Herstellen einer VPN Verbindung mit dem Cisco Secure Client

Inhalt

Allgemeines 2
VPN mit Cisco Secure Client unter Windows 3
Installation / Ersteinrichtung 3
Verbinden 4
Verbindung trennen 5
VPN mit Cisco Secure Client unter MacOS 6
Systemanforderungen 6
Installation / Ersteinrichtung 6
Verbinden 8
Verbindung trennen 9
VPN mit Cisco Secure Client unter Linux 10
Ersteinrichtung 10
Verbinden 11
Verbindung trennen 11
Bekannte Fehler 12
VPN mit Cisco Secure Client unter iOS 13
Installation 13
Verbinden 14
Verbindung trennen 15
VPN mit Cisco Secure Client unter Android 16
Installation / Ersteinrichtung 16
Verbinden 17
Verbindung trennen 18

Allgemeines

Download
Alle hier erwähnten Downloads finden Sie in unserem Kundenportal https://kundenportal.mk.de.

Wechseln Sie dort in den Bereich „MK-VPNConnect“ und klicken Sie auf die Kachel „Downloads“.

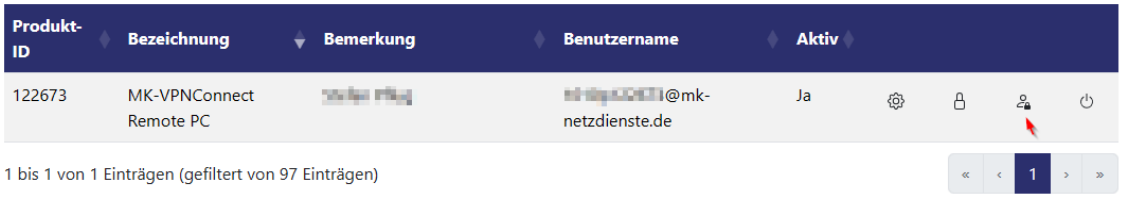
Für einen Client benötigen Sie die Cisco Secure Client Installationsdateien für das jeweilige Betriebssystem und ein VPN-Profil.
Bei den Windows und MacOS Installationsdateien ist das VPN-Profil bereits in den Paketen integriert.
Bei einer Linux Installation laden Sie das „MK Cisco-Secure Client VPN-Profil“ bitte separat herunter.

Obligatorische Zwei-Faktor-Authentifizierung
Zur Anmeldung am VPN benötigen Sie neben Ihrem Benutzernamen im Format

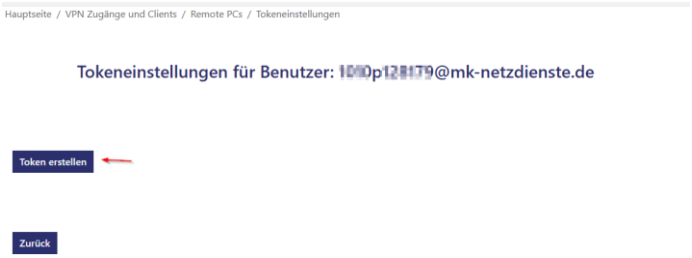
[Kunden-Nr]p[ArtikelID]@mk-netzdienste.de

eine Kombination aus Ihrem persönlichem VPN-Kennwort und einem sechsstelligem Zwei-Faktor-Token.

Wichtig: Sollten Sie bislang keinen zweiten Faktor benötigt haben, müssen Sie diesen vor dem Wechsel auf den Cisco Secure Client im Bereich „MK-VPNConnect“ des Kundeportals unterhalb der Kachel „Remote PC“ pro Benutzer erstellen



Über das Benutzer-Symbol erhalten Sie Zugriff auf die Token Einstellungen und können über den Button „Token erstellen“ einen Token für den Benutzer anlegen.



Anschließend können Sie wieder in die Token Einstellungen des Benutzers wechseln und den Token betrachten oder als PDF herunterladen.



Zur 2FA können Sie Authentifizierungsapps. wie z.B. Authy von Twilio, Google Authenticator, Microsoft Authenticator, FreeOTP Authenticator und kompatible Apps benutzen. Sie finden diese in den App-Stores Ihres mobilen Geräts.

