JShop Server

simple. effective. e-commerce

Installation Manual

Documentation Version: 2.2.0
(Revision Date: 06/04/2009)

Table of Contents

1 Introduction

1.1 Welcome

Welcome to the installation manual for JShop Server. This manual will take you through the process of installing JShop Server for the first time on your web server. Some basic procedures need to be followed in order to install JShop Server and the following facilities will be required by the installation process:

- An FTP (File Transfer Protocol) client through which you can upload the JShop Server files to your web server.
- You will require your web hosting server's database connection details and database name. If you have not already done so, most hosting control panels provide the facility to setup a mySQL database, and choose the username and password. You need to note these details down.
- The path to your files on the server. Each hosting account has a full server path, a path to all the files on that hosting account. If you do not know what your full server path is your hosting company will be able to tell you what it is.

You will not require any in-depth PHP knowledge or mySQL administration knowledge in order to perform the installation.

1.2 Installation Service

We do offer an installation service for JShop Server which is available by logging into the Registered Users Area, selecting 'Your Licenses' and then selecting 'Order Extra Services'. This is priced at 50 GBP (plus VAT at the prevailing United Kingdom rate where applicable.) This installation service will provide a professional installation of JShop Server, setup of the database and permissions as per the 'Installing JShop Server' section of this documentation. Once complete you will then have a fully working installation ready to use.

If you have any questions about the installation service please feel free to contact us at sales@jshop.co.uk and we'll be happy to help.

1.3 Requirements

In order to be able to use JShop Server on your web server there are a number of requirements that it must meet. These are split into two different categories, those which are the core requirements needed in order to run JShop Server and those that are optional, depending on the features you intend to use in the system.

Core Requirements

This list of requirements is needed to run JShop Server and are required no matter what functionality you use within the system.

- PHP 4.1.0 or above
- MySQL 4.0 or above
- PHP should not be running in Safe Mode

Optional Requirements

These requirements depend upon the features you use in JShop Server.

- cURL with SSL support is required for some payment gateways. Currently USA ePAY requires it for

authorising transactions and PayPal requires it for sending notification of payment status to JShop Server. All other payment gateways operate without this need. This is installed as an extension to PHP and most hosting companies support this by default.

- If you wish to take credit card details yourself or use some payment gateways, such as USA ePAY, a secure server that runs over the same web space as your normal web space is required. For instance, your web root should be accessible under http:// and https:// and the web root is the same in both instances.
- The GD graphics library extension to PHP needs to be enabled to use the image resizing facilities built into JShop Server (these can be disabled if GD is not available)
- If you intend to use the search engine safe URL options in JShop Server, this may require the use of an Apache-based server, the activation of mod_rewrite and the use of .htaccess files. These topics are covered later on in this manual.

2 Installing JShop Server

2.1 Downloading and Unzipping

All installation .zip files can be downloaded from the JShop Server Registered Users Area. This can be accessed with the user ID and password provided to you when you purchased our software. The URL for the Registered Users Area is:

https://www.jshopecommerce.com/jssusers/

Once you have downloaded the full installation zip file for the latest version of our software (we do provide access to previous versions also should you require them for any reason) you should unzip this file.

Once completed you should have a directory within which are all the JShop Server files in multiple directories suitable for uploading.

Note: At no point during the installation process should you ever upload the full installer .zip file for JShop Server. Uploading this can potentially provide access to our system to those that have not purchased the system. Unfortunately, due to this happening previously, we now reserve the right to revoke licenses where we find that this has happened under our standard license terms, which covers the distribution of our installers.

2.2 Editing static/config.php

Before uploading the files to your server, you will need to edit the config.php file which you'll find located in the 'static' directory. The config.php file contains all the basic setup information that JShop Server needs to operate and much of the information within this will be specific to your web hosting. Editing the config.php file can be done with any text editor, on Windows computers Notepad should be sufficient.

