# Grouper v2.5 customize UI security headers



This wiki gives examples on how to customize the Grouper UI security headers for your institution.

Note: There is a different Grouper feature to create a custom UI per group.

## Adding security headers

Web security scans may result in recommendations to add browser headers to lessen the risk of hijacking vectors. There are ways to add these headers via Apache, TomEE/Tomcat, or through the web application. The following demonstrates how these headers can be added to the Grouper UI via web.xml customizations

TomEE and Tomcat have a Filter class available for adding certain browser security headers. With the default settings, adding the filter to /opt/grouper /grouperWebapp/WEB-INF/web.xml will set:

- Strict-Transport-Security: Strict-Transport-Security: max-age=0 (parameter hstsEnabled)
- X-Frame-Options: DENY (parameter antiClickJackingEnabled)
- X-Content-Type-Options: nosniff (parameter blockContentTypeSniffingEnabled)
- X-XSS-Protection: 1; mode=block (parameter xssProtectionEnabled)

```
    <!-- https://tomcat.apache.org/tomcat-8.5-doc/config/filter.html
      * By default, sets:
      *    - (hstsEnabled) Strict-Transport-Security: Strict-Transport-Security: max-age=0
      *    - (antiClickJackingEnabled) X-Frame-Options: DENY
      *    - (blockContentTypeSniffingEnabled) X-Content-Type-Options: nosniff
      *    - (xssProtectionEnabled) X-XSS-Protection: 1; mode=block
     -->
    <filter>
        <filter-name>httpHeaderSecurity</filter-name>
        <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
        <async-supported>true</async-supported>
        <!-- these are defaults -->
        <!--
        <init-param>
            <param-name>hstsEnabled</param-name>
            <param-value>true</param-value>
        </init-param>
        <init-param>
            <param-name>antiClickJackingEnabled</param-name>
            <param-value>true</param-value>
        </init-param>
        <init-param>
            <param-name>blockContentTypeSniffingEnabled</param-name>
            <param-value>true</param-value>
        </init-param>
        <init-param>
            <param-name>xssProtectionEnabled</param-name>
            <param-value>true</param-value>
        </init-param>
        -->

        <!--  for the HSTS header, the default is hstsIncludeSubDomains=false and hstsMaxAgeSeconds=0. Setting
these
               from the defaults will enhance security
        -->
        <!--
        <init-param>
            <param-name>hstsIncludeSubDomains</param-name>
            <param-value>true</param-value>
        </init-param>
        <init-param>
            <param-name>hstsMaxAgeSeconds</param-name>
            <param-value>15768000</param-value>
        </init-param>
        -->
    </filter>
    <filter-mapping>
        <filter-name>httpHeaderSecurity</filter-name>
        <url-pattern>/*</url-pattern>
    </filter-mapping>
```

The Content-Security-Policy (CSP) header is one header that can't be added with the Tomcat supported filters. A separate Grouper filter class exists[2.5.28] to enable this header. The init parameter `value` can define an arbitrary CSP value. If a value is not set, the built-in default is a reasonable set of options for Grouper (allow inline Javascript including evals).

```
    <filter>
        <filter-name>ContentSecurityPolicyFilter</filter-name>
        <filter-class>edu.internet2.middleware.grouper.ui.ContentSecurityPolicyFilter</filter-class>
        <!-- default value is already suitable for Grouper
        <init-param>
            <param-name>value</param-name>
            <param-value>frame-ancestors 'none'; default-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-
inline' 'unsafe-eval';</param-value>
        </init-param>
        -->
    </filter>
    <filter-mapping>
        <filter-name>ContentSecurityPolicyFilter</filter-name>
        <url-pattern>/*</url-pattern>
    </filter-mapping>
```

Add a custom header image

Customize the text