

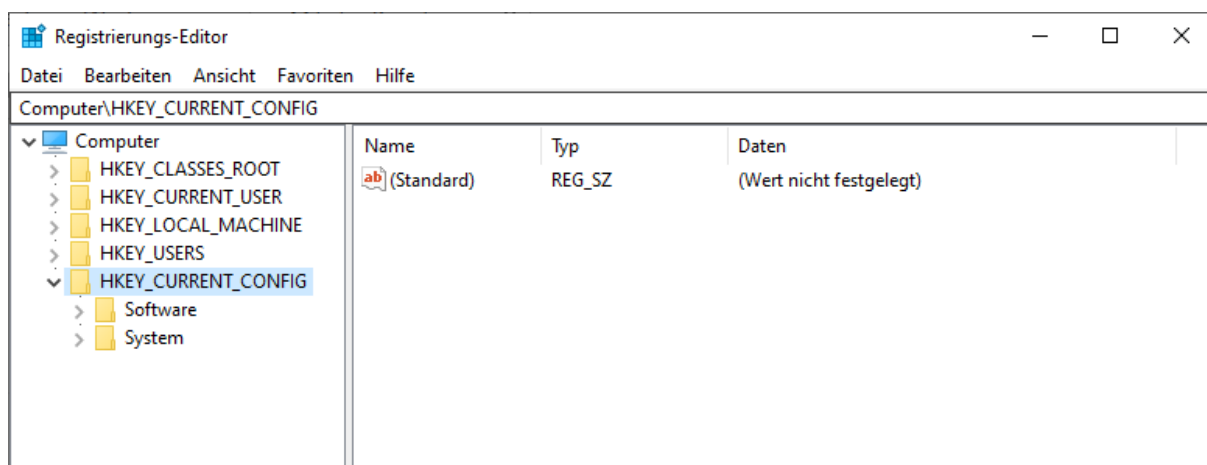


Umgang mit der Registry



Mit Hilfe der Powershell ist das Einsehen und Bearbeiten der Registry recht einfach. In dieser Doku zeige ich einige Beispiele, wie wir zu definierten Hives gelangen, und die gesetzten Werte auslesen bzw. verändern.

Der Aufbau der Registry ähnelt dem des Dateisystems. Statt Ordner und Unterordner gibt es in der Registry Schlüssel und Unterschlüssel, statt Dateien sind es hier Werte.



HKEY_CLASSES_ROOT enthält zumeist Dateinamenserweiterungen und die dazugehörigen Programmverknüpfungen. Die meisten Schlüssel verweisen auf eine Class-ID (CLSID), zu dem ein gleichnamiger Schlüssel unter "HKEY_CLASSES_ROOT\Clsid\" existiert. Dabei handelt es sich um Funktionen meist in DLL-Dateien, die Windows oder eine Anwendung für die interne Nutzung registriert haben.

Unter **HKEY_CURRENT_USER** sind alle Einstellungen des aktuell angemeldeten Benutzers gespeichert. Unterhalb von „HKEY_CURRENT_USER\SOFTWARE“ legen Anwendungen bei der Installation und Konfiguration ihre Daten ab. Die Windows-Konfiguration ist unter "HKEY_CURRENT_USER\SOFTWARE\Microsoft" zu finden.



Umgang mit der Registry

HKEY_LOCAL_MACHINE speichert systemspezifische Einstellungen für Windows und Anwendungen. Diese können in der Regel durch einen Administrator geändert werden und gelten für alle Benutzer. Im Zweig unter "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet" finden wir die Einstellungen für Dienste und Treiber.

HKEY_USERS enthält Schlüssel mit Benutzer-IDs.

- S-1-5-18 ist der Benutzer "System"
- S-1-5-19 gehört zu "NT Authority" und
- S-1-5-20 zu "Network Service".

Die beiden anderen IDs sind die des aktuellen Benutzers und entsprechen dem Inhalt von "HKEY_CURRENT_USER" beziehungsweise "HKEY_CLASSES_ROOT".

HKEY_CURRENT_CONFIG ist eine Verlinkung zu den Schlüsseln unterhalb von "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Hardware Profiles\Current\". Dadurch erreicht man für jegliche Anwendungen, einen kürzeren Pfad, um auf die Werte zu greifen zu können.

Fangen wir damit an, dass wir uns zuerst die beiden wichtigsten Pfade ansehen. Navigiert wird in der Registry ähnlich wie im Windows Explorer. Das sind die Pfade HKEY_LOCAL_MACHINE (HKLM) und HKEY_CURRENT_USER (HKCU).

Wir öffnen die Powershell mit administrativen Rechten und setzen folgende Befehle ab:

Get-PSDrive -Name HKLM

Get-PSDrive -Name HKCU

```
Administrator: Windows PowerShell

PS C:\Windows\system32> Get-PSDrive -Name HKLM 1
Name           Used (GB)  Free (GB) Provider      Root           CurrentLocation
-----
HKLM            0.00      16.00     Registry      HKEY_LOCAL_MACHINE
HKLM            0.00      16.00     Registry      HKEY_LOCAL_MACHINE

PS C:\Windows\system32> Get-PSDrive -Name HKCU 2
Name           Used (GB)  Free (GB) Provider      Root           CurrentLocation
-----
HKCU            0.00      16.00     Registry      HKEY_CURRENT_USER
HKCU            0.00      16.00     Registry      HKEY_CURRENT_USER

PS C:\Windows\system32>
```



Umgang mit der Registry

Mit diesen 3 Befehlen navigieren wir schon etwas tiefer in die Untiefen der Verzweigungen.

