

**Virtual Private Networks – Cisco Secure Client / Anyconnect VPN
Microsoft Windows / Linux / macOS**

Inhaltsverzeichnis

1. Einführung
2. Distribution der Cisco Secure Client / Anyconnect VPN Software
3. Windows 10 / Windows 11
4. Linux (Ubuntu 20.04 LTS)
5. macOS
6. FAQ

1. Einführung

Der Cisco Secure Client / Anyconnect VPN (kurz: Anyconnect) ist das favorisierte VPN Zugangsangebot des JSC. Dieser VPN Client kann als Nachfolger der bisherigen IKEv1/IPSEC-basierten VPN Varianten bei Bedarf eingesetzt werden.

Insbesondere können bewährte Mechanismen wie beispielsweise die unterschiedlichen Tunnel-Policies *fzj* oder *fzj-nosplit* (siehe FAQ Frage 8) unmittelbar benutzergesteuert ausgewählt werden. Zudem kann bei Bedarf der Anyconnect VPN Client parallel zu L2TP/IPSEC (TKI-0387) installiert werden. Die Kompatibilität mit den Virenscannern ‚TREND Micro Apex One‘ und ‚Microsoft Windows Defender‘ ist gegeben.

Die Anyconnect-Software und die entsprechenden VPN-Gateway-Konfigurationen werden in vielen wissenschaftlichen Einrichtungen angeboten. Wechselseitig ist damit eine entsprechende Interoperabilität und Konnektivität zwischen den Forschungseinrichtungen gewährleistet.

Technik – Hintergrund: Die Absicherung der Datenübertragung erfolgt mit TLS (TCP Port 443) oder DTLS (UDP Port 443). Die DTLS basierte Übertragung wird dabei bevorzugt.

Voraussetzung zur Nutzung dieser Software ist ein gültiges Benutzerzertifikat. Hinweis: Aufgrund von geänderten Anforderungen an Benutzerzertifikate hat der DFN diesen Dienst zum 29.08.2023 eingestellt. Der neue Dienstleister Sectigo (GEANT TCS) übernimmt ab dann die Ausstellung der Benutzer-Zertifikate.

Zertifikatswünsche (GEANT TCS) müssen per formloser E-Mail an user-services.jsc@fz-juelich geschickt werden. Nach einer eventuellen Ausweiskontrolle erhalten Sie eine E-Mail Einladung mit einem Link (Antragsformular).

Zulassungen/Accounts (Mitarbeiter) zur VPN-Benutzung können für Mitarbeiter beim "Office for User Services (user-services.jsc@fz-juelich.de)" beantragt werden

https://intranet.fz-juelich.de/de/organisation/it-portal/software_services/infrastruktur/vpn

Sollten Zugänge für Kooperationspartner erforderlich sein, ist eine individuelle Konfiguration nötig. Für Beratung und Fragen dazu stehen die Ansprechpartner im JSC zur Verfügung (EMAIL: vpn@fz-juelich.de).

2. Distribution der Cisco Secure Client / Anyconnect VPN Software

Die Installation (Administrator-Rechte nötig) sollte *OFFLINE* erfolgen. Dazu können die sogenannten *PreDeploy Images* verwendet werden. Diese werden auf dem System pcsrv

<\\pcsrv.zam.kfa-juelich.de\Public\VPN-Software\Cisco-Anyconnect>

zum Download im Intranet angeboten. Bitte halten Sie kurzzeitig für die Installation den Virenschanner an.

Sollte die Cisco Secure Client / Anyconnect VPN Software (kurz: Anyconnect) auf einem System nicht lauffähig oder installierbar sein, steht mit der Open Source Lösung OpenConnect eine kompatible Alternative zur Verfügung. Insbesondere Ubuntu Anwender können die mit der Distribution bereitgestellten Pakete installieren und nutzen.

3. Windows 10 / Windows 11

Voraussetzung für den erfolgreichen Verbindungsaufbau ist ein gültiges Benutzerzertifikat (DFN oder Sectigo GÉANT TCS) im Windows-Zertifikatspeicher (Zertifikate – Aktueller Benutzer). Die Installation der VPN-Software erfordert Administratorrechte.

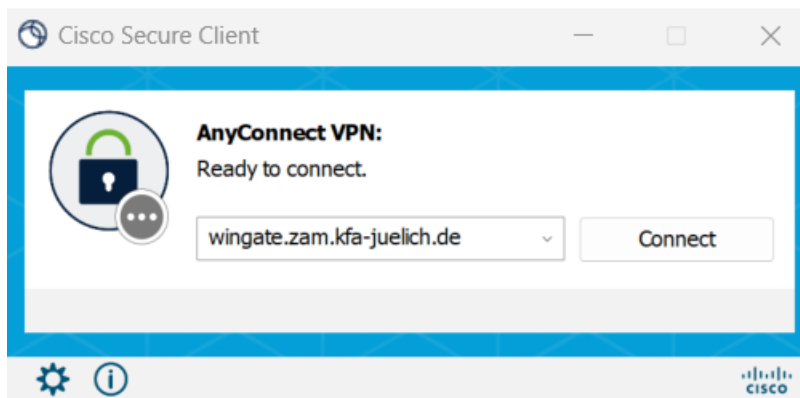
Die Installation kann mit dem bereitgestellten Pre-Deployment-Image (oder neuer)

cisco-secure-client-win-5.0.03072-core-vpn-predeploy-k9.msi

erfolgen. Benutzung:

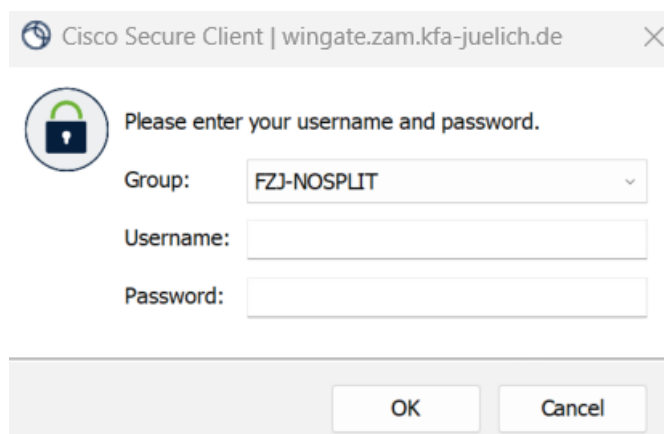
- Sie können ab sofort mit dem installierten Programm die Verbindung herstellen.
- Sie finden das Programm unter Start - Alle Apps - Cisco Secure Client

