Keep Secure

Keep Secure support guide

Version 1.0

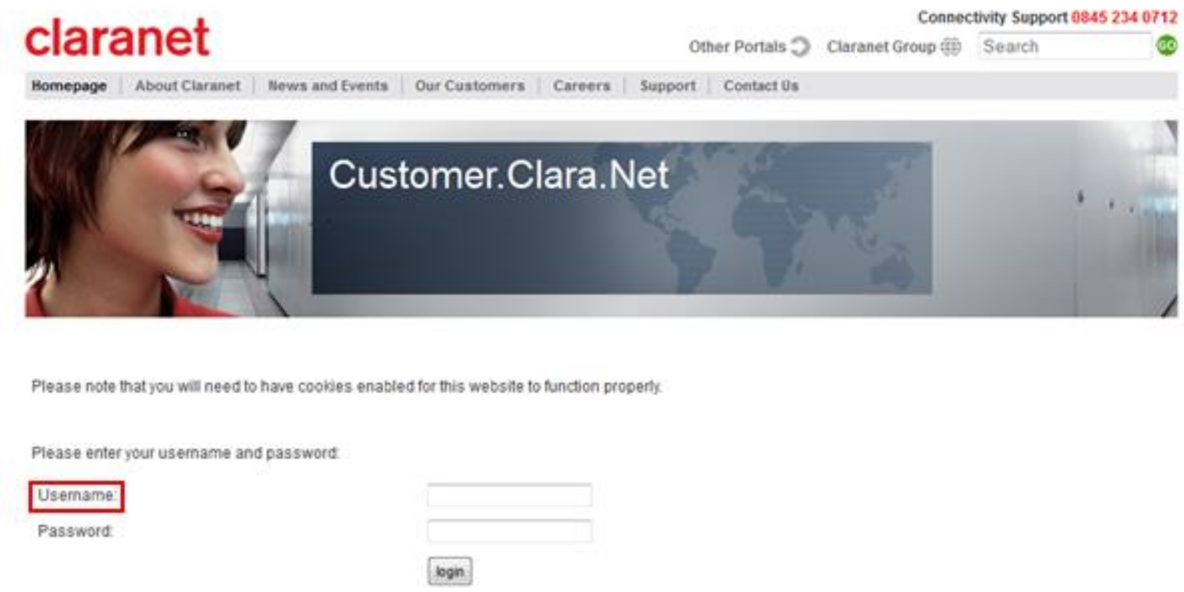
Contents

1 Resetting passwords

Please note: to change the password for a Dircon, Via, or Freeuk email; you must contact our **support team**.

A password change can take up to 15 minutes to go active. To reset your password for your broadband or any @clara.co.uk/@clara.net email account, you can login to **https://customer.clara.net**, (shown below).

Your username will be the first part of the email address i.e. the part before the @clara.co.uk



Please note that you will need to have cookies enabled for this website to function properly.

