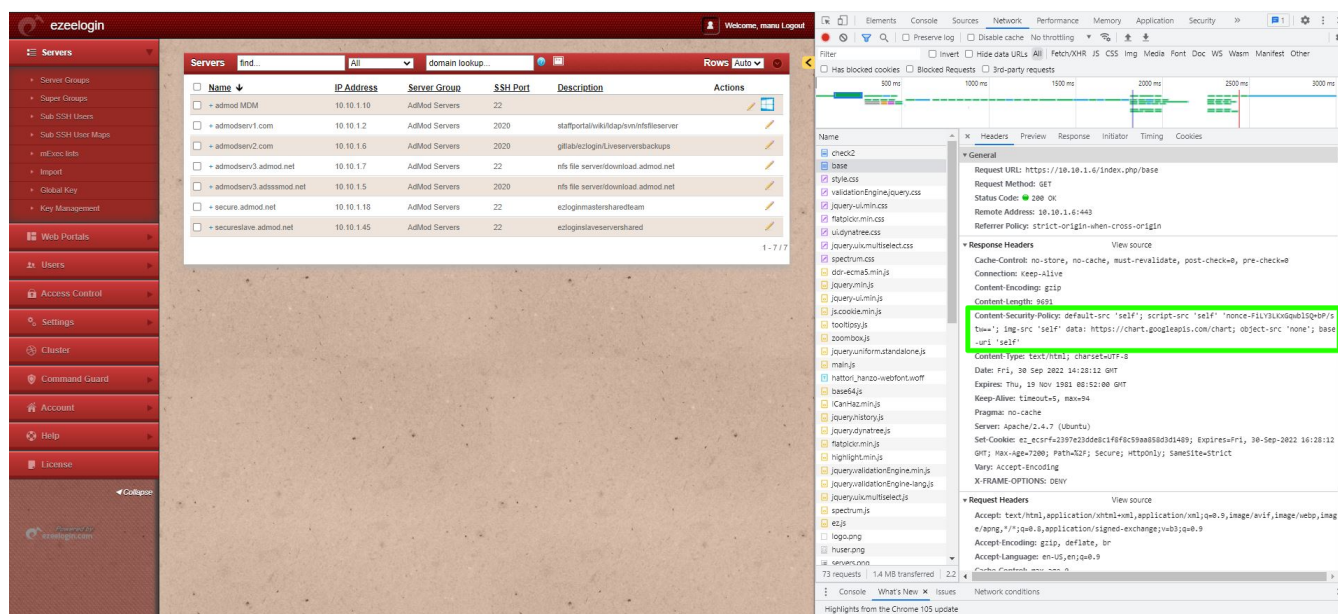# Content Security Policy in Ezeelogin GUI

Content Security Policy (CSP) in the Ezeelogin web framework explained

Content-Security-Policy headers have been updated in the **Ezeelogin version 7.29.0**. Refer below article to update Ezeelogin to the latest version.

[Upgrade the Ezeelogin Jumpserver to the latest version](#)

Ezeelogin GUI uses dynamic scripts and it needs to use **nonce**. But nonce needs to be dynamic and hence cannot be set in httpd.conf or any web server configuration because it is only static. **CSP headers are set from the Ezeelogin application itself**. Users need not set any headers in httpd.conf for Ezeelogin. Refer below screenshot to view the CSP header being set when the user accesses the Ezeelogin web panel - without any 'unsafe' option.

To view the **Content-Security-Policy**, use the **F12 key** or **right-click on the Ezeelogin software GUI -> Inspect -> Network -> base-> Headers -> Response Headers -> Content-Security-Policy**. Refer below screenshot.

