



Gruppenrichtlinienobjekt ID > Namen > ID

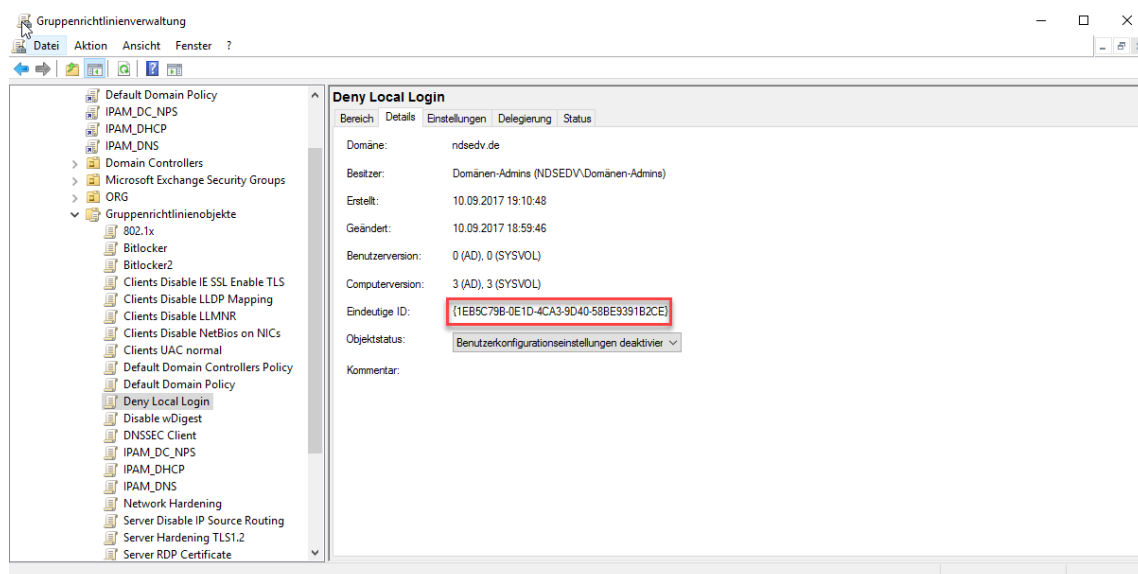
Mit diesem Oneliner können wir anhand einer „ID“ den Namen des Gruppenrichtlinienobjekts herausfinden.

```
Get-GPO -all | where {$_.id -match "1EB5C79B-0E1D-4CA3-9D40-58BE9391B2CE"}  
Get-GPO -all | where {$_.id -match "5CD089A4-51D7-402C-9872-AA02208212F1"}
```

Die IDs begegnen uns im SYSVOL Verzeichnis oder z.B. im Event-Log.

```
Administrator: Windows PowerShell ISE  
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe  
Unbenannt1.ps1* X  
1 get-gpo -all | where {$_.id -match "1EB5C79B-0E1D-4CA3-9D40-58BE9391B2CE"}  
2 get-gpo -all | where {$_.id -match "5CD089A4-51D7-402C-9872-AA02208212F1"}  
3  
  
PS C:\Windows\system32> get-gpo -all | where {$_.id -match "1EB5C79B-0E1D-4CA3-9D40-58BE9391B2CE"}  
  
DisplayName      : Deny Local Login  
DomainName       : ndsedv.de  
Owner            : NDSEDV\Domänen-Admins  
Id               : 1eb5c79b-0e1d-4ca3-9d40-58be9391b2ce  
GpoStatus        : UserSettingsDisabled  
Description      :  
CreationTime     : 10.09.2017 19:10:48  
ModificationTime: 10.09.2017 18:59:46  
UserVersion      : AD Version: 0, SysVol Version: 0  
ComputerVersion  : AD Version: 3, SysVol Version: 3  
WmiFilter        :  
  
PS C:\Windows\system32> get-gpo -all | where {$_.id -match "5CD089A4-51D7-402C-9872-AA02208212F1"}  
  
DisplayName      : Bitlocker  
DomainName       : ndsedv.de  
Owner            : NDSEDV\Domänen-Admins  
Id               : 5cd089a4-51d7-402c-9872-aa02208212f1  
GpoStatus        : AllSettingsEnabled  
Description      :  
CreationTime     : 03.12.2017 09:44:46  
ModificationTime: 03.12.2017 09:44:46  
UserVersion      : AD Version: 0, SysVol Version: 0  
ComputerVersion  : AD Version: 14, SysVol Version: 14  
WmiFilter        :  
  
PS C:\Windows\system32>
```