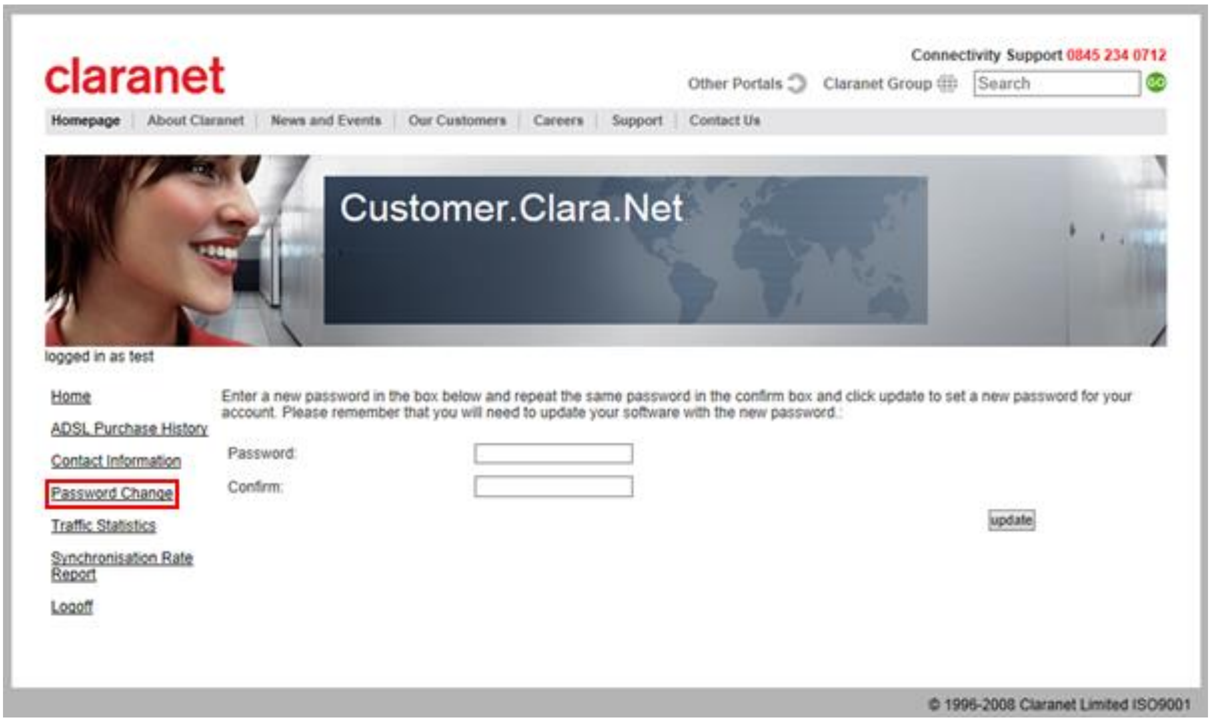
Please enter your username and password:

Username:

Password:

login

Once you have logged in, click on the **Password Change** button which is shown below and enter your new password and reconfirm the new password.



logged in as test

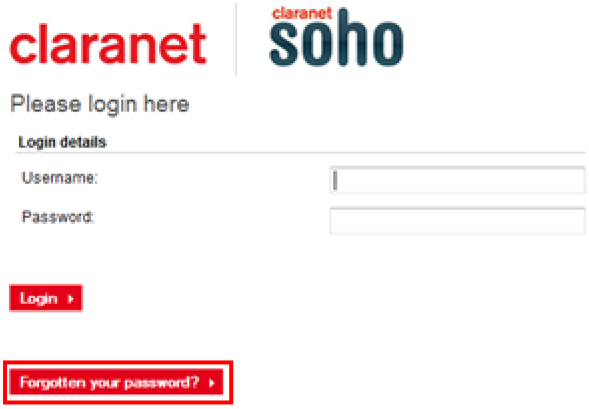
Enter a new password in the box below and repeat the same password in the confirm box and click update to set a new password for your account. Please remember that you will need to update your software with the new password.

Password:

Confirm:

However, to reset your hosting control panel password, you will need to login to your control panel at **https://admin.clarahost.co.uk**.

If you have forgotten your current password, there is a **forgotten password** button which will send an email directly to the contact email address listed on the account.