VPN-Gateways: **wingate.zam.kfa-juelich.de**



... oder ‚Backup-Zugang‘

wingateb.zam.kfa-juelich.de

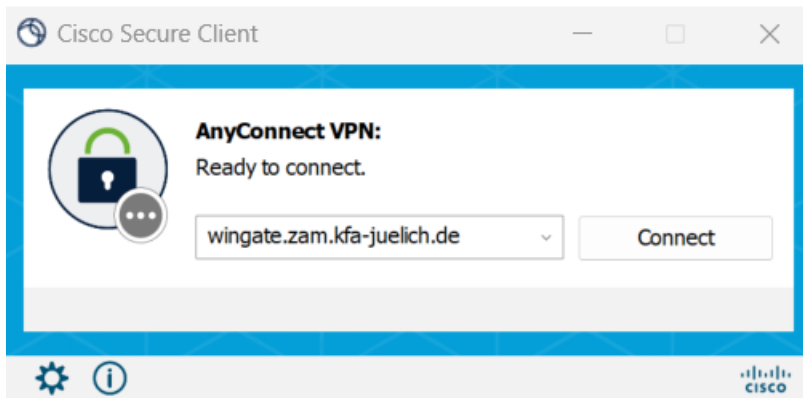


Mögliche Group-Policy auswählen.
(siehe FAQ Frage 8)

VPN-Benutzerkennung!



Verbindungs-ICON in der Task-Leiste:



Detailinformation (hier nach dem ‚CONNECT‘) anzeigen durch ‚Click‘ auf das Symbol.



Mittlerweile haben zahlreiche Anwender im HomeOffice eine über DS-Lite realisierte Internet Anbindung; in diesem Fall ist das Protokoll IPv6 beim Verbindungsaufbau zu favorisieren (die suboptimale Kombination aus Carrier-Grade-NAT und UDP beim Internet Provider wird dabei vermieden).

Soll der Transport über IPv6 erfolgen, können die VPN-Gateways über die vollqualifizierten Namen (FQDNs)

wingate6.zam.kfa-juelich.de
wingateb6.zam.kfa-juelich.de

erreicht werden. Im VPN-Tunnel werden sowohl IPv4 als IPv6 Nutzerdaten übertragen. Beispiel und Kontrolle: IPv6 VPN-Tunnel und wingate6b.zam.kfa-juelich.de

The screenshot shows the Cisco Secure Client interface for a Virtual Private Network (VPN) connection. The window title is "Cisco Secure Client". The main heading is "Secure Client". Below this, the "Virtual Private Network (VPN)" section is active, with tabs for "Preferences", "Statistics", "Route Details", "Firewall", and "Message History". The "Statistics" tab is selected, showing connection information and address information.

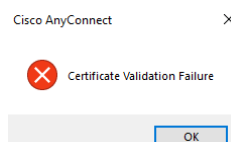
Connection Information	
State:	Connected
Tunnel Mode (IPv4):	Split Exclude
Tunnel Mode (IPv6):	Split Exclude
Dynamic Tunnel Exclusion:	None
Dynamic Tunnel Inclusion:	None
Duration:	00:00:41
Session Disconnect:	None
Management Connection State:	Disconnected (user tunnel active)

Address Information	
Client (IPv4):	134.94.57.191
Client (IPv6):	2001:638:404:3800:0:0:3800:ACC3
Server:	2001:638:404:6FB8:0:0:6FB8:1 ← wingate6.zam.kfa-juelich.de

At the bottom of the statistics window, there are "Reset" and "Export Stats" buttons.

Fehlerursachen und Meldungen:

(I) das Benutzerzertifikat ist nicht korrekt installiert oder vorhanden



(II) lokale Remote Desktop Session (RDP) oder Internetverbindungsfreigabe (ICS) aktiv



4. Linux (Ubuntu 20.04 LTS)

Voraussetzung für den erfolgreichen Verbindungsaufbau ist ein gültiges Benutzerzertifikat (DFN oder Sectigo GEANT TCS). Die Installation der VPN-Software erfordert ROOT-Rechte.

Aufgrund der besseren Integration in die diversen Linux-Derivate wird der Einsatz der kompatiblen Open-Source Software ‚openconnect‘ empfohlen. Diese Software ist kompatibel zur Cisco Anyconnect Lösung und wird bei allen gängigen Derivaten als installierbares Paket (openconnect) angeboten. Die Steuerung der VPN-Verbindung kann auf Shell-Ebene (ROOT-Rechte) oder bei Bedarf auch durch den Network-Manager in der grafischen Benutzeroberfläche erfolgen:

```
openconnect -k PKCS12 -c {file.pfx} wingate.zam.kfa-juelich.de
```

