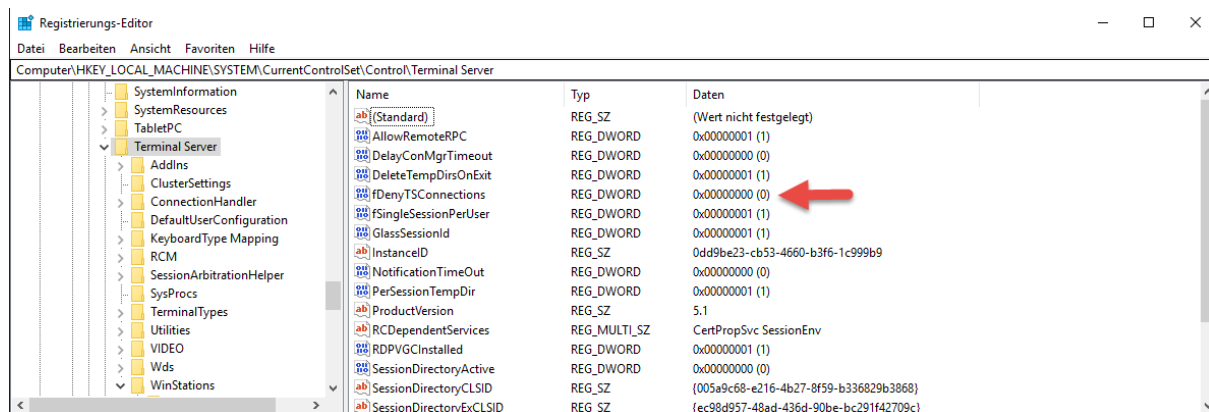




Sicherheitsempfehlung beim Einsatz von RDP

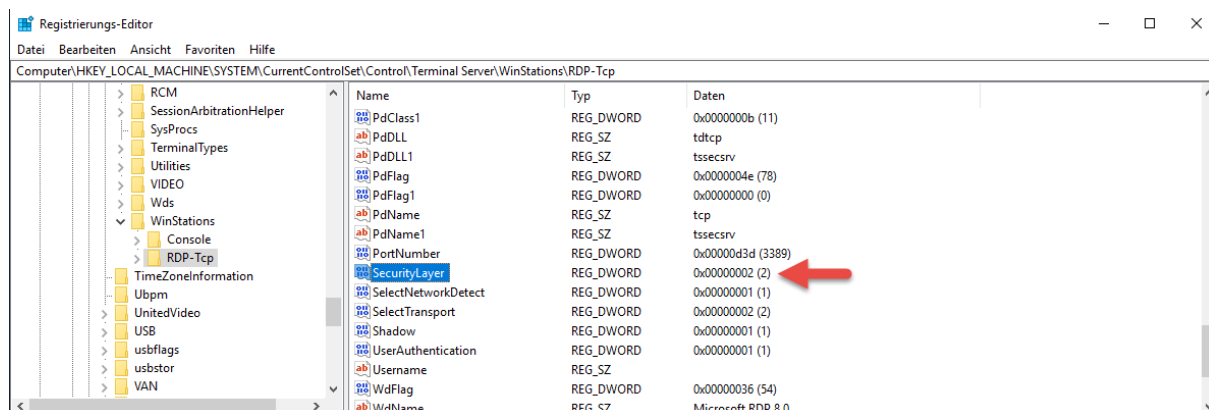
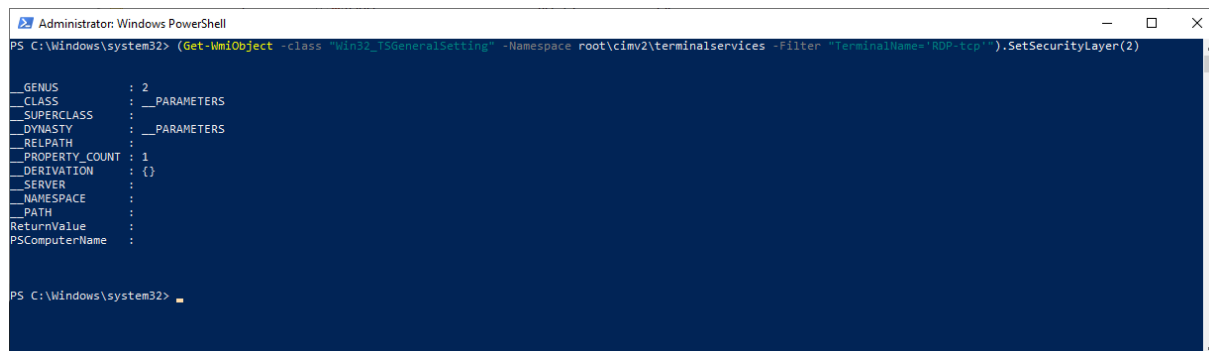
Zuerst aktivieren wir Remote Desktop.

