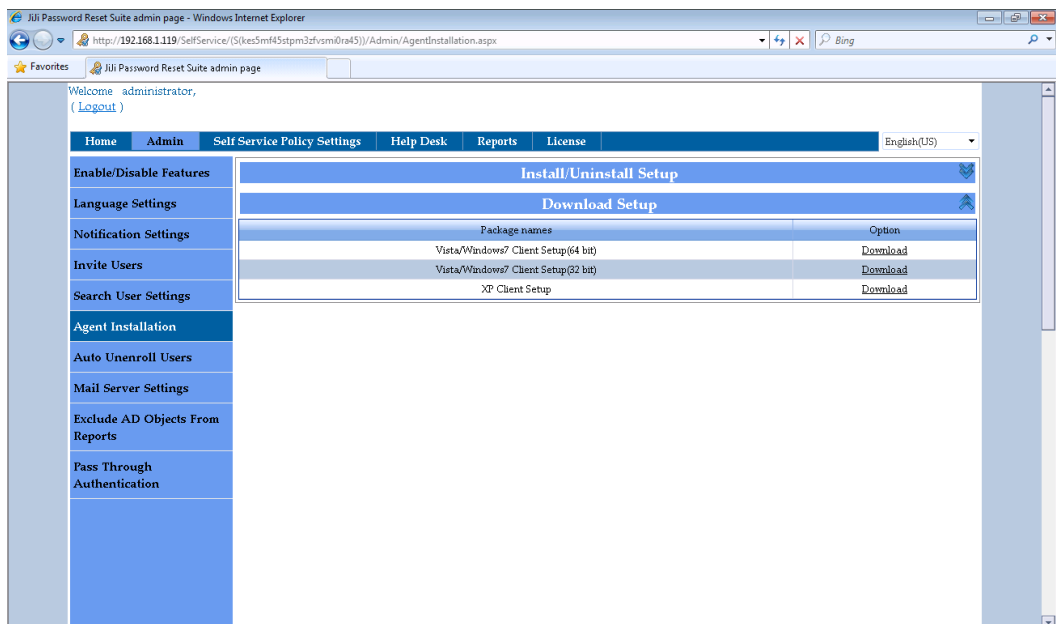
- Select the computer in which it has to be installed. Enter username and password and click proceed button.

Figure 1.49.



- You can also download the packages and install it in your machine.

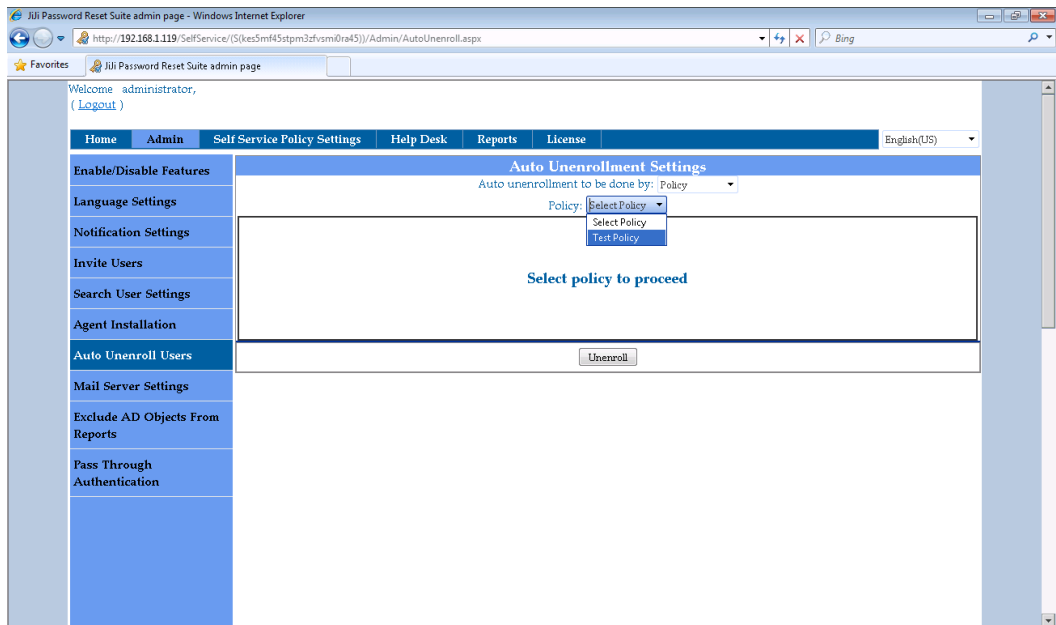
Figure 1.50.



Auto Unenroll Users

- You can apply unenrollment settings to the selected AD objects or selected policy.

Figure 1.51.



- Select AD Objects or Policy and click '**Unenroll**' button. Users under them will be unenrolled.

Figure 1.52.

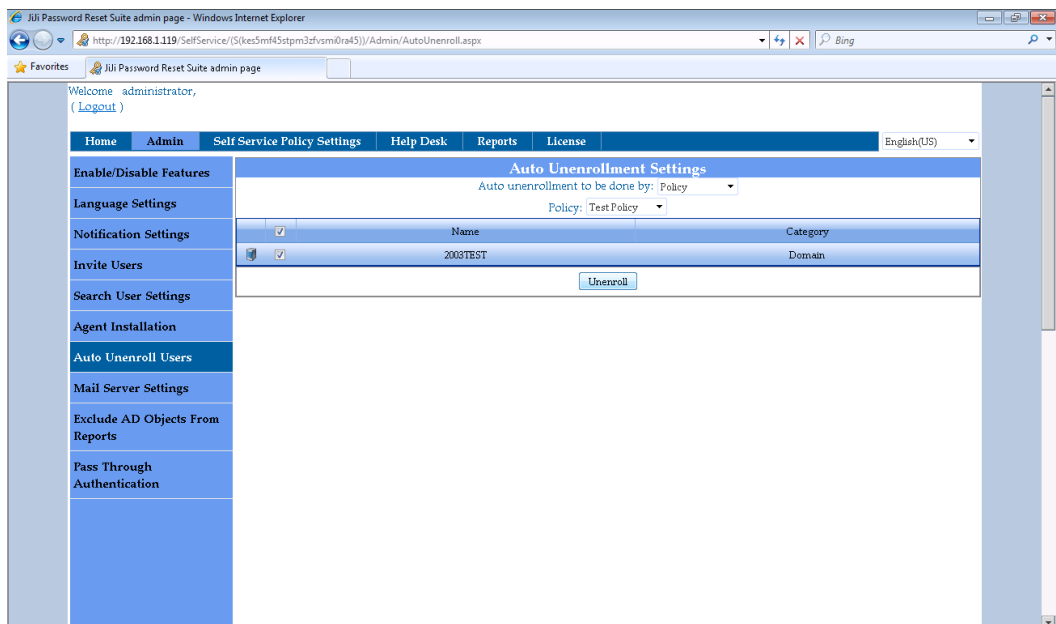
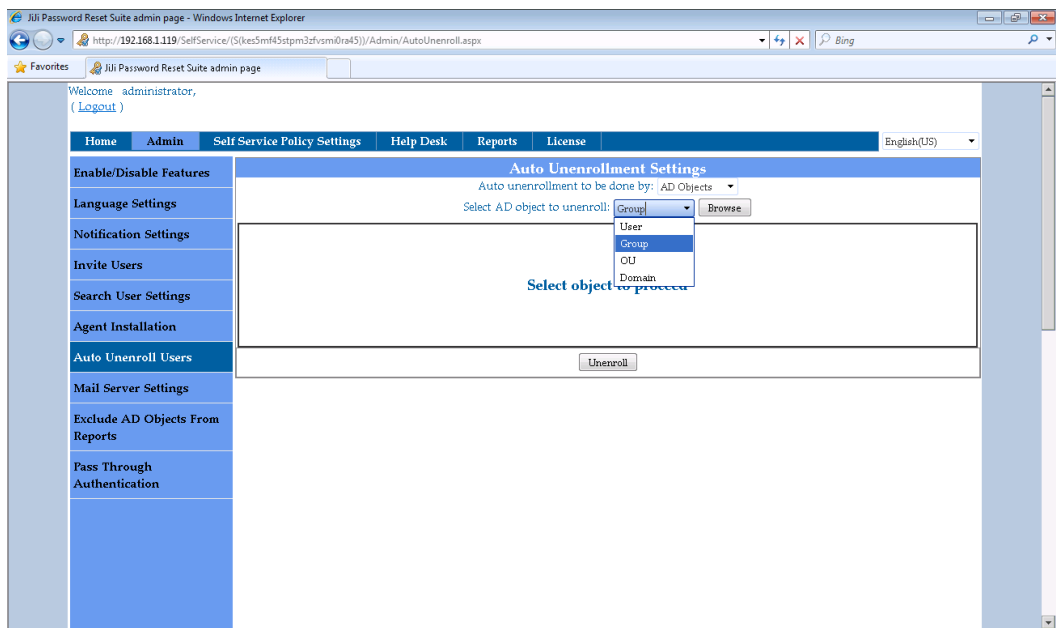


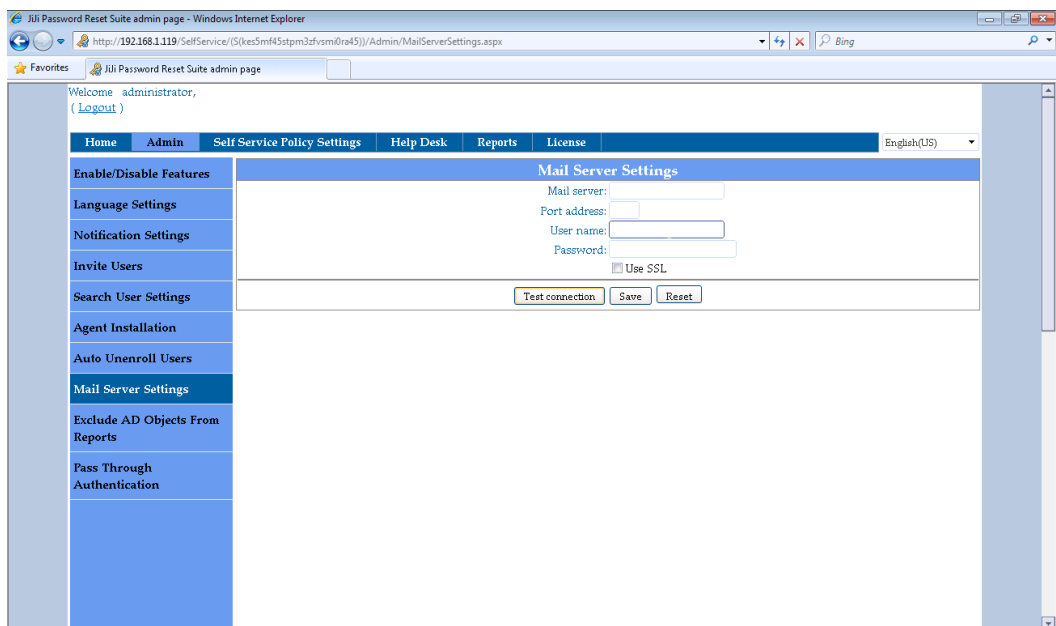
Figure 1.53.



Mail Server Settings

- Enter the mail server details and click '**Test connection**' button to test the settings.

Figure 1.54.



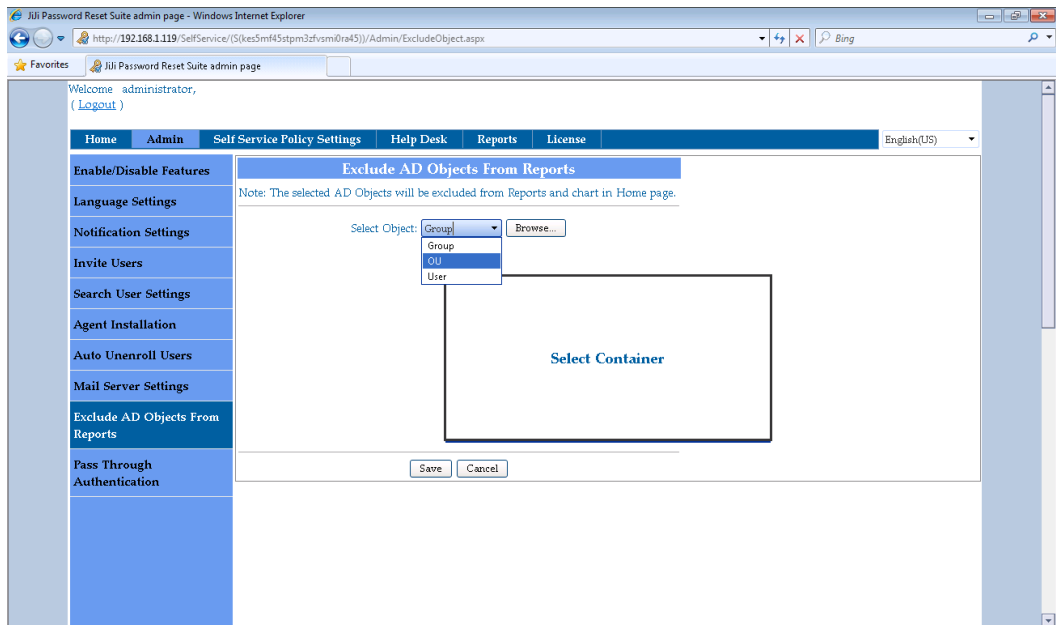
- If test is success save the settings by clicking '**Save**' button.

Exclude AD Objects from Reports

If you do not need audits for certain AD Objects you can exclude it from the reports. Excluded objects will not be listed both in chart and in homepage.

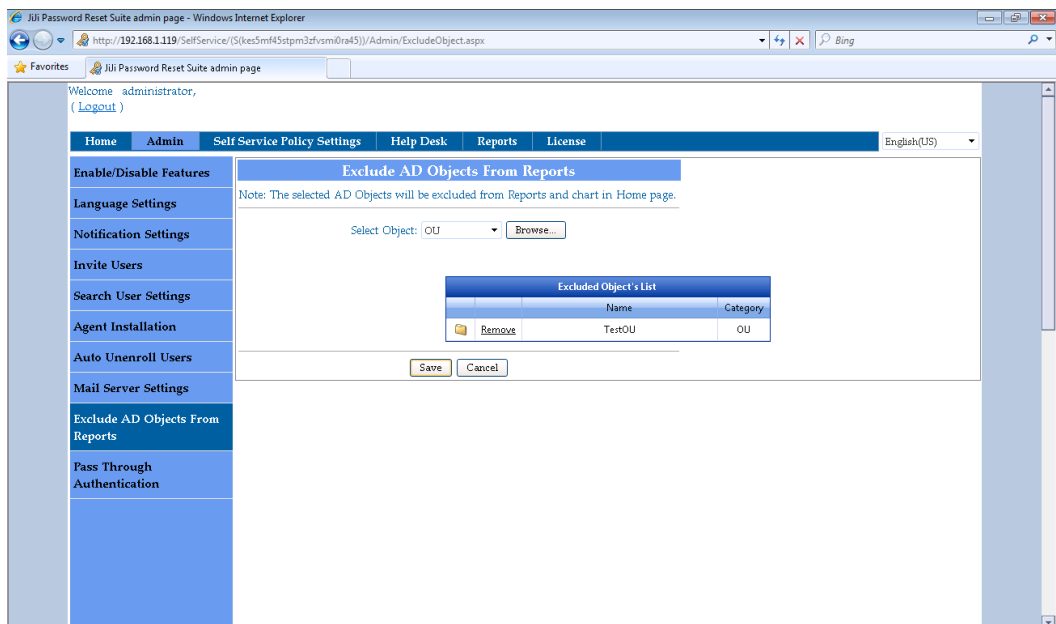
- Select object and click '**Browse**' button.