VPN mit Cisco Secure Client unter Windows

Installation / Ersteinrichtung

Schritt 1

Nutzen Sie das korrekte Paket in Abhängigkeit von Ihrer Prozessorarchitektur:
Für X64 kompatible Prozessoren:
cisco-secure-client-win-5.1.xx.xxx-predeploy-GW2.zip

oder für ARM64 kompatible Prozessoren:
cisco-secure-client-win-arm64.5.1.xx.xxx-predeploy-GW2.zip

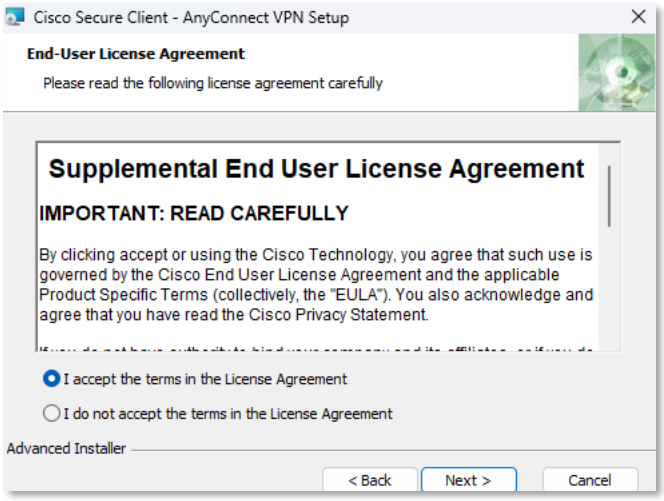
Wichtig: Entpacken Sie das Archiv
und führen die
cisco-secure-client-win-5.x.xx.xxx-core-vpn-predeploy-k9.msi
bzw.
cisco-secure-client-win-arm64-5.x.xx.xxx-core-vpn-predeploy-k9.msi
in dem entstandenen Verzeichnis aus.



Schritt 2

Lesen Sie die Lizenzbedingungen und akzeptieren Sie sie gegebenenfalls durch auswählen von
„I accept the terms in the License Agreement“ und klicken Sie anschließend auf „Next“.

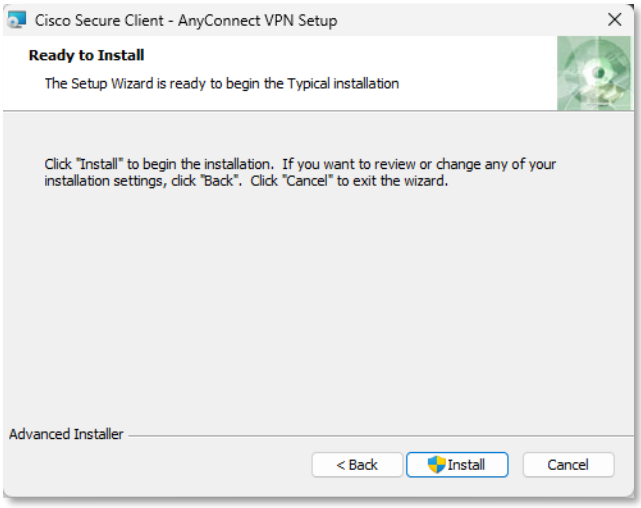
Falls Sie nicht mit den Bedingungen einverstanden sind, ist eine Nutzung des VPN-Dienstes leider nicht möglich.



Schritt 3

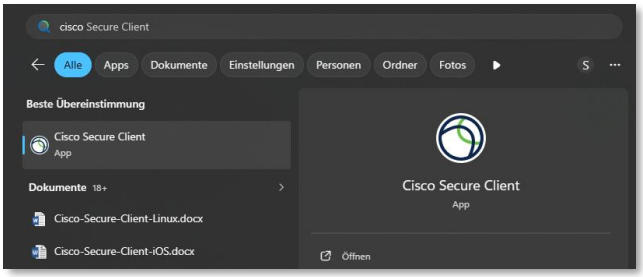
Bestätigen Sie durch einen Klick auf "Install". Sollte Windows Sie anschließend noch fragen, ob Sie Änderungen am Computer durch das Programm zulassen möchten, bestätigen Sie auch dies. Hierfür benötigen Sie Administratorenrechte. Sollten Sie diese nicht haben, dann wenden Sie sich an Ihren lokalen IT Ansprechpartner.

Die Installation findet dann ohne weiteres Zutun Ihrerseits statt. Anschließend können Sie das Installationsprogramm mit einem Klick auf "Finish" beenden.



