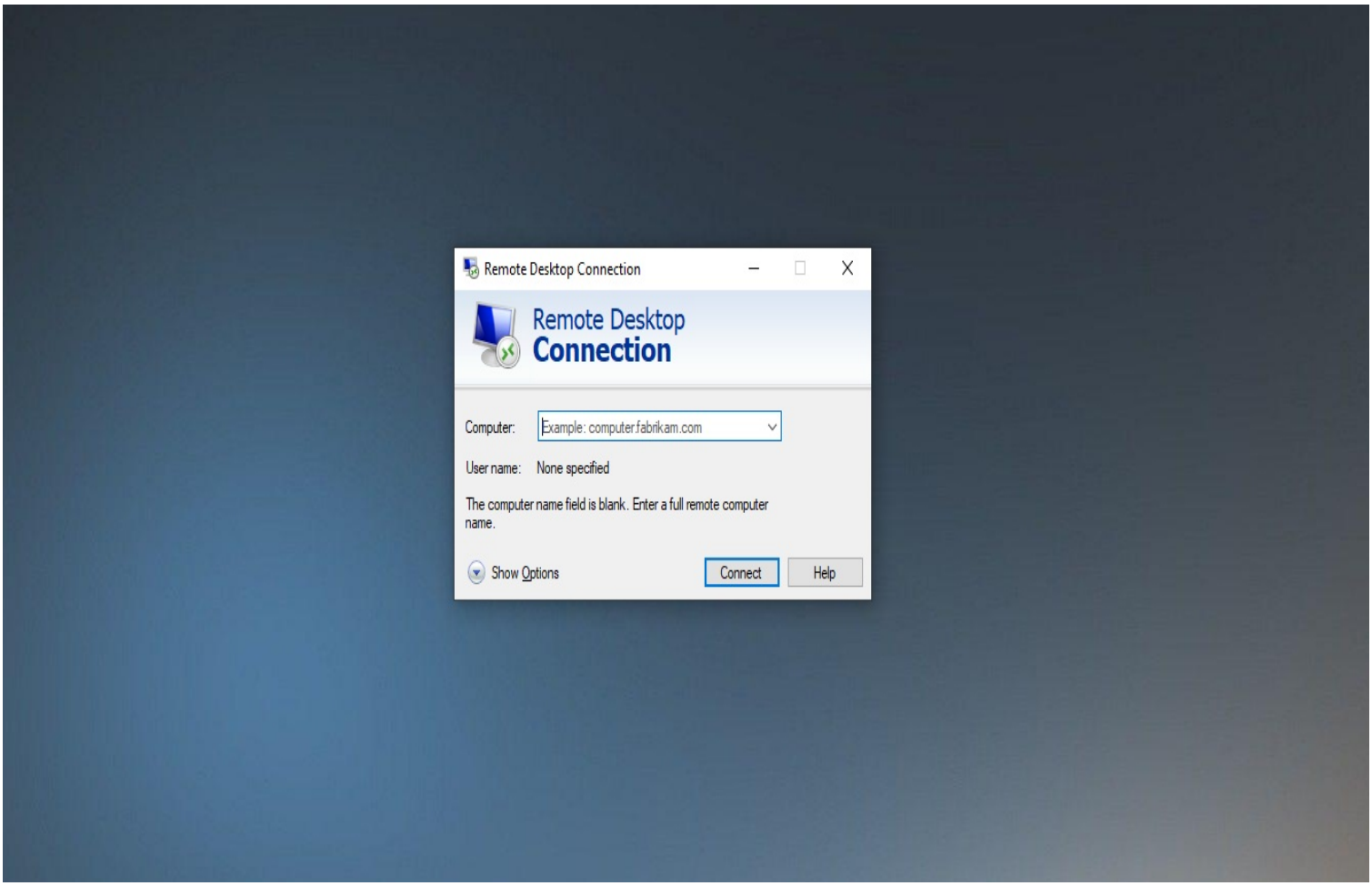
Forcing RDP to use TLS Encryption

427 Krishnaja August 2, 2024 Common Errors & Troubleshooting, General 20551

How to force RDP to use TLS Encryption?