Figure 1.55.



- Add it in Excluded objects list and click 'Save' button.

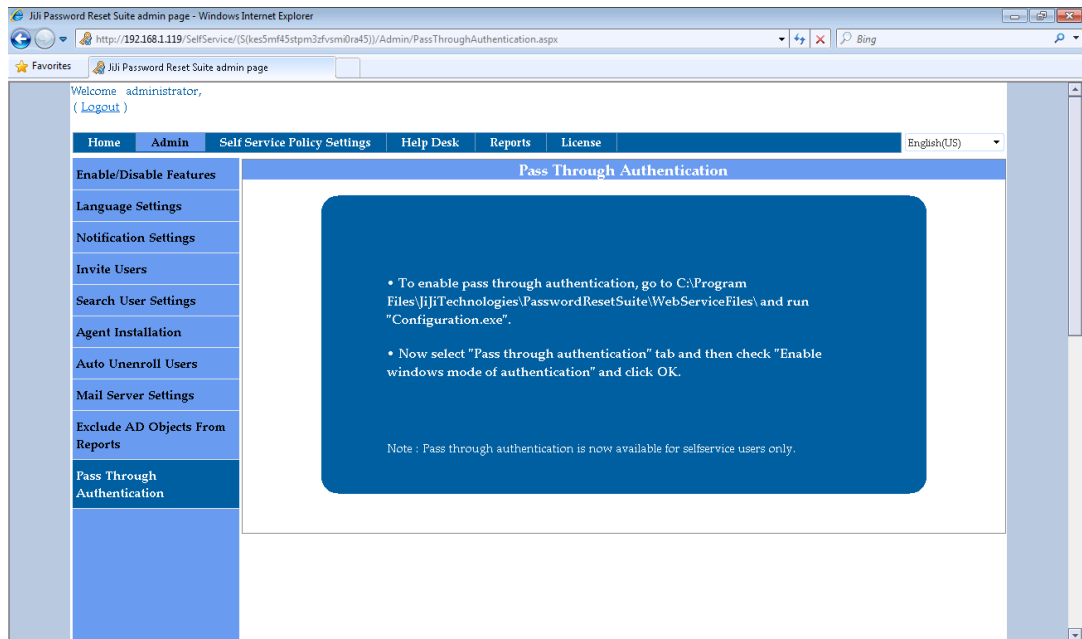
Figure 1.56.



Pass Through Authentication

This is to enable **Windows Mode of Authentication** while logon. This is available for self service users only.

Figure 1.57.



Note

If you had not enable it while installation, follow the steps given in Pass Through Authentication tab to make it enable.

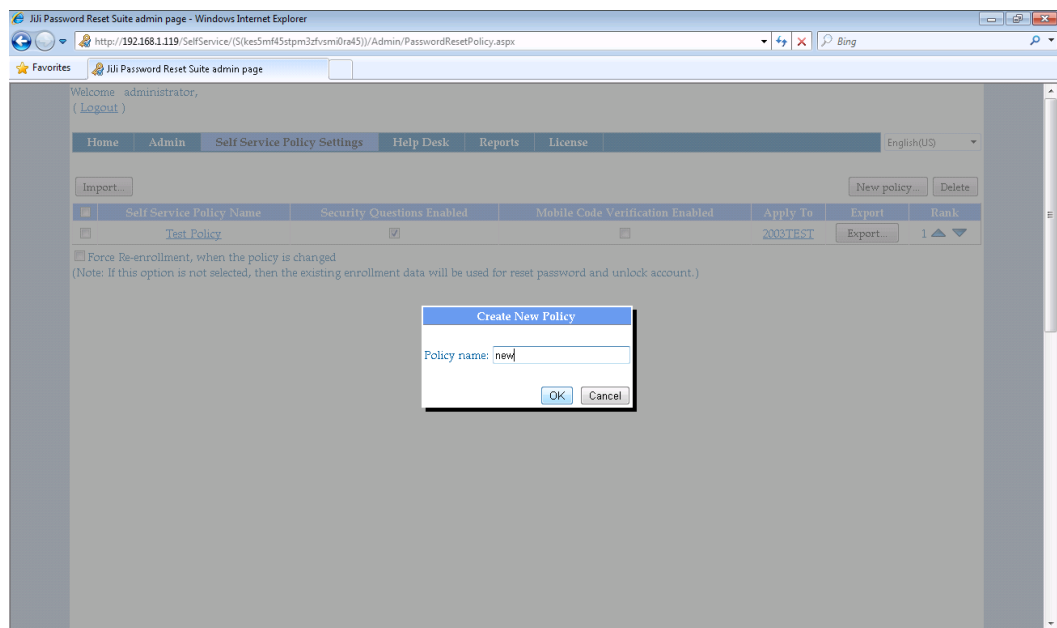
SELF SERVICE POLICY SETTINGS

Click on Self Service Policy Settings in Admin Web. A default policy will be already available. You can edit it or create your own policy for Self Service users.

Creating and Deleting Policies

- Click 'New Policy' button to create new policy. Enter Policy name and click 'OK' button.

Figure 1.58.



- Follow the settings explained in the succeeding sections to apply for this new policy.
- To delete, select the policy and click **Delete** button.

Ranking Policies

If the user is present in group as well as OU and if different policies were applied to user, group and OU, then the Policy will be assigned based on the priority. First priority will be given for user next for group and then for OU.

If the same user is present in different groups, we can assign priority using rank

i.e. when a group has to be assigned with highest priority, shift it to highest rank.

Export and Import

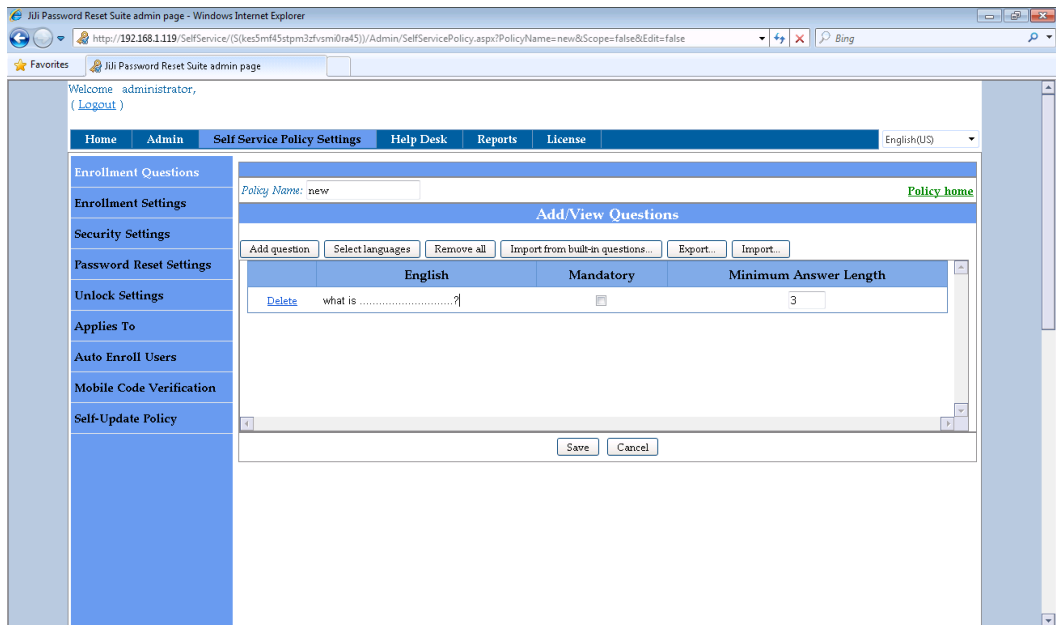
You can create policy and export it to any location. To import the file from any location, click import button and add the file which contains the policies.

Enrollment Questions

To edit the policy settings, click on the **Self Service Policy Setting tab** and then click policy which has to be edited. Now start editing as per your need.

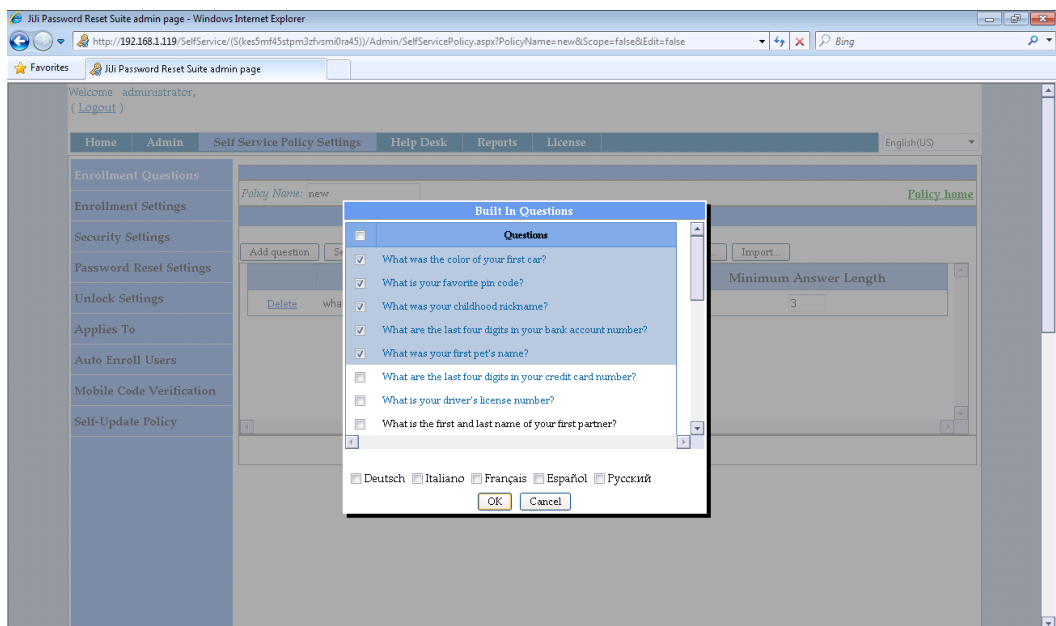
- In Enrollment Questions setting, you can add your own questions or builtin questions. These must be answered by the users for authorization.
- Click **Add question** button, type your own questions and click **Save** button.

Figure 1.59.



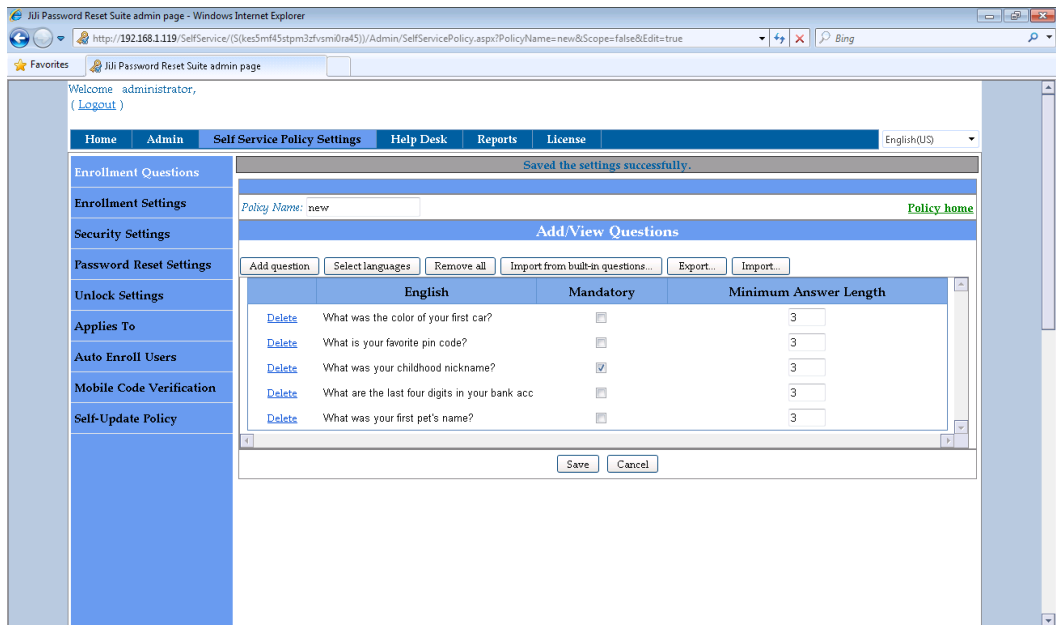
- To use built-in questions, click **'Import from built-in questions'** button. Select questions and click **'OK'** button.

Figure 1.60.



- You can also select languages of your choice to create questions.
- Set whether the question is mandatory or not.
- Set minimum length for answers so that while entering the answers, users can be avoided from entering it with less than the length specified here. Save the settings.

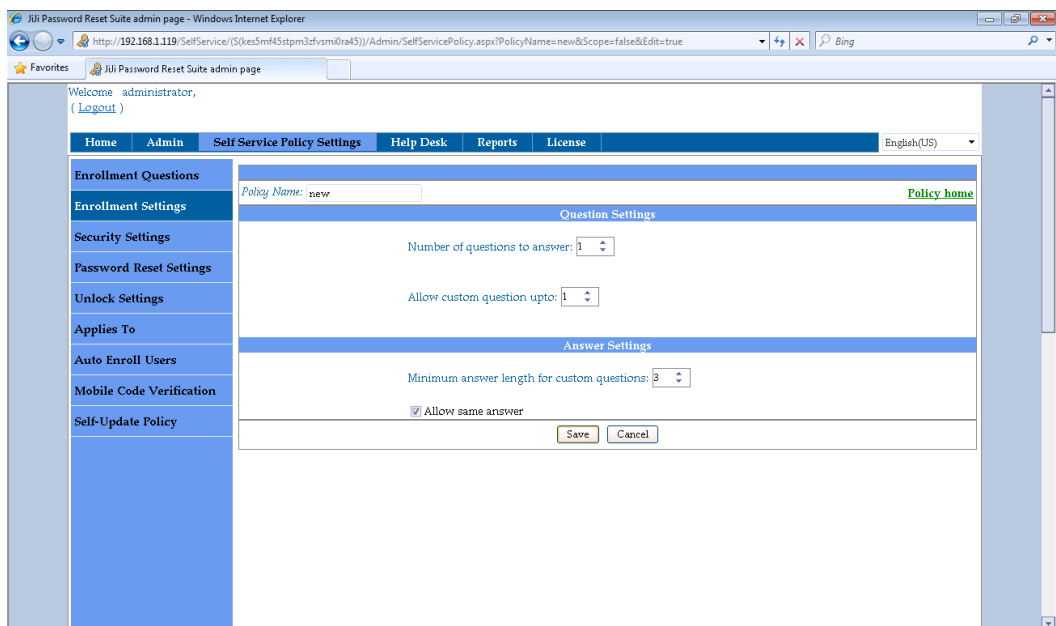
Figure 1.61.



