

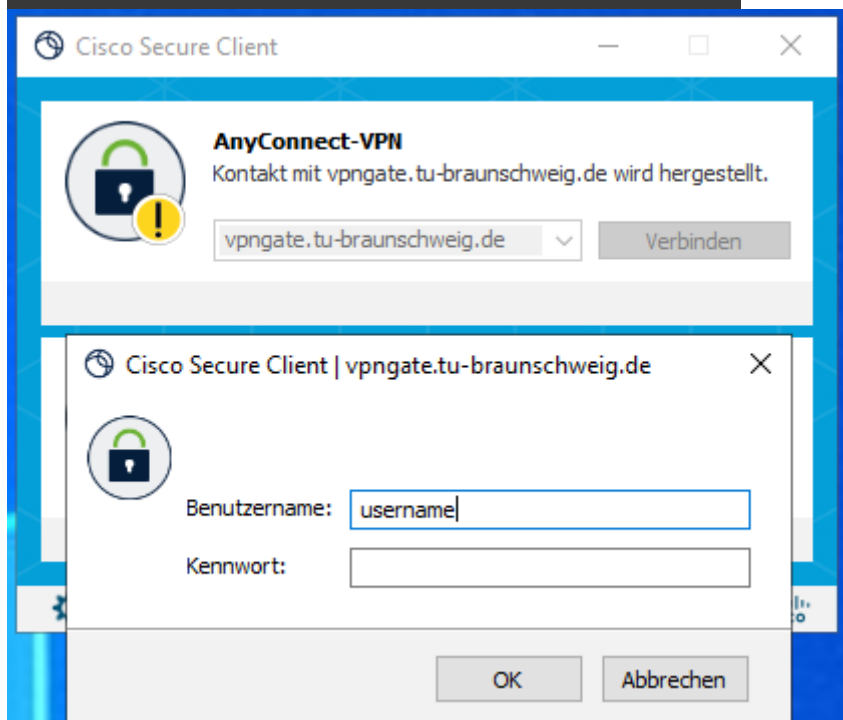
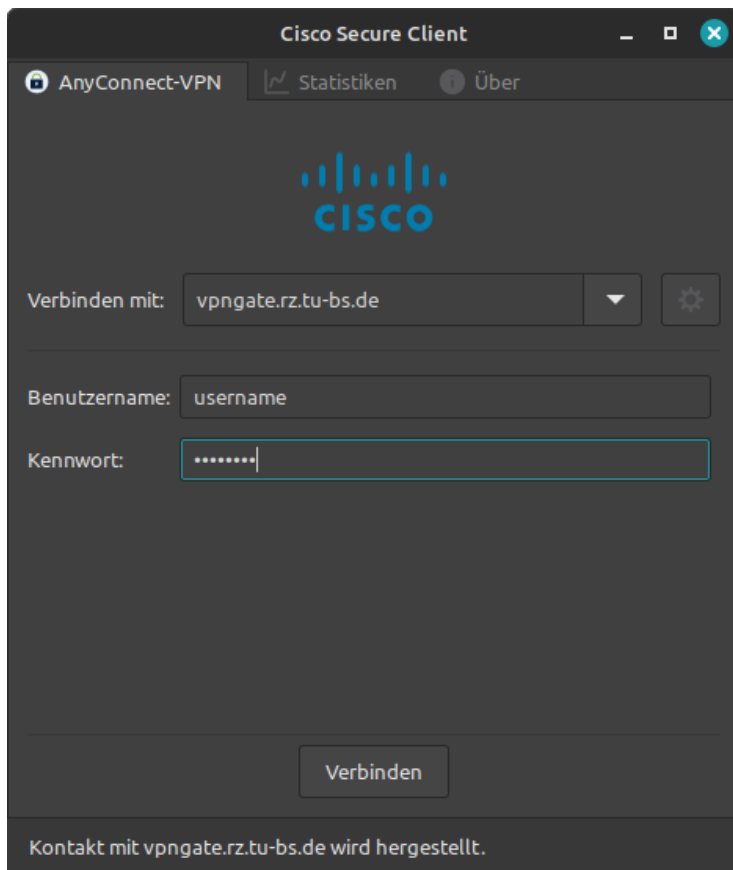
Cisco Secure Client nutzen

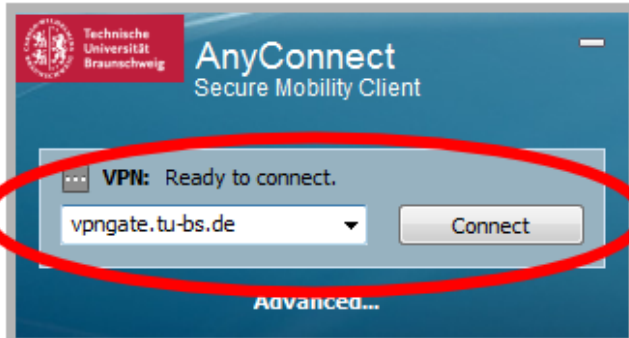
Beschreibt, wie der Cisco Secure Client erstmals eingerichtet wird und welche Optionen es bei der Profilauswahl gibt.