Get-PSDrive -Name HKLM

cd HKLM:

dir system

```
Auswählen Administrator: Windows PowerShell
PS C:\Windows\system32> Get-PSDrive -Name HKLM
Name            Used (GB)  Free (GB)  Provider      Root              CurrentLocation
-----
HKLM             0.00      0.00      Registry      HKEY_LOCAL_MACHINE

PS C:\Windows\system32> cd HKLM:\
PS HKLM:\> dir system

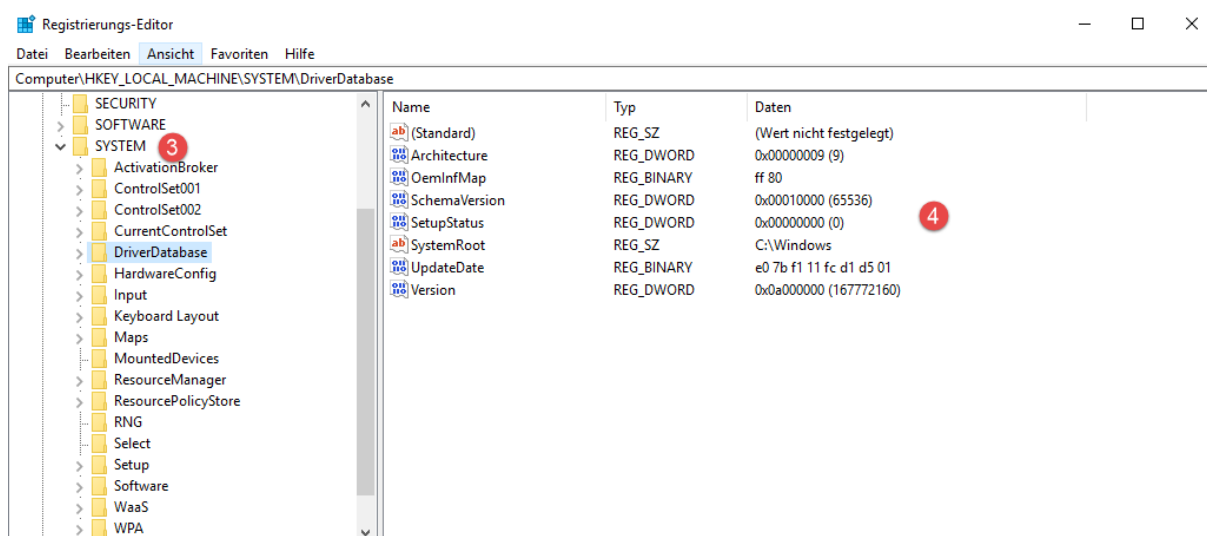
Hive: HKEY_LOCAL_MACHINE\system

Name            Property
-----
ActivationBroker
ControlSet001
ControlSet002
DriverDatabase
                Version       : 167772160
                SchemaVersion : 65536
                Architecture : 9
                UpdateDate  : {224, 123, 241, 17...}
                SetupStatus  : 0
                SystemRoot   : C:\Windows
                OemInfMap    : {255, 128}
                LastConfig   : {ba634d56-c7a9-ac56-8b0b-704c5c2c495c}
                LastId      : 0
HardwareConfig
Input
Keyboard Layout
Maps
MountedDevices
                \DosDevices\C:           : {68, 77, 73, 79...}
                \??\Volume{2574ba73-1ea7-11ea-a46f-806e6f6e6963} : {92, 0, 63, 0...}
                \??\Volume{2574ba74-1ea7-11ea-a46f-806e6f6e6963} : {92, 0, 63, 0...}
                \DosDevices\A:       : {92, 0, 63, 0...}
                \DosDevices\D:       : {92, 0, 63, 0...}
ResourceManager
                CustomizationFlags       : 16
                MaxPriorityToReleaseWhilePausing : 37
                TerminalResourceSetPriority : 32
ResourcePolicyStore
RNG
                ExternalEntropyCount : 1
                Seed                   : {82, 117, 110, 110...}
Select
                Current       : 1
                Default       : 1
                Failed        : 0
                LastKnownGood : 2
Setup
                CmdLine       :
                OOBEInProgress : 0
                OsloaderPath  : \
                RespecializeCmdLine : Sysprep/sysprep.exe /respecialize /quiet
                RestartSetup  : 0
                SetupPhase    : 0
                SetupSupported : 1
                SetupType     : 0
                SystemPartition : \Device\HarddiskVolume1
                SystemSetupInProgress : 0
                CloneTag       : {Sat Sep 15 00:21:38 2018}
                WorkingDirectory : C:\Windows\Panther
Software
WaaS
WPA
CurrentControlSet

PS HKLM:\>
```

