EMAIL ENCRYPTION GATEWAY

Email Encryption Gateway TLS Guide

ciphermail
email encryption

April 26, 2017, Rev: 5454

1 Introduction

This guide will briefly explain how to enable TLS for the CipherMail Email Encryption Virtual Appliance.

> **Note**
>
> This guide should only be used with the CipherMail Community Edition. CipherMail Enterprise and SME Edition has an easy to use Web GUI page for installing the TLS certificate.

Note: commands that should be executed by the user are shown on lines starting with a *$* sign (the *$* sign is not part of the command to execute). The commands can be copied and pasted to the command line.

2 Convert pfx/p12 file to PEM format

Postfix requires a plain text PEM encoded file.

> **Note**
>
> This section can be skipped if you already have the certificate and key in PEM encoded form. If the key and certificate are already in PEM form, copy the key and certificate to a single file called `tls.pem` and make sure that the key is not encrypted.

The following commands will extract the certificate and private key from the private key file. The private key file is password protected. The password should therefore be entered when extracting the certificate and private key. The certificate and key will be stored in the file `/etc/postfix/tls.pem`.

```
$ cd /usr/share/djigzo-web/ssl/
$ sudo bash -c 'openssl pkcs12 -in sslCertificate.p12 -nokeys > /etc/postfix/tls.pem'
$ sudo bash -c 'openssl pkcs12 -in sslCertificate.p12 -nocerts -nodes >> \
/etc/postfix/tls.pem'
```

Note: On the question “Enter Import Password:” use the password `djigzo`

Set ownership The PEM file should be owned by root and only readable by root.

```
$ sudo chown root:root /etc/postfix/tls.pem
$ sudo chmod 400 /etc/postfix/tls.pem
```

3 Configure Postfix

Postfix TLS support should be enabled by uncommenting a number of lines from the MTA configuration file. The MTA configuration file can be edited on the *MTA config file* page (Admin→MTA config→MTA config file)
Remove the starting # character from all lines that start with `#smtpd_tls_`. The resulting lines should look like:

```
smtpd_tls_cert_file = /etc/postfix/tls.pem
smtpd_tls_key_file = $smtpd_tls_cert_file
smtpd_tls_security_level = may
smtpd_tls_loglevel = 1
smtpd_tls_exclude_ciphers = EXPORT, LOW
```

After changing the configuration, click the *Apply* button.

4 Finish

Postfix should now support StartTLS. TLS support can be checked using openssl from the command line:

```
$ openssl s_client -connect 127.0.0.1:25 -starttls smtp
```

For more information on TLS support for Postfix see http://www.postfix.org/TLS_README.html.