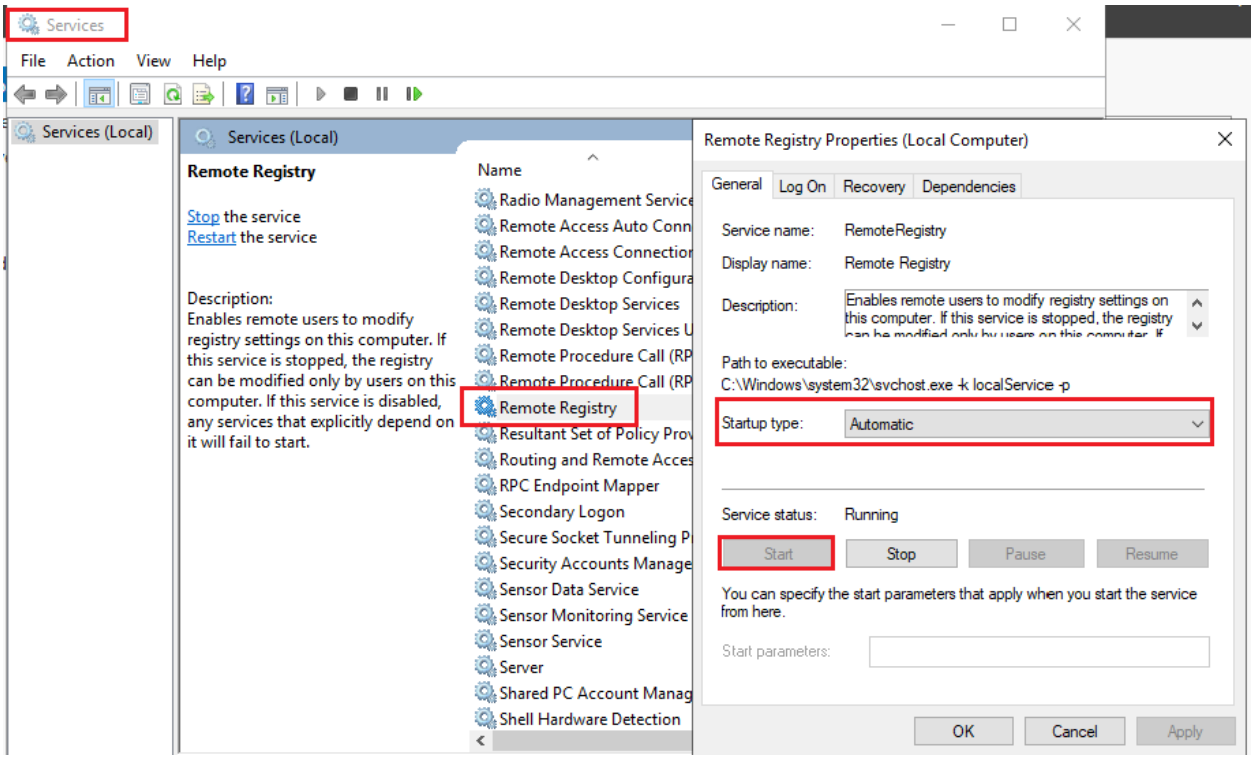
Prerequisite for Windows Credentialed Scan:

To perform a credentialed scan on Windows systems using Nessus, you need to meet several prerequisites on the target Windows machine. These allow Nessus to log in remotely, retrieve detailed information, and detect more vulnerabilities.

