RDP - VDI Themen

Unter Windows 10 ist der Remotedesktop auf eine Verbindung beschränkt.
Man kann dieses auch aufbohren.

- RDP - Enable multiple connections - Patch der termserv.dll
- Ausschalten Button im Startmenü für einen Benutzer deaktibvieren
- RDP - Meldung was verbunden werden soll, bei selbstsigniertem Zertifikat.
- Windows Remotedesktop/Terminalserver Unbekannte Remotedesktop Warnung

RDP - Enable multiple connections - Patch der termserv.dll

Beschreibung:

Unter Windows 10 ist der Remotedesktop auf eine Verbindung beschränkt.
Man kann dieses auch aufbohren.

Methode 1, manual:

Um die Beschränkung für die Anzahl der gleichzeitigen RDP-Benutzerverbindungen in Windows 10 ohne Verwendung von RdpWrapper aufzuheben, können Sie die Original-termsrv.dll-Datei ersetzen. Dies ist die Hauptbibliotheksdatei, die vom Remote-Desktop-Dienst verwendet wird. Die Datei befindet sich im Verzeichnis C:\Windows\System32.

Bevor Sie die termsrv.dll-Datei bearbeiten oder ersetzen, ist es ratsam, eine Sicherungskopie zu erstellen. Dies hilft Ihnen, zur Originalversion der Datei zurückzukehren, wenn dies erforderlich ist. Öffnen Sie die erhöhte Eingabeaufforderung und führen Sie den Befehl aus in einer PowerShell aus:

```
copy c:\Windows\System32\termsrv.dll termsrv.dll_backup
```

Dann müssen Sie Eigentümer der Datei werden. Ändern Sie den Eigentümer einer Datei von TrustedInstaller auf die lokale Administratorengruppe mit dem Befehl:

```
takeown /F c:\Windows\System32\termsrv.dll /A
```

Ausgabe:

```
SUCCESS: The file (or folder): c:\Windows\System32\termsrv.dll now owned by the administrators group
```

Gewähren Sie nun der lokalen Administratorengruppe Vollzugriffsrechte auf die termsrv.dll-Datei mit Hilfe von icacls.exe:

```
icacls c:\Windows\System32\termsrv.dll /grant Administrators:F
```

Ausgabe:

```
processed file: c:\Windows\System32\termsrv.dll Successfully processed 1 files; Failed processing 0 files.
```

Danach stoppen Sie den Remote-Desktop-Dienst (TermService) über die Konsole services.msc oder über die Eingabeaufforderung mit dem Befehl:

```
net stop TermService
```

Bevor Sie fortfahren, müssen Sie Ihre Version (Build-Nummer) von Windows 10 herausfinden. Öffnen Sie die PowerShell-Konsole und führen Sie den Befehl in einer Powershell aus:

```
Get-ComputerInfo | select WindowsProductName, WindowsVersion
```

In meinem Fall ist Windows 10 Build 21H1 installiert.

Öffnen Sie dann die termsrv.dll-Datei mit einem HEX-Editor (zum Beispiel Tiny Hexer). installationsdatei im Anhang , läuft auch unter Linux mit Wine.

Abhängig von Ihrer Windows-Build-Version müssen Sie den String gemäß der Tabelle unten finden und ersetzen.

Windows build	**Find the string**	**Replace with**
Windows 11 RTM (21H2 – 22000.258)	39 81 3C 06 00 00 0F 84 4F 68 01 00	B8 00 01 00 00 89 81 38 06 00 00 90
Windows 10 x64 21H2	39 81 3C 06 00 00 0F 84 DB 61 01 00	
Windows 10 x64 21H1	39 81 3C 06 00 00 0F 84 2B 5F 01 00	
Windows 10 x64 20H2	39 81 3C 06 00 00 0F 84 21 68 01 00	
Windows 10 x64 2004	39 81 3C 06 00 00 0F 84 D9 51 01 00	
Windows 10 x64 1909	39 81 3C 06 00 00 0F 84 5D 61 01 00	
Windows 10 x64 1903	39 81 3C 06 00 00 0F 84 5D 61 01 00	
Windows 10 x64 1809	39 81 3C 06 00 00 0F 84 3B 2B 01 00	
Windows 10 x64 1803	8B 99 3C 06 00 00 8B B9 38 06 00 00	
Windows 10 x64 1709	39 81 3C 06 00 00 0F 84 B1 7D 02 00	

Achtung!!
Der Tiny Hexer-Editor kann die termsvr.dll-Datei nicht direkt aus dem System32-Ordner bearbeiten. Kopieren Sie sie auf Ihren Desktop und ersetzen Sie die Originaldatei nach der Änderung!!!