Enrollment Settings

- Set the number of questions to be answered, number of custom questions to be created by users.
- Set the minimum answer length for custom questions.
- Check the '**Allow same answer**' check box to allow users to enter same answers for two or more questions.
- Click '**Save**' button to save the settings.

Figure 1.62.



Security Settings

a) Answer settings

- In answer settings, If you check the '**Show hidden text**' check box, the user can have this option to view all their hidden enrollment answers, passwords which they type while changing or resetting passwords.
- Check '**Allow case insensitive answers**' check box to allow users to enter case insensitive answers for enrollment questions.

b) Incorrect Answers Lockout Settings

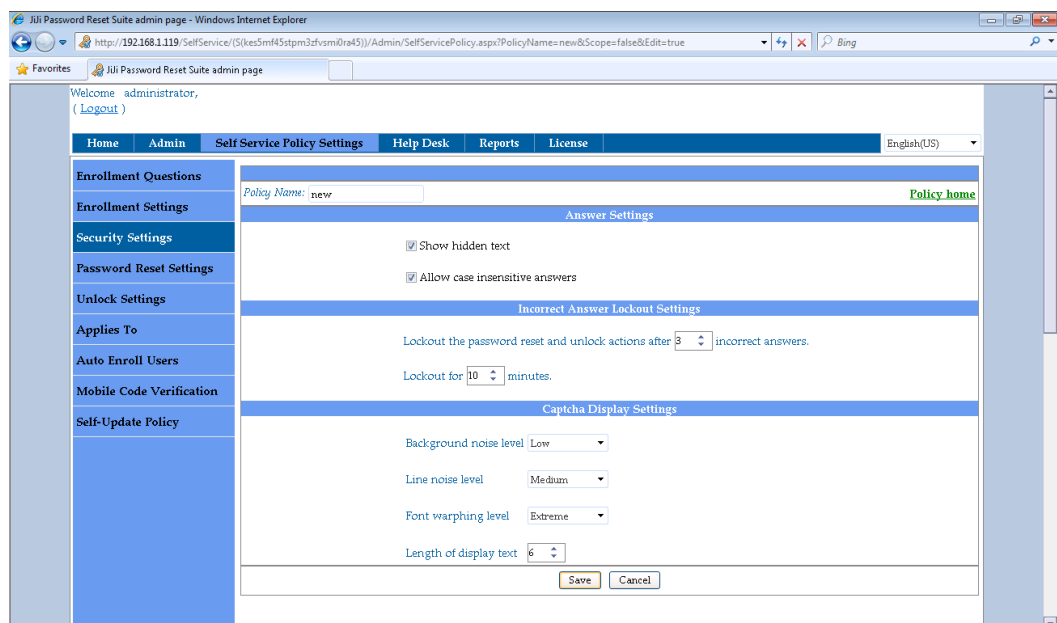
- You can set to Lockout password reset after certain number of incorrect answers. Lockout duration can also be set.
- If the users try with wrong answers for more than the specified number of times they will be lockedout from resetting the password. They cannot try to reset password till the completion of lockout duration.

c) Captcha Display Settings

You can set the following settings to None, Low, High, Medium, Extreme in Captcha Display.

- Background noise level
- Line noise level
- Font warping level
- Length of display text

Figure 1.63.



Password Reset Settings

a) Answer Settings

You can set to answer all the questions while password resetting or you can allow to answer certain number of random question.

b) General Settings

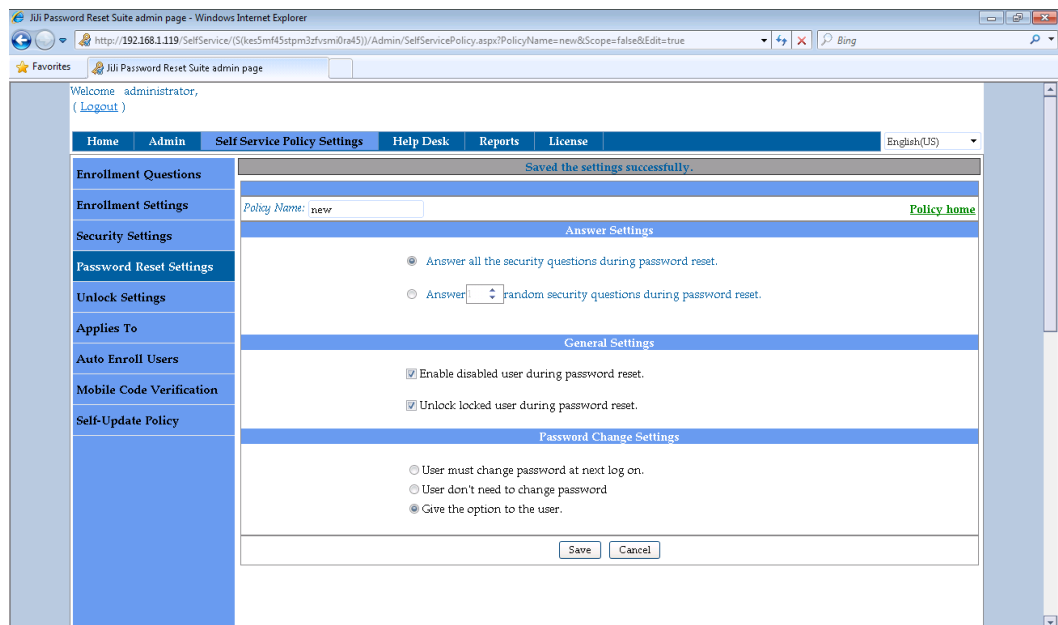
You can enable the disabled user and unlock the locked users along with password reset.

c) Password Change Settings

You can set any one of the three options for the user who tries to change password.

- User must change password at next log on.
- User don't need to change password
- Give the option to the user.

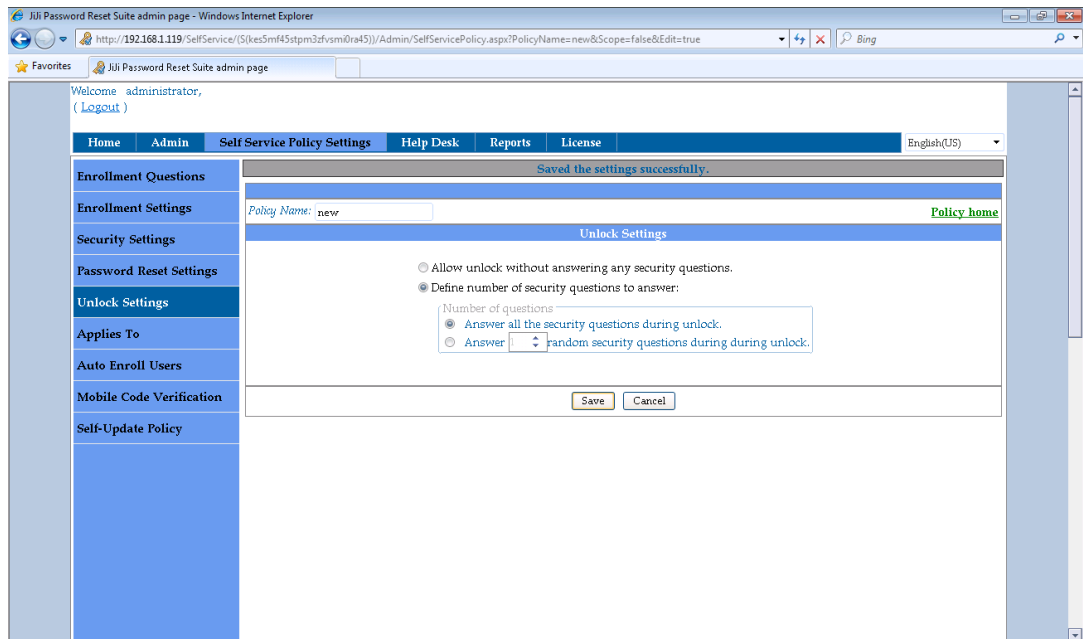
Figure 1.64.



Unlock Settings

You can either allow users to unlock without answering the security questions or define number of questions to be answered by them while unlocking.

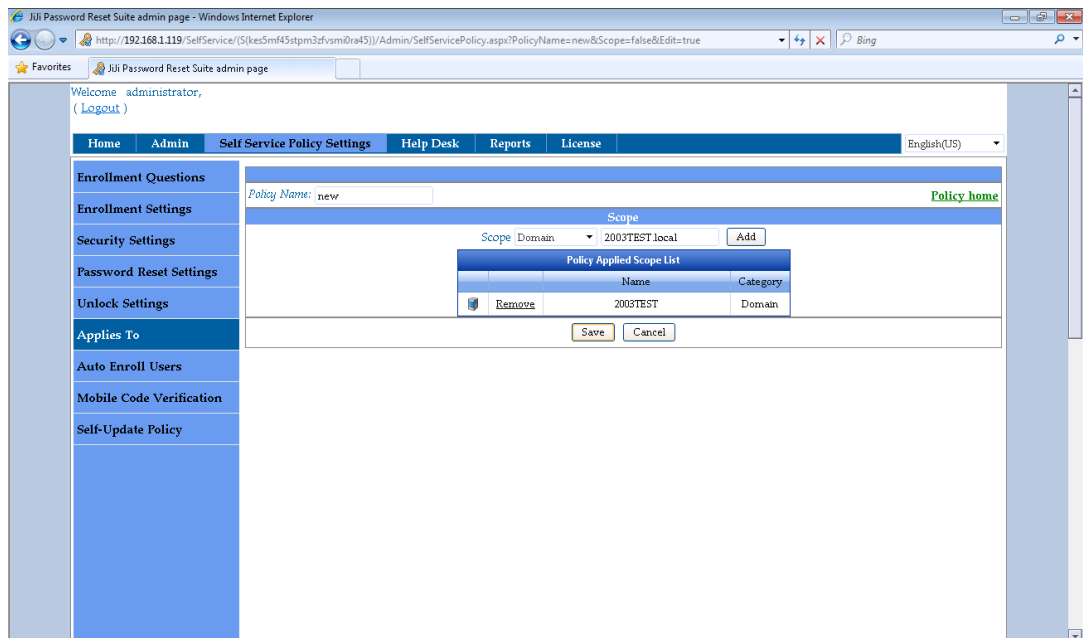
Figure 1.65.



Applies to Settings

You can select a scope such as User/Group/OU/Domain to apply the selected policy.

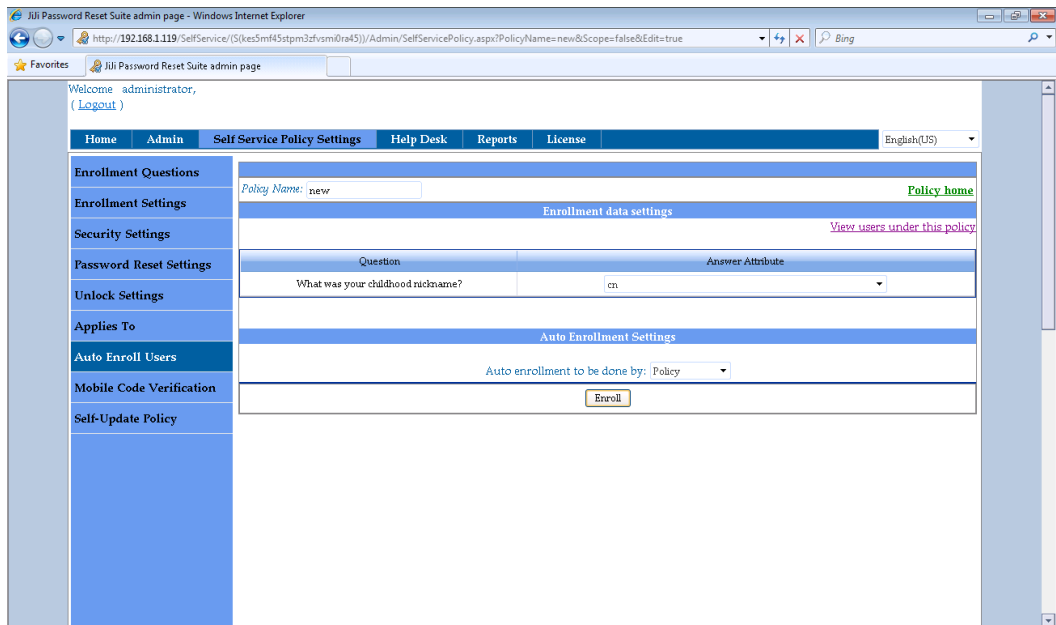
Figure 1.66.



Auto Enroll Users

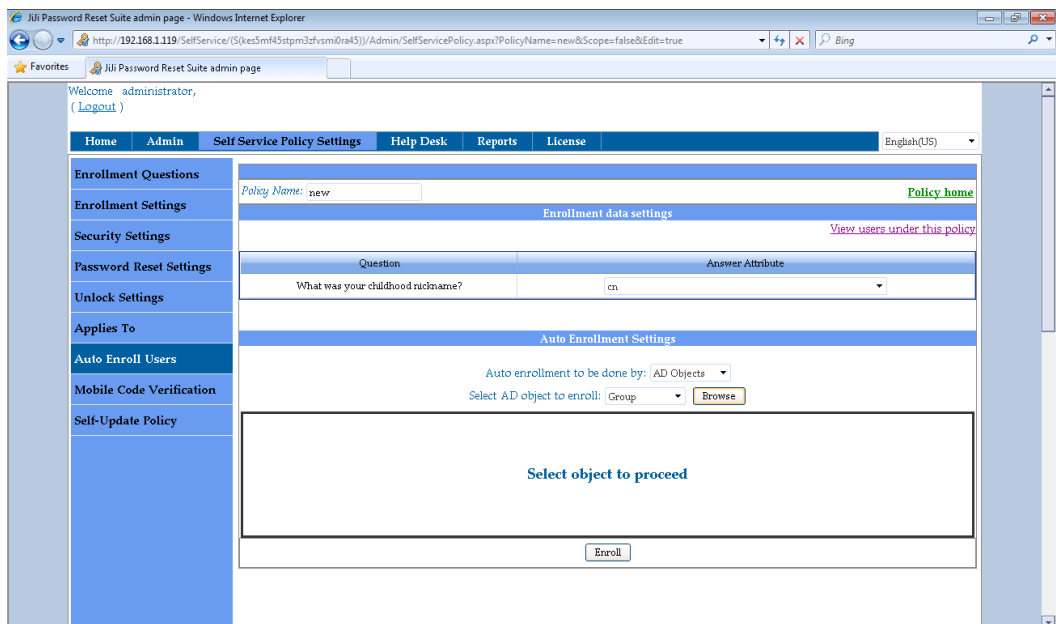
- If users under certain policy were not enrolled you can auto enroll them.
- Select certain questions and corresponding Answer attribute.