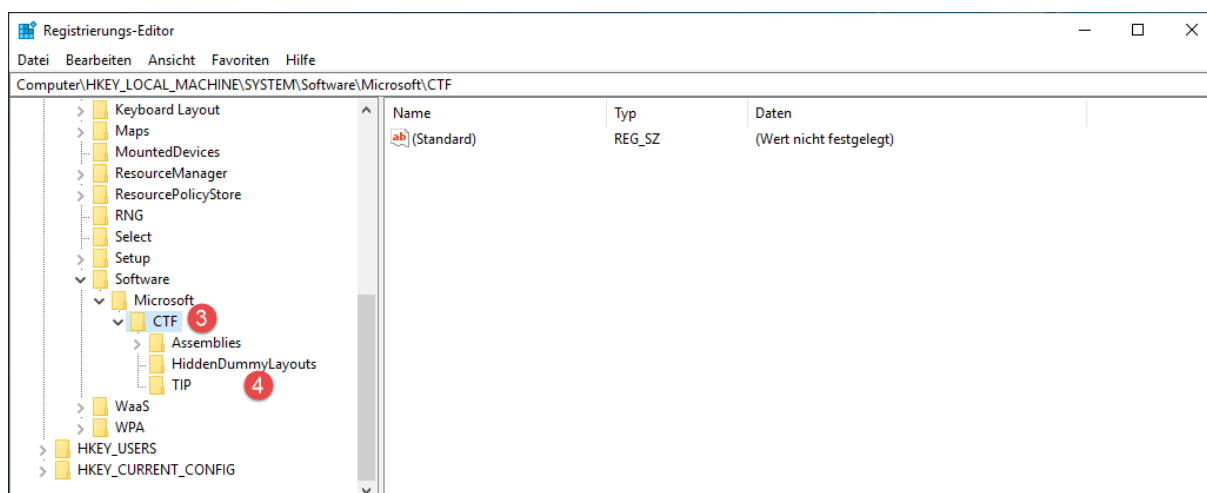
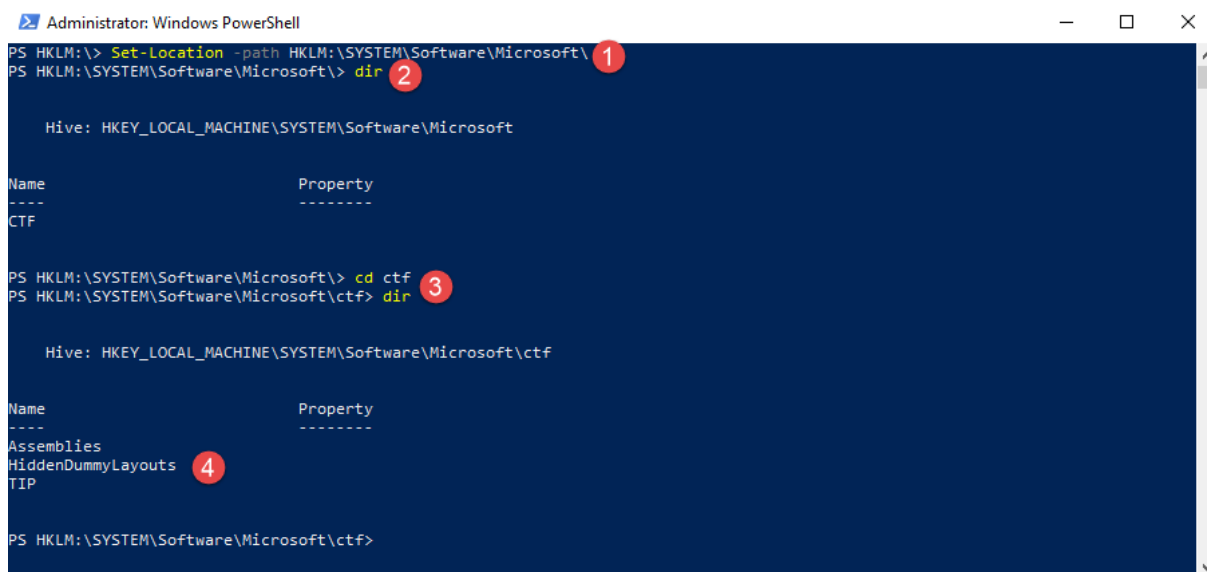


Umgang mit der Registry



Es ist auch möglich direkt zu einem Pfad zu springen und zwar über...

```
Set-Location -path HKLM:\SYSTEM\Software\Microsoft\  
cd ctf  
dir
```





Umgang mit der Registry

Mit **cd** navigieren wir vorwärts und mit **cd..** rückwärts mit **cd /** springen wir zurück zum Stammverzeichnis

```
Administrator: Windows PowerShell
PS HKLM:\> cd system
PS HKLM:\system> cd .\Software\
```

Mit diesem Befehl lassen wir uns sofern vorhanden alle Properties unter dem Schlüssel Software anzeigen.