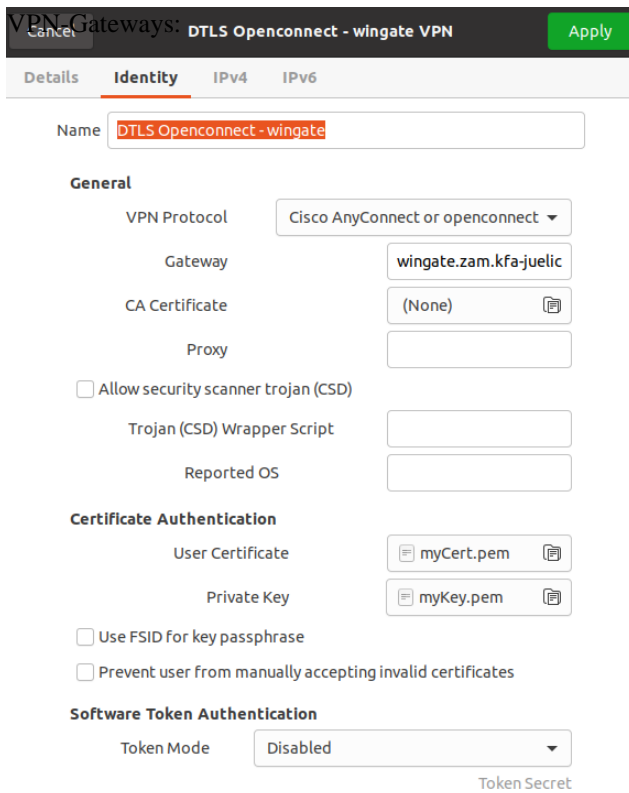
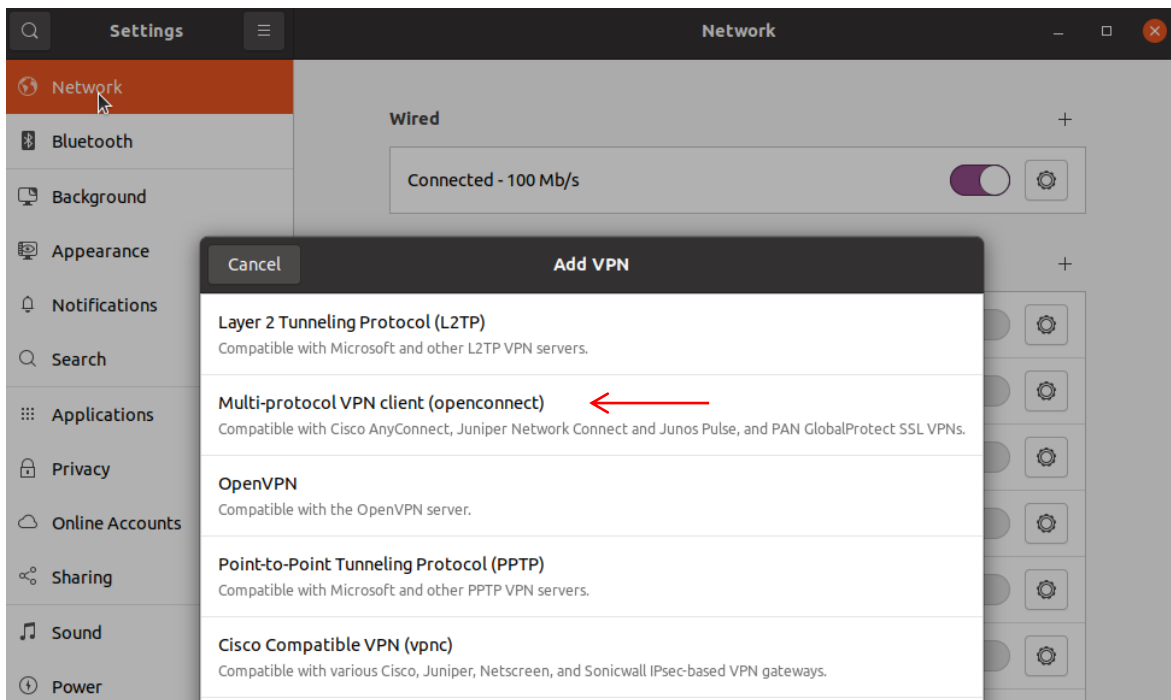
Zur Vorbereitung der Konfiguration im Network-Manager ist gegebenenfalls nach der Software-Installation (bei Ubuntu Gnome Desktop: network-manager-openconnect und network-manager-openconnect-gnome)

```
sudo apt install network-manager-openconnect
sudo apt install network-manager-openconnect-gnome
```

die eigene persönliche PKCS12-Datei (hier im Beispiel: file.pfx genannt - Benutzerzertifikat aus der Global-Zertifizierungshierarchie des DFN-Vereins oder alternativ von GEANT TCS) mit den folgenden Befehlen zu konvertieren; schützen Sie dabei den exportierten privaten Schlüssel mit einer ‚Pass Phrase‘:

```
openssl pkcs12 -in {file.pfx} -clcerts -nokeys -out myCert.pem
openssl pkcs12 -in {file.pfx} -nocerts -out myKey.pem
```

Erstellen der Konfiguration:

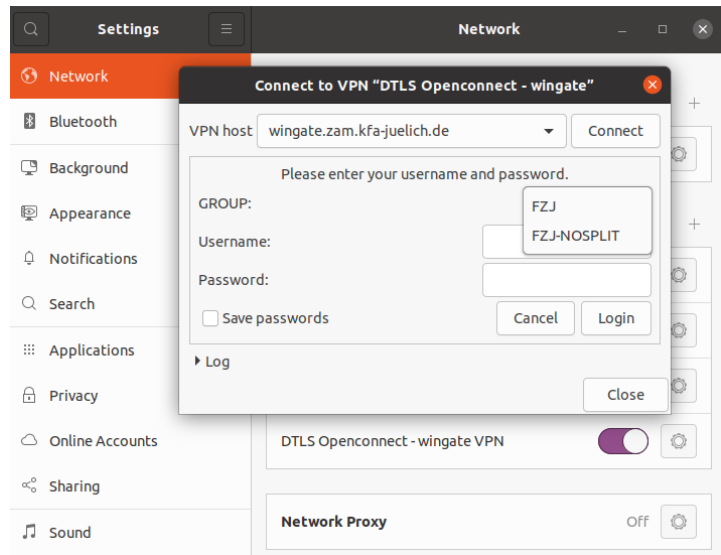
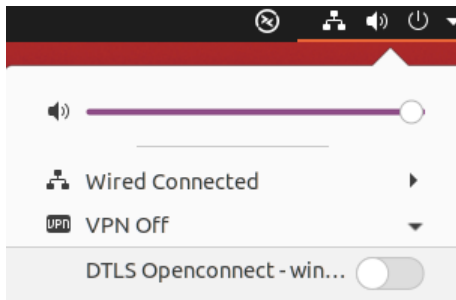


wingate.zam.kfa-juelich.de

oder (Backup-Zugang)

