Dovestones Software

AD Self Password Reset

Installation and configuration

Manual v3.0

CONTENTS

1 INTRODUCTION

Users forgetting their passwords is a common headache for IT departments. AD Self Password Reset allows your users to safely reset their own password without calling the IT helpdesk.

AD Self Password Reset includes a number of ways to help reduce the pain of forgotten passwords and locked out users.

Password Expiry Reminder emails prompt users to change their password before it expires which can help to reduce the number of locked out users.

Should users forget their password Users can reset it by answering a number of questions or receiving a reset code via SMS message to their mobile.

We've added a number of other useful features, one such feature is 'Helpdesk'. This allows the 'Helpdesk Group' to reset the passwords of the 'Managed Users Group'. An ideal scenario for this is teachers being given the ability to reset their students' passwords right there in the classroom, no need to call the helpdesk.

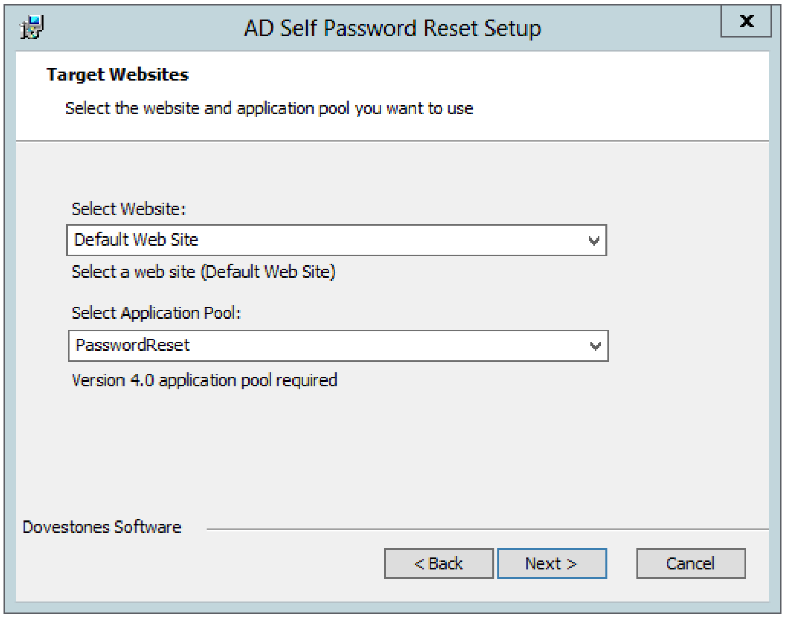
Thanks to your feedback we're improving AD Self Password Reset all the time, please keep your feedback coming.

1.1 Installation

Step 1 Double click the ADSelfPasswordResetSetup Installer

Step 2 Begin the installation. Click Next >

Step 3 Select the website where you want to install AD Self Password Reset, the Application will be installed in a sub-folder of the web site (e.g. C:\intepub\wwwroot\PasswordReset). Then select an Application Pool for the program to use or type the name PasswordReset. Click Next.



AD Self Password Reset Setup

Target Websites

Select the website and application pool you want to use

Select Website: Default Web Site

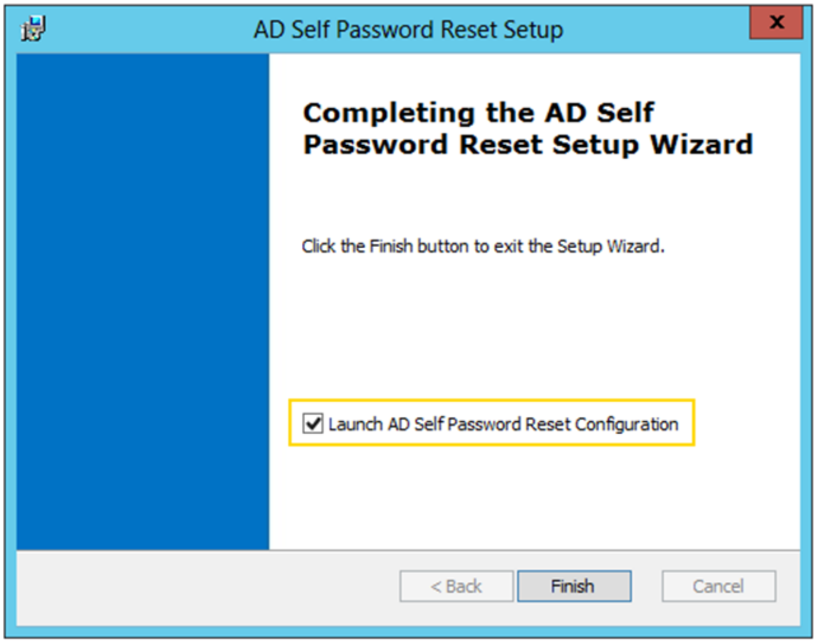
Select a web site (Default Web Site)

Select Application Pool: PasswordReset

Version 4.0 application pool required

Dovestones Software

Step 4 At the end of the installation wizard choose 'Launch AD Self Password Reset Configuration' to run the Configuration exe.



AD Self Password Reset Setup

Completing the AD Self Password Reset Setup Wizard

Click the Finish button to exit the Setup Wizard.

☑ Launch AD Self Password Reset Configuration

Step 5 Finally click Finish

1.2 Removal

To remove the program, follow the steps below.

Step 1 Go to Add/Remove Programs (Settings > Control Panel)

Step 2 In the list of currently installed programs locate AD Self Password Reset

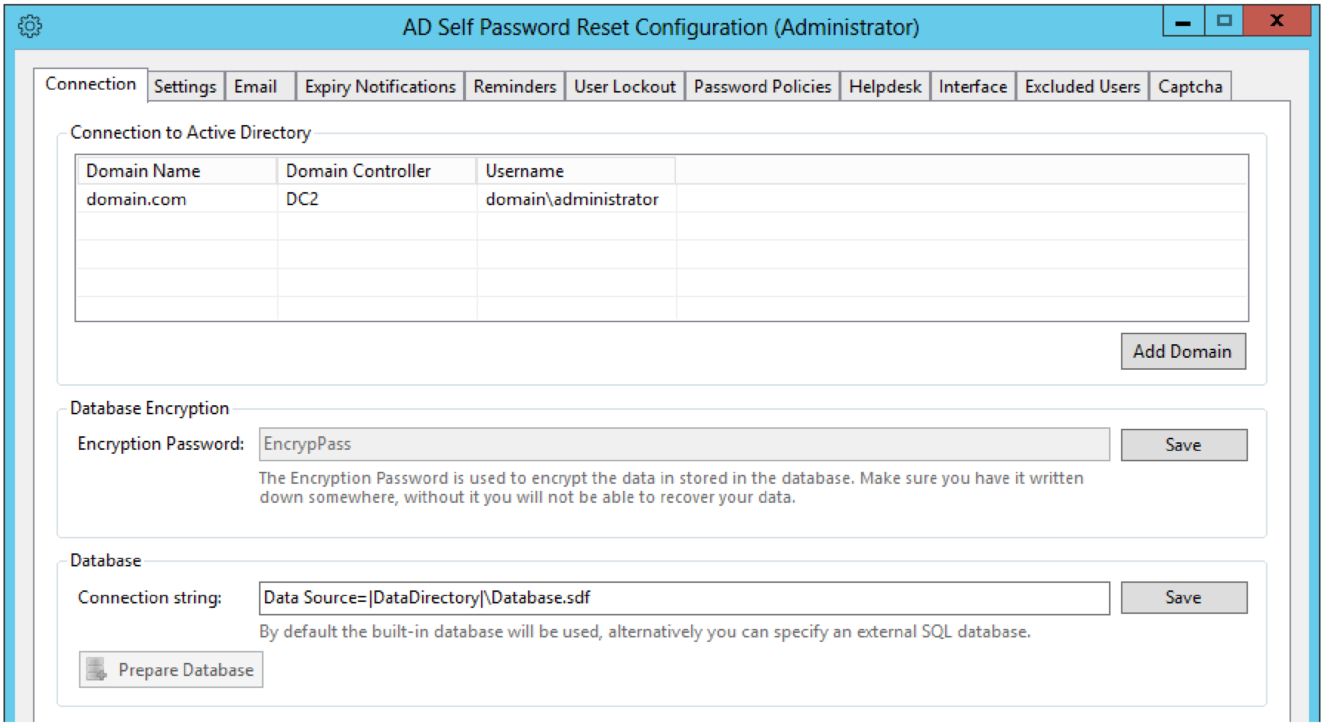
Step 3 Click the Remove button on the right.

1.3 Initial Configuration

Before the application can be used it needs to be configured. To do this follow the steps below.

Step 1 Run the AD Self Password Reset Configuration program

Step 2 When the Configuration program opens click the 'Add Domain' button, then enter a username and password from here add a user account that has permission to reset user passwords. Click Test to confirm a successful connection to Active Directory. Then click OK. If you receive a 'Access Denied' error message try running the Configuration program using 'Run As Administrator'.



Domain Name	Domain Controller	Username
domain.com	DC2	domain\administrator

Encryption Password: EncrypPass

The Encryption Password is used to encrypt the data in stored in the database. Make sure you have it written down somewhere, without it you will not be able to recover your data.

Connection string: Data Source=|DataDirectory|\Database.sdf

By default the built-in database will be used, alternatively you can specify an external SQL database.

1.4 Database Encryption

On the Connection tab in the 'Database Encryption' text box enter a password that will be used to encrypt the data stored in the database then click Save. Make a note of this password somewhere secure as should you need to recover the database you will need it.

1.5 Database Connection

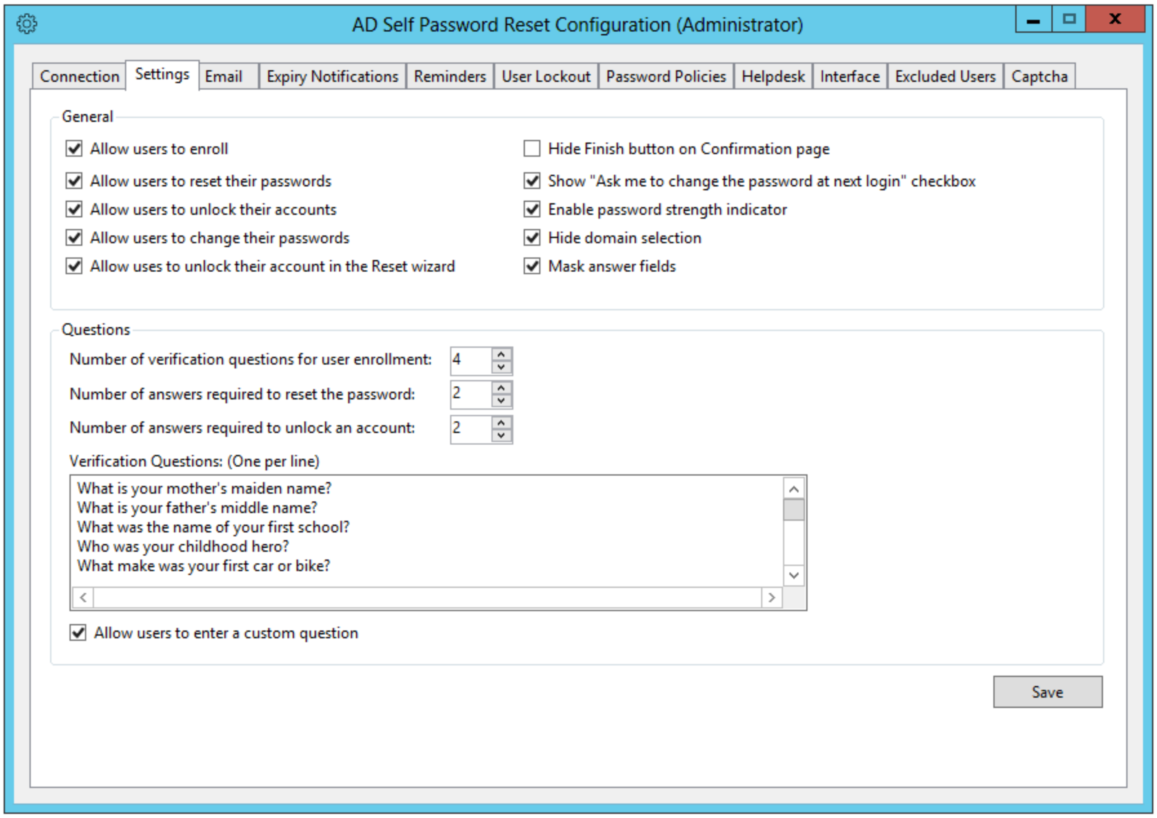
By default, the program will use the built-in SQL Compact database, should you want to use an external SQL server then enter the connection string into the 'Connection string' text box and click Save. To prepare the external SQL database click the ‘Prepare Database’ button the program will then create the necessary tables.

