Top 10 Group Policy PowerShell Commands

In addition to the Group Policy Management Console (GPMC), Microsoft provides a set of Windows PowerShell cmdlets you can use to manage Group Policy. To use the Group Policy PowerShell cmdlets, you must have GPMC installed on the device where you will run the cmdlets. To check if the Group Policy PowerShell module is installed on a device, run the command below, which will display all the available Group Policy cmdlets available if the module is installed.

Creating a new Group Policy Object

Let's start by creating a new Group Policy object (GPO). The command below creates a new GPO called 'Netwrix PCs' and adds a comment to describe the its purpose:

```
New-GPO -Name "Netwrix PCs” -Comment "Client settings for Netwrix PCs"
```

The command creates an empty GPO with no settings. If you have starter GPOs configured in your Active Directory domain, you can create a new GPO based on their settings. The following command creates a new GPO called 'Netwrix PCs' based on the 'Windows 10 MS Security Settings' GPO:

```
New-GPO -Name "Netwrix PCs" -StarterGPOName "Windows 10 MS Security Settings"
```

You can optionally link the GPO to a domain, domain controller's organizational unit (OU) or site using piping. The command below creates a new GPO and links it to the Clients OU in the ad.contoso.com domain:

```
New-GPO -Name "Netwrix PCs" | New-GPLink -Target "ou=clients,dc=ad,dc=contoso,dc=com"
```

To unlink a GPO, use the Remove-GPLink cmdlet:

```
Remove-GPLink -Name "Netwrix PCs" -Target "ou=clients,dc=ad,dc=contoso,dc=com"
```