Schritt 4

Klicken Sie auf das Cisco Secure Client-Icon in der Taskleiste. Sollte das Symbol dort nicht vorhanden sein, starten Sie aus dem Startmenü (über das Windows-Icon links unten in der Taskleiste) die Software "Cisco Secure Client".

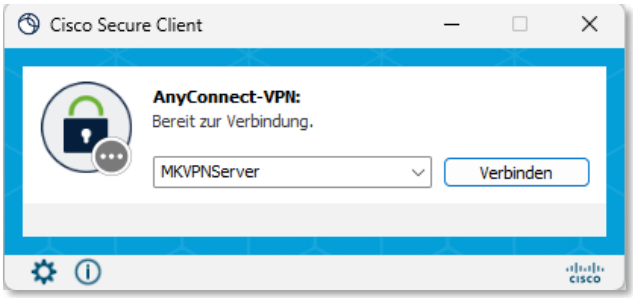


Verbinden

Schritt 1

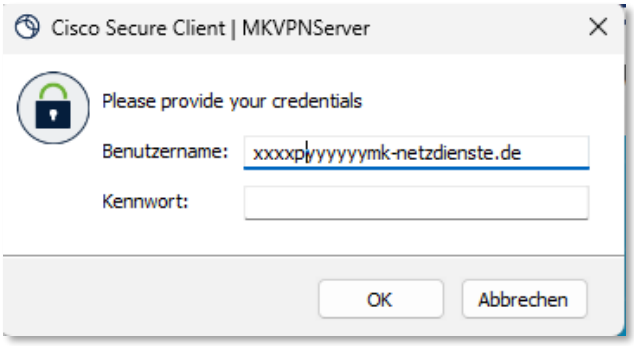
Das Feld sollte bereits mit „MKVPNServer" vorbelegt sein.
**Sollte dies nicht der Fall sein, wurde die Installation in Schritt 1. vermutlich direkt aus dem Archiv heraus gestartet.*

Klicken Sie jetzt auf "Verbinden".



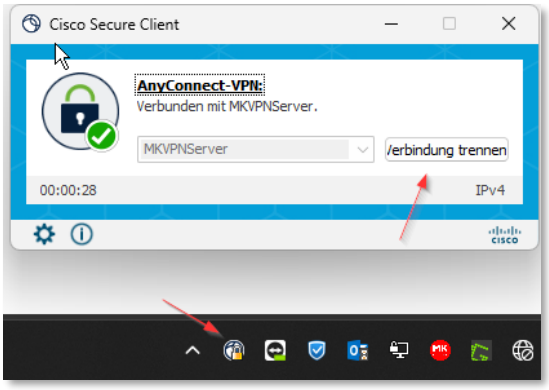
Schritt 2

Geben Sie jetzt Ihre Zugangsdaten für Ihren VPN Account in Form von Username und Passwort + Token ein.



Verbindung trennen

Wenn Sie die Verbindung nicht länger benötigen, klicken Sie wieder auf das "Cisco Secure Client"-Icon in der Taskleiste und wählen "Verbindung Trennen".



VPN mit Cisco Secure Client unter MacOS

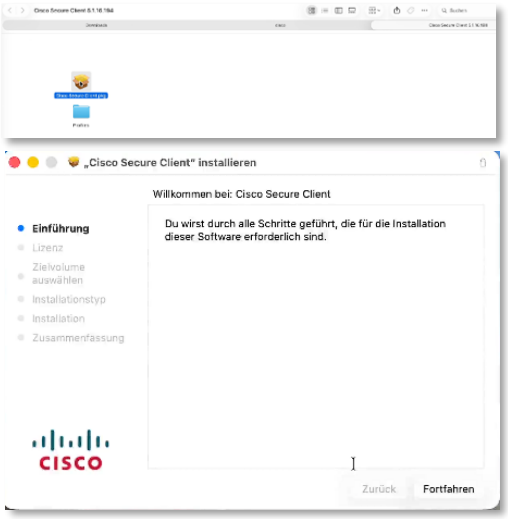
Systemanforderungen

Sie müssen mindestens eine der folgenden Versionen von MacOS installiert haben:
MacOS 14 (Sonoma) Version 14.5 oder höher
MacOS 15 (Sequoia)
MacOS 26 (Tahoe)

