Enabling SSL in MITS Tomcat

Applies to: MITS | Component: Tomcat (bundled instance) | Level: Advanced

> **Upgrade note:** These changes may be overwritten when MITS is upgraded. Back up your keystore and reapply this configuration after each upgrade.

PHASE 1 — CERTIFICATE SETUP

1. Stop the MITS service

MITS will be unavailable while SSL is being configured.

2. Navigate to the MITS conf directory

Open a terminal and change into the Tomcat config directory. All subsequent commands should be run from here.

PATH

```
<mits_install>/webserver/conf
```

3. Generate a public/private key pair

Uses the bundled JRE's keytool to create a 2048-bit RSA keypair in a new keystore file.

COMMAND

```
../../jre/bin/keytool -genkeypair \
  -alias server \
  -keyalg RSA \
  -keysize 2048 \
  -keystore mits-tomcat.jks \
  -dname "CN=<domain>" \
  -storepass <password>
```

EXAMPLE

```
../../jre/bin/keytool -genkeypair \
  -alias server -keyalg RSA -keysize 2048 \
  -keystore mits-tomcat.jks \
  -dname "CN=alpha.example.com" \
  -storepass password_goes_here
```

4. Generate a certificate signing request (CSR)

COMMAND

```
../../jre/bin/keytool -certreq \
```

```
  -alias server \
  -keystore mits-tomcat.jks \
  -file mits-tomcat.csr \
  -storepass <password> \
  -ext san=dns:<domain>
```

EXAMPLE

```
../../jre/bin/keytool -certreq \
  -alias server -keystore mits-tomcat.jks \
  -file mits-tomcat.csr \
  -storepass password_goes_here \
  -ext san=dns:alpha.example.com
```

5. Sign the certificate with your domain registrar

Submit `mits-tomcat.csr` to your CA. Follow their process to obtain a signed certificate, then place the resulting file on the MITS server or a network location it can reach.

6. Import the signed certificate into the keystore

COMMAND

```
../../jre/bin/keytool -importcert \
  -alias server \
  -keystore mits-tomcat.jks \
  -storepass <password> \
  -file <signed_cert_file>
```

EXAMPLE

```
../../jre/bin/keytool -importcert \
  -alias server -keystore mits-tomcat.jks \
  -storepass password_goes_here \
  -file cert_with_chain.pem
```

7. Back up mits-tomcat.jks

Copy the keystore to a safe location before proceeding. You will need it to restore SSL after future MITS upgrades without going through the signing process again.

PHASE 2 — TOMCAT CONFIGURATION

8. Edit server.xml

Open the file at `[MITS_Install]/webserver/conf/server.xml`. Two changes are needed:

A — Update the non-SSL connector

Locate the existing HTTP connector and ensure `redirectPort` is set to `8443`.

NON-SSL CONNECTOR (VERIFY REDIRECTPORT)

```
<Connector address="127.0.0.1"
  port="8080" protocol="HTTP/1.1"
  connectionTimeout="20000"
  redirectPort="8443" URIEncoding="UTF-8"
  compression="on"
  maxPostSize="16777216"
  useSendfile="false"
  compressableMimeType="text/html,text/xml,text/plain,
    text/css,text/javascript,application/javascript,
    image/svg+xml"/>
```

B — Uncomment and configure the SSL connector

Find the commented-out SSL connector block and remove the surrounding `<!--` and `-->`. Then apply the edits below.

SSL CONNECTOR (AFTER EDITS)

```
<Connector port="443"
  protocol="org.apache.coyote.http11.Http11NioProtocol"
  maxThreads="150" SSLEnabled="true"
  URIEncoding="UTF-8" compression="on"
  maxPostSize="16777216" scheme="https"
  useSendfile="false" secure="true"
  compressableMimeType="text/html,text/xml,...">
  <SSLHostConfig protocols="+TLSv1.2" ciphers="...">
    <Certificate
      certificateKeystoreFile="conf/mits-tomcat.jks"
      certificateKeystorePassword="<your_password>"
      type="RSA" />
  </SSLHostConfig>
</Connector>
```

> **Port note:** Change 8443 to 443 so users do not need to specify a port in the URL. Preserve the full cipher list from the original file.

9. Update firewall rules

Open inbound port `443` to the MITS server. Remove or retain port `8080` access based on your environment's requirements.

10. Save server.xml and restart the MITS service

Start the service and confirm it comes up without errors before testing.

11. Verify the secure URL

Navigate to your domain over HTTPS and confirm the certificate is valid.

EXAMPLE

```
https://alpha.example.com
```

If users were previously accessing MITS over HTTP, update them with the new address or configure a DNS-level redirect from the non-secure path.