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



Dann stellen wir den Security Layer auf TLS ein:

(Get-WmiObject -class "Win32_TSGeneralSetting" -Namespace root\cimv2\terminalservices -Filter "TerminalName='RDP-tcp']").SetSecurityLayer(2)



Erklärung zu den möglichen Parametern:

SecurityLayer = 0 - Bei einer niedrigen Sicherheitsstufe wird das genutzt was der Client anzubieten hat.

SecurityLayer = 1 - Bei einer mittleren Sicherheitsstufe verhandeln Server und Client die Authentifizierungsmethode aus, bevor eine Remotedesktopverbindung hergestellt wird.

SecurityLayer = 2 - Mit der hohen Sicherheitsstufe wird TLS erzwungen!



Sicherheitsempfehlung beim Einsatz von RDP

Dann setzen wir den Client Connection Encryption Level auf HIGH-Level. Jetzt wird vorausgesetzt das mindestens 128 Bit eingesetzt wird. Es folgt nun mehr keine Aushandlung der Verschlüsselungsstufe zwischen Client und Server. Kann ein Partner nicht mindestens 128 Bit anbieten, wird der Verbindungsversuch sofort beendet.

```
(Get-WmiObject -class "Win32_TSGeneralSetting" -Namespace root\cimv2\terminalservices -Filter "TerminalName='RDP-tcp']").SetEncryptionLevel(3)
```

```
Administrator: Windows PowerShell
PS C:\Windows\system32> (Get-WmiObject -class "Win32_TSGeneralSetting" -Namespace root\cimv2\terminalservices -Filter "TerminalName='RDP-tcp']").SetEncryptionLevel(3)
__GENUS          : 2
__CLASS          : __PARAMETERS
__SUPERCLASS    : 
__DYNASTY       : __PARAMETERS
__RELPATH       : 
__PROPERTY_COUNT : 1
__DERIVATION    : {}
__SERVER        : 
__NAMESPACE     : 
__PATH          : 
Return_Value    : 
PSComputerName  :
```

Name	Typ	Daten
KeyboardLayout	REG_DWORD	0x00000000 (0)
LanAdapter	REG_DWORD	0x00000000 (0)
LoadableProtocol_Object	REG_SZ	{5828227c-20cf-4408-b73f-73ab70b8849f}
MaxConnectionTime	REG_DWORD	0x00000000 (0)
MaxDisconnectionTime	REG_DWORD	0x00000000 (0)
MaxIdleTime	REG_DWORD	0x00000000 (0)
MaxInstanceCount	REG_DWORD	0xffffffff (4294967295)
MinEncryptionLevel	REG_DWORD	0x00000003 (3)
NWLogonServer	REG_SZ	
OutBufCount	REG_DWORD	0x00000006 (6)
OutBufDelay	REG_DWORD	0x00000064 (100)
OutBufLength	REG_DWORD	0x00000212 (530)
Password	REG_SZ	
PdClass	REG_DWORD	0x00000002 (2)
PdClass1	REG_DWORD	0x0000000b (11)
PdDLL	REG_SZ	tdtcp

Erklärung zu den Encryption-Level-Parametern:

Niedrig (1): Alle vom Client an den Server gesendeten Daten sind mindestens mit 56-Bit verschlüsselt. Der Server sendet an den Client aber unverschlüsselt.

