

DJIGZO EMAIL ENCRYPTION

Djigzo Gateway TLS Guide



Author: Martijn BRINKERS

July 2, 2010, Rev: 4252

1 Introduction

This guide will briefly explain how to enable TLS for the Djigzo gateway SMTP server. This guide assumes that a TLS certificate and associated private key is available as a .pfx file or as separate PEM files¹.

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 Extract certificate and private key from PFX

Postfix requires a separate certificate and key file. If the key and certificate are stored in a PFX file, the certificate and key should be extracted.

Note: This section can be skipped if the certificate and key are already in separate files.

The following commands will extract the certificate and private key from the pfx file. The pfx file is password protected and the password for the pfx file should therefore be entered when extracting the certificate and private key. The certificate will be stored in the file *ssl.pem* and the private key will be stored in the file *ssl.key*².

```
$ openssl pkcs12 -in ssl.pfx -nokeys > ssl.pem
$ openssl pkcs12 -in ssl.pfx -nocerts -nodes > ssl.key
```

Note: It is assumed that the pfx file is named *ssl.pfx*. Change this to match the real pfx filename.

2.1 Copy certificate and private key to Postfix directory

Postfix need to be able to read the certificate and private key. The certificate and private key file will be moved to a sub-directory of the Postfix directory.

```
$ sudo mkdir /etc/postfix/ssl
$ sudo mv ssl.key /etc/postfix/ssl/
$ sudo mv ssl.pem /etc/postfix/ssl/
```

Because the private key file is not password protected, the private key file should only be readable by root.

```
$ sudo chmod 400 /etc/postfix/ssl/*
```

¹Postfix requires that the key file is PEM encoded and not password protected.

²Postfix requires that the private key is not password protected. By adding the parameter *-nodes* the extracted private key will not be encrypted.

3 Configure Postfix

Postfix TLS support should be enabled by adding a few lines to the Postfix main configuration file (`main.cf`). The easiest way to edit the Postfix main configuration file is by using the *MTA raw config* page. The *MTA raw config* page can be opened by clicking **Admin**→**MTA config**→**MTA raw config**.

The following lines should be added to the Postfix main configuration file:

```
smtp_tls_CApath = /etc/postfix/certs/  
smtpd_tls_cert_file = /etc/postfix/ssl/ssl.pem  
smtpd_tls_key_file = /etc/postfix/ssl/ssl.key  
smtpd_tls_security_level = may  
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache  
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
```

By pressing the *Apply* button, all changes will be saved and the updated MTA configuration will be reloaded.

4 Finish

Postfix should now support StartTLS. Using OpenSSL it can be checked whether TLS is correctly setup:

```
$ openssl s_client -connect 192.168.178.52:25 -starttls smtp
```

Note: replace 192.168.178.52 with the correct IP address of the Djigzo gateway.

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