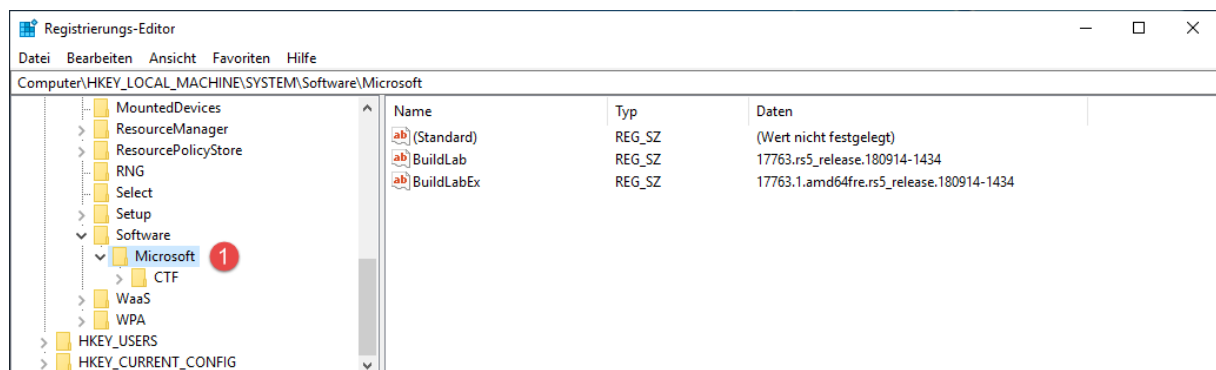
Get-ChildItem

```
Administrator: Windows PowerShell
PS HKLM:\SYSTEM\Software> Get-ChildItem 1

Hive: HKEY_LOCAL_MACHINE\SYSTEM\Software

Name                Property
----                -
Microsoft            BuildLab      : 17763.rs5_release.180914-1434
                    BuildLabEx   : 17763.1.amd64fre.rs5_release.180914-1434

PS HKLM:\SYSTEM\Software>
```



```
Administrator: Windows PowerShell
PS HKLM:\SOFTWARE\Policies\Microsoft\> Get-ChildItem 1

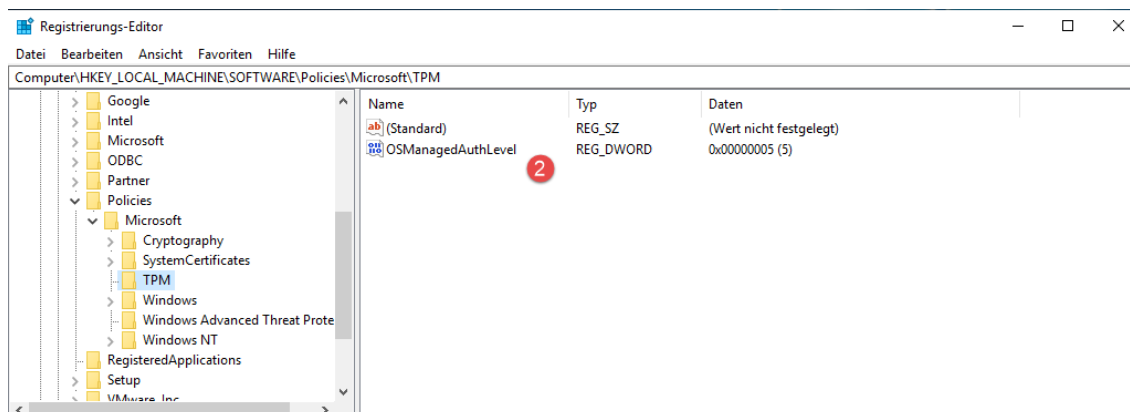
Hive: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft

Name                Property
----                -
Cryptography        OSManagedAuthLevel : 5 2
SystemCertificates
TPM
Windows
Windows Advanced Threat
Protection
Windows NT

PS HKLM:\SOFTWARE\Policies\Microsoft\>
```