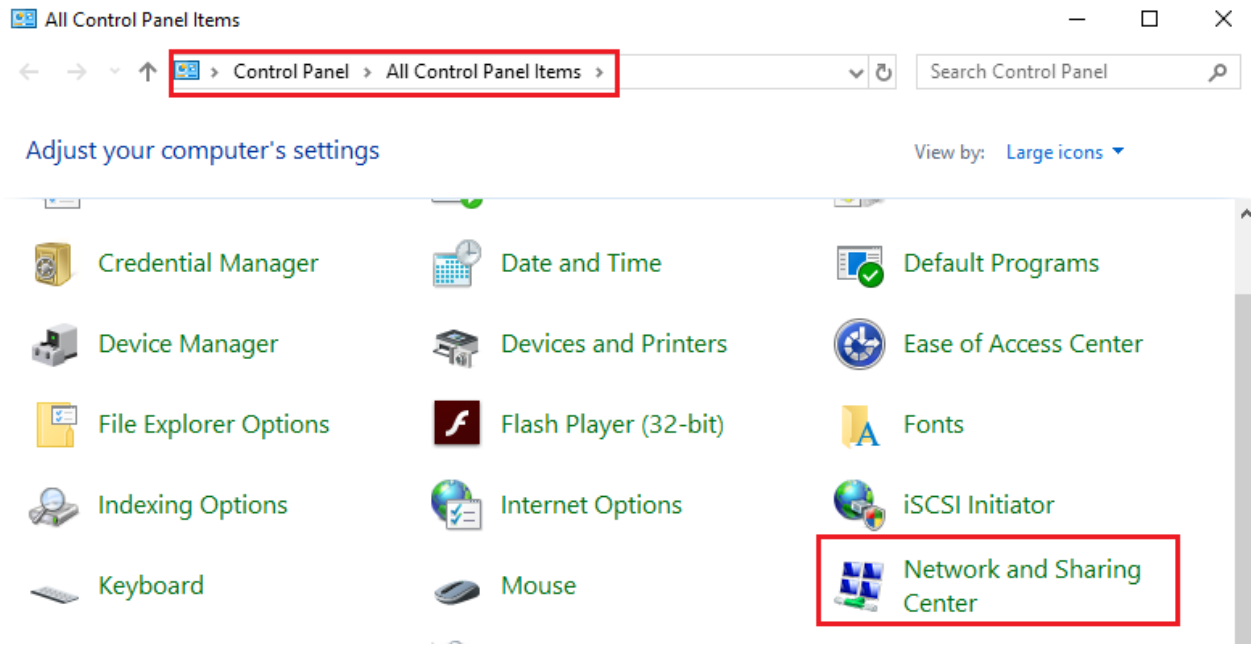
Enable Remote Registry:

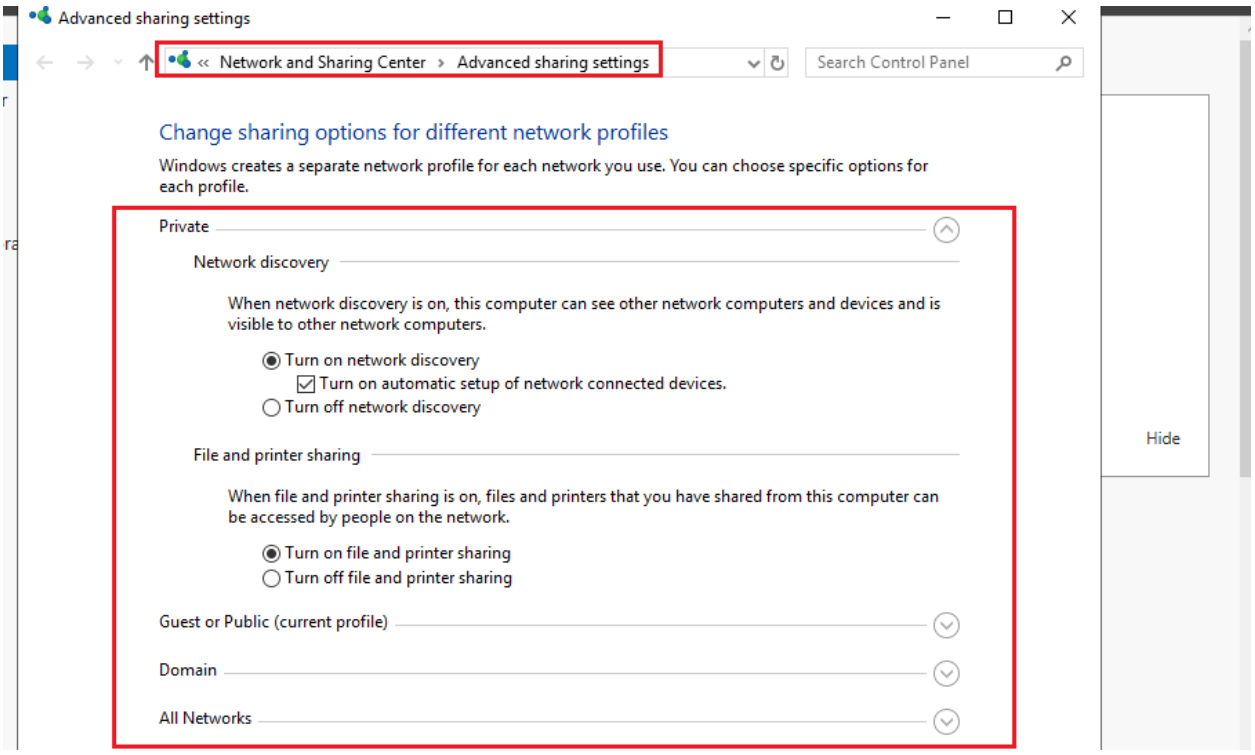
Click on the start icon and then type “services.msc” and hit “enter.” Go to “remote registry,” double-click on it, and then click on “startup type.” Select “automatic” and then “apply” and hit “okay.”



