Remote-Zugriff

Das Arbeiten über Remotedesktop ermöglicht Flexibilität und Sicherheit.

- Verbindung zu einem Remotedesktop (Terminalserver) aufbauen
- Zugriff auf den Terminalserver mittels Remote Desktop Connection Manager (RDCMan)
- Verbindungseinstellungen für den Terminalserver anpassen
- Fernzugriff mittels VPN und TightVNC
- VPN mittels Wireguard herstellen
- VPN mittels Securepoint SSL-VPN herstellen
- VPN mittels VPN Access Manager herstellen
- Remoteaudio Kamera und Mikrophone auf dem Terminalserver nutzen
- Fehlermeldungen (Logs) vom Securepoint SSL-VPN Client anzeigen und abspeichern
- Wireguard Verbindung ohne Adminrechte konfigurieren

Verbindung zu einem Remotedesktop (Terminalserver) aufbauen

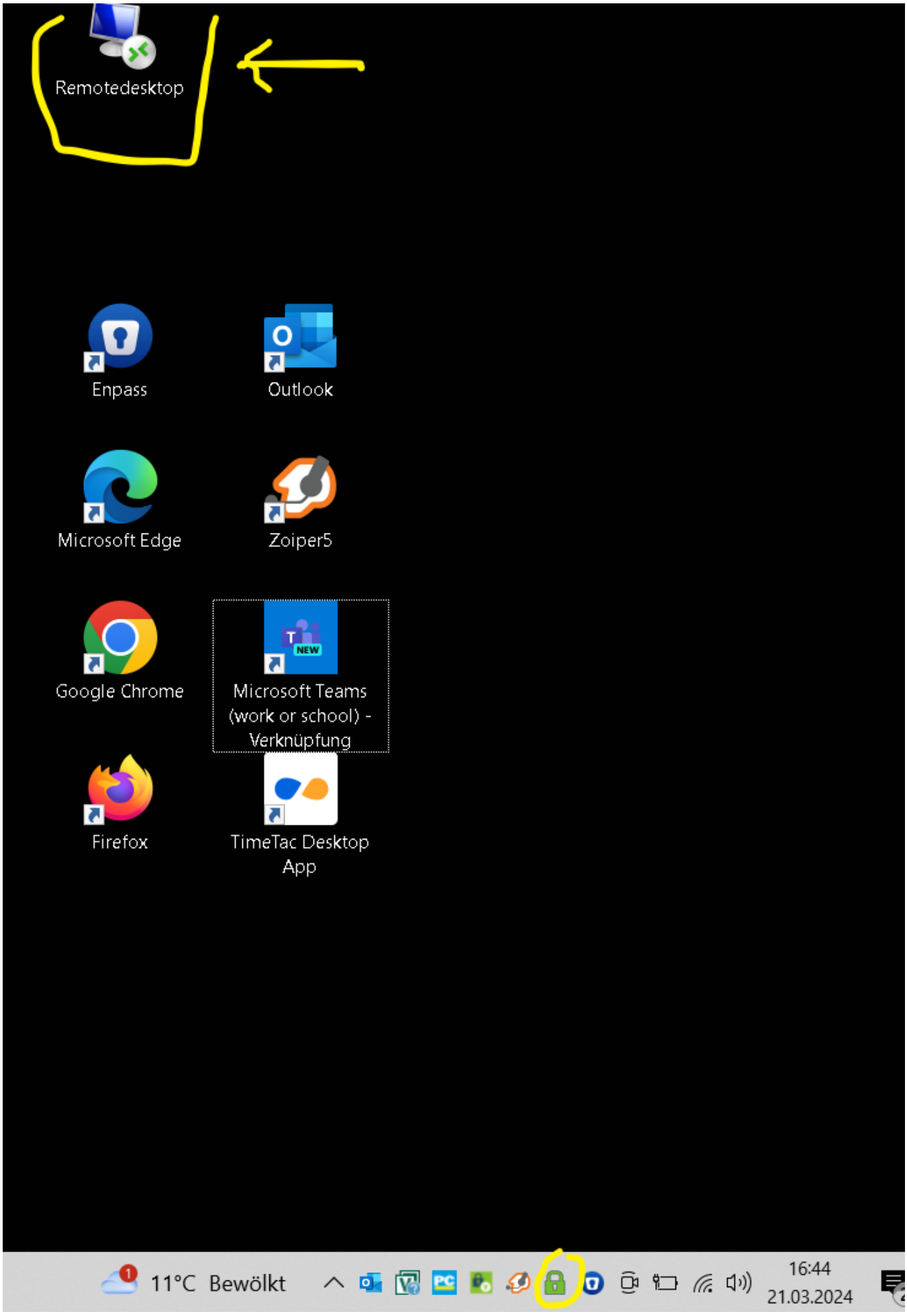
Wenn Sie einen VPN-Verbindung benötigen, nutzen Sie bitte eine der folgenden Anleitungen

Wireguard: VPN mittels Wireguard ... | PC-SPEZIALIST Wiki

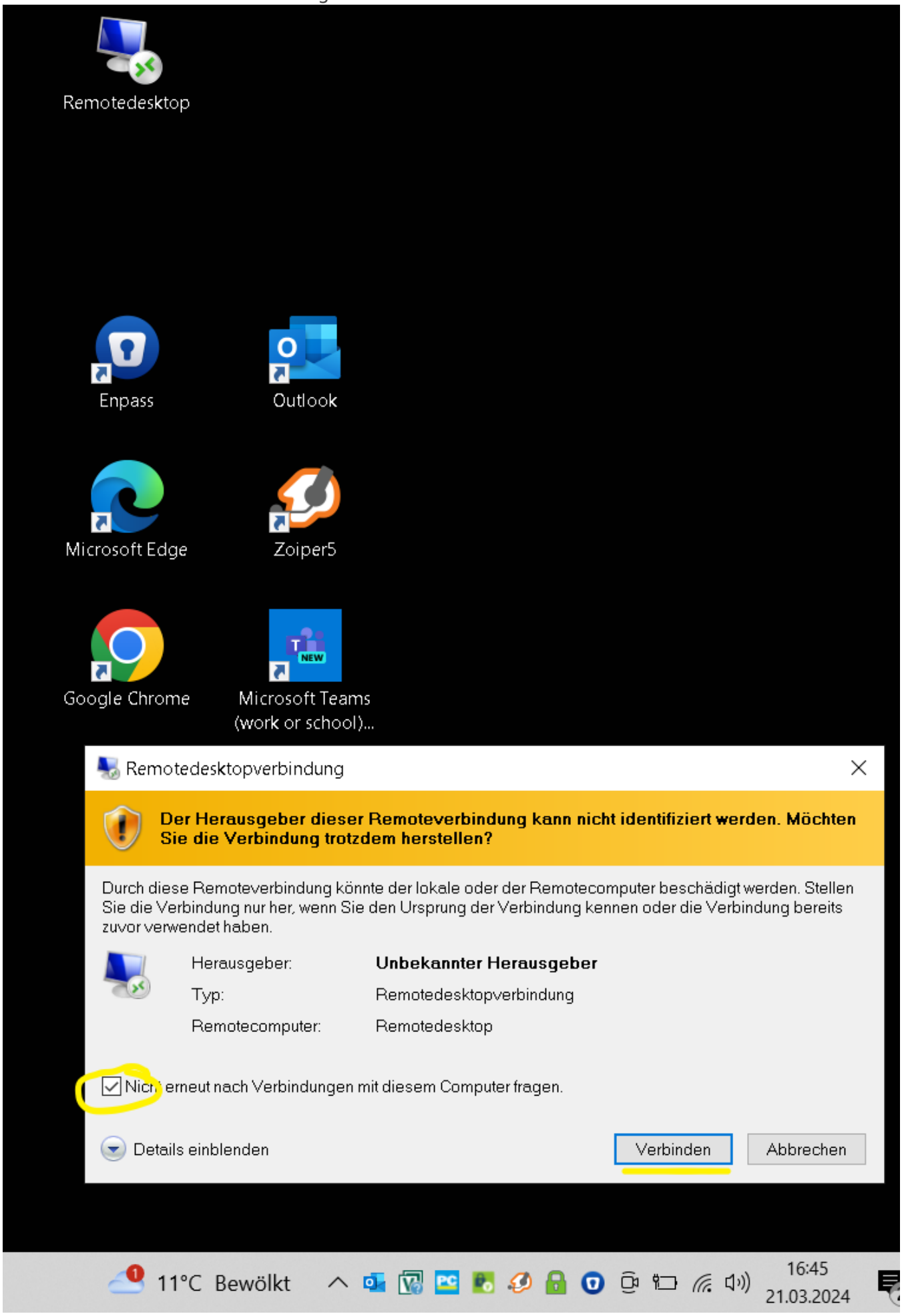
Securepoint SSL VPN: VPN mittels Securepoin... | PC-SPEZIALIST Wiki

