CIPHERMAIL EMAIL ENCRYPTION

# CipherMail Gateway Upgrade Guide


April 17, 2016, Rev: 10792

# Contents

# 1 Introduction

This guide briefly explains how to upgrade CipherMail to a new version. Sections 2 and 3 and will explain the general upgrade procedure. Section 4 will provide version specific upgrade notes and steps.

# 2 Backup

Before doing any upgrade create a backup of all the system settings with the *Backup Manager* (see Admin → Backup manager). The backup contains all the relevant system settings like users, certificates, keys, MTA settings etc.

**Note:** the SSL certificate for the CipherMail Web admin is not backed-up and should therefore be manually installed after the backup has been restored.

# 3 Upgrade procedure

The actual upgrade procedure depends on how CipherMail is installed/used.

**Note:** after the upgrade, restart your browser or clean the browser cache to make sure that updated CSS files are being refreshed.

## 3.1 Virtual Appliance

If the Virtual Appliance is used, the new Virtual Appliance should be imported into VMware or Hyper-V and the backup should be imported into the new Virtual Appliance. If the default SSL certificate has been replaced it should be imported manually into the new Virtual Appliance.

**Note:** after the backup has been restored, you are advised to immediately create a new backup to make sure that your backup is up-to-date.

## 3.2 Using the packages

If the gateway has been installed with one of the provided packages (.deb or .rpm) the gateway can be upgraded “in place” by installing the new packages. Files which are locally changed (i.e., manually changed on the command line) should be backed-up because some of these files might be overwritten.

### 3.2.1 Upgrade On Ubuntu/Debian

An existing installation of CipherMail can be upgraded in place by installing the new deb packages[1].

[1] If local changes have been made to specific configuration files, the system asks whether to overwrite, merge or keep the local changes. Review the changes and if required, manually apply the required changes after the new packages have been installed

#### Stop services

```
$ sudo service postfix stop
$ sudo service djigzo stop
$ sudo service tomcat6 stop
```

**Note:** Replace tomcat6 with tomcat7 if Tomcat 7 is used instead of Tomcat 6.

#### Update packages

**Note:** If CipherMail is configured for MySQL or Oracle, skip installing the djigzo-postgres package

```
$ sudo dpkg -i djigzo_3.0.5-0_all.deb
$ sudo dpkg -i djigzo-postgres_3.0.5-0_all.deb
$ sudo dpkg -i djigzo-web_3.0.5-0_all.deb
```

#### Clear Tomcat cache

After an upgrade, the Tomcat cache file should be cleared.

> **Note**
>
> Tomcat caches certain files. The cache is not cleared even after a restart of Tomcat. To make sure that files from the previous version of CipherMail do not interfere with files from the newly installed version, you are strongly advised to clear the Tomcat cache.

```
$ sudo rm -r /var/cache/tomcat6/Catalina/localhost/
```

**Note:** Replace tomcat6 with tomcat7 if Tomcat 7 is used instead of Tomcat 6.

#### Restart services

```
$ sudo service tomcat6 restart
$ sudo service djigzo restart
$ sudo service postfix restart
```

**Note:** Replace tomcat6 with tomcat7 if Tomcat 7 is used instead of Tomcat 6.

### 3.2.2 Upgrade On RedHat/CentOS

An existing installation of CipherMail can be upgraded in place by installing the new rpm packages[2].

[2] After upgrading, it's advised to check whether there are any .rpmsave or .rpmnew files. If so, review the changes and if required, manually apply the required changes after the new packages have been installed.

#### Stop services

```
$ service postfix stop
$ service djigzo stop
$ service tomcat stop
```

**Note:** Replace tomcat with tomcat5 or tomcat6 if running on RedHat/CentOS 5 or RedHat/CentOS 6 respectively.

#### Update packages

**Note:** If CipherMail is configured for MySQL or Oracle, skip installing the djigzo-postgres package

```
$ rpm -U djigzo-3.0.5-0.noarch.rpm
$ rpm -U djigzo-postgres-3.0.5-0.noarch.rpm
$ rpm -U djigzo-web-3.0.5-0.noarch.rpm
```

#### Clear Tomcat cache

After an upgrade, the Tomcat cache file should be cleared.

> **Note**
>
> Tomcat caches certain files. The cache is not cleared even after a restart of Tomcat. To make sure that files from the previous version of CipherMail do not interfere with files from the newly installed version, you are strongly advised to clear the Tomcat cache.

```
$ rm -fr /var/cache/tomcat/work/Catalina/localhost/
```

**Note:** Replace tomcat with tomcat5 or tomcat6 if running on RedHat/CentOS 5 or RedHat/CentOS 6 respectively.

#### Restart services

```
$ service tomcat restart
$ service djigzo restart
$ service postfix restart
```

**Note:** Replace tomcat with tomcat5 or tomcat6 if running on RedHat/CentOS 5 or RedHat/CentOS 6 respectively.

### 3.2.3 Complete reinstall

If a complete reinstall has been done, instead of an “in place” upgrade, the backup should be restored and the SSL certificate should be imported.