Enable File and Printer Sharing:

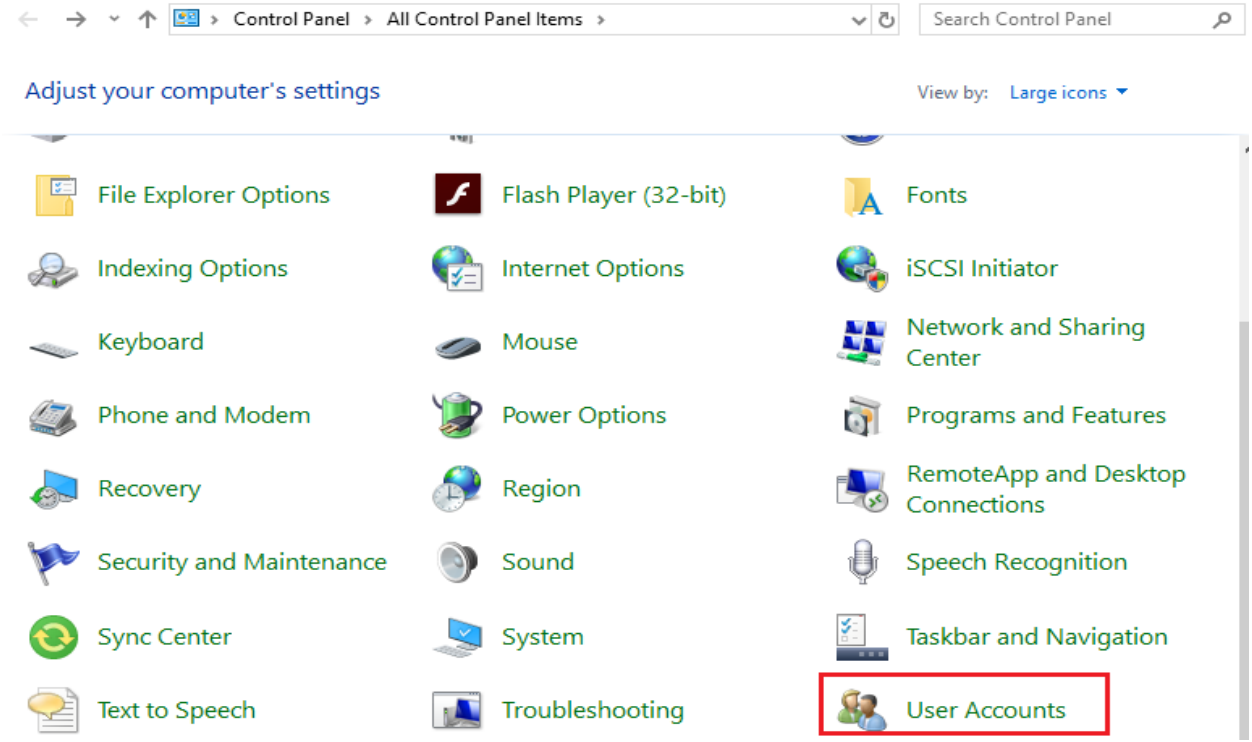
Control Panel > Network and Sharing Center > Advanced Sharing Settings. Enable file & printer sharing through "Advanced sharing settings".