Client-kompatibel (2): Alle zwischen dem Client und dem Server gesendeten Daten sind verschlüsselt, basierend auf der vom Client unterstützten maximalen Schlüsselstärke. Ist nur was für sehr alte Umgebungen! Sollte es heute gar nicht mehr geben.

Hoch (3): Alle zwischen dem Client und dem Server gesendeten Daten sind mindestens 128-Bit verschlüsselt.

FIPS (4): Alle zwischen Client und Server gesendeten Daten werden mit validierten Verschlüsselungsmethoden gemäß Federal Information Processing Standard 140-1 geschützt. Hierbei handelt es sich um die höchste Sicherheitsstufe. Diese sollte nur eingesetzt werden, wenn alle Partner kompatibel sind.



Sicherheitsempfehlung beim Einsatz von RDP

Dann aktivieren wir die User Authentication (NLA) für Remote Desktop:

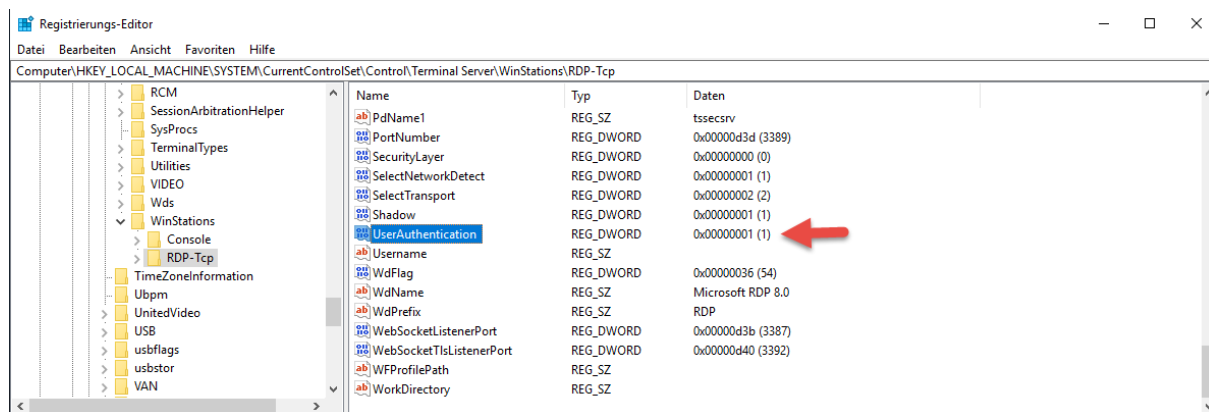
```
(Get-WmiObject -class "Win32_TSGeneralSetting" -Namespace root\cimv2\terminalservices -Filter "TerminalName='RDP-tcp']").SetUserAuthenticationRequired(1)
```

```
Administrator: Windows PowerShell
PS C:\Windows\system32> (Get-WmiObject -class "Win32_TSGeneralSetting" -Namespace root\cimv2\terminalservices -Filter "TerminalName='RDP-tcp']").SetUserAuthenticationRequired(1)

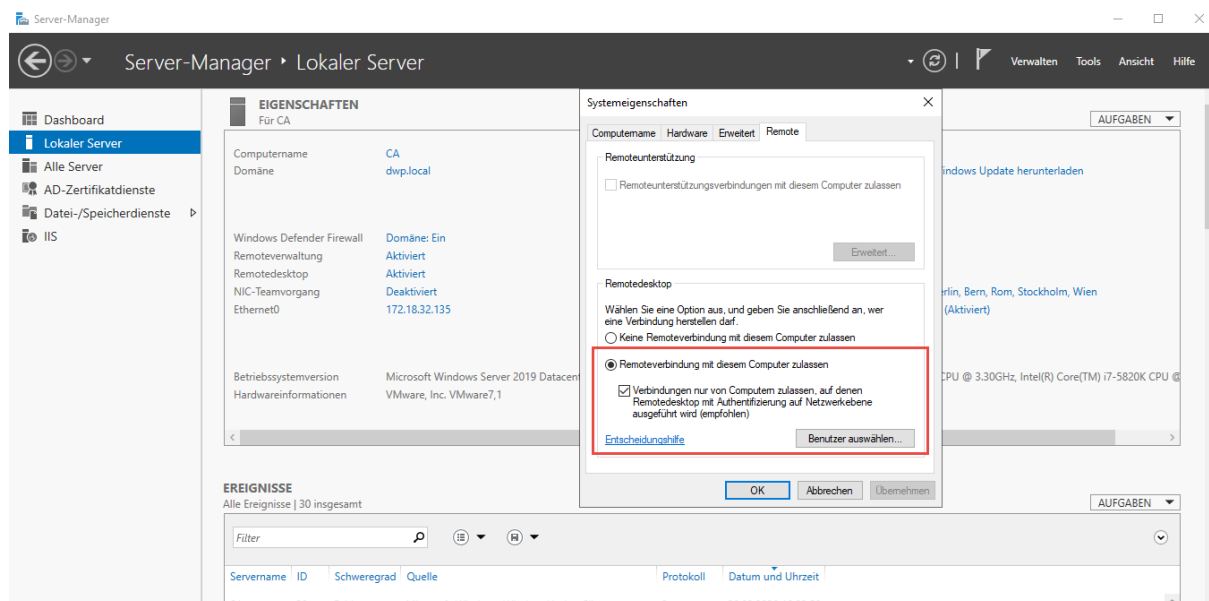
GENUS          : 2
CLASS          : __PARAMETERS
SUPERCLASS     : 
DYNASTY       : __PARAMETERS
RELPATH       : 
PROPERTY_COUNT : 1
DERIVATION    : {}
SERVER        : 
NAMESPACE     : 
PATH          : 
ReturnValue   : 
PSComputerName :

PS C:\Windows\system32>
```