- [VPN-Client "Cisco Secure Client" erstmals starten](#)
- [VPN an anderen Einrichtungen nutzen](#)
- [Grundsätzliche Fehlerbehebung](#)

VPN-Client "Cisco Secure Client" erstmals starten

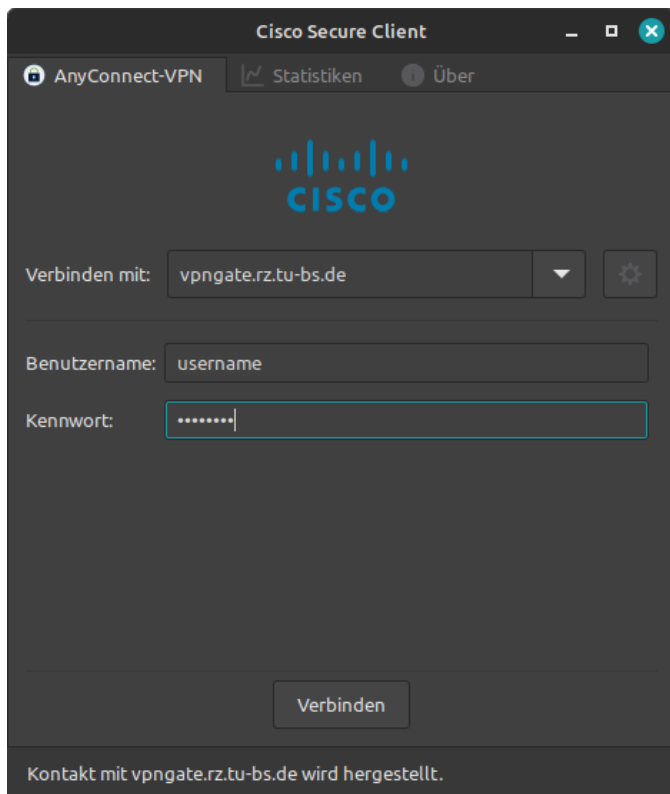
Die Verwendung des Clients ist unabhängig davon, auf welchem Betriebssystem er installiert ist. Für die Verwendung ist ebenso unerheblich, wie der Client genau aussieht, was unter Mac OS X, Windows und Linux jeweils leicht unterschiedlich ist. Die Versionen für Smartphones unterscheiden sich naturgemäß stärker von den Desktop-Versionen, weswegen Sie hier bitte der Beschreibung im vorhergehenden [Abschnitt](#) folgen. In dieser Anleitung werden wir nicht jeden Schritt mit einem Screenshot aller Versionen belegen, sondern uns an unterschiedlichen Beispielen orientieren. Hier zunächst ein kurzer Überblick über das unterschiedliche Aussehen der Clients unter den verschiedenen Betriebssystemen:



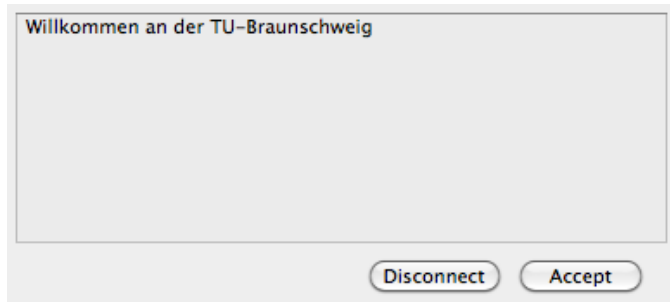


(Screenshot einer älteren Version des Clients, funktional aber gleich)

Wenn Sie den Client das erste Mal starten, müssen Sie im Feld "Connect (to)" den Hostnamen des VPN-Servers *vpngate.tu-bs.de* (oder *vpngate.tu-braunschweig.de* oder *vpngate.rz.tu-bs.de*) eingeben.



Geben Sie dann im Feld Benutzername Ihre TUBS-ID und das dazugehörige Kennwort ein.



Nach Eingabe Ihrer Benutzerdaten und Auswahl des Profils gehen sie auf [**OK**]. Dann wird der Tunnel aufgebaut. Als nächstes sehen Sie eine Willkommensnachricht, die Sie noch mit [**Accept/Akzeptieren**] bestätigen müssen.



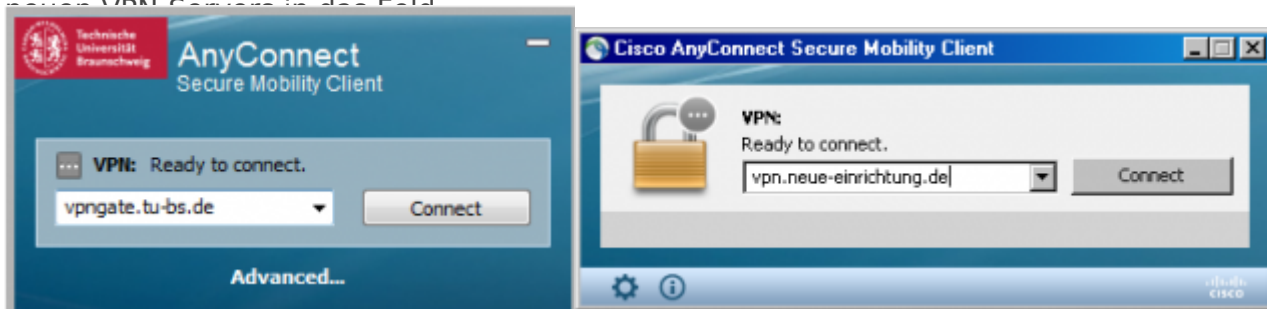
In der Regel verschwindet nun das AnyConnect-Fenster. Sie finden stattdessen ein Icon in der Task-/Programmleiste Ihres Desktops. Wenn Sie dieses Icon anklicken, öffnet sich das Fenster erneut.



Das Icon wird mit einem Schloss angezeigt, solange eine VPN-Verbindung besteht. Sobald Sie das Fenster öffnen und [**Disconnect**] drücken, verändert sich das Icon. Das Schloss ist nun nicht mehr zu sehen.

VPN an anderen Einrichtungen nutzen

Wenn Sie an mehr als einer Einrichtung den AnyConnect VPN-Client benutzen müssen oder sollen, dann können Sie dies ohne erneute Installation des Programms tun. Starten Sie den Client. Klicken Sie in das Feld „Connect to:“ bzw. „VPN: Ready to connect:“ hinein und Tippen Sie den Namen des neuen VPN Servers in das Feld.



Die vorstehenden Abbildungen von verschiedenen Betriebssystemen sollen eines verdeutlichen: Statt der vorkonfigurierten Werte lässt sich in das Feld jederzeit der Name eines anderen VPN-Servers eintragen zu dem man Verbindung aufbauen möchte und der Verbindungen über den AnyConnect Client zulässt.

Grundsätzliche Fehlerbehebung

Sollten bei der Installation, dem manuellen Update oder dem automatischen Update Probleme während der Installationsroutine oder dem Verbindungsaufbau bestehen, sollte als Erstes der installierte Virens Scanner und die installierte Firewall (zusätzlich zu der Windows internen Firewall) überprüft werden. Grundsätzlich ist es ratsam die Firewall erst **nach** der Installation des VPN-Clients zu installieren, falls eine zusätzliche Firewall gewünscht wird. Sollten weiterhin Probleme auftreten, bitte eine komplette Deinstallation des VPN Clients (inklusive aller ggf. vorhandenen älteren Versionen) vornehmen. Hierzu bitte nach der Deinstallation folgende Ordner manuell löschen falls sie noch vorhanden sind (Windows).

- C:\ProgramData\Cisco\Cisco Secure Connect VPN Client\
- C:\Users\„IhrBenutzername“\AppData\Local\Cisco\

Anschließend sollten Sie einen Neustart durchführen und danach den aktuellen AnyConnect Client herunterladen und manuell installieren:

<https://www.tu-braunschweig.de/it/downloads/software>

Erfolgreich getestet wurde der aktuelle VPN Client unter den Betriebssystemen Windows 8.1, Windows 10, Windows 11, Linux und Mac OS X (Intel). Sowohl ohne als auch mit dem von der TU Braunschweig angebotenen Virens Scanner. Der Einsatz anderer Virens Scanner oder Firewalls können zu einem erheblichen Mehraufwand bei der Installation führen und werden offiziell nicht unterstützt. Sollten Fehler auftreten, halten Sie bitte die Versionsinformationen zu der genutzten Java Version, dem Betriebssystem und dem genutzten VPN Client bereit und geben Sie diese bei einer Störungsmeldung mit an.

OpenSuse

Unter OpenSuse 15.1 Leap kommt es aktuell zum Fehler **„install: cannot create regular file '/lib/systemd/system/vpnagentd.service': No such file or directory“** . Dazu bitte dem [Fix auf der Herstellerseite](#) folgen.