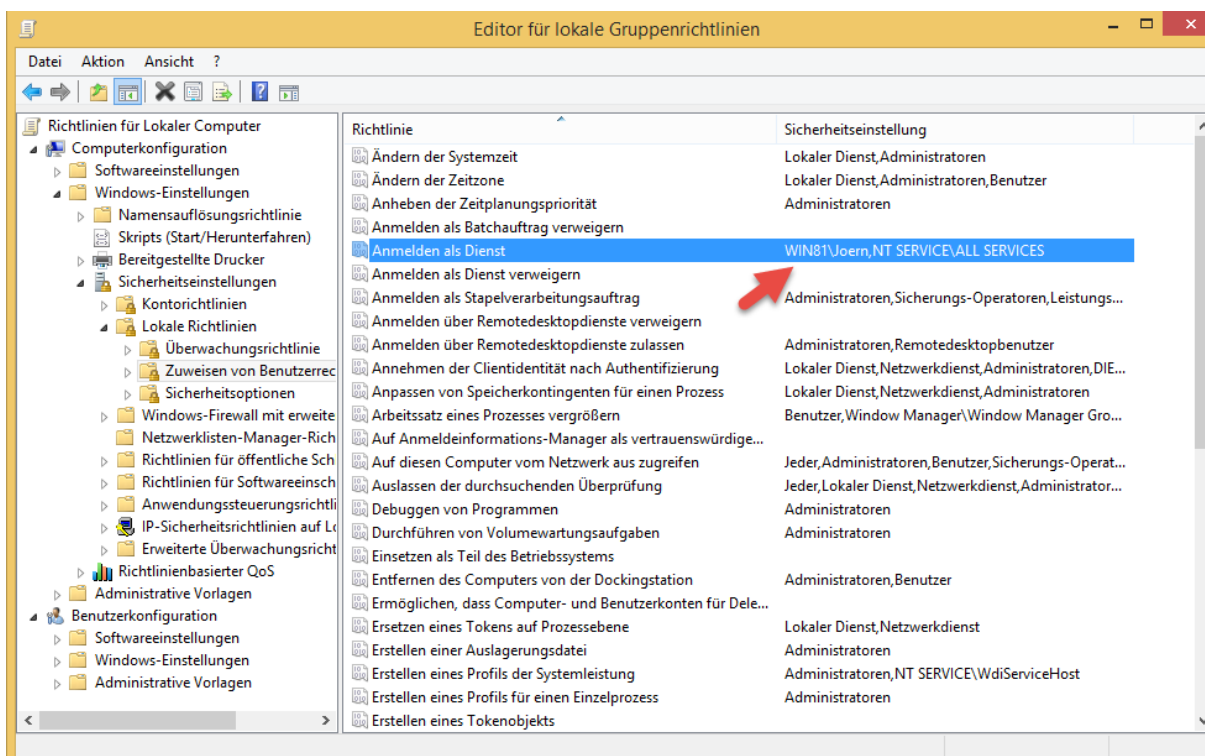




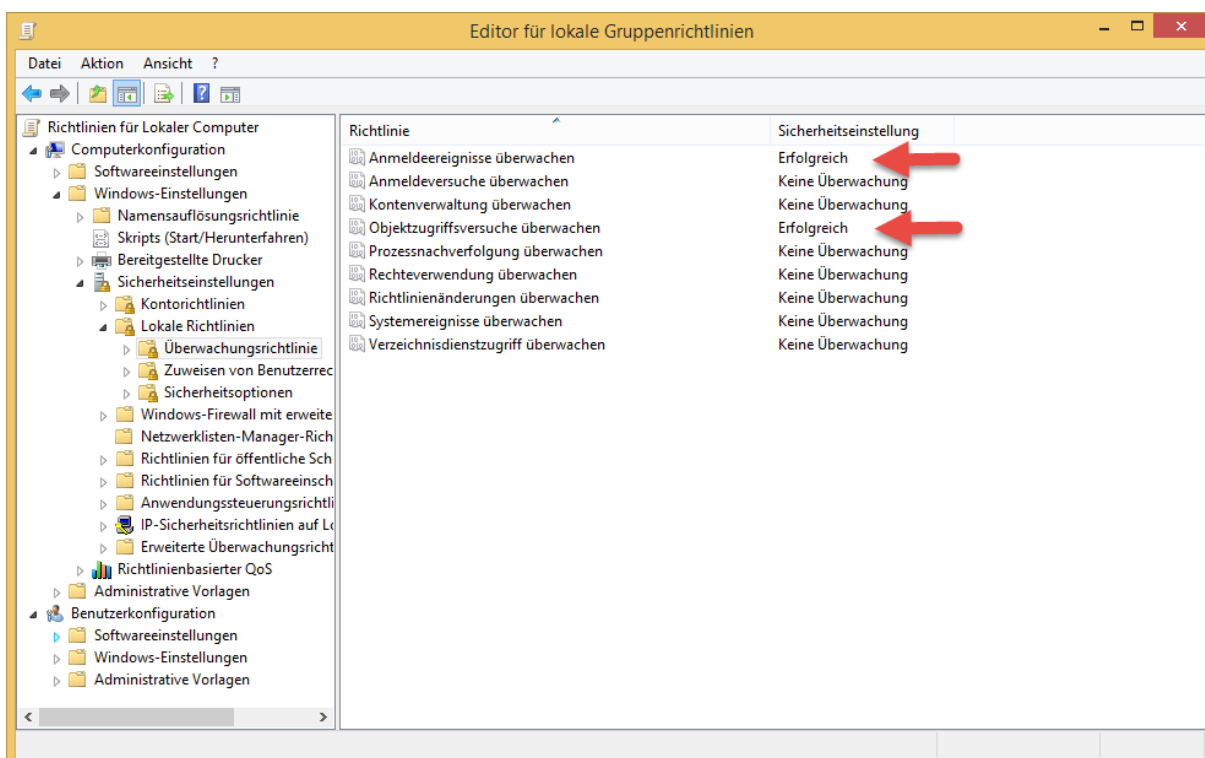
Standard Sicherheitsrichtlinien zurücksetzen

In diesem Dokument möchte ich beschreiben, wie angewandte Sicherheitsrichtlinien auf einem Client System zurückgesetzt werden können. Der Grund dafür kann unterschiedlich sein; Domänenbeitritt nicht möglich, Dateisystem oder Registry falsch berechtigt

Konfigurierte Sicherheitsrichtlinie als Beispiel:



Konfigurierte Überwachungsrichtlinie als Beispiel:

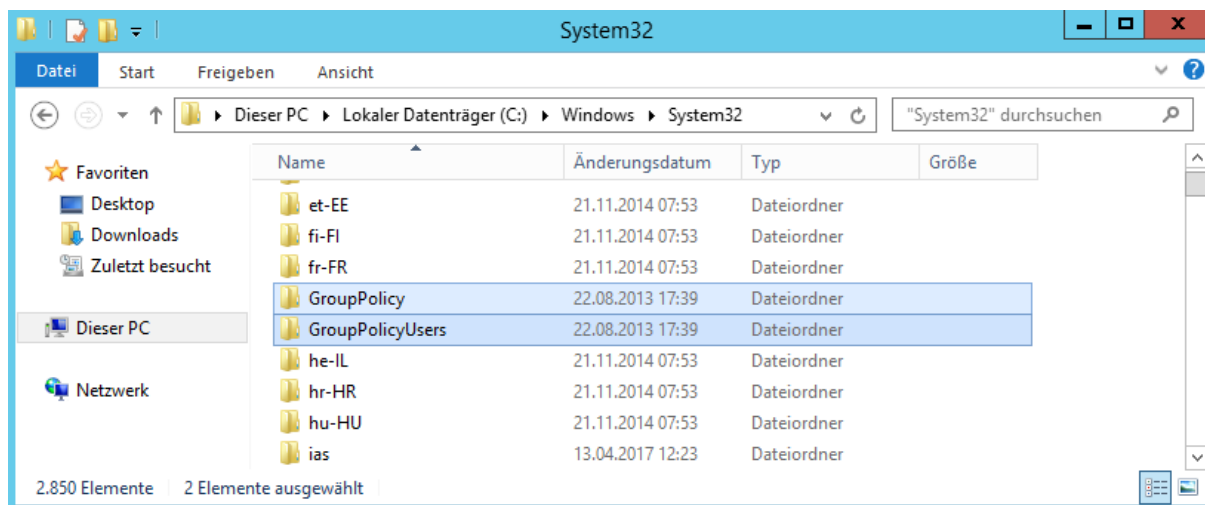




Standard Sicherheitsrichtlinien zurücksetzen

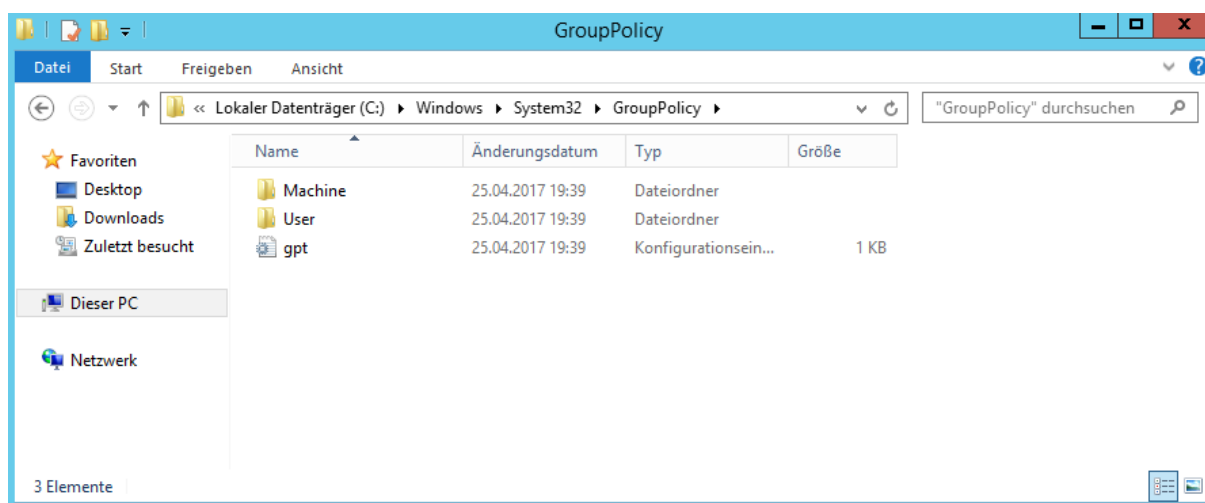
Der Speicherort der Einstellungen im Dateisystem ist:

C:\Windows\System32\GroupPolicy



Speicherort in der Registry:

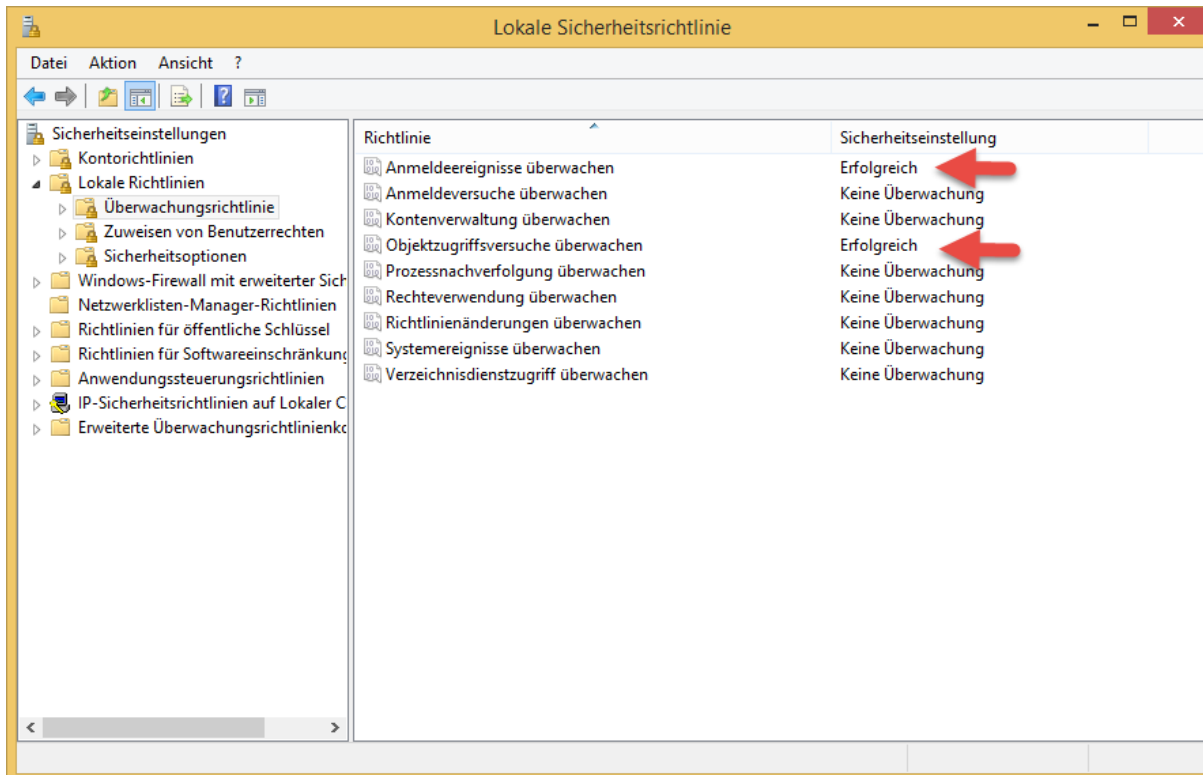
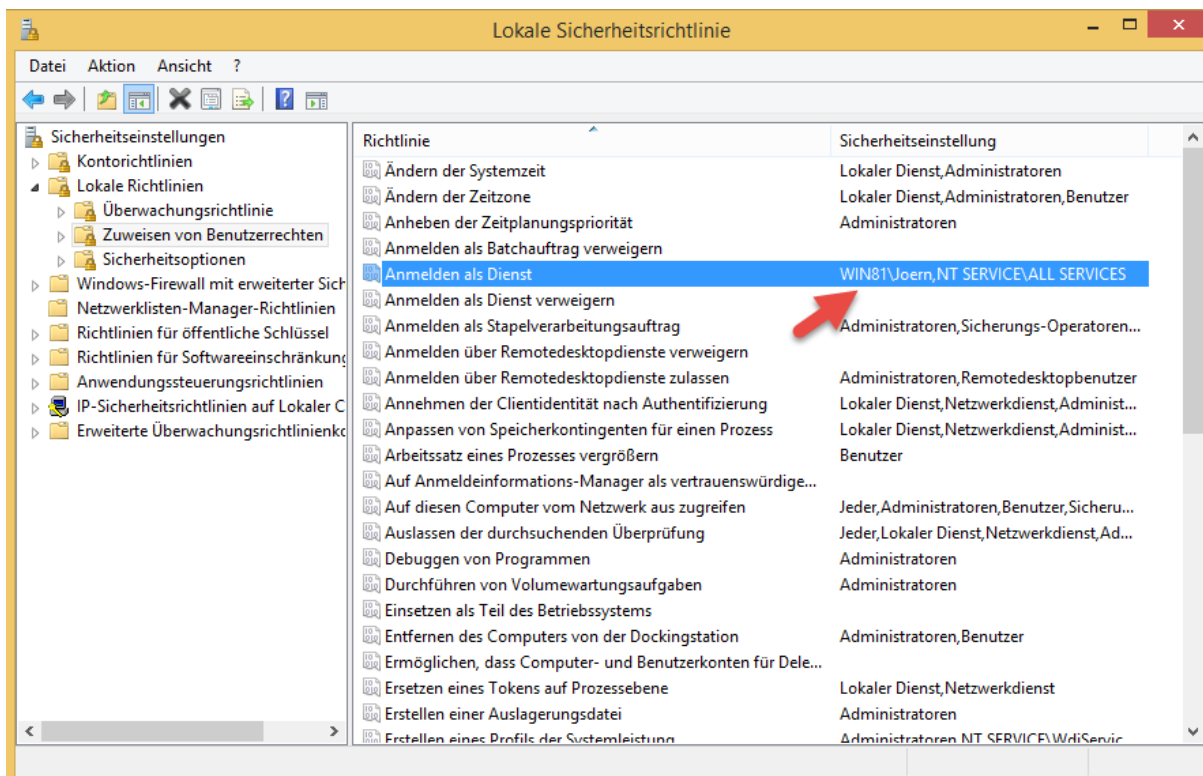
Machine = HKEY_LOCAL_MACHINE; User = HKEY_CURRENT_USER





Standard Sicherheitsrichtlinien zurücksetzen

Die lokalen Sicherheitsrichtlinien (Local Security Policies) sind aufzurufen über das Tool secpol.msc:

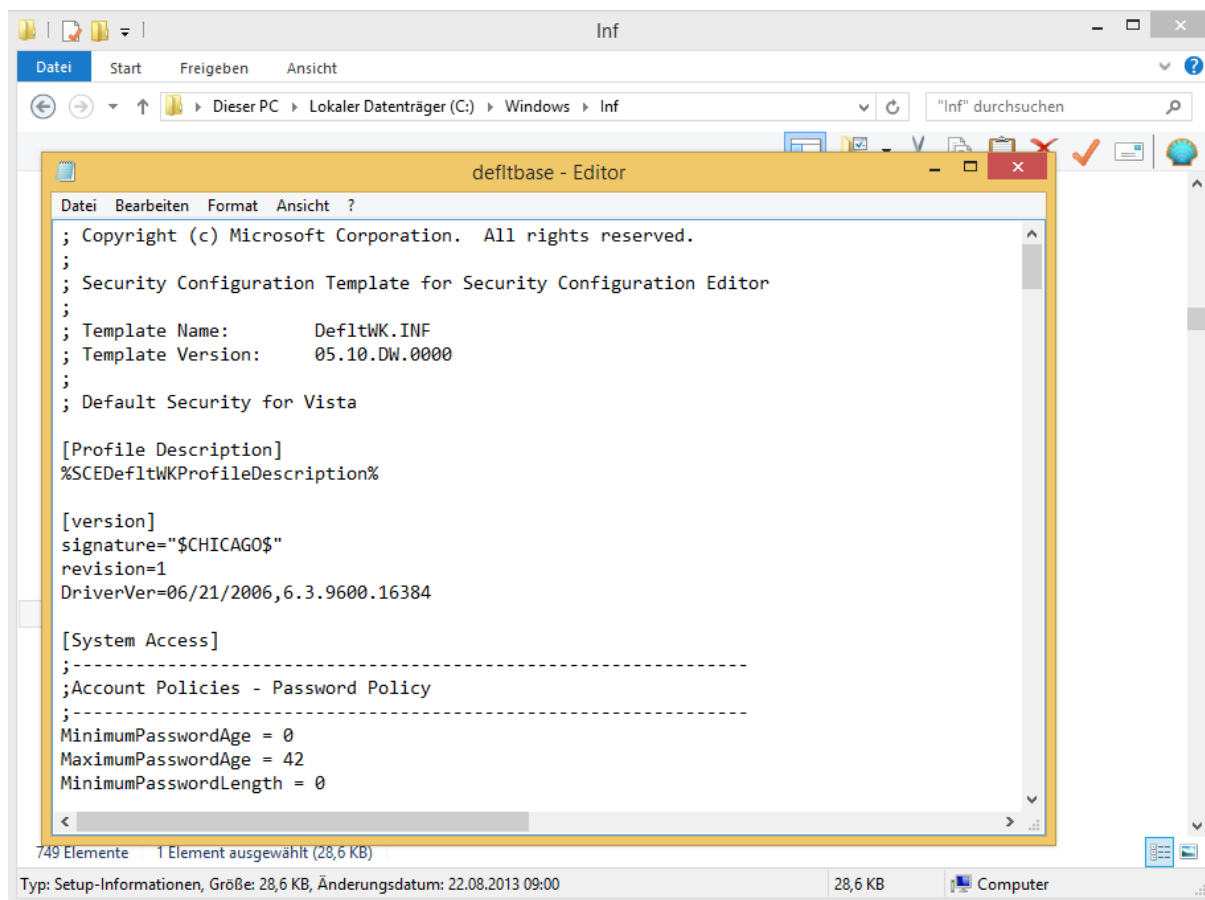




Standard Sicherheitsrichtlinien zurücksetzen

Reset-Befehl:

C:\Windows\Inf\defltbase.inf = Template aus dem die Wiederherstellung initiiert wird.





Standard Sicherheitsrichtlinien zurücksetzen

Dieser Befehl setzt die Richtlinien auf Basis des oben gezeigten Templates zurück.