You should not need to edit any other .php files from the JShop Server distribution and only the following options need to be edited in the config.php file:

`$databaseHost`	Enter the name of your mySQL database host. This will normally be localhost.
`$databaseUsername`	Username to access the mySQL database
`$databasePassword`	Password to access the mySQL database
`$databaseName`	The name of your mySQL database. If this does not already exist, JShop Server will attempt to create this database.
`$jssStoreWebDirHTTP`	Enter the full URL of where JShop Server will be, e.g. http://www.domain.com/shop/ (the trailing slash must be included)
`$jssStoreWebDirHTTPS`	This should be the URL of the same directory as above but under HTTPS. If you do not have SSL please enter the same URL here (without https://) as you entered for $jssStoreWebDirHTTP (the trailing slash must be included)
`$jssShopImagesWeb`	Sub-directory off $jssStoreWebDirHTTP where the shopimages can be found. You should not need to change this. (the trailing slash must be included)
`$jssShopFileSystem`	This is the full absolute server path to JShop Server. It should be to the

	same directory as you entered for $jssStoreWebDirHTTP. For instance, on Linux this might be: /var/www/html/shop/ (the trailing slash must be included)
`$jssShopImagesFileSystem`	Again this is the absolute server path to JShop Server's shopimages directory. For instance, on Linux this might be: /var/www/html/shop/shopimages/ (the trailing slash must be included)
`$jssCacheDir`	This is the directory to use for the caching facilities within JShop Server. The default location for this is a sub-directory of your main JShop Server directory, although there is no reason why you cannot enter a directory here that's outside of your web root for greater security.
`$teaEncryptionKey`	This is the encryption key that will be used to store credit card details within JShop Server. It should be a combination of 32 letters and numbers. Note: Please ensure that you change this, even if you are not storing credit card details for off-line processing. JShop Server will need this for some payment gateways where credit card details are taken on your server and stored temporarily before being passed to the gateway, e.g. USA ePay. It is important that you do not use the standard string that is included in config.php by default as this would present a security risk.
`$jssRegistrationCompany`	Enter your JShop Server registration company name
`$jssRegistrationCode`	Enter your registration code given to you when you purchased JShop Server.

Note: For JShop Server registration company name and registration code can be found on the 'Your Licenses' page in the Registered Users Area.

2.3 Uploading to Your Server

In order to upload the files to your web hosting, you will require an FTP client. Generally built in clients in browsers are not recommended and many third party FTP applications are available. For instance, on Windows, Mac OS and Linux a free FTP client called Filezilla is a good option: http://filezilla-project.org/

Once you have your FTP client and have setup a profile for your web hosting (this will require your hosting's FTP address, username and password, all of which you can obtain from your hosting company) you are then ready to connect to the server and upload the files.

Generally your hosting account will have a public_html, web, www or htdocs folder which is termed your web root. This is where files are stored when you access your site. If you do not already have a web site running on your hosting, you can install directly into this directory, otherwise you can create a sub-directory (called something like 'shop', for instance) and upload your JShop Server files into that.

Once you have completed the upload of the files you will be ready to run the JShop Server installation script.

Note: Most FTP programs have an automatic setting for the upload mode for different file types. If yours does not you will need to ensure that all .php and .html files are uploaded in ASCII format and all .png, .gif and .jpg files are uploaded in Binary mode.

2.4 Basic Directory Permissions

In order for JShop Server to be able to perform some of its actions, PHP needs permission to be able to read/ write/create and delete in certain directories. These directories are:

```
shopimages/ (and all sub-files and directories).
templates/ (and all sub-files and directories).
files/
cache/
```

All these directories and their sub-directories / files should be set to 777 (apart from any index.html files) via. chmod and this can normally be done through an FTP program. This ensures that JShop Server can create images for products and sections in your store. For the templates directory you have two options, one or both of which may be available on your server, depending on how it is configured. Those with dedicated servers are advised to use option 2, those on shared / virtual servers may have to use option 1 but can contact their hosting company if they would like to use option 2, who should be able to help you. If you are running on a Windows server you will not need to set permissions. In addition on some Linux servers where PHP is running as a CGI you may not need to change the permissions at all due to the username that PHP runs as on the server being the same as your FTP username.