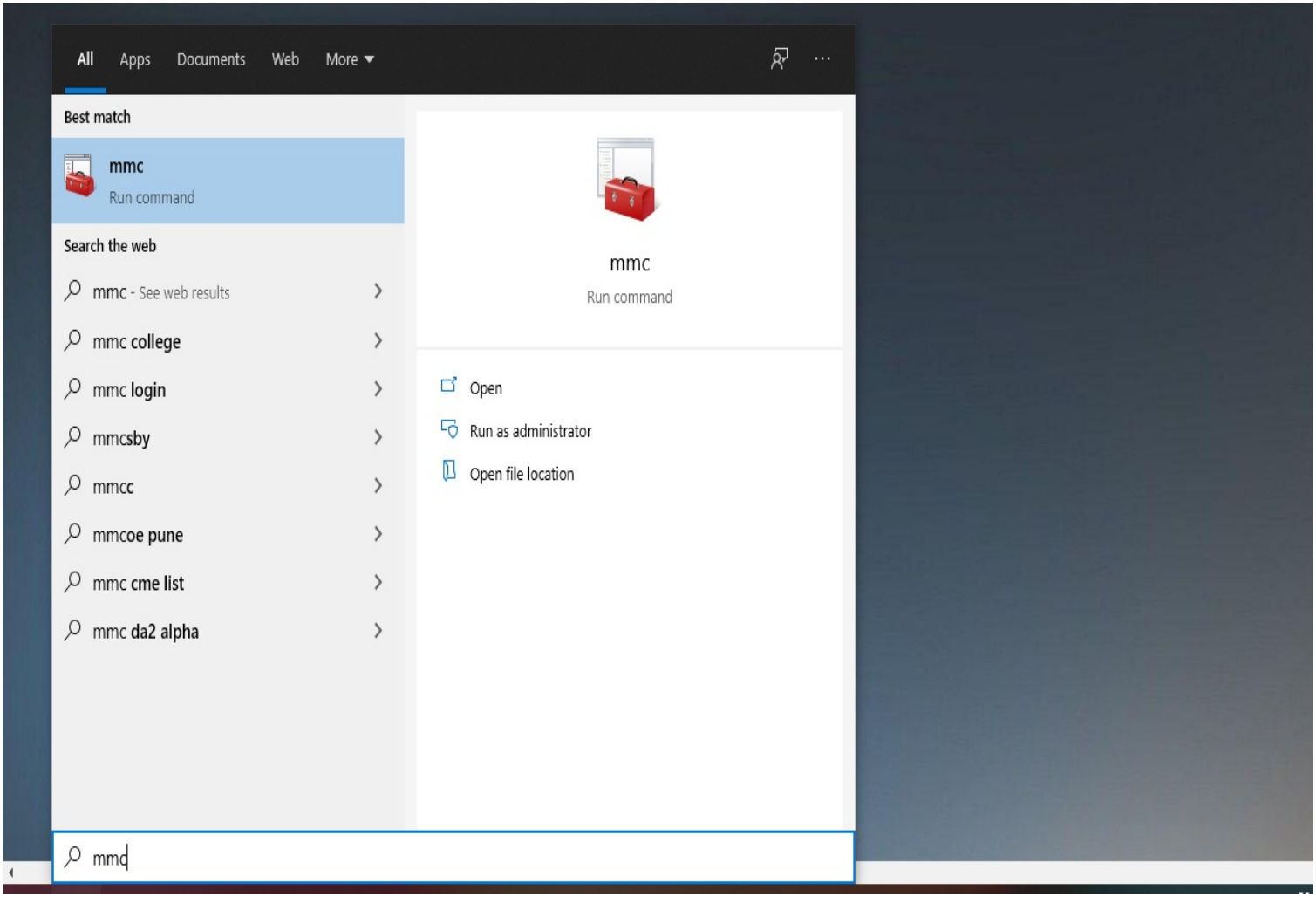
Overview: This article provides instructions on how to force Remote Desktop Protocol (RDP) to use TLS encryption.