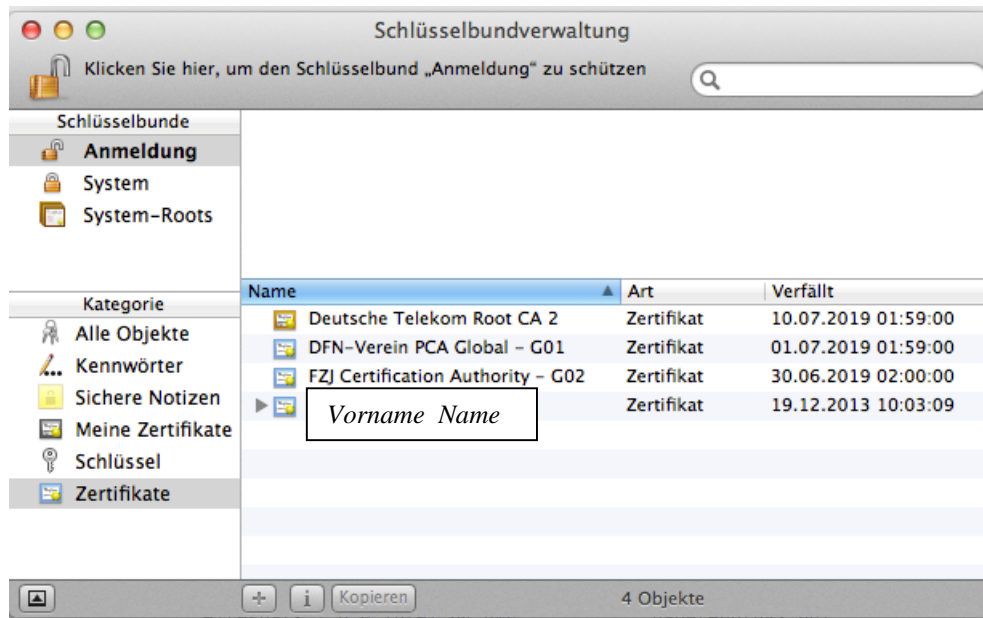
wingateb.zam.kfa-juelich.de

Aufbau der VPN-Verbindung (bzgl. ‚GROUP‘ siehe FAQ Frage 8):



5. macOS

Voraussetzung für die nachfolgenden Schritte ist ein gültiges Benutzerzertifikat aus der Global-Zertifizierungshierarchie des DFN-Vereins oder von GEANT TCS.



Die Installation erfordert Administratorrechte und kann mit dem bereitgestellten Pre-Deployment-Image

cisco-secure-client-macos-5.0.03072-predeploy-k9.dmg

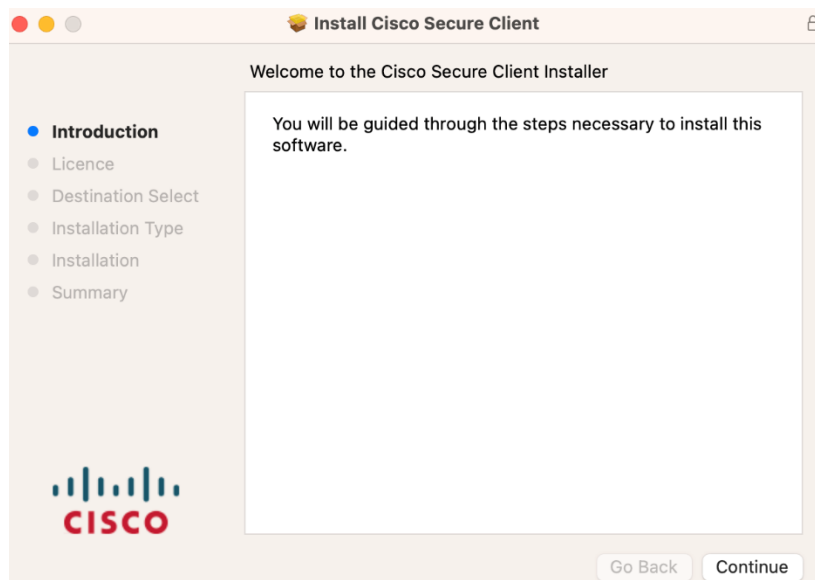
(oder neuer) erfolgen.

