

eMudhra certificate compromise: GraalVM Native Image advisory

Last updated: October 23, 2026

Native Image captures the default trust store and certificate blocklist at build time. Updating the JDK or replacing its `lib/security/blocked.certs` file does not update an existing native image executable. See [Certificate Management in Native Image](#) for details on build-time capture and runtime trust-store overrides.

The following options are only applicable if you use the default JDK trust manager:

Option 1: Remove the affected trust roots and rebuild

Back up the trust store used to build the application, then remove:

- **emSign ECC Root CA - G3**
- **AAA Certificate Services**, which provides the cross-signed trust path

For the default JDK trust store, the [Java advisory](#) provides these commands. Run them using the JDK used by Native Image:

```
keytool -delete -cacerts -alias "emsigneccrootcag3 [jdk]"
keytool -delete -cacerts -alias "comodoaaaca [jdk]"
```

Then rebuild your native images and redeploy.

Option 2: Override the trust store without rebuilding (expert option)

For applications using the default Java TLS trust manager, an existing native executable can use a replacement trust store at startup:

```
./application \  
-Djavax.net.ssl.trustStore=/absolute/path/hotfix-truststore.p12 \  
-Djavax.net.ssl.trustStoreType=PKCS12
```

Prepare a replacement store as described above. Restart the application with the replacement store. No rebuild is required for this option. However, keep in mind that the replacement store replaces, rather than supplements, the embedded default trust store.

Option 3: Enable and verify revocation checking

The [Java advisory](#) describes enabling TLS revocation checking with:

```
-Dcom.sun.net.ssl.checkRevocation=true  
-Dcom.sun.security.enableCRLDP=true
```

Do not assume that adding these flags to an existing native image is sufficient!

Relevant settings may have been captured during build-time class initialization. Before relying on this option, confirm that the executable rejects the affected chains and that revocation checking behaves appropriately when revocation information is unavailable.

Also, these settings affect all applicable Java TLS certificate validations in the executable, not only certificates associated with eMudhra. Unavailable or expired revocation information can cause otherwise legitimate connections to fail.

Validate the remediation

GraalVM Native Image applications using Java TLS certificate validation may trust certificate chains containing the compromised eMudhra intermediate CA certificates. Oracle's [Java advisory](#) describes the incident and provides JDK updates and mitigation options.

Test rejection against the incident's test endpoints. Two published examples cover the eMudhra and AAA cross-signed paths:

- <https://dv-g3b-emudhra.we-have-a-problem.com/>
- <https://dv-g3b-aaa-emudhra.we-have-a-problem.com/>

Configure a test instance of the native image application to request these URLs without credentials or application data. The [incident site](#) also provides `chains.zip` covering all twelve TLS test hosts. The two URLs above are a spot check, not complete coverage.

The options described above apply to applications using Java's default TLS trust infrastructure. Applications using custom trust managers, independently configured TLS contexts, or separate native TLS libraries require assessment and remediation of those configurations.