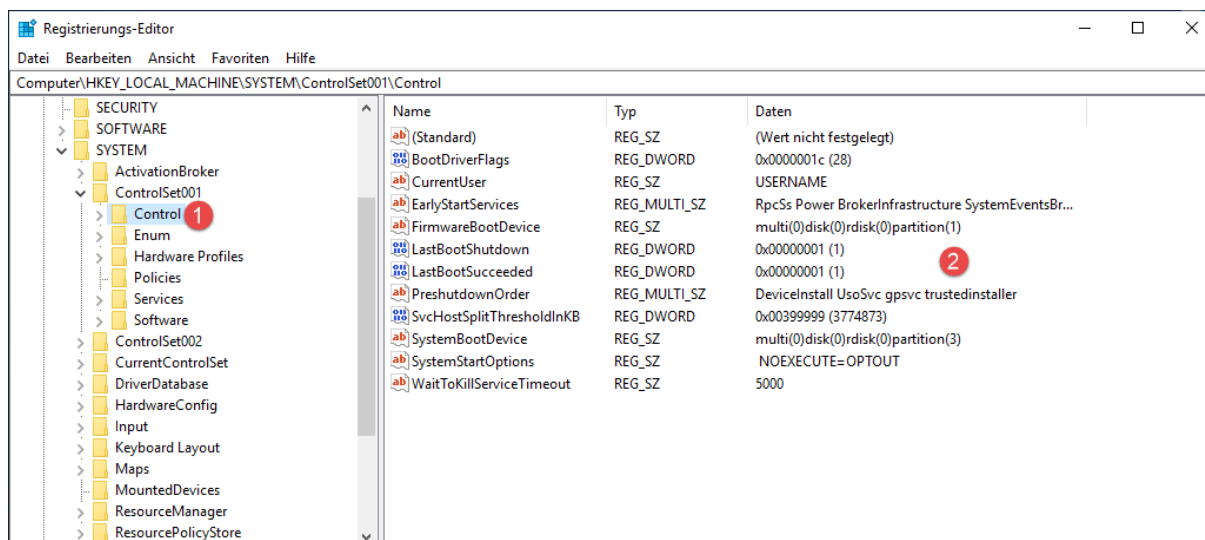
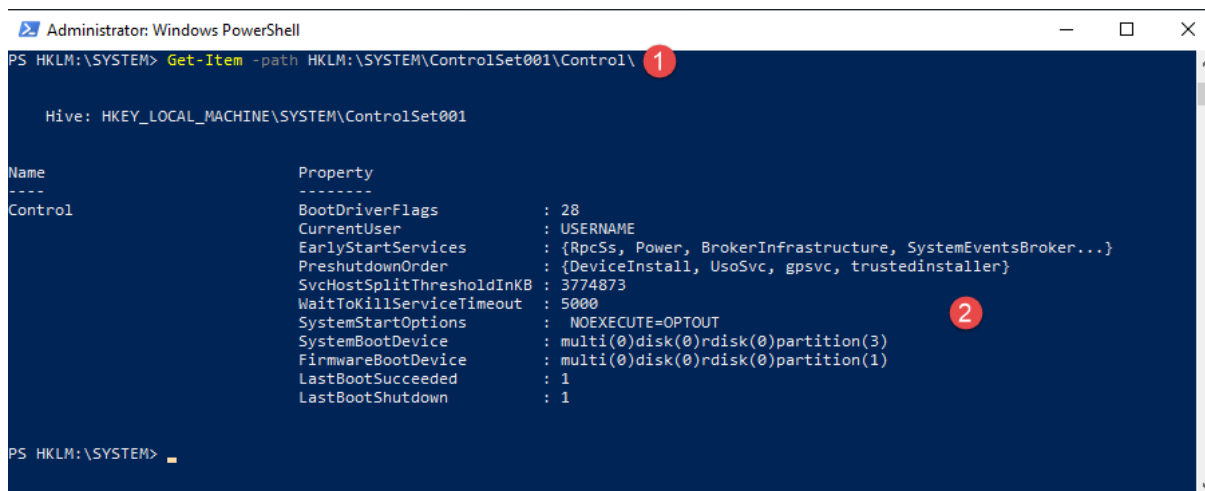


Umgang mit der Registry



Mit diesem Befehl lassen wir uns die Properties gezielt ab unter dem Schlüssel Control anzeigen.

Get-Item -path HKLM:\SYSTEM\ControlSet001\Control





Umgang mit der Registry

Schauen wir uns gleich an, wie wir die Parameter von Registry-Einträgen ändern können. Aber zuerst legen wir welche an. Und zwar vom TYP REG_SZ unterhalb von SOFTWARE.

New-ItemProperty -path 'HKLM:\SOFTWARE\' -name DerWindowsPapst1

New-ItemProperty -path 'HKLM:\SOFTWARE\' -name DerWindowsPapst2 -Value "TEST"

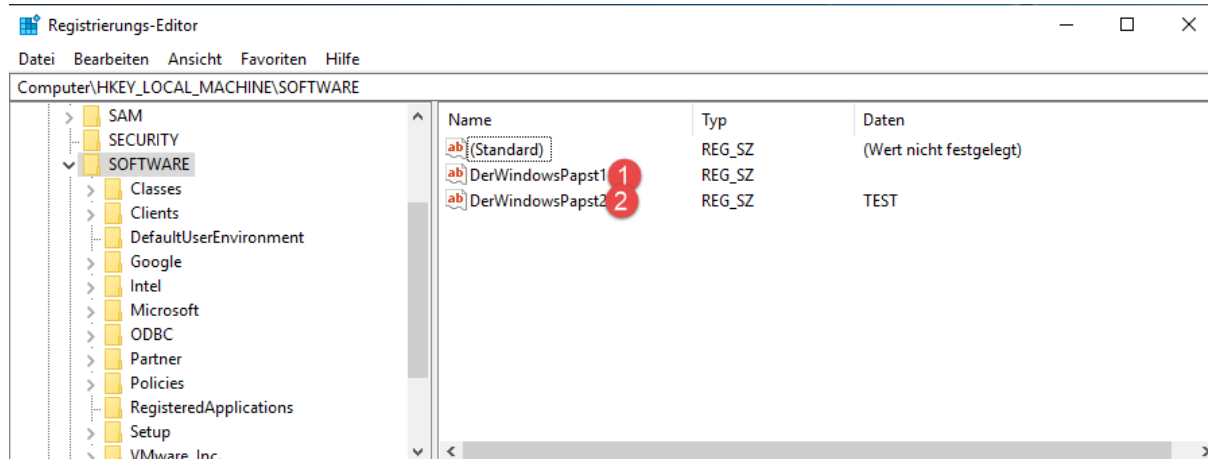
```
Administrator: Windows PowerShell
PS HKLM:\SOFTWARE\Policies\Microsoft\> New-ItemProperty -path 'HKLM:\SOFTWARE\' -name DerWindowsPapst1 1

DerWindowsPapst1 :
PSPath           : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\
PSParentPath     : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE
PSChildName      : SOFTWARE
PSDrive          : HKLM
PSProvider       : Microsoft.PowerShell.Core\Registry

PS HKLM:\SOFTWARE\Policies\Microsoft\> New-ItemProperty -path 'HKLM:\SOFTWARE\' -name DerWindowsPapst2 -Value "TEST" 2

DerWindowsPapst2 : TEST
PSPath           : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\
PSParentPath     : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE
PSChildName      : SOFTWARE
PSDrive          : HKLM
PSProvider       : Microsoft.PowerShell.Core\Registry

PS HKLM:\SOFTWARE\Policies\Microsoft\>
```



