



BEFINE

**cryptshare**<sup>®</sup>

# *Large File Transfer*

*made easy and secure*

## *Cryptshare Appliance Administration*

8 November 2011, for Appliances based on openSUSE 11.2/11.4

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)  
Telefon: +49 761 38913-0  
Fax: +49 761 38913-115

# Cryptshare Appliance Administration

1.	Hardware Appliance	4
2.	Virtual Appliance	4
2.1.	Supported Versions.....	4
2.2.	Installation .....	4
2.2.1.	Installation using OVF .....	4
2.2.2.	Installation without OVF .....	4
2.3.	Extend available disk space for Cryptshare transfers .....	4
3.	Administration	5
3.1.	Ports in use .....	5
3.1.1.	Cryptshare activities .....	5
3.1.2.	Additional Ports .....	5
3.2.	Cryptshare Appliance Package .....	5
3.2.1.	Cryptshare Appliance Daemon.....	5
3.2.2.	Automatic Self-Tests of a Cryptshare Appliance.....	6
3.2.3.	Launching Self-Tests of a Cryptshare Appliance Manually .....	6
3.2.4.	Modifying the Tests .....	6
3.2.5.	Linux Distribution Update .....	6
3.2.5.1.	Update Process.....	7
3.2.5.2.	First Notification by the System .....	7
3.2.5.3.	Second Notification by the System .....	7
3.2.5.4.	Enabling/Disabling an Automatic Linux Distribution Update .....	7
3.2.5.5.	Performing a Linux Distribution Update Manually .....	7
3.2.6.	Configuring the Appliance Package.....	8
3.2.6.1.	<i>logfile</i> .....	8
3.2.6.2.	<i>resetInterval</i> .....	8
3.2.6.3.	<i>testInterval</i> .....	8
3.2.6.4.	<i>distLog</i> .....	8
3.2.6.5.	<i>doUpdate</i> .....	8
3.2.6.6.	<i>distUpdate</i> .....	9
3.2.6.7.	<i>updateMessage</i> .....	9

## Cryptshare Appliance Administration

3.2.6.8.	services.....	9
3.2.6.9.	firewallReq .....	9
3.2.6.10.	websiteHost .....	9
3.2.6.11.	websiteReq .....	9
3.3.	Updating the Software Using the Automatic Process.....	10
3.3.1.	Manual Update.....	10
3.3.2.	Cryptshare Updates .....	10
3.4.	Mailing/Postfix .....	10
3.4.1.	Changing the Administrator's Address.....	10
3.4.2.	Changing the Mail Gateway .....	11
3.4.3.	Authentication Data for a Relay Host.....	11
3.5.	SSL Certificate .....	11
3.5.1.	Public SSL certificate .....	11
3.5.1.1.	Installation of the public SSL certificate .....	11
3.5.1.2.	Installation of the key file .....	11
3.5.1.3.	Installation of the Certificate Signing Request File.....	12
3.5.2.	Installation of an intermediate certificate.....	12
3.5.3.	Installation of a root certificate .....	12
3.5.4.	Installation of a private SSL certificate.....	12
3.6.	Update Repository Management .....	12
3.6.1.	Activate/deactivate repository for Cryptshare 2.5 .....	12
3.6.2.	Activate/Deactivate repository for Cryptshare 2.6.....	13

## 1. Hardware Appliance

During the installation of a hardware appliance, please be aware that network interface no. 1 will be used as the network configuration has been set up to use that interface.

## 2. Virtual Appliance

### 2.1. Supported Versions

Cryptshare Virtual Appliances are created on an ESXi Server 3.5 so the Virtual Machine version is version 4.

This version is compatible to VMware ESX Server version 3.0 and higher and VMware Server 1.0 and higher.

### 2.2. Installation

#### 2.2.1. Installation using OVF

If delivered with an 'ovf' file, the Appliance can be imported via the import mechanism of the VMware product in use.