## 3.3 Using the TAR distribution

If the gateway has been installed with the TAR distribution, the gateway can be upgraded "in place" by installing the TAR the same way as it was previously installed. Files which are locally changed (i.e., manually changed from the command line) should be backed-up because these files will be overwritten. Settings which are stored in the database are not overwritten.

After an "in place" upgrade there is no need to restore the backup or reinstall the SSL certificate. If a complete reinstall has been done, instead of an "in place" upgrade, the backup should be restored and the SSL certificate should be imported.

**Note:** don't forget to restart Tomcat after the upgrade!

# 4 Version specific upgrade notes

This section contains version specific upgrade notes and steps for upgrading a CipherMail gateway to a new version. When upgrading from an older version, all intermediate upgrade steps and notes are relevant. For example when upgrading from version 1.1 the upgrade notes of 1.2.x and 1.3.1 are relevant.

## 4.1 Upgrade from version $\leq$ 1.2.x

### 4.1.1 Manually selected certificates

The main difference, from an upgrade perspective, between version 1.2.x and $\geq$ 1.3.1 is that 1.3.1 introduced a *Certificate Trust List* (see *Administration Guide* for more information).

With versions prior to 1.3.1 if a certificate was manually selected it was implicitly assumed to be valid even if it was expired. Version 1.3.1 now uses a *Certificate Trust List* to control whether a certificate is valid when the PKI rules says it's not ("white list"). A *Certificate Trust List* gives you better control over the trust decision process. Since version 1.3.1 however, manually selected certificates are no longer assumed to be valid by default. Because of this change, it might happen that certificates which were manually selected, even though the certificates were PKI wise not valid (for example the root was not installed), will no longer be used for encryption. To make the gateway use those certificates, the certificates should now be "white listed" by adding them to the *Certificate Trust List*.

CipherMail Version $\geq$ 1.3.1 contains an upgrade tool which can automatically add any manually selected and invalid certificates to the *Certificate Trust List*. The upgrade tool should be manually executed from the bash command shell with the following commands[3]:

```
$ cd /usr/share/djigzo
$ java -cp djigzo.jar mitm.application.djigzo.tools.Upgrade \
-version 1.3
```

[3] If CipherMail is installed in a different directory change the paths accordingly.

After the command has finished executing check the *Certificate Trust List* to see if any entries were added.

**Note:** you only need to run the upgrade tool once and only if you have manually selected invalid certificates for a user or domain and would like the gateway to use those certificates for encryption.

### 4.1.2 Tomcat is now the default

Since version 1.3.1 Tomcat will now be the default Servlet container (previous versions used Jetty). The main reason for this is that Tomcat is better supported with Red Hat/CentOS. If you do an "in place" upgrade to version 1.3.1 and would like to continue using Jetty you should make sure that the SSL certificate is still read and write-able by Jetty after the upgrade:

```
$ sudo chown jetty /usr/share/djigzo-web/ssl/sslCertificate.p12
$ sudo chmod 660 /usr/share/djigzo-web/ssl/sslCertificate.p12
```

**Note:** this is only required if you do an "in place" upgrade and want to continue using Jetty instead of Tomcat.

### 4.1.3 PostgreSQL differences

CipherMail by default uses the PostgreSQL database. Versions of CipherMail prior to 1.3.1 stored a backup of the PostgreSQL database in binary form. This however, can lead to problems when the backup should be restored on server with a different (older or newer) version of PostgreSQL because the binary format is non-portable. Since release 1.3.1 CipherMail will store the database backup in text form to make sure the backup is portable.

**Note:** PostgreSQL used with Red Hat/CentOS is older than the version used with Ubuntu 8.04. If you would like to restore a backup which was created on a Ubuntu version of CipherMail to a gateway that runs on Red Hat/CentOS you should first install version 1.3.2 of CipherMail on the Ubuntu machine and create a new backup. This ensures that the backup uses the text format. The new backup can now be imported into the gateway that runs on Red Hat/CentOS.

## 4.2 Upgrade from version 1.3.1

The following new functions of CipherMail require a change to the Postfix main configuration file (main.cf):

1. Since version 1.3.2 the administrator can specify whether subdomains of the relay domains are accepted as well. With CipherMail prior to 1.3.2 subdomains were always accepted by default.
2. SMTP client authentication can be enabled.

Version 1.3.2 comes with an updated Postfix main configuration file (main.cf). If CipherMail however is updated from a previous version, the Postfix main configuration file is not automatically updated[4].