Als nächstes legen wir einen neuen Schlüssel an und darunter einen neuen Eintrag vom TYP DWORD.

New-Item -path "HKLM:\Software\DerWindowsPapst1"

```
Administrator: Windows PowerShell
PS HKLM:\SOFTWARE\Policies\Microsoft\> New-Item -path "HKLM:\Software\DerWindowsPapst1" 1

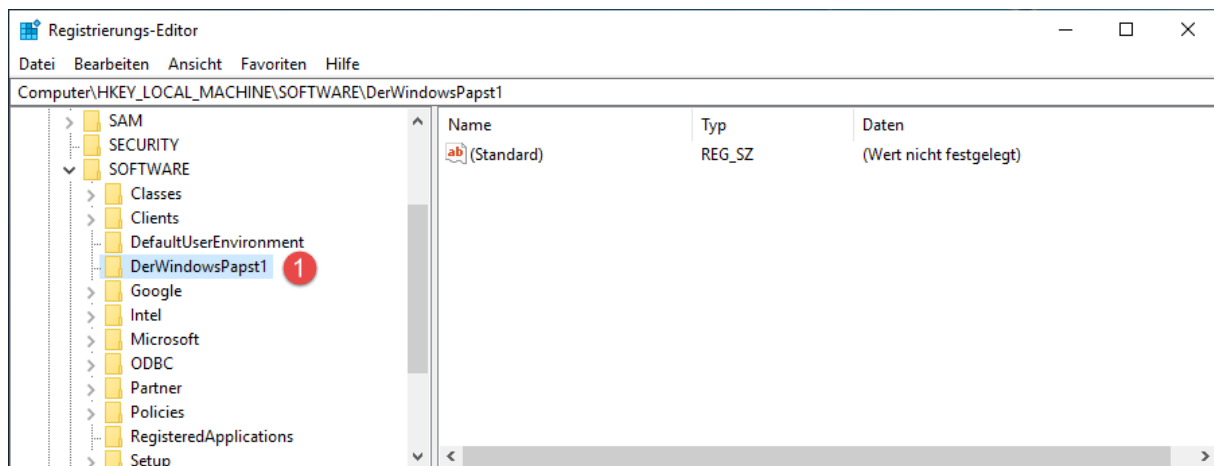
Hive: HKEY_LOCAL_MACHINE\Software

Name      Property
----      -
DerWindowsPapst1

PS HKLM:\SOFTWARE\Policies\Microsoft\>
```