#### 2.2.2. Installation without OVF

If an 'ovf' is not available or the import is not working, a new virtual machine can be set up alternatively. Use the received 'vmdk' file as the virtual disk for the new machine when setting up the new virtual machine.

It is recommended to use 'SuSE Linux Enterprise Server 11 (32bit)' or higher as guest operating system. For all further options the default option selected by the wizard can be used.

### 2.3. Extend available disk space for Cryptshare transfers

By default the available disk space for uploads is very limited (approx. 6-7GB). Therefore it is recommended to add an additional virtual disk with the preferred size to the appliance.

To configure the additional virtual disk as upload directory, start the following command:

- *csAdministration*
- Select option '3) Appliance Configuration' in the menu displayed
- Select option '4) Attach additional harddisk as upload directory for Cryptshare' in the menu displayed

The script will attach the new disk to the system and configure it as new upload directory. Reboot of the Appliance is not necessary.

## 3. Administration

Cryptshare Appliances are configured for minimal administration effort and pre-configured with the network settings provided by you.

Nevertheless it can be necessary to modify those settings, for example when the server is moved to another network.

### 3.1. Ports in use

#### 3.1.1. Cryptshare activities

Function	Protocol	Port (incoming)	Description
Cryptshare Interface	User http	80	Necessary for redirection to Port 443
Cryptshare Interface	User https	443	Necessary for secure access to the user interface.
Cryptshare Administration Interface	https	8080	Necessary for administrating the Cryptshare application. It is recommended to give access to that port only to administrators.

#### 3.1.2. Additional Ports

Function	Protocol	Port (outgoing)	Description
Cryptshare Updates	http	80	Updates for the Cryptshare application
Patch Updates	http	80	Updates for other software components of the system.
ClamAV database updates	virus http	80	Updates for the virus database for the virus scanner clamAV
Connection to the mail relay host	smtp	25	When using a relay server.

### 3.2. Cryptshare Appliance Package

Cryptshare Appliances are equipped with an additional Appliance package that ensures the permanent monitoring of the Cryptshare system and can perform a controlled operating system update to a newer Linux distribution whenever this is required.

#### 3.2.1. Cryptshare Appliance Daemon

The Cryptshare Appliance daemon is a service that runs in the background and continuously monitors the correct operation of the Cryptshare Appliance. The daemon also controls the automated process of a Linux distribution update. See 3.2.5 Linux Distribution Update.

## 3.2.2. Automatic Self-Tests of a Cryptshare Appliance

By default the Cryptshare Appliance daemon runs self-tests every two minutes. The resulting data is stored in a log file.

The following tests are being performed:

- Verifying the status of the relevant services. These include:
  - Apache Web Server: `apache2`
  - E-Mail Server: `postfix`
  - ClamAV Virus Scanner: `clamd`
  - Updating service for ClamAV: `freshclam`
  - Firewall: `SuSEfirewall2`
- Verifying if open ports are specified correctly in the firewall settings.
- Verifying the availability of the Cryptshare website.

## 3.2.3. Launching Self-Tests of a Cryptshare Appliance Manually

All tests can also be launched by running a script from the command line. The results will be displayed on the screen.

For manual execution use the command `'csAdministration'`, and select option `'5) Initiate Appliance self tests'` from the menu.

## 3.2.4. Modifying the Tests

If required it is possible to adjust the check values for the tests. See Section '3.2.6 Configuring the Appliance Package' for details.

## 3.2.5. Linux Distribution Update

Cryptshare appliances use openSuSE Linux as operating system. In normal use it will be necessary to update the operating system to a newer version from time to time, because the old version may no longer be supported by the manufacturer which means that no security updates will be provided any longer. The Cryptshare appliance is capable of performing operating system updates automatically and thereby makes sure that security updates will be received and applied.

Since such an update involves major changes to the system, the automatic update must be enabled by an administrator first.

