

# AmazaCart Advanced Security

## UserGuide

### 1. Create Your Public and Private Keys

1. Open your hosting [cPanel](#)
2. In the Security section, click on 'GnuPG Keys'
3. Go to the 'Create a New Key' section
4. **Your Name:** whatever you want it to be - like your company name
5. **Your Email:** choose an email you will be able to remember when you configure the Advanced Security Module
6. **Comment:** Just a note for your own purposes - like 'Shop Encryption Keys'
7. **Key Password:** Choose a Password that you will enter when you go to look at orders or other encrypted data
8. **Expire Date:** Enter the number of years or weeks you want these keys to be good for. It's more secure to change often, but if you don't want the hassle of doing this again, choose a very long time period.
9. **Key Size:** The higher the number the more secure - many people choose '2048'
10. Click 'Generate Key'

### 2. Download Keys to Your PC and Delete Them From the Server

1. FTP to your hosting account
2. Notice there is a new directory named .gnupg  
This is on the same level as public\_html, not inside of it.
3. Change the permissions on .gnupg to 003. If you are not able to view files in the folder you may need to put permissions to 750.
4. Download the 'pubring.gpg' and 'secring.gpg' files to your local PC.
5. Delete all files in .gnupg. Be sure you saved a copy (#4 above) first.
6. Now you are ready to re-upload them through your shop admin.

### 3. Configure the Advanced Security Module

1. Go to your shop Admin and click on 'Modules'
2. Be sure Advanced Security is listed as one of the modules. If it isn't, contact us to order this module.
3. Be sure the Advanced Security module is checked. If it isn't, put a check in the box and click 'Update' at the bottom of the page.
4. Click on 'Advanced Security' to configure settings

5. **Home Directory:** Type in the path to the .gnupg directory.  
Generic example: /web/YourHostingUsername/.gnupg  
An example for hosting account 'bigmall': /web/bigmall/.gnupg
6. **GnuPG executable path:** /usr/local/bin/gpg
7. **GnuPG user id:** The email address you used when you created your keys
8. **Encrypt admin order mail notifications:** Only select this if you are planning on also installing your security keys into your email program, otherwise you won't be able to view details of your email notifications.
9. **Encrypt order details stored in database:** Do check this, but only after you have installed the keys. Otherwise you won't be able to view any information about orders that are placed prior.
10. **Clear master password after login and logoff:** Check this for added security.
11. Click 'Update' to save all your GnuPG settings
12. **Install keypair:**  
Browse on your PC to find the public and private keys that you created in cPanel and downloaded to your PC. and click 'Upload'.  
  
If you get an error message 'Invalid Keypair', after you Upload the keypair, you will ALSO have to manually ftp those 2 files up to the .gnupg folder. After you upload them, change the permissions back to 003 on the .gnupg directory. Then go back to your shop admin and click 'Update' under the advanced security module. The 2 keys should now show up under 'GnuPG keyring settings.'
13. **Download Secret Key:** You won't have to do this, as you already have a copy of the keys on your local PC. BUT... if we installed the keys for you, you SHOULD download your secret key so that you will also have a copy.
14. **Test AdvancedSecurity configuration:** You must do this to confirm the keys are installed properly.
15. **Master password:** Enter the Key Password you used when you created your keys, and click 'Test configuration'.
16. Confirm that all Configurations options say 'OK'.  
Except.... If 'GnuPG executable path' shows a red 'NOT FOUND' it should still be OK.
17. Confirm that both tests for encrypt and decrypt say '[Passed]'

That's it! Just remember to enter your password when you go to orders, so that you can see the decrypted information.