VPN Access Manager: VPN mittels VPN Access... | PC-SPEZIALIST Wiki

- Verbinden Sie sich nun mit dem Remotedesktop. Das Symbol ist ein Monitor mit zwei grünen Pfeilen. Dort ist in der Regel der Name oder die IP-Adresse des Rechners bereits hinterlegt.

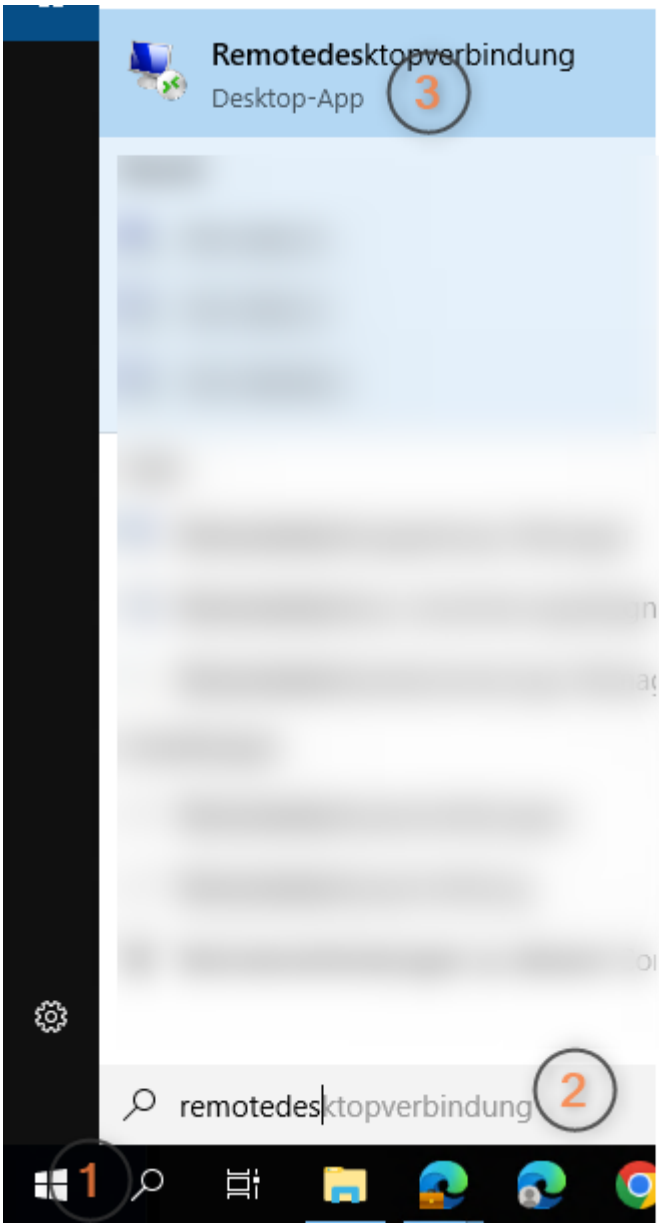

Remotedesktop
Enpass
Outlook
Microsoft Edge
Zoiper5
Google Chrome
Microsoft Teams (work or school) - Verknüpfung
Firefox
TimeTac Desktop App
11°C Bewölkt
16:44
21.03.2024

- Sie können der Remoteverbindung vertrauen.



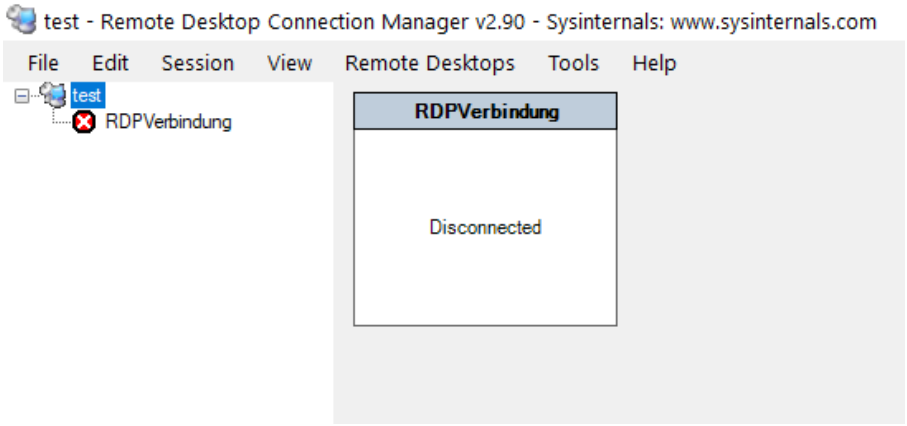
- Melden Sie sich nun mit den Zugangsdaten an und es kann losgehen.

Sollten Sie das Symbol nicht auf dem Desktop sehen, suchen Sie bitte danach:
Klicken Sie auf die Lupe bzw. das Suchfeld (1) und geben **Remotedesktopverbindung (2)** ein.
Klicken Sie das Suchergebnis an.
Danach

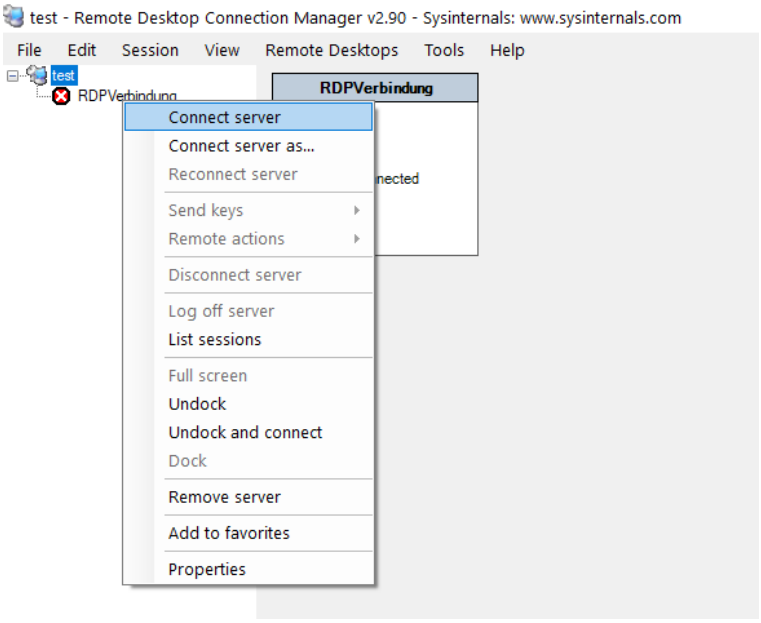


Zugriff auf den Terminalserver mittels Remote Desktop Connection Manager (RDCMan)

Desktop -> Verzeichnis RDCMan -> RDCman.exe starten



Rechtsklick auf die "**RDPVerbindung**"



Linksklick auf "**Connect Server**"

Entweder die Zugangsdaten sind gespeichert oder es müssen Benutzername und Passwort eingegeben werden

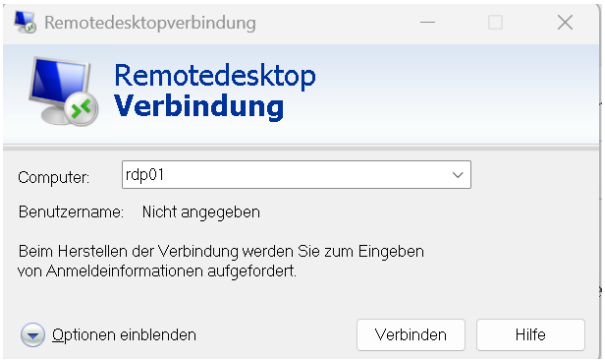
Vollbild kann über die Tastenkombination **STRG+ALT+UMBRUCH** gestartet oder verlassen werden.