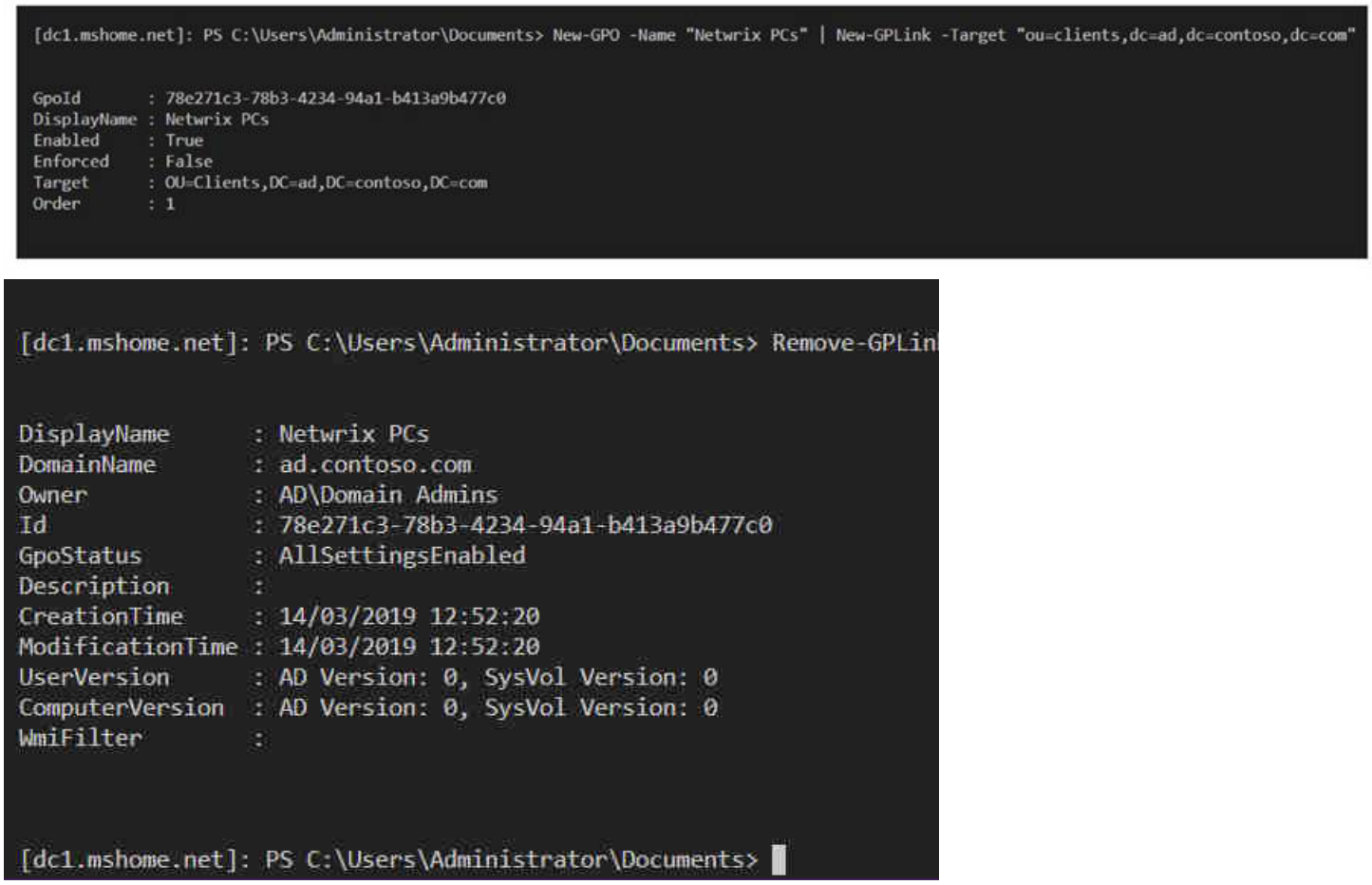

Figure 1. How to link and unlink a GPO

Getting information about a GPO

Once a GPO is created, you can use Get-GPO to return information like GPO status, creation time and last modification time:

```
Get-GPO -Name "Netwrix PCs”
```

If you want more information, pipe the object created by Get- GPO to Get-GPOReport. The script below creates an HTML report that gives information about the GPO similar to what you might see in the Group Policy Management Console:

```
Get-GPO -Name "Netwrix PCs" | Get-GPOReport -ReportType HTML -Path c:\temp\report.html
```