Note: Some of the security risks associated with running your templates, cache, files and shopimages directories with permissions set to '777' are mitigated with the advice in the Securing Directories section of this manual.

Option 1: Using Mode 777 To Grant PHP Rights To The templates Directory

Set the templates directory, the compiled sub-directory and all files in those directories to 777 via. chmod. It is not advisable to leave these directories as 777 at all times as it will represent a security risk. However, when you are editing templates through the administration system or getting JShop Server to create compiled versions of templates it will have to be set to 777 for this to work correctly. If the permissions aren't correct, JShop Server will show an error message on your store. When you are not editing or compiling templates, you can change the permissions to 775 which still gives JShop Server rights to read the files which is all it will need. Using this method you will always be able to upload templates to the template directory through FTP.

Rather than having to do these individually if you have Telnet or SSH access you can use the following on Linux to do this:

```
chmod -R 777 /var/www/html/shop/templates
```

or

```
chmod -R 775 /var/www/html/shop/templates
```

Option 2: Changing Ownership Of The templates Directory

Find out what user the web server is running as. This is often nobody, httpd or apache. Your web hosting company should be able to tell you what user the web server is running as. You will then need to either Telnet or SSH into your web server to change ownership of the templates directory to the web server user – this gives PHP full access rights to the templates directory. The following commands are for linux and are shown as an example of changing permissions:

```
chown -R nobody:nobody /var/www/html/shop/templates
chmod -R 770 /var/www/html/shop/templates
```

The first of those commands changes the owner and group of the templates directory and all sub-directories and files to user nobody. The second sets read/write/execute permissions for the owner and the group, but doesn't allow it for anybody else. If you wanted to allow read and execute permissions for anybody else (for your own convenience through FTP for example), then you can change the chmod to the following:

```
chmod  775  /var/www/html/shop/templates
```

Note: Using this method you will not be able to upload templates to the templates directory using FTP. This will have to be done through the template administration system in JShop Server. Although this could be an inconvenience for some people we strongly suggest that you use this option if at all available on your server. Even if you run on a shared / virtual server, your web host should be able to do this for you.