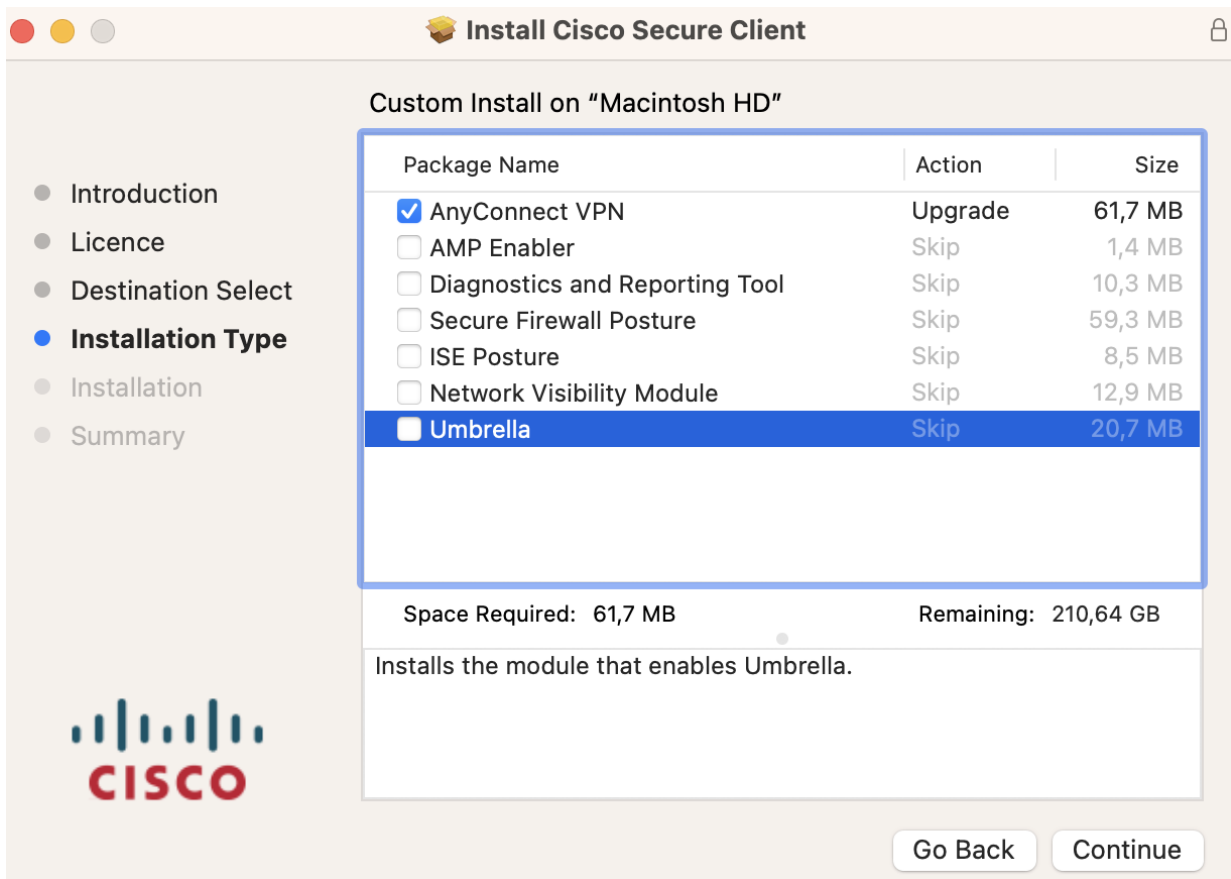
Die nachfolgende Vorgehensweise gilt allgemein für die Versionen 5.x:



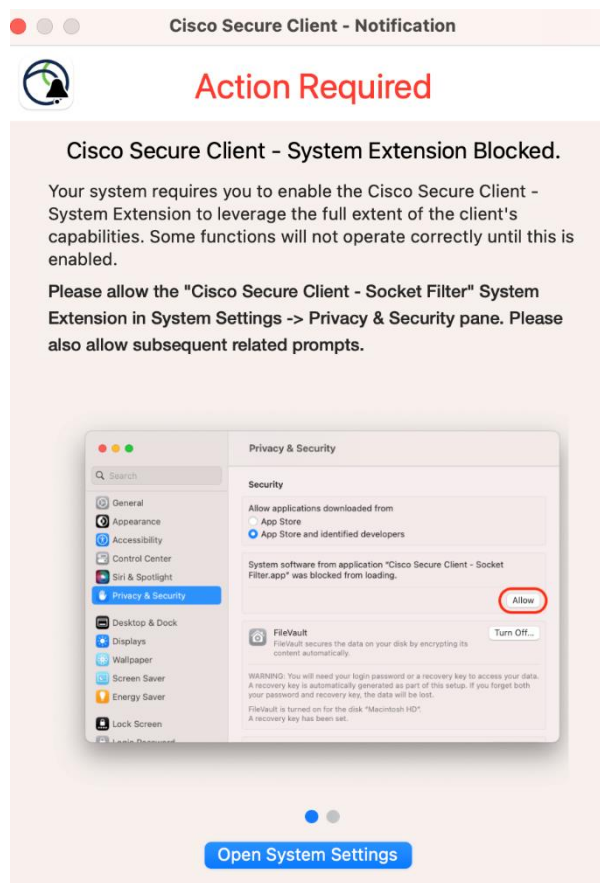
‚Cisco Secure Client.pkg‘ auswählen

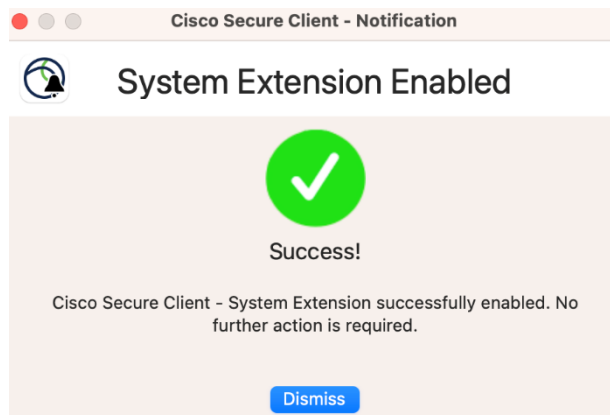
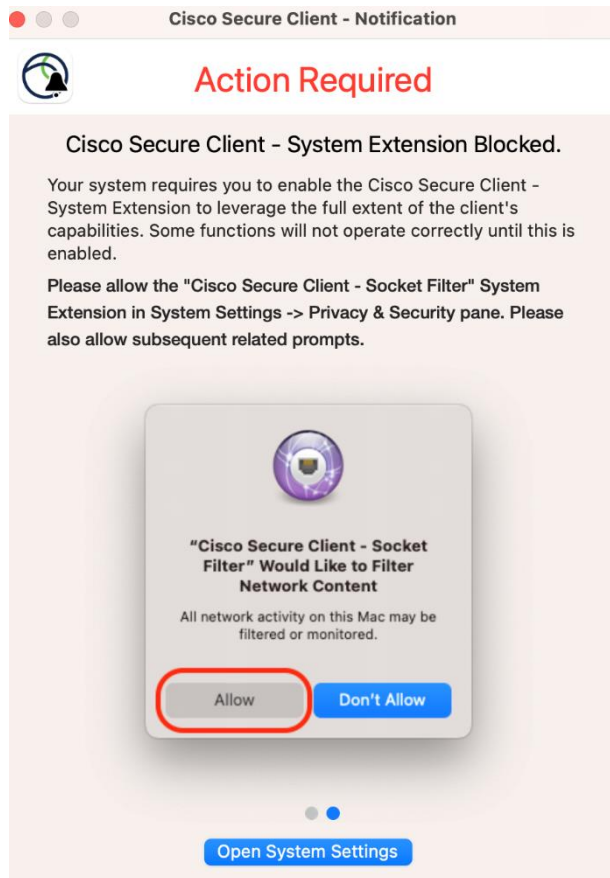
Bestätigen Sie die Lizenzbedingungen. **Installieren Sie bitte nur die VPN-Komponente.**