Weitere Details gibt es unter https://learn.microsoft.com/de-de/sysinternals/downloads/rdcman.

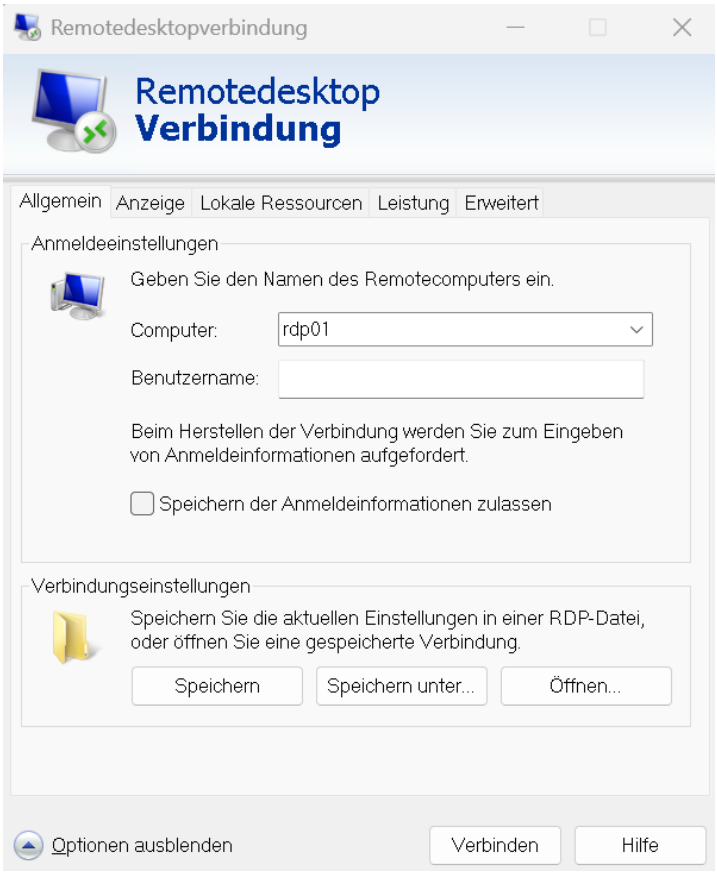
Verbindungseinstellungen für den Terminalserver anpassen

Wenn Sie mittels der App**Remotedesktop**  eine Verbindung zum Terminalserver herstellen, haben Sie einige Einstellmöglichkeiten.

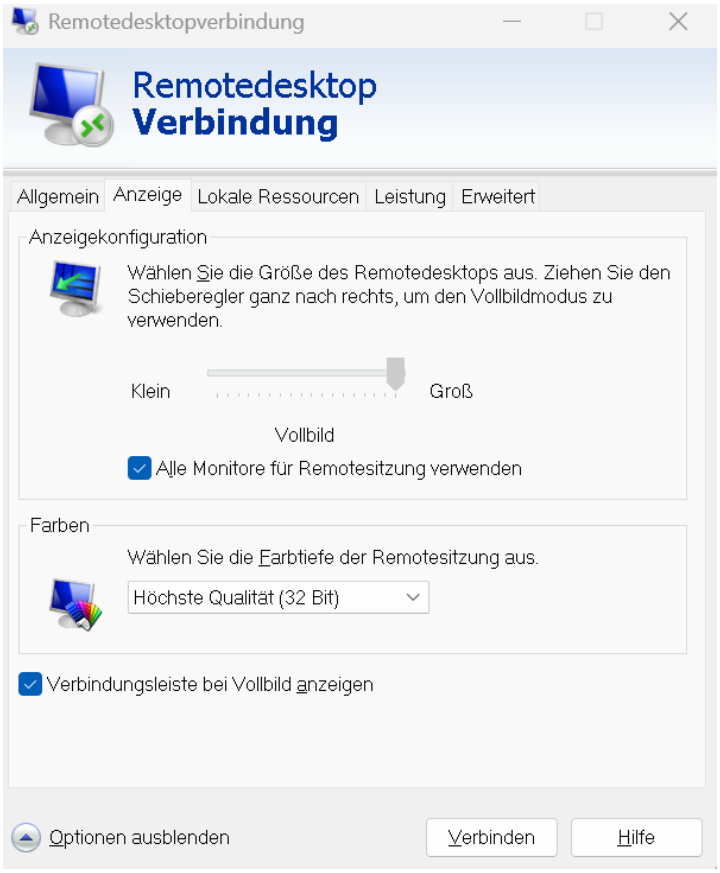
Starten Sie die App und klicken auf "Optionen einblenden"



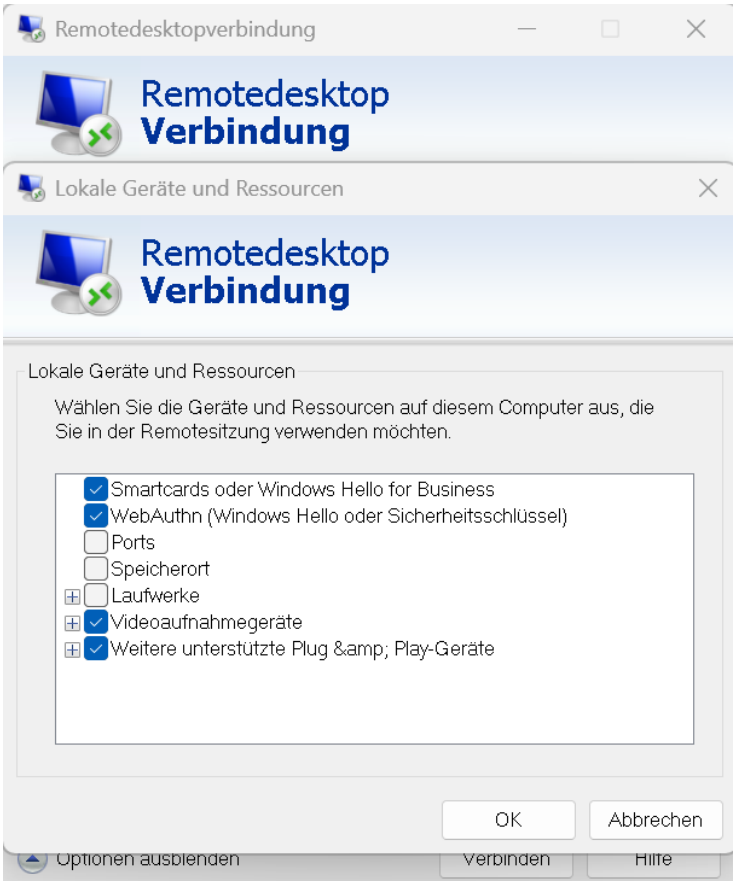
Sie erhalten diese Ansicht



Unter dem Reiter "**Anzeige**" können Sie zum Beispiel den Haken bei "**Alle Monitore für Remotesitzung verwenden**" setzen, wenn sie über mehrere Bildschirme verfügen und diese nutzen möchten.