Windows Remote Desktop Protocol (RDP) is widely used by system administrators to provide remote operators access to internal systems and servers. In a shocking oversight, this connection does not use strong encryption by default. To force RDP to use TLS Encryption follow below steps

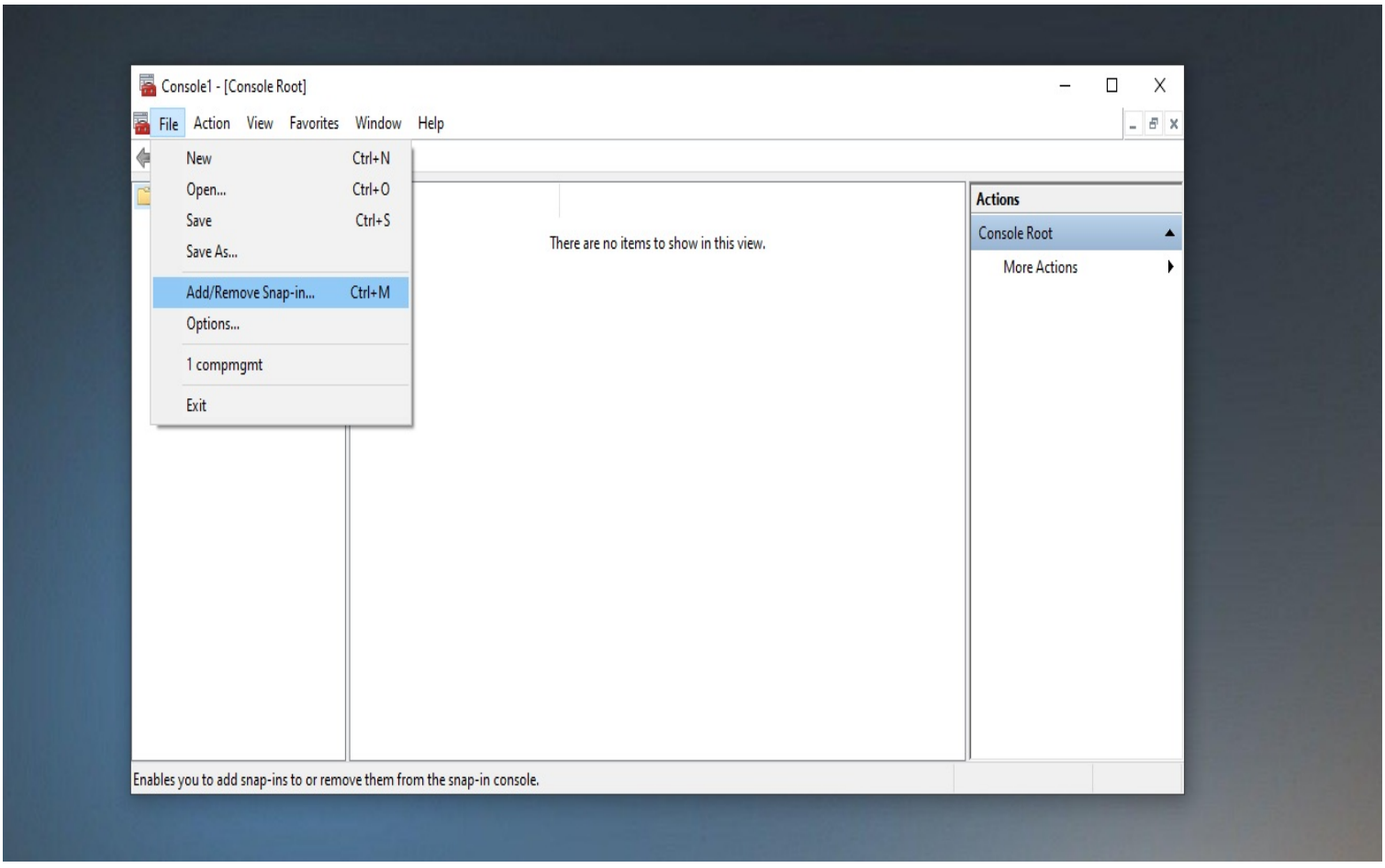
Step 1: Open the Root console

Open the search bar and type "**mmc**" or run **mmc.exe** from the Run application. Select the top application, which will open the system console.

