


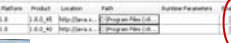







## Chrome



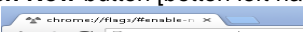
### Java settings –

[Note: Running the latest version Java might result in intermittent access issues with Timekeeper applications over VPN]

1. Click start  → Open Control Panel → Double click Java icon .
2. Click Java tab .
3. Click View and enable Java , then click cancel.
4. Click Security tab .
5. Check Enable Java content in the browser .
6. Click Advanced tab  → under **Default Java for browser**, **check** Mozilla family.
7. Under the Advanced tab, make sure there's a check mark next to the settings below. Leave *Use SSL 2.0 compatible ClientHello format* uncheck. Click Apply button.

- a.  Default Java for browsers
- Microsoft Internet Explorer
  - Mozilla Family
- b.  Advanced Security Settings
- Use certificates and keys in browser keystore
  - Enable blacklist revocation check
  - Enable caching password for authentication
  - Use SSL 2.0 compatible ClientHello format
  - Use TLS 1.0
  - Use TLS 1.1
  - Use TLS 1.2

### Browser settings -

1. If running version 42.x and above, open Chrome  browser and type `chrome://flags/#enable-ntpapi`  and press enter.
2. Click **Enable** under Enable NPAPI and then click **Relaunch Now** button [botton left hand corner] .
3. Once Chrome browser is back up, type `connect.cps.edu`  and press enter.