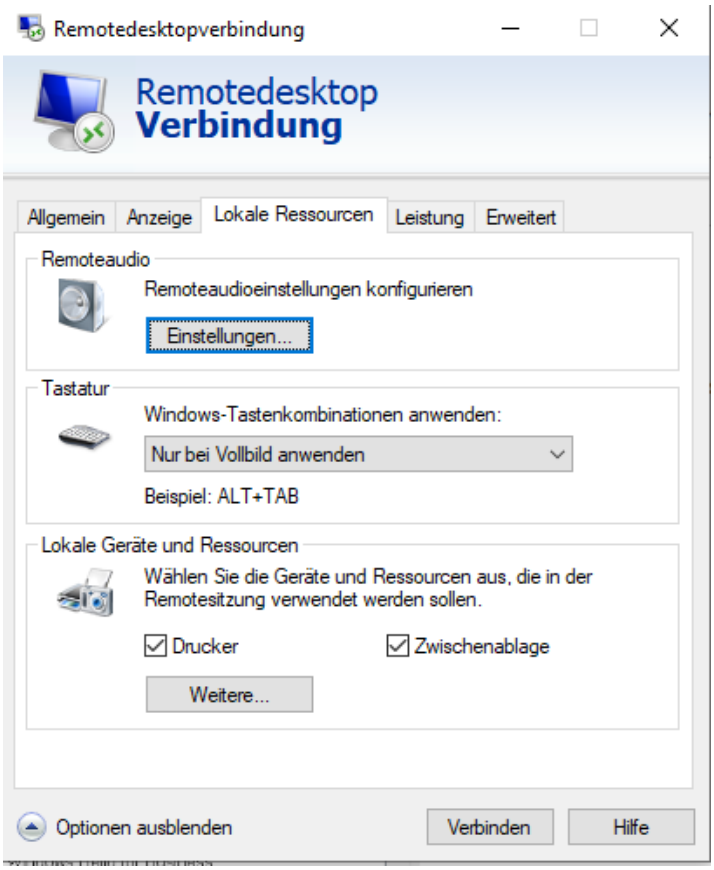


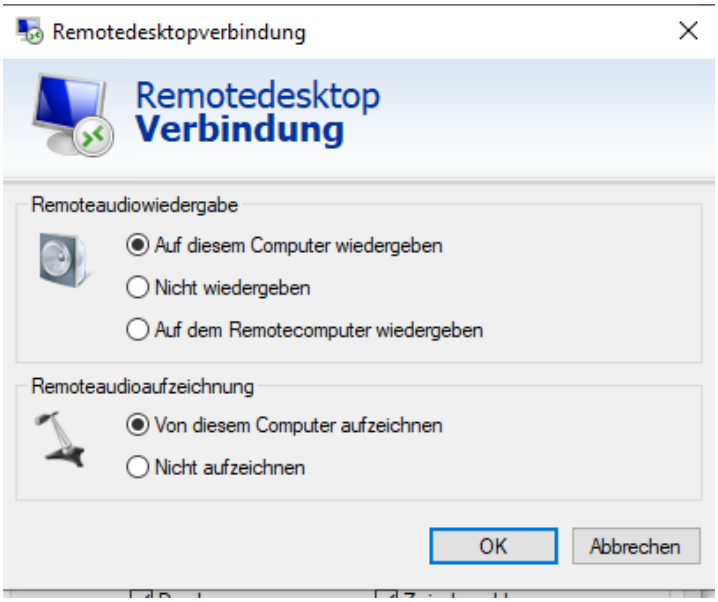
Unter dem Reiter "**Lokale Ressourcen**" können Sie im Bereich "**Lokale Geräte und Ressourcen** " auf "**weitere**" klicken



Hier haben Sie zum Beispiel die Möglichkeit, die Geräte für "**Videoaufnahme**" einzubinden.

Und unter "Lokale Ressourcen" "Remoteaudio" können Sie mit einem Klick auf "Einstellungen" festlegen, wie mit Lautsprechern bzw. Mikrophonen umgegangen werden soll





So werden Videokonferenzen auch auf dem Terminalserver möglich.

Fernzugriff mittels VPN und TightVNC

Um aus der Ferne auf einen PC und/oder Server zugreifen zu können sind mehrere Schritte nötig

1.) Aufbau der VPN-Verbindung. Es gibt verschiedene Optionen.

- Securepoint SSL VPN: VPN mittels Securepoin... | PC-SPEZIALIST Wiki

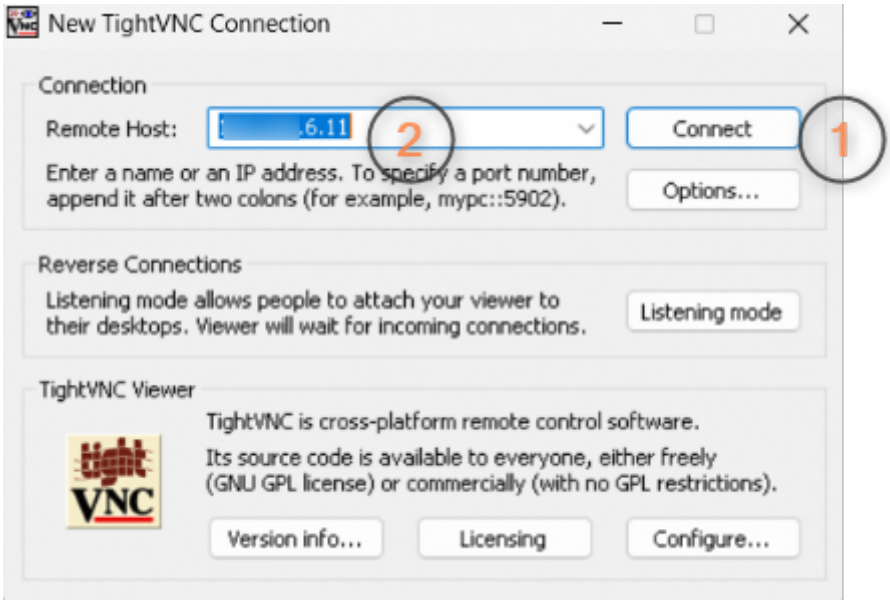
- VPN AccessManager (Shrewsoft): VPN mittels VPN Access... | PC-SPEZIALIST Wiki

- Wireguard: VPN mittels Wireguard ... | PC-SPEZIALIST Wiki

2.) Herstellern der Verbindung mittels TightVNC Viewer

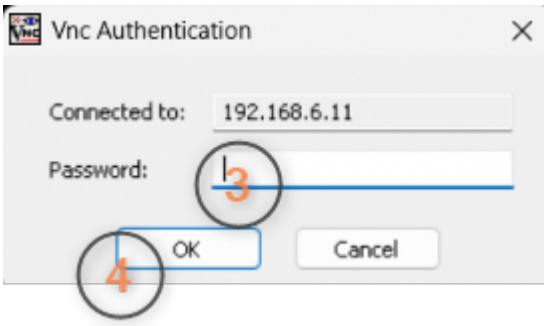
Sie finden das Programm über die Suchfunktion von Windows 

Nach dem Start der Software klicken Sie auf **Connect** (1)
Sollte bei **RemoteHost** (2) nichts eingetragen sein, muss dort die **IP-Adresse des Computers** eingetragen werden, auf den Sie aus der ferne zugreifen wollen



Weitere Einstellungen sind nicht notwendig

Hier geben Sie noch das **Passwort** (3) ein und klicken auf **OK** (4)



3.) Anpassen der Bildschirmeinstellung

Sollten Sie von einem Gerät mit einem Bildschirm, z.B. einen Notebook auf einen PC mit mehreren Bildschirmen zugreifen, empfiehlt es sich, die weiteren Bildschirme temporär zu deaktivieren

Konfiguration von mehr... | PC-SPEZIALIST Wiki

Den Vollbild-Modus von TightVNC aktiviert oder deaktiviert man mit den Drücken von STRG + ALT + SHIFT + F gleichzeitig

VPN mittels Wireguard herstellen

Sie haben auf Ihrem Computer die Software **Wireguard** installiert.