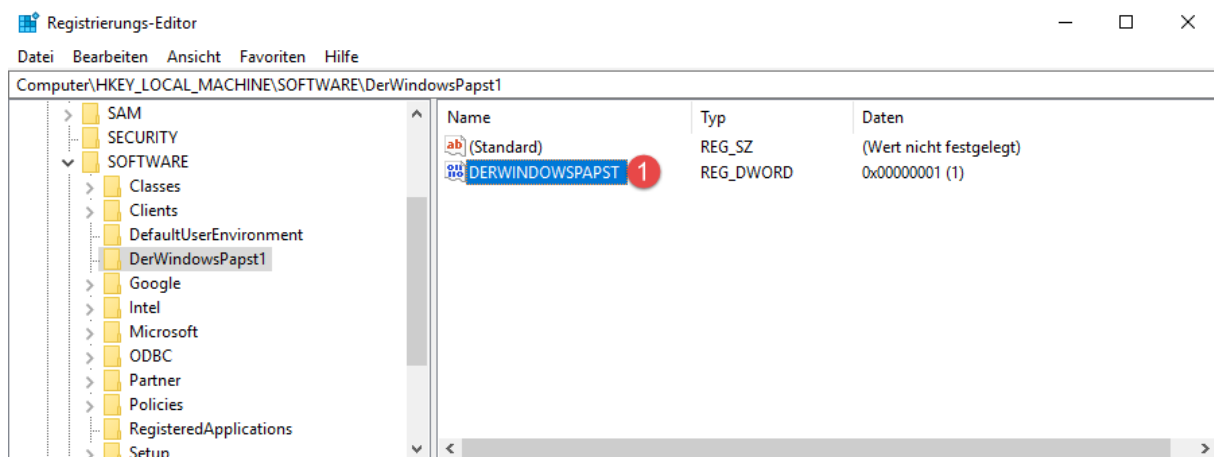


Umgang mit der Registry



Legen wir nun ein ItemProperty unterhalb des neuen Schlüssels „DerWindowsPapst1“ an.

```
New-ItemProperty -path "HKLM:\Software\DerWindowsPapst1" -name  
DERWINDOWSPAPST -PropertyType DWORD -value 1
```



Weitere Beispiele zu den Typen (String, DWORD, MultiString)

```
New-ItemProperty -path "HKLM:\Software\DerWindowsPapst1" -name  
DERWINDOWSPAPST -PropertyType DWORD -value 1
```

```
New-ItemProperty -path "HKLM:\Software\DerWindowsPapst1" -name  
DERWINDOWSPAPST1 -PropertyType String -value "1"
```

```
New-ItemProperty -path "HKLM:\Software\DerWindowsPapst1" -name  
DERWINDOWSPAPST2 -PropertyType MultiString -value "Der-Windows-Papst","1","2"
```

PowerShell Type	Registry Type
Binary	REG_BINARY
DWord	REG_DWORD
ExpandString	REG_EXPAND_SZ
MultiString	REG_MULTI_SZ
None	-
QWord	REG_QWORD
String	REG_SZ
Unknown	-

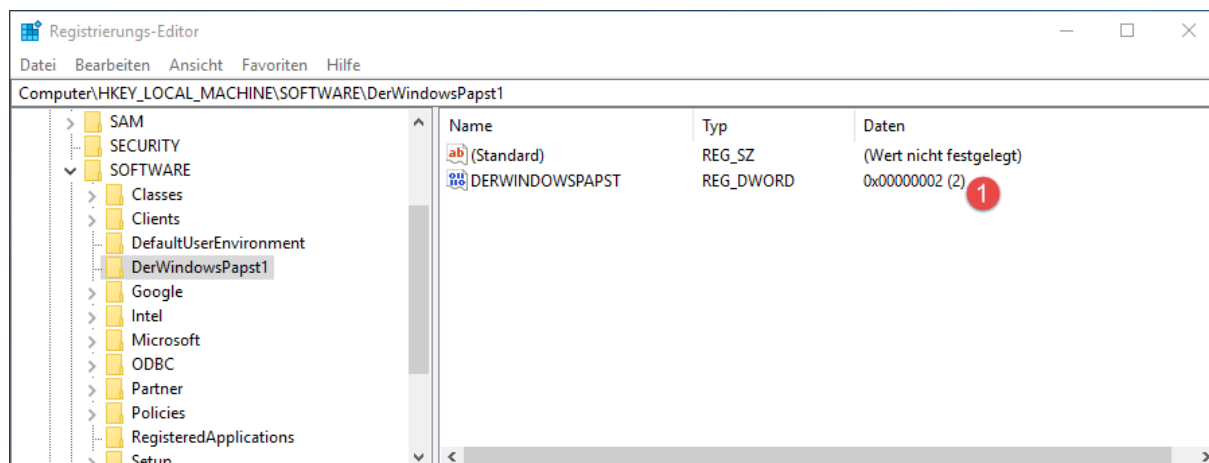


Umgang mit der Registry

Gehen wir nun über und ändern den Wert des Eintrags von 1 auf 2.

Set-ItemProperty -Path "HKLM:\Software\DerWindowsPapst1" DERWINDOWSPAPST -Value 2 -Force

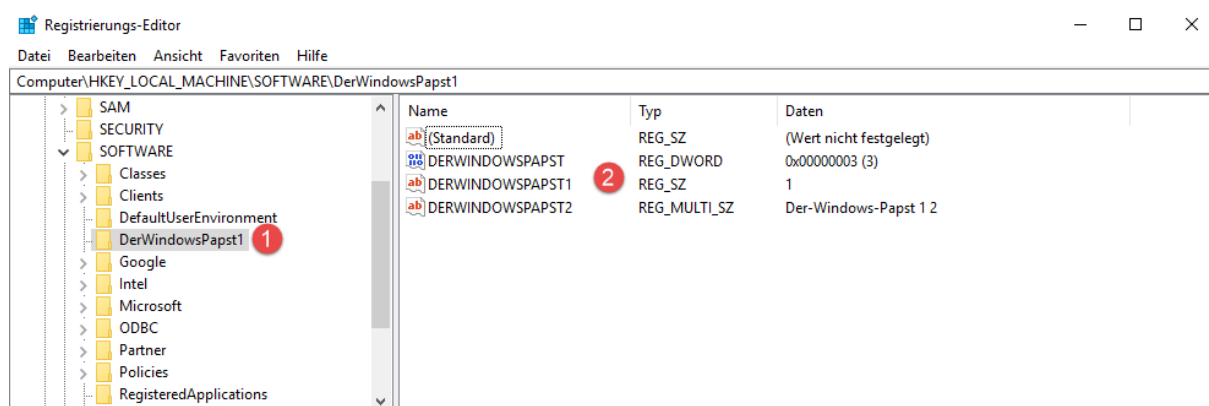
```
Administrator: Windows PowerShell
PS HKLM:\SOFTWARE\Policies\Microsoft\> Set-ItemProperty -Path "HKLM:\Software\DerWindowsPapst1" DERWINDOWSPAPST -Value 2 -Force
PS HKLM:\SOFTWARE\Policies\Microsoft\>
```



