



BEFINE

**cryptshare**®

# ***LARGE FILE TRANSFER***

*made easy and secure*

## ***Cryptshare Administration Guide***

Version 2.5 and higher

Linux Operating Systems only

Befine Solutions AG  
Bebelstraße 17  
79108 Freiburg  
Germany

Web: [www.befine-solutions.com](http://www.befine-solutions.com)  
E-Mail: [info@befine-solutions.com](mailto:info@befine-solutions.com)  
Phone: +49 761 38913-0  
Fax: +49 761 38913-115

## *Cryptshare Administration Guide*

1. General	5
1.1. Operating Systems covered by this manual .....	5
1.2. The Cryptshare Licence .....	5
1.2.1. Cryptshare since version 2.6 .....	5
2. Administration of the Application	6
2.1. Apache Web Server .....	6
2.1.1. SSL Configuration .....	6
2.1.2. PHP Configuration .....	6
2.2. Languages .....	6
2.3. Log Data .....	6
2.4. Transfer Administration .....	6
2.4.1. Deletion of a Transfer .....	6
2.4.2. Cancelling a Transfer Lock .....	7
3. Cryptshare Administration Interface	7
3.1. General .....	7
3.2. Login .....	7
3.3. Changing passwords .....	7
3.4. Cryptshare License Terms .....	7
3.5. Section 'Overview' .....	8
3.6. Section 'Configuration' .....	8
3.6.1. Company Information .....	8
3.6.2. Base-URL .....	8
3.6.3. Pre-processing data to scan for viruses .....	8
3.7. Section 'Policy' .....	9
3.7.1. Automated creation of a default rule set .....	9
3.7.2. Sender address pattern .....	9
3.7.3. Recipient address pattern .....	9
3.7.4. Network pattern .....	9
3.7.5. Permissions .....	10
3.7.5.1. Accept transfers .....	10

## *Cryptshare Administration Guide*

3.7.5.2.	Deny transfers.....	10
3.7.5.3.	Default Permissions .....	10
3.7.5.4.	Log File Names.....	10
3.7.5.5.	Log Messages.....	10
3.7.5.6.	Log Zip Content.....	10
3.7.5.7.	Show File Names .....	10
3.7.5.8.	Show File Names – User Interface.....	11
3.7.5.9.	Show Zip Content.....	11
3.7.5.10.	Download Notification .....	11
3.7.5.11.	Download Notification – User Interface .....	11
3.7.5.12.	Individual Sender Addresses.....	11
3.7.5.13.	Some Policy Examples.....	11
3.8.	Section 'Log'.....	12
3.8.1.	General .....	12
3.8.2.	Versions before 2.5.1 .....	12
3.8.3.	Version 2.5.1 and higher .....	13
3.8.3.1.	Compatibility to older versions.....	13
3.8.3.2.	Converting old log data .....	13
3.9.	Section 'Licence' .....	14
3.9.1.	Versions from 2.6 on .....	14
3.9.1.1.	Status.....	14
3.9.1.2.	Expiration Date .....	14
3.9.1.3.	Subscription Date.....	15
3.10.	Section 'Terms of Use' .....	15
3.11.	Section 'Languages'.....	15
3.12.	Section 'User Interface Design' .....	15
4.	SSL Certificate	16
4.1.	Location of the SSL Certificate Files.....	16
4.2.	Certificate Signing Request (CSR) .....	16
4.3.	Private SSL Certificate .....	16

## *Cryptshare Administration Guide*

4.3.1. openSuSE.....	17
4.3.2. Other Linux Distributions .....	17
4.4. Public SSL Certificate.....	17
4.5. Cryptshare Robot .....	17
5. PHP Configuration	18
5.1. Maximal Upload Size.....	18
5.2. Further Parameters .....	19

## 1. General

### 1.1. Operating Systems covered by this manual

Operating System	Is supported
openSuSE >= 11.1	yes
Debian	yes
Fedora	yes
Red Hat Enterprise (RHEL)	no
SuSE Linux Enterprise (SLES)	no

If you are free to choose from the supported operating systems we suggest installing on an openSuSE platform, as an RPM Package is available for this platform. For the other platforms installation takes place using an installation script.

Supported operating systems other than openSuSE will be titled with 'Other Linux Distributions' in the rest of this document.

Please note that Windows installations are covered by a separate manual.

### 1.2. The Cryptshare Licence

Cryptshare requires a valid licence key to run. The key contains a list of the client's licensed e-mail domains that correspond to the total number of licensed e-mail users. The licence type will be either for a defined license term or perpetual, depending on what has been purchased.