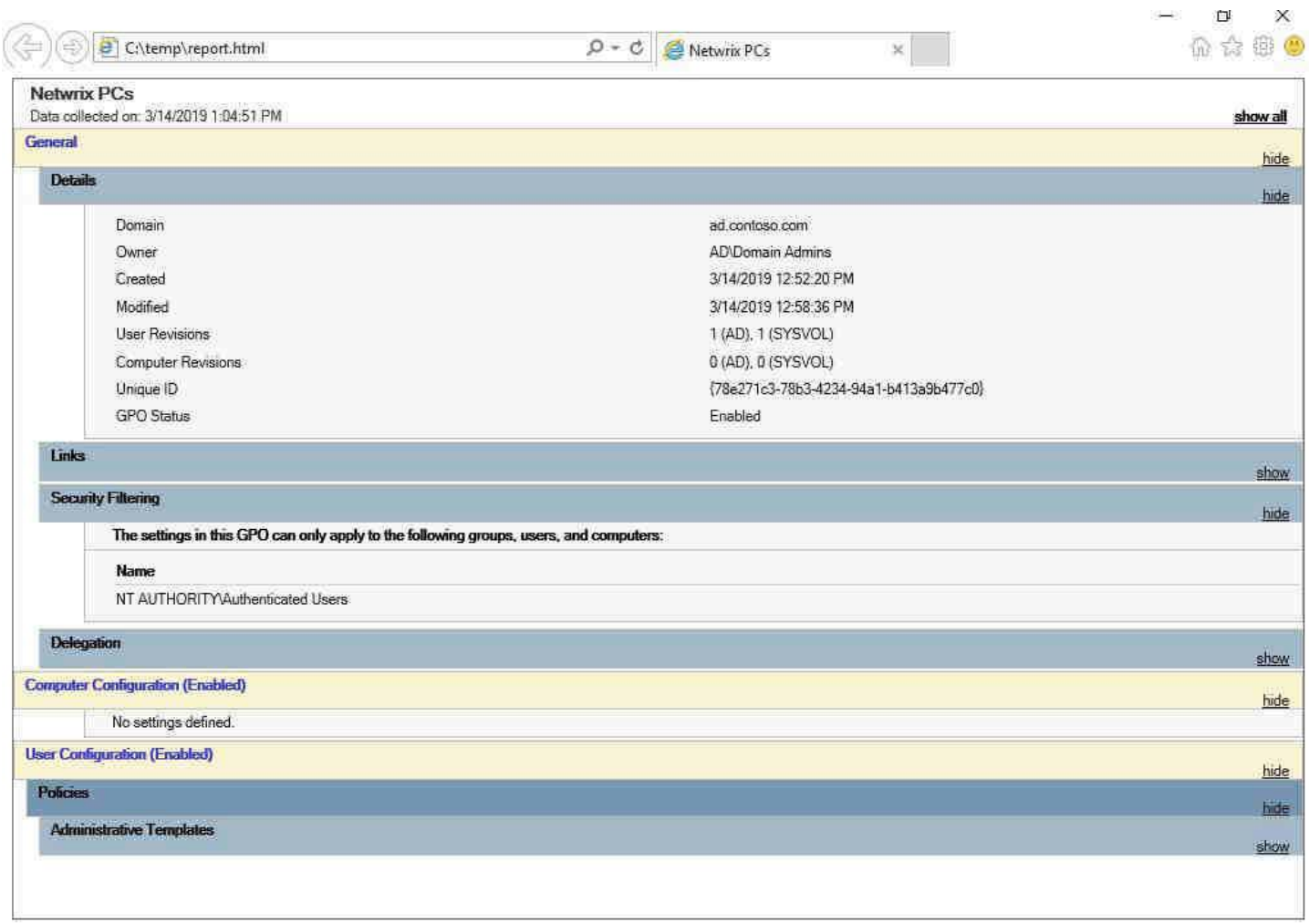

Figure 2. HTML report with detailed data about a specific GPO

Configuring Group Policy settings

If you know the location for a registry-based Group Policy setting, you can use the Set-GPRegistryValue cmdlet to configure it. Registry-based Group Policy settings are those that appear under Administrative Templates in GPMC. Set-GPRegistryValue can also be used to set registry values that are not covered by Group Policy settings. For example, if you want to configure registry settings for third-party applications that don't have an ADMX file for Group Policy, Set-GPRegistryValue is a quick way to configure the settings you need. The following command sets a screensaver timeout of 300 seconds for the logged-in user:

```
Set-GPRegistryValue -Name "Netwrix PCs” -Key "HKCU\Software\Policies\Microsoft\Windows\Con- trol Panel\Desktop" -ValueName ScreenSaveTime- Out -Type DWord -Value 300
```

You can specify either computer configuration or user configuration settings using Set- GPRegistryValue The registry path in the -Key parameter below starts with "HKCU" (which stands for "HKEY_CURRENT_USER"). If you want to configure a computer setting instead, replace "HKCU" with "HKLM" (which expands to HKEY_LOCAL_MACHINE)

To get detailed information about a registry key configured in a GPO, use Get-GPRegistryValue:

```
Get-GPRegistryValue -Name "Netwrix PCs" -Key "HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop"
```

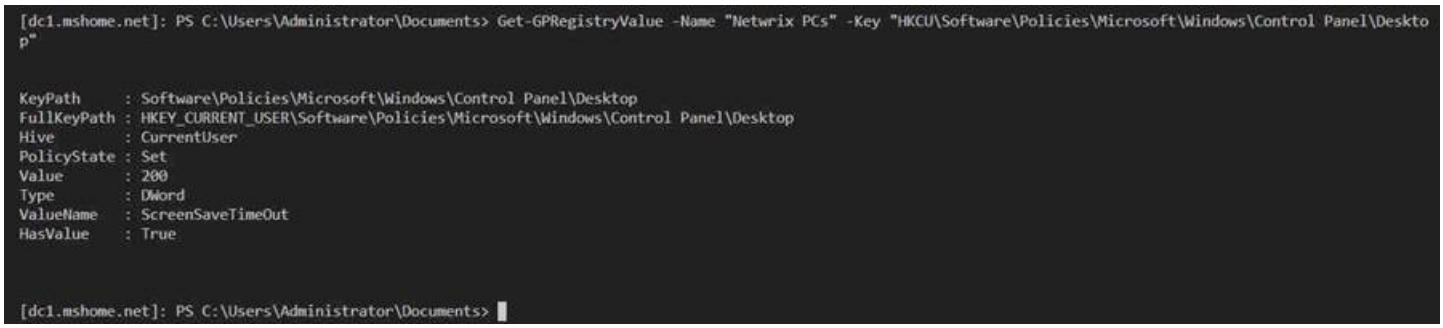

Figure 3. How to get detailed information about a registry key configured in a GPO

To remove a registry setting from a GPO, use Remove-GPRegistryValue:

```
Remove-GPRegistryValue -Name "Netwrix PCs" -Key "HKCU\Software\Policies\Microsoft\Windows\Control Panel\ Desktop" -ValueName ScreenSaveTimeOut
```

The three cmdlets above have Group Policy Preference equivalents if you decide to use Preferences instead of Policies to set registry keys: Set-GPPrefRegistryValue, Get-GPPrefRegistryValue, and Remove-GPPrefRegistryValue.