Zum Beispiel ist meine Version von Windows 10 x64 Build 21H1 (19043.1320) mit der Version der termsrv.dll-Datei 10.0.19041.1320. Öffnen Sie die termsrv.dll-Datei in Tiny Hexer und suchen Sie den Text:

```
39 81 3C 06 00 00 0F 84 2B 5F 01 00
```

und ersetzen diese durch

```
B8 00 01 00 00 89 81 38 06 00 00 90
```

Speichern Sie die Datei und starten Sie den TermService mit dem Command

```
net stop TermService
```

Wenn etwas schief geht und Sie Probleme mit dem Remote-Desktop-Dienst haben, stoppen Sie den Dienst und ersetzen Sie die modifizierte termsrv.dll-Datei durch die Originalversion über den copy Befehl.

```
copy termsrv.dll_backup c:\Windows\System32\termsrv.dll
```

Methode 2, manual über PowerShell komfortabler:

> **Hinweis:** Das Script nicht in einer Terminalsitzung aufrufen, sondern direkt am PC, ist es eine VM dann über die Console, ansonsten habt Ihr ein defektes System!!

Um die termsrv.dll-Datei nicht manuell mit einem HEX-Editor zu ändern, können Sie das folgende PowerShell-Skript verwenden, um den Patch automatisch anzuwenden. Dieses Skript basiert auf der Windows PowerShell-Version und funktioniert nicht auf der modernen PowerShell Core. Das Skript ist universell und kann verwendet werden, um die termsrv.dll-Datei in allen Ausgaben von Windows 10 (1809+) und Windows 11 zu patchen.

Hier der Code, das script stammt von :

https://github.com/maxbakhub/winposh/blob/main/termsrv_rdp_patch.ps1

PowerShellScript

```
# PowerShell script used to patch termsrv.dll file and allow multiple RDP connections on
Windows 10 (1809 and never) and Windows 11
# Details here http://woshub.com/how-to-allow-multiple-rdp-sessions-in-windows-10/


# Stop RDP service, make a backup of the termsrv.dllfile and change the permissions
Stop-Service UmRdpService -Force
Stop-Service TermService -Force
$termsrv_dll_acl = Get-Acl c:\windows\system32\termsrv.dll
Copy-Item c:\windows\system32\termsrv.dll c:\windows\system32\termsrv.dll.copy
takeown /f c:\windows\system32\termsrv.dll
$new_termsrv_dll_owner = (Get-Acl c:\windows\system32\termsrv.dll).owner
cmd /c "icacls c:\windows\system32\termsrv.dll /Grant $($new_termsrv_dll_owner):F /C"
# search for a pattern in termsrv.dll file
$dll_as_bytes = Get-Content c:\windows\system32\termsrv.dll -Raw -Encoding byte
$dll_as_text = $dll_as_bytes.forEach('ToString', 'X2') -join ' '
$patternregex = ([regex]'39 81 3C 06 00 00(\s\S\S){6}')
$patch = 'B8 00 01 00 00 89 81 38 06 00 00 90'
$checkPattern=Select-String -Pattern $patternregex -InputObject $dll_as_text
If ($checkPattern -ne $null) {
   $dll_as_text_replaced = $dll_as_text -replace $patternregex, $patch
}
Elseif (Select-String -Pattern $patch -InputObject $dll_as_text) {
   Write-Output 'The termsrv.dll file is already patched, exiting'
   Exit
}
else {
   Write-Output "Pattern not found "
}
# patching termsrv.dll
[byte[]] $dll_as_bytes_replaced = -split $dll_as_text_replaced -replace '^', '0x'
Set-Content c:\windows\system32\termsrv.dll.patched -Encoding Byte -Value
$dll_as_bytes_replaced
# comparing two files
fc.exe /b c:\windows\system32\termsrv.dll.patched c:\windows\system32\termsrv.dll
# replacing the original termsrv.dll file
Copy-Item c:\windows\system32\termsrv.dll.patched c:\windows\system32\termsrv.dll -Force
Set-Acl c:\windows\system32\termsrv.dll $termsrv_dll_acl
Start-Service UmRdpService
Start-Service TermService
```

Oder im Anhang als Download. Diese Datei zum beispiel auf den Desktop speichern

Nun eine Powershell als Admin öffnen.
Ändern Sie die PowerShell-Ausführungsrichtlinieneinstellungen für die aktuelle Sitzung:

```
Set-ExecutionPolicy Bypass -Scope Process -Force
```

Nun das Script ausführen

```
C:\users\<benutzername>\desktop\rdp_patch.ps1
```

Das Skript kann nach der Installation von Windows-Updates ausgeführt werden, um sofort Änderungen an der termsrv.dll-Datei vorzunehmen (Sie müssen die termsrv.dll-Datei nicht nach jeder Update-Installation im HEX-Editor ändern).

Der Vorteil der Methode, mehrere RDP-Sitzungen in Windows 10 oder 11 zu aktivieren, indem die termsrv.dll-Datei ersetzt wird, besteht darin, dass Antivirenprogramme nicht darauf reagieren (im Gegensatz zu RDPWrap, das von vielen Antivirenprogrammen als Malware/HackTool/Trojaner erkannt wird).

Der Hauptnachteil besteht darin, dass Sie die termsrv.dll-Datei jedes Mal manuell bearbeiten müssen, wenn Sie das Windows 10-Build aktualisieren (oder wenn Sie die Version der termsrv.dll-Datei während der Installation monatlicher kumulativer Updates aktualisieren). Und wenn Sie RDPWrapper verwenden, müssen Sie auch die rdpwrap.ini-Datei nach der Installation von Windows-Updates aktualisieren.

In diesem Artikel haben wir uns angesehen, wie Sie die Beschränkung für die Anzahl gleichzeitiger RDP-Benutzerverbindungen entfernen und einen kostenlosen Terminalserver auf Desktop-Versionen von Windows ausführen können.

Ausschalten Button im Startmenü für einen Benutzer deaktibvieren

Beschreibung:

Die VDI ist ja ein normaler Windows 10/11 Pro Rechner der per Remotedesktop bedient wird.
Leider kommt es öfter vor, macht der Gewohnheit das der Computer (VDI) dann über Herunterfahren ausgeschaltet wird.
Einschalten für den Benutzer nicht möglich.

Hier ein REG KEY , der bei dem Benutzer ausgeführt werden muss, bei dem das Menu auch deaktiviert werden soll.
Hat zum Beispiel noch einen weiteren Admin Benutzer, bleibt der davon unberührt.
Der KEY muss bei den Benutzer ausgeführt werden, der den Startrmenüeintrag herunterfahren NICHT haben soll.

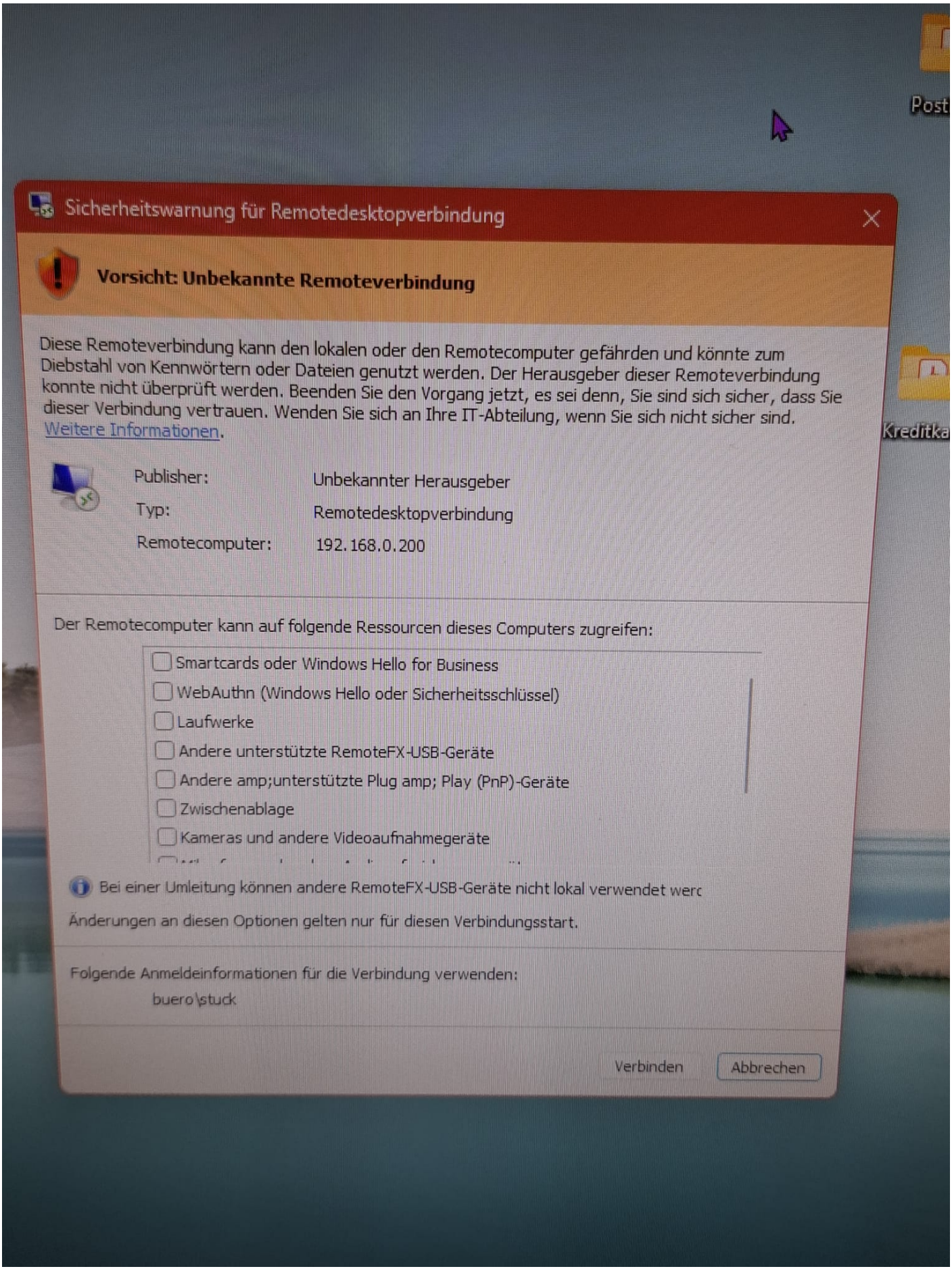
Hier der KEY: deactivate_shutdown_entry_start_menu_for_current_user.reg

Danach den Benutzer abmelden/ wieder anmelden.
Der Eintrag ist weg ;-)

RDP - Meldung was verbunden werden soll, bei selbstsigniertem Zertifikat.

Beschreibung:

Seid einem Windows update muss man jedes mal bestätigen, was alles in die Remotesitzung durchgeschleift werden soll.
Dies kann man ünterdrücken.


Sicherheitswarnung für Remotedesktopverbindung
Vorsicht: Unbekannte Remoteverbindung
Diese Remoteverbindung kann den lokalen oder den Remotecomputer gefährden und könnte zum Diebstahl von Kennwörtern oder Dateien genutzt werden. Der Herausgeber dieser Remoteverbindung konnte nicht überprüft werden. Beenden Sie den Vorgang jetzt, es sei denn, Sie sind sich sicher, dass Sie dieser Verbindung vertrauen. Wenden Sie sich an Ihre IT-Abteilung, wenn Sie sich nicht sicher sind.
Weitere Informationen.
Publisher: Unbekannter Herausgeber
Typ: Remotedesktopverbindung
Remotecomputer: 192.168.0.200
Der Remotecomputer kann auf folgende Ressourcen dieses Computers zugreifen:
Smartcards oder Windows Hello for Business
WebAuthn (Windows Hello oder Sicherheitsschlüssel)
Laufwerke
Andere unterstützte RemoteFX-USB-Geräte
Andere amp;unterstützte Plug amp; Play (PnP)-Geräte
Zwischenablage
Kameras und andere Videoaufnahmegeräte
Bei einer Umleitung können andere RemoteFX-USB-Geräte nicht lokal verwendet werc
Änderungen an diesen Optionen gelten nur für diesen Verbindungsstart.
Folgende Anmeldeinformationen für die Verbindung verwenden:
buero\stuck
Verbinden
Abbrechen

Lösung:

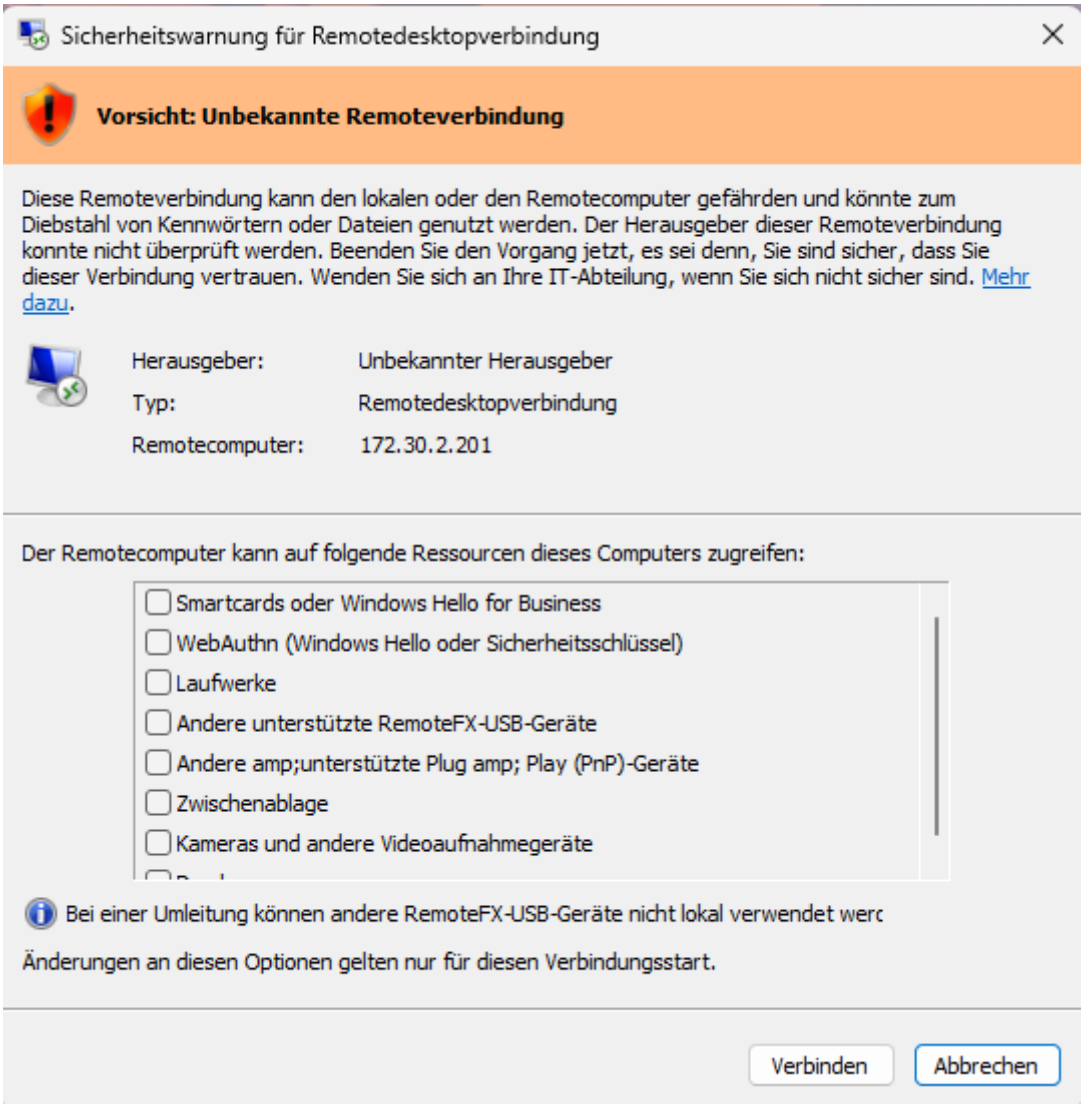
Die rdp Datei. mit nem Texteditor bearbeiten und folgende Zeile hinzufügen.
rechtklick drauf -> öffnen mit -> editor öffnen
Zeile am ende Einfügen.

```
authentication level:i:0
```

Fertig.

Windows Remotedesktop/Terminalserver Unbekannte Remotedesktop Warnung

Beschreibung:



Lösung:

Methode 1: Registry-Anpassung (Einfachste Lösung für lokale PCs)

Diese Methode schaltet die Warnmeldung systemweit ab, ignoriert aber bei zukünftigen Verbindungen den Warnhinweis.

1. Drücken Sie `Win + R`, geben Sie `regedit` ein und bestätigen Sie mit Enter.
2. Navigieren Sie zu diesem Pfad: `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Terminal Services\Client`
3. Klicken Sie mit der rechten Maustaste in den rechten Bereich und erstellen Sie einen **Neuen DWORD-Wert (32-Bit)**.
4. Benennen Sie diesen exakt: `RedirectionWarningDialogVersion`
5. Doppelklicken Sie auf den neuen Wert und setzen Sie die **Basis auf Hexadezimal** sowie den **Wert auf 1**.
6. Starten Sie Ihren PC neu, um die Änderungen zu übernehmen.

Oder RedirectionWarningDialogVersion.reg REG Datei importieren, das selbe in Grün.