Installation / Ersteinrichtung

Schritt 1

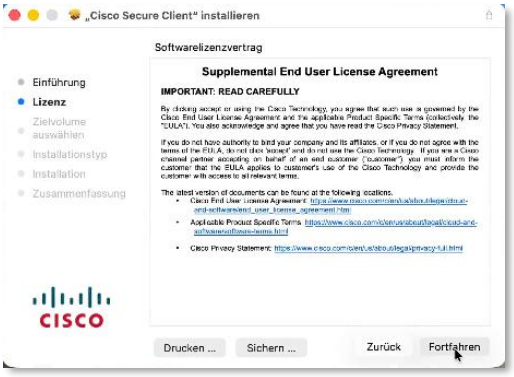
Mounten Sie die aus dem Kundenportal heruntergeladene DMG Datei *cisco-secure-client-macos-5.x.xx.xxx-predeploy-k9 GW2.dmg* (durch Doppelklick) und starten Sie die Paketinstallation durch Doppelklick auf die darin enthaltene .pkg Datei.



Ersteinrichtung – Schritt 2

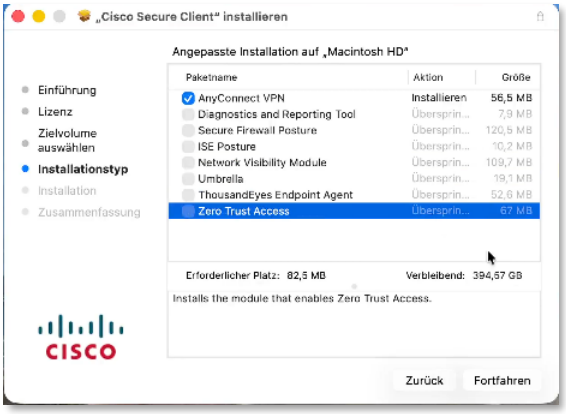
Klicken Sie dann auf der ersten Dialogseite auf "Fortfahren".

Lesen und akzeptieren Sie danach die Lizenzbedingungen. Falls Sie nicht mit den Bedingungen einverstanden sind ist eine Nutzung des VPN-Dienstes leider nicht möglich.



Ersteinrichtung - Schritt 3

Auf manchen Macs haben Sie nun die Gelegenheit, den Ort der Installation festzulegen. In der Regel ist der Standard Installationsort ("Macintosh HD") bereits vorausgewählt.

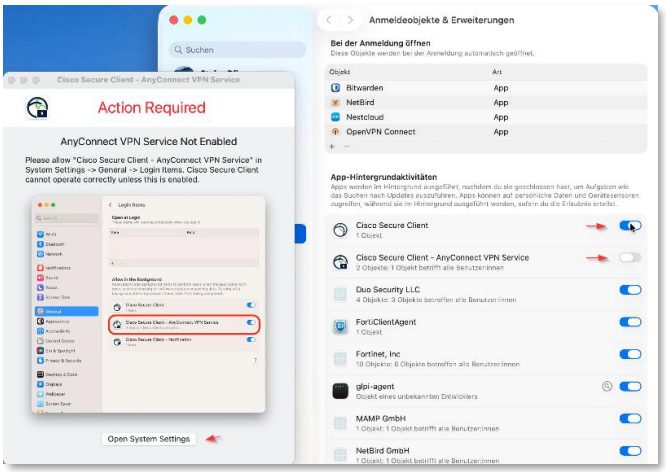


Unter Installationstyp deselektieren Sie bitte alle Punkte außer „AnyConnect VPN“ und klicken Sie auf „Fortfahren.“

Sollte sich ein Dialog mit dem Titel "Installationsprogramm" und der Meldung "Installationsprogramm versucht, neue Software zu installieren" öffnen, geben Sie bitte Ihr Benutzerpasswort ein
(Ihr Mac-Passwort - nicht das VPN Passwort!).
Klicken Sie auf "Software installieren".