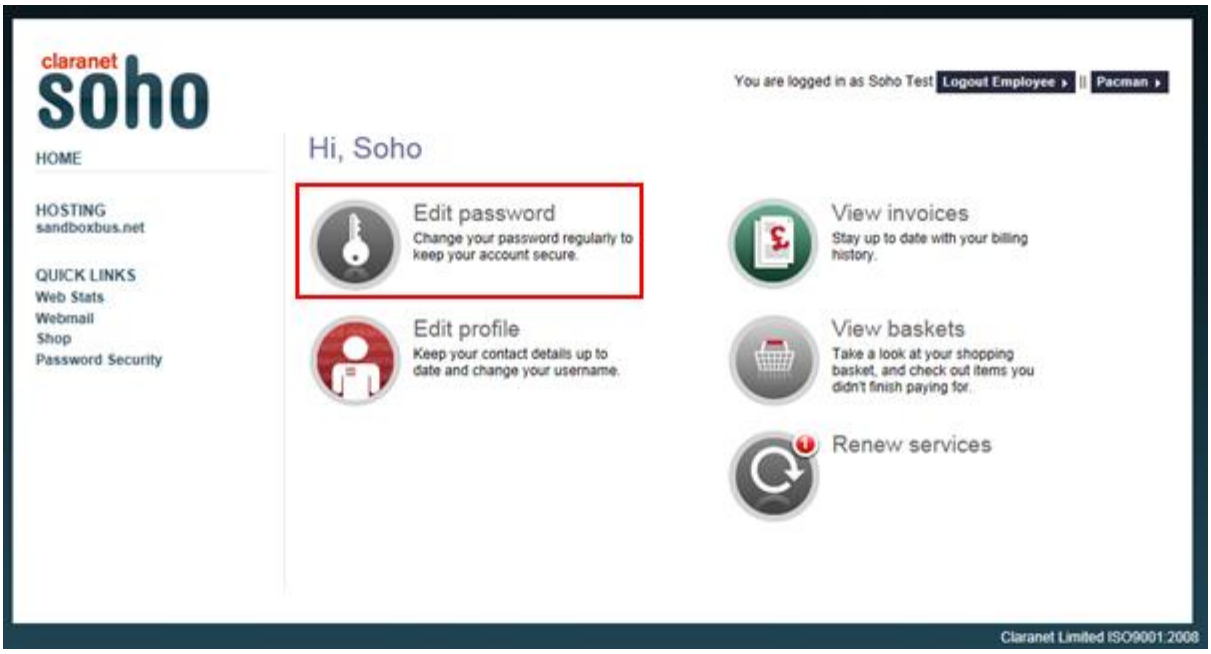
Please login here

Login details

Username:

Password:

Once you have logged into the clarahost control panel, click on the main menu where there is an **Edit password** button. This will allow you to change your control panel password.



You are logged in as Soho Test

Hi, Soho

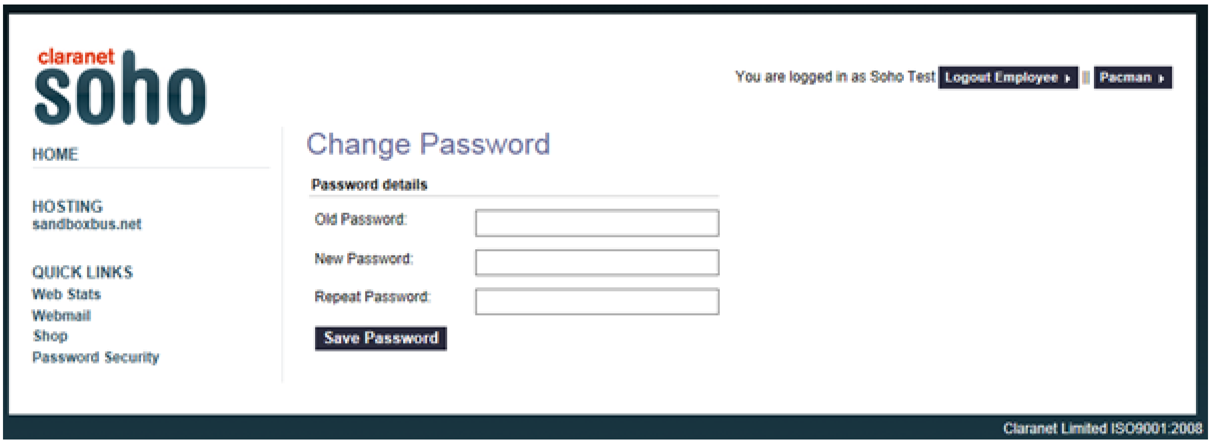
Edit password: Change your password regularly to keep your account secure.

Edit profile: Keep your contact details up to date and change your username.

View invoices: Stay up to date with your billing history.

View baskets: Take a look at your shopping basket, and check out items you didn't finish paying for.

Click on the **Edit password** button shown on the screen shown below and confirm your current password. Then enter your new password, confirm it and click **Save Password**.