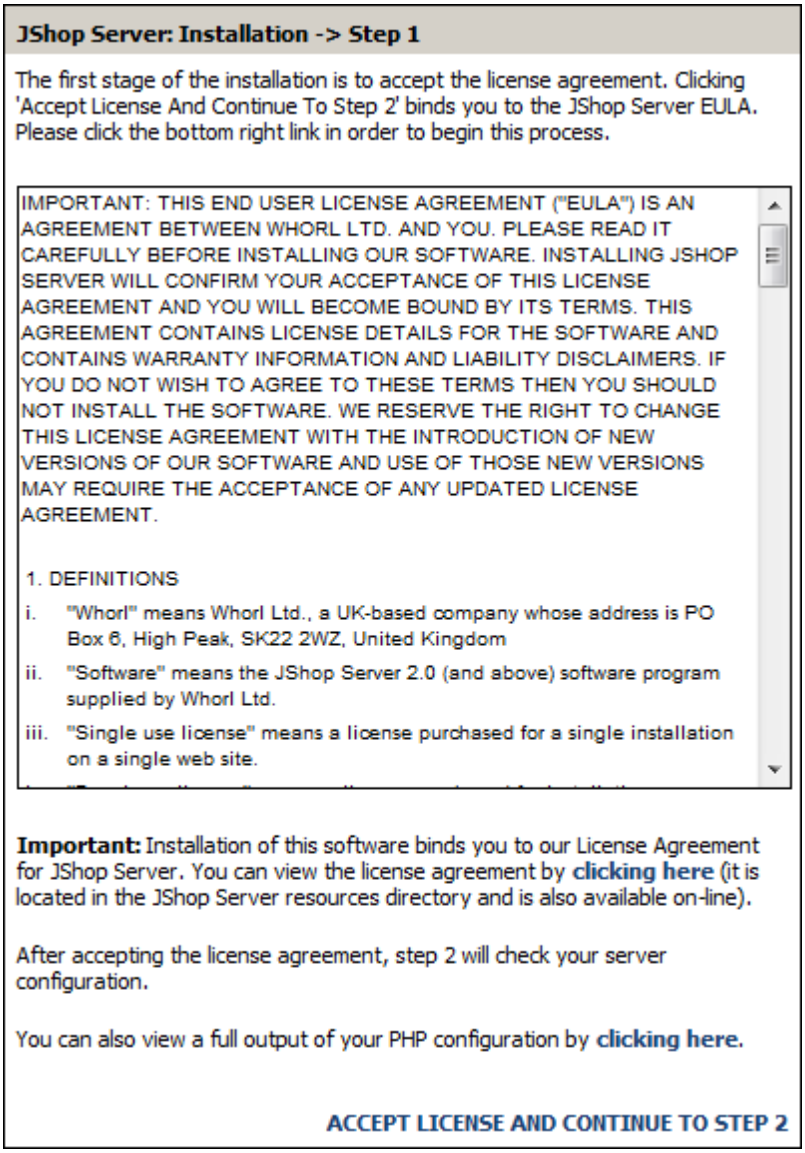
2.5 Running install.php

You are now ready to run the JShop Server installation script which will check some of your settings, check the status of PHP on your server and, if everything looks OK, will install the JShop Server database.

You'll need to open a web browser and navigate to the install.php script on the server, e.g.:

http://www.domain.com/install/install.php

Once you have done this, you will see the standard JShop Server installation welcome screen..



This screen give you the option of reviewing the end user license agreement and agreeing to those terms before installing. From this point, all you have to do is follow the instructions on screen.

If the installation script encounters a problem with any of your settings it will alert you before allowing you to continue. A common issue is the installer telling you that it cannot connect to the database. If this happens you should consult your hosting provider for more information on what the correct connection details should be - unfortunately these will be specific to your hosting environment and we won't be able to tell you what they are.

2.6 Starting JShop Server

That's JShop Server installed. To open up the administration system in your web browser go to admin/index.php, e.g.:

http://www.domain.com/shop/admin/index.php

You will be asked for a username and password. The default settings are as follows:

Username: administrator
Password: administrator

To open the shop in your web browser, you would go to:

http://www.domain.com/shop/

Note: Remove the install directory before you do anything else, as leaving it on the server can present a security risk.

3 Advanced Setup Options

3.1 mod_rewrite and .htaccess

The Safe URL options in JShop Server, if enabled, may require you to setup mod_rewrite rules in .htaccess file on your server so your server can route the requests to the correct pages. These instructions are only applicable to Apache-based servers. If you are using a different web hosting environment please refer to your system's documentation or discuss similar options available with your System Administrator.

Many servers don't require this as they are setup as standard to, for instance, look for section.php if you just provide the filename section. However, if your server does require a .htaccess you should consult with your hosting company for detailed information, but there's a basic format that should work in most cases. The example below is a .htaccess for a JShop Server store running from the store directory (e.g. http://www.domain.com/store/)

```
RewriteEngine on
Options +SymlinksIfOwnerMatch
RewriteRule ^/store/(.*).php/(.*) /store/$1.php?$2
```

More detailed examples may be given by your hosting company and it may be that you have to ask them to enable mod_rewrite if they don't allow .htaccess files to turn it on.

4 Security Considerations

4.1 Summary

The issue of server security goes way outside the remit of this documentation and is an ever changing discipline. However, this section provides some general advice on helping you to secure your hosting environment when using JShop Server. You should pay particular attention to the Securing Directories section as this will help mitigate cross-account issues especially on shared hosting setups (where multiple different customers have sites on the same server.)