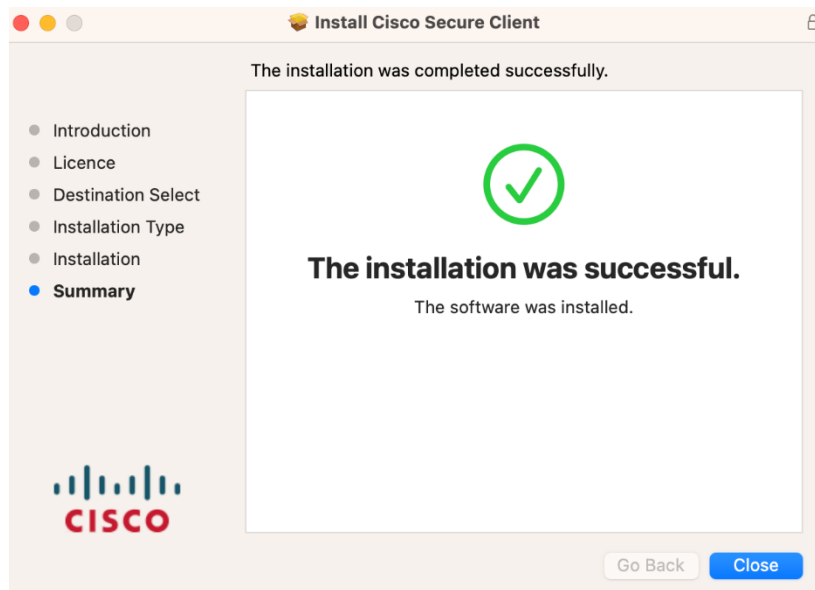




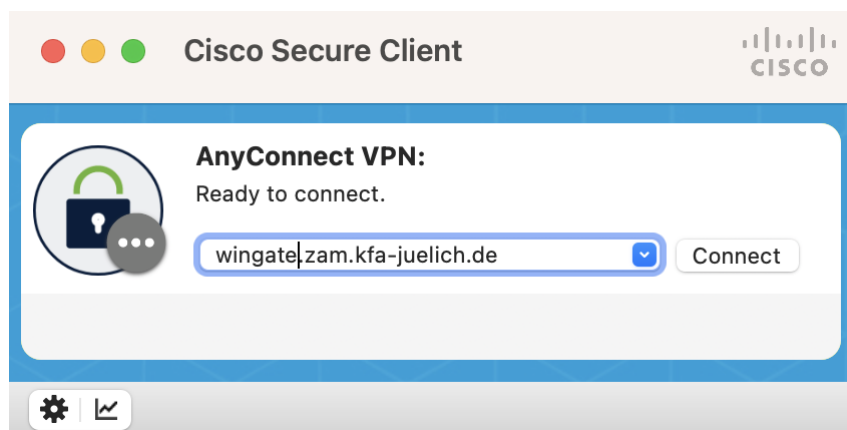
Die Ausnahmeeinstellung für Anyconnect (System Extension) ist vorzunehmen.







Benutzung:



Akzeptieren Sie gegebenenfalls einmalig beim ersten Verbindungsaufbau die Server-Zertifikate **wingate.zam.kfa-juelich.de** bzw. **wingateb.zam.kfa-juelich.de**.

Erlauben Sie beim Verbindungsaufbau den Zugriff auf das eigene Benutzer-Zertifikat im Schlüsselbund. (Falls kein gültiges Zertifikat verfügbar ist, endet der Verbindungsversuch mit der Meldung ‚Certificate Validation Failure‘.)

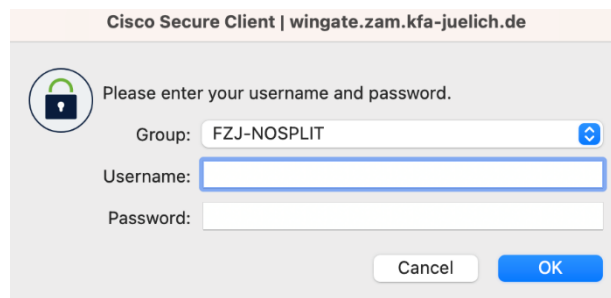
VPN-Gateways:

wingate.zam.kfa-juelich.de

oder (Backup-Zugang)