You are logged in as Soho Test

Change Password

Password details

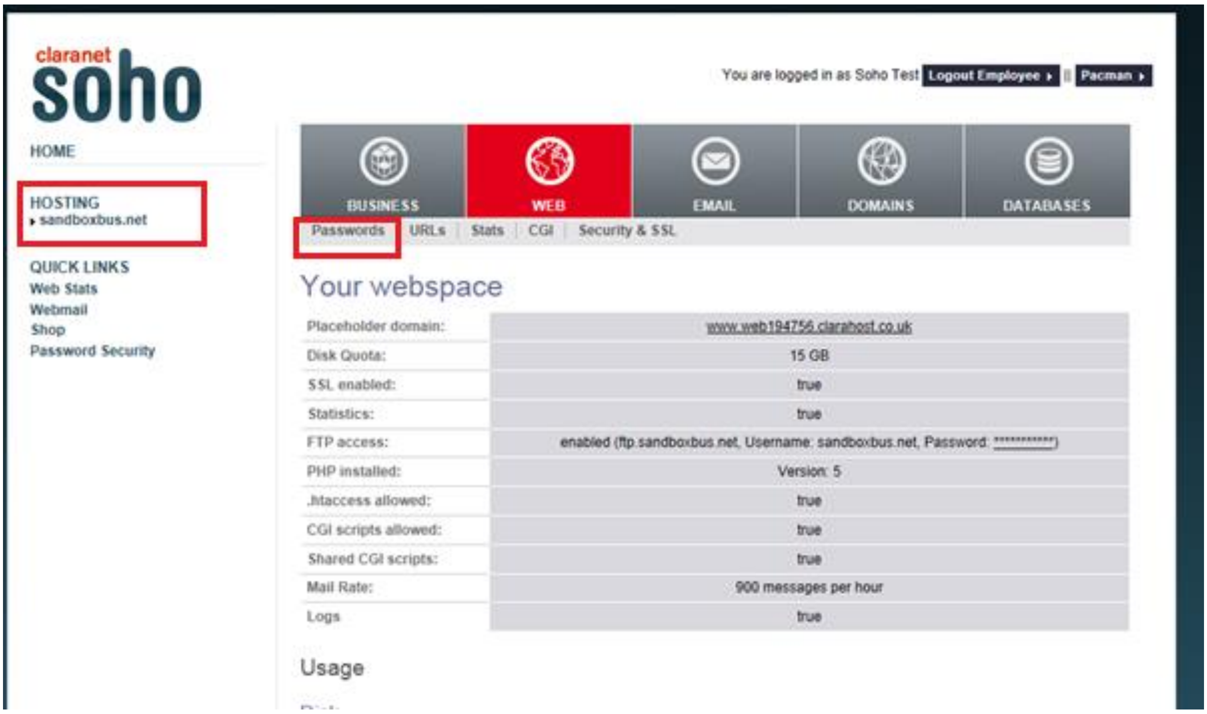
Old Password:

New Password:

Repeat Password:

To reset the FTP password for your website, you must click on your domain name on the left hand side of the screen (under the hosting header). Then click on the large **WEB** button at the top of the screen.

To view your current FTP password, click on the row of underlined stars in the FTP Access field.