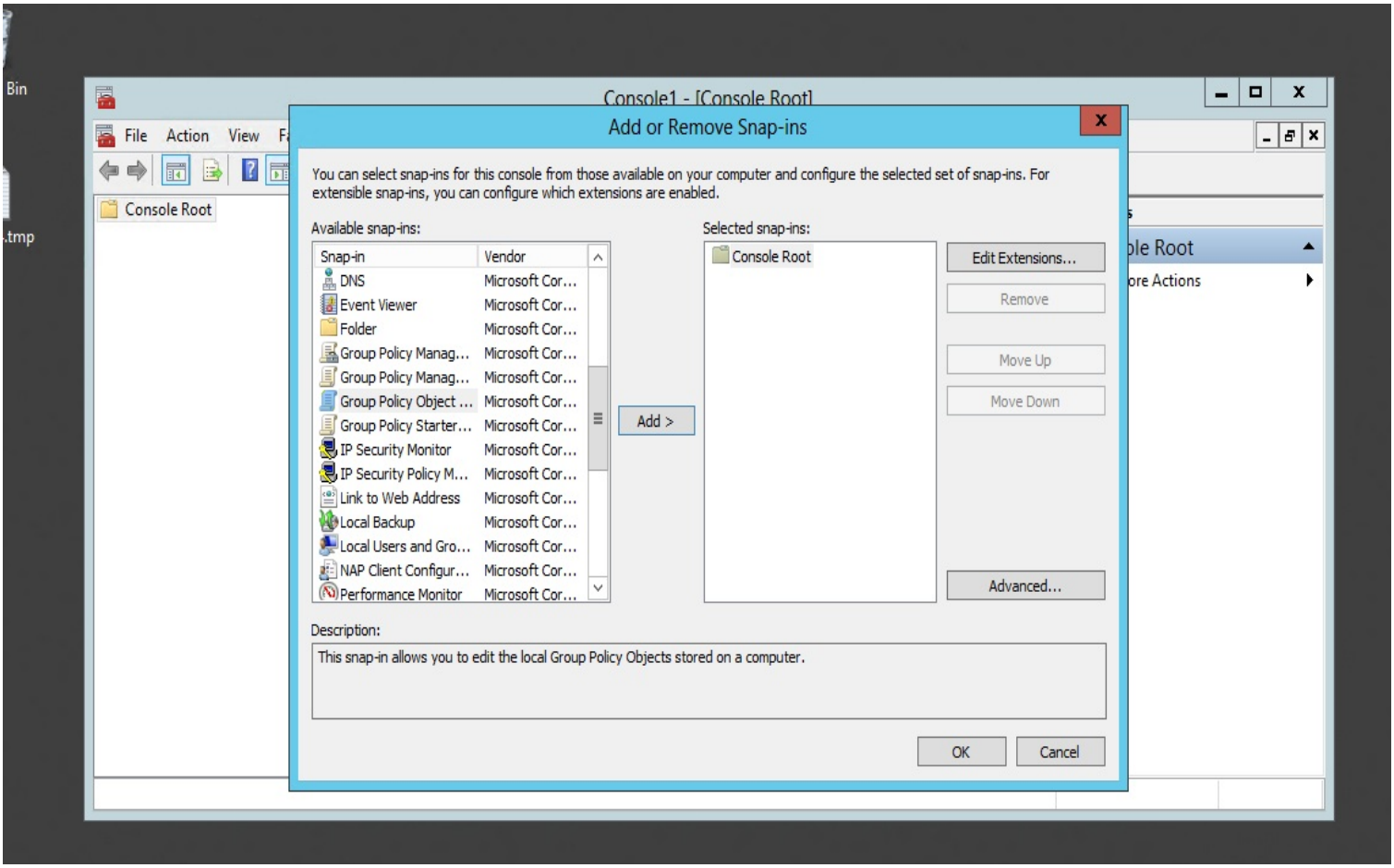


Step 2: Open the **Group Policy Editor Snap-in**

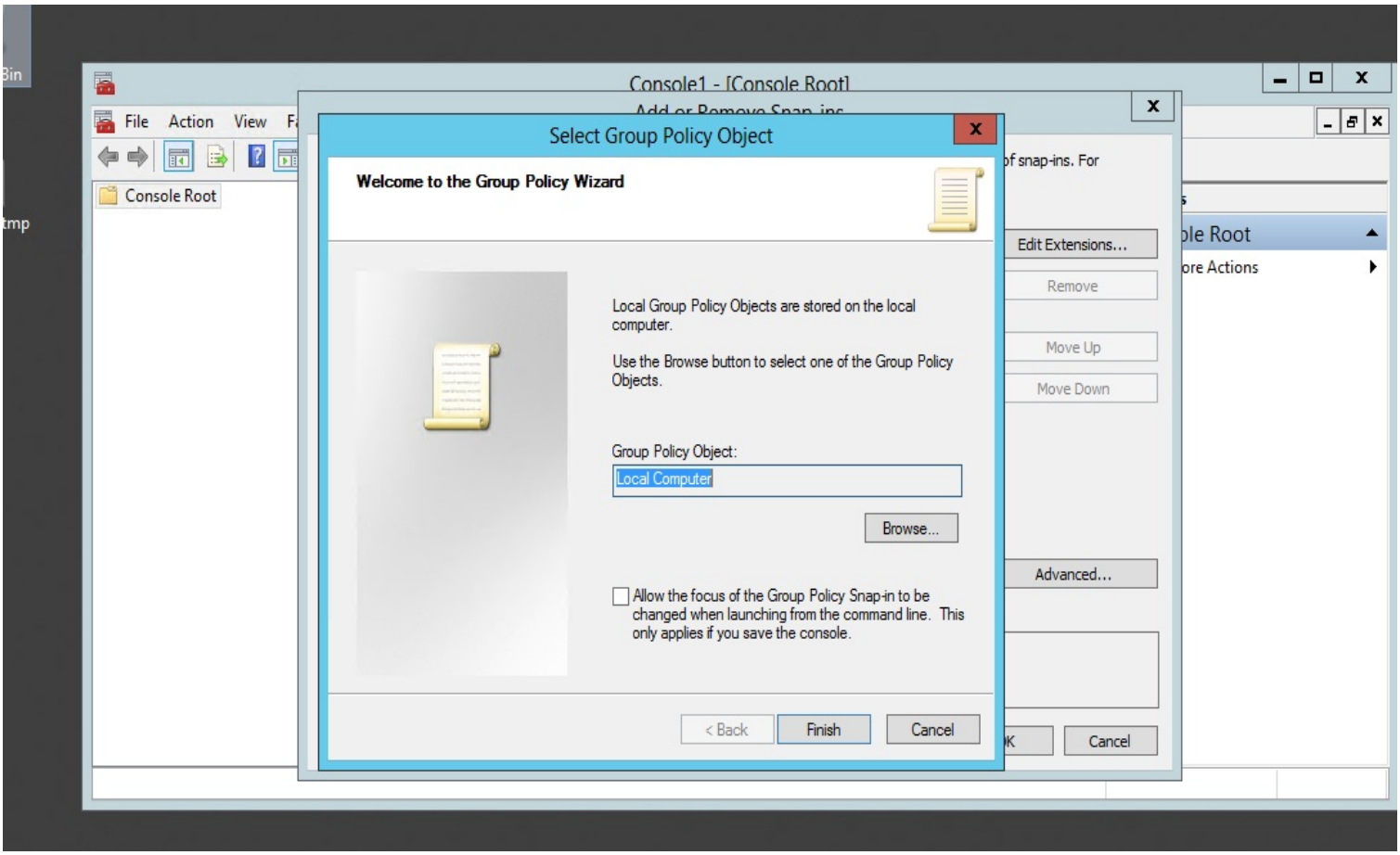
Open **File** -> **Add/Remove Snap-in** and select **Global Policy Editor**.



Step 3: Select "**Group Policy Editor**" and click on "**Add**" the selected snap-in.

