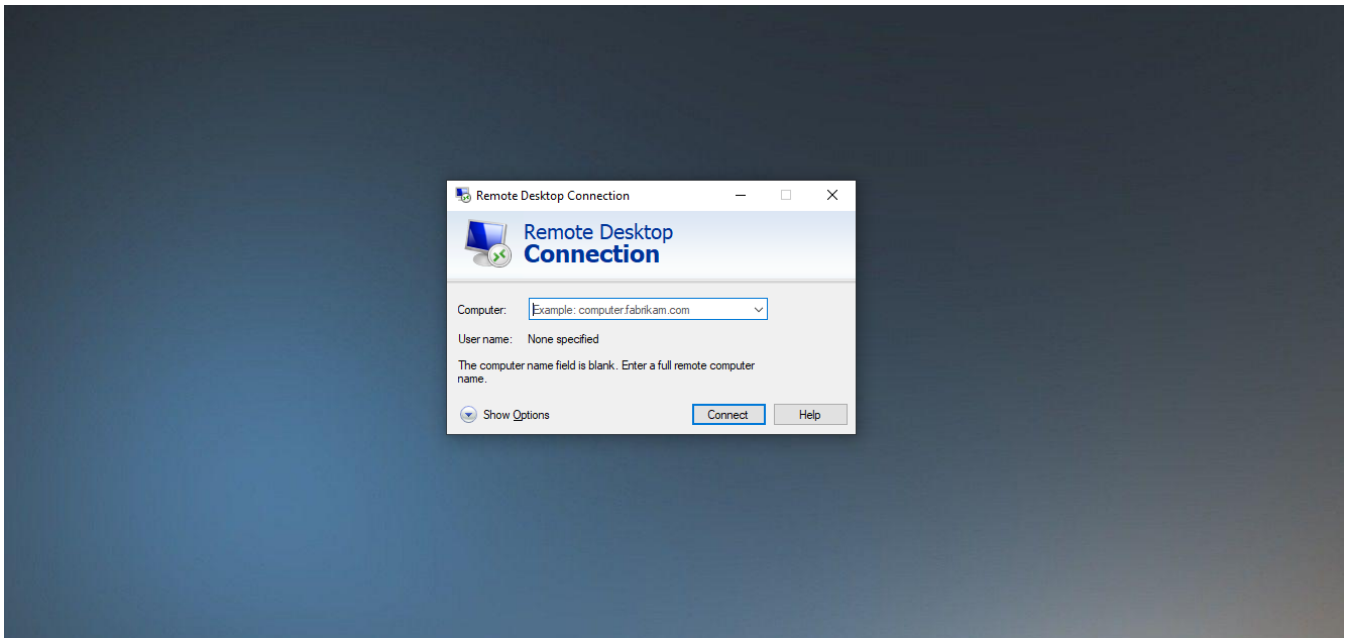
Forcing RDP to use TLS Encryption

427 Krishnaja August 16, 2021 Common Errors & Troubleshooting 7838

Forcing RDP to use TLS Encryption

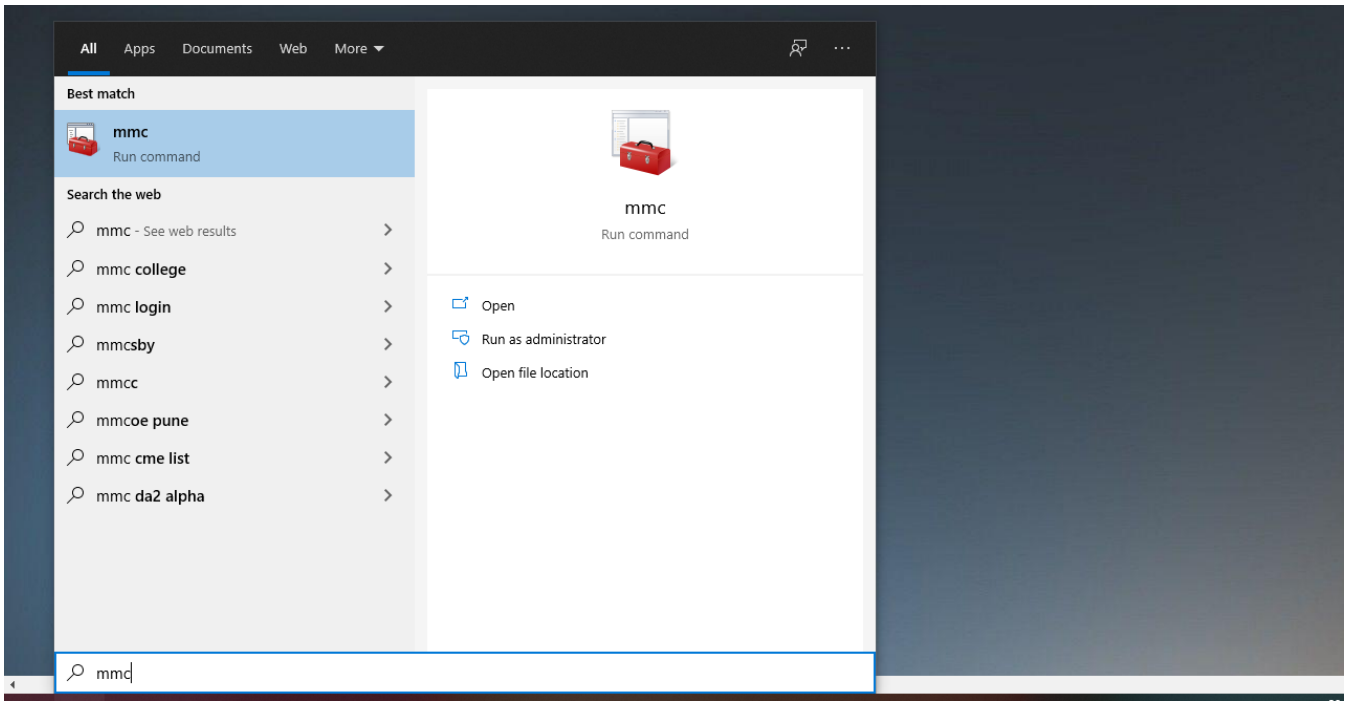
Windows Remote Desktop Protocol (RDP) is widely used by system administrators to provide remote operators access