Initial configuration is now complete; you can continue to configure the program or perform some initial tests by going to the URL where the program is installed e.g. http://server/PasswordReset.

2 SETTINGS

2.1 General

Unchecking options in the General section (see below) will disable these specific features from the application. For example, unchecking ‘Allow users to unlock their accounts’ will remove this option from users.



General

☑ Allow users to enroll
☑ Allow users to reset their passwords
☑ Allow users to unlock their accounts
☑ Allow users to change their passwords
☑ Allow uses to unlock their account in the Reset wizard

□ Hide Finish button on Confirmation page
☑ Show "Ask me to change the password at next login" checkbox
☑ Enable password strength indicator
☑ Hide domain selection
☑ Mask answer fields

Questions

Number of verification questions for user enrollment: 4
Number of answers required to reset the password: 2
Number of answers required to unlock an account: 2

Verification Questions: (One per line)

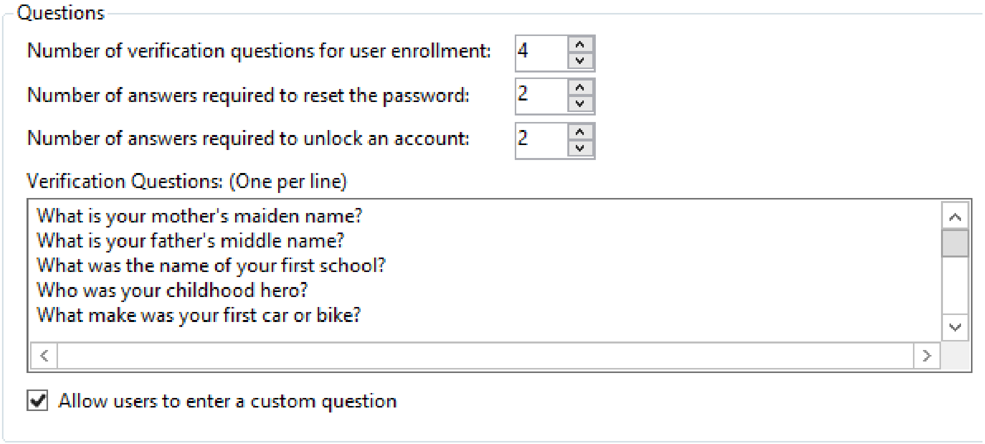
What is your mother's maiden name?
What is your father's middle name?
What was the name of your first school?
Who was your childhood hero?
What make was your first car or bike?

☑ Allow users to enter a custom question

2.2 Questions Group

You can specify how many questions your users will be asked during enrolment and how many questions they will need to answer to reset/change their password. You can add your own or remove the default questions.

Note the option 'Allow users to enter a custom question', this allows users to create their own question.



Questions

Number of verification questions for user enrollment: 4

Number of answers required to reset the password: 2

Number of answers required to unlock an account: 2

Verification Questions: (One per line)

What is your mother's maiden name?
What is your father's middle name?
What was the name of your first school?
Who was your childhood hero?
What make was your first car or bike?

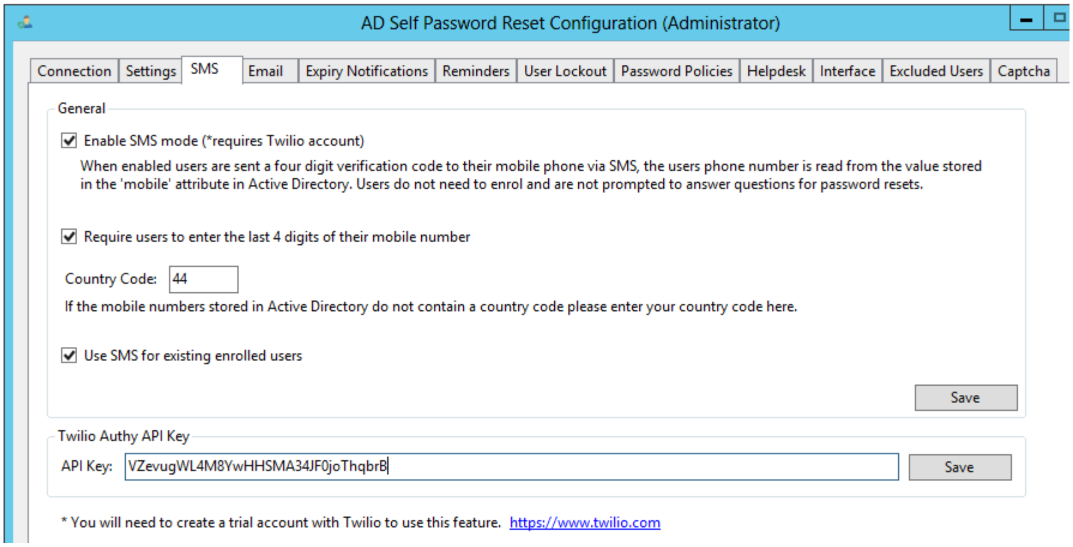
☑ Allow users to enter a custom question

2.3 Choosing Questions

Pay close attention to the type of questions the users can choose, take care not to choose questions were the information is easily learned, for example asking, 'Where do you live?' could be easily learned. A more secure question to ask would be 'Where did your parents meet' as this could be a city or an event etc. Allowing the user to create their question can add security as the user may ask a question only they could ever know the answer to. The user is limited to creating just 1 question to ensure they don't create easily guessable questions.

2.3 SMS

The SMS mode allows users to reset their password without the need to enroll. If the user has a mobile number stored in the 'Mobile' field in Active Directory then when the user goes to Reset their password a message is sent to their mobile containing a password reset code. The user is prompted to enter the code, if the correct code is entered the user can reset their password.



AD Self Password Reset Configuration (Administrator)

General

☑ Enable SMS mode (*requires Twilio account)

When enabled users are sent a four digit verification code to their mobile phone via SMS, the users phone number is read from the value stored in the 'mobile' attribute in Active Directory. Users do not need to enrol and are not prompted to answer questions for password resets.

☑ Require users to enter the last 4 digits of their mobile number

Country Code: 44

If the mobile numbers stored in Active Directory do not contain a country code please enter your country code here.

☑ Use SMS for existing enrolled users

Twilio Authy API Key

API Key: VZevugWL4M8YwHHSMA34JF0joThqbrB

* You will need to create a trial account with Twilio to use this feature. https://www.twilio.com

Require users to enter the last 4 digits of their mobile number

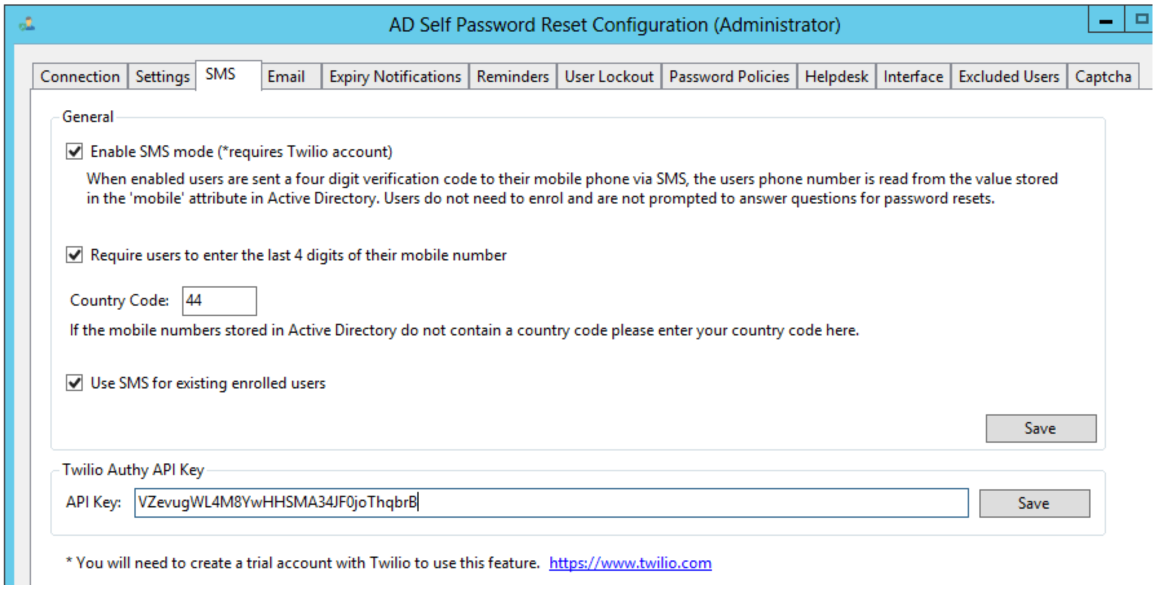
When the option ‘Require users to enter the last 4 digits of their mobile number’ is checked users will be asked to confirm the last 4 digits of their mobile number before they can proceed.

Country Code

If the users mobile number stored in Active Directory does not contain a country code then you can enter a country code here.

Use SMS for existing enrolled users

The option ‘Use SMS for existing enrolled users’ will force all enrolled users to use SMS rather than answering questions. This is ideal for customers who already have enrolled users and want to switch to SMS only. If the option is unchecked enrolled users will be asked to answer questions when they click Reset and new users who have a mobile number stored in Active Directory will use SMS. This helps if you want some users to use questions/answers (if they don’t have a mobile) and you want some users to use SMS (they don’t need to enroll).



General

☑ Enable SMS mode (*requires Twilio account)

When enabled users are sent a four digit verification code to their mobile phone via SMS, the users phone number is read from the value stored in the 'mobile' attribute in Active Directory. Users do not need to enrol and are not prompted to answer questions for password resets.

☑ Require users to enter the last 4 digits of their mobile number

Country Code: 44

If the mobile numbers stored in Active Directory do not contain a country code please enter your country code here.

