

Hardening Tomcat

Secure SSL ciphers

If you are running your Tomcat installation behind a reverse proxy, these recommendations will not be needed, as Tomcat is not terminating SSL/TLS.

Change the HTTP connector please use the following ciphers (<tomcat>\conf\server.xml)

```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,  
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,  
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256,  
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_GCM_SHA256
```

List updated: 2018-02-07

Secure headers

If you are running your Tomcat installation behind a reverse proxy, these recommendations will not be needed, as Tomcat is not terminating SSL/TLS.

In the SERVER web.xml (<tomcat>\conf\web.xml) uncomment the following sections

```
<filter>  
  <filter-name>HTTPHeaderSecurity</filter-name>  
  <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>  
  <async-supported>true</async-supported>  
  <init-param>  
    <param-name>antiClickJackingOption</param-name>  
    <param-value>SAMEORIGIN</param-value>  
  </init-param>  
</filter>
```

```
<filter-mapping>  
  <filter-name>HTTPHeaderSecurity</filter-name>  
  <url-pattern>/*</url-pattern>
```

Additional CSRF filtering

The TS platform is already safe from CSRF attacks. CSRF tokens are generated at login and required for all data altering transactions.

The TS implementation does not use rotating or page specific CSRF tokens, so if additional security is needed use the OWASP implementation.

Additional security filters

Tempus Serva comes with multiple additional security features

- Lock user session to IP
- Lock service to listed countries
- Use passcode sent by SMS

The filters are activated by uncommenting the code in the applications /WEB-INF/web.xml.

Note that the filters can be set any part of the application: login, designer, webinterface and rest.

Validating your site

You can use the following services to check the security of your installation

Test SSL

Tip: Remember to check "Do not show the results on the boards"

<https://www.ssllabs.com/ssltest/>

<https://sikkerpånettet.dk/>

Test Headers

<https://tools.geekflare.com/report/header-security-test>