## 3.2.5.1. Update Process

The process consists of steps that run in succession, where the corresponding components of the system are updated followed by a reboot of the whole system.

After a restart, the Cryptshare package is updated to ensure compatibility with the current PHP version in use.

It is critically important that the update procedure is not interrupted manually to avoid inconsistencies in the system.

If an error occurs and is detected by the update mechanism, the process will be interrupted and attempts are made to roll back the steps that have been taken so far. The administrator will receive an e-mail about a failed attempt to update the system.

Please note that due to technical reasons messages or actions during the process will be displayed or logged with a possible delay of a couple of minutes.

## 3.2.5.2. First Notification by the System

The administrator will be requested by e-mail to enable the process 14 days before the date when a Linux distribution update will be rolled out. You can change the number of days you want to have this information in advance. See 3.2.6 Configuring the Appliance Package. Please note that this notification only takes place once.

## 3.2.5.3. Second Notification by the System

This notification is sent only if a Linux distribution update is enabled and reminds the administrator that the update will be performed on the following night.

## 3.2.5.4. Enabling/Disabling an Automatic Linux Distribution Update

To activate/deactivate the automated distribution update, start the following commands:

- Type in the command *'csAdministration'*
- Select option *'2) Operating System Update'*
- Select option *'1) Activate/Deactivate the automatic Operating System update'*

The script will guide you through the steps required to enable or disable an update.

It is highly recommended to perform a Linux distribution update when it is available. If you do not intend to run an update manually, please enable it to be done automatically now.

## 3.2.5.5. Performing a Linux Distribution Update Manually

If you do not wish to update the system automatically or it is too late to enable an automatic update, you can initiate the distribution update process manually:

- Type in the command *'csAdministration'*
- Select option *'2) Operating System Update'*
- Select option *'2) Upgrade Operating System...'*

Depending on the system, the process takes 1 to 2 hours. Do not interrupt this process!

## 3.2.6. Configuring the Appliance Package

All settings for the Appliance package are being stored in the configuration file 'csappdaemon.properties'. The file is located in '/opt/cryptshare/appliance/conf'.

The most common settings of the Appliance package can be changed by using the command 'csAdministration'. Additional settings (section 3.2.6.8 to 3.2.6.11) can only be changed in the configuration file directly.

Please note that changes should only be done if absolutely necessary. Available settings are described in the sections below.

### 3.2.6.1. logfile

<b>Default value</b>	/var/log/csappdaemon.log
<b>Possible values</b>	Any location
<b>Meaning</b>	The location of the log file for test results and entries by the Cryptshare daemon

csAdministration → 3) Appliance Configuration → 1) Set path to the Cryptshare Daemon log file

### 3.2.6.2. resetInterval

<b>Default value</b>	24
<b>Possible values</b>	1-168
<b>Meaning</b>	An interval in hours for the daemon log file to be reset

csAdministration → 3) Appliance Configuration → 2) Define the reset interval for the Daemon log file

### 3.2.6.3. testInterval

<b>Default value</b>	120
<b>Possible values</b>	1-86400
<b>Meaning</b>	An interval in seconds for the Cryptshare daemon to repeat a system check

csAdministration → 3) Appliance Configuration → 3) Define the test interval for the Daemon log file

### 3.2.6.4. distLog

<b>Default value</b>	/var/log/distupdate
<b>Possible values</b>	Any location
<b>Meaning</b>	The location of a log file to store actions performed in a Linux distribution update

csAdministration → 2) Operating System Update → 3) Specify the log file which the Distribution Update will log its output to

### 3.2.6.5. doUpdate

<b>Default value</b>	no
<b>Possible values</b>	yes,no
<b>Meaning</b>	Defines whether an automatic Linux distribution update is scheduled. This setting can also be enabled by running the script 'EnableDistUpdate.php'.

csAdministration → 2) Operating System Update → 1) Activate/Deactivate the automatic Operating System update