☑ Use SMS for existing enrolled users

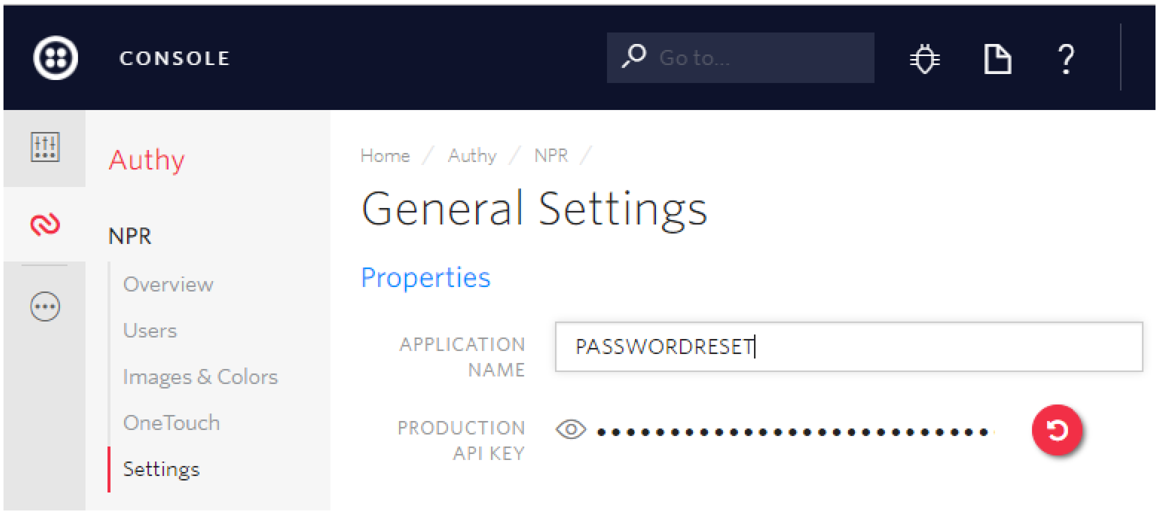
Twilio Authy API Key

API Key: VZevugWL4M8YwHHSMA34JF0joThqbrB

* You will need to create a trial account with Twilio to use this feature. https://www.twilio.com

Twilio Authy API Key

To send SMS messages the program requires a Twilio Authy API Key which can be obtained from https://twilio.com. Twilio offer a trial to all customers who sign up, which includes a free balance for you to experiment with. Getting a Twilio API key is straight forward, simply register with Twilio, once registered locate Authy in the menu and add an 'Application', give the application a friendly name such as PasswordReset then copy the API Key from the Settings section of the Application you created and paste it into the API Key text box on the SMS tab.



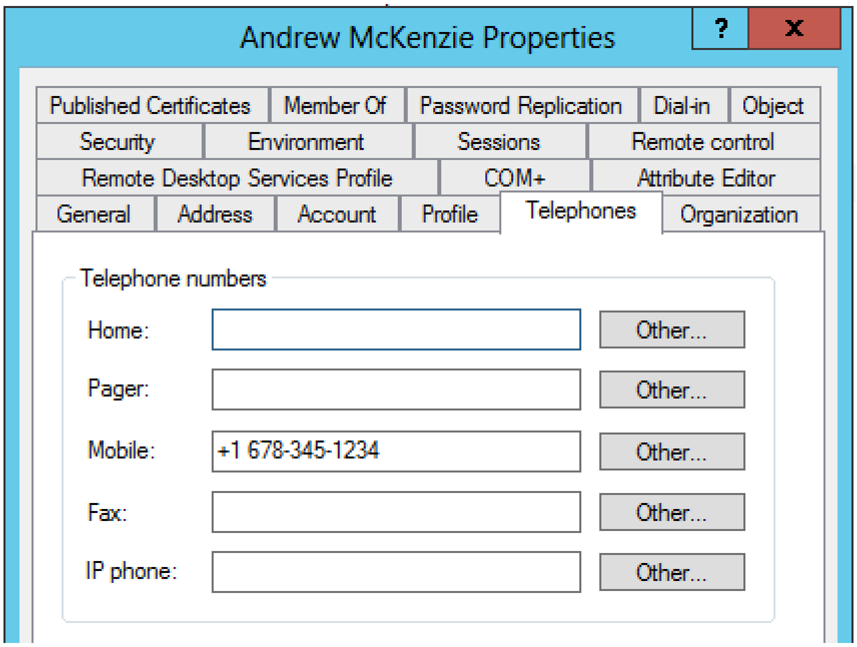
General Settings

Properties

APPLICATION NAME: PASSWORDRESET

PRODUCTION API KEY: ••••••••••••••••••••••••••

The Active Directory user below has a value in the mobile field.



Telephone numbers

Home:

Pager:

Mobile: +1 678-345-1234

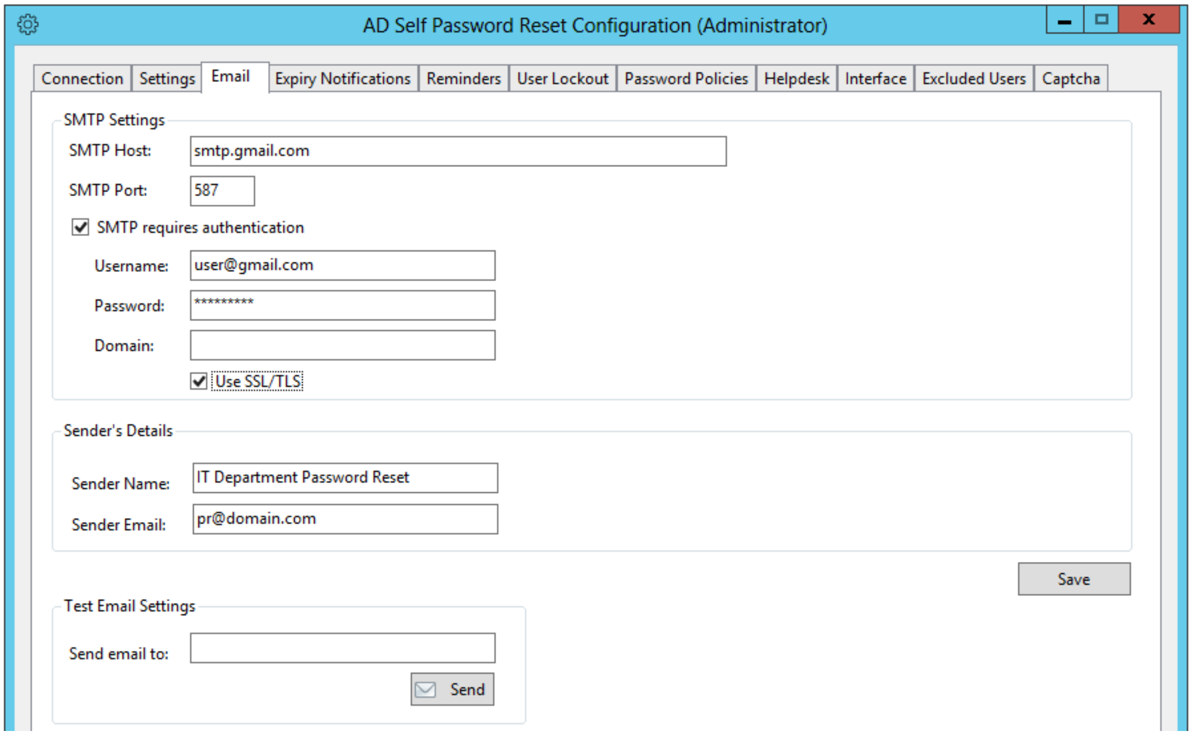
Fax:

IP phone:

3 EMAIL

The Email tab is used to configure how the program will send emails, emails are sent when a user enrolls, resets their password or their password is due to expire and also to remind users to enroll (via the admin page).

Enter the details of your mail server, the mail server, the example below is using gmail but this could be your local Exchange server or Office 365.



AD Self Password Reset Configuration (Administrator)

SMTP Settings

SMTP Host: smtp.gmail.com

SMTP Port: 587

☑ SMTP requires authentication

Username: user@gmail.com

Password: *********

Domain:

☑ Use SSL/TLS

Sender's Details

Sender Name: IT Department Password Reset

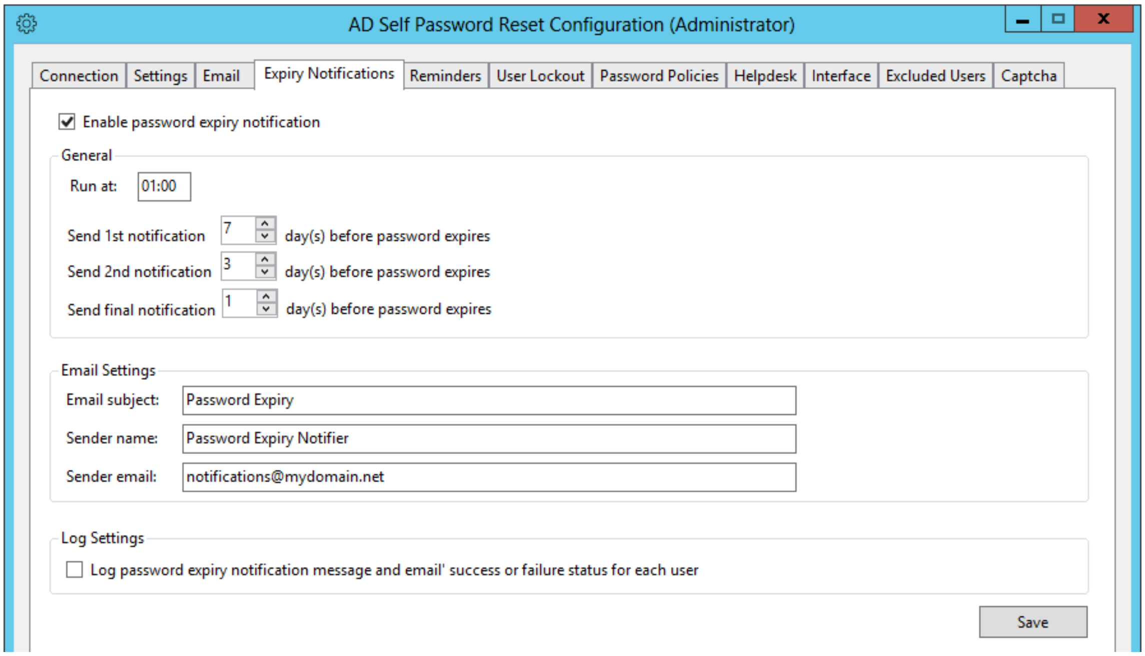
Sender Email: pr@domain.com

Test Email Settings

Send email to:

4.1 Expiry Notifications

On the Expiry Notifications tab you can enable or disable the password expiry notifications. When a user's password is due to expire they can be notified via email, this may prevent them from forgetting their password in the first place. When the password reminder email is sent out the user can click a link to password reset home page to change their password (email templates can be customized). You can choose how frequently to notify users of that their password will expire.



AD Self Password Reset Configuration (Administrator)

☑ Enable password expiry notification

General

Run at: 01:00

Send 1st notification 7 day(s) before password expires

Send 2nd notification 3 day(s) before password expires

Send final notification 1 day(s) before password expires

Email Settings

Email subject: Password Expiry

Sender name: Password Expiry Notifier

Sender email: notifications@mydomain.net

Log Settings

☐ Log password expiry notification message and email' success or failure status for each user

4.2 Reminders

Via the admin page (http://localhost/passwordreset/admin) you are can see who and who hasn’t enrolled. You can also send users an email reminding them to enroll. Note the admin page can only be accessed via a URL that contains the sever name or IP address (http://localhost/.., http://sever/.., http://10.0.0.5/..).