Das bedeutet, dass sich der Benutzer auf Netzwerkebene (Kerberos, NTLM) authentifizieren muss.



Das Ergebnis der empfohlenen Einstellungen sieht dann wie folgt aus:





Sicherheitsempfehlung beim Einsatz von RDP

Dann aktivieren wir die Firewall-Gruppenregeln für Remote Desktop:

Englisches OS:

```
netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes
```

oder

```
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

Deutsches-OS:

```
netsh advfirewall firewall set rule group="RemoteDesktop" new enable=yes
```

```
Administrator: Windows PowerShell
PS C:\Windows\system32> netsh advfirewall firewall set rule group="remotedesktop" new enable=yes
3 Regel(n) wurde(n) aktualisiert.
OK.
PS C:\Windows\system32>
```

Name	Gruppe	Profil	Aktiviert	Aktion	Außer Kraft setzen	Programm	Lokale Adresse	Remoteadresse	Pr...
Registrierungs- und Verwaltungsprotokoll der Zertifizieru...	Zertifizierungsstelle	Alle	Ja	Zulassen	Nein	%systemro...	Beliebig	Beliebig	TC
Registrierungs- und Verwaltungsprotokoll der Zertifizieru...	Zertifizierungsstelle	Alle	Ja	Zulassen	Nein	System	Beliebig	Beliebig	TC
Registrierungs- und Verwaltungsprotokoll der Zertifizieru...	Zertifizierungsstelle	Alle	Ja	Zulassen	Nein	%systemro...	Beliebig	Beliebig	TC
Remotedesktop - (TCP-WSS-in)	Remotedesktop (WebSocket)	Alle	Nein	Zulassen	Nein	System	Beliebig	Beliebig	TC
Remotedesktop - (TCP-WSS-in)	Remotedesktop (WebSocket)	Alle	Nein	Zulassen	Nein	System	Beliebig	Beliebig	TC
Remotedesktop - Benutzermodus (TCP eingehend)	Remotedesktop	Alle	Ja	Zulassen	Nein	%SystemR...	Beliebig	Beliebig	TC
Remotedesktop - Benutzermodus (UDP eingehend)	Remotedesktop	Alle	Ja	Zulassen	Nein	%SystemR...	Beliebig	Beliebig	UD
Remotedesktop - Schatten (TCP eingehend)	Remotedesktop	Alle	Ja	Zulassen	Nein	%SystemR...	Beliebig	Beliebig	TC
Remotedienstverwaltung (NP eingehend)	Remotedienstverwaltung	Alle	Nein	Zulassen	Nein	System	Beliebig	Beliebig	TC
Remotedienstverwaltung (RPC)	Remotedienstverwaltung	Alle	Nein	Zulassen	Nein	%SystemR...	Beliebig	Beliebig	TC
Remotedienstverwaltung (RPC-EPMAP)	Remotedienstverwaltung	Alle	Nein	Zulassen	Nein	%SystemR...	Beliebig	Beliebig	TC
Remote-Ereignisprotokollverwaltung (NP eingehend)	Remote-Ereignisprotokollve...	Alle	Nein	Zulassen	Nein	System	Beliebig	Beliebig	TC
Remote-Ereignisprotokollverwaltung (RPC)	Remote-Ereignisprotokollve...	Alle	Nein	Zulassen	Nein	%SystemR...	Beliebig	Beliebig	TC
Remote-Ereignisprotokollverwaltung (RPC-EPMAP)	Remote-Ereignisprotokollve...	Alle	Nein	Zulassen	Nein	%SystemR...	Beliebig	Beliebig	TC

Firewall-Regeln für RDP gezielt abfragen:

```
Get-NetFirewallRule -Name RemoteDesktop-UserMode-In-TCP
```

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-NetFirewallRule -Name RemoteDesktop-UserMode-In-TCP

Name                : RemoteDesktop-UserMode-In-TCP
DisplayName          : Remotedesktop - Benutzermodus (TCP eingehend)
Description          : Eingehende Regel für den Remotedesktopdienst, die RDP-Datenverkehr zulässt. [TCP 3389]
DisplayGroup        : Remotedesktop
Group                : @FirewallAPI.dll,-28752
Enabled              : False
Profile              : Any
Platform             : {}
Direction            : Inbound
Action               : Allow
EdgeTraversalPolicy  : Block
LooseSourceMapping   : False
LocalOnlyMapping     : False
Owner                :
PrimaryStatus        : OK
Status               : Die Regel wurde erfolgreich vom Speicher aus analysiert. (65536)
EnforcementStatus    : NotApplicable
PolicyStoreSource    : PersistentStore
PolicyStoreSourceType : Local

PS C:\Windows\system32>
```



Sicherheitsempfehlung beim Einsatz von RDP

Die Firewall gezielt für die Domäne aktivieren:

```
Set-NetFirewallRule -Name RemoteDesktop-UserMode-In-TCP -Enabled True -Profile Domain
```

```
Auswählen Administrator: Windows PowerShell
PS C:\Windows\system32> Get-NetFirewallRule -Name RemoteDesktop-UserMode-In-TCP

Name                : RemoteDesktop-UserMode-In-TCP
DisplayName          : Remotedesktop - Benutzermodus (TCP eingehend)
Description         : Eingehende Regel für den Remotedesktopdienst, die RDP-Datenverkehr zulässt. [TCP 3389]
DisplayGroup        : Remotedesktop
Group               : @FirewallAPI.dll,-28752
Enabled             : False
Profile             : Any
Platform            : {}
Direction           : Inbound
Action              : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping  : False
LocalOnlyMapping    : False
Owner               :
PrimaryStatus       : OK