## 3.2.6.6. distUpdate

<b>Default value</b>	2010-08-30/2011-04-29
<b>Possible values</b>	Date for the next scheduled update formatted as YYYY-MM-DD
<b>Meaning</b>	The date scheduled for a Linux distribution update to run csAdministration → 2) Operating System Update → 4) Define the date for the next Distribution Update

## 3.2.6.7. updateMessage

<b>Default value</b>	14
<b>Possible values</b>	1-*
<b>Meaning</b>	Defines the interval between the administrator notification and the Linux distribution update csAdministration → 2) Operating System Update → 5) Set the notification scheme for Distribution Update

## 3.2.6.8. services

<b>Default value</b>	apache2 postfix clamd freshclam SuSEfirewall2
<b>Possible values</b>	Services with an 'rc' init script
<b>Meaning</b>	The services to include in the ServiceCheck test

## 3.2.6.9. firewallReq

<b>Default value</b>	22 25 80 443 8080
<b>Possible values</b>	The parameter 'FW_SERVICES_EXT_TCP' in the firewall settings
<b>Meaning</b>	The test verifies if this value is defined in the firewall settings

## 3.2.6.10. websiteHost

<b>Default value</b>	https://localhost/upload1.php
<b>Possible values</b>	URLs starting with 'http' or 'https'
<b>Meaning</b>	The URL to check the availability of the Cryptshare website

## 3.2.6.11. websiteReq

<b>Default value</b>	before Solutions AG
<b>Possible values</b>	Any text that is part of the website
<b>Meaning</b>	The text is used to validate the code of the web page received using 'websiteHost' to ensure that the page can be processed correctly

## 3.3. Updating the Software Using the Automatic Process

Most updates are performed automatically daily at midnight – 24:00h according to your system time zone settings. If manual steps are required, the administrator will be notified via e-mail.

Appliance use two repositories for performing updates. A default openSUSE update repository and a Cryptshare update repository. The first repository is used for installation of the latest versions of the components of the operating system such as ClamAV. The second is for updating the Cryptshare application and the Cryptshare Appliance package.

Both repositories are updated on a regular basis and checked for compatibility with the installed Cryptshare software. This ensures correct operation of the Cryptshare Appliance after an update was performed.

### 3.3.1. Manual Update

If you wish to perform an update, which requires manual intervention, proceed as follows:

- Type in *'csAdministration'*
- Select option *'1) Start interactive patch routine'*
- Follow the instructions on the screen.

### 3.3.2. Cryptshare Updates

The Cryptshare update mechanism is required to obtain the latest versions of files in a Cryptshare installation. An update of the Cryptshare software is only possible if a valid licence is available for the new Cryptshare version. Your annual subscription package ensures you have the right to use the latest version.

Please contact your reseller to purchase any additional licenses you require.

## 3.4. Mailing/Postfix

The Cryptshare Appliance has been configured to use a Postfix server and uses it as the default mail server. Therefore *'localhost'* is specified as the SMTP server in Cryptshare.

A Postfix server offers detailed reports of exchanged data and multiple attempts to send messages, for example when the destination server is not available. Moreover, it can store authentication data, in case the specified relay server requires authentication.

### 3.4.1. Changing the Administrator's Address

If the e-mail address of the Administrator is changed, you need to make corresponding changes to the Postfix server. Making changes over the Administration Interface is not sufficient as they apply only to the Cryptshare software package.

- Open the file *'/etc/aliases'*.
- Go to a line with the following or a similar text - *'root: <administrator e-mail address>'*.
- Specify the new address.
- Restart the Postfix server by using the command *rcpostfix restart*.

## 3.4.2. Changing the Mail Gateway

If the Appliance has no dedicated mail server and an external server is used to send messages, it may be necessary to adapt the settings of the Postfix server in case the network is restructured.