Hier sehen wir die Eindeutige ID zum GPO „Deny Local Login“





Gruppenrichtlinienobjekt ID > Namen > ID

Hier sehen wir die Eindeutige ID zum GPO „Bitlocker“

The screenshot shows the Group Policy Management console. The left pane displays a tree view of Group Policy Objects (GPOs) under 'Gruppenrichtlinienobjekte'. The 'Bitlocker' GPO is selected. The right pane shows the details for this GPO:

Bereich	Details	Einstellungen	Delegation	Status
Domäne:	ndsedv.de			
Besitzer:	Domänen-Admins (NDSEDV\Domänen-Admins)			
Erstellt:	03.12.2017 09:44:46			
Geändert:	03.12.2017 09:44:46			
Benutzerversion:	0 (AD), 0 (SYSVOL)			
Computerversion:	14 (AD), 14 (SYSVOL)			
Eindeutige ID:	{5CD089A4-51D7-402C-9872-AA02208212F1}			
Objektstatus:	Aktiviert			
Kommentar:				

Das Ganze lässt sich auch umgekehrt ausführen: Suche anhand des Displayname

The screenshot shows a Windows PowerShell ISE window with the following PowerShell script and output:

```
1 get-gpo -all | where {$_.Displayname -match "Deny Local Login"}
2 get-gpo -all | where {$_.id -match "{5CD089A4-51D7-402C-9872-AA02208212F1}"}
3
```

```
PS C:\Temp\backup> get-gpo -all | where {$_.Displayname -match "Deny Local Login"}

DisplayName      : Deny Local Login
DomainName       : ndsedv.de
Owner            : NDSEDV\Domänen-Admins
Id               : 1e85c79b-0e1d-4ca3-9d40-58be9391b2ce
GpoStatus        : UserSettingsDisabled
Description      :
CreationTime     : 10.09.2017 19:10:48
ModificationTime : 10.09.2017 18:59:46
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 3, SysVol Version: 3
WmiFilter        :
```



Gruppenrichtlinienobjekt ID > Namen > ID

Erstellen wir nun ein Backup aller GPO und speichern diese mit dem Displaynamen anstelle der ID ab. Dafür müssen wir nach dem Backup den Displaynamen aus der Manifest-Datei auslesen und die Ordner entsprechend umbenennen.

Erstelle das Backup und speichere diese mit der Backup-ID ab.

```
[CmdletBinding()]
param(
    [parameter()]
    [ValidateScript({Test-Path $_ -PathType Container})]
    [string]$Path = 'C:\Temp\Backup'
)
Get-GPO -All | Backup-GPO -Path $Path -Comment ('Backup wurde erstellt am: {0}' -f
(Get-Date -Format G))
$xml]$manifest = Get-Content (Join-Path $Path 'manifest.xml')
foreach ($gppBackup in $manifest.Backups.BackupInst) {
    Rename-Item -Path (Join-Path $Path $gppBackup.Id.InnerText) -NewName
($gppBackup.GPODisplayName.InnerText -replace '[:\\]', '')
}
```

Administrator: Windows PowerShell ISE

Search for name.ps1* Backup-GPO with Name.ps1 X GPO Backup.ps1

```
1 [CmdletBinding()]
2 param(
3     [parameter()]
4     [ValidateScript({Test-Path $_ -PathType Container})]
5     [string]$Path = 'C:\Temp\Backup'
6 )
7
8 Get-GPO -All | Backup-GPO -Path $Path -Comment ('Backup wurde erstellt am: {0}' -f (Get-Date -Format G))
9 [xml]$manifest = Get-Content (Join-Path $Path 'manifest.xml')
10 foreach ($gppBackup in $manifest.Backups.BackupInst) {
11     Rename-Item -Path (Join-Path $Path $gppBackup.Id.InnerText) -NewName ($gppBackup.GPODisplayName.InnerText -replace '[:\\]', '')
12 }
```