Applying Group Policy settings

Provided that your GPO is linked to a domain, OU or site, it will apply to user and computer objects below where it is linked. But if you want to force a Group Policy update on a remote server or other device, you can use Invoke-GPUpdate. Running Invoke-GPUpdate without any parameters will force an update of user and computer configuration settings on the local computer. The command below forces a Group Policy update on serverl for user configuration settings only:

```
Invoke-GPUpdate -Computer "ad\server1" -Target "User"
```

Reviewing which GPOs are applied to a user or computer

To get information about which GPOs are applied to a user or computer, you can generate a Resultant Set of Policy (RSoP) report using the Get-GPResultantSetOfPolicy cm- dlet. The command below generates a report for the computer called "dc1" and writes the results to the c:\temp directory:

```
Get-GPResultantSetOfPolicy -Computer dc1 -ReportType HTML -Path c:\temp\dc1rsop.html
```

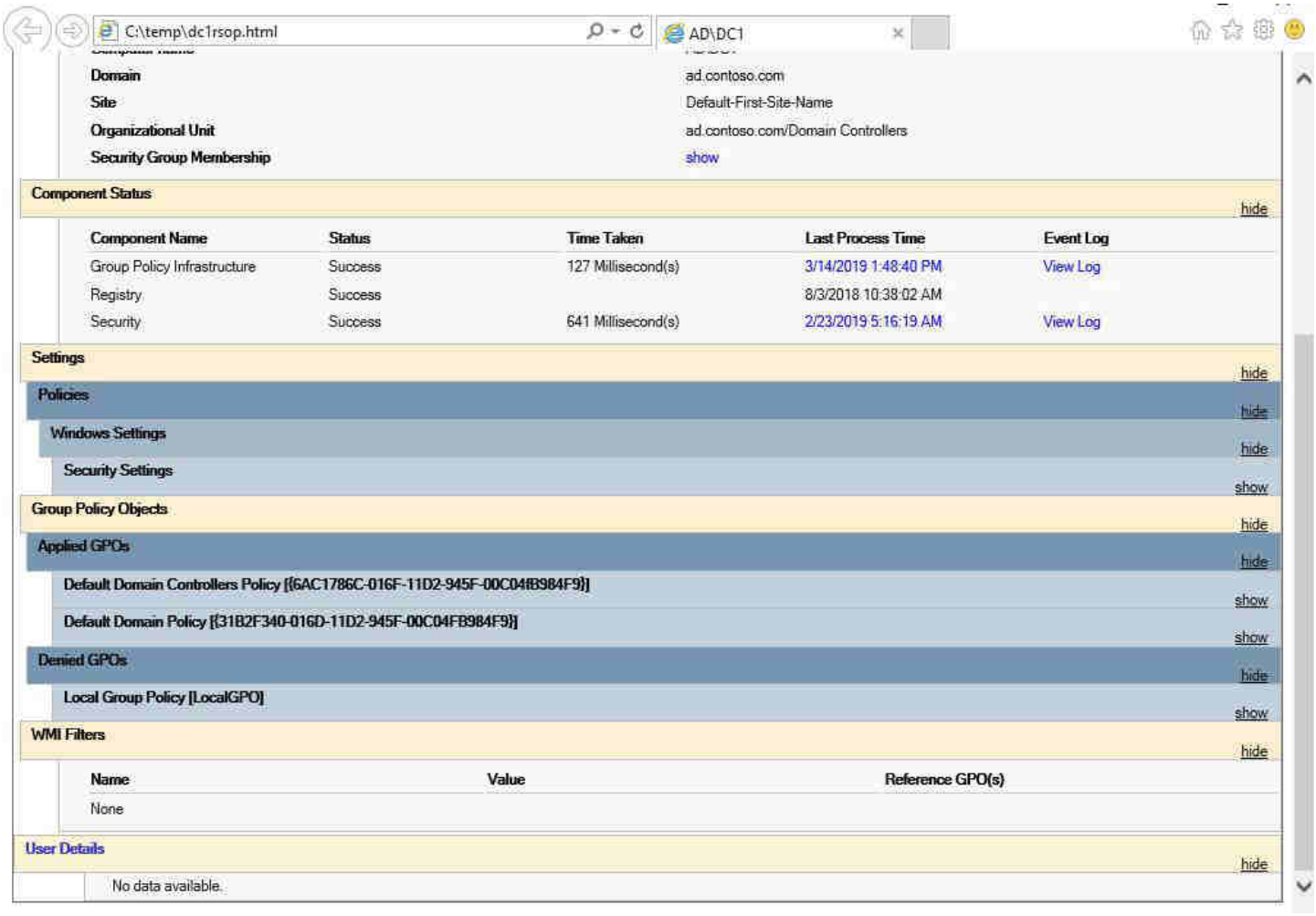

Figure 4. How to get information about which GPOs are applied to a user or computer