Figure 1.67.



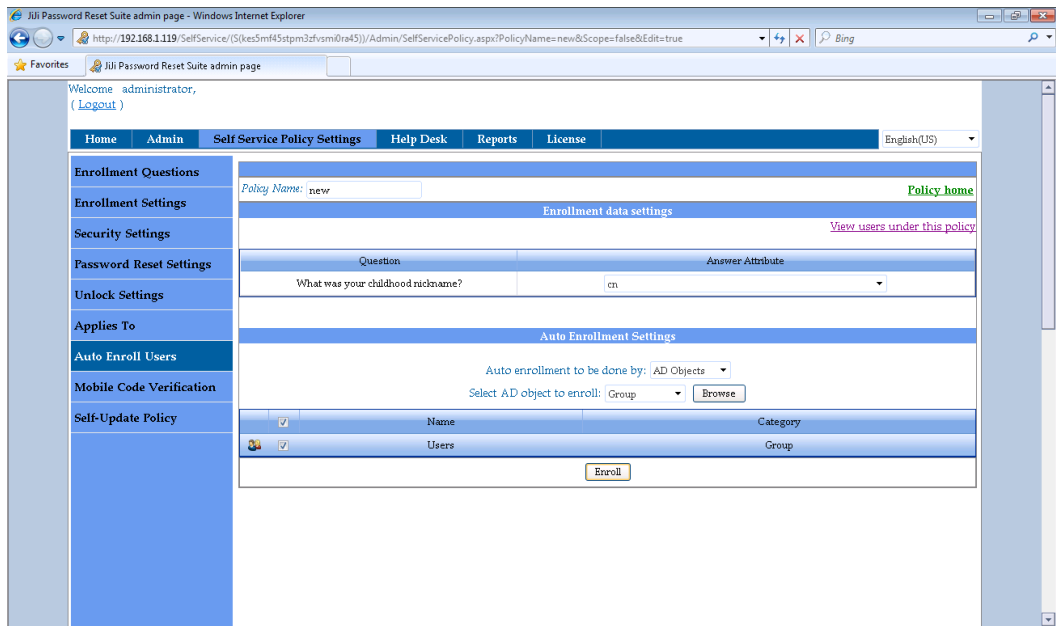
- You can apply auto enrollment settings to users of selected policy or to selected AD Objects.

Figure 1.68.



- Select object and click '**Enroll**' button. Enrollment settings will be applied to all the selected users.

Figure 1.69.



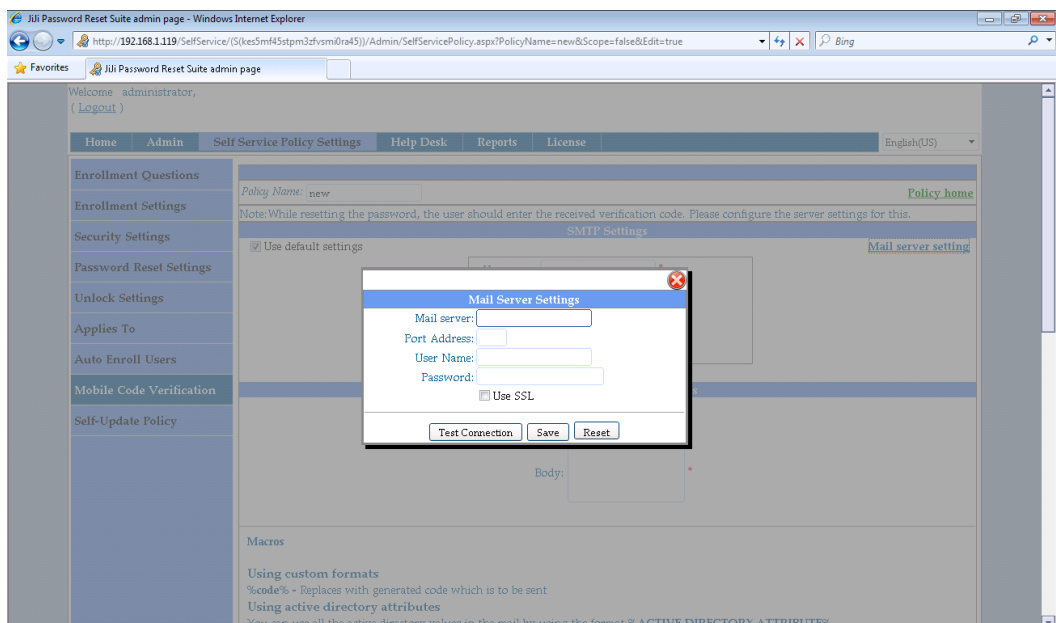
Mobile Code Verification

These settings are used to create mobile code for users to authenticate while resetting their passwords.

a) Smtip Settings

- If you have already configured mail server settings in admin page, then check 'Use default settings' checkbox otherwise click the 'Mail server setting' link label at the right corner.
- Enter details and click 'Test Connection' button to test the setting.
- Click 'Save' to save the settings.

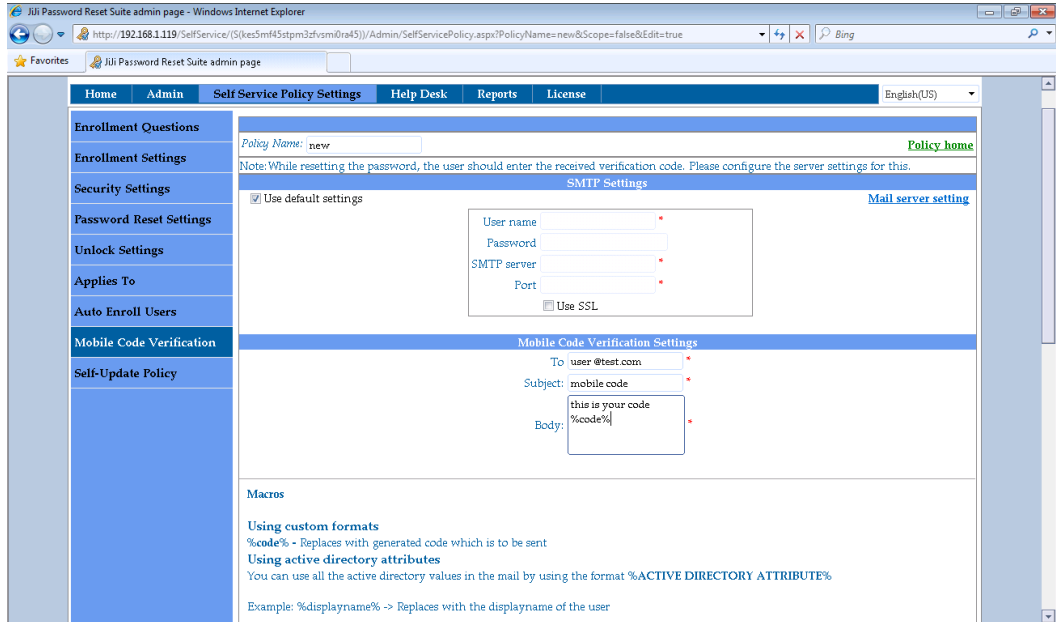
Figure 1.70.



b) Mobile Code Verification Settings

- Enter the email id to which the code is to be send.
- Type the subject. Use the macro %code% in the body, which will be replaced by the generated code value.

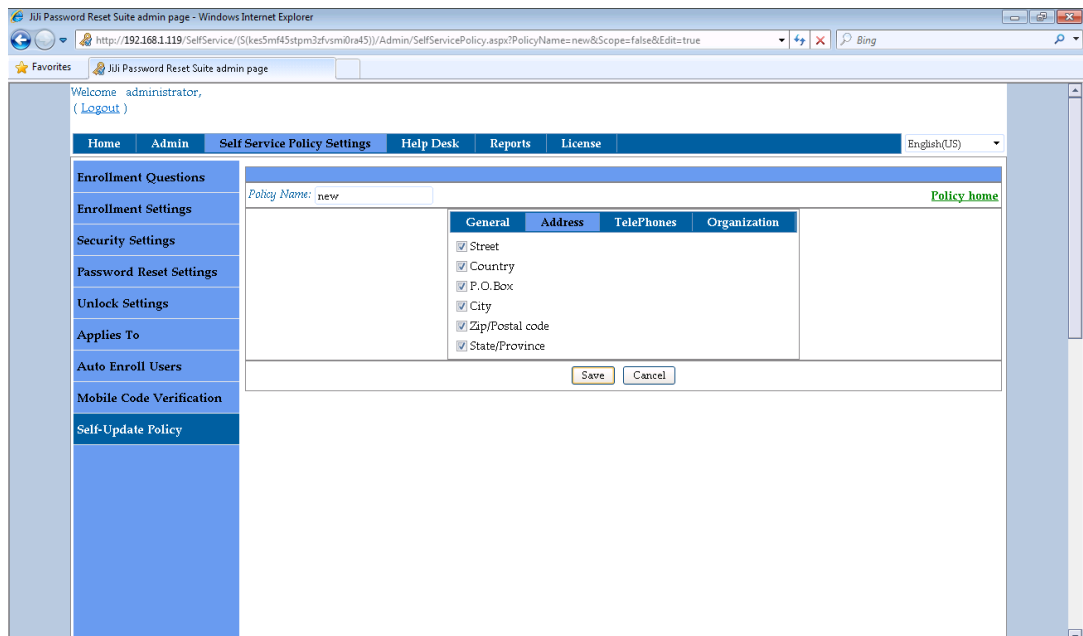
Figure 1.71.



Self-Update Policy

Here you can check on certain user informations which are to be updated by the users while working with self service.

Figure 1.72.



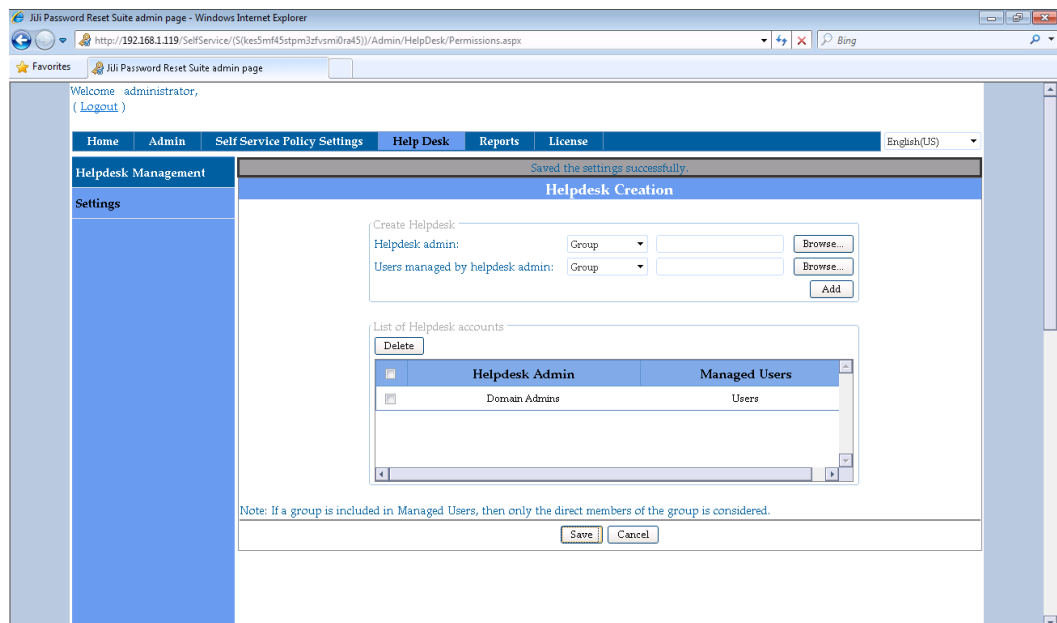
Help Desk

Administrator can delegate authority to a particular user or groups called help desk authority. Help desk can effectively manage all those users who need to perform password reset or to unlock account.

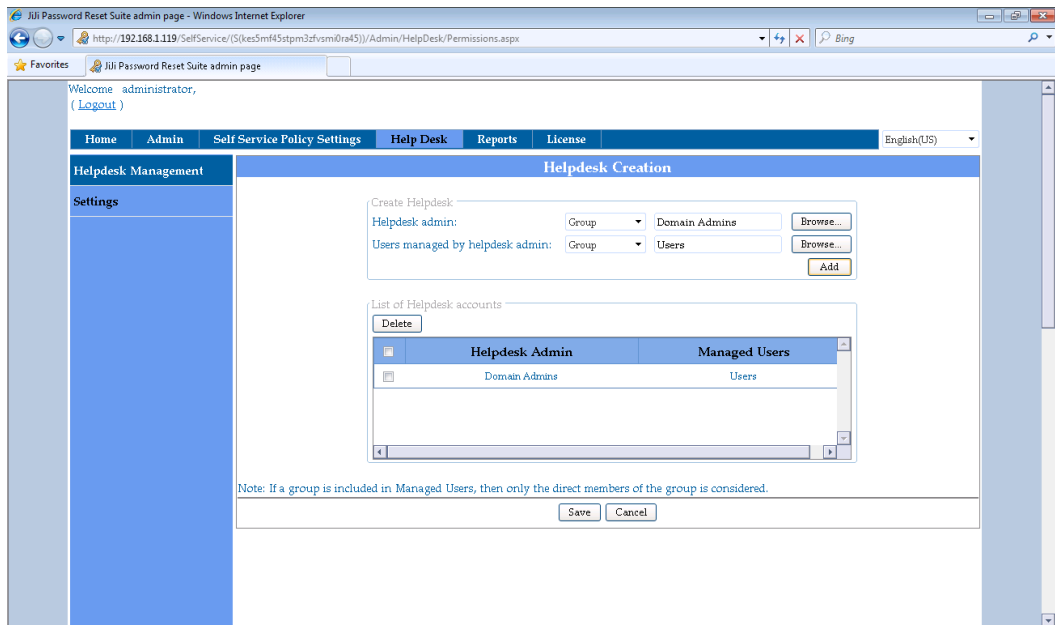
Help Desk Creation

- Select a user or group or OU as Help desk admin.
- Select the users or group or OU to be managed by the help desk team. These users can contact the help desk team in case if they lost their password or if their account is locked out.
- Click '**Add**' button to add the created help desk account.

Figure 1.73.



- Similarly you can add many help desk accounts consisting of help desk admin and managed users.
- Click '**Save**' to save the settings.

Figure 1.74.