In addition to all the advice given in this chapter, it is vitally important that you install any JShop Server patches or updates as they are released by us. Unfortunately, in our experience, when vulnerabilities have been discovered in our software, as they are will all software, although we produce patches and make them available within hours of the issue coming to light, many users do not install these and those installations subsequently can be infiltrated. This happens far too often, and simply installing the patches we make available would stop this.

This section also contains some best-practice approaches for helping increase the security of your web store through settings available in JShop Server.

If you would like to know more about server administration and security, the following books may be of interest to you:

- Linux Administration (A Beginners Guide) by Steve Shah (Published by Osborne, ISBN 0-07-212229-3)
- Administering Apache by Arnold, Almeida and Miller (Published by McGraw Hill, ISBN 0-07-212291-9)
- MySQL by Paul DuBois (Pubished by New Riders, ISBN 0-7357-0921-1)
- Web Security Sourcebook by Avial D. Rubin et. al. (Published by Wiley, ISBN 0-471-18148-X)
- E-Commerce Security by Anup K. Ghosh (Published by Wiley, ISBN 0-471-19223-6)

Note: If you are using a virtual hosting solution rather than your own server, many of the changes you can make to increase security may not be available to you as you may not have access to configuration files for Apache and PHP or to the user tables in mySQL.

4.2 General Advice

Included within each of the directories for JShop Server is an index.html file. This is the default page shown when somebody accesses the directory from the web, without accessing a file within that directory. For instance, without this file in the routines directory people would be able to view a directory listing of all the files in that directory. Although not directly a security risk, it is always advisable to restrict access to directories that should not be viewed from the web.

If your server does not use index.html as the default file for a directory, you should change the name of index.html to the supported default name.

If you are running your own server you should be aware that the normal, basic install of web server software isn't setup for the best security, it's normally setup for a balance between functionality and security. It is always advisable to investigate ways of making your system more secure. A common mistake is to leave all the installed services running, even if they're not being used. A good rule of thumb is that any port that is open on a server constitutes a further security risk to the server so, if you're not using the FTP service for instance, don't start the FTP service.

Note: Always make sure you keep your server software up to date. Patches are released for all server software that rectify recent security alerts or update server software to remove possible security threats. This really can't be stressed enough.

4.3 Storing Credit Card Details

We can't stress this enough - don't! It's available in JShop Server for legacy reasons but we do not advise doing this under any circumstances. With modern card acceptance rules, especially PCI compliance, storing credit card details carries with it both a lot of risk and can be very costly. In addition with Mastercard SecureCode and Verified by Visa rules it's actually in the merchant's benefit not to take credit card details for processing through a point of sale machine, as transactions authenticated by the cardholder with either of these methods results in liability shift for the merchant in case of fraudulent charge backs.

There should be no reason for any web store to store credit card details these days but something we often hear from merchants is that they want to do it because they shouldn't be charging the card until the goods are ready to dispatch. This is correct but with most reputable payment gateways offering pre-authorisation facilities where the card is checked, and in some circumstances the funds ring-fenced, but the card is not actually charged until the merchant follows this up with a 'release', this argument does not apply.

If you still want to take credit card details directly, then we would finally suggest that you discount this if you don't intend to use a dedicated server setup with a dedicated hardware firewall, maintained to a high standard by web hosting professionals and that you seek PCI compliance to the degree necessary for your company's transaction levels. In addition you should ensure that your merchant account provider is also aware of this.

Note: Fundamentally we understand that some merchants may still wish to take credit card details directly for processing through a point of sale machine but you do so at your own risk.

4.4 The 'admin' Directory

Due to the way that JShop Server is written it does not rely on the administration system being held in a directory called 'admin' (as it is by default.) There is no reason why this name should stay the same after installation and you can easily change this through your chosen FTP program.

Although this won't guarantee that a potential hacker will not be able to find your renamed admin directory but it creates an extra barrier to access.

The only consideration to bear in mind when doing this is that, when we produce updates to the system, you should remember to rename the admin directory in the update zip file to match the name of the directory on your server to ensure that the updated administration system files are correctly uploaded.