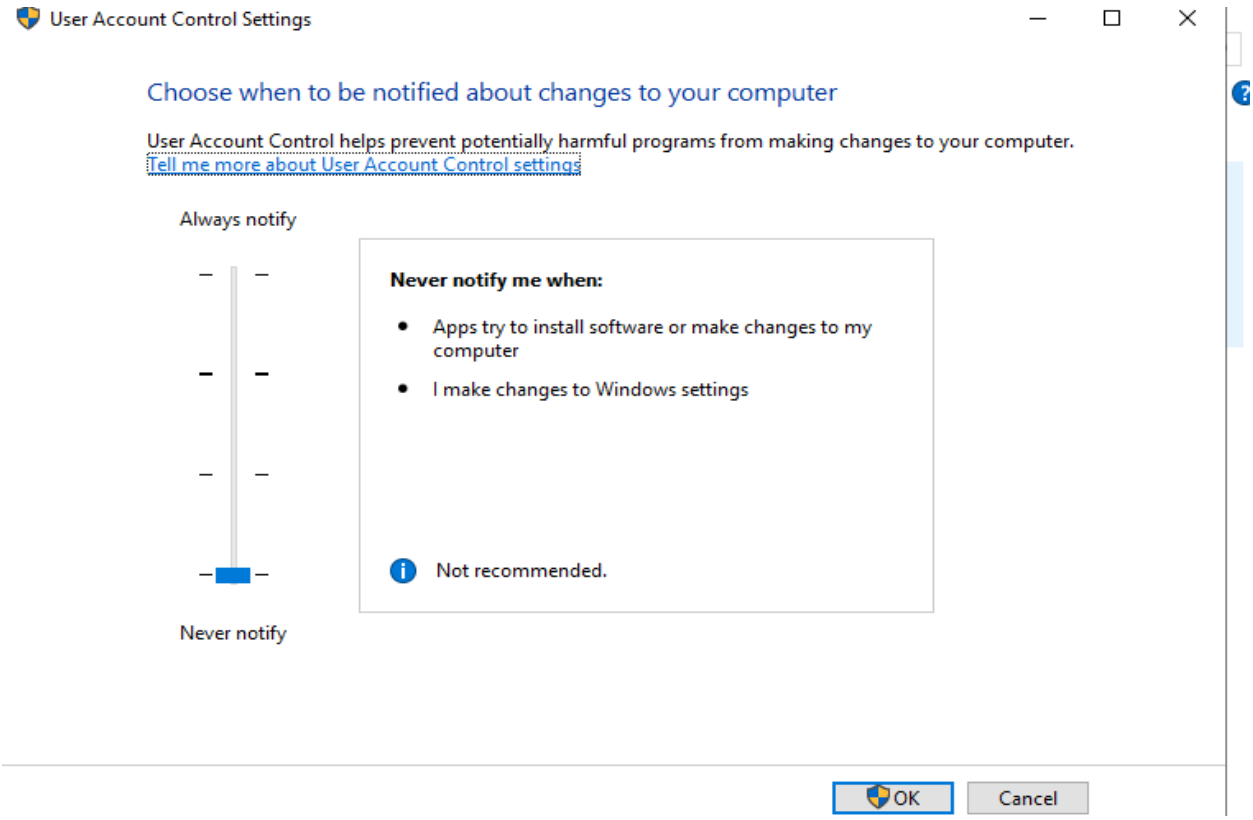




Disable UAC for Remote Admins:

Go to “user account control” and set it to “never notify,” hit “okay.”

