


Importing Custom SSL Certificates

You can generate your own `ssl_keystore` and `ssl_truststore` files by running the `configure.sh` script with the `-nocerts` flag. The `-nocerts` flag suppresses automatic generation of keystore and truststore files. The location of your own storefiles should also be specified in the `mapr.login.conf` file. Contact MapR Support for assistance in generating JKS-format storefiles from your vendor-supplied certificates.

The default keystore contents are generated during installation. To add an existing certificate and its corresponding key from a vendor to the keystore, use the `keytool` command.

 **Note:** The default password for the keystore is `changeit`.

The following steps assume your vendor has delivered the certificate in Java KeyStore (JKS) format, or another format supported by the `keytool` utility.

1. Run the `configure.sh` script with the `-nocerts` flag.
2. Run the `keytool` command to import your certificate into the keystore.
 - Use a syntax similar to the following:

```
keytool -import -trustcacerts -file  
    <certificate>.crt -alias <hostname> -keystore <keystore_location>
```

3. Verify that the certificate is now in the keystore using the `keytool` command.

```
keytool -list -v -keystore <keystore_location>
```

4. Contact MapR Support to modify the `mapr.login.conf` file.