Ersteinrichtung – Schritt 4

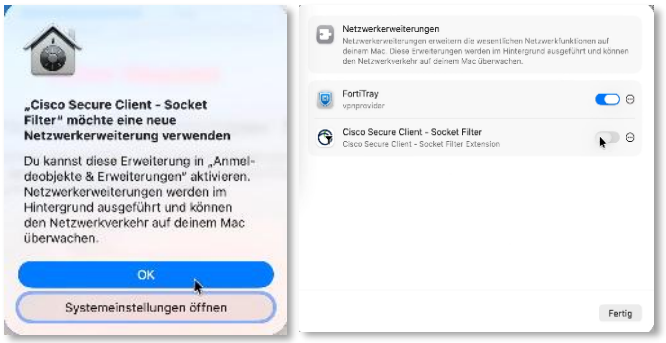
Während der Installation weist das Installationsprogramm auf diverse benötigte Rechte hin, die Sie jetzt selbstständig freigeben müssen. Klicken Sie jetzt auf Schaltfläche "Systemeinstellungen öffnen/Open System Settings".



Sie sollten sich jetzt im Menüpunkt "Allgemein / Anmeldeobjekte und Erweiterungen" befinden. Im Abschnitt App-Hintergrundaktivitäten aktivieren Sie die beiden Schalter
„Cisco Secure Client“ und
„Cisco Secure Client – Any Connect VPN Service“.

Bestätigen Sie die Einstellungen durch Eingabe Ihres Benutzerpasswortes / Fingerprint.

Anschließend fordert ein Dialog noch zur Aktivierung des Cisco Secure Client - Socket Filters“ auf.
Klicken Sie auf „Systemeinstellungen öffnen“.



Setzen Sie den Schalter bei
„Cisco Secure Client – Socket Filter“ und bestätigen dies erneut durch die Eingabe Ihres Benutzerpasswortes.

Klicken Sie in der Nachfrage
„Darf Cisco Secure Client – Socket Filter
„Netzwerkinhalte filtern“
auf „Erlauben“

Klicken Sie auf „Fertig“



Der Installationsvorgang sollte jetzt abgeschlossen sein. Schließen Sie das Fenster "Die Installation war erfolgreich".

Sie sollten Ihren Mac jetzt sicherheitshalber einmal neustarten.



Verbinden

Schritt 1

Starten Sie den "Cisco Secure Client", z.B. über das Launchpad.

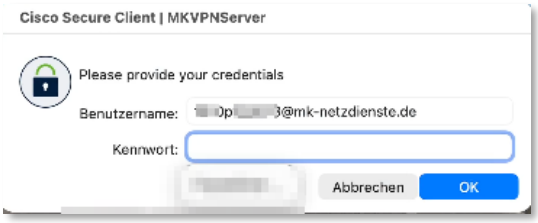
Das Feld sollte bereits mit „MKVPNServer“ vorbelegt sein.

Klicken Sie jetzt auf "Verbinden".



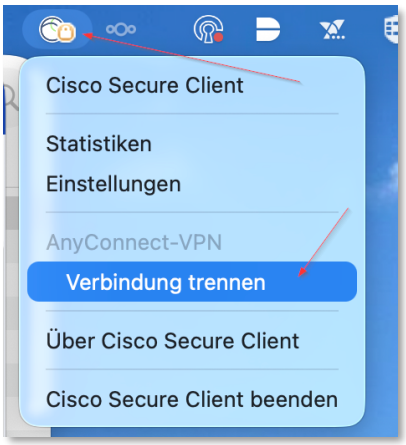
Verbinden – Schritt 2

Geben Sie jetzt Ihre Zugangsdaten für Ihren VPN Account in Form von Username und Passwort + Token ein.



Verbindung trennen

Wenn Sie die Verbindung nicht länger benötigen, klicken Sie auf das Cisco Secure Client-Icon im Panel und wählen "Verbindung trennen"



VPN mit Cisco Secure Client unter Linux

Die Nachfolgende Anleitung ist mit der Client-Version 5.1.16.194 erstellt worden.

Ersteinrichtung

Schritt 1

Nutzen Sie das korrekte Paket in Abhängigkeit von Ihrer Linux Distribution und Prozessorarchitektur (X64/ARM64):
cisco-secure-client-linux64-5.x.xx.xxx-predeploy-deb-k9.tgz
cisco-secure-client-linux64-5.x.xx.xxx-predeploy-rpm-k9.tgz
cisco-secure-client-linux-arm64-5. x.xx.xxx-predeploy-deb-k9.tgz
cisco-secure-client-linux-arm64-5. x.xx.xxx-predeploy-rpm-k9.tgz

Zusätzlich sollte das „MK Cisco-Secure Client VPN-Profil" in Form der Datei acvpn.xml vorliegen.