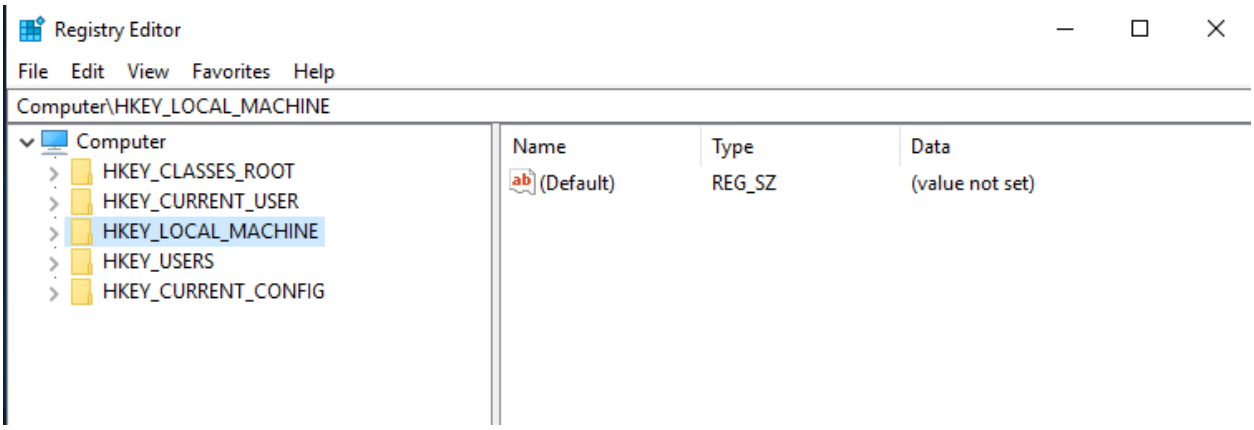


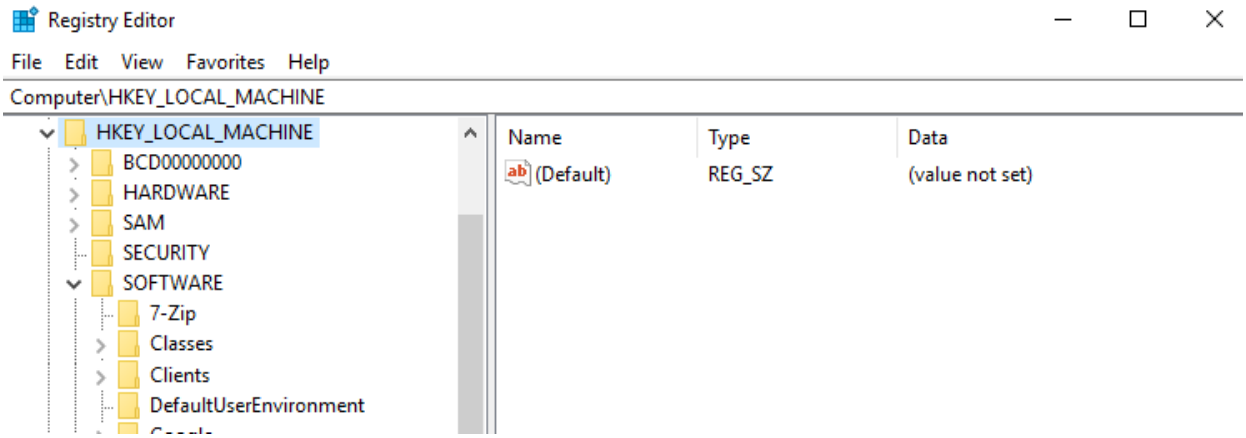


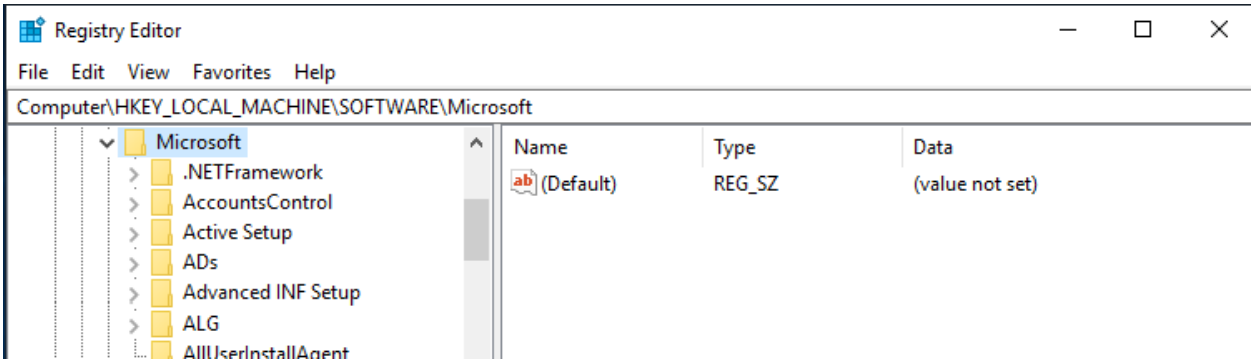
Registry Service:

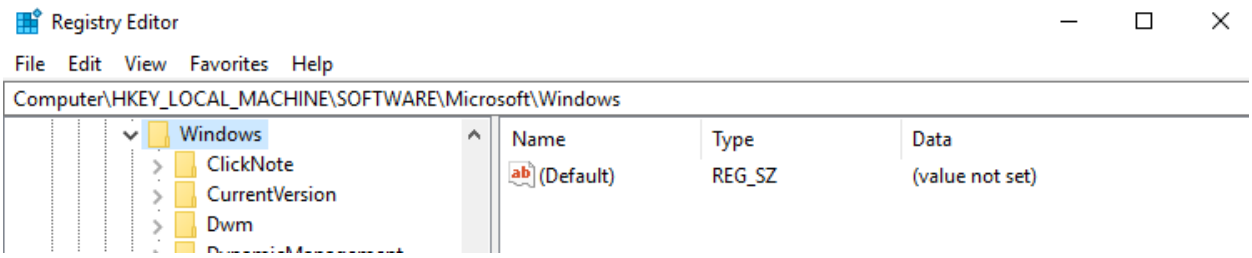
