Tip of the Week: Session Timeout Duration

Ever noticed that unlike your bank, your social media accounts keep you logged in for months at a time? Session timeout durations are important in reducing the risk of exposure to session-based attacks. These are attacks where a hacker can use a valid session ID and hijack it. In order to do so, the session must be active. Session timeouts give attackers less time to use a valid session ID. As a law firm handling sensitive client data, it is your responsibility and obligation to evaluate your firm's environment of risk. Setting up a session timeout duration is a security enhancement that TimeSolv offers its users. This week's Tip of the Week takes a look at how to customize your firm's session timeout duration.

As a firm Admin, click on **Account>Settings**. Towards the bottom of the **General** tab, you will see a '**Security**' section. The first field under it is '**Session Timeout Duration (hours)**'; this is the length of time a user can remain logged on to the TimeSolv web app while there is no activity taking place. TimeSolv automatically ends a Tiimekeeper's session once the defined amount of time has elapsed. For example, if you would like inactive users to be automatically logged out after 30 minutes, enter 0.5.

TimeSolv's default value is set to 30 minutes.

If you find you are being logged out sooner than your Session Timeout Duration settings note the session keep-alive only works when the following conditions are met:

- The browser is open, which implies the computer is on.
- The browser has a TimeSolv web app main page in it.
- The computer is connected to the Internet.

Unless the above conditions are met, the user will be logged out in the defined amount of time. If the user wants to close the browser, disconnect

the Internet, sleep, hibernate, or shut-down the computer, TimeSolv will not keep the session alive.

If you'd like to contact TimeSolv support for help, please call 1.800.715.1284 or Contact support!

Contact Support