Refer below screenshot to find Content-Security-Policy with **"unsafe-inline"** in prior Ezeelogin version 7.29.0.
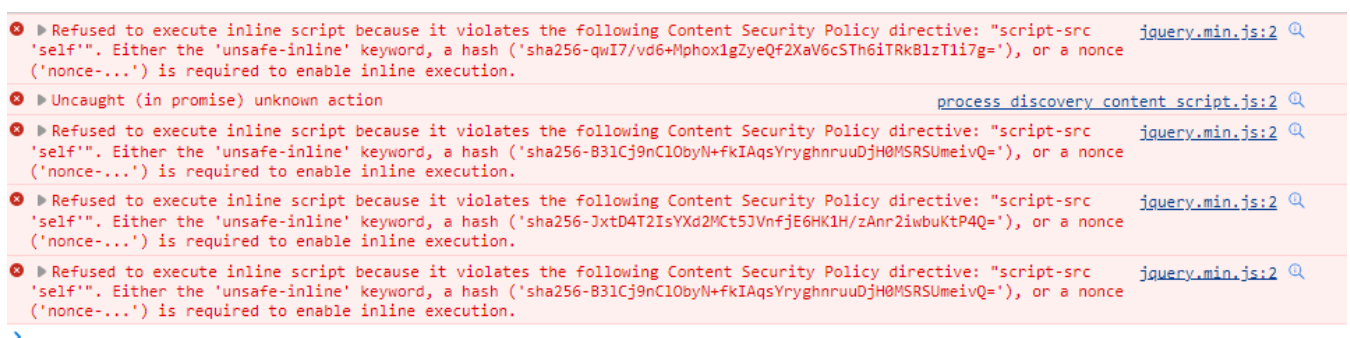
To view the **Content-Security-Policy**, use the **F12** key or **right-click on the Ezeelogin software GUI -> Inspect -> Network -> base-> Headers -> Response Headers -> Content-Security-Policy**. Refer below screenshot.

Header always set Content-Security-Policy "default-src 'self'; style-src 'self' '**unsafe-inline**'; frame-ancestors 'self'; script-src 'self' '**unsafe-inline**';"
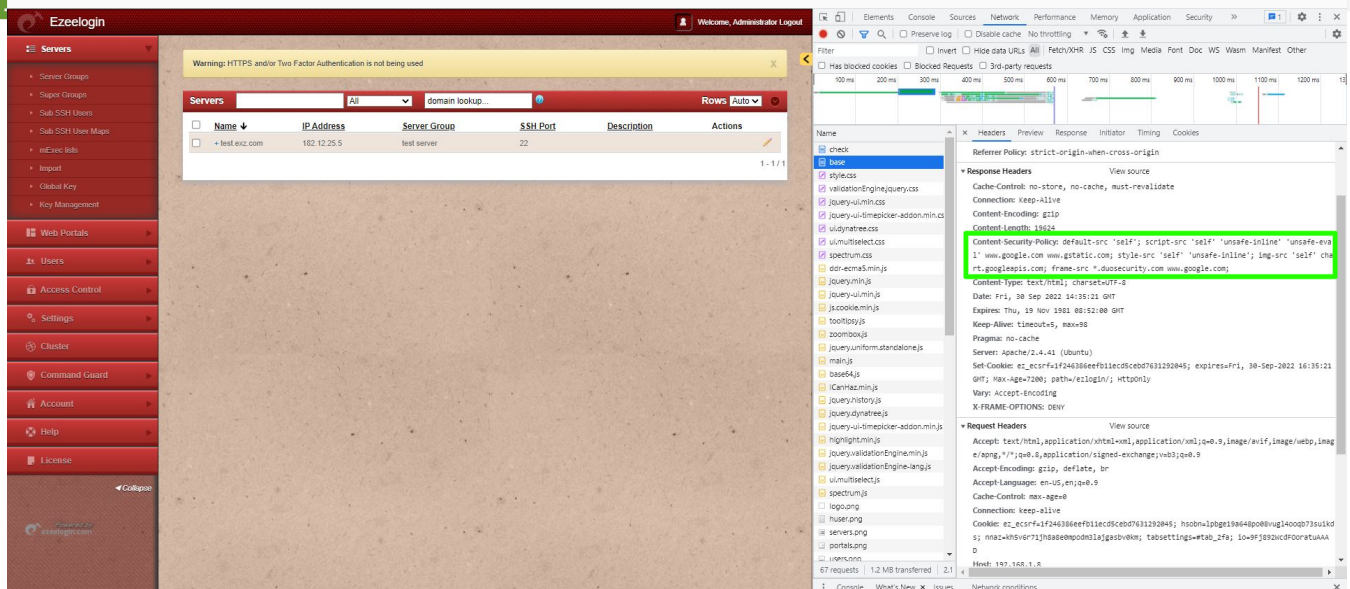
Error when enabling **Header always set Content-Security-Policy "default-src 'self'; frame-ancestors 'self';"** in httpd.conf.

Refer below screenshot for the browser console error when **Header always set Content-Security-Policy "default-src 'self'; frame-ancestors 'self';"** is enabled in **httpd.conf**.

Online URL: https://www.ezeelogin.com/kb/article/content-security-policy-in-ezeelogin-gui-553.html