RunAsAdmin PowerShell

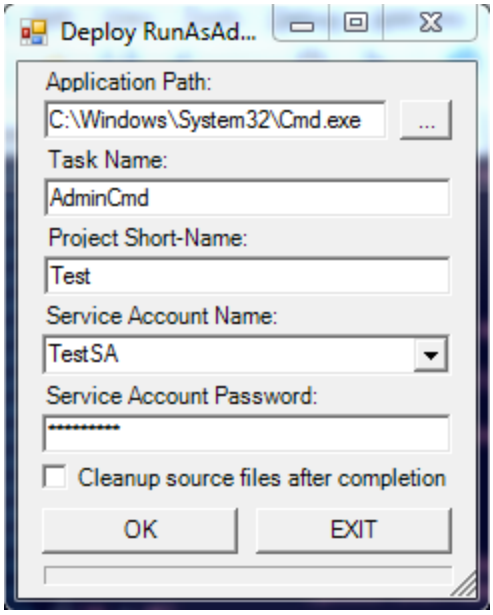
RunAsAdmin is an application to help adhere to the best practice of least privileges. It creates an .exe that the user can double click and it will execute a program with elevated privileges. Users must be in a local group in order to execute the process.

To implement a new RunAsAdmin program, extract the RunAsAdmin.zip to the C:\Tools\ directory.

From an Administrator PowerShell prompt do the following:

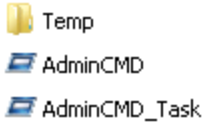
PS> cd C:\Tools\
PS C:\Tools\> .\Deploy-RunAsAdmin.ps1

The Deploy RunAsAdmin window will appear



Application Path: The path to the application you want to run with elevated privileges.
Task Name: The name given to the application (will be the name of the exe the user will run)
Project Short-Name: A “name” for the project, allows for multiple programs to utilize a single group for user access.
Service Account Name: The name of the Service Account that will be an Administrator and will run the program. If the SA doesn’t exist, it will be created.
Service Account Password: The password for the SA. If the SA exists, password must match existing password.
Cleanup Checkbox: If checked, the source files will be deleted, leaving only the files for the process in C:\Tools.

In the C:\Tools\[Task Name] Directory



The .exe WITHOUT "_Task" (AdminCMD in this case) is the one that the user will execute. It is recommended that you place a shortcut on the users desktop to that .exe

In order for a user to run the .EXE and execute the program, they must be placed in the _TaskRunner local group. (in the example below, the Project Name is "Test")