4.3 User Lockout

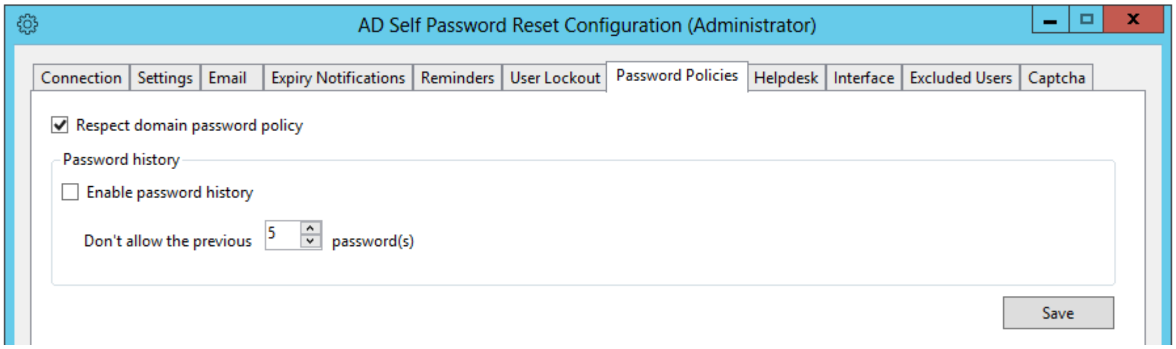
Should a user repeatedly provide incorrect answers the program can prevent further attempts at guessing the answers by locking the user for a specified amount of time. On the User Lockout tab you specify how many failed attempts would prevent access and how soon they are allowed to try again. To prevent scripts being run to gain access use Captcha tab.

4.4 Password Policies

By default the program will ensure passwords being set conform to the domain password policy, you can disable this check should you need to on this tab.

To prevent users using the same password continuously you can enable the password history feature. This forces the user to choose a different password each time.

To prevent users using the same password continuously you can enable the password history feature. This forces the user to choose a different password each time.



☑ Respect domain password policy

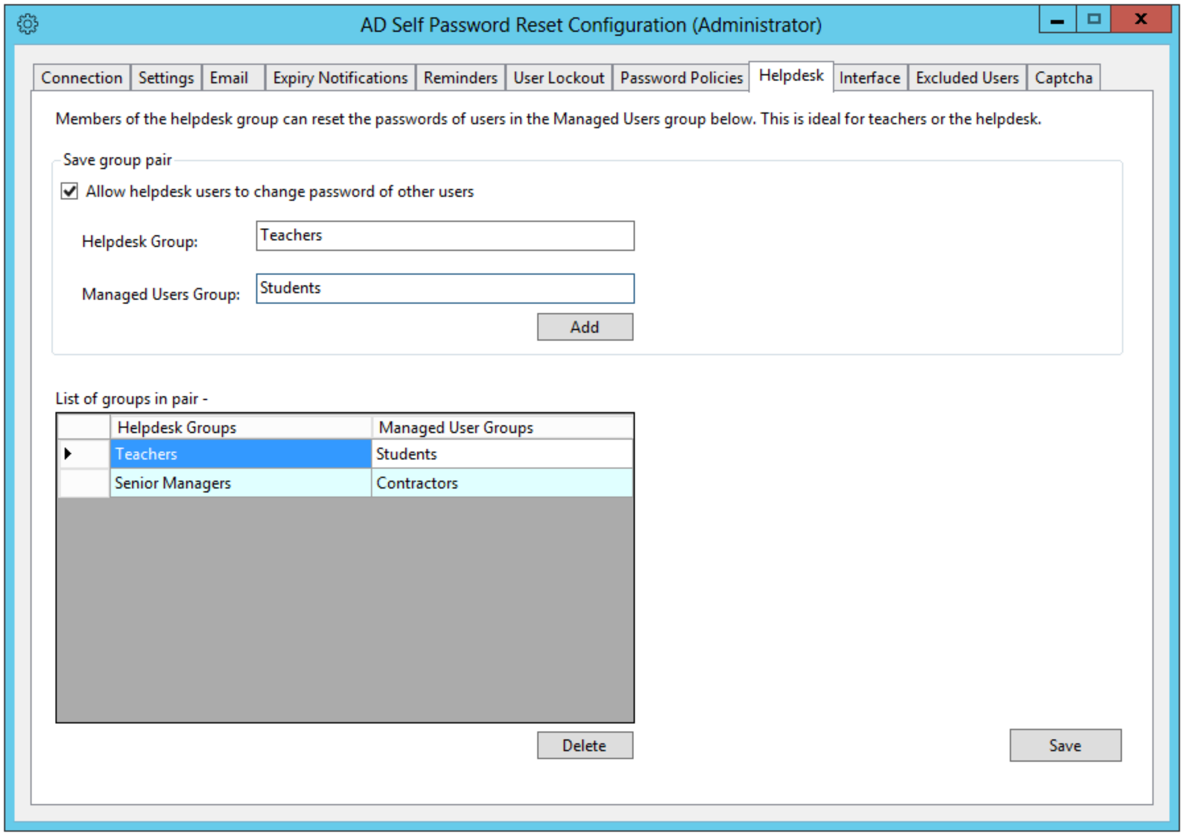
Password history

□ Enable password history

Don't allow the previous 5 password(s)

4.5 Helpdesk

You can allow a specified group of users the ability to change the password of another group of users. The feature is ideal for teachers as they can reset student’s passwords so there is no need for students to enroll or call the IT department, students don’t need to be enrolled for the tutor to use this feature. It can also be used by Helpdesk staff so they don’t need to access Active Directory to reset passwords. To use this feature, add the name of both groups and click Add and then Save.



Members of the helpdesk group can reset the passwords of users in the Managed Users group below. This is ideal for teachers or the helpdesk.

Save group pair

☑ Allow helpdesk users to change password of other users

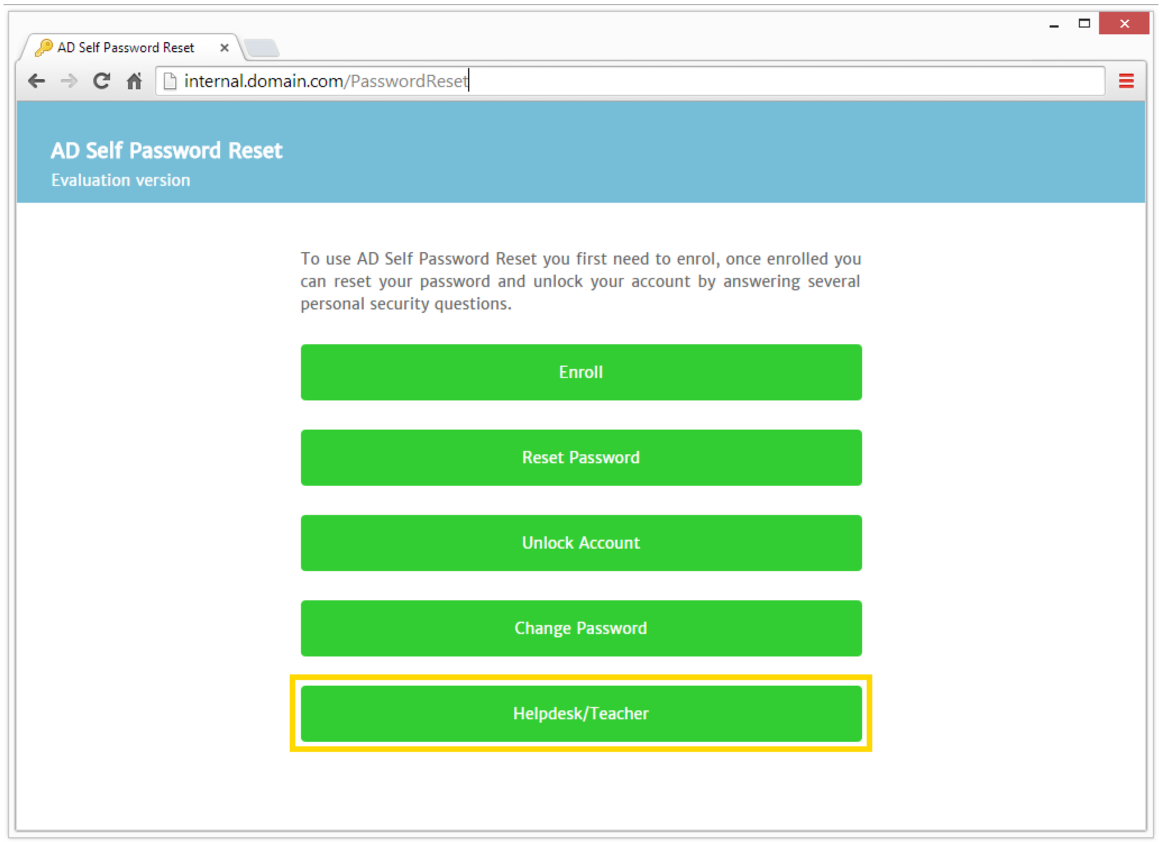
Helpdesk Group: Teachers

Managed Users Group: Students

List of groups in pair -

Helpdesk Groups	Managed User Groups
Teachers	Students
Senior Managers	Contractors

Enabling the Helpdesk feature will add a button to the main page, the Helpdesk/Teacher button can be used by members of the Helpdesk group, other users will be denied access. You can change the text shown on this button on the Interface tab.



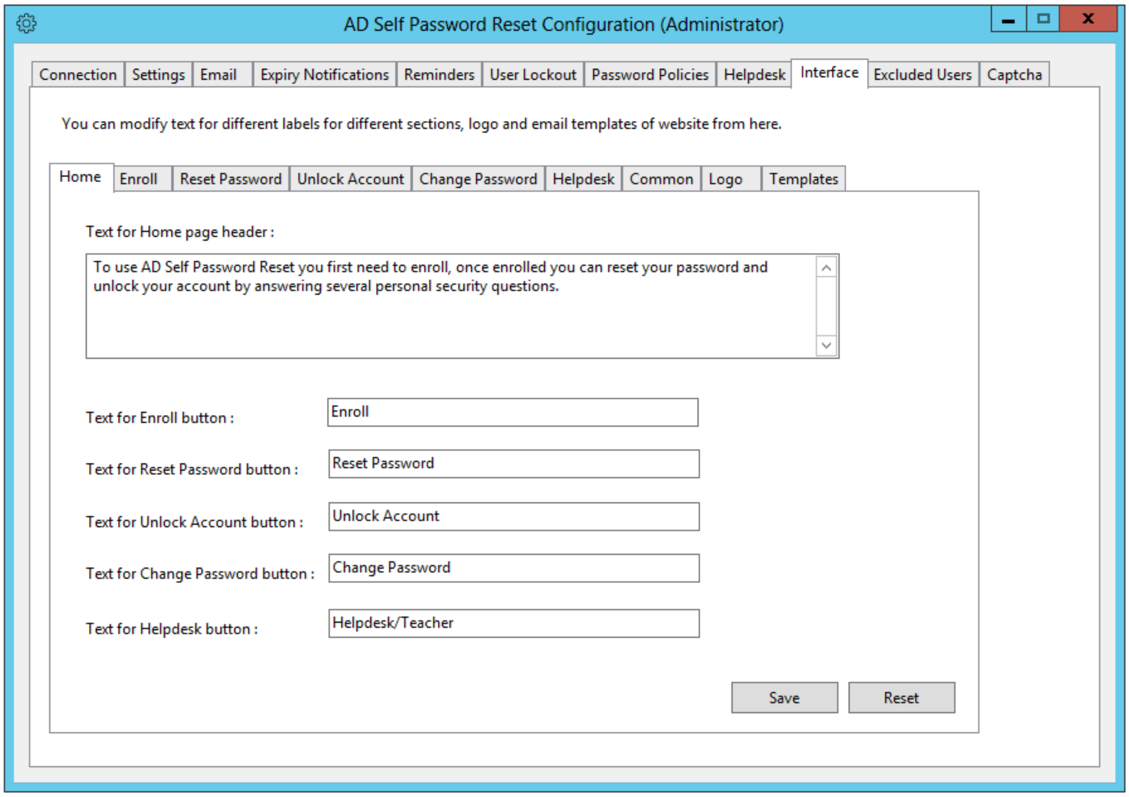
AD Self Password Reset

Evaluation version

To use AD Self Password Reset you first need to enrol, once enrolled you can reset your password and unlock your account by answering several personal security questions.