If Cryptshare is unable to detect a valid licence it will notify you giving a licence error, and should this happen transfers cannot be made.

#### 1.2.1. Cryptshare since version 2.6

Due to changes in the licensing model, this version of Cryptshare is not compatible with other license key files. After installing this Cryptshare version you first need to install a new Cryptshare license key using the Administration Interface.

It is also not possible to operate earlier Cryptshare Versions with a key of the new structure.

A key of the new structure can be identified by the missing version number.

## 2. Administration of the Application

The configuration file 'options.txt' in the subdirectory 'application/htdocs/conf' is critical for the configuration of Cryptshare. Generally a manual adjustment of this file is not necessary, as this can be done using the Administration Interface.

### 2.1. Apache Web Server

#### 2.1.1. SSL Configuration

Cryptshare creates a virtual host configuration file complete with SSL configuration during the installation. To launch the Cryptshare website there must be a valid SSL certificate preinstalled. If there is no valid SSL Certificate the Apache Web Server cannot be started.

#### 2.1.2. PHP Configuration

The web server must be restarted whenever changes in the PHP configuration have been made. This is being done by using the following commands:

- Apache openSuSE: rcapache2 restart
- Apache Linux (other): /etc/init.d/httpd restart

### 2.2. Languages

Please refer to chapter '3.11 - Section 'Languages''

### 2.3. Log Data

Please refer to chapter '3.8 - Section 'Log''

### 2.4. Transfer Administration

The filing directory for transfer data can be configured via the Administration Interface. All files of a transfer are encrypted and stored on the server. Thus the File-ID equals the name of the encrypted file. Metadata related to a transfer are also stored as files. For each recipient one metafile with the Meta-ID as name is stored. The Meta/File-IDs belonging to a transfer are to be found in the Cryptshare Log.

#### 2.4.1. Deletion of a Transfer

Should a specific transfer be deleted, it is generally sufficient to delete the transfers' metadata. Therefore the approach is as follows:

- Identify the Meta-ID of the transfer to be deleted by viewing the log in the Administration Interface.
- Delete the metadata from the upload directory of the server.
- Optionally you can remove the appending data sets from the transfer. To do this repeat the previous steps with the File-ID.

## 2.4.2. Cancelling a Transfer Lock

Cryptshare contains a mechanism for assault detection at the triggering of a transfer download. If a password for a download is typed incorrectly repeatedly, the transfer is deleted or blocked (depending on the configuration you have set).

In case of blocking, the transfer can be reactivated by deleting the Lock-File of the transfer from the upload directory. To do so, proceed as described in chapter '2.4.1 - Deletion of a Transfer'. A Lock-File is named with the additional file extension '.lock'.

## 3. Cryptshare Administration Interface

### 3.1. General

Cryptshare has an Administration Interface from Version 2.2 onwards, with which alterations in the configuration of the Cryptshare Server can easily be made.

For technical reasons settings concerning PHP, cannot be changed via the Administration Interface. This primarily applies to the settings for the configuration of the maximum upload size. Please see section '5 - PHP Configuration'

### 3.2. Login

After the first login the password must be changed. The following passwords are set by default:

Username	Password	Description
Administrator	cryptshare	Default login for the administrator
AssistAdmin	assistadmin	Additional administrator without permission to view log data
LogViewer	logviewer	User who only is allowed to view log data.

### 3.3. Changing passwords

Only the 'Administrator' user can change passwords. All other user accounts do not have permissions to change the password, not even their own password.

### 3.4. Cryptshare License Terms

You need to agree to the Cryptshare License Terms in order to use Cryptshare. Neither the User- nor the Administration Interface are accessible before the license terms have been accepted.

Once accepted, the licence terms can be viewed in the Cryptshare web interface at any time.

## 3.5. Section 'Overview'

This tab is available from Cryptshare Version 2.4 onwards and displays a dump of relevant server data. If an error is detected in the configuration, it is highlighted accordingly.

## 3.6. Section 'Configuration'

This is the main page of the Administration Interface. Most options are preset with default values and should be amended. By moving the cursor over the information-symbols a help text with a short description will pop up.

The following options should be reviewed and if necessary altered:

- Company Information
- Base URL
- Sender Address
- SMTP Host
- Preprocess Command
- Administrator E-Mail
- Logfile notification interval
- Space warning

The most important options are described in detail below.