to internal systems and servers. In a shocking oversight, this connection does not use strong encryption by default.



1.Open the Root console

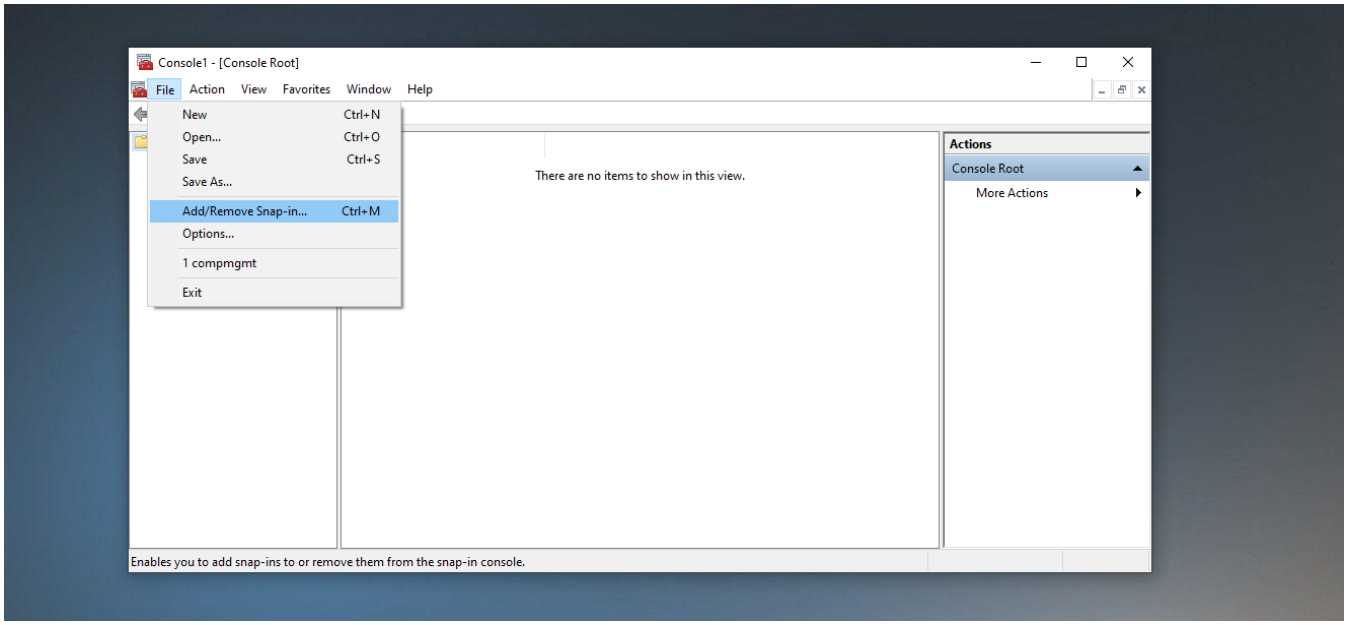
Open the search bar and type "mmc" or run mmc.exe from the Run application. Select the

top application, which will open the system console.