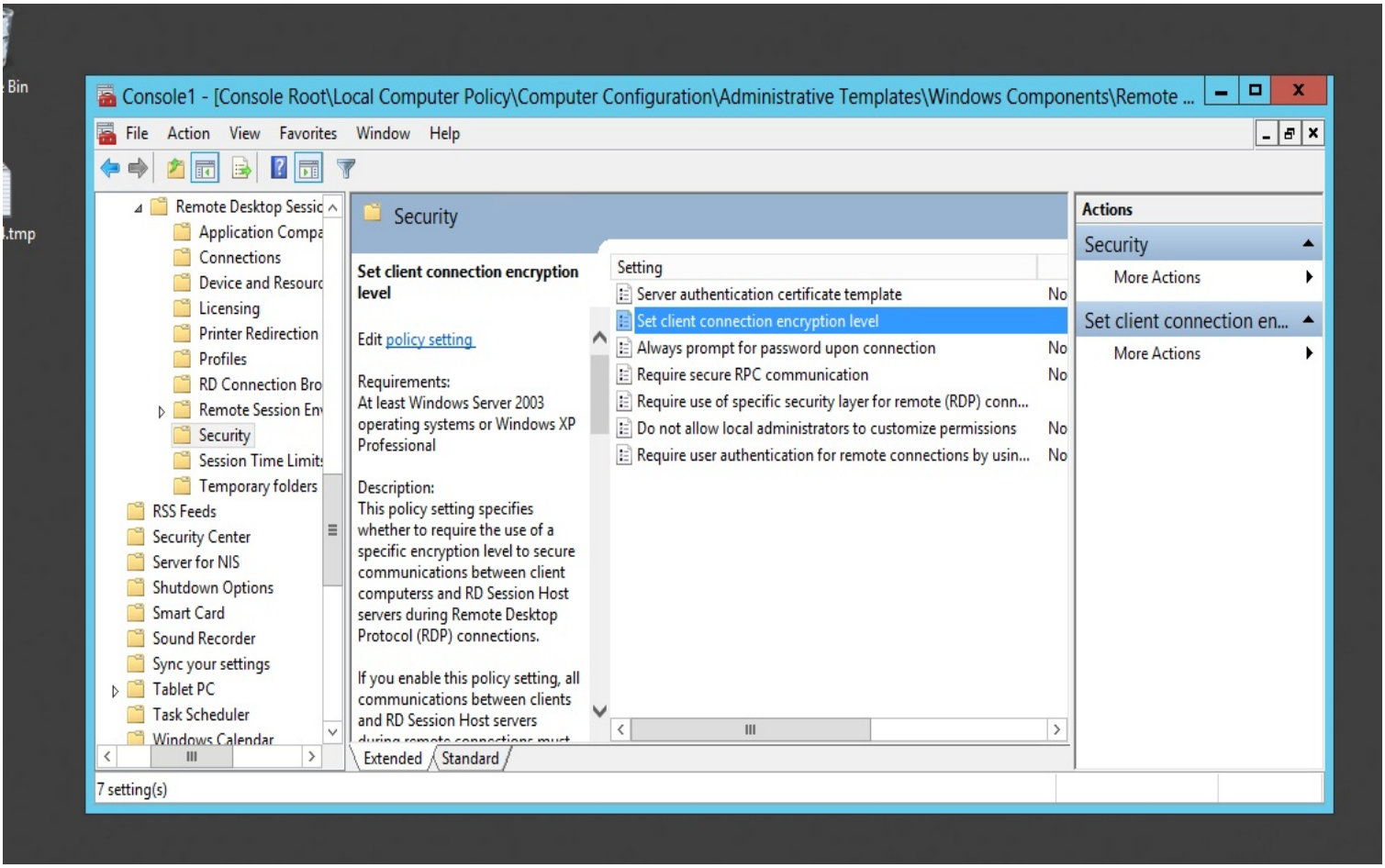


Step 4: Select the "**Local Computer**", this should be the default and select "**Finish**" > "**Ok**"



