solve, automate, speed up

AutoIt

AutoIt Cheat Sheet

Delete registry key, reg delete

```
RegDelete('HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run'
```

RunWait command with pipe

```
RunWait(@ComSpec & ' /c ' & 'echo 1 | "C:\Program Files (x86)\Cisco\Cisco A
```

To monitor whats actually happening use:

```
RunWait(@ComSpec & ' /c ' & 'echo 1 | "C:\Program Files (x86)\Cisco\Cisco A
```

Show computername, use it as variable

Use `& @computername &` for computername insert in text:

```
MsgBox(0, "Error", "Your computername is " & @computername & ".")
```

Or just `@computername` for variable:

```
$cn=@computername
MsgBox(0, "Error", "Your computername is " & $cn & ".")
```

Write file

Basic:

```
Local $file = FileOpen("\\log_server\log1\test.log", 1)

FileWrite($file, "this is text. CRLF means [press enter]" & @CRLF)
FileClose($file)
```

This is advanced:

```
Local $file = FileOpen("test.txt", 1)

; Check if file opened for writing OK
If $file = -1 Then
    MsgBox(0, "Error", "Unable to open file.")
    Exit
EndIf

FileWrite($file, "Line1")
FileWrite($file, "Still Line1" & @CRLF)
FileWrite($file, "Line2")

FileClose($file)
```

if exist directory

```
$f1="C:\Users\user1"
$f2="C:\documents and settings\user1"
If (FileExists($f1) or FileExists($f2)) Then
   MsgBox(4096, $f1, "Exists")
Else
   RunAsWait("user1", "domain-com", "sdfJUFE6e3!dfs", 1, "","")
EndIf
```

The point of this program is to cache user profile for future use if computer has no network connection.

Write in registry

```
#RequireAdmin
;================================
; Simple Way To Disable UAC
; Author : M3
;================================

sDisableUAC()

Func sDisableUAC()
Local $Result , $sHKLM ,$sPath
```

```
$sHKLM = "HKEY_LOCAL_MACHINE"
$sPath = "\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\"
RegWrite($sHKLM & $sPath ,"ConsentPromptBehaviorAdmin","REG_DWORD","0")
Sleep(100)
; Start Execute your Script Here
EndFunc
```

Ping Forever

Classic ping command with -t switch:

```
$cName = InputBox('PingForever','Type a computername to ping:')
if StringLen($cName) > 0 Then
RunWait(@ComSpec & ' /c ' & 'ping -t ' & $cName)
Else
MsgBox(0,'Info','No computername was entered. Exiting.. Bye. Have a nice da
EndIf
```

AutoIt User Input

```
$cName = InputBox('Remote assistance','Type a computername to connect:')

if StringLen($cName) > 0 Then
 RunWait('mstsc /v:' & $cName & ' /f')
 Else
 MsgBox(0,'Info','No computername was entered. Exiting.. Bye. Have a nice d
 EndIf
```

Pass variable to AutoIt command

```
if $CmdLine[0] = 0 Then
 MsgBox(0, 'Note', 'Computername variable must be specified for this comman
 Exit
 EndIf

if StringLen($CmdLine[1]) > 0 Then
 RunWait('mstsc /v:' & $CmdLine[1] & ' /f')

 EndIf
```

Turn of windows firewall, RunAs

You can create AutoIt program that use local administrator user that have rights to do the trick.
Enter local administrator password and compile the program.

`FirewallOff.au3:`

```
Local $sUserName = "administrator"
Local $sPassword = ""

RunAs($sUserName, @ComputerName, $sPassword, 0, "netsh firewall set opmode
```

Run application as domain administrator

```
Local $sUserName = "domain_administrator_username"
Local $sPassword = "Top_secret_Passw0rd!"
Local $sDomainName = "domain-name"

RunAsWait($sDomainName, $sPassword, $sDomainName, 1, "C:\Program Files\Micr
```

AutoIt String Length

```
$String = 'CatOnRug.NET'
MsgBox(0, '', 'Lenght of string ' & $String & ' is ' & StringLen($String))
```

Run Remote Desktop Connection, wait exit code

This will start mstsc and wait until it completely ends and only then go to next command:

```
RunWait(@WindowsDir & "\system32\mstsc.exe", @WindowsDir, @SW_MAXIMIZE)
MsgBox(0, "Next command","going to next command")
```

RunWait Net LocalGroup

```
RunWait(@ComSpec & ' /c ' & 'Net LocalGroup "Administrators" "DomainName\Us
```

"Administrators" is built in group. There can be any other group that exists.
"DomainName\Username" is username of domain.

No comments:

Post a Comment