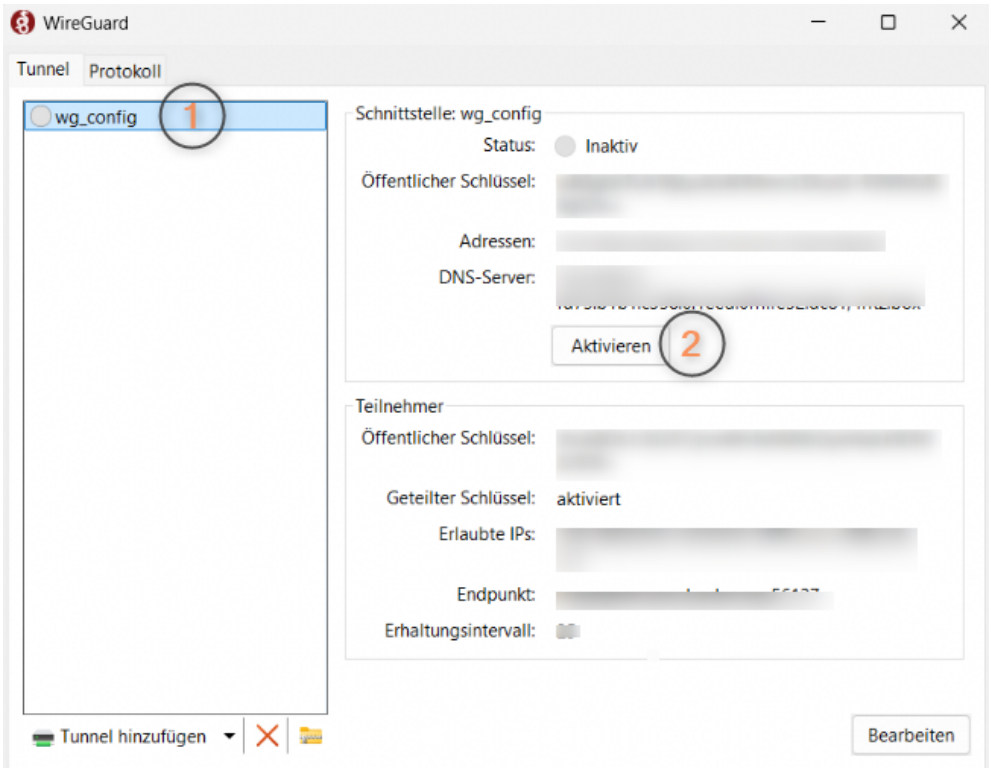
Wireguard wird üblicherweise mit dem Start von Windows geladen. Sie finden das Symbol  neben Datum und Uhrzeit in der rechten Ecke.

Vielleicht ist es auch hinter diesem Symbol  versteckt.

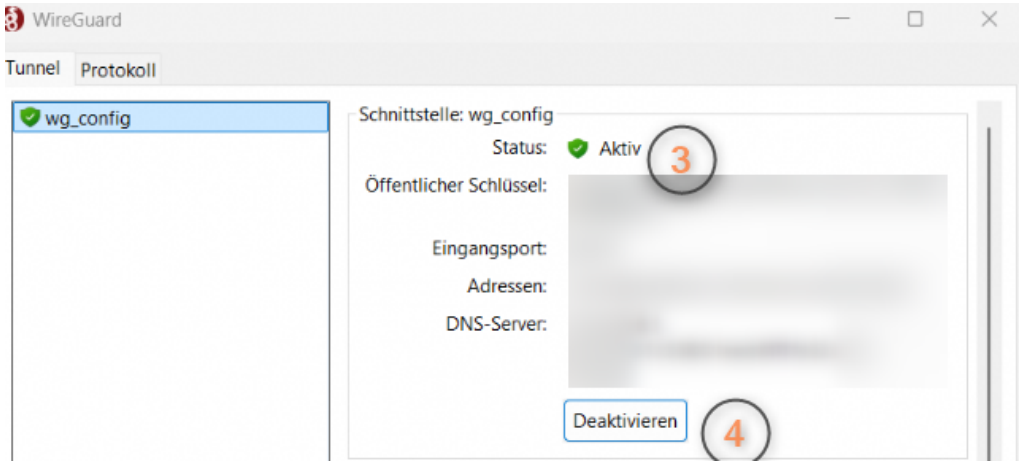
Sie können auch über das Suchfenster 

danach suchen und das Programm starten

In der Software sehen Sie Ihr Profil (1) und klicken auf Aktivieren (2)



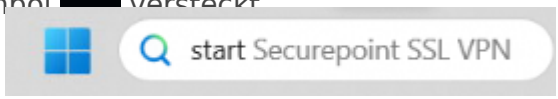
Wenn die Verbindung erfolgreich aufgebaut ist, erkennen Sie dies am Status: Aktiv (3) und können die Verbindung mit Deaktivieren (4) beenden


WireGuard
Tunnel
Protokoll
wg_config
Schnittstelle: wg_config
Status:
Aktiv
3
Öffentlicher Schlüssel:
Eingangsport:
Adressen:
DNS-Server:
Deaktivieren
4

VPN mittels Securepoint SSL-VPN herstellen

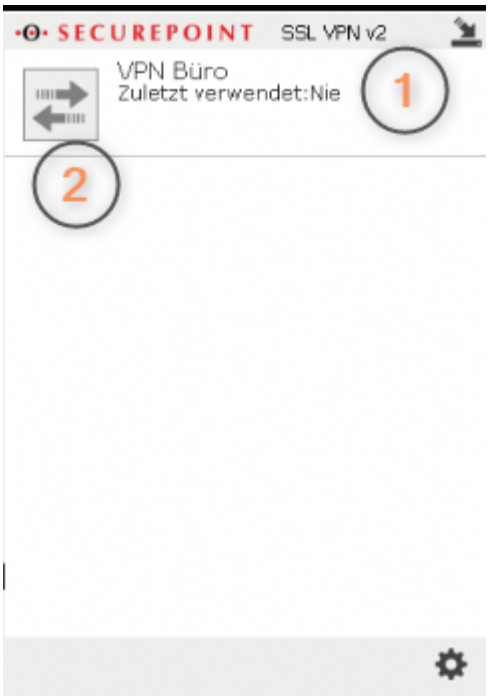
Sie haben auf Ihrem Computer die Software **Securepoint SSL VPN** installiert.
Securepoint SSL VPN wird üblicherweise mit dem Start von Windows geladen. Sie finden das Symbol neben Datum und Uhrzeit in der rechten Ecke

Vielleicht ist es auch hinter diesem Symbol versteckt

Sie können auch über das Suchfenster 

danach suchen und das Programm starten.

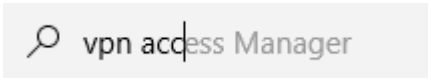
Mit einem Doppelklick auf öffnen Sie das Programm und sehen Ihr VPN-Profil (1) und starten die Verbindung mit einem Mausklick (2)



Sobald die Verbindung hergestellt ist, wird das Fenster automatisch minimiert und das Symbol in der Taskleiste wird Grün dargestellt

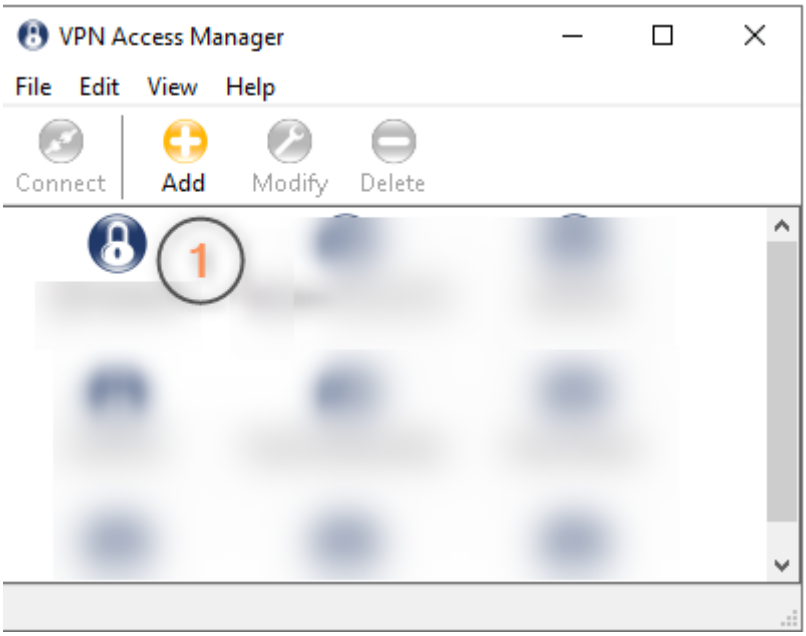
VPN mittels VPN Access Manager herstellen

Sie haben auf Ihrem Computer die Software **VPN Access Manager** installiert.
VPN Access Manager wird nicht mit dem Start von Windows geladen.