5 Interface

All the text seen by users can be changed on the Interface tab, you can also add a logo and change the colours used on the buttons and header. The logo should be 185px wide by 60px high and no larger than 30kb.



You can modify text for different labels for different sections, logo and email templates of website from here.

Text for Home page header : To use AD Self Password Reset you first need to enroll, once enrolled you can reset your password and unlock your account by answering several personal security questions.

Text for Enroll button : Enroll

Text for Reset Password button : Reset Password

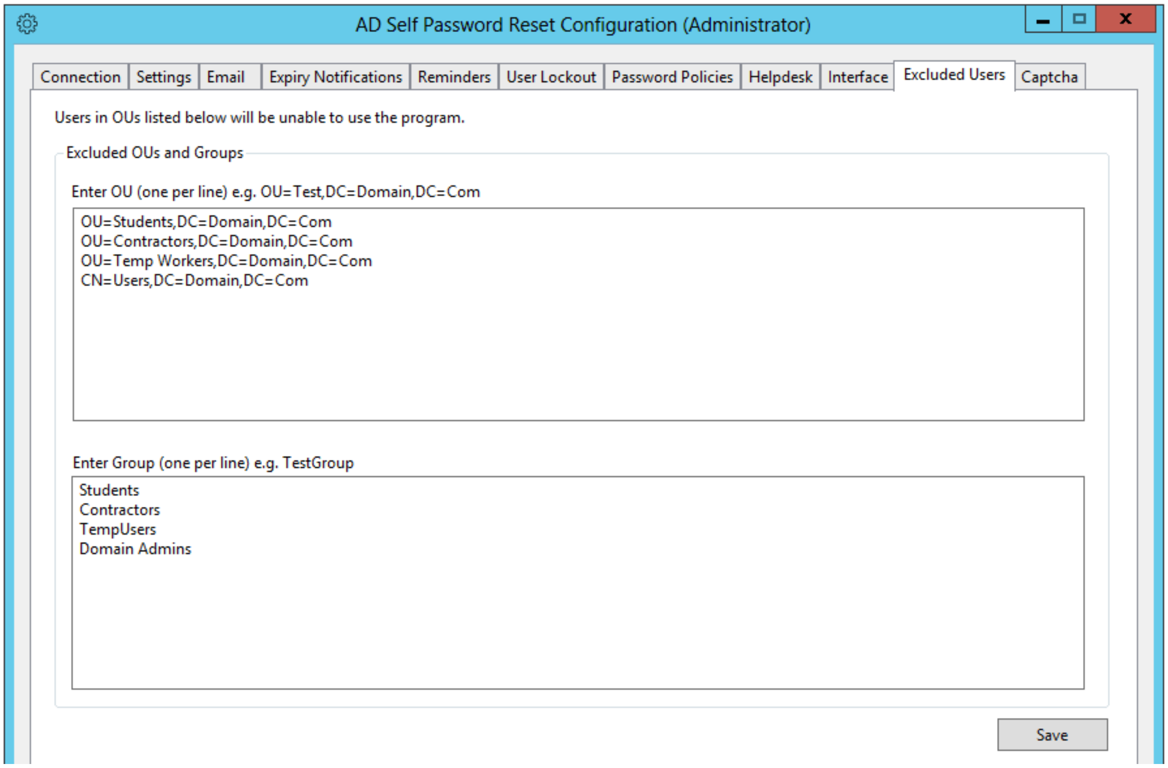
Text for Unlock Account button : Unlock Account

Text for Change Password button : Change Password

Text for Helpdesk button : Helpdesk/Teacher

5.1 Excluded Users

If you want to prevent selected users from using AD Self Password Reset then you can do this by adding Organization Units or groups to the Exclude tab. For example adding the organizational unit OU=Students,DC=Domain,DC=Com would prevent any users in the Students OU from using the program. Adding a group Students has the same effect.



Users in OUs listed below will be unable to use the program.

Excluded OUs and Groups

Enter OU (one per line) e.g. OU=Test,DC=Domain,DC=Com

```
OU=Students,DC=Domain,DC=Com
OU=Contractors,DC=Domain,DC=Com
OU=Temp Workers,DC=Domain,DC=Com
CN=Users,DC=Domain,DC=Com
```

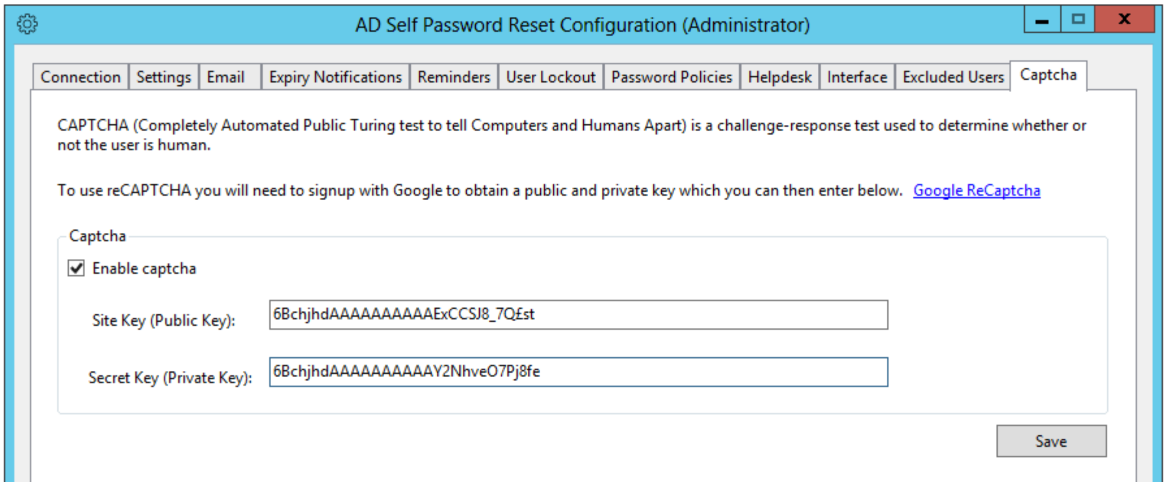
Enter Group (one per line) e.g. TestGroup

```
Students
Contractors
TempUsers
Domain Admins
```

5.1.1 Captcha

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a challenge-response test used to determine whether or not the user is human.

To use CAPTCHA you will first need to register with Google's free reCAPTCHA service to obtain a public and private key. After registration you need to the site address where users will access AD Self Password Reset e.g. http://internal.domain.com, you will then be given a public and private key, copy these keys and paste them into the corresponding text boxes and click Save.



CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a challenge-response test used to determine whether or not the user is human.

To use reCAPTCHA you will need to signup with Google to obtain a public and private key which you can then enter below. Google ReCaptcha

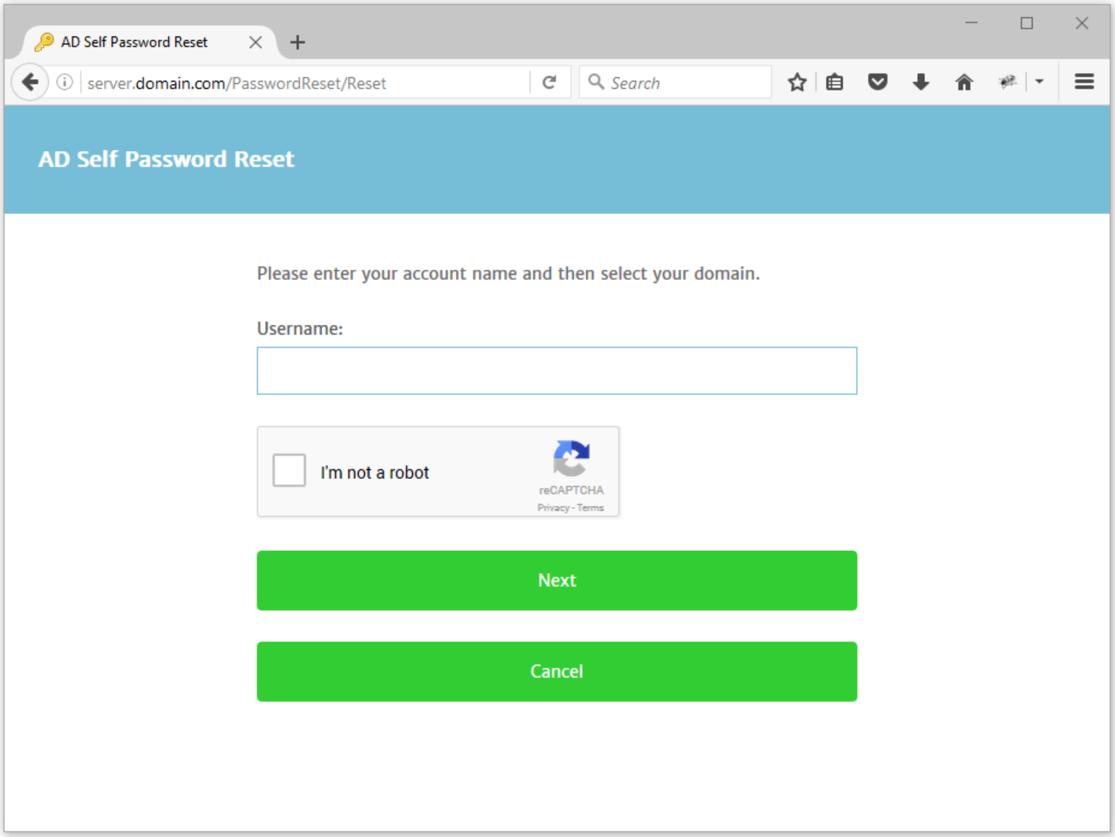
Captcha

☑ Enable captcha

Site Key (Public Key): 6BchjhdAAAAAAAAAAExCCSJ8_7Q£st

Secret Key (Private Key): 6BchjhdAAAAAAAAAAY2NhveO7Pj8fe

The CAPTCHA is shown when a user tries to reset their password or unlock their account. The CAPTCHA is shown before the user enters any details other than their username to ensure the user is human before attempts to answer questions are made.



AD Self Password Reset

Please enter your account name and then select your domain.

Username:

□ I'm not a robot

5.1.2 Enrollment

Unless SMS mode is enabled users will need to enroll before they can reset their passwords or unlock their accounts. Enrollment only takes a few minutes and involves entering their username and password to confirm the users identity and then answer a number of questions.

Which questions the user can choose from and how many they need to answer to enroll are defined by the administrator via the Configuration program (see Settings tab above).