Status              : Die Regel wurde erfolgreich vom Speicher aus analysiert. (65536)
EnforcementStatus   : NotApplicable
PolicyStoreSource   : PersistentStore
PolicyStoreSourceType : Local

PS C:\Windows\system32> Set-NetFirewallRule -Name RemoteDesktop-UserMode-In-TCP -Enabled True -Profile Domain
PS C:\Windows\system32> Get-NetFirewallRule -Name RemoteDesktop-UserMode-In-TCP

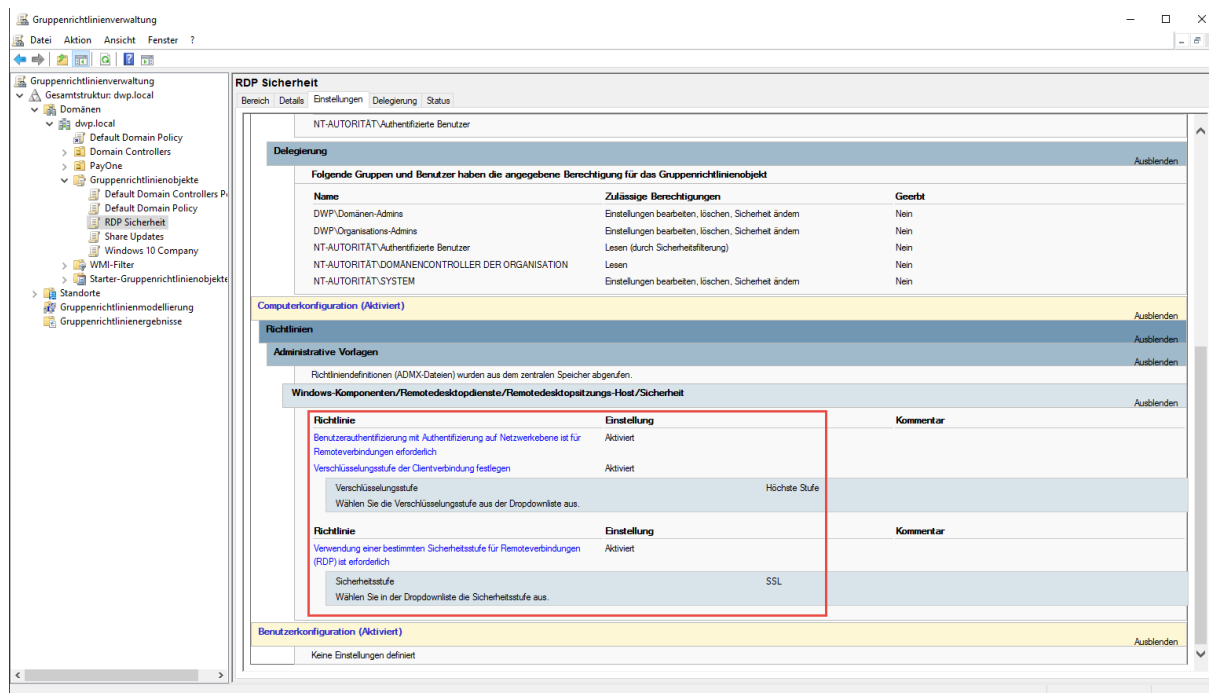
Name                : RemoteDesktop-UserMode-In-TCP
DisplayName          : Remotedesktop - Benutzermodus (TCP eingehend)
Description         : Eingehende Regel für den Remotedesktopdienst, die RDP-Datenverkehr zulässt. [TCP 3389]
DisplayGroup        : Remotedesktop
Group               : @FirewallAPI.dll,-28752
Enabled             : True
Profile             : Domain
Platform            : {}
Direction           : Inbound
Action              : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping  : False
LocalOnlyMapping    : False
Owner               :
PrimaryStatus       : OK
Status              : Die Regel wurde erfolgreich vom Speicher aus analysiert. (65536)
EnforcementStatus   : NotApplicable
PolicyStoreSource   : PersistentStore
PolicyStoreSourceType : Local

PS C:\Windows\system32>
```



Sicherheitsempfehlung beim Einsatz von RDP

Die oben gezeigten Einstellungen spiegeln diese Richtlinie wieder.



Optional

RDP per REG-KEY deaktivieren:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 1 /f
```

RDP per Powershell deaktivieren:

```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server'-name "fDenyTSConnections" -Value 1
```

Abfrage des NLA-Levels (Network Authentication Level):

```
(Get-WmiObject -class "Win32_TSGeneralSetting" -Namespace root\cimv2\terminalservices -Filter "TerminalName='RDP-tcp']").UserAuthenticationRequired
```

Firewall (RDP Gruppe) wieder deaktivieren:

```
Disable-NetFirewallRule -DisplayGroup "RemoteDesktop"
```