### 3.6.1. Company Information

Please pay attention when indicating company information and make sure that they comply with the local laws of electronic Information and communication services and data protection.

### 3.6.2. Base-URL

This URL is used to build the links in e-mail notifications. In addition you are re-routed to this URL, when opening the Cryptshare web site. This way re-routing can be effected from http to https, which is strongly advised.

### 3.6.3. Pre-processing data to scan for viruses

You can use the pre-processing option to have your uploaded data virus checked before the files get encrypted and a notification to the recipient takes place.

To do so, put the same command into the field as you would have used in BASH. For instance, to scan for viruses with ClamAV, enter 'clamscan' into the input field.

## 3.7. Section 'Policy'

Via the Policy it is possible to configure who may use the server. The list of policy entries is processed from top to bottom. If an applicable entry is found, this entry will be used. All following entries will be ignored. Therefore please make sure that the entries are listed in the correct order.

The construction of policy rules consists of 4 elements which are described in more detail in the chapters 3.7.2, 3.7.3, 3.7.4 and 3.7.5

### 3.7.1. Automated creation of a default rule set

You can use the button 'Derive default rule set' for deriving default policy rules for all e-mail domains listed in your Cryptshare license.

#### **Derive default rule set**

This generates the default rule set for each e-mail domain that is part of your license and adds it to your policy.

For more detailed information about the default rule see the examples section 'Default Rule Set'.

This operation can be performed at any time. Already existing rule sets won't be affected. Also there won't be any duplicates if default rule sets are already existent.

### 3.7.2. Sender address pattern

Regular expression for checking the e-mail address of the sender. The entry of complete e-mail addresses or certain sender patterns like domains is possible. To allow all members of an e-mail domain as senders, a term like '\*.?\*@yourdomain.com' may be used.

### 3.7.3. Recipient address pattern

Regular expression for checking the e-mail address of the recipient. Please see chapter '3.7.2 - Sender address '.

### 3.7.4. Network pattern

CIDR Notation for an IP Address, respectively an IP address range. By configuring an IP address and the appropriate net mask it is possible to check on the IP address of the sender. If the sender is not part of this IP address range, he is not permitted to perform a Cryptshare transfer.

## 3.7.5. Permissions

Every rule in the policy list can have its own specific permissions. This way additional transfer options for specific sender/recipient combinations can be given.

### 3.7.5.1. [Accept transfers](#)

General permission to perform a transfer on the server. There are no additional permissions activated.

### 3.7.5.2. [Deny transfers](#)

Performing a transfer is not allowed on the server. Additional options are therefore not available.

Please note that 'deny' rules should always be on top of the policy list for security reasons as the list is processed from top to bottom. This way it is made sure that 'deny' rules have a higher priority than any 'allow' rules.

### 3.7.5.3. [Default Permissions](#)

When a new policy rule is created, default permissions will automatically be set which grant the right to perform a transfer on the server. The following options will be enabled additionally:

- Show File Names
- Show File Names – User Interface
- Download Notification
- Download Notification – User Interface

Please read the corresponding chapters for additional information.

### 3.7.5.4. [Log File Names](#)

The default settings only log the file IDs instead of the file names. If this option activated the file names of a transfer are additionally logged with their original file name.

### 3.7.5.5. [Log Messages](#)

If this option is activated, the additional comment message that the sender can enter during the upload process for the transfer is logged.

### 3.7.5.6. [Log Zip Content](#)

If this option is activated, Zip files will be opened and the list of files that are within the Zip file is logged. This option is only functional, if the option '3.7.5.4 - Log File Names' is also activated.

### 3.7.5.7. [Show File Names](#)

If this option is activated, e-mail notifications to the participants of a transfer contain the file names of the transfer.

## 3.7.5.8. Show File Names – User Interface

If this option is activated, an additional checkbox in the user interface is displayed giving the sender the possibility to decide whether the file names in the e-mail notifications will be shown or not.

If the option '3.7.5.7 - Show File Names' is activated, this checkbox will automatically be preselected, but can be deactivated manually.

## 3.7.5.9. Show Zip Content

If this option is activated, Zip files will be opened and its contents will be listed in the e-mail notifications. This option is only functional if the option '3.7.5.7 - Show File Names' is also activated.

## 3.7.5.10. Download Notification

If this option is activated, the sender will receive an e-mail notification when files of the transfer are downloaded.

## 3.7.5.11. Download Notification – User Interface

If this option is activated, an additional checkbox is displayed in the user interface giving the sender the possibility to decide whether he wants to be notified when a file from the transfer is downloaded.