Wir gehen davon aus, dass sich die Pakete in Ihrem Downloadverzeichnis befinden.

Ersteinrichtung - Schritt 2

Öffnen Sie ein Terminal und gehen wie folgt vor:

#wechseln in das Download Verzeichnis des akt. Benutzers
cd ~/Downloads

#entpacken des Downloads (Dateinamen anpassen)
sudo tar -vxzf cisco-secure-client-linux-k9.tgz*

#Installation des VPN Paketes auf apt basierenden Betriebssystemen
es muss nur ein Paket (cisco-secure-client-vpn_5.x.xx.xxx_xxx64.deb) installiert werden
sudo apt install ./cisco-secure-client-vpn_*.deb

Installation des VPN Paketes auf rpm basierenden Betriebssystemen:
es muss nur ein Paket (cisco-secure-client-vpn-5.x.xx.xxx_xxx64.rpm) installiert werden
sudo dnf install ./cisco-secure-client-vpn-5.rpm*

#*Kopieren Sie das heruntergeladene* VPN-Profil in das Applikationsverzeichnis:
sudo mv acvpn.xml /opt/cisco/secureclient/vpn/profile/acvpn.xml

Verbinden

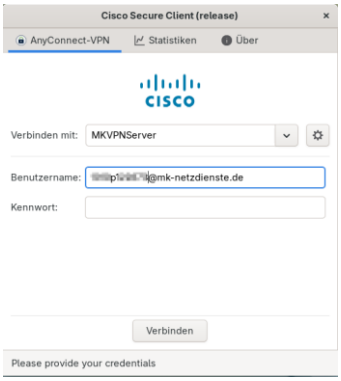
Schritt 1

Öffnen Sie die Cisco Secure Client Applikation.
Das Feld „Verbinden mit:“ sollte bereits mit „MKVPNServer“ vorbelegt sein.
Und klicken Sie auf „Verbinden“



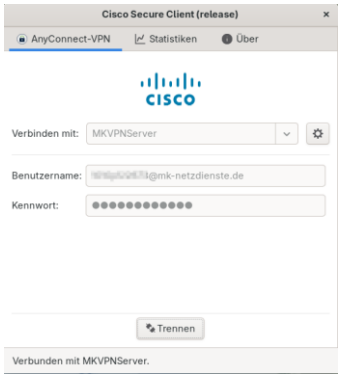
Verbinden – Schritt 2

Geben Sie jetzt Ihre Zugangsdaten für Ihren VPN Account in Form von Username und Passwort + Token ein.



Verbindung trennen

Wenn Sie die Verbindung nicht länger benötigen, wählen Sie das Register „AnyconneCt VPN“ im "Cisco Secure Client“
und klicken auf "Verbindung Trennen".



Bekannte Fehler

- Die Installation des RPM Paketes des Cisco Secure Client in der Version 5.1.16
  bleibt unter Fedora Workstation während des %pretrans Skriptes hängen..
  Workaround:
  Das Skript verhindert nur ein Downgrade und kann mittels
  sudo dnf install ./cisco-secure-client-vpn-5.1.16.194-1.x86_64.rpm --setopt=tsflags=nopretrans
  übersprungen werden

VPN mit Cisco Secure Client unter iOS

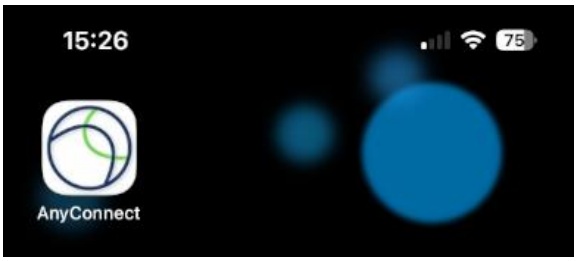
Installation

Schritt 1

Installieren Sie Cisco Secure Client aus dem AppStore und starten Sie es.