Finally, for an extra level of protection on the admin directory, in addition to the default user authentication system that is built into JShop Server's administration system, you can password protect the admin directory. This would be achieved with a .htaccess file on Linux requiring the entry of a username and password to get to the login screen. Although this may appear to be inconvenient to some users, it adds a second level of authentication and is worthwhile considering. Most hosting control panels provide options to password protect directories from their interfaces, so no technical knowledge should be required to achieve this.

4.5 Changing administrator Username

Version 2.1.2 introduced the ability to rename the default 'administrator' username to a username of your choosing. We strongly recommend that you do this through the 'Users' section of the administration system as it avoids having a common, well known username for a potential hacker to attack with.

In addition to changing the username please also refer to the main JShop Server manual, specifically the chapter on the 'Users' section of the administration system as there are a number of in-built facilities to stop brute force attacks on the login and help protect your installation.

4.6 PHP Settings

There are a number of settings within PHP that can help to bolster your site's security. You will need access to the php.ini file for PHP on your server in order to make these changes. If you do not have access to the php.ini file (for instance, if your site is hosting on a virtual hosting system) then you will not be able to make these changes.

1. Register Globals. JShop Server does not require register globals to be turned on, unlike other PHP-driven shopping cart solutions. It is always advisable to turn register globals off as it can present a security risk.

4.7 Securing Directories

On Apache-based servers you can use .htaccess files to help limit what can be accessed from certain directories and it's advisable to use the following advice for each of the directories that may require quite relaxed permissions to enable PHP to be able to read, write, add files and delete files. However, especially on shared hosting environments, this can lead to a security risk that allows other users on the server to upload files to these directories for possible execution.

templates Directory

Create a .htaccess file and place this in the templates directory. This will stop any .html, .req (which JShop Server's template system uses for some compiled template files) and .php files being accessible from the web. It will still allow the template system to operate, .css files and image files to be accessed which will be required for your store design to show correctly.

```
<Files ~ "\.(html|req|php)$">
   order allow,deny
   deny from all
</Files>
```

files Directory

The files directory should require no access at all from the web and so you can safely use htaccess to password protect this directory. Your web hosting control panel will more than likely provide the facility to password protect a directory.

cache Directory

The cache directory should require no access at all from the web and so you can safely use htaccess to password protect this directory. Your web hosting control panel will more than likely provide the facility to password protect a directory.

shopimages Directory

Only image files need to be accessible from the web for this directory and the following .htaccess file will stop access to .html and .php files.

```
<Files ~ "\.(html|php)$">
   order allow,deny
   deny from all
</Files>
```

For Windows IIS users, or other server brands, please consult your own documentation and your system administrator.

5 Additional Information

5.1 Installing for Local Development

These days there's nothing to stop you from developing your e-commerce site locally, on your own PC, before installing it on your web server. PC users can install both PHP and mySQL on their local machines and, with a personal web server such as Xitami (http://www.xitami.com/) you can install, develop and run your whole site without going on-line.

Alternatively there is a project called EasyPHP (http://www.easyphp.org/) that provides a single installer for PHP, mySQL, Apache and phpMyAdmin.

Finally, there's another option called WAMPSERVER which, like EasyPHP, provides an all in one installation. We generally prefer WAMPSERVER as it's more user-friendly, especially for novices. It can be downloaded here: http://www.wampserver.com/en/

Please note that we cannot provide detailed support for the installation or setup of any of the above packages.

5.2 phpMyAdmin

For those users that want good, quick access to their mySQL databases we suggest using phpMyAdmin. This is a web-based administration system for mySQL that allows you to do any database function without resorting to the normal mySQL command line interface.

Note: If you are installing phpMyAdmin on your server, you should ensure that you provide adequate security to those files – normally by using a .htaccess file to require a username and password to be entered before granting access to phpMyAdmin. PhpMyAdmin doesn't include its own username and password system.

Index