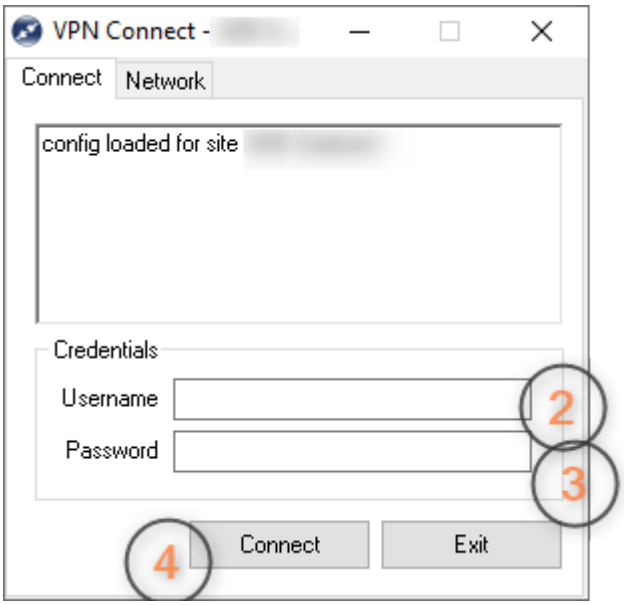
Sie können über das Suchfenster 

danach suchen und das Programm starten

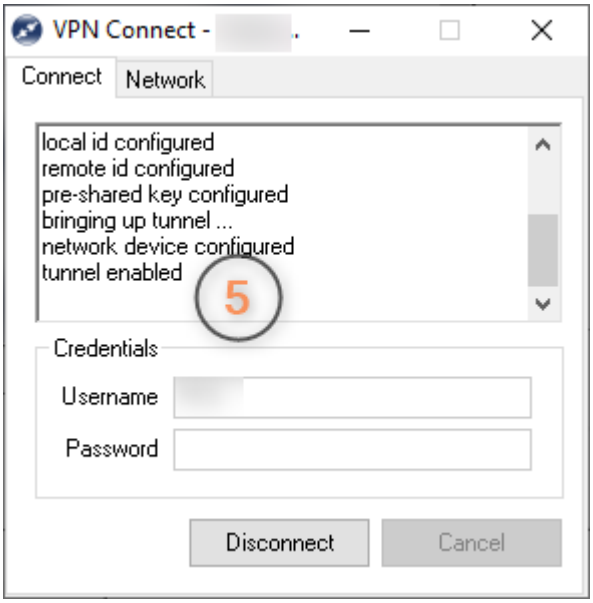
In der Software sehen Sie Ihr Profil (1) und führen darauf einen Doppelklick aus



Hier geben Sie Benutzername (2) und Passwort (3) ein und klicken auf Connect (4)



Ist die Verbindung erfolgreich hergestellt, erkennen Sie dies daran: tunnel enabled (5)

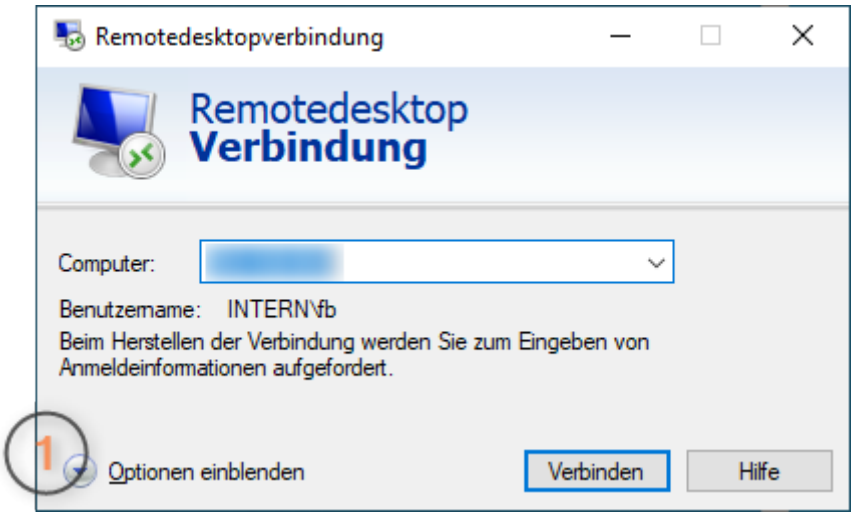


Remoteaudio Kamera und Mikrophone auf dem Terminalserver nutzen

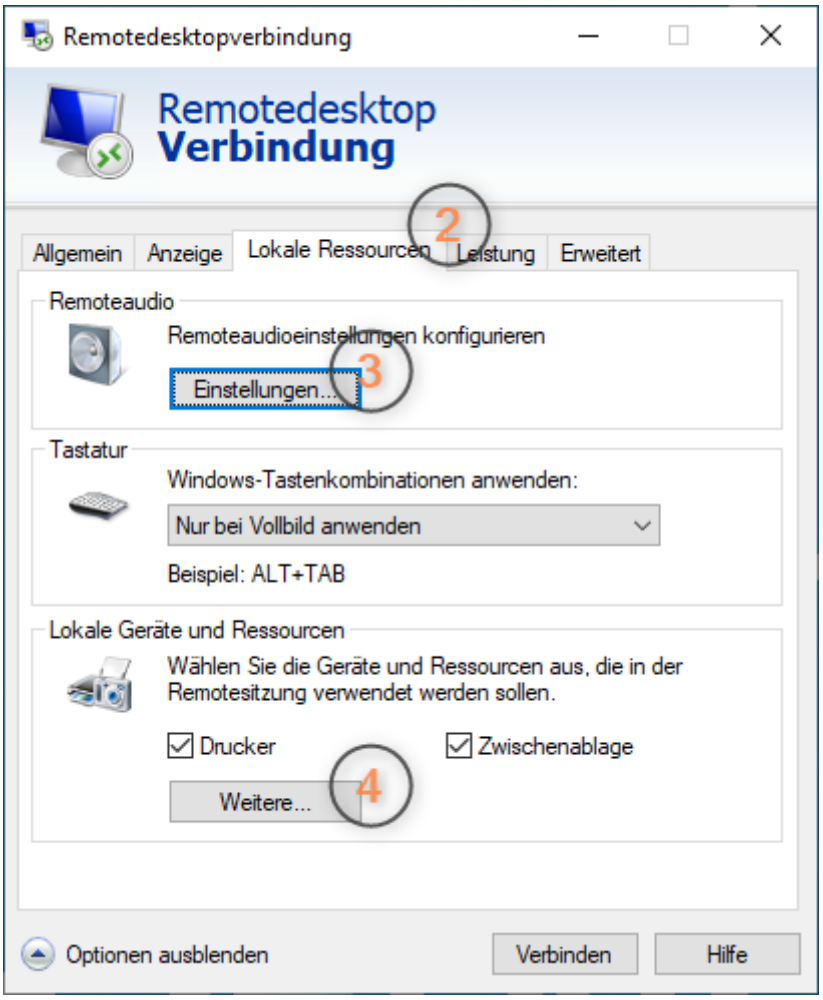
Sie möchten Audio und Video auf dem Terminalserver nutzen, um zum Beispiel dort Telefante führen oder TEAMS nutzen zu können

1.) Konfiguration auf dem PC oder Notebook, mit dem die Verbindung zum Terminalserver hergestellt wird

Zuerst **Optionen einblenden** (1)