CreationTime : 27.12.2017 15:27:38
DomainName : ndsedv.de
Comment : Backup wurde erstellt am: 27.12.2017 15:27:35
DisplayName : Server RDP Certificate
GpoId : f951cc8a-e9e1-46c3-bdf1-82eeace9b17e
Id : 705833ad-766c-4c74-89ed-fd3d6bce69ea
BackupDirectory : C:\Temp\Backup
CreationTime : 27.12.2017 15:27:38
DomainName : ndsedv.de
Comment : Backup wurde erstellt am: 27.12.2017 15:27:35
DisplayName : Server Disable IP Source Routing
GpoId : fda05309-ee1e-4a87-b9f1-27744bb320e8
Id : cba91f9d-433c-4339-bfff-ed11150b6079
BackupDirectory : C:\Temp\Backup
CreationTime : 27.12.2017 15:27:38
DomainName : ndsedv.de
Comment : Backup wurde erstellt am: 27.12.2017 15:27:35

PS C:\Temp\backup>

Abgeschlossen | Ln 8 Spalte 1 | 95%



Gruppenrichtlinienobjekt ID > Namen > ID

Hier sehen wir den Inhalt des Ordners und die XML-Manifest Datei.

The screenshot shows a Windows File Explorer window titled 'Backup'. The address bar indicates the path: 'Dieser PC > Lokaler Datenträger (C:) > Temp > Backup'. The search bar contains the text '"Backup" durchsuchen'. The main pane displays a list of 23 subfolders and one file named 'manifest.xml'. The subfolders are named with GUIDs, and the 'manifest.xml' file is an XML document of 12 KB. The 'manifest.xml' file is highlighted with a blue selection bar.

Name	Änderungsdatum	Typ	Größe
{3F6B4D8B-62A8-4ACB-846A-73CD123562DE}	27.12.2017 15:27	Dateiordner	
{4D8AFFEC-EE88-4704-B996-BD5710C0EA4E}	27.12.2017 15:27	Dateiordner	
{6B96E005-C609-4965-89F7-CA7D521CEB05}	27.12.2017 15:27	Dateiordner	
{7D2EA934-1693-4E1A-BA9C-EBBF7EAB0E8}	27.12.2017 15:27	Dateiordner	
{8B90B4EB-9A78-4145-98B2-804DC09D945A}	27.12.2017 15:27	Dateiordner	
{65A06A41-3D11-4772-962C-441D0E61AB86}	27.12.2017 15:27	Dateiordner	
{85B42A45-9AEA-4355-B586-8B020C3B55E}	27.12.2017 15:27	Dateiordner	
{85E884D0-1B04-4995-82F8-C251A7EA7CA1}	27.12.2017 15:27	Dateiordner	
{98E4022B-CE07-4664-8062-A870DD28BF52}	27.12.2017 15:27	Dateiordner	
{765D9DDB-C134-40E6-A608-655F469A6550}	27.12.2017 15:27	Dateiordner	
{333231B6-C13C-4724-8BB0-90CBBE0ACC32}	27.12.2017 15:27	Dateiordner	
{705833AD-766C-4C74-89ED-FD3D6BCE69EA}	27.12.2017 15:27	Dateiordner	
{996721A8-0A16-4AB8-8BA4-54765DF8B911}	27.12.2017 15:27	Dateiordner	
{B5BFEDF5-72FA-4CCE-8561-8646254C3191}	27.12.2017 15:27	Dateiordner	
{B23F2ECE-E6F6-4D8F-BC55-23DD463824E9}	27.12.2017 15:27	Dateiordner	
{C6E9F7B7-16F0-4856-A09C-1AAC49C38694}	27.12.2017 15:27	Dateiordner	
{C7E3E525-60B4-41EF-85EA-7D7E03BBB349}	27.12.2017 15:27	Dateiordner	
{C50E1662-AF15-4675-A77C-BD9555FC4907}	27.12.2017 15:27	Dateiordner	
{C771547C-D4BD-401A-A258-1F7EB920BFDC}	27.12.2017 15:27	Dateiordner	
{CBA91F9D-433C-4339-BFFF-ED11150B6079}	27.12.2017 15:27	Dateiordner	
{DD9A2090-DBF5-4DD5-8008-C6D255AEB222}	27.12.2017 15:27	Dateiordner	
manifest.xml	27.12.2017 15:27	XML-Dokument	12 KB

Einsicht in die XML Manifest Datei:

The screenshot shows the XML content of the 'manifest.xml' file. The XML is structured as follows:

```
<?xml version="1.0" encoding="UTF-16" standalone="yes" type="text/xml" />
<ID>
  <![CDATA[
    {4D8AFFEC-EE88-4704-B996-BD5710C0EA4E}
  ]]>
</ID>
<Comment>
  <![CDATA[
    Backup wurde erstellt am: 27.12.2017 15:27:35
  ]]>
</Comment>
<GPODisplayName>
  <![CDATA[
    Bitlocker
  ]]>
</GPODisplayName>
</BackupInst>
<BackupInst>
  <GPOGuid>
    <![CDATA[
      {5cc22ba7-e1cd-43ca-8e4f-38d48ed2f40e}
    ]]>
  </GPOGuid>
  <GPODomain>
    <![CDATA[
      ndsedv.de
    ]]>
  ..
</BackupInst>
```