Step 1

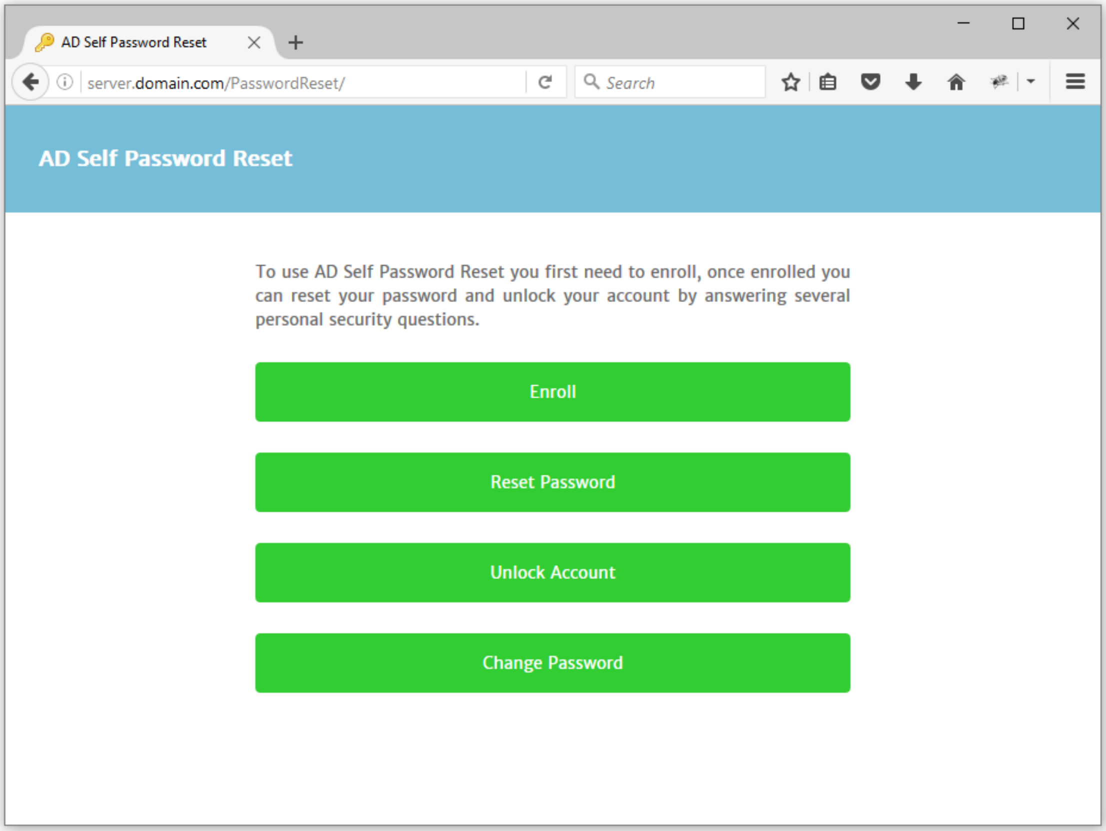
Open a web browser and navigate to

http://server/PasswordReset

http://10.0.0.1/PasswordReset

Step 2

To enroll a new user would click Enroll.

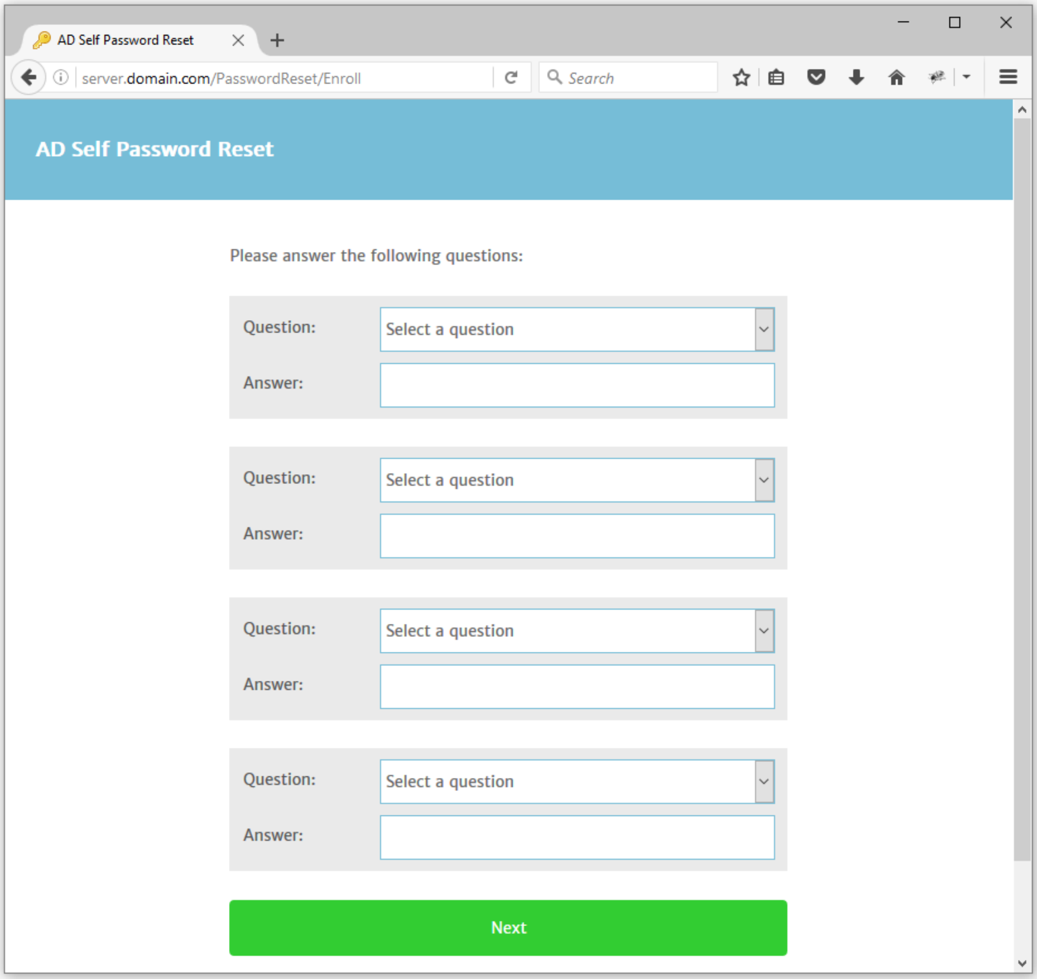


To use AD Self Password Reset you first need to enroll, once enrolled you can reset your password and unlock your account by answering several personal security questions.

Step 3

The user needs to answer a number of questions only they will know the answer to. The default is 4 questions this can be changed via the Settings tab in the Configuration program. On the Setting tab there is an option to allow users to create their own question, the option limits the user to creating just one custom question.

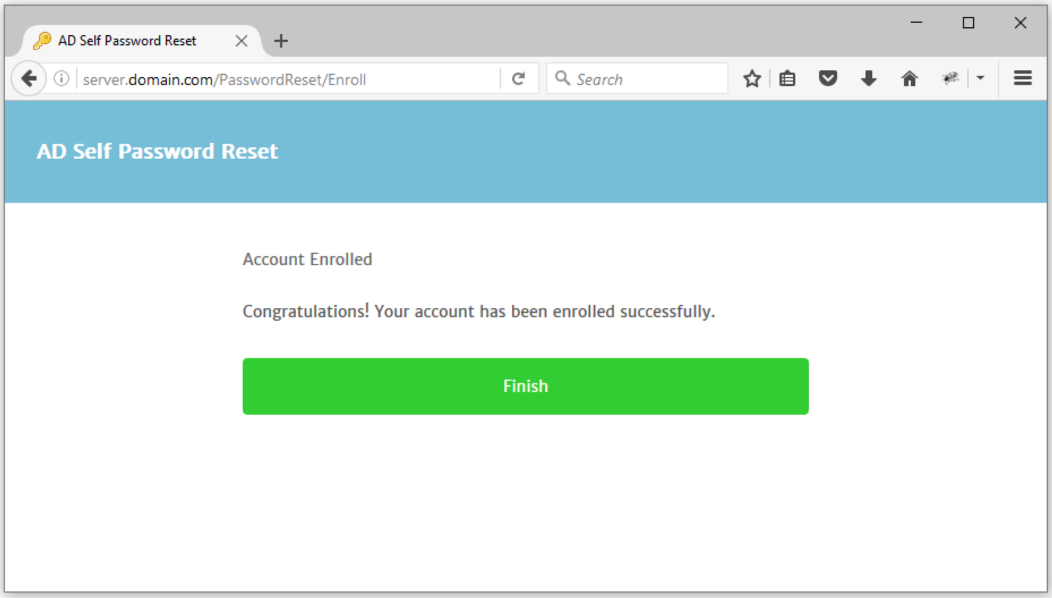
Each question and answer needs to be unique, after the user has successfully selected and answered each question clicking Next will complete the enrolment. The user is then able to reset and change their password at any time.



AD Self Password Reset

Please answer the following questions:

Question:	Select a question
Answer:	
Question:	Select a question
Answer:	
Question:	Select a question
Answer:	
Question:	Select a question
Answer:	



AD Self Password Reset

Account Enrolled

Congratulations! Your account has been enrolled successfully.