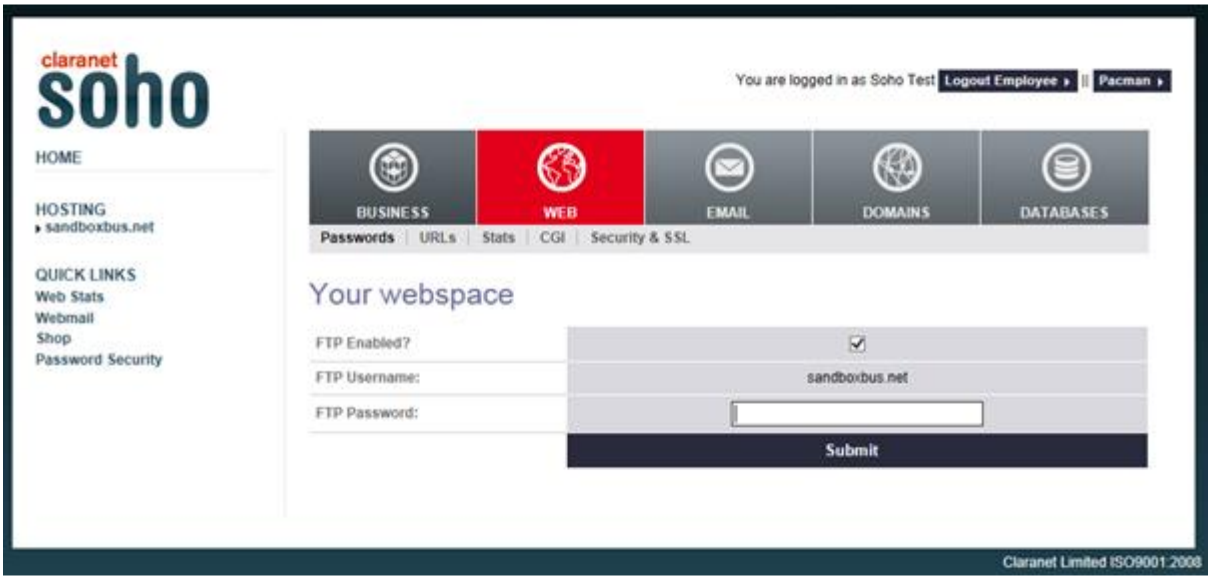


Your webspace

Placeholder domain:	www.web194756.clarahost.co.uk
Disk Quota:	15 GB
SSL enabled:	true
Statistics:	true
FTP access:	enabled (ftp.sandboxbus.net, Username: sandboxbus.net, Password: ***********)
PHP installed:	Version: 5
.htaccess allowed:	true
CGI scripts allowed:	true
Shared CGI scripts:	true
Mail Rate:	900 messages per hour
Logs	true

Usage

In **WEB** section, click the **password** sub option (just below the large buttons along the top of the screen). You will then see the screen shown below. Enter a new password and click submit.



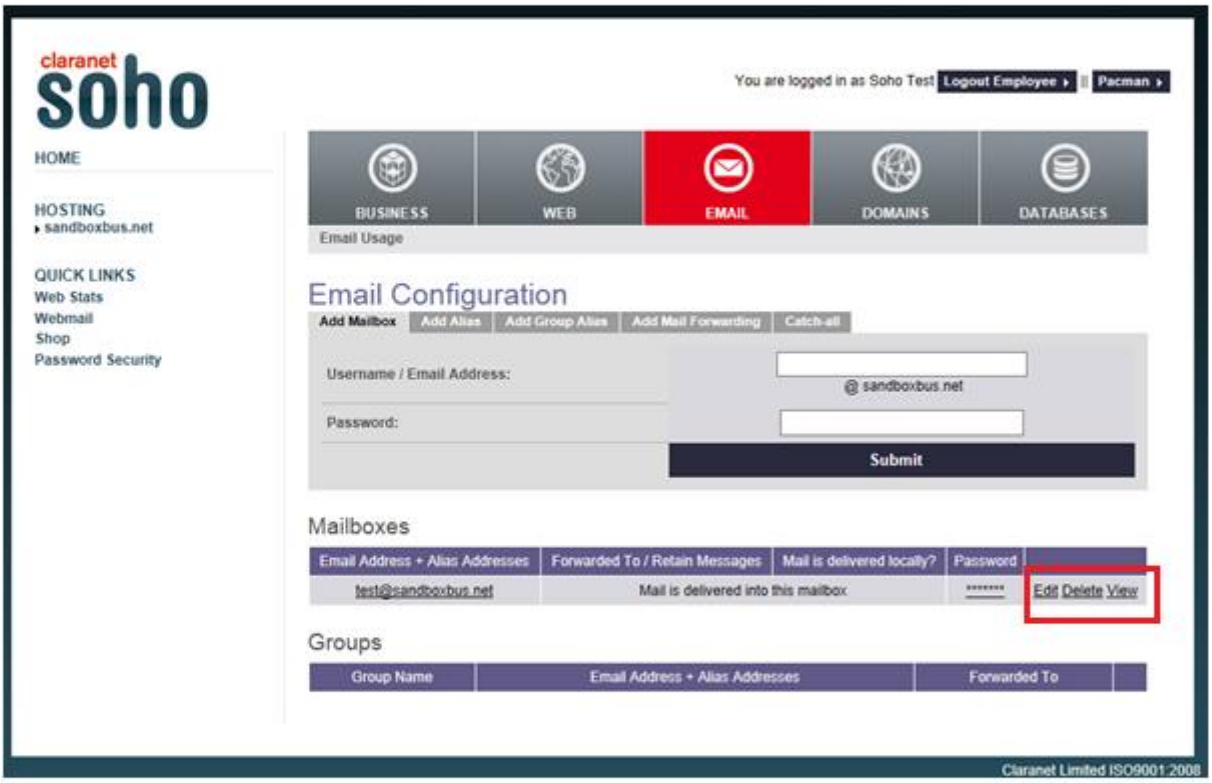
Your webspace

FTP Enabled?	☑
FTP Username:	sandboxbus.net
FTP Password:	

To reset the password for any of the mailboxes in your hosting control panel, click on the large **EMAIL** button at the top of the screen within the control panel.

