

# Security(ish)

commands the are mostly security and privacy related

- [Extract key/cert from PFX](#)
- [Postfix TLS](#)
- [OpenSSL tricks](#)

# Extract key/cert from PFX

1. Extract key from pfx file

```
openssl pkcs12 -in /path/to/file.pfx --nocerts -out /path/to/exported.key
```

2. Extract certificate from pfx file

```
openssl pkcs12 -in /path/to/file.pfx -clcerts -nokeys -out /path/to/cert.crt
```

3. decrypt private key if desired.

```
openssl rsa -in /path/to/exported.key -out /path/to/decrypted.key
```

# Postfix TLS

## Configuring Postfix to use TLS on CentOS 7

### 1. Install all required packages

```
yum install cyrus-sasl cyrus-sasl-devel cyrus-sasl-gssapi cyrus-sasl-md5 cyrus-sasl-plain postfix
```

### 1b. Backup default postfix config

```
cp /etc/postfix/main.cf /etc/postfix/main.cf_orig
```

### 2. Configure SMTP-AUTH and TLS using postconf

```
/usr/sbin/postconf -e 'smtpd_sasl_local_domain =fqdn.com'  
/usr/sbin/postconf -e 'smtpd_sasl_auth_enable = yes'  
/usr/sbin/postconf -e 'smtpd_sasl_security_options = noanonymous'  
/usr/sbin/postconf -e 'broken_sasl_auth_clients = yes'  
/usr/sbin/postconf -e 'smtpd_recipient_restrictions =  
permit_mynetworks,permit_sasl_authenticated,reject_unauth_destination'  
/usr/sbin/postconf -e 'inet_interfaces = all'  
/usr/sbin/postconf -e 'mynetworks = 127.0.0.0/8, 10.0.0.0/8, 192.168.1.0/24, 192.168.100.0/24'
```

### 3. Set postfix to allow LOGIN and PLAIN logins.

```
vim /etc/sasl2/smtpd.conf
```

```
pwcheck_method: saslauthd  
mech_list: plain login
```

### 4. Create key for SSL certificate signing request

```
mkdir /etc/postfix/ssl  
cd /etc/postfix/ssl/  
openssl genrsa -des3 -rand /etc/hosts -out smtpd.key 1024  
chmod 600 smtpd.key
```

### 5. Create the signing request with the key

```
openssl req -new -key smtpd.key -out smtpd.csr
```

## 6. Create the SSL certificate with the signing request and the key

```
openssl x509 -req -days 3650 -in smtpd.csr -signkey smtpd.key -out smtpd.crt
```

## 7. Create RSA key

```
openssl rsa -in smtpd.key -out smtpd.key.unencrypted  
mv smtpd.key.unencrypted smtpd.key
```

## 8. Create CA key and cert

```
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650
```

## 9. Configure postfix for TLS

```
/usr/sbin/postconf -e 'smtpd_tls_auth_only = no'  
/usr/sbin/postconf -e 'smtp_use_tls = yes'  
/usr/sbin/postconf -e 'smtpd_use_tls = yes'  
/usr/sbin/postconf -e 'smtp_tls_note_starttls_offer = yes'  
/usr/sbin/postconf -e 'smtpd_tls_key_file = /etc/postfix/ssl/smtpd.key'  
/usr/sbin/postconf -e 'smtpd_tls_cert_file = /etc/postfix/ssl/smtpd.crt'  
/usr/sbin/postconf -e 'smtpd_tls_CAfile = /etc/postfix/ssl/cacert.pem'  
/usr/sbin/postconf -e 'smtpd_tls_loglevel = 1'  
/usr/sbin/postconf -e 'smtpd_tls_received_header = yes'  
/usr/sbin/postconf -e 'smtpd_tls_session_cache_timeout = 3600s'  
/usr/sbin/postconf -e 'tls_random_source = dev:/dev/urandom'
```

## 10. Set servers hostname and mydomain in postfix config

```
/usr/sbin/postconf -e 'myhostname = host.yourdomain.com'  
/usr/sbin/postconf -e 'mydomain = yourdomain.com'
```

## 11. Check through the postfix config to verify all of the settings.

```
more /etc/postfix/main.cf
```

## 12. Stop sendmail and Start postfix, saslauthd

```
systemctl stop sendmail  
systemctl restart postfix  
systemctl restart saslauthd
```

# OpenSSL tricks

Download a site's certificate.

This command will connect to example.com on port 443 using the `s_client` subcommand and output the site's certificate information in text format using the `x509` subcommand. The `-text` option tells openssl to print the certificate information in human-readable text format, while the `-noout` option tells it not to output the certificate itself.

You can replace example.com with the hostname or IP address of the site you want to get the certificate for. The `< /dev/null` part of the command is used to prevent the `s_client` command from waiting for input.

```
openssl s_client -connect example.com:443 < /dev/null | openssl x509 -text -outform PEM > /path/to/cert.cer
```