5.2 Reset Password

Step 1

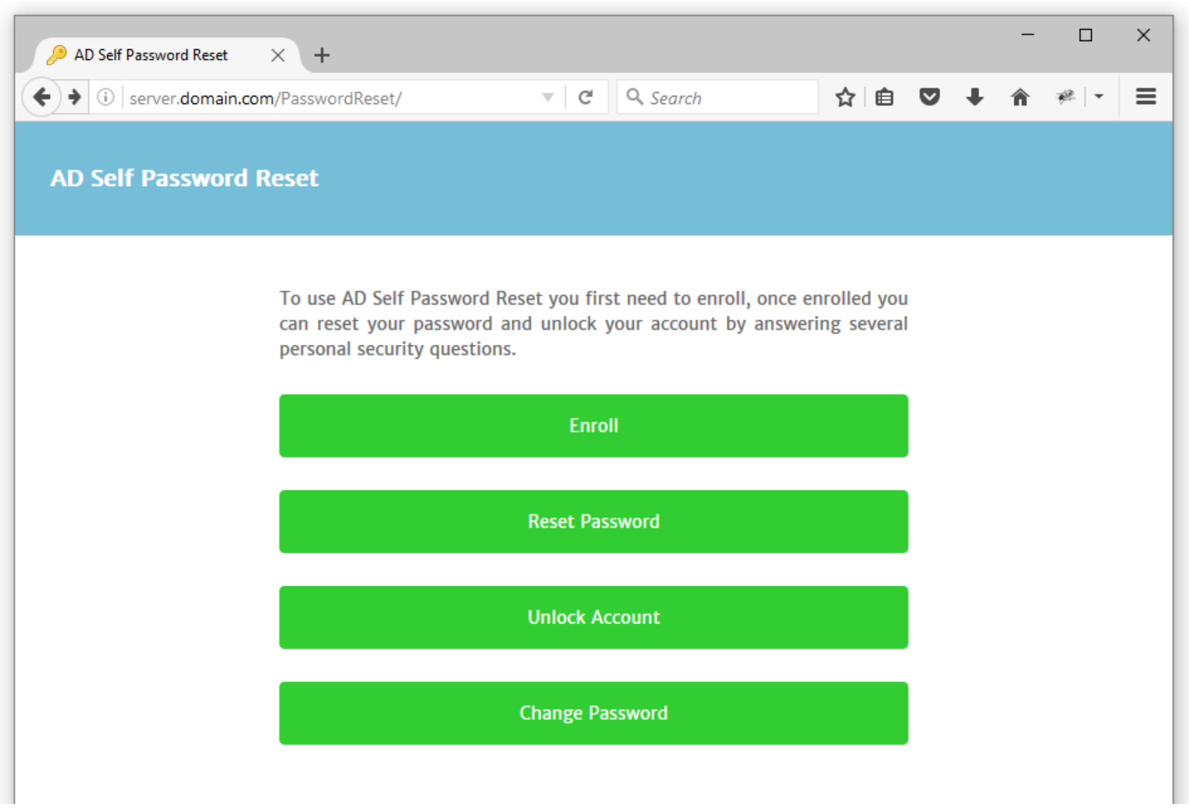
Open a web browser and navigate to

http://server/PasswordReset or

http://10.0.0.1/PasswordReset

Step 2

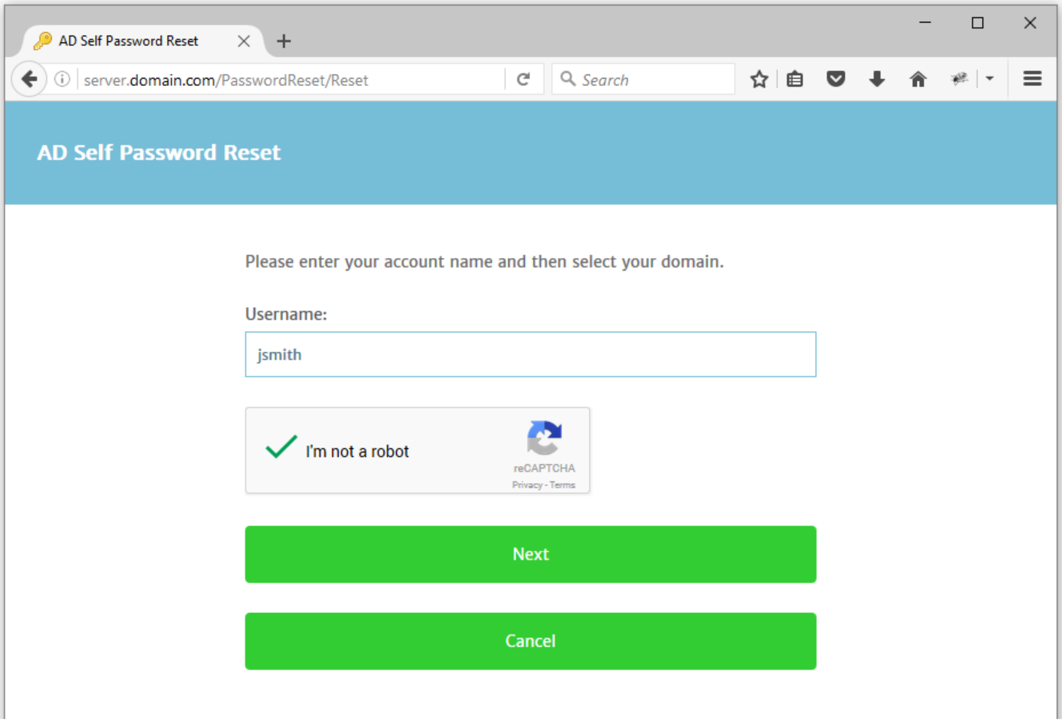
To reset a password, the user clicks the Reset Password button (the text can be changed via the Configuration program) or visits the URL http://server/passwordreset/reset.



To use AD Self Password Reset you first need to enroll, once enrolled you can reset your password and unlock your account by answering several personal security questions.

Step 3

The user then enters their username, if the Google Recaptcha has been enabled the user will need to pass the Recaptcha check.



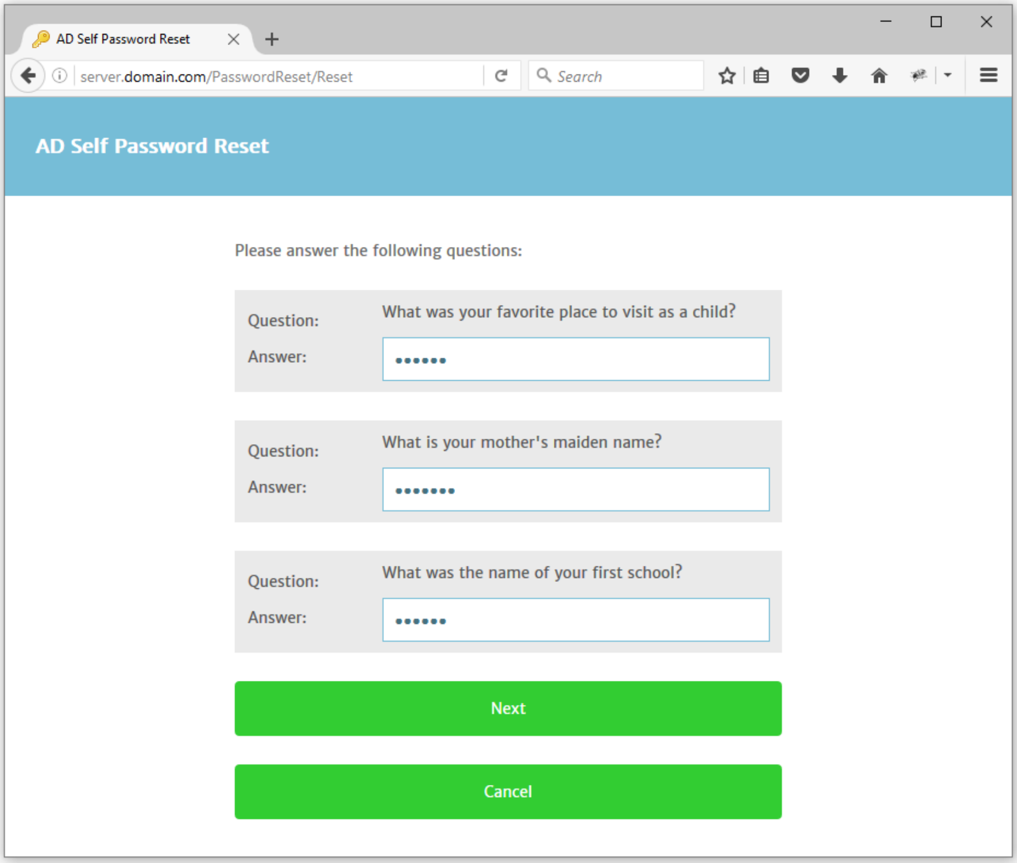
AD Self Password Reset

Please enter your account name and then select your domain.

Username:

jsmith

The user then answers a random selection of their questions and clicks Next.



AD Self Password Reset

Please answer the following questions:

Question: What was your favorite place to visit as a child?

Answer: ••••••

Question: What is your mother's maiden name?

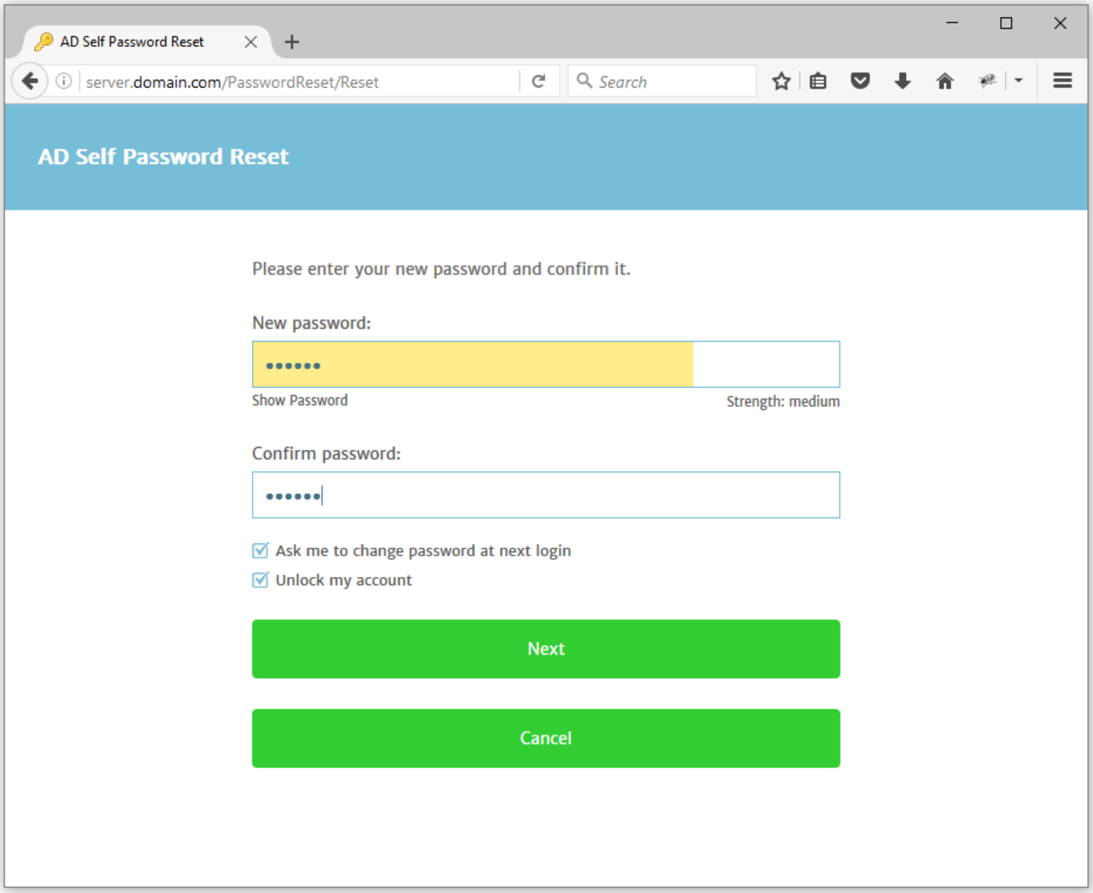
Answer: •••••••

Question: What was the name of your first school?

Answer: ••••••

Step 3

After successfully answering the questions the user can then enter a new password, the built-in strength indicator can be disabled in Configuration program.



Please enter your new password and confirm it.

New password:

••••••

Strength: medium

Confirm password:

••••••

☑ Ask me to change password at next login

☑ Unlock my account

Step 4

The user will see confirmation that their password was changed successfully.

5.3 Unlock Account

Step 1

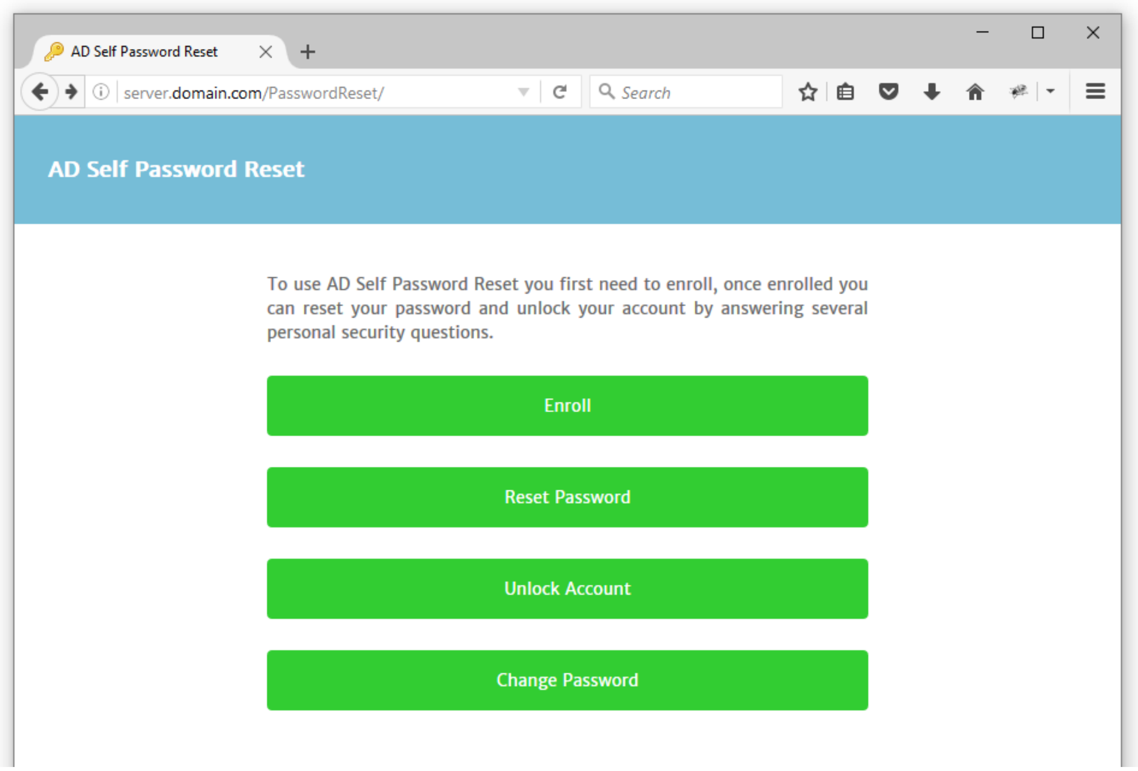
If the users account is locked, then the user can unlock their account by navigating to

http://server/PasswordReset or

http://10.0.0.1/PasswordReset

Step 2

To unlock a user account, click Unlock Account button.