Go to the "registry editor" and add a remote key by navigating to:

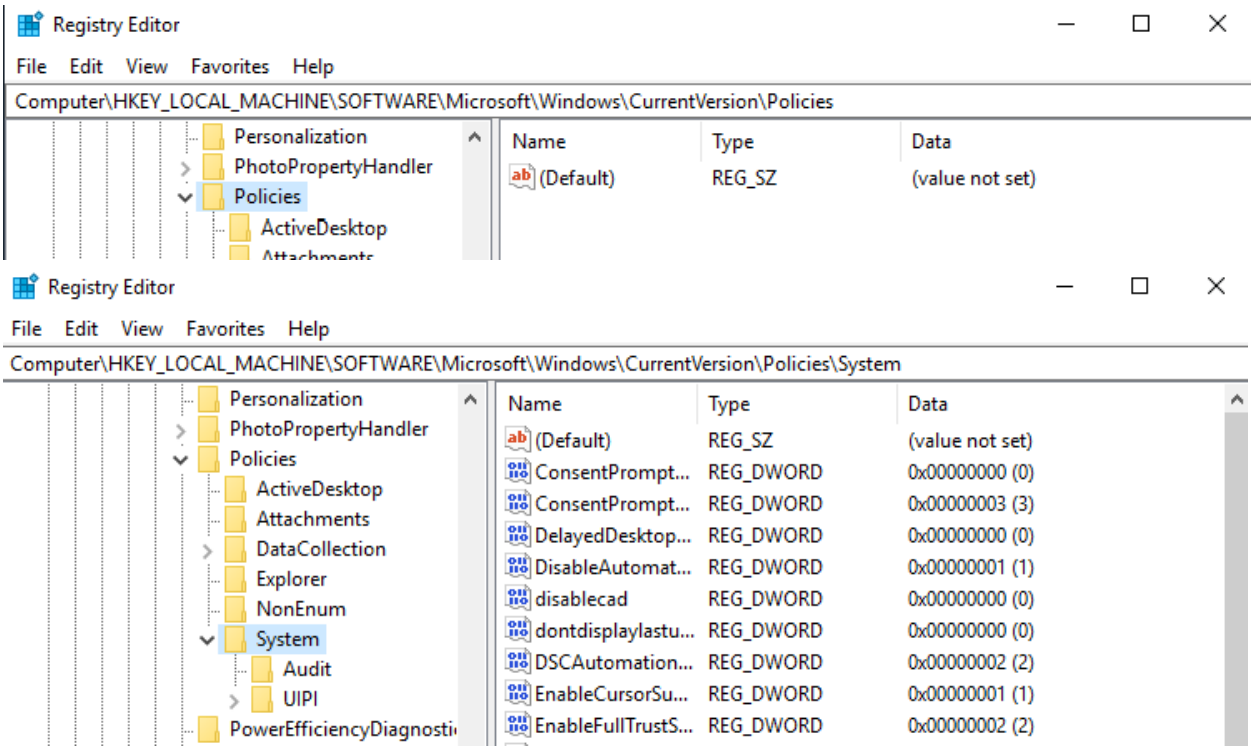
Local Machine > Software >Microsoft > Windows > CurrentVersion > Policies > System