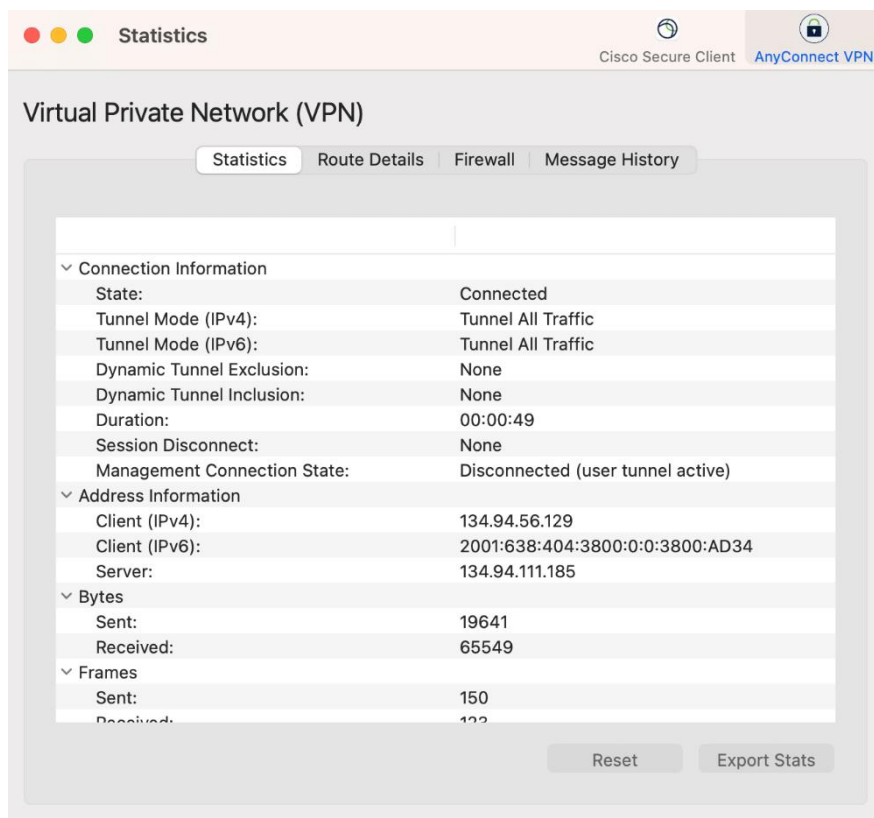
wingateb.zam.kfa-juelich.de

Mögliche Group-Policy im Feld ‚Group‘ auswählen (siehe FAQ Frage 8).



Die VPN-Benutzerkennung ist einzugeben.

Beispiel einer aktiven VPN-Verbindung → öffnen Verbindungs ICON:



Virtual Private Network (VPN)	
Statistics Route Details Firewall Message History	
▼ Connection Information	
State:	Connected
Tunnel Mode (IPv4):	Tunnel All Traffic
Tunnel Mode (IPv6):	Tunnel All Traffic
Dynamic Tunnel Exclusion:	None
Dynamic Tunnel Inclusion:	None
Duration:	00:00:49
Session Disconnect:	None
Management Connection State:	Disconnected (user tunnel active)
▼ Address Information	
Client (IPv4):	134.94.56.129
Client (IPv6):	2001:638:404:3800:0:0:3800:AD34
Server:	134.94.111.185
▼ Bytes	
Sent:	19641
Received:	65549
▼ Frames	
Sent:	150
Received:	122

Das ‚Message History‘ zeigt den zeitlichen Verlauf des Verbindungsaufbaus. Die Datei /var/log/system.log (Zugriff: Administratorrechte) enthält darüber hinaus Meldungen zur Diagnose von Verbindungsproblemen:

```
grep acvagent /var/log/system.log
```

Alternativ kann im Problemfall das ‚Diagnostic and Reporting Tool‘ nachinstalliert werden.

6. FAQ

1. Wer sind die richtigen Ansprechpartner bei weiteren Fragen?

Bei Fragen zum VPN-Antrag und Password-Reset:

Ansprechpartner: JSC "Office for User Services"

Telefon: 02461 61- 5642

E-Mail: user-services.jsc@fz-juelich.de

Halten Sie bitte die folgenden Informationen bereit oder teilen Sie diese mit:

Name und Organisationseinheit

VPN-Benutzername (z.B.m.mustermann)

Datum und Uhrzeit der Antragsstellung bzw. des Passwort-Resets

Bei Verbindungsproblemen und techn. Problemen:

Ansprechpartner: Abteilungskommunikationssysteme im JSC

Telefon: 02461 61 – 6440

E-Mail: vpn@fz-juelich.de

Halten Sie bitte die folgenden Informationen bereit oder teilen Sie diese mit:

Name und Organisationseinheit

VPN-Benutzername

Betriebssystem (Software: Cisco Anyconnect oder Openconnect)

Ihr Internet Provider zu Hause (Telekom, Vodafone, etc.)

IP-Adressen, die vom Provider zugewiesen wurden

Datum und Uhrzeit, wann Ihr Problem auftrat

2. Kann beim Import (Windows) eines Zertifikates die Funktion „Hohe Sicherheit für den privaten Schlüssel“ aktiviert werden?

Ja – dieses Sicherheitsfeature wird unterstützt.

3. Kann Start-Before-Logon (SBL) unterstützt werden?

Nein. Die Client-Authentifizierung mit Zertifikaten und SBL sind nicht kompatibel.

4. Welches Windows Firewall-Profil wird für den VPN-Adapter/Verbindung verwendet?

Nach der Installation ist der Cisco Anyconnect Adapter in allen Firewall-Profilen eingetragen (Name: LAN-Verbindung *n*, der Befehl `ipconfig /all` zeigt die Zuordnung der Indexnummer *n* zum aktiven Anyconnect Adapter). Dadurch gilt das „Öffentliche Profil“. In der „Windows Firewall mit erweiterter Sicherheit“ kann diese Auswahl im Menu „Geschützte Netzverbindungen“ explizit angepasst werden, um beispielsweise das „Private Profil“ für die VPN-Verbindung zu aktivieren.

5. Kann gleichzeitig die Windows Funktion ‚Internet Connection Sharing‘ genutzt werden?

Nein. Diese Komponente ist nicht kompatibel mit Anyconnect.

6. Welche VPN-Pool-Adressen müssen Systeme im JuNet bei der Firewall-Konfiguration beachten?

Bei der VPN-Einwahl (Verbindungsaufbau) werden IP-Adressen aus vordefinierten Bereichen vergeben. Die Bereiche sind

134.94.79.0/24
134.94.112.0/24
134.94.48.0/20
2001:638:404:3000::/52
2001:638:404:4f00::/64
2001:638:404:7000::/64

Je nach Sicherheitsanforderungen kann ein System im JuNet die Kommunikation durch entsprechende Einträge im Firewall Regelwerk blockieren oder erlauben. (Linux: TKI-0402 Linux Personal Firewall). Eine aktuelle Gesamtliste für alle VPN-Varianten (inkl. L2TPoverIPSEC) finden Sie unter

https://junet-portal.fz-juelich.de/cgi-bin/public/junet_server.cgi

7. Kann auf Freigaben (NetBIOS-Shares) im JuNet zugegriffen werden?

Ja. Die NetBIOS-Ports sind freigeschaltet! Beispiele zum Testen (Windows Client):

```
net time \\zelcds.zel.kfa-juelich.de
```

```
net view \\zelcds.zel.kfa-juelich.de
```