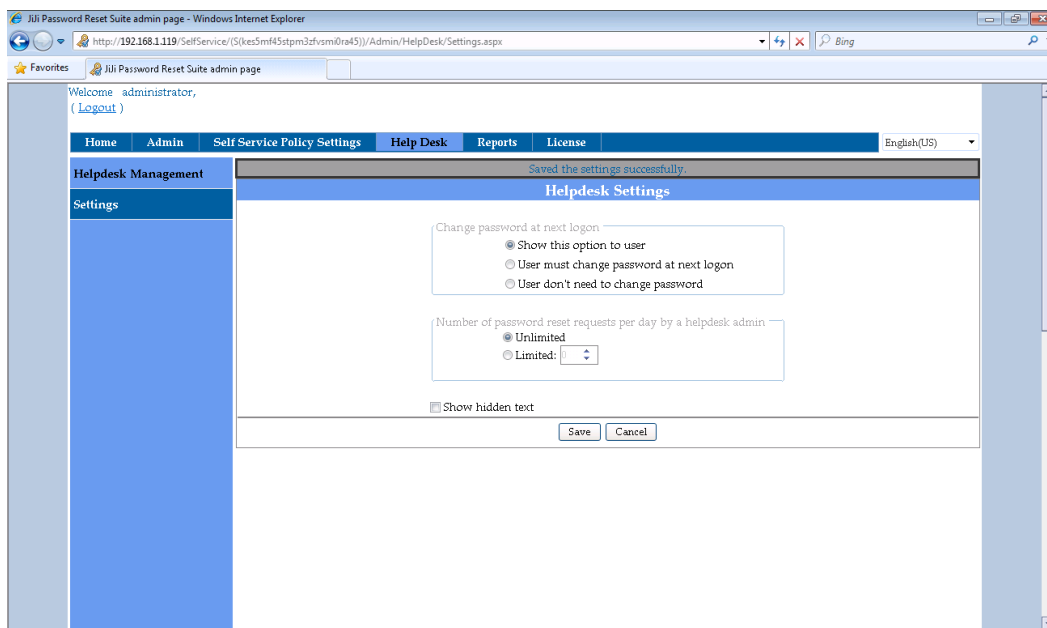
Help Desk Settings

- You can select any one of the following choices for change password option. Selected setting will be displayed in the help desk web.

Change password at next logon

- Show this option to user
- User must change password at next logon
- User don't need to change password
- If number of password reset requests per day by a helpdesk admin is set as limited then they can perform only the specified number of resets for the users those who were managed by them.

Figure 1.75.



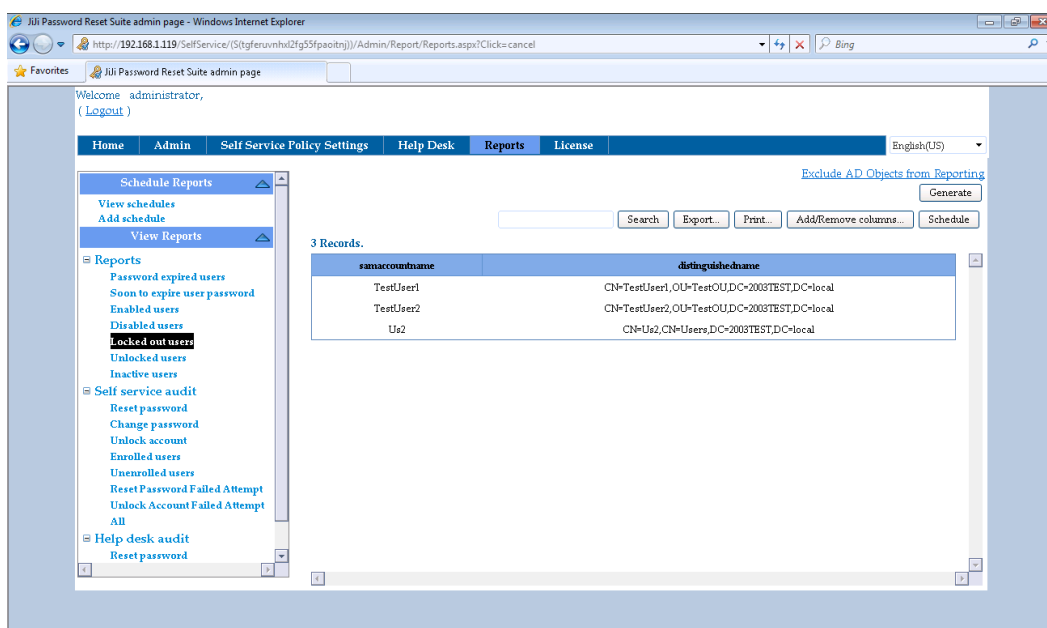
Reports

Reports helps to track the changes made in password by both help desk and Self Service users.

View Reports

- Click on the corresponding reports in the report column to view the change details.
- You can view the changes made in between certain dates.
- Click 'Add/Remove columns' button to add or remove the attributes column.

Figure 1.76.



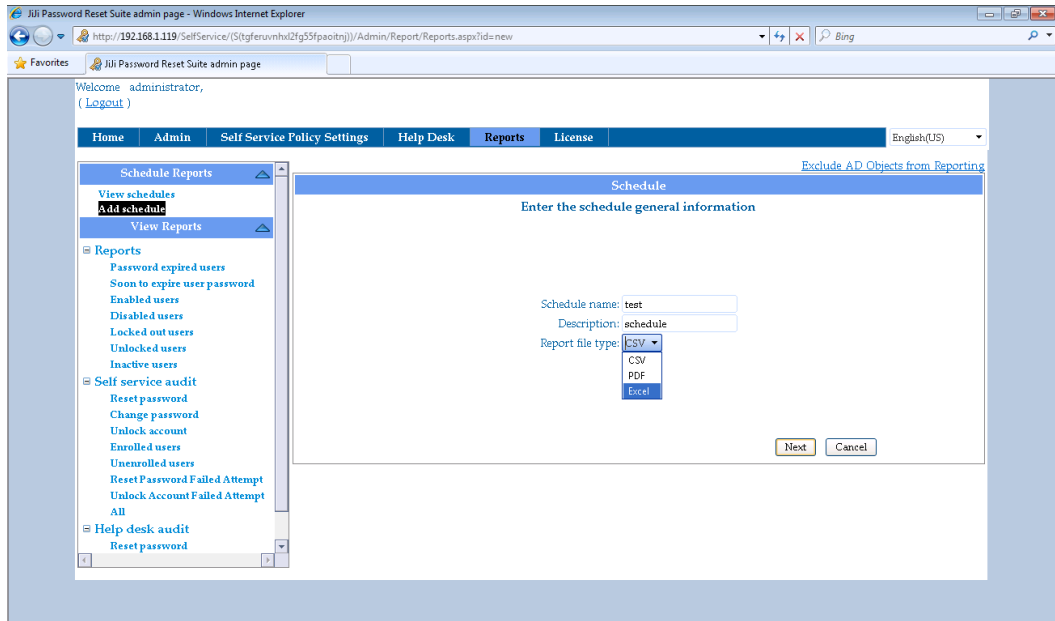
Schedule reports

You can schedule the reports to view it through e-mail at regular intervals of time. Generated reports will be send periodically to the provided e-mail id.

Add schedule

- Click 'Add schedule' tab. Enter schedule informations and click 'Next'.

Figure 1.77.



- Select the report category. You have three main types of reports. They are General, Self Service, Help Desk reports. Select Any of the needed reports from the left and shift it to right.

- **General Reports**

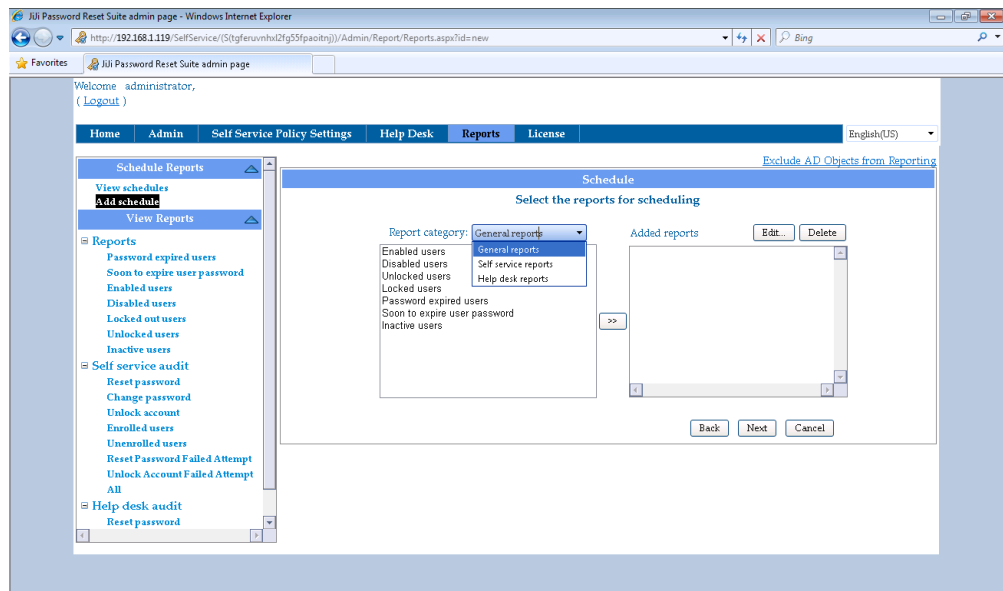
- Password expired users
- Soon to expire user password
- Enabled users
- Disabled users
- Locked out users
- Unlocked users
- Inactive users

- **Self Service Reports**

- Reset password
- Change password
- Unlock account
- Enrolled users

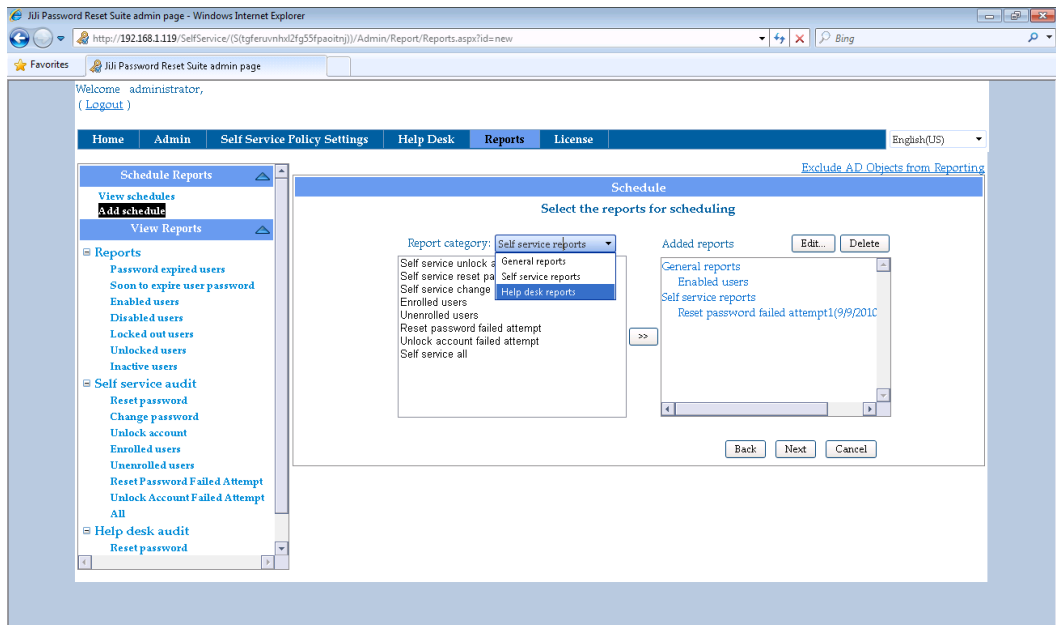
- Unenrolled users
- Reset Password Failed Attempt
- Unlock Account Failed Attempt
- All Self service reports
- **Help Desk Reports**
 - Reset password
 - Unlock account
 - All help desk reports

Figure 1.78.



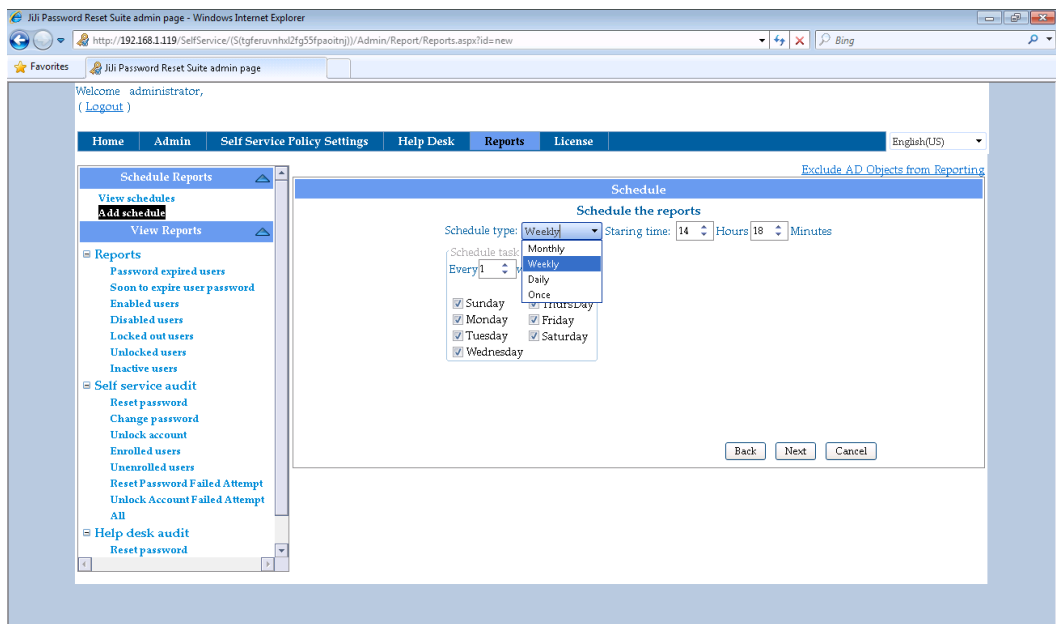
- You can select reports from general, self service and help desk for a single schedule.

Figure 1.79.



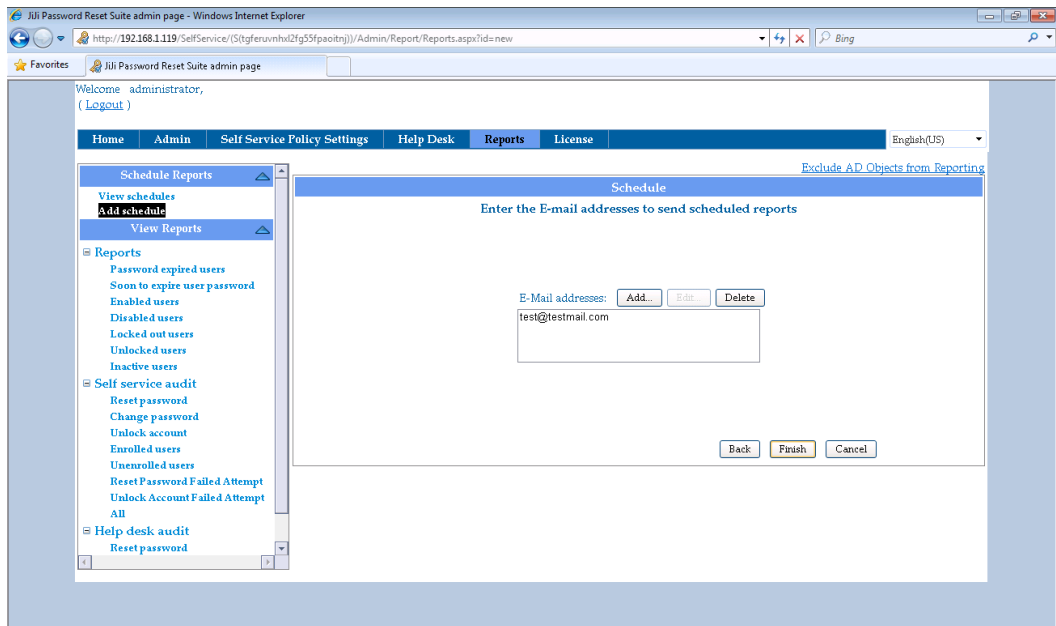
- Schedule the task for monthly or weekly or daily or once and click next.