If the option '3.7.5.10 - Download Notification' is also activated, this checkbox will automatically be preselected, but can be deactivated manually.

## 3.7.5.12. Individual Sender Addresses

If this option is activated, the e-mail notifications for the recipients will use the original sender's e-mail address in the SMTP envelope. In case of undeliverable notification mails, this allows SMTP non-delivery-reports to be sent back directly to the individual sender instead of the centrally defined sender address of the server.

## 3.7.5.13. Some Policy Examples

### **Default Rule Set**

In most cases the default rule set can be used. This rule set allows the use of the Cryptshare server for every e-mail address coming from a specific domain.

This rule set has to be defined for every domain that is part of your Cryptshare License.

Sender Pattern	Recipient Pattern	IP Pattern
.*	.*?@yourdomain.com	0.0.0.0/0
.*?@yourdomain.com	.*	0.0.0.0/0

The rule set assures that no external user can abuse the system for non-authorized use.

## *Specific E-Mail Address*

It is also possible to define a rule that applies to a specific e-mail address.

Sender Pattern	Recipient Pattern	IP Pattern
John.Doe@yourdomain.com	.*	0.0.0.0/0

This rule allows John Doe to perform a transfer to an arbitrary recipient. This also includes recipients that are not part of the licenced e-mail domain.

## *Specific IP Range*

Sender Pattern	Recipient Pattern	IP Pattern
.*	.*	192.168.2.10/32
.*?@yourdomain.com	.*	192.168.2.0/24

The first rule allows the host with the IP '192.168.2.10' to use an arbitrary sender address and gives permission to send to any recipient. Please note that at least one participant (sender or recipient) has to be part of a licensed Cryptshare domain.

The second rule allows only senders being part of 'yourdomain.com' to send to any recipient. The sender has to be part of the network '192.168.2.0' and the domain must be part of the Cryptshare License.

## **3.8. Section 'Log'**

### **3.8.1. General**

Cryptshare creates a file in which all relevant processes are logged. You can set the location where the log file is saved using the Administration Interface.

The archiving mechanism of Cryptshare makes sure that the log file does not become oversized. This is a configurable parameter in the Administration Interface.

### **3.8.2. Versions before 2.5.1**

Before Cryptshare version 2.5.1 log data is stored in a structured text file. This file can be viewed in any text editor available.

In older versions the Administration Interface offers the possibility to download the current log file only. It is not possible to view or download log data that has already been archived.

Besides the possibility of downloading the structured log file it is possible to export the selected view (Transfers, Warnings) as a CSV file.

### 3.8.3. Version 2.5.1 and higher

With version 2.5.1, logging has been changed from a structured text file to XML.

When updating an older Cryptshare version the installer will back up all existing logs and archives and convert them to the new format.

The possibility to export the current log data still remains. Additionally it is now possible to view and download archived log data also.

#### 3.8.3.1. Compatibility to older versions

As the new log format is XML new log data is not compatible to older versions of Cryptshare. This also applies the other way around – old log data cannot be viewed in the admin interface of newer Cryptshare versions. It has to be converted to the new format first.

#### 3.8.3.2. Converting old log data

The Cryptshare installer converts existing log data when updating to a newer version.

This process can also be initiated manually at any time.

The converting script can be started as follows:

- `php /opt/cryptshare/admin/htdocs/inc/cslogfix.php`
- Follow the instructions of the script

The converting script is interactive and gives hints on which steps are appropriate in the corresponding situation. In any case the full path to the Cryptshare log file has to be defined. The default path will be pre-selected.

Available possibilities are described below.

#### ***Step 1) Fix a Cryptshare log file***

Due to an error in earlier versions of Cryptshare there may be inconsistencies in the current log file.

This step fixes this error but does not change the format of the log (remains structured text).

**Advice:** Do not perform this step on log archives. This can cause unexpected results. Archives are not affected by the issue mentioned.

#### ***Step 2) Fix existing archives***

Due to an error in earlier versions of Cryptshare it is possible that log archives do not cover the same timeframe as they are labelled with in the file name.

This step merges existing archives and therefore creates archives with the correct timeframe and label.

### **Step 3) Get the match count for a specific log**

This step can be used to perform a manual check for inconsistent log data (as described in Step 1).

It feeds back the amount of valid log entries that have been found in the log.

### **Step 4) Convert one Cryptshare log to XML**

This step converts a single log file from an earlier Cryptshare version (structured text) to the new XML format.