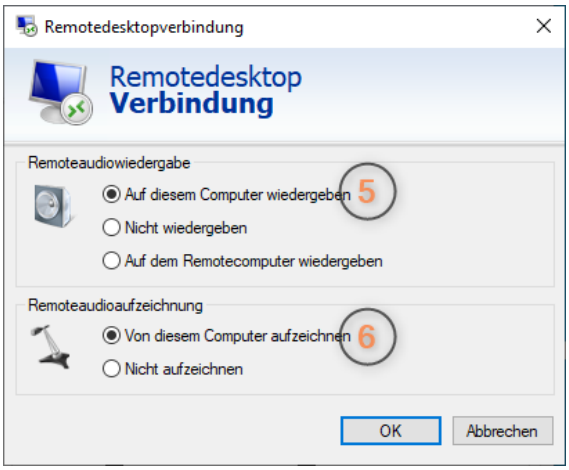


Wechsel zu **Lokale Ressourcen** (2)
Hier müssen **Einstellungen** (3) und **Weitere** (4) konfiguriert werden



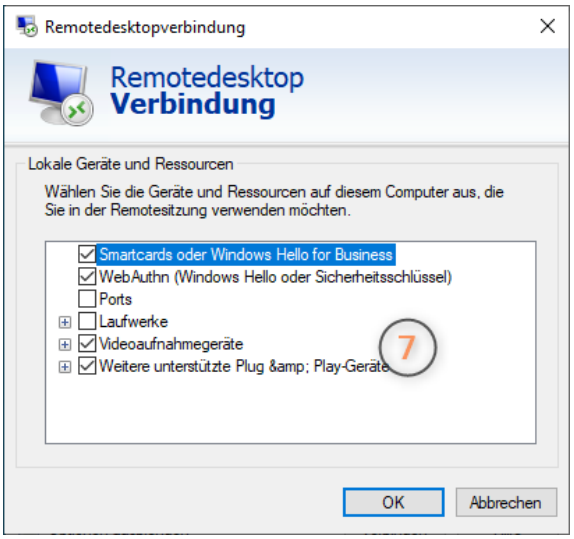
Einstellungen:

Hier wird eingestellt, dass sowohl die **Audiowiedergabe** (5) als auch die **Aufzeichnung** (6) vom PC auf dem Terminalserver übernommen wird



Weitere:

Hier wird eingestellt, dass auch die **Webcam** auf dem Terminalserver zur Verfügung steht



Mit **OK** schließen und mit **Verbinden** wir gewohnt Anmelden

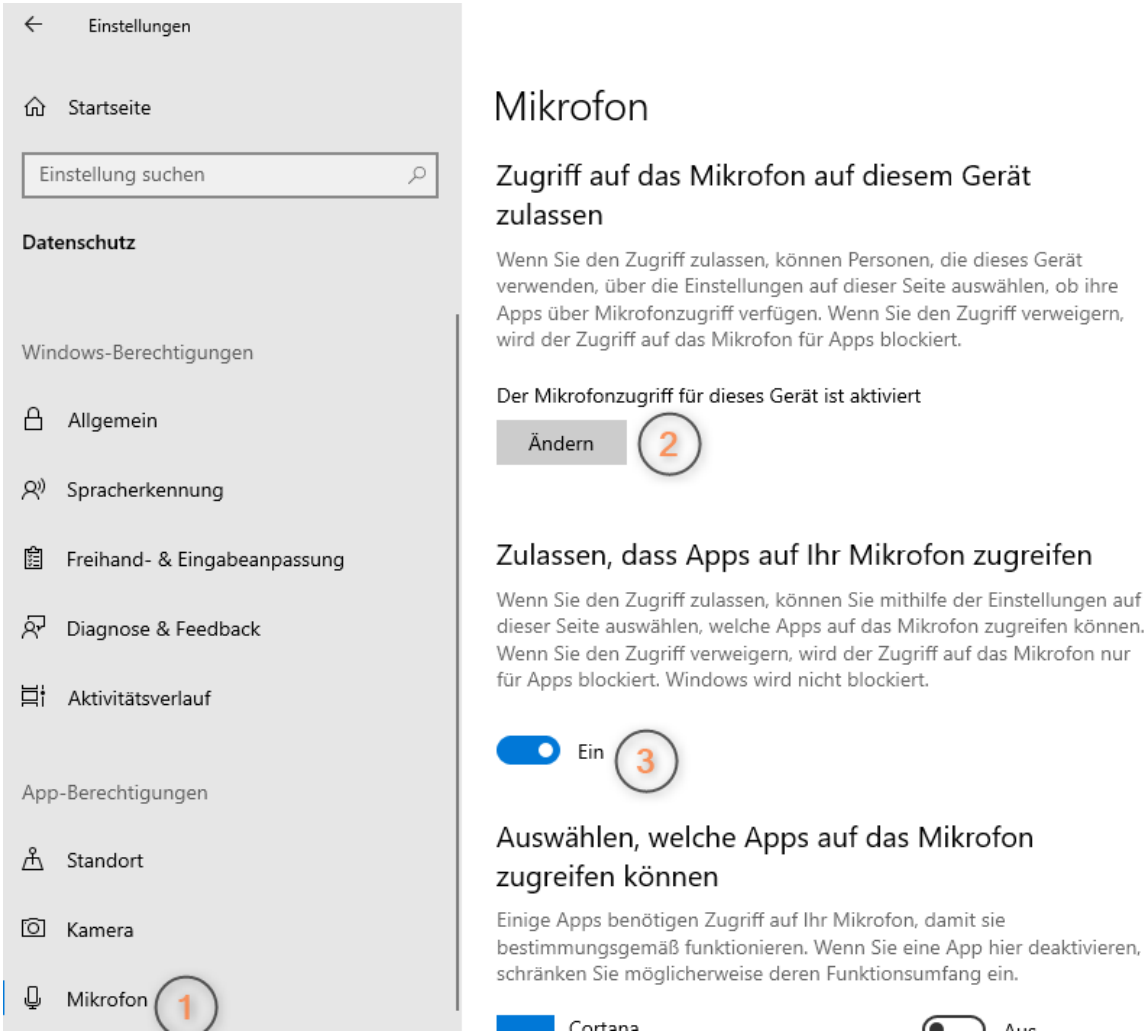
2.) Konfiguration auf dem Terminalserver

Mit **Linksklick** auf das **Windowslogo** und im Anschluß auf das **Zahnrad** die **Einstellungen** von Windows auf dem Terminalserver öffnen