Use the administration tool 'YAST'. Items in YAST can be selected with arrow keys, Tab, and Return.

- Start the YAST mail configuration interface: `yast mail`
- Use the 'standard' configuration type
- Go on with 'Next' to the page 'Outgoing Mail'
- Type in the new address for the mail server
- Finish the configuration process by using 'Next' and 'Finish'.

You don't need to restart the Postfix server manually. This is being done by YAST itself.

## 3.4.3. Authentication Data for a Relay Host

If the specified relay server requires authentication data, you can set them for the Postfix server. Use the administration tool 'YAST'. Items in YAST can be selected with arrow keys, Tab, and Return.

- Start the YAST mail configuration interface: `yast mail`
- Go on with 'Next' to the page 'Outgoing Mail' and select 'Authentication'.
- Specify the authentication data and confirm the changes by using 'OK'.
- Finish the configuration process by using 'Next' and 'Finish'.

You don't need to restart the Postfix server manually. This is being done by YAST itself.

## 3.5. SSL Certificate

### 3.5.1. Public SSL certificate

#### 3.5.1.1. Installation of the public SSL certificate

Once a public certificate is present, it can be installed on the appliance. To install the certificate on your appliance, proceed as follows:

- Copy the certificate to the appliance (e.g. with WinSCP)
- Start the command `'csAdministration'`
- Select option `'4) SSL certificate administration'`
- Select option `'1) Install public SSL certificate'`

#### 3.5.1.2. Installation of the key file

- Copy the key file to the appliance
- Start the command `'csAdministration'`
- Select option `'4) SSL certificate administration'`
- Select option `'2) Install key file'`

## 3.5.1.3. Installation of the Certificate Signing Request File

- Copy the Certificate Signing Request File (CSR) to the appliance
- Start the command *'csAdministration'*
- Select option *'4) SSL certificate administration'*
- Select option *'3) Install Certificate Signing Request file'*

## 3.5.2. **Installation of an intermediate certificate**

- Copy the intermediate certificate to the appliance
- Start the command *'csAdministration'*
- Select option *'4) SSL certificate administration'*
- Select option *'4) Install intermediate certificate'*

## 3.5.3. **Installation of a root certificate**

- Copy the root certificate to the appliance
- Start the command *'csAdministration'*
- Select option *'4) SSL certificate administration'*
- Select option *'5) Install root certificate'*

## 3.5.4. **Installation of a private SSL certificate**

Using the Cryptshare appliance package you can generate and install a private SSL certificate on your appliance:

- Start the command *'csAdministration'*
- Select option *'4) SSL certificate administration'*
- Select option *'6) Generate and install private SSL certificate'*
- Follow the instructions on the screen.

## 3.6. **Update Repository Management**

Since October 2011 every Cryptshare minor version uses its own repository.

For installation of the preferred Cryptshare version and permanent version updates, the corresponding repository should be activated.

### 3.6.1. **Activate/deactivate repository for Cryptshare 2.5**

To activate the repository for Cryptshare 2.5, proceed as follows:

- Start the command *'csAdministration'*
- Select option *'6) Update Repository Management'*
- Select option *'1) Activate repository for Cryptshare 2.5'*

To deactivate the repository for Cryptshare 2.5, proceed as follows:

- Start the command *'csAdministration'*
- Select option *'6) Update Repository Management'*
- Select option *'1) Deactivate repository for Cryptshare 2.5'*

## 3.6.2. Activate/Deactivate repository for Cryptshare 2.6

To activate the repository for Cryptshare 2.6, proceed as follows:

- Start the command *'csAdministration'*
- Select option *'6) Update Repository Management'*
- Select option *'2) Activate repository for Cryptshare 2.6'*

To deactivate the repository for Cryptshare 2.6, proceed as follows:

- Start the command *'csAdministration'*
- Select option *'6) Update Repository Management'*
- Select option *'2) Deactivate repository for Cryptshare 2.6'*