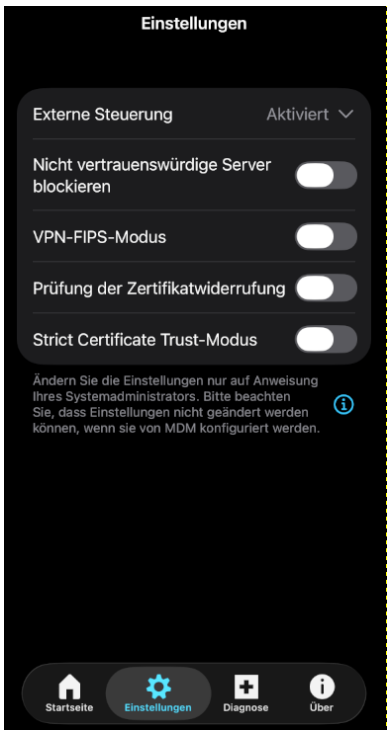
Öffnen der App – Schritt 2

Öffnen Sie den Client, welcher im vorherigen Schritt aus dem App-Store installiert wurde.



Ersteinrichtung - Schritt 3

Wechseln Sie in die **Einstellungen**
und stellen die **Externe Steuerung** auf „**Aktiviert**".



Ersteinrichtung – Schritt 4

Öffnen Sie dieses PDF auf dem Mobilgerät und klicken auf diesen Provisionsierungslink.

Alternativ können Sie auch den nebenstehenden QR-Code mit der Kamera-App öffnen

Ersteinrichtung – Schritt 5

Erlauben Sie die Anlage der VPN Verbindung und bestätigen Sie dies im nächsten Dialog mit Ihrem IPhone Gerätecode / Face-ID.

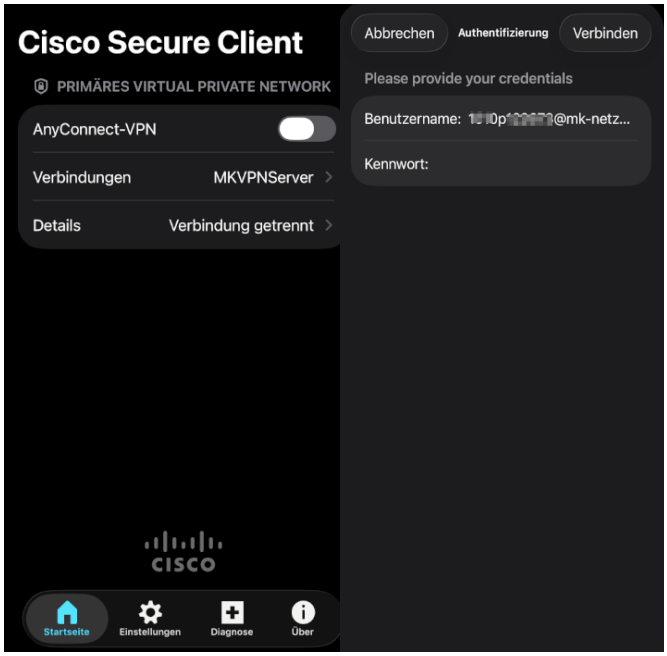


Verbinden

Schritt 1

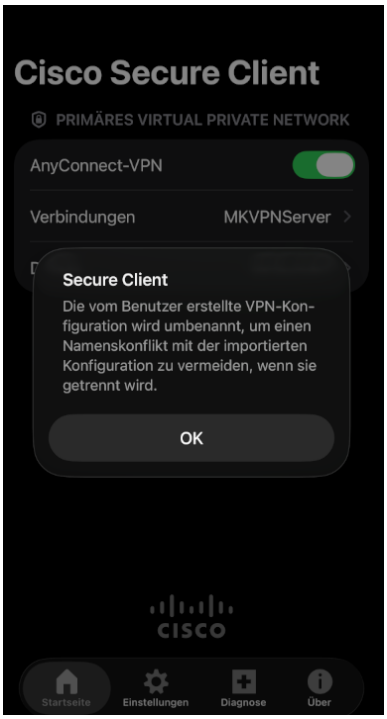
Aktivieren Sie den Schalter „AnyConnect-VPN". Im nächsten Schritt öffnet sich ein Anmeldefenster.

Geben Sie jetzt Ihre Zugangsdaten für Ihren VPN Account in Form von Username und Passwort + Token ein.



Verbinden – Schritt 2

Beim ersten Verbindungsaufbau wird das finale Profil vom Gateway importiert.
Die einmalige Meldung über den Namenskonflikt kann ignoriert werden.



Verbindung trennen

Wenn Sie die Verbindung nicht länger benötigen, deaktivieren Sie den Schalter „AnyConnect-VPN“.