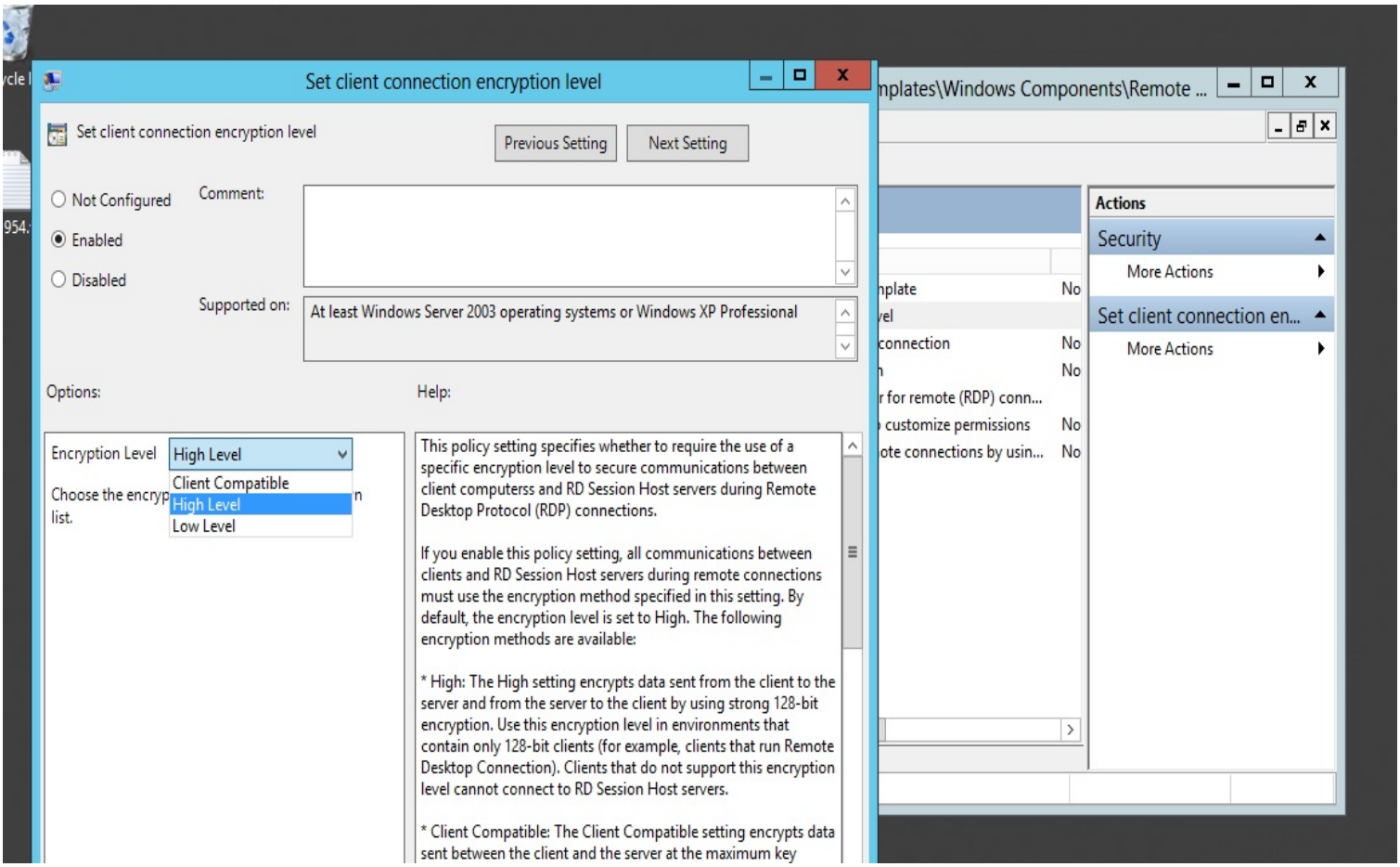
Step 5: Navigate to the RDP Session Security Policies

In the sidebar Navigate to **Local Computer Policy** -> **Computer Configuration** -> **Administrative Templates** -> **Windows Components** -> **Remote Desktop Services** --> **Remote Desktop Session Hosts** -> **Security**. Then select "**Set client encryption level**" and edit that policy.



