

Certificates and Keystores

As mentioned on [Installing API Management](#), you need a certificate to establish secure connections between clients and API Management, as well as between the different components of API Management itself.



We recommend using an official and valid certificate.

This certificates need to be stored in a Java keystore. On this page you can find some hints regarding certificate and keystore handling.

Certificate Requirements

A certificate consists of two files: **tls.key** and **tls.crt**. Concerning API Management, they must meet the following requirements:

- They have to be imported to a keystore called **apiman.jks**.
To create such a keystore, you can e.g. use the [KeyStore Explorer](#).
- The keystore alias must be **apimancert**.
- The certificate password and the keystore password **must be the same**.
- The following files must be present in folder **api-mgmt/configs**
 - tls.crt
 - tls.key
 - apiman.jks

Hints Regarding Certificate Handling

How to create a keystore if you already have valid certificate files

If you already have a tls.key and tls.crt, you can create a keystore like this:

```
openssl pkcs12 -export -in tls.crt -inkey tls.key -name apimancert -out apiman.p12
```

```
keytool -importkeystore -srckeystore apiman.p12 -srcstoretype PKCS12 -destkeystore apiman.jks -deststoretype JKS
```

File apiman.p12 is only needed temporary, you can delete it afterwards:

```
rm apiman.p12
```

How to export certificate files from a PFX file

If you have your certificate stored in a .pfx file, you need to export the certificate files.

```
openssl pkcs12 -in your_file_name.pfx -nocerts -out tls-encrypted.key
```

```
openssl pkcs12 -in your_file_name.pfx -clcerts -nokeys -out certificate.crt
```

```
openssl rsa -in tls-encrypted.key -outform PEM -out tls.key
```

How to export certificates from a keystore

If you have your official certificate in a keystore and you need the tls.crt and tls.key files, do the following:

On this Page:

- [Certificate Requirements](#)
- [Hints Regarding Certificate Handling](#)
 - [How to create a keystore if you already have valid certificate files](#)
 - [How to export certificate files from a PFX file](#)
 - [How to export certificates from a keystore](#)

Related Pages:

- [Installing API Management](#)

Related Documentation:

- [KeyStore Explorer](#)

```
keytool -importkeystore -srckeystore your_file_name.jks -destkeystore  
apiman.p12 -deststoretype PKCS12
```

```
openssl pkcs12 -in apiman.p12 -nokeys -out tls.crt
```

```
openssl pkcs12 -in apiman.p12 -nocerts -nodes -out tls.key
```

File apiman.p12 is only needed temporary, you can delete it afterwards:

```
rm apiman.p12
```