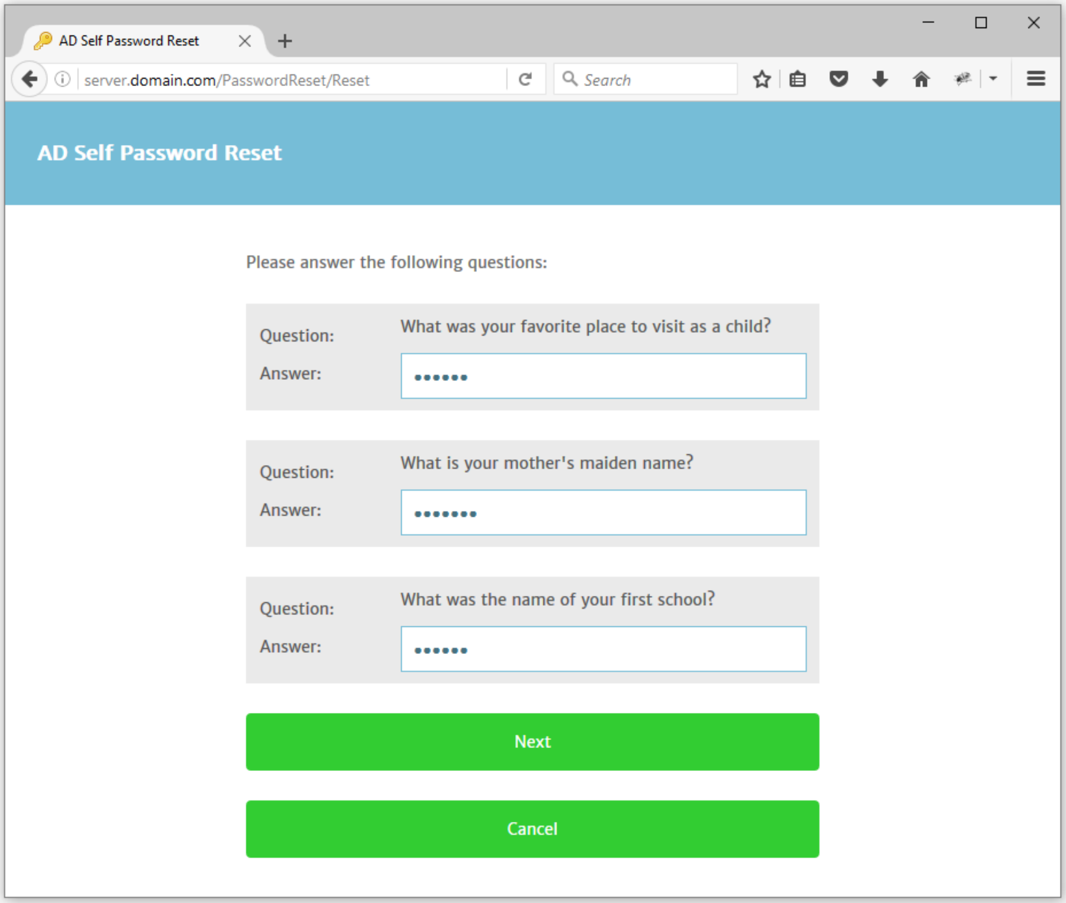
To use AD Self Password Reset you first need to enroll, once enrolled you can reset your password and unlock your account by answering several personal security questions.

Step 3

Enter username and domain. Click Next

Step 4

You will be asked to confirm the answers to two of the secret questions you set upon enrollment.



AD Self Password Reset

Please answer the following questions:

Question:	What was your favorite place to visit as a child?
Answer:	••••••
Question:	What is your mother's maiden name?
Answer:	•••••••
Question:	What was the name of your first school?
Answer:	••••••

Step 5

After successfully answering the questions the user will receive confirmation their account was unlocked successfully.

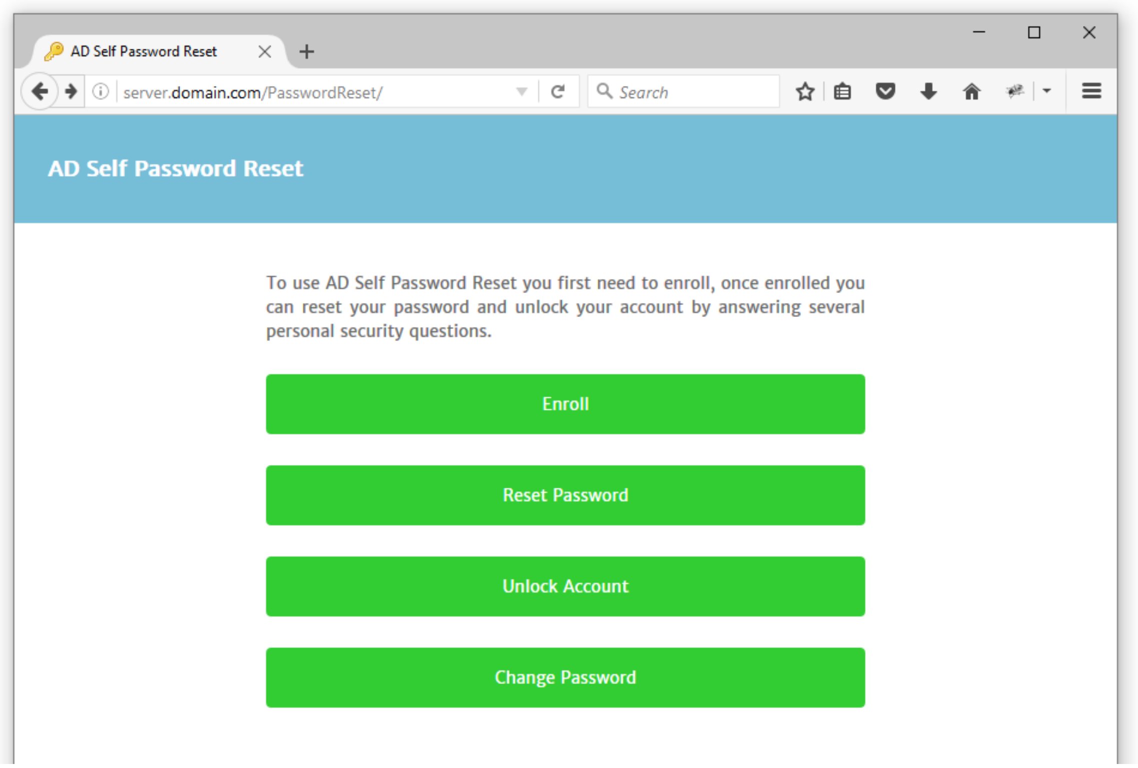
5.4 Change Password

Step 1

Open a web browser and navigate to http://server/PasswordReset

Step 2

To change your password, simple click Change Password

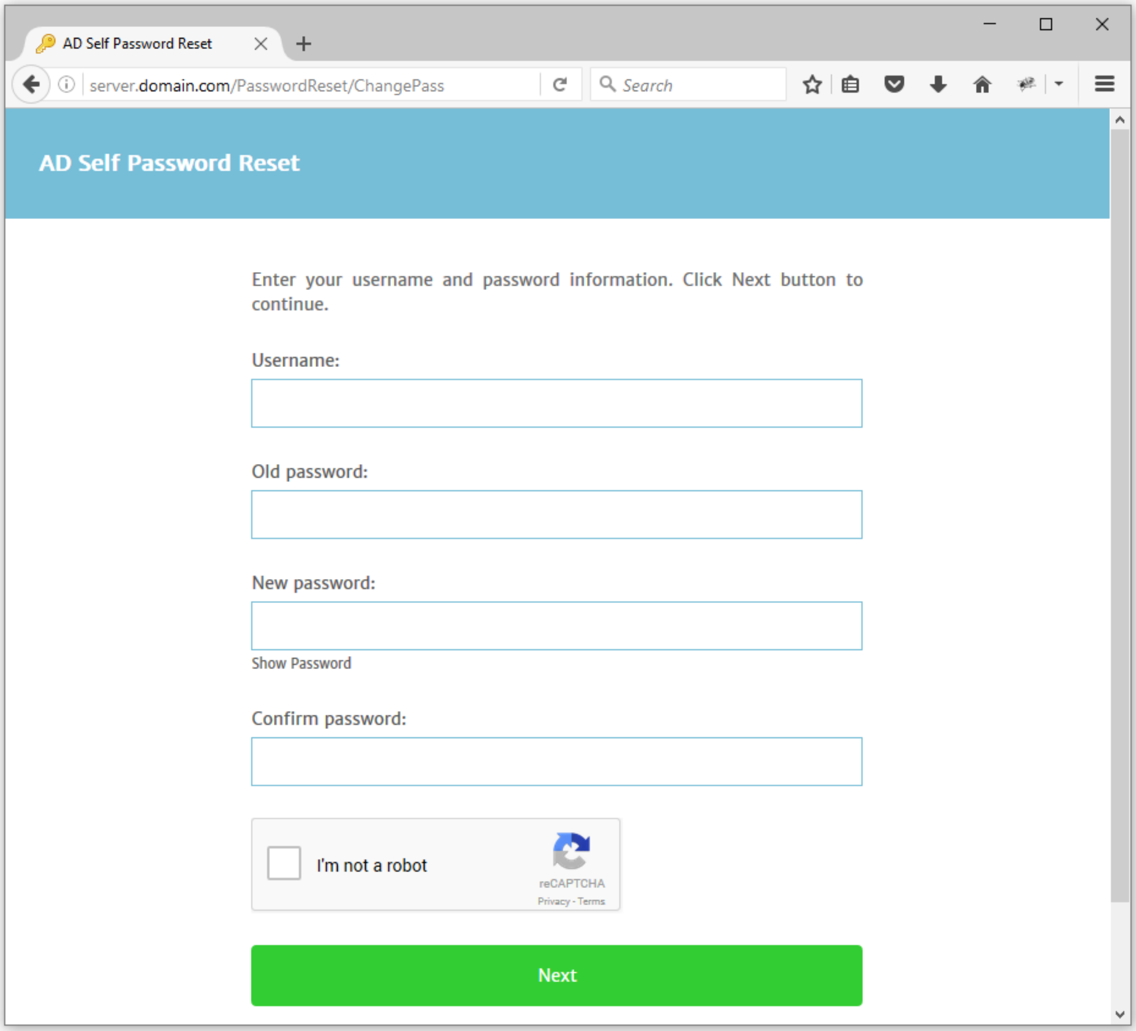


AD Self Password Reset

To use AD Self Password Reset you first need to enroll, once enrolled you can reset your password and unlock your account by answering several personal security questions.

Step 3

Enter the details below, select a new password. Click Next



AD Self Password Reset

Enter your username and password information. Click Next button to continue.

Username:

Old password:

New password:

Show Password

Confirm password:

□ I'm not a robot

Step 5

After successfully answering the questions the user will receive confirmation their password was changed successfully.

5.5 Help and Support

If you require any help installing or configuring AD Self Password Reset please contact support@dovestones.com.