<#

.SYNOPSIS

Outputs user applied group policies

.DESCRIPTION

This script shows user applied group policies as shown inside the EventLog

.PARAMETER <paramName>

Non at this point

.EXAMPLE

<Script Path>\script.ps1 MyDomain\MyUser

.INPUTS

Positional argument of the Down-Level Logon Name (Domain\User)

.OUTPUTS

List of applied group policies

.LINK

See http://www.controlup.com

#>

$ErrorActionPreference = "Stop" # another way to try to stop the script in case of errors. Important for Try/Catch usage.

$username = $args[0]

# Defines to filter by Event Id '4001' and by an positional argument which 'ControlUp' provide based on context

$Query = "\*[EventData[Data[@Name='PrincipalSamName'] and (Data='$username')]] and \*[System[(EventID='4001')]]"

try {

# Gets all the events matching the criteria by $Query

[array]$Events = Get-WinEvent -ProviderName Microsoft-Windows-GroupPolicy -FilterXPath "$Query"

$ActivityId = $Events[0].ActivityId.Guid

}

catch {

Write-Host "Could not find relevant events in the Microsoft-Windows-GroupPolicy/Operational log. `nThe default log size (4MB) only supports user sessions that logged on a few hours ago. Please increase the log size to support older sessions."

Exit 1

}

# Looks for Event Id '5312' with the relevant 'Activity Id' and stores it inside a variable

$message = Get-WinEvent -ProviderName Microsoft-Windows-GroupPolicy -FilterXPath "\*[System[(EventID='5312')]]" | Where-Object{$\_.ActivityId -eq $ActivityId}

# Displays the 'Message Property'

Write-Host $message.Message