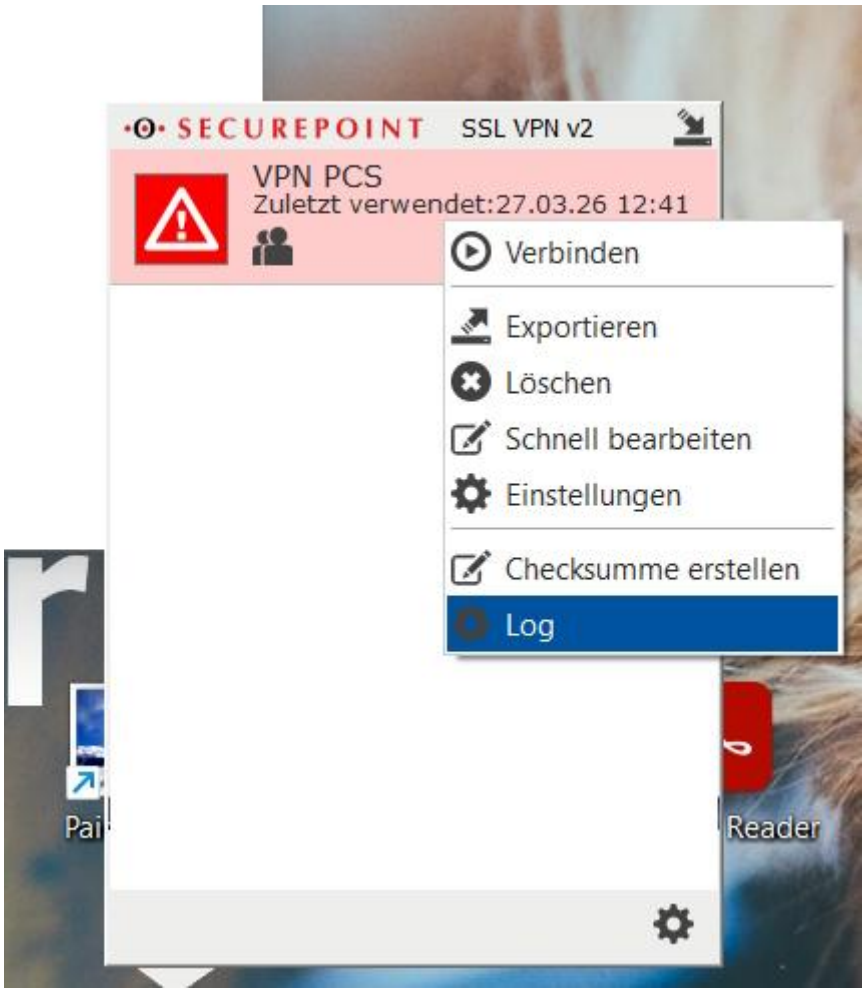
Dort anklicken

Einstellungen für **Mikrofon** (1) anklicken und dann (2) **Kontrolle**: Der Mikrofonzugriff für dieses Gerät ist aktiviert und Ein (3)



Die Datenschutzeinstellungen können für **Kamera** ebenso eingestellt werden

Fehlermeldungen (Logs) vom Securepoint SSL-VPN Client anzeigen und abspeichern

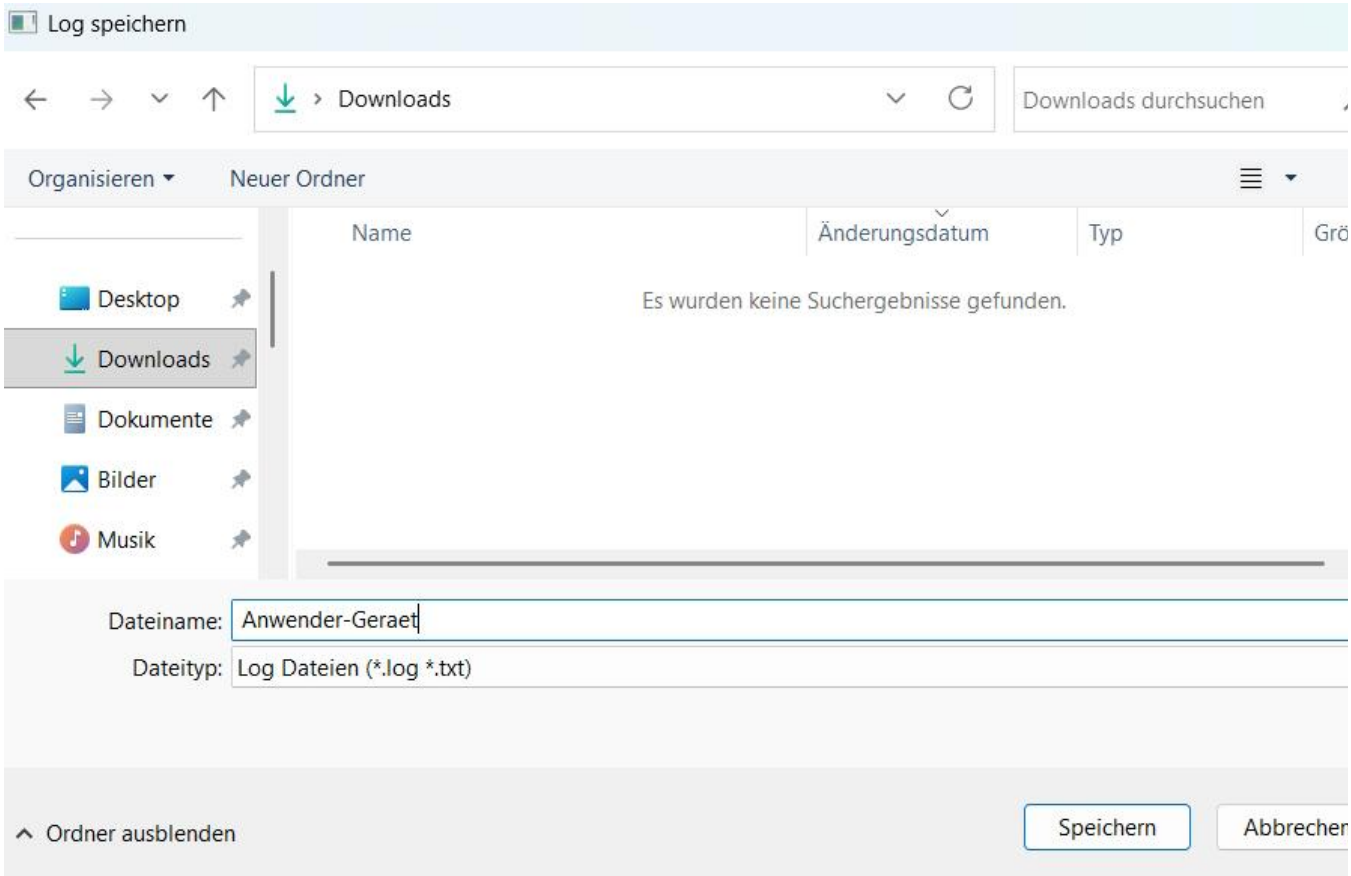
- Klicken Sie mit der rechten Maustaste auf die VPN-Verbindung und wählen Sie dort **Log** aus
- 

- Nun öffnet sich ein Fenster mit dem Log mit einer **Speichern** Option

- SECUREPOINT SSL VPN v2

```
2026-03-27 12:52:53 SIGUSR1[soft,tls-error] received, process restarting
2026-03-27 12:52:53 Restart pause, 1 second(s)
2026-03-27 12:52:54 TCP/UDP: Preserving recently used remote address: [AF_INET]
2026-03-27 12:52:54 Socket Buffers: R=[65536->65536] S=[65536->65536]
2026-03-27 12:52:54 UDPv4 link local: (not bound)
2026-03-27 12:52:54 UDPv4 link remote: [AF_INET]
ERROR: TLS error! See log for details
2026-03-27 12:53:54 TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network
connectivity)
2026-03-27 12:53:54 TLS Error: TLS handshake failed
2026-03-27 12:53:54 SIGUSR1[soft,tls-error] received, process restarting
2026-03-27 12:53:54 Restart pause, 1 second(s)
2026-03-27 12:53:55 TCP/UDP: Preserving recently used remote address: [AF_INET]
2026-03-27 12:53:55 Socket Buffers: R=[65536->65536] S=[65536->65536]
2026-03-27 12:53:55 UDPv4 link local: (not bound)
2026-03-27 12:53:55 UDPv4 link remote: [AF_INET]
ERROR: TLS error! See log for details
2026-03-27 12:54:55 TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network
connectivity)
2026-03-27 12:54:55 TLS Error: TLS handshake failed
Disconnected
```

Log stoppen Log löschen Speichern Schließe

- Suchen Sie nun einen Speicherort aus und speichern Sie das Log mit den Namen von Ihnen und dem Gerät ab
- 

Wireguard Verbindung ohne Adminrechte konfigurieren

Wireguard als Admin installieren und auch als Admin die *.conf Datei importieren

Dann jeweils in der (Admin)Powershell folgende Befehle eingeben:

```
reg add HKLM\SOFTWARE\WireGuard /v LimitedOperatorUI /t REG_DWORD /d 1 /f
```

```
net localgroup "Netzwerkkonfigurations-Operatoren" "BENUTZERNAME" /add
```

Hier natürlich den richtigen Benutzer statt BENUTZERNAME eintragen.

Dann am Besten den Rechner neustarten.

Wichtiger Hinweis: Der Benutzer kann die Verbindung nur aufbauen und trennen. Er darf keine neuen Verbindung anlegen und auch keine Verbindung löschen.