Prüfen wir doch mal eben, welche Einträge wir bereits angelegt haben.

Get-ItemProperty -Path "HKLM:\Software\DerWindowsPapst1"

```
Administrator: Windows PowerShell
PS HKLM:\SOFTWARE\Policies\Microsoft\> Get-ItemProperty -Path "HKLM:\Software\DerWindowsPapst1"
DERWINDOWSPAPST : 3
DERWINDOWSPAPST1 : 1
DERWINDOWSPAPST2 : {Der-Windows-Papst, 1, 2}
PSPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Software\DerWindowsPapst1
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Software
PSChildName : DerWindowsPapst1
PSDrive : HKLM
PSProvider : Microsoft.PowerShell.Core\Registry
PS HKLM:\SOFTWARE\Policies\Microsoft\>
```





Umgang mit der Registry

Fangen wir an Einträge zu löschen.

Remove-ItemProperty -Path "HKLM:\Software\DerWindowsPapst1" -Name "DERWINDOWSPAPST"

A screenshot of a Windows PowerShell window running as Administrator. The command prompt shows the command: `Remove-ItemProperty -Path "HKLM:\Software\DerWindowsPapst1" -Name "DERWINDOWSPAPST"`. A red circle with the number '1' is next to the command.

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
DERWINDOWSPAPST1	REG_SZ	1
DERWINDOWSPAPST2	REG_MULTI_SZ	Der-Windows-Papst 1 2

Jetzt löschen wir den ganzen Schlüssel „DerWindowsPapst1“

Remove-Item -Path "HKLM:\Software\DerWindowsPapst1" -Recurse

A screenshot of a Windows PowerShell window running as Administrator. The command prompt shows the command: `Remove-Item -Path "HKLM:\Software\DerWindowsPapst1" -Recurse`.

Damit es weitergehen kann, lege ich den Schlüssel wieder an, wir sind ja noch nicht fertig.

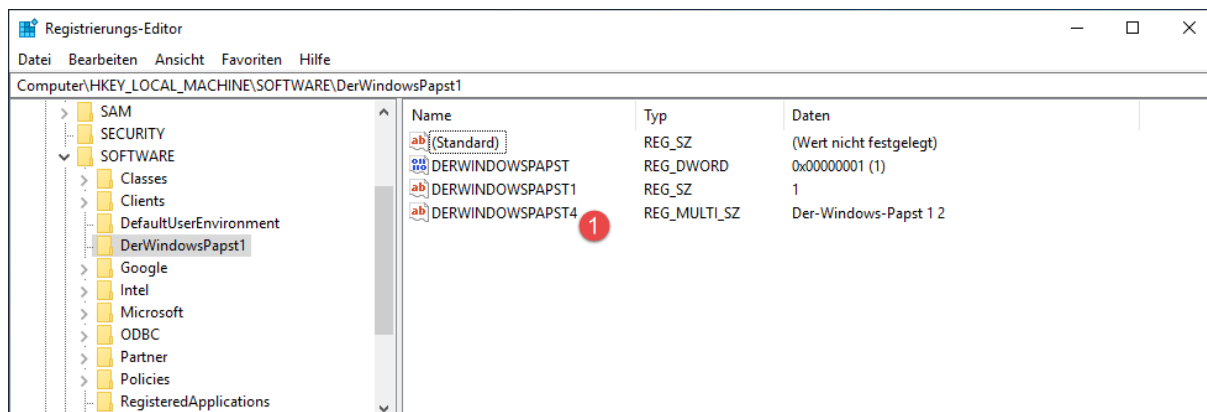
Jetzt benennen wir einen Eintrag um. Und zwar DERWINDOWSPAPST2 in DERWINDOWSPAPST4

Rename-ItemProperty -Path "HKLM:\Software\DerWindowsPapst1" -Name DERWINDOWSPAPST2 -NewName DERWINDOWSPAPST4

A screenshot of a Windows PowerShell window running as Administrator. The command prompt shows the command: `Rename-ItemProperty -Path "HKLM:\Software\DerWindowsPapst1" -Name DERWINDOWSPAPST2 -NewName DERWINDOWSPAPST4`. A red circle with the number '1' is next to the command.



Umgang mit der Registry



Zum Abschluss werden wir einen ganzen Schlüssel verschieben.

Move-Item "HKLM:\Software\DerWindowsPapst1*" "HKLM:\Software\Google"