Once you have clicked on the **EMAIL** button, it will list all of the current mailboxes on the screen as shown below.

To view the password for each mailbox, click on the row of underlined stars. To reset the password for any of the mailboxes, click the **Edit** button next to the specific mailbox and you can reset the password for that specific mailbox.



Email Configuration

Username / Email Address: @ sandboxbus.net

Password:

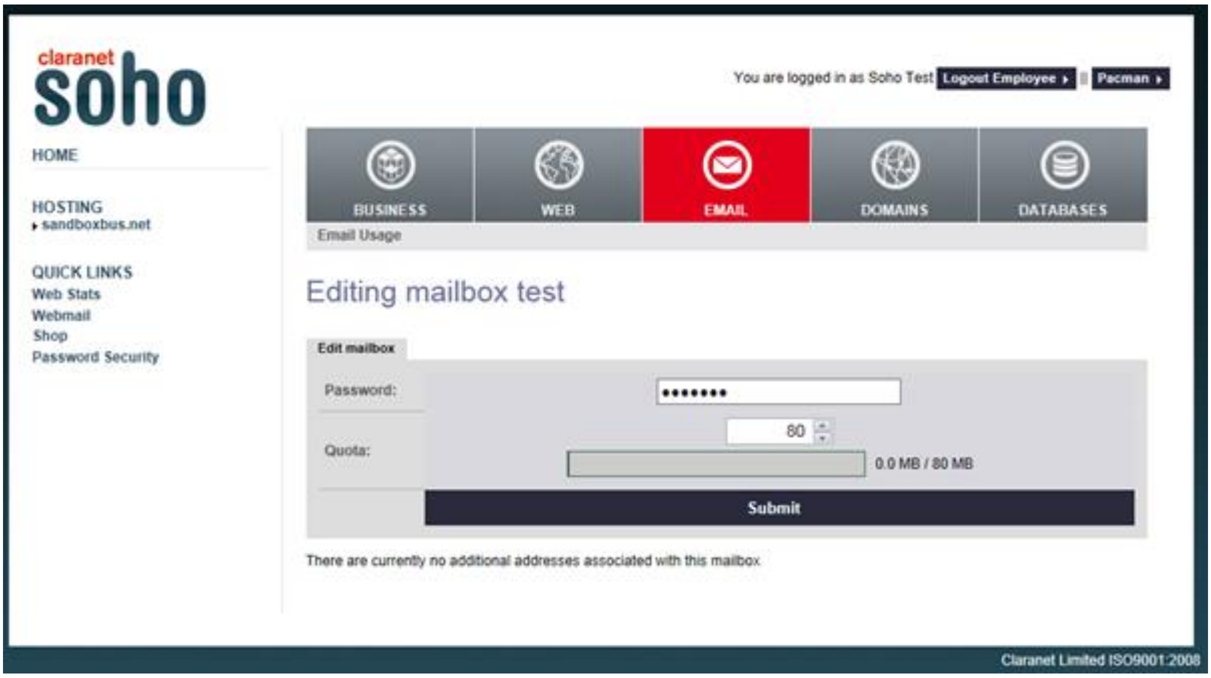
Mailboxes

Email Address + Alias Addresses	Forwarded To / Retain Messages	Mail is delivered locally?	Password	
test@sandboxbus.net	Mail is delivered into this mailbox		*******	Edit Delete View

Groups

Group Name	Email Address + Alias Addresses	Forwarded To	

Once you have clicked the edit button, you will see the screen below. You can then enter your new password for the mailbox and then click submit. The original password will still be in the field, so you will need to delete the row of dots before entering a new password.



