# DCDS OpenAM Configuration

This document shall document the procedure for configuring the Email service, enabling forgot password, and setting the user timeout in OpenAM 12.

## Enable Email Service

The email service will be required to notify the user when they reset their password. You’ll need an account with administrative access (e.g. amAdmin), and credentials for an SMTP server (e.g. gmail, or a corporate SMTP server)

1. Navigate to the Email Service configuration; Configuration -> Global -> Email Service
2. Complete the configuration
   1. Leave the default Email Message Implementation Class (org.forgerock.openam.services.email.MailServerImpl)

* 1. Mail Server Host Name – hostname of corporate SMTP server, or for gmail: smtp.gmail.com
  2. Mail Server Host Port – port SMTP server is running. For gmail: 465
  3. Mail Server Authentication Username – SMTP account username. For gmail: [username@gmail.com](mailto:username@gmail.com)
  4. Mail Server Authentication Password – SMTP account password
  5. Select SSL if appropriate. For gmail, select SSL.
  6. Email From Address – Address to use as the ‘from’ account. Some SMTP servers do not allow this, for example gmail does not and will use the account credentials for the ‘from’ field.
  7. Email Attribute Name – property representing the user’s email address. Default for OpenAM is ‘mail’
  8. Email Content – content body of email. Leaving it blank will produce an email with just the forgotten password link.
  9. Email Subject – Subject of the email to be sent to users. For example “Reset your DCDS password”

1. Save.

## Enable User Self Service

User Self Service consists of two functions; user self-registration and forgot password. Only the forgot password functionality is to be enabled.

1. Navigate to the User Self-Service configuration; Configuration -> Global -> User Self Service
2. Select the checkbox for Forgot Password for Users.
3. Leave the defaults.
4. Save.

## Set User Session Timeout

The session timeout is the time before a token becomes invalid; the default is 30 minutes and should be increased to prevent user session interruption.

1. Navigate to the Session Configuration; Configuration -> Global -> Session
2. Under Dynamic Attributes, set Maximum Session Time and Maximum Idle Time. These are in minutes, if a 24 hour session limit is desired set to “1440”