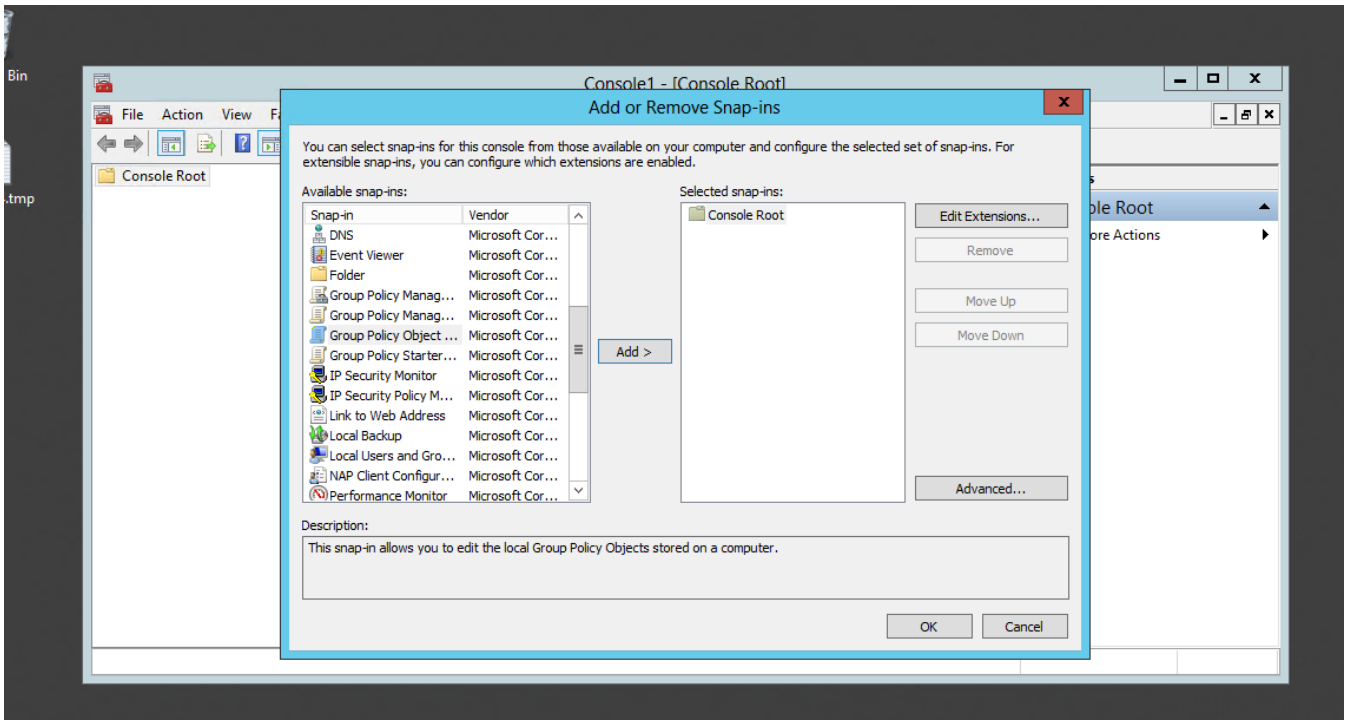


2.Open the Group Policy Editor Snap-in

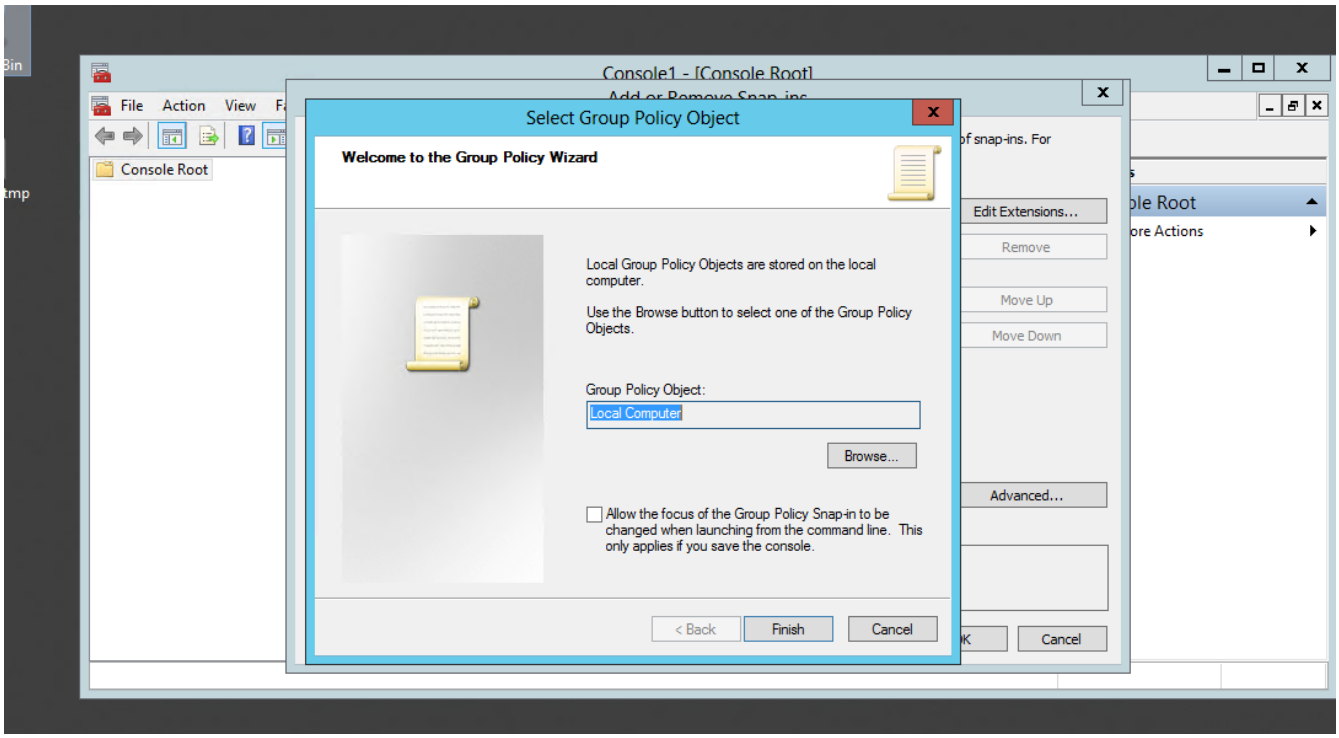
Open File > Add/Remove Snap-in and select Global Policy Editor.



Select "Group Policy Editor" and "Add" the selected snap-in.