Editing mailbox test

Password: •••••••

Quota: 80

0.0 MB / 80 MB

There are currently no additional addresses associated with this mailbox

2 Password security

Claranet SOHO believe it is important that we help our customers to be secure whilst online. For this reason, we have introduced strict criteria around the format of passwords in order to prevent your account being compromised by trojans or viruses.

When setting a new password, you must use a minimum of 6 characters and incorporate a mixture of letters, numbers and symbols. You will also not be able to use any of the following:

- The word ‘password’
- Your login name
- A person’s name
- Dictionary words
- Accepted characters ;@'#~[]/?.,<>{}!"$%^&*_-+=|`
- Not accepted characters :£\¬
- Maximum length is 16 characters

An example of a website used to generate passwords can be found here: **https://identitysafe.norton.com/password-generator/#**

Please note, when you do change your password, you will also need to change the password in any device or program that connects to your email account.

If your username is associated with your broadband connection, you will need to change the password on your router. If you are not sure of how to make this change, you can contact our **support team** for assistance.

3 Securing your wireless network

Encrypting your wireless network is the first step to securing your connection. Most third party routers will be delivered with encryption turned off, which will leave your network exposed if you don’t enable it.

When enabling your router’s encryption, make sure to use the strongest form that your network supports. Routers supplied by Claranet SOHO come with wireless encryption turned on.

Wireless Protected Access 2 protocol (WPA2) is the most recent and secure form of encryption. We strongly recommend using this type of encryption if it’s supported by your network. Other forms of encryption are Wireless Protected Access (WPA) and Wired Equivalent Privacy (WEP).

Please note, you have to use the same form of encryption across all devices on your network.
If your router only supports WEP, use 128 bit WEP keys and check the manufacturer’s website for any firmware updates that will add WPA support. If an update is unlikely, consider replacing your router with one that supports WPA and/or WPA2.

Change your network name and password to make it more difficult for anyone to hack into your router.

4 If my router has a firewall, why do I need these added security measures?

The firewall built into your router is designed to prevent hackers getting access to your computer from the internet. However, the firewall does not prevent people in range of your Wi-Fi signal from getting on your network or seeing your Wi-Fi traffic.

5 How can I secure my notebook at public Wi-Fi hotspots?

Most public hotspots don’t use encryption, so assume that anyone can see your internet traffic.

Here’s our top tips on securing your notebook:

Make sure it's a legitimate hotspot; there have been examples of people setting up pirate routers with the same name as a legitimate one. These routers can be used to capture personal data, so check the name of the wireless network before you connect.

Most places will have the network name written somewhere, if you can’t see it, ask someone.

Check your computer’s firewall is on and file sharing is off. Open the Control Panel and go to the Security Centre to check your firewall (the exact path will vary depending on what operating system you’re using).

If you’re using XP, you’ll need to go to Programs to turn file sharing off. However, if you’re using Vista, go to change settings and then click the Exceptions tab and follow the instructions.

Make sure you’re on a secure site before entering any personal details (passwords, bank details etc.). Check that the URL begins with https and look for a padlock. Some browsers display the padlock in the address bar or on the page so there’s no specific place to look.

These details are important because they show the website has built in their own encryption to protect your data.

Don’t leave your Wi-Fi radio on when travelling between hotspots. Hackers can use this to create a peer-to-peer Wi-Fi connection and access your computer.

6 Protecting against Viruses, Spyware and Malware

You should ensure that all of your PC’s/MAC’s have a fully up-to-date Security Suite installed with the latest updates. A good security suite should comprise of AntiVirus, Anti Spyware and Anti Malware facilities.

A common misconception is that MAC’s are immune to Viruses, this is NOT the case and they are vulnerable to being targeted. There is a wide variety of security software available for MAC’s as well as PC’s.

You can also secure your mobile phones and tablets and it is recommended to protect all devices.

If you run your own mail servers and need to protect your whole organisation from Viruses, Spam, Malware and Spyware, we recommend that you use our Symantec Services. These services can scan all emails to your domain name before even reaching your own mail server.

Symantec Web Services are also available to protect your organisation when users are browsing the internet. These services stop any users from being infected by any viruses that may be within websites which are visited.

For more information regarding the Symantec Email and Web services, please contact our **support team**.