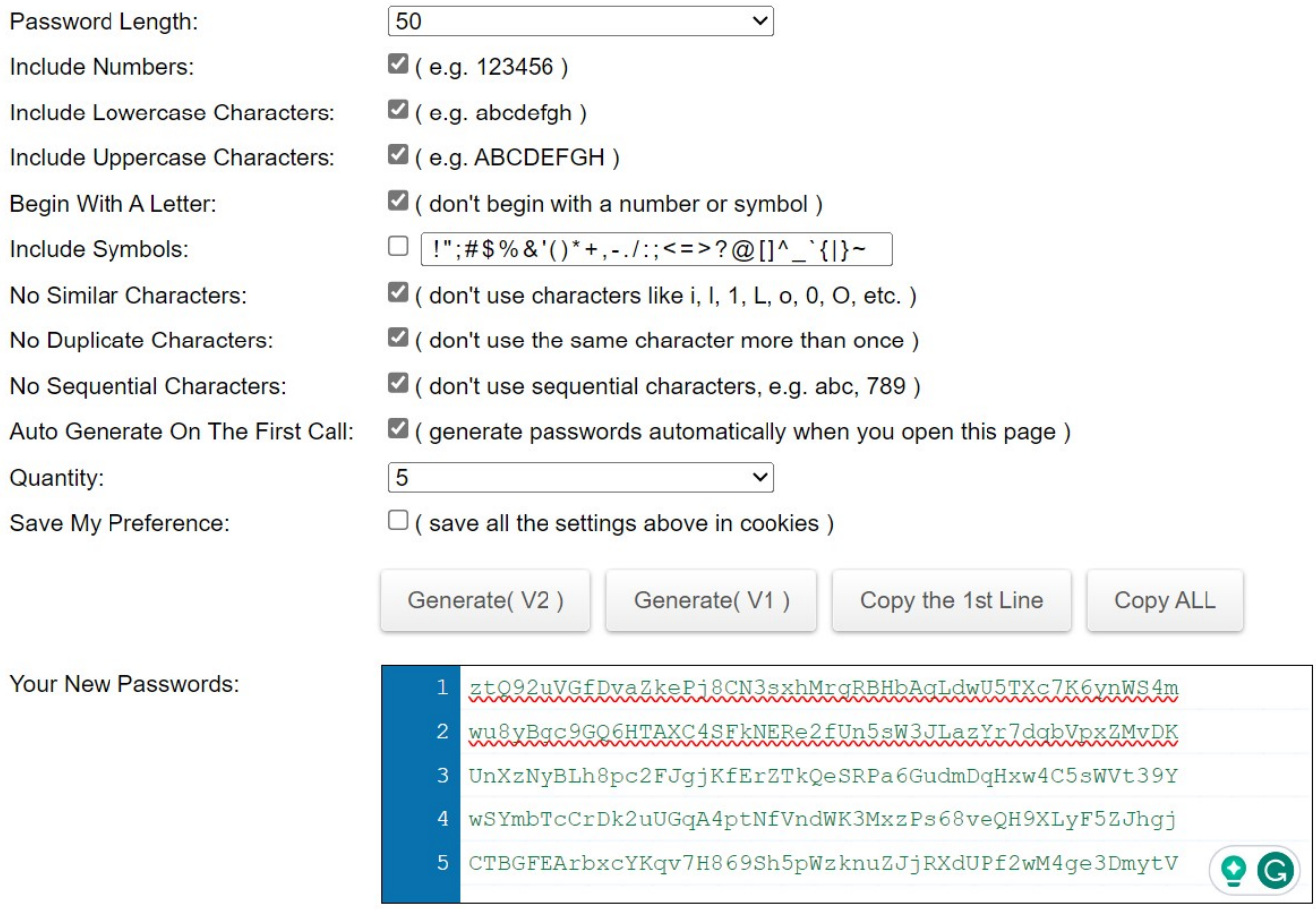
WSC Encryption Key

Create a strong encryption key

The encryption key is used to encrypt any data that end users place in the credentials form. The only way to see credentials is to provide the key to decrypt the information. Even anyone with access to your database cannot see any encrypted information. The only place the key is used is inside the WHMCS administration area. It's stored in hashed format. When creating an encryption key we advise you to use a website like Strong Random Password Generator (passwordsgenerator.net). Your key needs to be at least 16 letters and numbers long. These can be higher and lowercase but you cannot use special characters like @&*%^.

Here are a few **examples** of some strong strings.

```
ztQ92uVGfDvaZkePj8CN3sxhMrgRBHbAqLdwU5TXc7K6ynWS4m
wu8yBgc9GQ6HTAXC4SFkNERe2fUn5sW3JLazYr7dqbVpxZMvDK
UnXzNyBLh8pc2FJgjKfErZTkQeSRPa6GudmDqHxw4C5sWVt39Y
wSYmbTcCrDk2uUGqA4ptNfVndWK3MxzPs68veQH9XLyF5ZJhgj
CTBGFEArbxcYKqv7H869Sh5pWzknuZJjRXdUPf2wM4ge3DmytV
```



Key Security

You must keep a copy of the encryption key you use. Without the key, any data in the database will become inaccessible. We advise you to keep your key on a USB stick in a locked safe. Do not store it on the server with WHMCS and we advise you don't store it in an email account or Cloud storage account. If you do, store it in a password-protected zip file.

If you ever disable WSC you will need to enter the same encryption key again to access any credentials attached to current open support tickets. All data collected is deleted when support tickets are closed.

Revision #2
Created 22 December 2023 12:38:53 by DevGB
Updated 27 December 2023 13:40:40 by DevGB