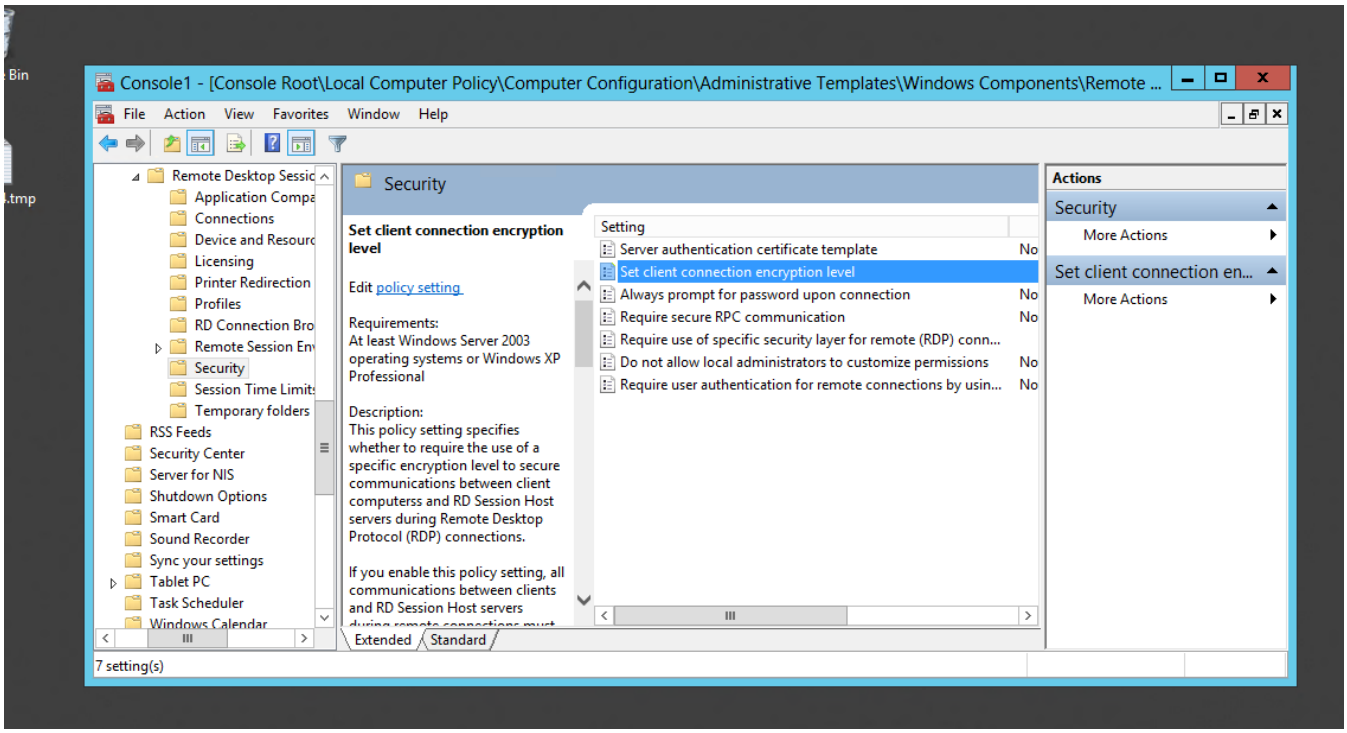
Select the "Local Computer" - this should be the default - and select "Finish" > "Ok"



3.Navigate to the RDP Session Security Policies