8. Der Zugriff auf elektronische Zeitschriften der ZB funktioniert nicht / ist nicht erlaubt.

Wegen der Split-Tunnel-Einstellung in der Tunnel-Policy *fzj* wird nur der IP-Traffic zu Rechnern im JuNet (134.94.0.0/16 bzw. 2002:638:404::/48) in den VPN-Tunnel geleitet. Die Kommunikation zum Internet erfolgt direkt über den jeweiligen Service-Provider (z.B. T-Online) mit deren IP-Adressen. Durch Änderung der VPN-Gruppe auf *fzj-nosplit* wird der gesamte IP-Traffic in den VPN-Tunnel geleitet und der Zugriff auf die Zeitschriften erfolgt mit einer gültigen JuNet-IP-Adresse (IPv4/IPv6).

9. Windows Anyconnect und DS-Lite im HomeOffice – IPv6 Transport

Die Kommunikation kann durch Verwendung der vollqualifizierten DNS Namen

```
wingate6.zam.kfa-juelich.de  
wingateb6.zam.kfa-juelich.de
```

fest auf Basis von IPv6 erfolgen.

10. Anyconnect und Linux

Die Installation erfolgt mit dem bereitgestellten Pre-Deployment-Image. Für die Installation werden Administratorrechte verlangt. Nutzen Sie aus dem Download-Bereich das jeweils aktuelle TAR-Archiv: anyconnect-predeploy-linux-64-4.5.03040-k9.tar.gz

Die nachfolgende Vorgehensweise gilt allgemein für die Versionen 4.x:

```
mount -r -t cifs //pcsrv.zam.kfa-juelich.de/public /mnt
```

Das Archiv in ein lokales Verzeichnis kopieren, auspacken und die Installation starten:

```
linux-oglv:~ #  
linux-oglv:~ # gunzip anyconnect-predeploy-linux-3.1.00495-k9.tar.gz  
linux-oglv:~ #  
linux-oglv:~ #  
linux-oglv:~ # dir *.tar  
-rwxr-xr-x 1 root root 21319680 Aug 30 04:15 anyconnect-predeploy-linux-3.1.00495-k9.tar  
linux-oglv:~ #  
linux-oglv:~ #  
linux-oglv:~ #  
linux-oglv:~ # tar -xvf anyconnect-predeploy-linux-3.1.00495-k9.tar
```

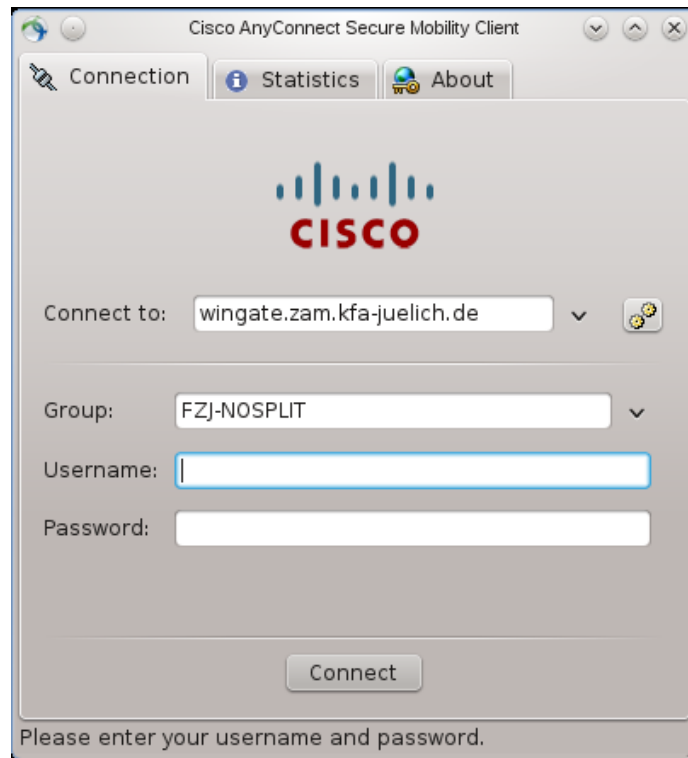
```
linux-oglv:~ #  
linux-oglv:~ # cd anyconnect-3.1.00495/  
linux-oglv:~/anyconnect-3.1.00495 #  
linux-oglv:~/anyconnect-3.1.00495 # cd vpn  
linux-oglv:~/anyconnect-3.1.00495/vpn #  
linux-oglv:~/anyconnect-3.1.00495/vpn #  
linux-oglv:~/anyconnect-3.1.00495/vpn # ls *.sh  
anyconnect_uninstall.sh vpn_install.sh vpn_uninstall.sh  
linux-oglv:~/anyconnect-3.1.00495/vpn #  
linux-oglv:~/anyconnect-3.1.00495/vpn # ./vpn_install.sh  
Installing Cisco AnyConnect Secure Mobility Client...
```

Die Verbindung kann wie folgt aufgebaut werden:

```
linux-oglv:~ #  
linux-oglv:~ # cd /opt/cisco/anyconnect/bin  
linux-oglv:/opt/cisco/anyconnect/bin #  
linux-oglv:/opt/cisco/anyconnect/bin # ./vpnui  
█
```

Statt der grafischen Bedienoberfläche

/opt/cisco/vpn/bin/vpnui



kann alternativ das Kommandozeilen-Tool

```
/opt/cisco/anyconnect/bin/vpn
```

```
VPN> connect wingate.zam.kfa-juelich.de
```

```
VPN> disconnect
```

genutzt werden. Speicherung der Zertifikate – ‚\$HOME/.cisco‘:

```
./cisco:  
certificates  
  
./cisco/certificates:  
client  
  
./cisco/certificates/client:  
myCert.pem private  
  
./cisco/certificates/client/private:  
myCert.key
```

(Stand: 05.09.2023 / Letzte Kontrolle: 05.09.2023)