VPN mit Cisco Secure Client unter Android

Installation / Ersteinrichtung

Schritt 1

Installieren Sie Cisco Secure Client aus dem PlayStore und starten Sie es.

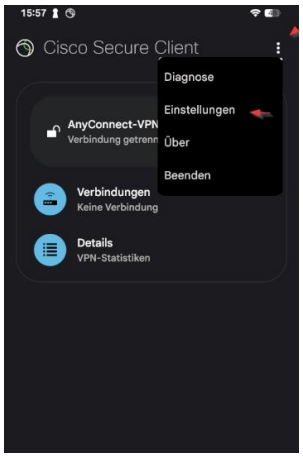
Öffnen der App – Schritt 2

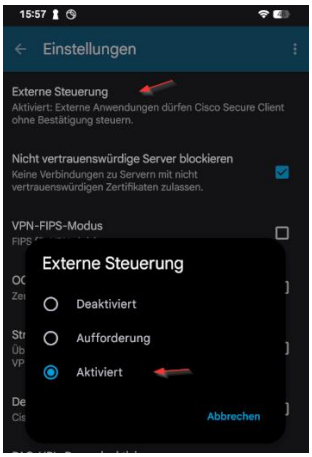
Öffnen Sie den Client, welcher im vorherigen Schritt aus dem App-Store installiert wurde.



Ersteinrichtung - Schritt 3

Wechseln Sie im ☰ Menu auf **Einstellungen** und stellen die **Externe Steuerung** auf „**Aktiviert**".





Ersteinrichtung – Schritt 4

Öffnen Sie dieses PDF auf dem Mobilgerät und klicken auf diesen Provisionsierungslink.

Alternativ können Sie auch den nebenstehenden QR-Code mit der Kamera-App öffnen

Der Erfolgreiche Import der Verbindung wird durch eine entsprechende Meldung quittiert.

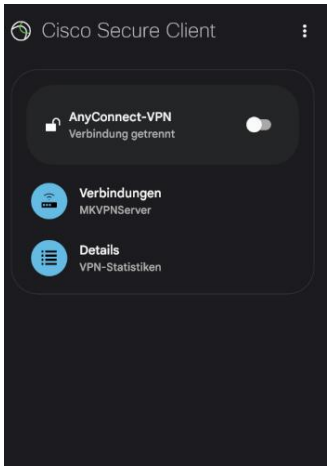


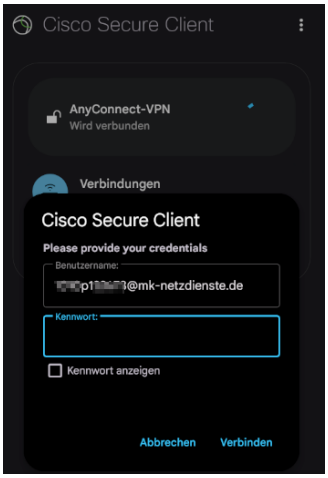
Verbinden

Schritt 1

Aktivieren Sie den Schalter „AnyConnect-VPN“.
Im nächsten Schritt öffnet sich ein Anmeldefenster.

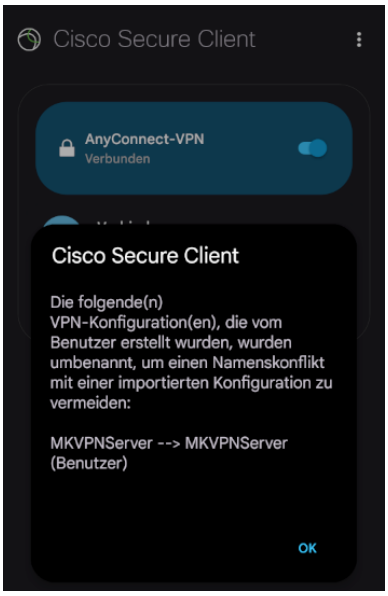
Geben Sie jetzt Ihre Zugangsdaten für Ihren VPN Account in Form von Username und Passwort + Token ein.





Verbinden – Schritt 2

Beim ersten Verbindungsaufbau wird das finale Profil vom Gateway importiert.
Die einmalige Meldung über den Namenskonflikt kann ignoriert werden.



Verbindung trennen

Wenn Sie die Verbindung nicht länger benötigen, deaktivieren Sie den Schalter „AnyConnect-VPN".