Installation GlobalProtect Agent Software

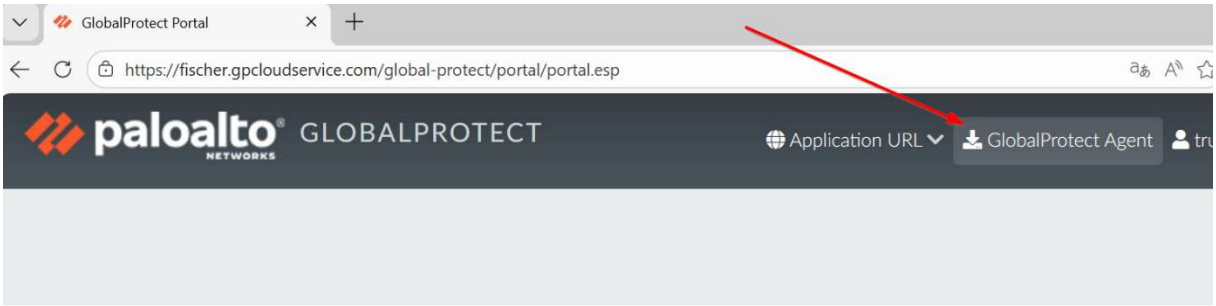
Voraussetzungen:

- fischer Anmeldedaten müssen vorliegen
- Für die Installation werden administrative Rechte benötigt. Daher kann es notwendig sein, einen Termin mit ihrem eigenen IT-Support zu koordinieren.

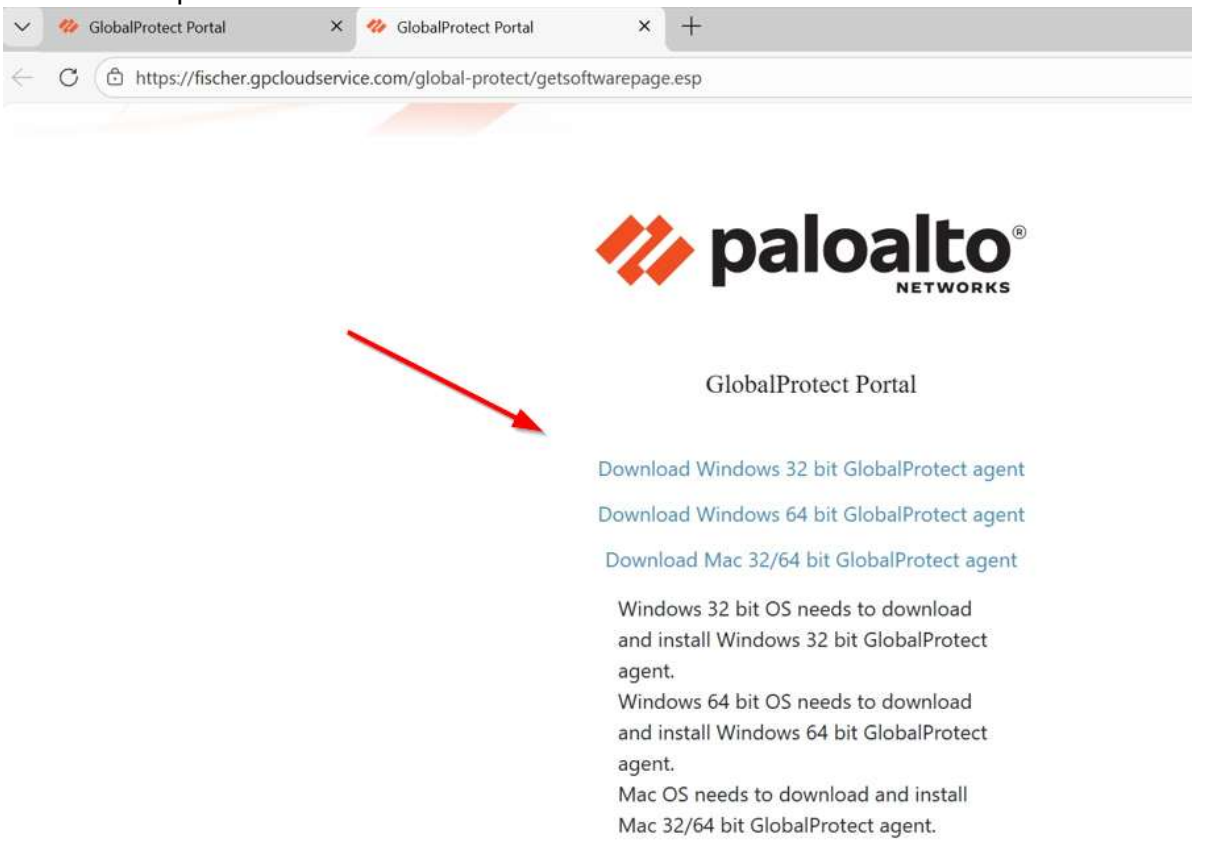
Sollte die GlobalProtect Agent Software bereits installiert sein, ist die Benutzung bereits bekannt. In diesem Fall kann einfach das Portal ‘fischer.gpcloudservice.com’ hinzugefügt werden.