Figure 1.80.



- Enter the e-mail id to send mail and click 'Finish' button.

Figure 1.81.



View Schedule

Here you can view history of all the schedules which were created before.

Chapter 6. WORKING WITH SELF SERVICE WEB

Administrator can provide certain rights to user for self resetting and self changing of passwords through self service password reset. To start with, users have to login and enroll themselves.

USER DETAILS

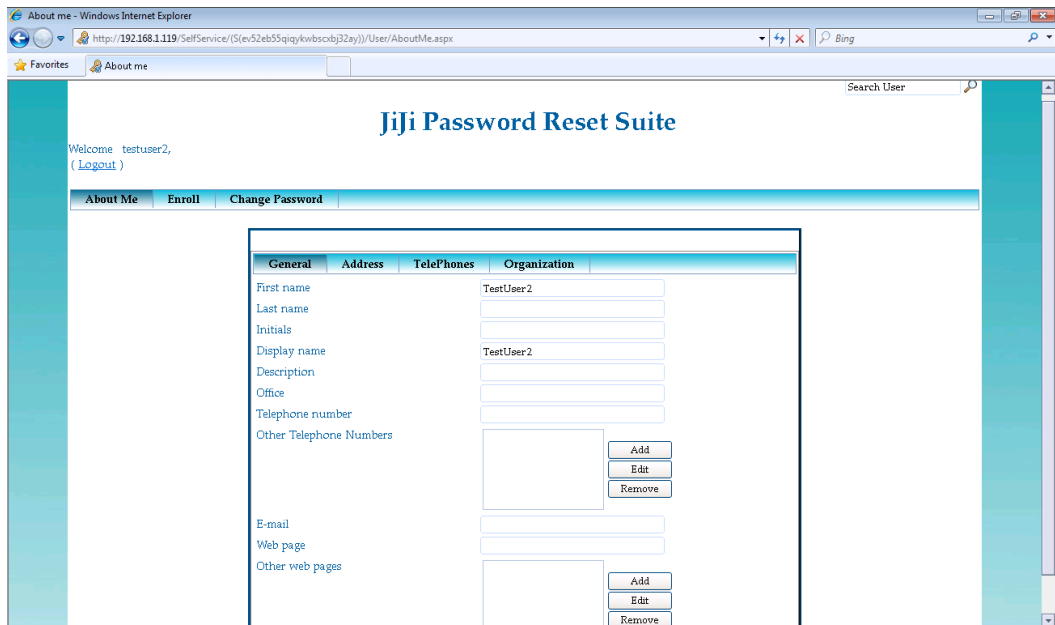
- Open Self Service Web home page and log in. Start -> Programs -> JiJi Technologies -> JiJi Password Reset Suite -> Web Client -> Self Service Web.

Figure 1.82.



- Login and click '**About me**' tab. Enter all the general, Address, Telephone, Organisation details and save them.

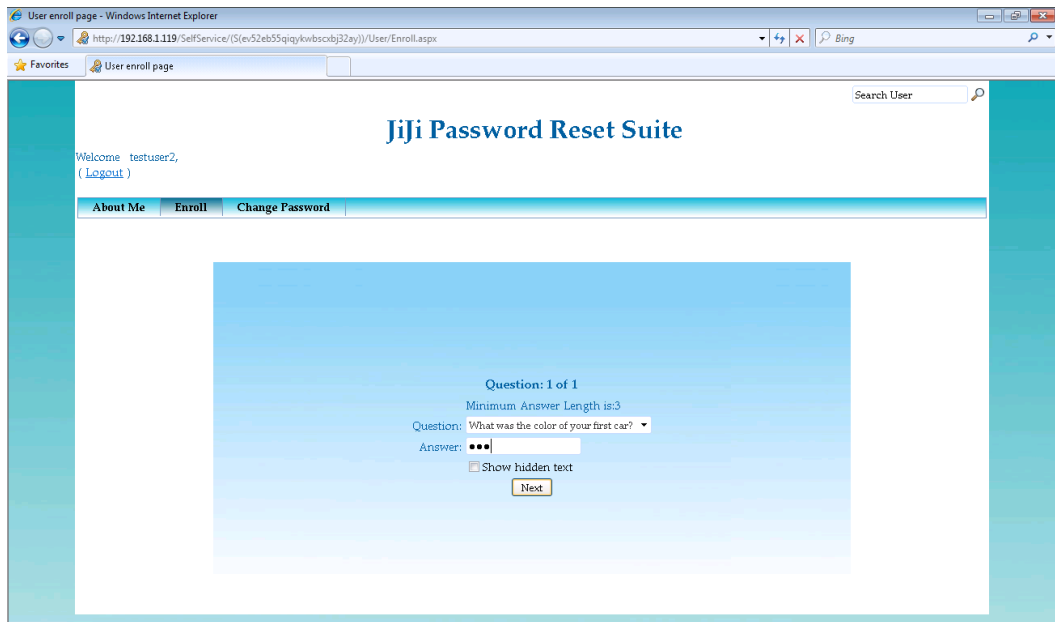
Figure 1.83.



ENROLLMENT

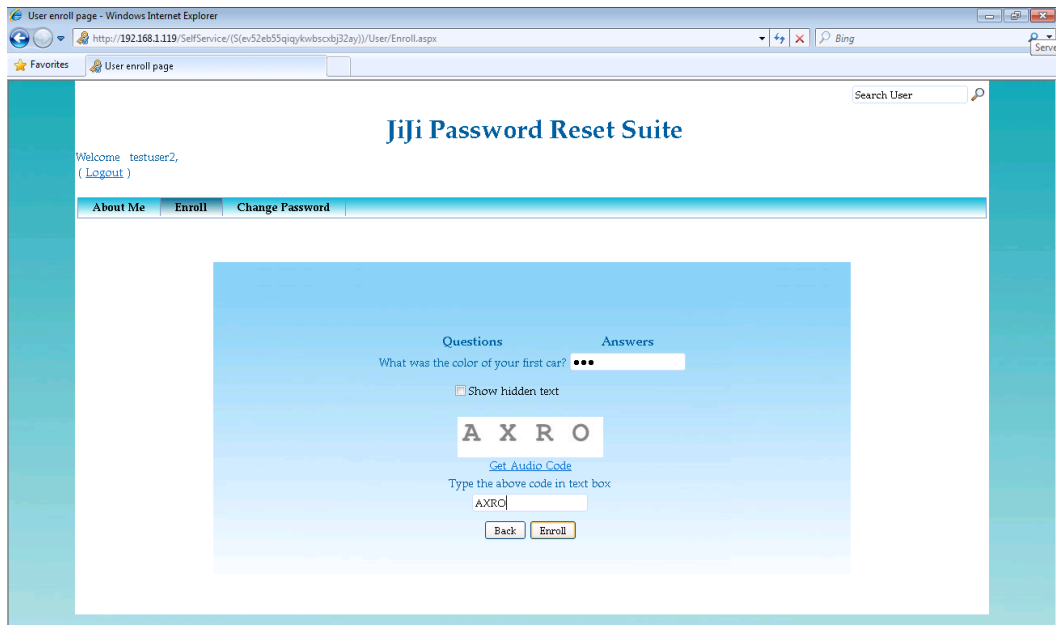
- Click 'Enroll' tab. Set of questions will be given to you.

Figure 1.84.



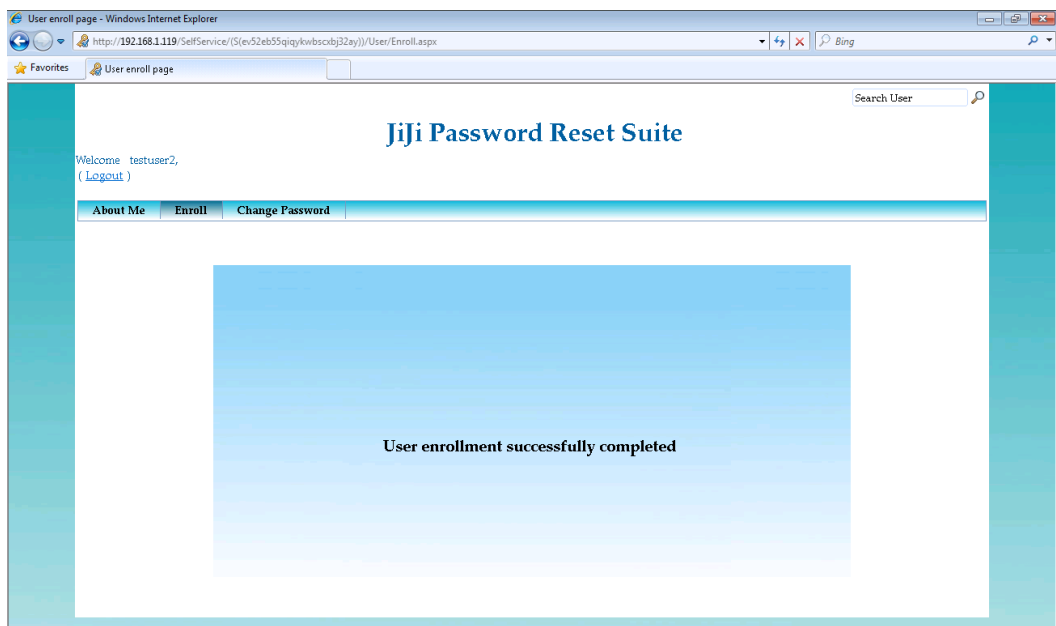
- Enter suitable answers for the questions and the captcha code.

Figure 1.85.



- Click '**Back**' if you have to edit the answers. Finally click '**Enroll**' button to finish your enrollment process.

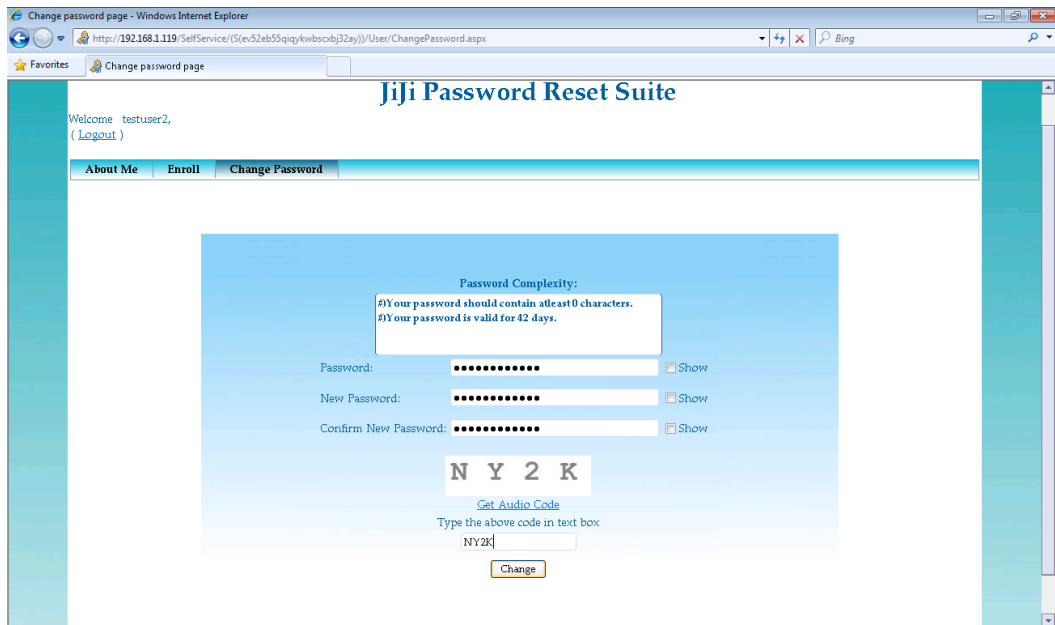
Figure 1.86.



CHANGE PASSWORD

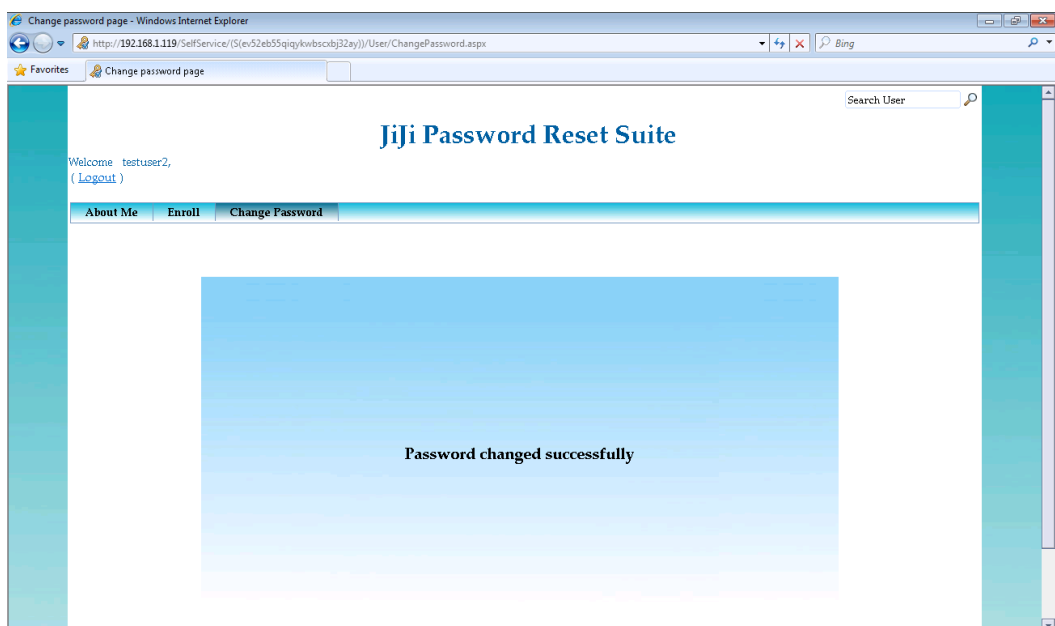
- Click on the 'Change Password' tab.
- Enter the old password and the new password.

Figure 1.87.



- The new password must meet all the password complexities as mentioned in the Password Complexity text box. Type the given code and click '**Change**' button.