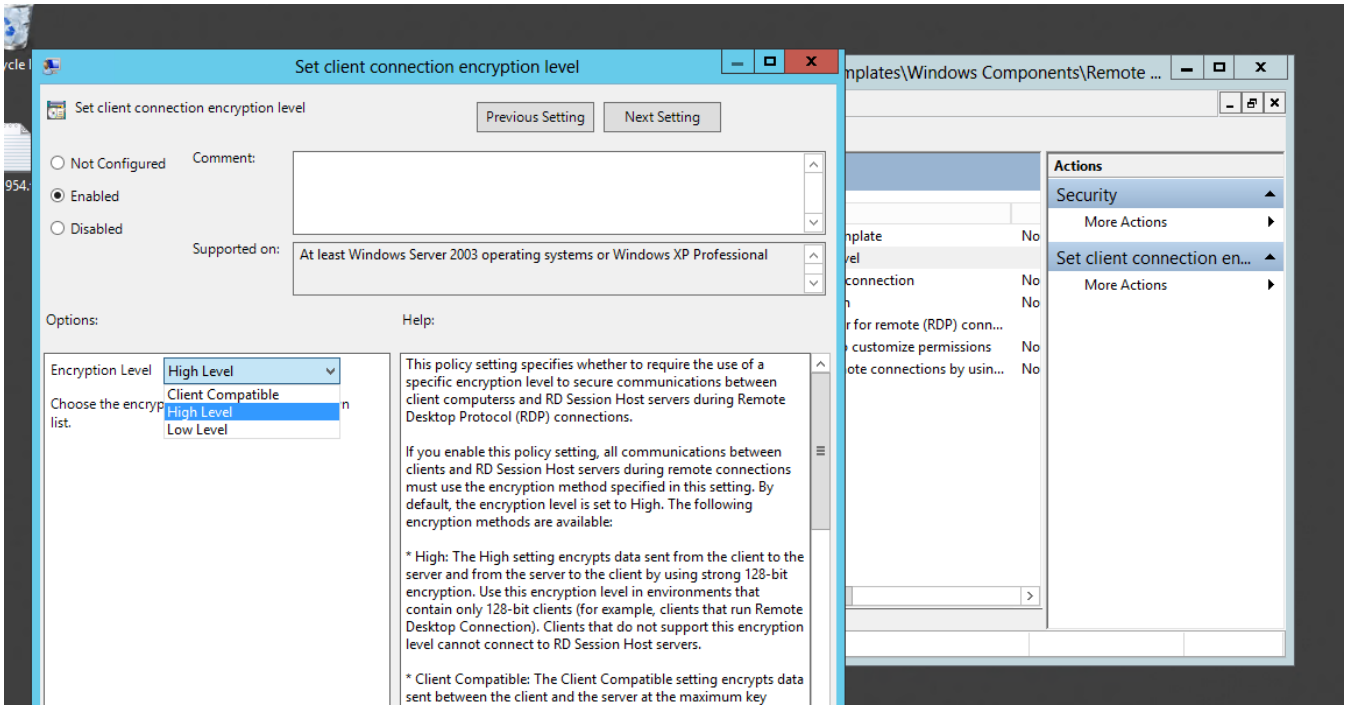
In the sidebar Navigate to Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components >Remote Desktop Services >Remote