A red rectangular box highlights the following section of the XML:

```
<GPODisplayName>
  <![CDATA[
    Bitlocker
  ]]>
</GPODisplayName>
</BackupInst>
<BackupInst>
  <GPOGuid>
    <![CDATA[
      {5cc22ba7-e1cd-43ca-8e4f-38d48ed2f40e}
    ]]>
  </GPOGuid>
```



Gruppenrichtlinienobjekt ID > Namen > ID

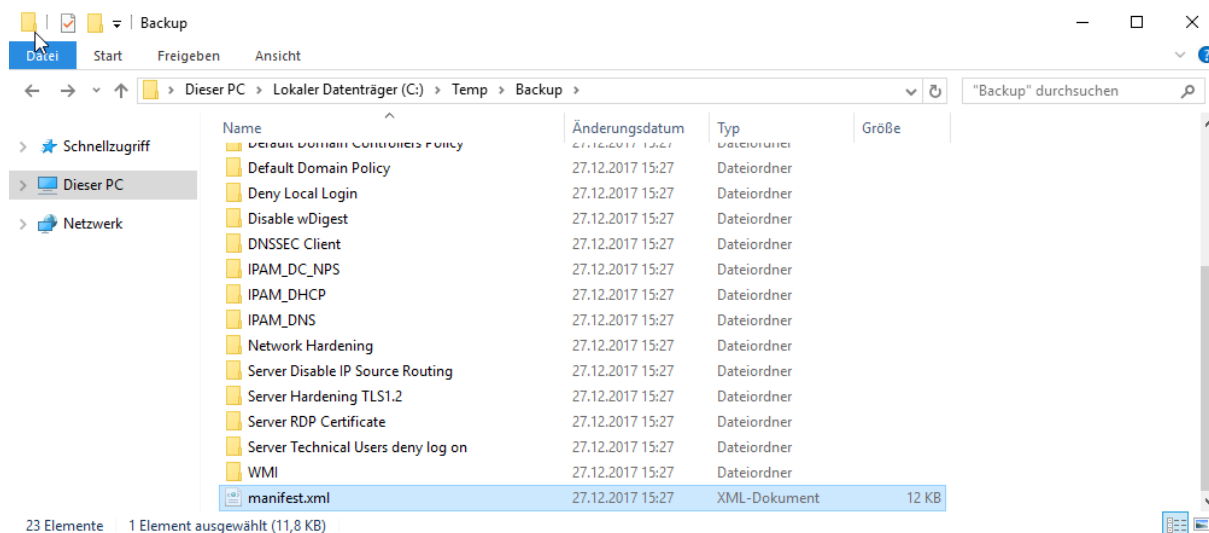
Als nächstes lesen wir die Manifest Datei ein und benennen die Ordner um:

```
1 [CmdletBinding()]
2 param(
3     [parameter()]
4     [validatescript({Test-Path $_ -PathType Container})]
5     [string]$Path = 'C:\Temp\Backup'
6 )
7
8 Get-GPO -All | Backup-GPO -Path $Path -Comment ('Backup wurde erstellt am: {0}' -f (Get-Date -Format G))
9 [xml]$manifest = Get-Content (Join-Path $Path 'manifest.xml')
10 foreach ($gpbBackup in $manifest.Backups.BackupInst) {
11     Rename-Item -Path (Join-Path $Path $gpbBackup.Id.InnerText) -NewName ($gpbBackup.GPODisplayName.InnerText -replace '[:\]', '')
12 }
```

```
PS C:\Temp\backup> [xml]$manifest = Get-Content (Join-Path $Path 'manifest.xml')
foreach ($gpbBackup in $manifest.Backups.BackupInst) {
    Rename-Item -Path (Join-Path $Path $gpbBackup.Id.InnerText) -NewName ($gpbBackup.GPODisplayName.InnerText -replace '[:\]', '')
}
PS C:\Temp\backup>
```

Abgeschlossen | Ln 9 Spalte 1 | 95%

Die Ordner wurden sauber umbenannt:





Gruppenrichtlinienobjekt ID > Namen > ID

Erstellen wir nun ein wöchentliches Backup der Richtlinien die verändert wurden, falls eine verändert wurde. Im Vorfeld sollte immer ein gesamtes Backup erstellt werden.