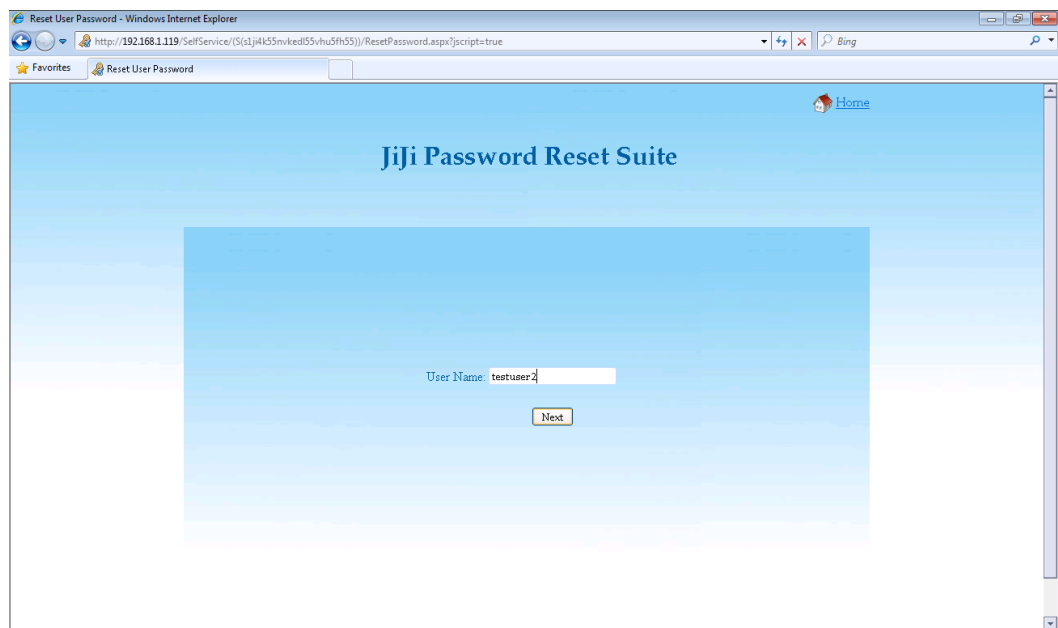
Figure 1.88.



RESET PASSWORD

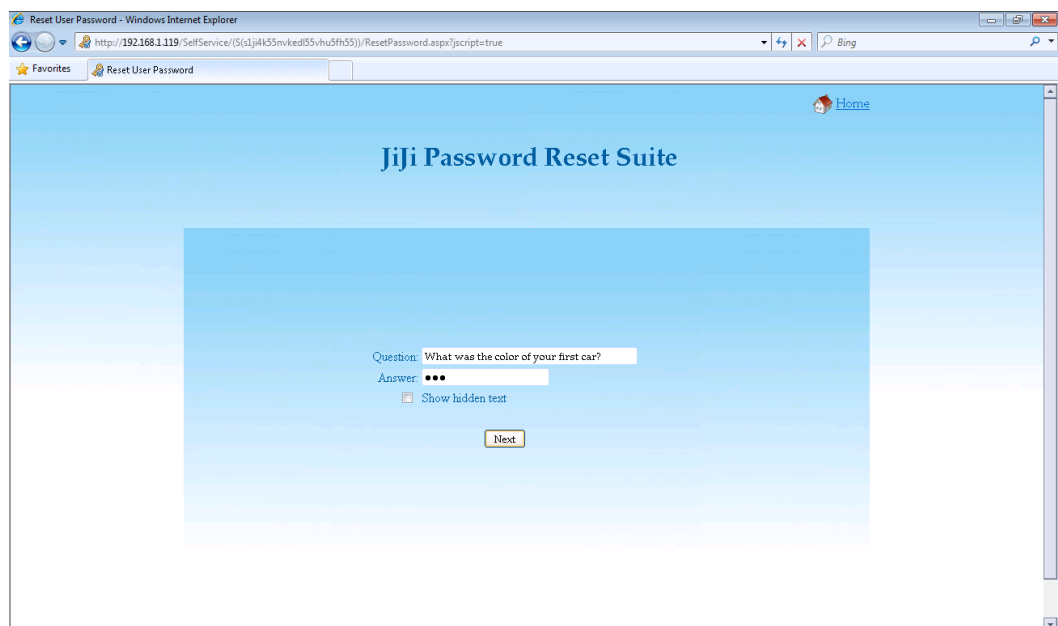
- If you forget your password and if you need to reset it, follow the given steps.
- Open Self Service Web. Click on the '**Reset Password**' option.
- Enter username and click '**Next**'.

Figure 1.89.



- Answer all the previously enrolled questions.

Figure 1.90.



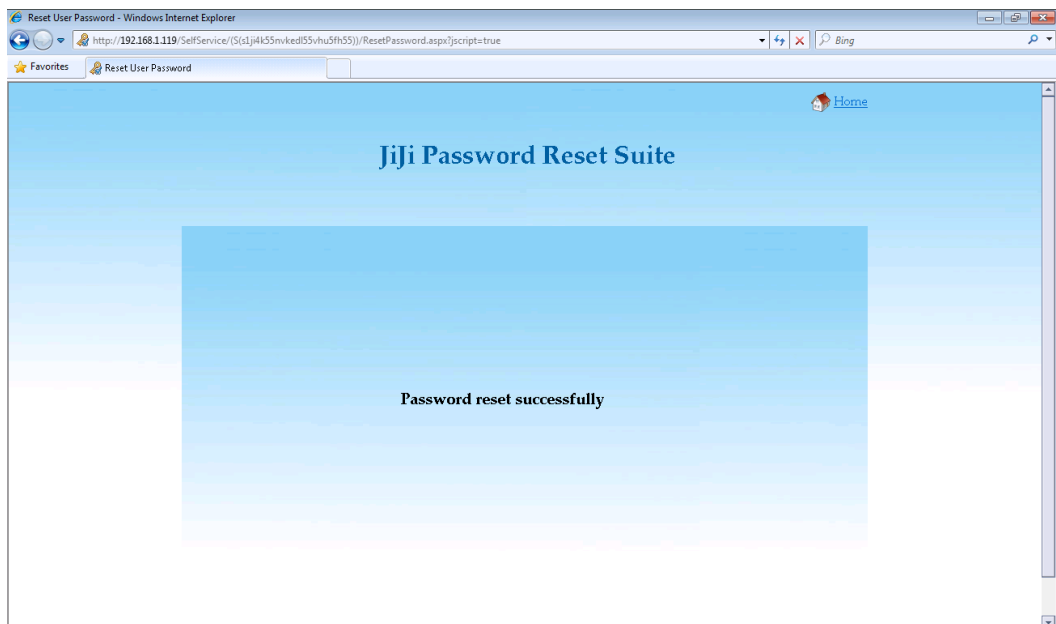
- Enter new password and code.

Figure 1.91.



- Click '**Reset**' button to reset your password successfully.

Figure 1.92.

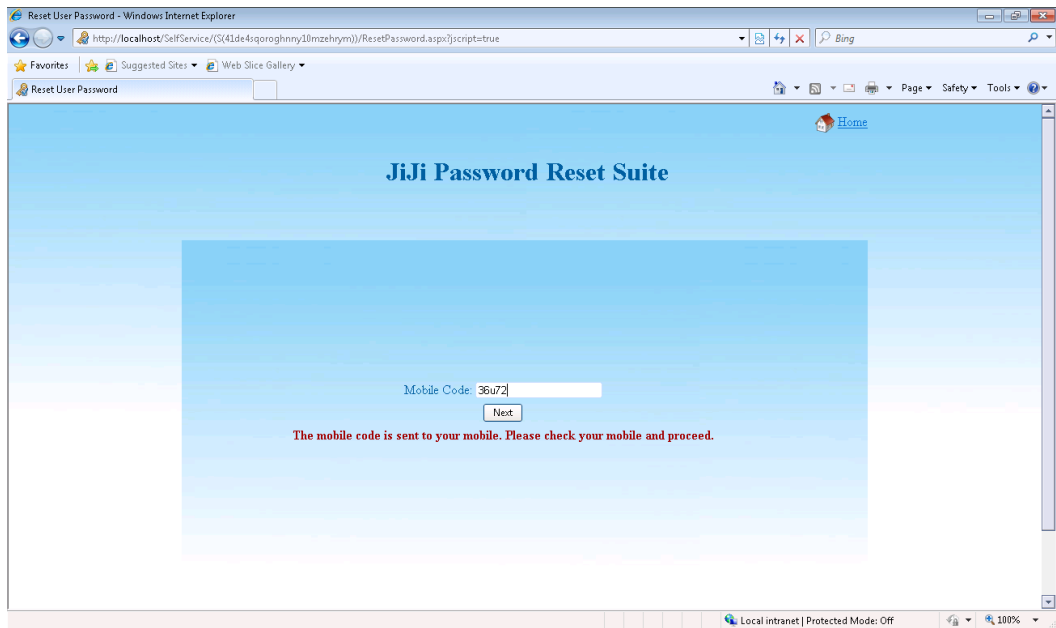


Reset Password using Mobile Code Verification

Administrator can enable two-way authentication by allowing users to enter the Mobile Code to reset their passwords.

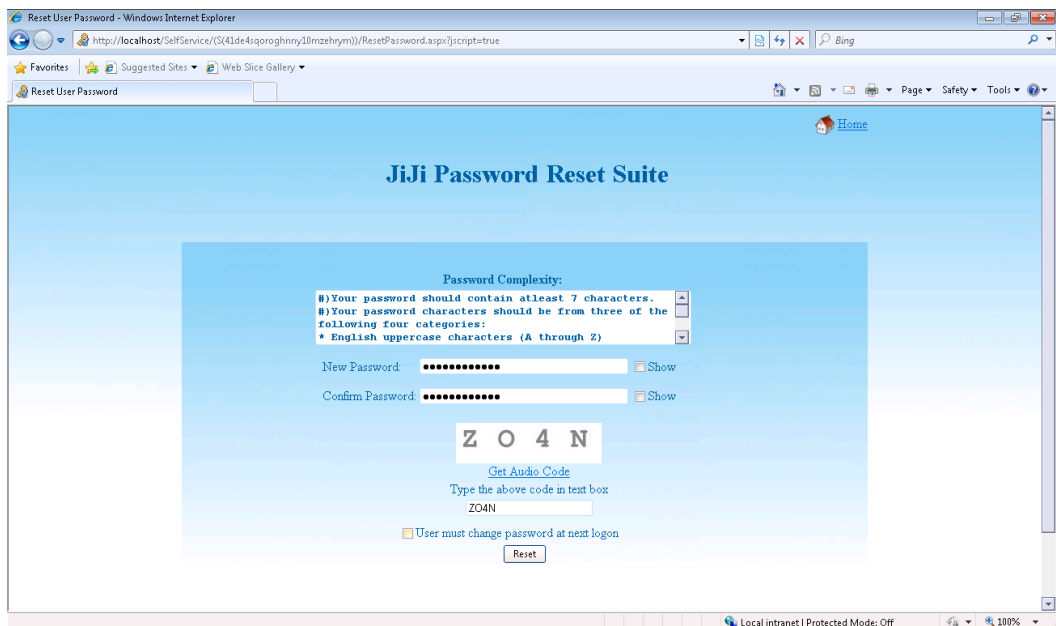
- After answering the security answers correctly, enter the secret code received through the mobile and click '**Next**'.

Figure 1.93.



- Enter the new password and click 'Reset' button.

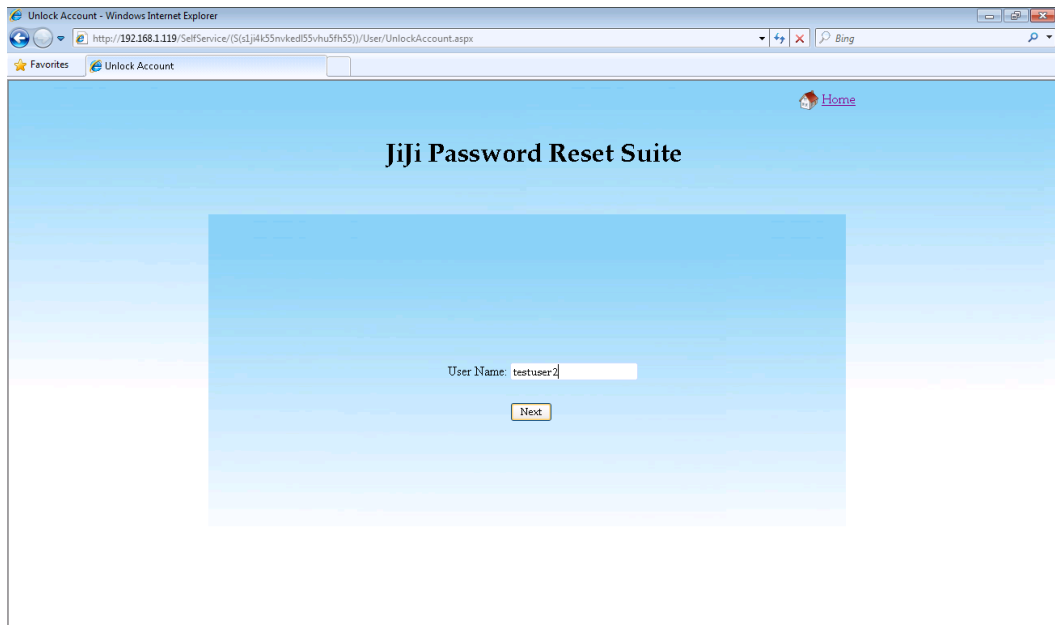
Figure 1.94.



Unlock Account

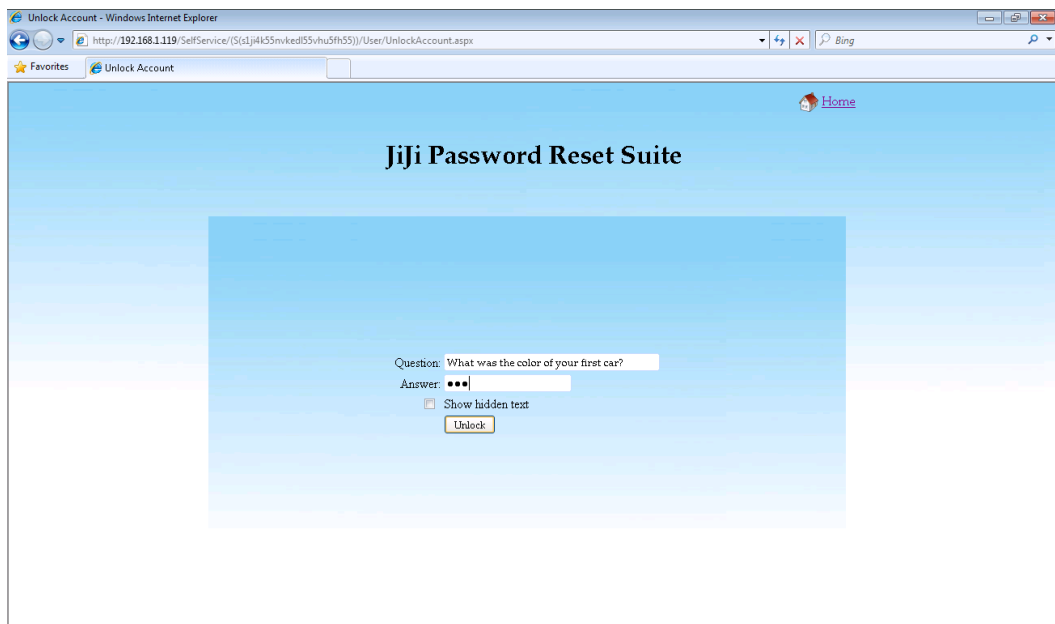
- Open Self Service Web. Click on the 'Unlock Account' option.
- Enter username and click 'Next'.