To support the two new functions (specify whether subdomains match and SASL support) the following lines should be added to Postfix main configuration file. The main configuration file can be edited with **Admin**→**MTA** and then selecting *MTA raw config*.

```
djigzo_parent_domain_matches_subdomains =
parent_domain_matches_subdomains = $djigzo_parent_domain_matches_subdomains
#smtp_tls_security_level = may
#smtp_sasl_auth_enable = yes
#smtp_sasl_password_maps = hash:/etc/postfix/smtp_client_passwd
#smtp_sasl_type = cyrus
#smtp_tls_CApath = /etc/postfix/certs/
#smtp_sasl_security_options =
```

**Note:** If these two new functions are not required you can skip adding these lines.

## 4.3 Upgrade from version $\leq$ 2.1.x

**new portal functionality** The *PDF reply* and external *Quarantine view* pages are now handled by a separate war file (djigzo-portal.war). If the PDF reply page, external Quarantine view page or the new portal functionality should be used, the CipherMail Portal context should be added. See the quick install guide or install guide on how to add the portal context(see paragraph *Adding the Web portal context*).

**Note:** The CipherMail Virtual Appliance already contains the new portal functionality. You only need to enable the portal functionality if you installed CipherMail using the .deb, .rpm or .tar.gz installers.

**PDF reply URL and Quarantine URL** Because the *PDF reply* and external *Quarantine view* functionality are now handled using a separate war file, the *PDF reply URL* and *Quarantine URL* should be updated.

**Note:** Since version 2.3.1, the default reply URL and Quarantine URL are based on the portal *Base URL*. It is therefore advised to change the Base URL of the portal and only change the Reply URL if the PDF reply page or Quarantine view runs separately from the portal. For more information see the Administration guide.

[4]Because the configuration file can be manually edited, an automatic merge is not reliable.

**Wildcard domains** The way wildcard domains are handled has been changed. In version ≤ 2.1.x, test.example.com did not inherit from *.example.com. Since release 2.3.1, test.example.com inherits from *.example.com.

**Default settings** The default value of some settings have been changes

- Default password length is now 16 bytes instead of 8 bytes.
- DLP *quarantine on error* is now true by default.

## 4.4 Upgrade from version ≤ 2.4.x

**Phone number allowed** The SMS option "Phone number allowed" is no longer enabled by default. This is a non-backward compatible change since the default value changed. To revert back to the old behavior, enable the global "Phone number allowed" option.

**Back-end heap size** "Dynamic" memory allocation is now enabled by default for the DEB and RPM packages. The CipherMail back-end now by default uses a heap size of 0.6 * available memory (see /etc/default/djigzo). With previous releases the heap size was set to 512 MB.

## 4.5 Upgrade from version ≤ 2.10.x

### Postfix configuration

An additional injection port on port 10027 for mail sent by GUI (from the *PDF reply* and *Compose a test email* page) was added to make sure that any changes done on the smtpd on port 25 do not interfere with email injection from the GUI.

The easiest way to upgrade master.cf is to copy the new version over the old version:

```
$ sudo cp /etc/postfix/master.cf /etc/postfix/master.cf.bak
$ sudo cp /etc/postfix/djigzo-master.cf /etc/postfix/master.cf
$ sudo service postfix restart
```

Alternatively instead of replacing the old master.cf file with the new, the following service setting can be added to the postfix master config file (master.cf):

### Ubuntu/Debian

```
# injection port for mail sent by web gui
127.0.0.1:10027 inet  n       -       -       -       10      smtpd
            -o smtpd_helo_restrictions=
            -o smtpd_client_restrictions=
            -o smtpd_sender_restrictions=
            -o smtpd_recipient_restrictions=permit_mynetworks,reject
            -o smtpd_tls_security_level=
```

```
            -o mynetworks=127.0.0.0/8
            -o syslog_name=postfix/10027
            -o message_size_limit=${djigzo_before_filter_message_size_limit}
```

**RedHat/CentOS**

```
# injection port for mail sent by web gui
127.0.0.1:10027 inet  n       -       n       -       10      smtpd
            -o smtpd_helo_restrictions=
            -o smtpd_client_restrictions=
            -o smtpd_sender_restrictions=
            -o smtpd_recipient_restrictions=permit_mynetworks,reject
            -o smtpd_tls_security_level=
            -o mynetworks=127.0.0.0/8
            -o syslog_name=postfix/10027
            -o message_size_limit=${djigzo_before_filter_message_size_limit}
```

**Database connection**

The database connection is now specified in a separate xml file. If CipherMail has been configured to use an external database, update the file:

`/usr/share/djigzo/conf/database/hibernate.connection.xml`.

**Tomcat configuration**

The Tomcat SSL/TLS configuration file has been updated to only support strong ciphers. Compare the currently installed Tomcat configuration file with the new Tomcat configuration file and check whether any changes to the list of supported ciphers is required.