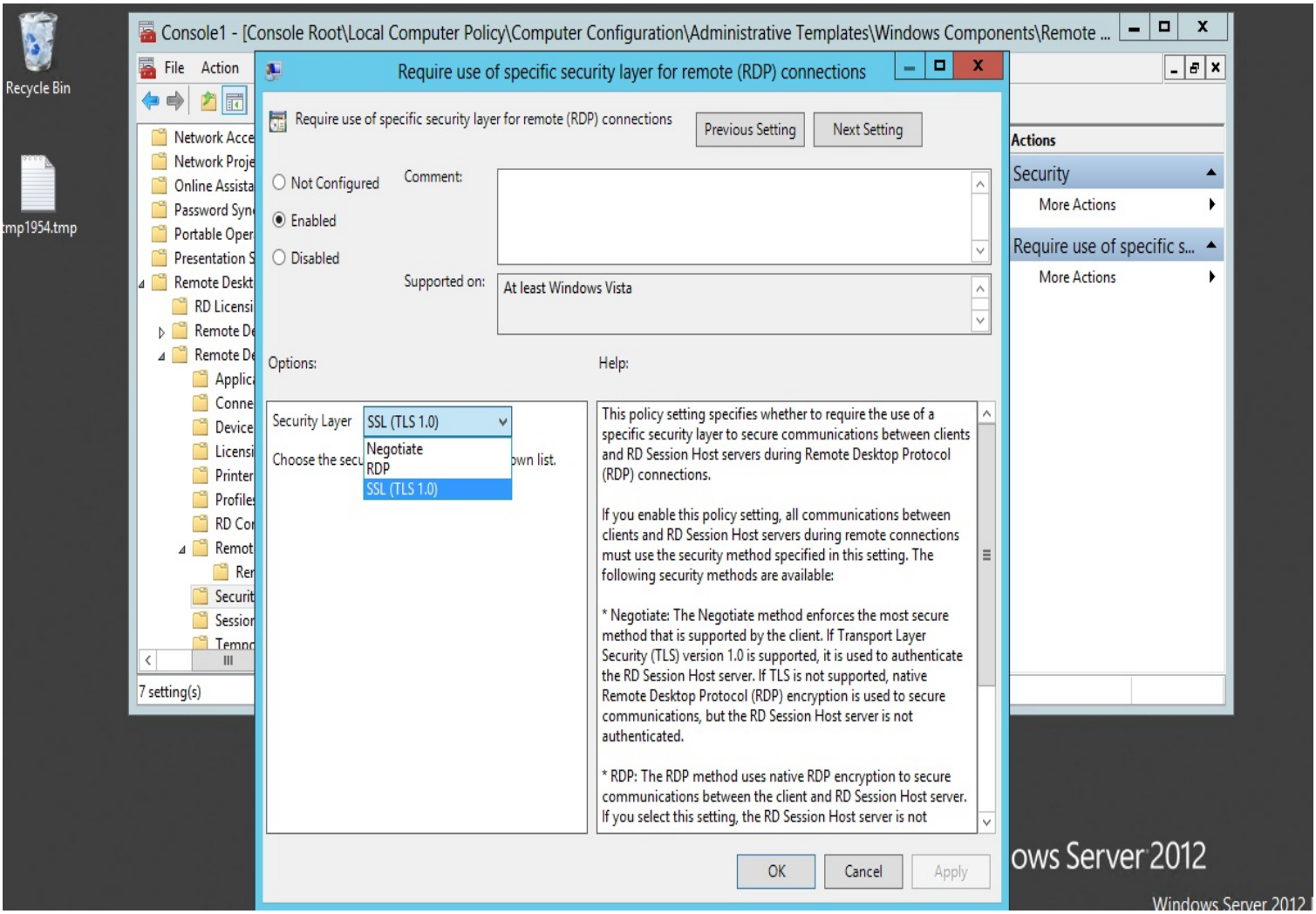
Step 6: Require the Highest native Encryption possible

Edit the "**Set client encryption level policy**".



Step 7: A better idea -> **Force TLS instead**

Edit the "**Require use of specific security layer for remote (RDP) connections**" policy.



Online URL: https://www.ezeelogin.com/kb/article/forcing-rdp-to-use-tls-encryption-427.html