Installation von FortiClient VPN unter Windows

Inhaltsverzeichnis

- Installation
- Einrichtung einer VPN-Verbindung

Ähnliche Artikel

- Installation von OpenFortiVPN unter Linux
- How to install OpenFortiVPN on Linux
- Installation von FortiClient VPN unter Windows
- How to install the FortiClient VPN on Android
- How to install the FortiClient VPN on iOS
- How to install the FortiClient VPN on MacOS
- How to install the FortiClient VPN on Windows
- Installation von Forticlient VPN unter MacOS
- Installation von FortiClient VPN für Android
- Installation von FortiClient VPN für iOS

Installation

Die Installation des Clients verläuft Windows-typisch: Download der Datei Forti-Client und Ausführung mit Administrator-Rechten. Es öffnet sich ein *Set up-Assistent*, der zur Akzeptanz der Lizenzvereinbarung auffordert und anschließend seine Arbeit macht. Der Setup-Prozess legt auf dem Desktop eine Verlinkung auf das Client-Programm an:

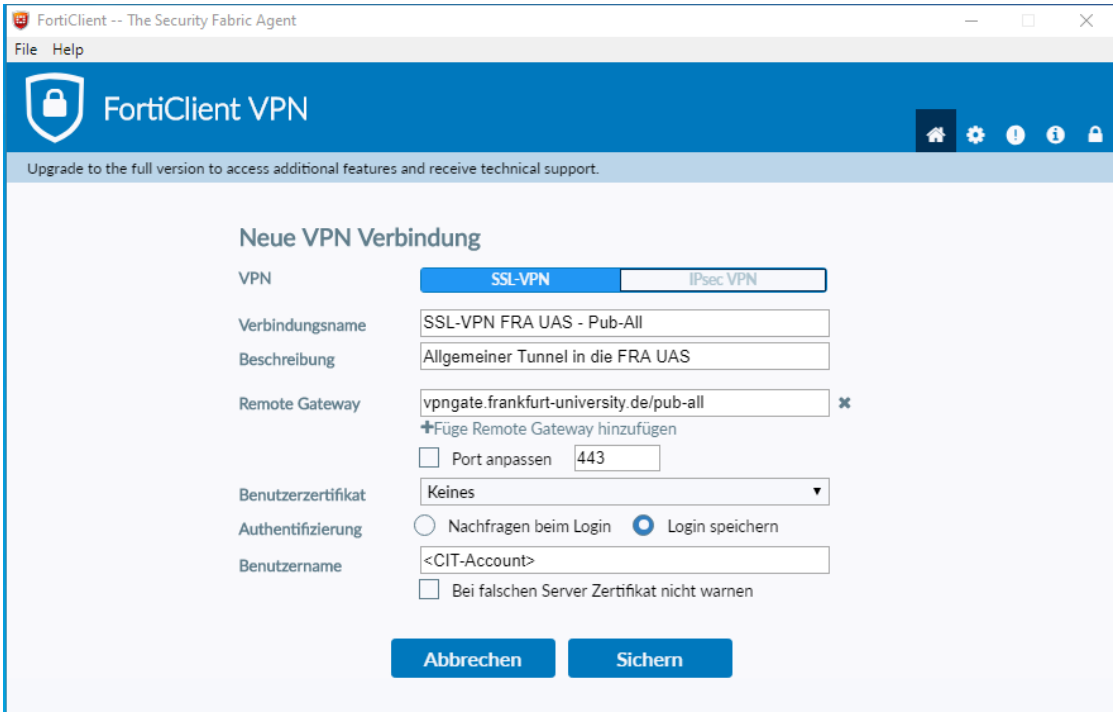


Einrichtung einer VPN-Verbindung

Die Nutzung des Clients bedarf keiner erweiterten Rechte, kann also von Standardbenutzern ausgeführt werden. Nach dem Start wird zunächst eine Bestätigung abgefragt, dass man sich im klaren darüber ist, dass Fortinet für den kostenlosen Client keinerlei Support übernimmt - nun ja, dafür haben wir ja unser Support-Team 😃. Danach kann's dann ans Einrichten der VPN-Verbindung gehen:



Der Client kann sowohl SSL- wie IPsec-VPN-Verbindungen herstellen, daher darauf achten, dass hier der Bereich SSL-VPN ausgewählt ist. Die Felder sollten für den Standard-Tunnel in etwa so ausgefüllt werden:



- Verbindungsname: frei wählbare Kennzeichnung der Verbindung
- Beschreibung: ebenfalls frei wähl- bzw. verzichtbar
- Remote Gateway:
    - Zieladresse (für alle zentralen SSL-VPNs der FRA UAS gleich): vpngate.frankfurt-university.de und

    - Bereich (REALM): (unterscheidet sich bei anderen Tunneln): /pub-all
- Port: 443 (wie vorgegeben)
- Benutzerzertifikat: keines (wie vorgegeben)
- Authentifizierung: durch Nutzer frei wählbar
- Benutzername: Login des CIT-Accounts
    - die Option *Bei falschen Server Zertifikat nicht warnen* ist nicht erforderlich (VPN-Zugang verfügt über öffentliches Zertifikat) und sollte nicht aktivert werden!

Konfiguration sichern, dann öffnet sich der Login-Screen:



