HowTo – Remotedesktop-Konfiguration

Kategorie	Windows Administration
Autor	Lugstein Markus
Datum	
Version	1.0

Inhalt

1. Ziel der Anleitung

> Ziel dieser Anleitung ist es, den Remote Desktop (RDP) auf einem Windows-System zu aktivieren, den Zugriff auf einen bestimmten Benutzer zu beschränken, den Standard-Port von 3389 auf 3390 zu ändern, eine passende Firewall-Regel zu erstellen und die Verbindung anschließend erfolgreich zu testen.
>
> Zusätzlich wird gezeigt, wie die Konfiguration teilweise oder vollständig mit PowerShell durchgeführt werden kann.

2. Voraussetzungen

- Windows-System mit lokalen Administratorrechten
- Zugriff auf die Systemeinstellungen, die Windows-Registrierung und PowerShell
- Benutzerkonto „admin.huber“ ist bereits vorhanden
- Zugriff auf die Windows Defender Firewall mit erweiterter Sicherheit
- PowerShell als Administrator ausführbar
- Remotedesktopverbindung (mstsc) für den Verbindungstest verfügbar

3. Warnhinweise

⚠️ Änderungen an der Windows-Registrierung können bei falscher Durchführung zu Systemfehlern führen.

⚠️ Vor Änderungen am RDP-Port sollte idealerweise ein Wiederherstellungspunkt oder ein Backup erstellt werden.

⚠️ Wird der neue Port nicht korrekt in der Firewall freigegeben, ist keine Verbindung mehr möglich.

⚠️ PowerShell-Befehle müssen mit Administratorrechten ausgeführt werden.

⚠️ Der Zugriff sollte nur autorisierten Benutzern erlaubt werden.

4. Übersicht der Aufgabe

Im Rahmen dieser Aufgabe sind folgende Arbeitsschritte durchzuführen:

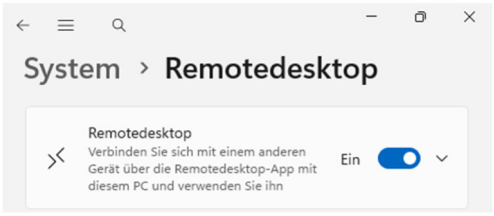
- Remote Desktop auf dem System aktivieren
- RDP nur für den Benutzer „admin.huber“ konfigurieren
- Den Standard-RDP-Port von 3389 auf 3390 ändern
- Eine Firewall-Regel für den neuen Port erstellen

- Die Verbindung mit der Remote Desktop Connection testen
- Die Konfiguration zusätzlich per PowerShell nachvollziehen bzw. ausführen

5. Schritt-für-Schritt Anleitung

5.1 Schritt 1 – Remote Desktop aktivieren

Variante über die grafische Oberfläche



1. Öffnen Sie die Windows-Einstellungen (System).
2. Navigieren Sie zu System → Remotedesktop.
3. Aktivieren Sie die Option Remotedesktop aktivieren.
4. Bestätigen Sie die Sicherheitsabfrage.

Variante über PowerShell:

1. Öffnen Sie PowerShell als Administrator.
2. Führen Sie folgenden Befehl aus:

```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -Name "fDenyTSConnections" -Value 0
```

3. Aktivieren Sie zusätzlich die zugehörigen Firewall-Regeln für Remotedesktop:

```
Enable-NetFirewallRule -DisplayGroup "Remotedesktop"
```

Ergebnis:

Remote Desktop ist auf dem System aktiviert.

5.2 Schritt 2 – Benutzer für RDP berechtigen

Variante über die grafische Oberfläche:

1. Bleiben Sie im Bereich Remotedesktop.
2. Klicken Sie auf Benutzer auswählen, die remote auf diesen PC zugreifen können.
3. Fügen Sie den Benutzer admin.huber hinzu.
4. Entfernen Sie gegebenenfalls nicht benötigte Benutzer aus der Liste.

Variante über PowerShell:

1. Öffnen Sie PowerShell als Administrator.
2. Fügen Sie den Benutzer zur lokalen Gruppe Remotedesktopbenutzer hinzu:

```
Add-LocalGroupMember -Group "Remotedesktopbenutzer" -Member "admin.huber"
```

Hinweis:

Auf englischsprachigen Systemen kann die Gruppe "Remote Desktop Users" heißen.

Optionaler Prüfbefehl:

```
Get-LocalGroupMember -Group "Remotedesktopbenutzer"
```

Ergebnis:

Der Benutzer admin.huber ist für den Remotedesktopzugriff berechtigt.

5.3 Schritt 3 – Standard-RDP-Port in der Registry ändern

Variante über die grafische Oberfläche:

1. Öffnen Sie den Registrierungs-Editor mit regedit.
2. Navigieren Sie zu folgendem Pfad:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

3. Öffnen Sie den Eintrag **PortNumber**.
4. Stellen Sie die Anzeige auf **Dezimal** um.
5. Ändern Sie den Wert von **3389** auf **3390**.
6. Speichern Sie die Änderung.

Variante über PowerShell:

1. Öffnen Sie PowerShell als Administrator.
2. Setzen Sie den neuen Port mit folgendem Befehl:

```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -Name "PortNumber" -Value 3390
```

Optionaler Prüfbefehl:

```
Get-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -Name "PortNumber"
```

Ergebnis:

Der RDP-Dienst ist auf den neuen Port **3390** umgestellt.

5.4 Schritt 4 – Firewall-Regel für Port 3390 erstellen

Variante über die grafische Oberfläche:

1. Öffnen Sie die **Windows Defender Firewall mit erweiterter Sicherheit**.
2. Wählen Sie **Eingehende Regeln → Neue Regel**.
3. Wählen Sie **Port** aus.
4. Markieren Sie **TCP** und tragen Sie **3390** ein.

5. Wählen Sie **Verbindung zulassen**.
6. Aktivieren Sie die gewünschten Profile, z. B. **Domäne, Privat** und bei Bedarf **Öffentlich**.
7. Vergeben Sie einen Namen, z. B. **RDP Port 3390**.

Variante über PowerShell:

1. Öffnen Sie PowerShell als Administrator.
2. Erstellen Sie die Firewall-Regel mit folgendem Befehl:

```
New-NetFirewallRule -DisplayName "RDP Port 3390" -Direction Inbound -Protocol TCP -LocalPort 3390 -Action Allow
```

Optionaler Prüfbefehl:

```
Get-NetFirewallRule -DisplayName "RDP Port 3390"
```

Ergebnis:

Die Firewall erlaubt eingehende Verbindungen über den Port **3390**.

5.5 Schritt 5 – System bzw. Dienst neu starten

Variante über die grafische Oberfläche:

1. Starten Sie den Computer neu

Variante über PowerShell:

1. Starten Sie das System mit folgendem Befehl neu:

```
Restart-Computer
```

Ergebnis:

Die Änderungen an Port und Freigaben sind aktiv.

5.6 Schritt 6 – Verbindung testen

Variante über GUI:

1. Öffnen Sie die Anwendung Remotedesktopverbindung (mstsc).
2. Geben Sie den Rechnernamen oder die IP-Adresse mit Port an, zum Beispiel:
   PC-NAME:3390
   oder
   192.168.1.10:3390
3. Starten Sie die Verbindung.
4. Melden Sie sich mit dem Benutzer, z.B. **admin.huber** an.

Variante über PowerShell:

1. Starten Sie die Remotdesktopverbindung per PowerShell:

```
mstsc
```

2. Testen Sie optional vorher die Port-Erreichbarkeit mit:

```
Test-NetConnection -ComputerName localhost -Port 3390
```

Hinweis:

Für einen Test von einem anderen Gerät muss statt localhost der tatsächliche Rechnername oder die IP-Adresse angegeben werden.

Ergebnis:

Die Verbindung zum Zielsystem wird erfolgreich über den Port 3390 hergestellt.

5.7 Schritt 7 – Gesamtausführung per PowerShell

Die folgenden Befehle können gesammelt in einer PowerShell-Sitzung mit Administratorrechten ausgeführt werden:

```
# Remote Desktop aktivieren
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -Name "fDenyTSConnections" -Value 0

# Standard-Firewallregeln für Remotedesktop aktivieren
Enable-NetFirewallRule -DisplayGroup "Remotedesktop"

# Benutzer für RDP berechtigen
Add-LocalGroupMember -Group "Remotedesktopbenutzer" -Member "admin.huber"

# RDP-Port auf 3390 ändern
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -Name "PortNumber" -Value 3390

# Neue Firewall-Regel für Port 3390 erstellen
New-NetFirewallRule -DisplayName "RDP Port 3390" -Direction Inbound -Protocol TCP -LocalPort 3390 -Action Allow

# Port testen
Test-NetConnection -ComputerName localhost -Port 3390
```

Hinweis:

Nach der Portänderung sollte das System neu gestartet werden:

```
Restart-Computer
```

6. Ergebnis / Kontrolle

Die Aufgabe gilt als erfolgreich abgeschlossen, wenn folgende Punkte geprüft wurden:

- Remote Desktop ist aktiviert
- Der Benutzer **admin.huber** ist für den Zugriff berechtigt
- Der Registry-Wert **PortNumber** wurde auf **3390** gesetzt
- Die Firewall-Regel für **TCP-Port 3390** ist vorhanden
- Die Anmeldung per **Remotedesktopverbindung** funktioniert erfolgreich

7. Dokumentation / Abgabe

Für die Abgabe sollen folgende Nachweise erstellt werden:

- Screenshot der aktivierten **Remotedesktop-Einstellungen**
- Screenshot der Benutzerberechtigung mit admin.huber
- Screenshot der Registry-Änderung des Eintrags **PortNumber = 3390**
- Screenshot der erstellten **Firewall-Regel**
- Screenshot oder kurzer Nachweis des erfolgreichen Verbindungstests
- Optional: Screenshot oder Kopie der verwendeten **PowerShell-Befehle**

8. Anhang (optional)

Optional können zusätzlich folgende Informationen ergänzt werden:

- Verwendeter Computername oder IP-Adresse
- Datum und Uhrzeit des Tests
- Hinweise zu Problemen und deren Lösung
- Liste der verwendeten PowerShell-Befehle
- Zusätzliche Sicherheitsmaßnahmen, z. B. Einschränkung auf bestimmte Netzwerke

Firewall ausschalten

```
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False
```