It is recommended to assure the consistency of the log file using step 1) if the file is not an archive.

### **Step 5) Convert all existing log data**

This step converts all existing log data (current and archived) to the new XML format.

Do only perform this step when you are sure that the current log file is consistent (Step 1). This step operates on the current log file as well as on archived log data.

### **Step a) – Default – Steps 1, 2 and 5**

This step executes several of the above mentioned steps in a specific order. This causes all log data to be fixed and converted to the new XML format.

### **Step b) Steps 1 and 2**

This step executes several of the above mentioned steps in a specific order. This causes log data only to be fixed. Conversion to the new format is not being performed.

## **3.9. Section 'Licence'**

In this tab the licence which is required to use Cryptshare can be uploaded. Relevant data from the licence, such as registered domains, are displayed.

### **3.9.1. Versions from 2.6 on**

The Cryptshare license contains information about the license authorization of Cryptshare or add-on products. The following Information can be found in the license.

#### **3.9.1.1. Status**

Indicates whether this product is licensed or not. There are 3 differentiations:

- Product is licensed
- Product is not licensed
- Expiration date is exceeded

#### **3.9.1.2. Expiration Date**

The expiration date defines how long you are eligible to use the product. After expiration the status will change to 'expired'.

### 3.9.1.3. Subscription Date

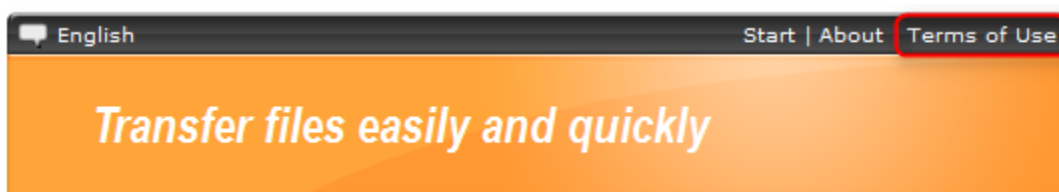
The subscription date defines how long the product is authorized to receive updates. If you install an update after this date, Cryptshare cannot be used.

## 3.10. Section 'Terms of Use'

Cryptshare can be configured so that every user has to accept Terms of Use created by you when verifying.

To define the Terms of Use, you can create a text and add it via the Administration Interface or you can set an external link.

Users can see the Terms of Use at any time via a link in the head of the User Interface.



## 3.11. Section 'Languages'

In this section you can install Language Packages for either Cryptshare or one of its add-on products.

Some language packages only contain translations for the User Interface. In this case, even if another language is selected, the Administration Interface will be displayed in English language.

## 3.12. Section 'User Interface Design'

You can customize the look of your Cryptshare User Interface to reflect your Corporate Design by applying 'User Interface Design Packages' (previously called "CI-Packages") to your Cryptshare system. Using the web-based UI Design Generator in the support area of our web site <http://www.cryptshare.com>, you can create and download your own UI Design package at any time. Installation of this package can be done in this section of the Cryptshare Administration interface.

## 4. SSL Certificate

An SSL Certificate is required to ensure a safe data transfer to the Cryptshare Server. A private or a public certificate can be used.

For creation of a certificate/certificate signing request the tool 'openssl' (<http://www.openssh.com>) is required.

### 4.1. Location of the SSL Certificate Files

The files that will be created in the steps described below need to be stored into the following directories. In general on Linux systems they can be found in the folder '/etc/' respectively in a subdirectory. On openSuSE Systems directory paths are the following:

SSL Key File:	'/etc/apache2/ssl.key/server.key'
SSL Certificate Signing Request (CSR):	'/etc/apache2/ssl.csr/server.csr'
SSL Certificate:	'/etc/apache2/ssl.crt/server.crt'

### 4.2. Certificate Signing Request (CSR)

The CSR is required for both, a private and a public certificate. Hence it must be available in any case.

Specifications made during the creation of a request should conform to the 'whois' entry of the originator. The 'Common Name' or 'Name' must accord with the servers' host address (for example 'cryptshare.befine-solutions.com'). A faulty designation can result in a certificate error. Further optional details can be left out.