Desktop Services >Remote Desktop Session Hosts > Security.Then select "Set client encryption level" and edit that policy.



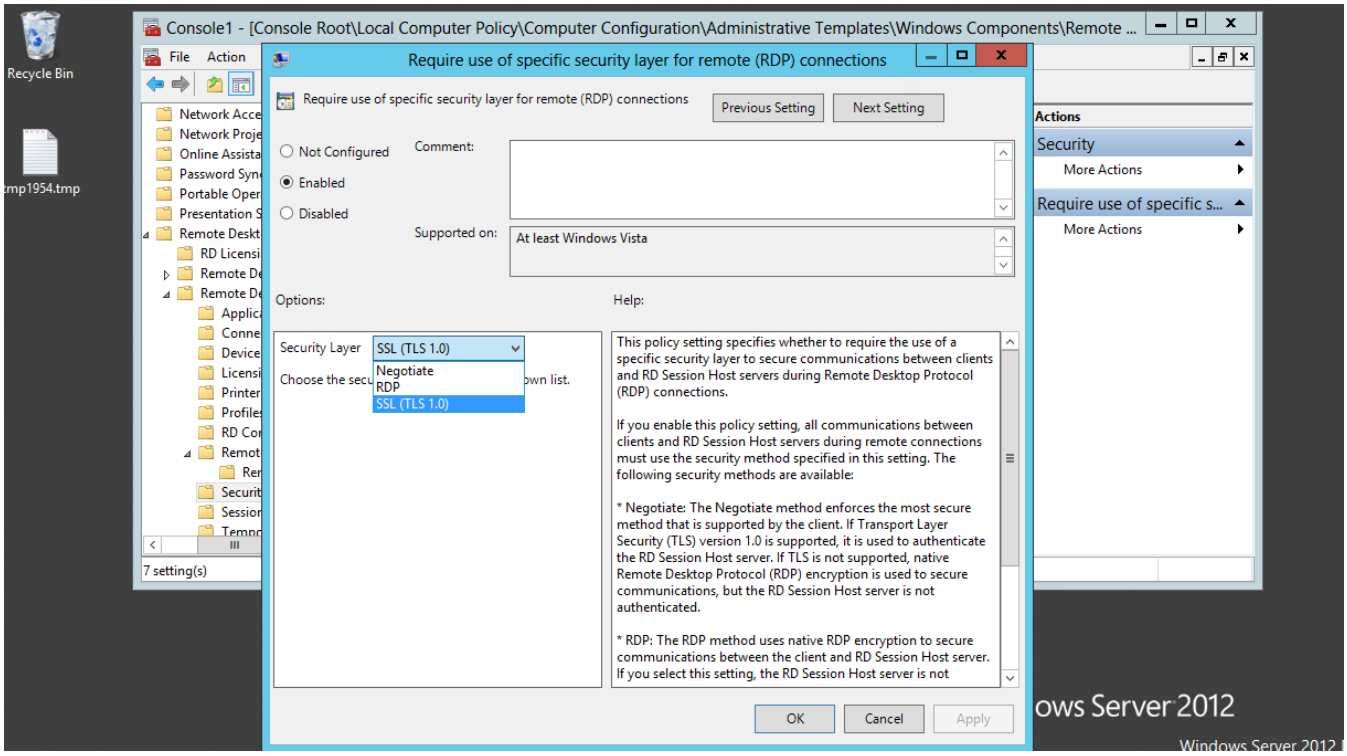
4.Require the Highest native Encryption possible

Edit the "Set client encryption level policy".



5.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