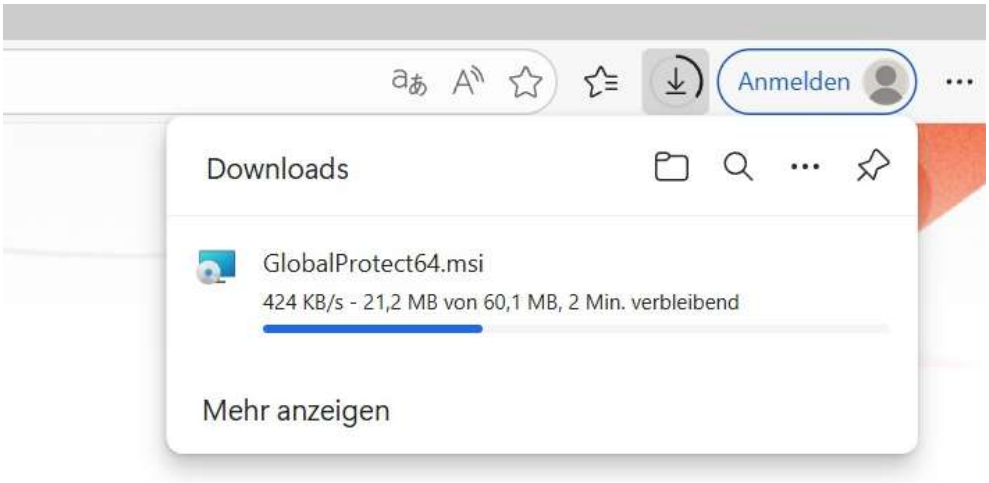
Ist die Software noch nicht installiert, bitte laden Sie sie herunter und installieren sie:

Dazu im Browser 'https://fischer.gpcloudservice.com' eingeben und dort mit den fischer Anmeldedaten einloggen. Nach der Anmeldung auf 'GlobalProtect Agent' navigieren:



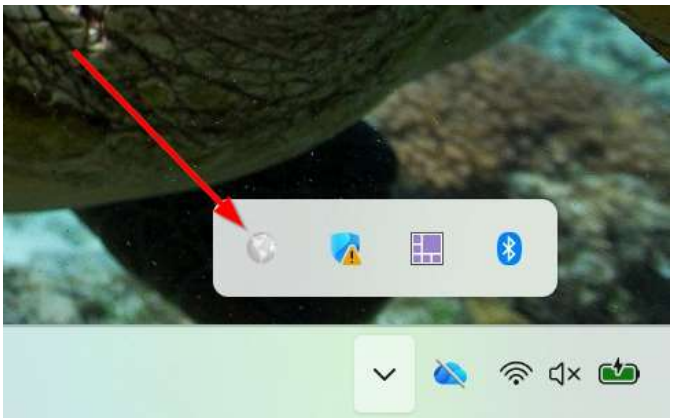
Und die entsprechende Installationsdatei herunterladen:





Danach die heruntergeladene Datei mit administrativen Rechten installieren. Sollte ein Reboot erforderlich sein, wird darauf im Installationsprozess hingewiesen.

Nach der Installation befindet sich im Systray das Symbol des GlobalProtect Agents, jedoch ist die Software noch nicht aktiviert.