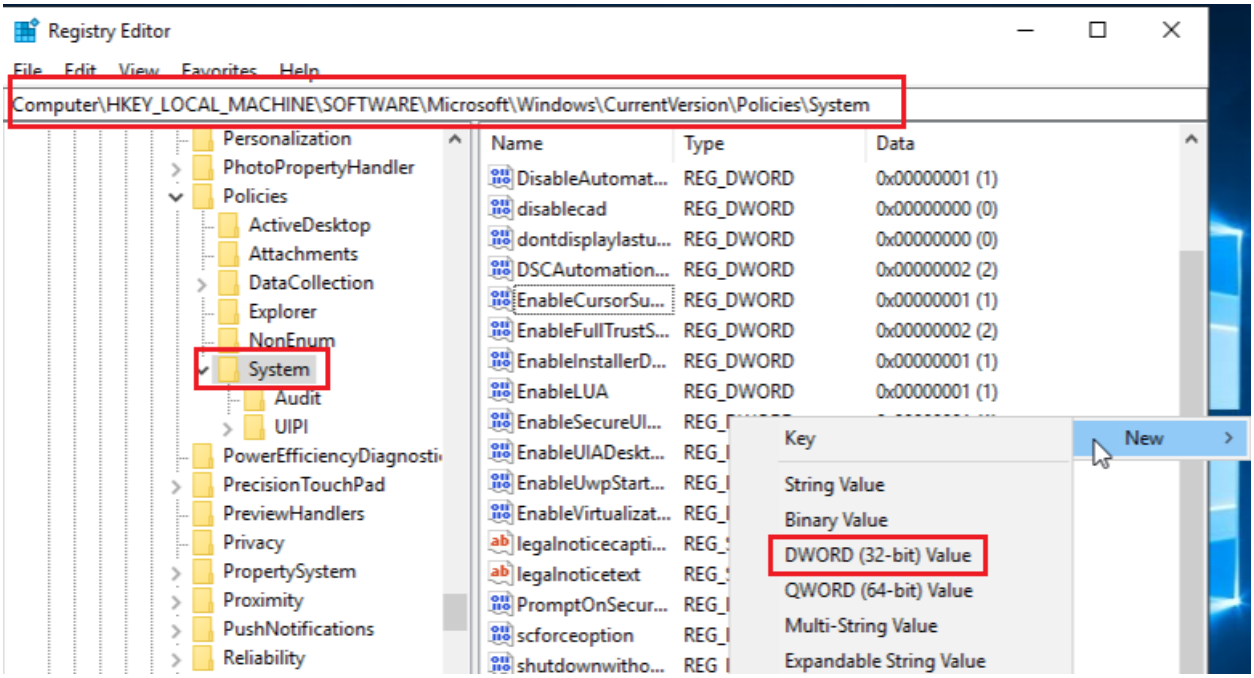








Right-click anywhere on the screen, select "new" and create a "Dword" called "LocalAccountTokenFilterPolicy."



Then double-1click on the one you just created and set its value to “1.”