

mstsc 與 STK Agent 共存：AutoAdminLogon 動態切換

STK Agent (session_pusher / STK_RDP_Watch) 2026-06-25

一、訴求與現象

從公司用 Microsoft 遠端桌面(mstsc)連客戶 PC(有跑 STK Agent)，客戶才剛開機、查過根本沒人 RDP，一連上卻立刻被踢：「由於已有另一個連線到遠端電腦，您已經中斷連線」。需求：讓 mstsc 進客戶端能正常使用，同時不影響 Agent 自動跑、不影響客戶重開機自動登入，也讓 StkWebScreen 的 RDP 跟隨能用。

二、診斷與根因

診斷心法：裝 Agent「之前」TeamViewer 也能 mstsc、裝「之後」才壞 → 唯一變數是 Agent 安裝。逐一隔離：停 STK_Agent_Boot / STK_Agent_Watchdog、設 ForceAutoLogon=0 → 仍被踢；刪 STK_RDP_Watch + AutoAdminLogon=0 → 通；最後單獨還原 AutoAdminLogon=1 → 又被踢。結論：兇手是 AutoAdminLogon。

項目	結論
STK_Agent_Boot / Watchdog	清白（停用仍被踢）
ForceAutoLogon	清白（設 0 仍被踢；它只在 AutoAdminLogon=1 時才有作用，否則空轉）
STK_RDP_Watch / TeamViewer	清白
AutoAdminLogon=1	★兇手：Windows 用戶端只有一個互動 session，AutoAdminLogon=1 會「console 一空出來就自動把使用者登回 console」；mstsc 接管=console 空出來→被搶回→踢 mstsc

本質衝突：不踢 mstsc 要 AutoAdminLogon=0；但客戶重開機自動登入跑 Agent 又必須 AutoAdminLogon=1。

三、踩坑與陷阱

陷阱	說明
誤判 ForceAutoLogon	一開始把 ForceAutoLogon 壓 0，證實無用——踢不踢的唯一開關是 AutoAdminLogon。
Agent 非 elevated	Agent 在使用者 session 非系統權限，寫不到 HKLM；改 Winlogon 要靠 SYSTEM 身分的 session_pusher。
32-bit + WOW64 重導向	session_pusher 是 32-bit，64-bit Windows 下 subprocess('tscon') 被 WOW64 把 System32 重導向到 SysWOW64（沒有 tscon.exe）→ [WinError 2]。需用 %SystemRoot%\Sysnative\tscon.exe。reg.exe 兩邊都有不受影響。
連入瞬間 race	第一次 mstsc 連上瞬間 AutoAdminLogon 若還是 1 會被踢一次；1 秒內壓 0，重連一次就穩。

四、解決方法（自動切換）

在 session_pusher.py（SYSTEM 身分、由 STK_RDP_Watch 排程每秒跑 --watch）新增 manage_autologon()：

情況	動作
有人 mstsc 連入（RDP-Tcp# session，含握手 Connected/ConnectQuery）	AutoAdminLogon=0 → console 不搶回，mstsc 不被踢
沒人 mstsc	AutoAdminLogon=1 → 客戶重開機自動登入、手機操控正常
mstsc 斷線後 console 非 Active 且有 Disconnected 使用者 session	tscon /dest:console 把桌面拉回 console → Agent/手機操控自動恢復
ForceAutoLogon	不碰（維持 install 值，空轉無害，反讓誤登出也能回桌面）

reg 節流：有 RDP 每秒檢查（搶在被踢前壓 0）、無 RDP 15 秒一次，只在值需變才寫；tscon 每 6 秒重試到 console 回 Active。DefaultUserName/DefaultPassword 不動（沿用 install）。

五、使用技術與用法

技術	用法
WTS session 列舉	session_pusher 每秒列舉 session，依名稱 RDP-Tcp# 與狀態判斷有無 mstsc 連入。

技術	用法
Winlogon 登錄切換	reg add/query AutoAdminLogon，依 RDP 有無動態切 0/1。
tscon 重接 console	mstsc 斷線後把 Disconnected 的使用者 session 用 tscon /dest:console 拉回實體 console。
Sysnative 繞 WOW64	32-bit 行程用 %SystemRoot%\Sysnative\tscon.exe 直達 64-bit System32。
.new 熱抽換部署	丟 session_pusher.exe.new，跑著的 rdp_watch.bat 迴圈自動 swap+重啟。

六、驗證

客戶端實測 (C:\StkRdp\session_pusher.log) 可重複：AutoAdminLogon 1→0 (rdp=True) 連入防踢、tscon 1 /dest:console (rc=0)
斷線拉回、AutoAdminLogon 0→1 重新武裝。注意：AutoAdminLogon=1 要真的自動登入需 DefaultUserName/DefaultPassword 存在。