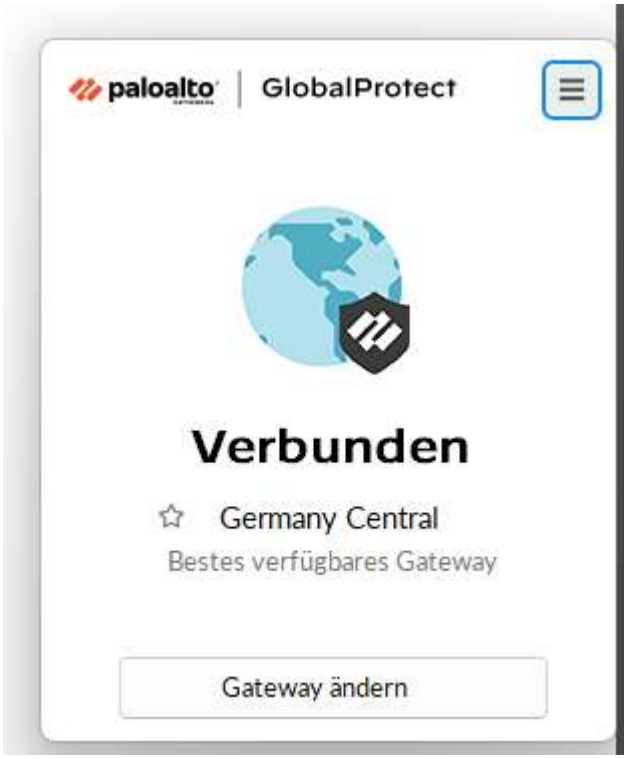


Um sie zu aktivieren und die fischer-spezifischen Einstellungen zu erhalten, bitte einmal auf das Symbol im Systray klicken. Der Agent öffnet sich und dann auf 'Loslegen' klicken.

Im Feld Portal bitte 'fischer.gpcloudservice.com' eingeben und auf ‘Verbinden’ klicken. Es erfolgt eine Authentifizierung im lokalen Default-Browser. Dort bitte wieder mit den fischer Anmeldedaten anmelden (mit MFA).

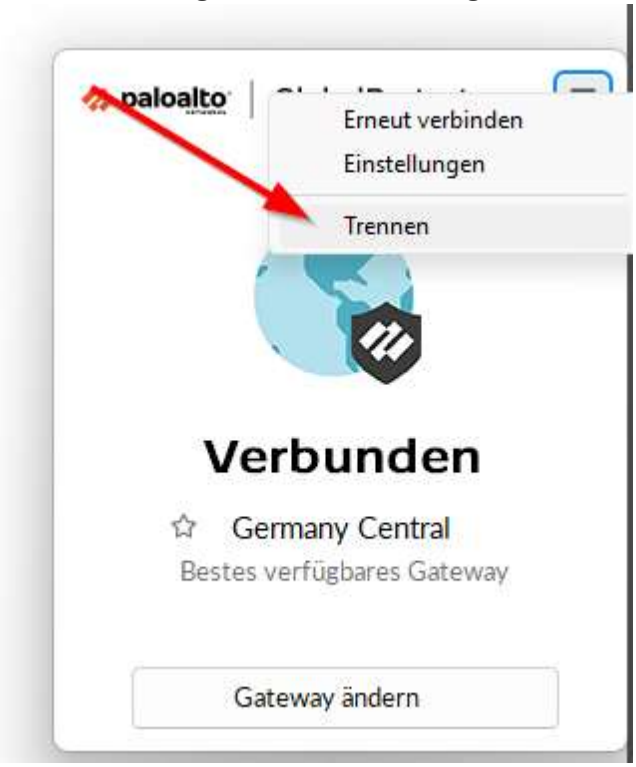
Möglicherweise erhalten Sie eine Auswahl von Computerzertifikaten aus Ihrem lokalen Zertifikatsspeicher. Hier müssen sie dann eines auswählen, bevor es weitergeht. Dieses Zertifikat spielt für die Verbindung selber aber keine Rolle und wird auch nicht ausgewertet oder weitergegeben.

Nach der erfolgreichen Anmeldung verbindet sich der Agent zum nächsten verfügbaren Gateway.



Danach sollten Sie kurz prüfen, ob Sie die notwendigen Ressourcen bei fischer erreichen können.

