Quick commands (Windows)

Nameresolution via other server than default

```
nslookup somewhere.com some.dns.server
```

Get Windows client join status

```
dsregcmd /status
```

Get applied GPO status on Windows client

```
gpresult /h C:\LocalData\GPResult.html
```

Get RDS license status

```
(Invoke-WmiMethod -PATH (gwmi -namespace root\cimv2\terminalservices -class
win32_terminalservicesetting).__PATH -name GetGracePeriodDays).daysleft
```

```
wmic /namespace:\\root\CIMV2\TerminalServices PATH Win32_TerminalServiceSetting WHERE (__CLASS
!="") CALL GetGracePeriodDays
```

Rejoin device to Microsoft Entra ID

```
dsregcmd /forcerecovery
```

Restart Computer to BIOS/UEFI

```
shutdown /r /fw
```

Delete specific files recursive

```
$source = "<sourcepath>"
$fileextension = "<filextension>"
get-childitem $source -include *$fileextension | foreach ($_) {remove-item $_.fullname}
```

Run PowerShell as admin from different session

```
Start-Process PowerShell -verb runas
```

Get last reboot time

```
Get-WmiObject win32_operatingsystem | select csname,
@{LABEL='LastBootUpTime';EXPRESSION={$_.ConverttoDateTime($_.lastbootuptime)}}
```

Delete Windows Hello Container

```
certutil.exe -DeleteHelloContainer
```

Reset Windows to Factory Settings

```
systemreset
```

Set error action in PowerShell session

```
$erroractionpreference = "silentlycontinue"
```

Test network connection

Test TCP port

```
Test-NetConnection -ComputerName <youripaddress> -Port <yourport>
```

```
$ipaddress = "<youripaddress>"
$port = "<yourport>"
$connection = New-Object System.Net.Sockets.TcpClient($ipaddress, $port)
if ($connection.Connected) {
     Write-Host "Success"
} else {
     Write-Host "Failed"
}
```

Test UDP port

```
$ipaddress = "<youripaddress>"
$port = "<yourport>"
$connection = New-Object System.Net.Sockets.UdpClient($ipaddress, $port)
if ($connection.Connected) {
     Write-Host "Success"
} else {
     Write-Host "Failed"
}
```

Check if address goes through proxy

```
([System.Net.WebRequest]::GetSystemWebProxy()).getProxy("https://lucanoahcaprez.ch")
```

This returns an object containing the information about the connection. If the "Host" property does not contain the original requested URL, there is a setting on Windows present. This setting defines the Proxy and the address of the proxy can be viewed in the "Host" property on the response object of this command.

Manage Local Windows Groups

Add Microsoft Entra ID user to administrator group

```
$Email = ""
Add-LocalGroupMember -SID "S-1-5-32-544" -Member "AzureAD\$EMail"
```

Add Microsoft Entra ID user to remote desktop group

```
$Email = ""
Add-LocalGroupMember -SID "S-1-5-32-555" -Member "AzureAD\$EMail"
```

Open Windows Control Panel pages

Printer overview

```
explorer shell:PrintersFolder
```

Turn On/Off Windows Feature

```
optionalfeatures
```

Advanced System Properties

```
SystemPropertiesAdvanced
```

PowerShell Module Management

List installed modules

```
Get-InstalledModule
```

Manage Windows File System

Add System Hardlink

```
mklink /d <C:\MyLocalFolder> <X:\MyRemoteFolder>
```

System Context

Use PSExec to run something in system context

Download the latest version of Sysinternal's PSExec: [PsExec - Sysinternals | Microsoft Learn]

```
.\PsExec.exe  -i -s cmd.exe
```

Object Handling

Get Properties of PSCustomObject

```
$<YourPS1Object>.psobject.Properties.Name
```

NTP & Time Settings

Check NTP Server settings

```
w32tm /query /configuration
```

Set Default Windows NTP Server

```
w32tm /config /manualpeerlist:time.windows.com,0x1 /syncfromflags:manual /reliable:yes /update
```

Revision #29
Created 2022-12-01 13:54:30 UTC
Updated 2026-09-24 17:21:42 UTC by Luca Noah Caprez