User Authorization

Authorization is a necessary condition for users to access the internet.

General Information

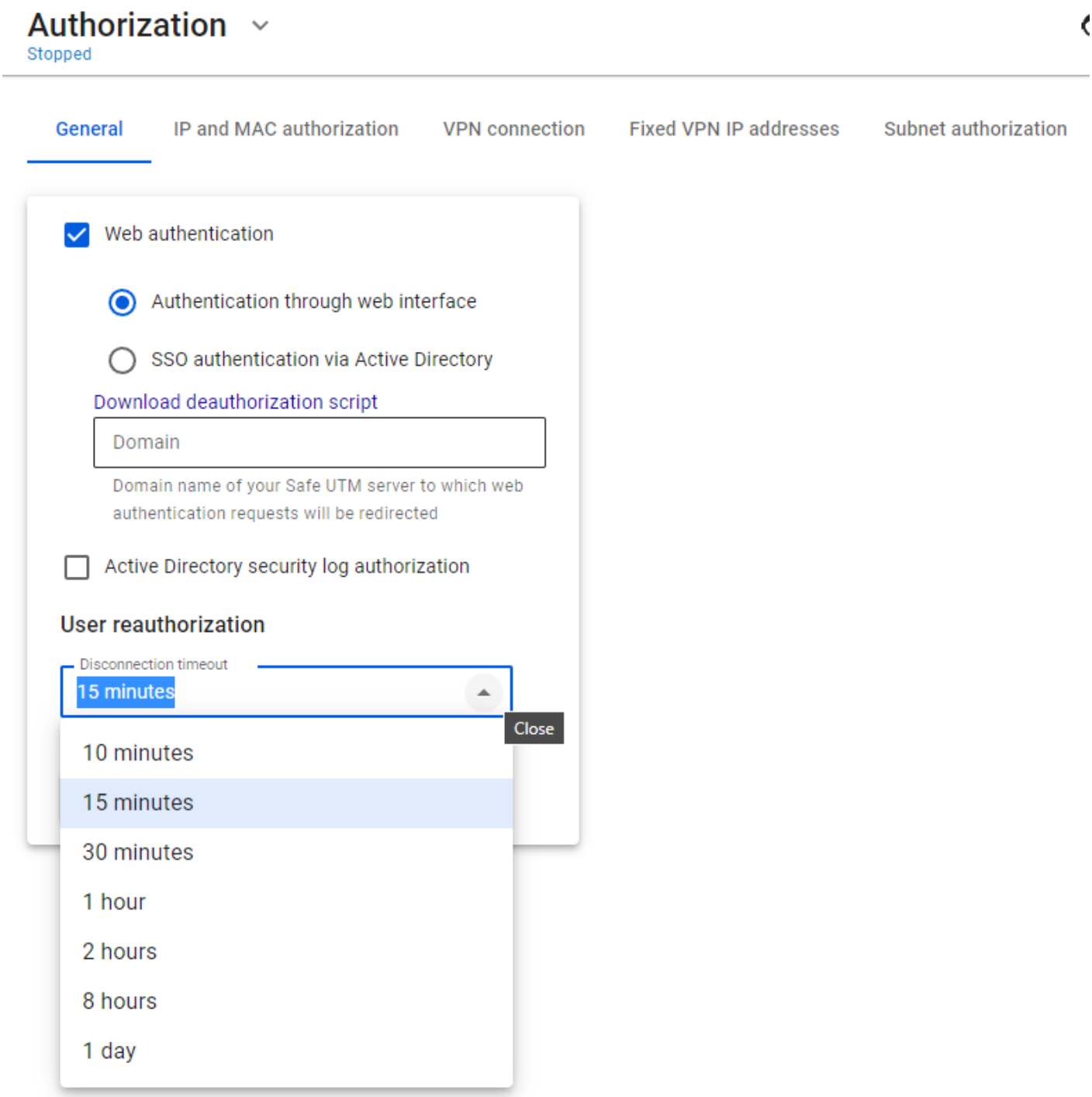
There are several authorization methods that you can find in this subsection.

All types of authorizations on SafeUTM are IP-based (based on the host IP address) and any authorization session is bound to the IP of the host from which it was installed. Simultaneous authorization of up to five devices is possible under one user account (by dynamic authorization methods, web, Kerberos/NTLM, security logs of Active Directory domain controllers, and VPN).

The user is automatically logged out when inactive (no internet connections) for 15 minutes (except connections via VPN).

> Keep in mind, that the operating system itself can also generate traffic (for example Windows telemetry) without user intervention. Because of this, the timeout for the user will be constantly reset and will not be able to function correctly.

You can change the time of automatic logout using the settings **Disconnection timeout** by going to **Users -> Authorization**:



For the new timeout to be applied, you need to reboot SafeUTM.

You can also authenticate users connecting via VPN using **IPSec IKEv2**, **SSTP**, **L2TP IPSec**, **PPTP**, and **PowerShell scripts**.

Revision #6
Created 22 August 2022 14:56:33 by Val Redman
Updated 11 October 2022 23:57:23 by Val Redman