Figure 1.95.



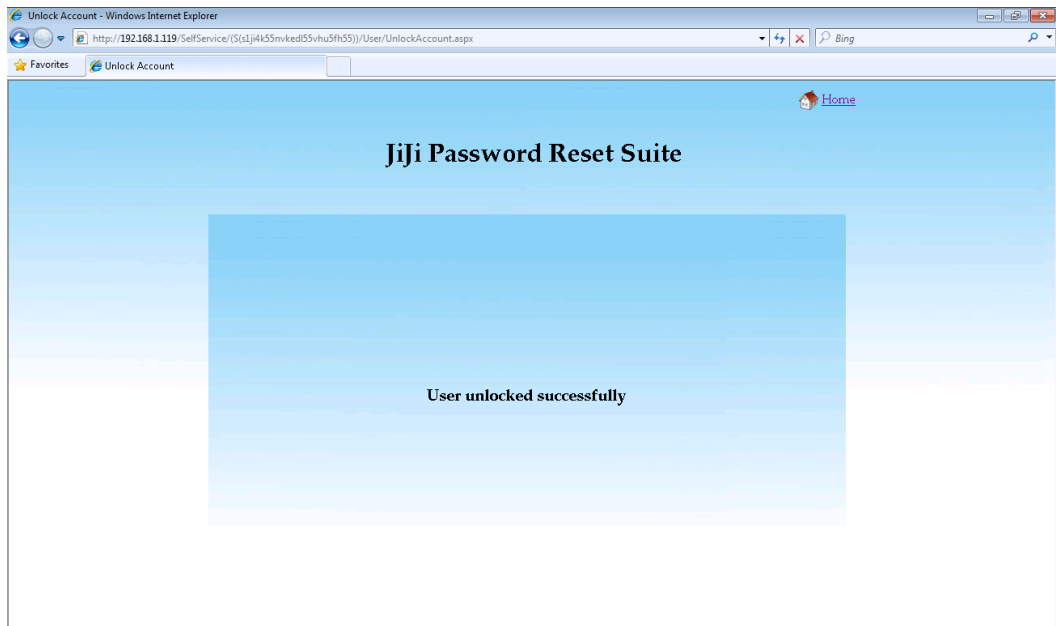
- Answer all the previously enrolled questions.

Figure 1.96.



- Click '**Unlock**' button to unlock successfully.

Figure 1.97.



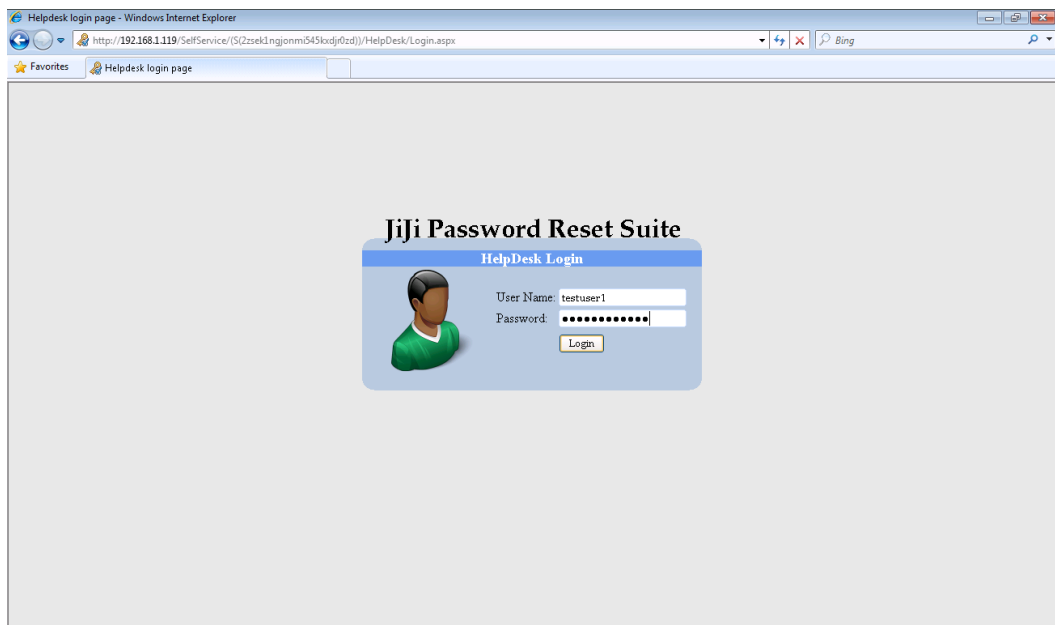
Chapter 7. WORKING WITH HELP DESK WEB

Help desk staffs have the permissions to reset users password and reset the locked out account . They can perform these operations for users those who were managed by them.

Reset Password

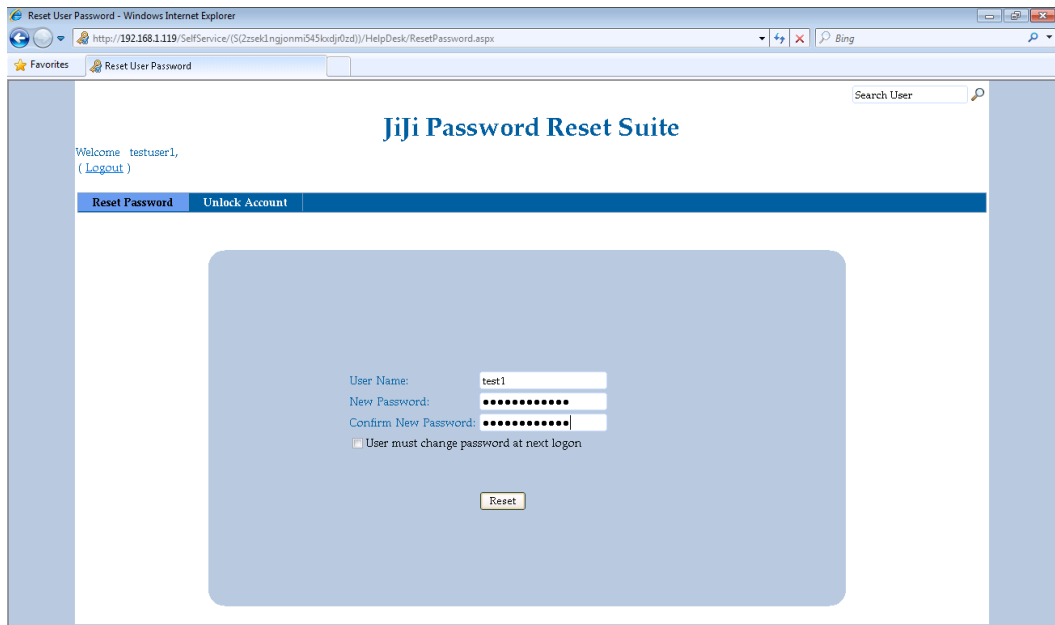
- Open Help Desk Web home page. Start -> Programs -> JiJi Technologies -> JiJi Password Reset Suite -> Web Client -> Help Desk Web.
- A loginpage for help desk will be opened.

Figure 1.98.



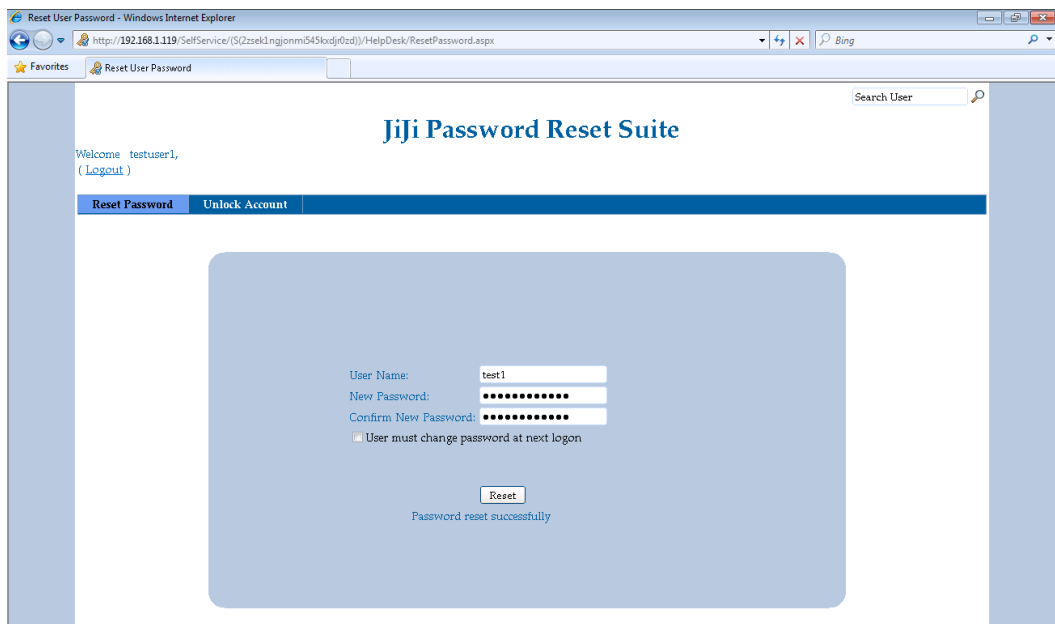
- Login and click '**Reset Password**' tab.
- Enter user name whose password is to be reset, new password and then click '**Reset**' button.

Figure 1.99.



- Now the password is reset successfully.

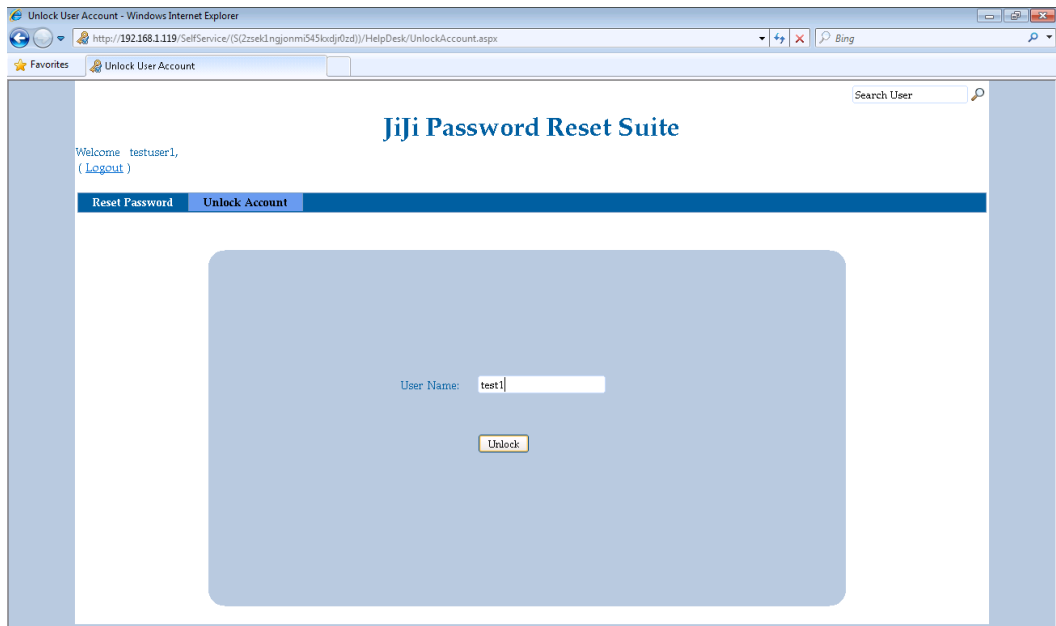
Figure 1.100.



UNLOCK ACCOUNT

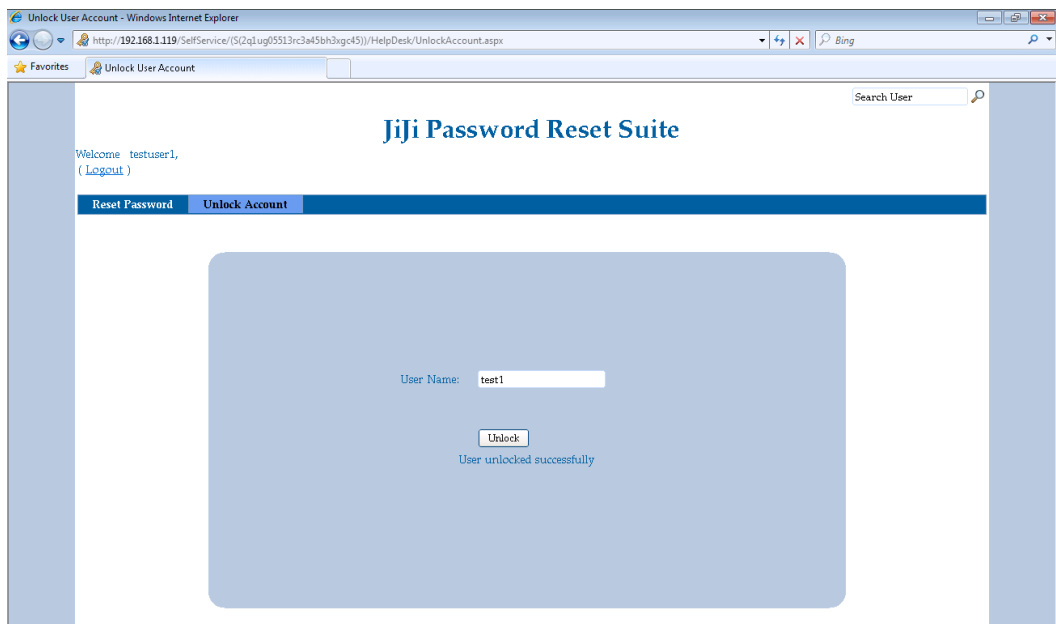
- Click 'Unlock Account' tab.
- Enter user name who requested to unlock the account.

Figure 1.101.



- Click 'Unlock' button to unlock it successfully.

Figure 1.102.



Chapter 8. LICENSE REGISTRATION

Features will vary for different types of licenses. Following types of licenses are available for JPRS.

- **Help Desk Standard**- Features such as schedule, general reports, mail server settings are not available in this license.
- **Help Desk Professional**- All features related to help desk are available.
- **Self Service Starter**- Agent installation, schedule, general reports are not available.
- **Self Service Standard**- Agent installation feature is not available in this type of license.
- **Self Service Professional**- All features related to self service are available.
- **Combo**- All features of both self service and help desk are available.
- **Combo Basic**-Features of both self service and help desk are available except agent installation.