Führe das Skript einmal manuell aus um zu zeigen, dass das auch funktioniert.

```
$Today=(get-date).ToShortDateString()
$AllGPOs=Get-GPO -All
foreach ($GPO in $AllGPOs) {
    if ($GPO.ModificationTime.ToShortDateString() -eq $Today){
        Backup-GPO -GUID $GPO.Id -Path "C:\Temp\Backup weekly"
    }
}
```

```
Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe
Search for name.ps1* Backup GPO with Name.ps1 GPO Backup.ps1 X
1 $Today=(get-date).ToShortDateString()
2 $AllGPOs=Get-GPO -All
3 foreach ($GPO in $AllGPOs) {
4     if ($GPO.ModificationTime.ToShortDateString() -eq $Today){
5         Backup-GPO -GUID $GPO.Id -Path "C:\Temp\Backup weekly"
6     }
7 }
PS C:\Temp\Backup weekly> C:\Users\NDS\Desktop\LogOnScript\GPO Backup.ps1
DisplayName      : 802.1x
GpoId            : 604a958b-0de2-43a6-b4d8-b492087a59ce
Id              : 4bd57232-be42-4791-a997-c3a564cf03bd
BackupDirectory : C:\Temp\Backup weekly
CreationTime     : 27.12.2017 15:44:17
DomainName      : ndsedv.de
Comment         :
PS C:\Temp\Backup weekly>
Abgeschlossen | Ln 5 Spalte 61 | 95%
```



Gruppenrichtlinienobjekt ID > Namen > ID

Das Ganze sollte jetzt über den Taskplaner eingerichtet werden und voila. Natürlich lassen sich die wöchentlichen Backups auch von vorneherein mit dem Displaynamen abspeichern oder umbenennen wie in diesem Beispiel. Den Pfad kurz angepasst und die markierten Zeilen ausgeführt.

```
1 [CmdletBinding()]
2 param(
3     [parameter()]
4     [ValidateScript({Test-Path $_ -PathType Container})]
5     [string]$Path = 'C:\Temp\Backup weekly'
6 )
7
8 Get-GPO -All | Backup-GPO -Path $Path -Comment ('Backup wurde erstellt am: {0}' -f (Get-Date -Format G))
9 [xml]$manifest = Get-Content (Join-Path $Path 'manifest.xml')
10 foreach ($gpBackup in $manifest.Backups.BackupInst) {
11     Rename-Item -Path (Join-Path $Path $gpBackup.Id.InnerText) -NewName ($gpBackup.GPODisplayName.InnerText -replace '[:\V]', '')
12 }
```

```
PS C:\Temp\Backup weekly> [CmdletBinding()]
param(
[parameter()]
[ValidateScript({Test-Path $_ -PathType Container})]
[string]$Path = 'C:\Temp\Backup weekly'
)
PS C:\Temp\Backup weekly> [xml]$manifest = Get-Content (Join-Path $Path 'manifest.xml')
foreach ($gpBackup in $manifest.Backups.BackupInst) {
    Rename-Item -Path (Join-Path $Path $gpBackup.Id.InnerText) -NewName ($gpBackup.GPODisplayName.InnerText -replace '[:\V]', '')
}
PS C:\Temp\Backup weekly>
```

Wenn jedoch die Backups direkt mit dem Displaynamen abgespeichert werden sollen, dann nutzen wir dieses Skript:

```
[CmdletBinding()]
param(
    [parameter()]
    [ValidateScript({Test-Path $_ -PathType Container})]
    [string]$Path = 'C:\Temp\Backup weekly'
)
$Today=(get-date).ToShortDateString()
$AllGPOs=Get-GPO -All
foreach ($GPO in $AllGPOs) {
    if ($GPO.ModificationTime.ToShortDateString() -eq $Today){
        Backup-GPO -GUID $GPO.Id -Path "C:\Temp\Backup weekly"
    }
}

[xml]$manifest = Get-Content (Join-Path $Path 'manifest.xml')
foreach ($gpBackup in $manifest.Backups.BackupInst) {
    Rename-Item -Path (Join-Path $Path $gpBackup.Id.InnerText) -NewName
($gpBackup.GPODisplayName.InnerText -replace '[:\V]', '')
}
```