To create the request, proceed as follows:

- Create key: `openssl genrsa -des3 -out server.key 2048`
- Change name of file 'server.key' into 'server.key.secure'.
- Decode key: `openssl rsa -in server.key.secure -out server.key`
- Create request: `openssl req -new -days 365 -key server.key -out server.csr`

### 4.3. Private SSL Certificate

A private SSL Certificate created by you offers equal protection to a public certificate. But it may cause a certificate safety warning when a user visits your Cryptshare web site. In this case the warning must be confirmed to be able to make use of the page. Users of Cryptshare-installations must import this certificate into their browser to avoid future safety warnings.

## 4.3.1. openSuSE

It is possible to create a certificate using the script 'certificate.sh' from directory '/usr/share/doc/packages/apache2'

Alternatively the command from chapter '4.3.2 - Other Linux Distributions' can be used.

## 4.3.2. Other Linux Distributions

Use the following command to create an SSL Certificate valid for 365 days:

```
openssl x509 -in server.csr -out server.crt -req -signkey server.key - days 365
```

## 4.4. Public SSL Certificate

A public certificate can be issued by a commercial certificate authority like

- Thawte : [www.thawte.com](http://www.thawte.com)
- VeriSign: [www.verisign.com](http://www.verisign.com)
- GlobalSign: [www.globalsign.com](http://www.globalsign.com)

or any other certificate authority.

These certificates are known to most browsers and so do not cause certificate errors. The page can be used directly by the browser.

## 4.5. Cryptshare Robot

If despite the use of an official certificate a certificate failure occurs during use of the Cryptshare Robot, the certificate in use must be added to the Java certificate store.

The operation is as follows:

- Open the prompt
- Go to the contents of your Java Runtime Environment and subsequently to the subdirectory 'bin'.
- Execute following command:  
'keytool -import -trustcacerts -keystore ../lib/security/cacerts -alias <sitename> -file <SSL Certificate>'

The default password for the Java certificate store is 'changeit'. Confirm the question if the certificate is trustworthy with 'Yes'.

## 5. PHP Configuration

Cryptshare is a PHP application and therefore some settings must be made in an additional configuration file alongside the 'normal' Cryptshare configuration over the Administrator interface. This is the file 'php.ini' which is to be found in the directory '/etc/' respectively '/etc/php5/apache2/'.

Please remember that modifications of the configuration are not effective until the web server is restarted.

### 5.1. Maximal Upload Size

To adjust the maximum upload size for the Cryptshare server, the following parameters must be adapted:

Parameter	Value	Description
post_max_size	2003M	Defines the maximal allowed size of the entire POST-requests. Is this size exceeded, the request is aborted at the beginning of the request. In this case the user does not get a notification. Therefore this parameter should always be set to the maximum value (2003M)
upload_max_filesize	2000M	Indicates the maximum possible size of all files in one upload. Cryptshare uses this value to show an error message when this limit is exceeded (indication on the user interface, elimination of the Upload at overstepping size)

## 5.2. Further Parameters

The following settings should be configured as listed for optimal performance:

Parameter	Value	Description
max_file_uploads	1000	Maximum amount of files a transfer can contain. By default this value is set to 20 which may be too low for certain use cases.  Please be aware that Cryptshare accepts uploads with larger numbers of files but will only deliver the number of files specified by this value.
safe_mode	Off	By activating the „safe mode“ access to files and functions can be limited. This option must stay deactivated during operating Cryptshare (equates the standard setting).
expose_php	Off	This parameter defines if the http-response contains information concerning the PHP version in use.
max_execution_time	28800	Maximum script-execution time in seconds. There must be enough time allowed for the upload of large file transfers.
max_input_time	28800	The maximum admitted time for processing data in seconds. There must be enough time allowed for the upload of large file transfers.
memory_limit	128M	Maximum admitted memory consumption of a script.
error_reporting	E_ALL	Defines the detail level of the logging. If the parameter E_ALL is set, all notifications are logged.
display_errors	Off	Indicates, whether error messages are displayed on the site.
log_errors	On	Indicates, whether error messages are logged (in the PHP default log file)
magic_quotes_gpc	Off	If activated, input data is automatically encrypted.
file_uploads	On	Activates the possibility to upload files on the server.
upload_tmp_dir	/tmp	The temporary directory for uploads before encryption and displacement to the Cryptshare-upload folder.
allow_url_fopen	Off	Processes URLs like files. For safety reasons this option should be set to 'Off'
session.use_only_cookies	1	Defines if the users' Session-ID is only transferred via Cookie. Should be activated, to hinder Session-Hijacking.
session.cookie_httponly	1	Indicates, if a cookie can only be set per http-header (and not for ex. per JavaScript). This hinders certain forms of Cross-Site-Scripting.