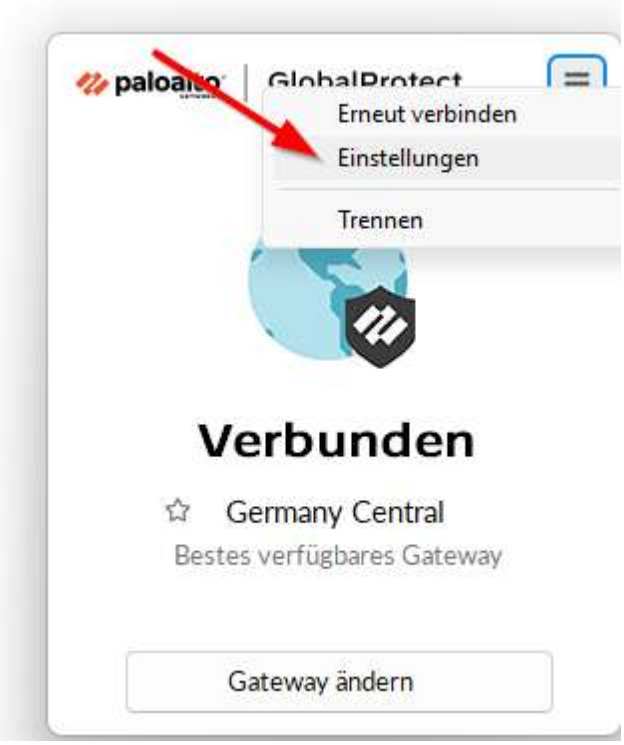
Die Verbindung kann nach der Tätigkeit wieder getrennt werden:

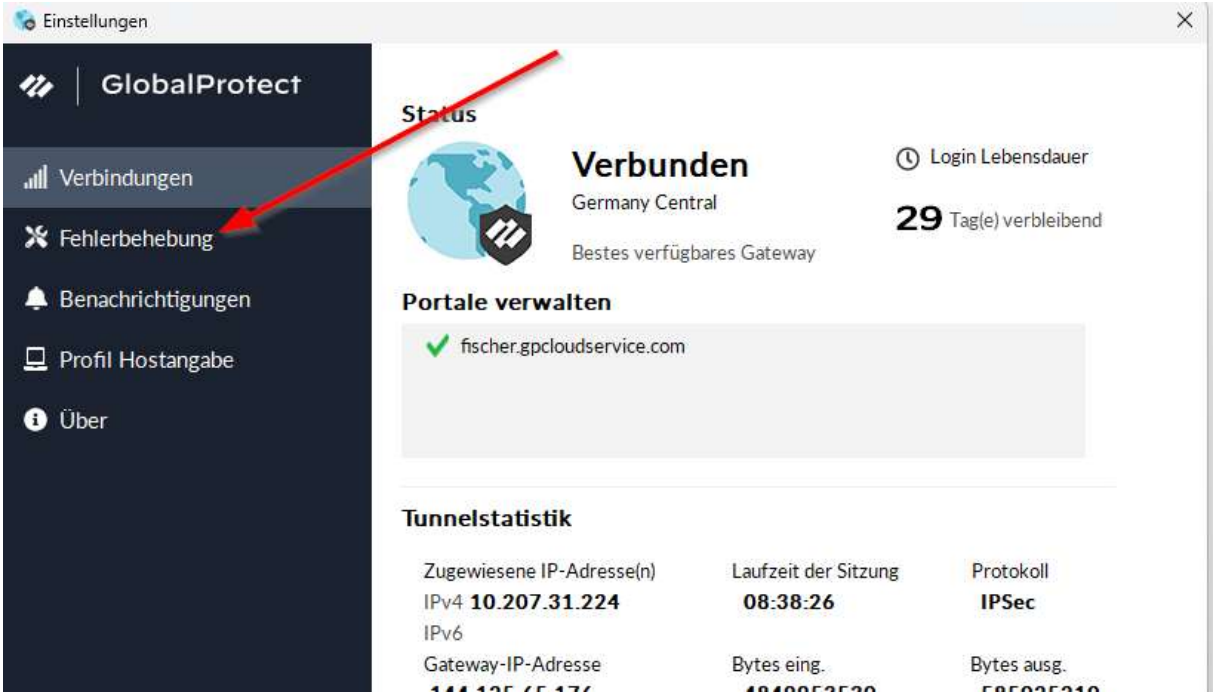


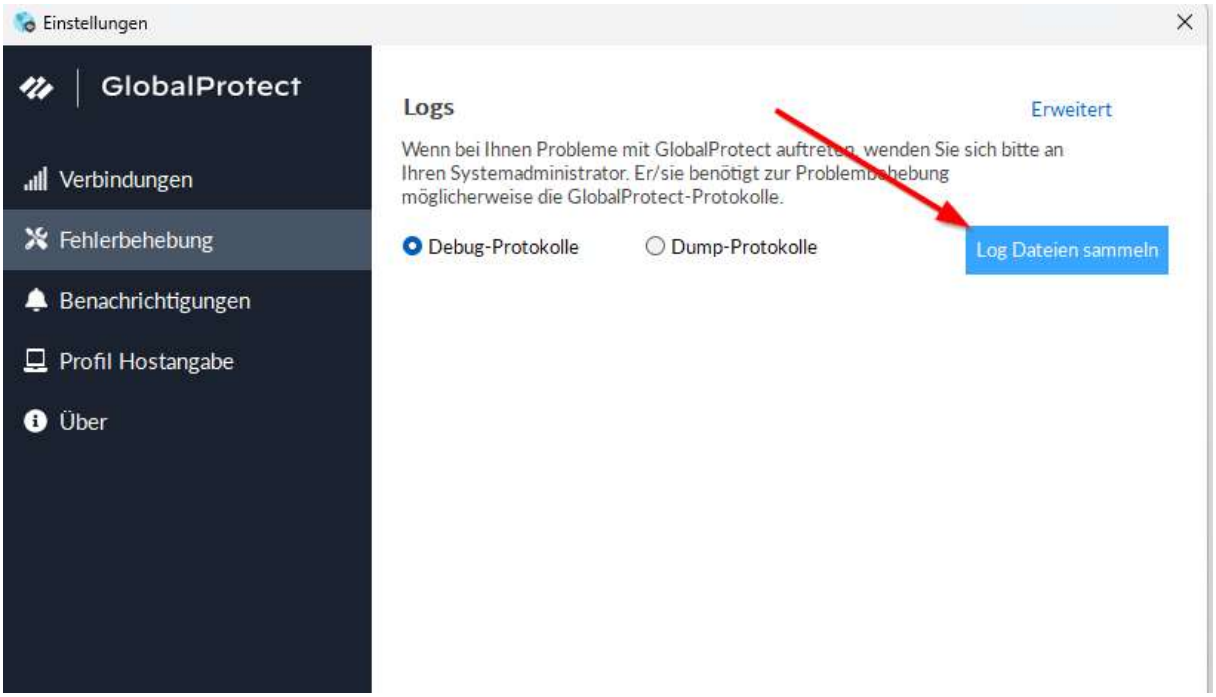
Alle bisherigen Eingaben bleiben in Ihrem lokalen Benutzerprofil gespeichert, sodass bei erneuter Verbindung nur gelegentlich die MFA eine Re-Authentifizierung verlangen wird.

Hinweis: bei Wechsel des lokalen Benutzerprofils muss die Aktivierung erneut durchgeführt werden.

Sollte es zu einem Supportfall kommen, könnten Sie nach Logfiles gefragt werden. Diese Logfiles können wie folgt erzeugt werden:

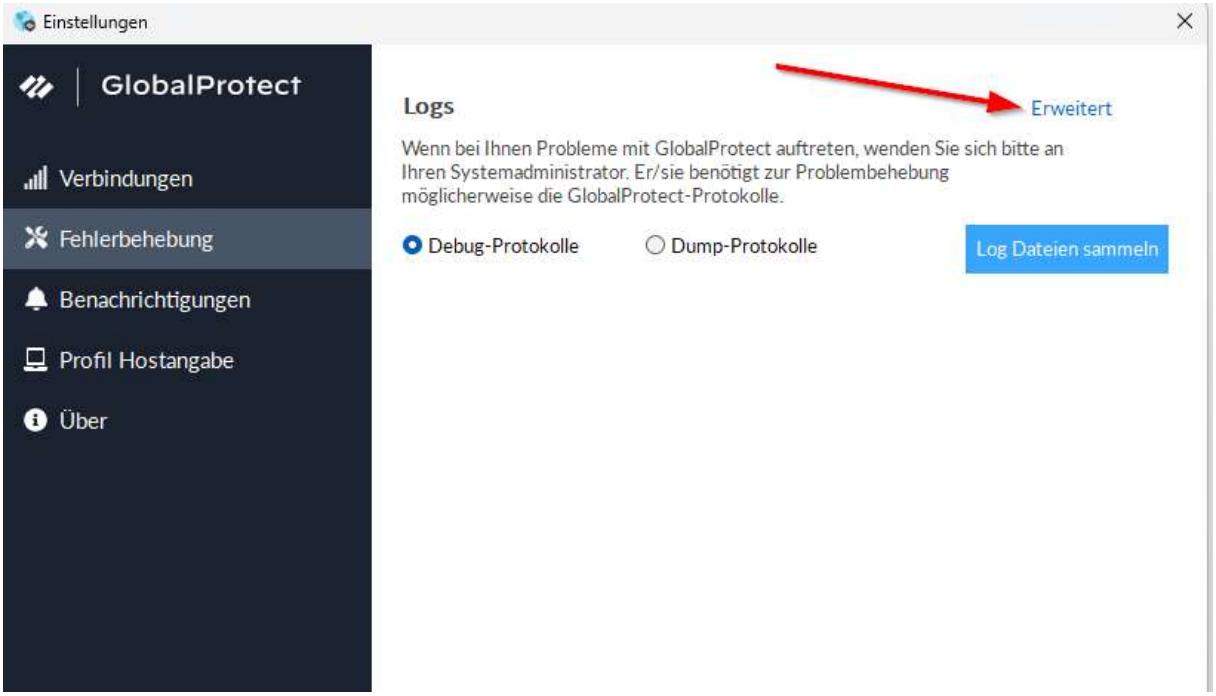


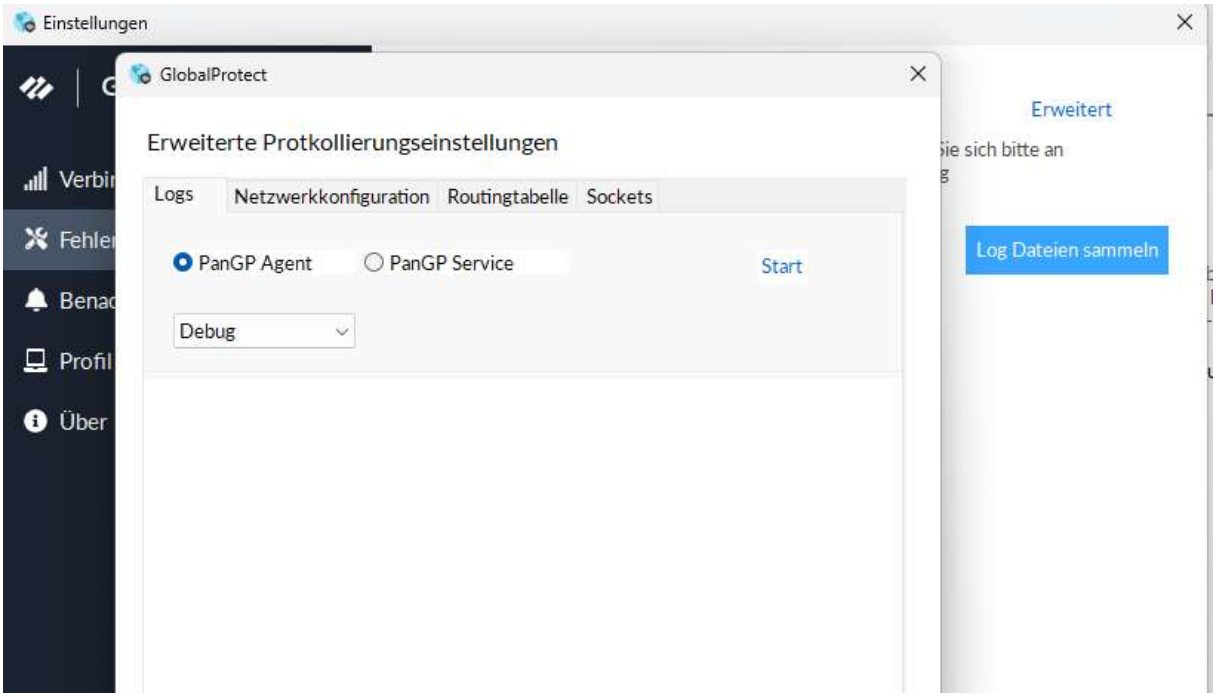




Sie werden dann nach einem Ordner gefragt, in dem die Logfiles als ZIP-Datei abgelegt werden. Bitte stellen Sie uns diese ZIP-Datei auf Anfrage zur Verfügung.

In sehr seltenen Fällen müssen wir den PaloAlto Support mit einschalten. Hier werden häufig erweiterte Logfiles angefragt. Diese können erzeugt werden, indem die erweiterte Ansicht gewählt wird:





Dann bitte weiter verfahren wie vom Support angefragt, da hier kein ZIP generiert wird.