sccedit /configure /cfg %windir%\inf\defltbase.inf /db defltbase.sdb /verbose

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>sccedit /configure /cfg %windir%\inf\defltbase.inf /db defltbase.sdb /verbose
0 Prozent abgeschlossen (0/111) Bereich Privilege Rights verarbeiten
1 Prozent abgeschlossen (1/111) Bereich Privilege Rights verarbeiten
2 Prozent abgeschlossen (2/111) Bereich Privilege Rights verarbeiten
3 Prozent abgeschlossen (3/111) Bereich Privilege Rights verarbeiten
4 Prozent abgeschlossen (4/111) Bereich Privilege Rights verarbeiten
5 Prozent abgeschlossen (5/111) Bereich Privilege Rights verarbeiten
6 Prozent abgeschlossen (6/111) Bereich Privilege Rights verarbeiten
7 Prozent abgeschlossen (7/111) Bereich Privilege Rights verarbeiten
8 Prozent abgeschlossen (8/111) Bereich Privilege Rights verarbeiten
9 Prozent abgeschlossen (9/111) Bereich Privilege Rights verarbeiten
10 Prozent abgeschlossen (10/111) Bereich Privilege Rights verarbeiten
11 Prozent abgeschlossen (11/111) Bereich Privilege Rights verarbeiten
12 Prozent abgeschlossen (12/111) Bereich Privilege Rights verarbeiten
13 Prozent abgeschlossen (13/111) Bereich Privilege Rights verarbeiten
14 Prozent abgeschlossen (14/111) Bereich Group Membership verarbeiten
15 Prozent abgeschlossen (15/111) Bereich Group Membership verarbeiten
16 Prozent abgeschlossen (16/111) Bereich Group Membership verarbeiten
17 Prozent abgeschlossen (17/111) Bereich Group Membership verarbeiten
18 Prozent abgeschlossen (18/111) Bereich Registry Keys verarbeiten
19 Prozent abgeschlossen (19/111) Bereich Registry Keys verarbeiten
20 Prozent abgeschlossen (20/111) Bereich Registry Keys verarbeiten
21 Prozent abgeschlossen (21/111) Bereich Registry Keys verarbeiten
22 Prozent abgeschlossen (22/111) Bereich Registry Keys verarbeiten
23 Prozent abgeschlossen (23/111) Bereich Registry Keys verarbeiten
24 Prozent abgeschlossen (24/111) Bereich Registry Keys verarbeiten
25 Prozent abgeschlossen (25/111) Bereich Registry Keys verarbeiten
26 Prozent abgeschlossen (26/111) Bereich Registry Keys verarbeiten
27 Prozent abgeschlossen (27/111) Bereich Registry Keys verarbeiten
28 Prozent abgeschlossen (28/111) Bereich Registry Keys verarbeiten
29 Prozent abgeschlossen (29/111) Bereich Registry Keys verarbeiten
30 Prozent abgeschlossen (30/111) Bereich Registry Keys verarbeiten
31 Prozent abgeschlossen (31/111) Bereich Registry Keys verarbeiten
32 Prozent abgeschlossen (32/111) Bereich Registry Keys verarbeiten
33 Prozent abgeschlossen (33/111) Bereich Registry Keys verarbeiten
34 Prozent abgeschlossen (34/111) Bereich Registry Keys verarbeiten
35 Prozent abgeschlossen (35/111) Bereich Registry Keys verarbeiten
36 Prozent abgeschlossen (36/111) Bereich Registry Keys verarbeiten
37 Prozent abgeschlossen (37/111) Bereich Registry Keys verarbeiten
38 Prozent abgeschlossen (38/111) Bereich Registry Keys verarbeiten
39 Prozent abgeschlossen (39/111) Bereich Registry Keys verarbeiten
40 Prozent abgeschlossen (40/111) Bereich Registry Keys verarbeiten
41 Prozent abgeschlossen (41/111) Bereich Registry Keys verarbeiten
42 Prozent abgeschlossen (42/111) Bereich Registry Keys verarbeiten
43 Prozent abgeschlossen (43/111) Bereich Registry Keys verarbeiten
44 Prozent abgeschlossen (44/111) Bereich Registry Keys verarbeiten
45 Prozent abgeschlossen (45/111) Bereich Registry Keys verarbeiten
46 Prozent abgeschlossen (46/111) Bereich Registry Keys verarbeiten
47 Prozent abgeschlossen (47/111) Bereich Registry Keys verarbeiten
48 Prozent abgeschlossen (48/111) Bereich Registry Keys verarbeiten
49 Prozent abgeschlossen (49/111) Bereich Registry Keys verarbeiten
50 Prozent abgeschlossen (50/111) Bereich Registry Keys verarbeiten
51 Prozent abgeschlossen (51/111) Bereich Registry Keys verarbeiten
52 Prozent abgeschlossen (52/111) Bereich Registry Keys verarbeiten
53 Prozent abgeschlossen (53/111) Bereich Registry Keys verarbeiten
54 Prozent abgeschlossen (54/111) Bereich Registry Keys verarbeiten
55 Prozent abgeschlossen (55/111) Bereich Registry Keys verarbeiten
56 Prozent abgeschlossen (56/111) Bereich Registry Keys verarbeiten
57 Prozent abgeschlossen (57/111) Bereich Registry Keys verarbeiten
58 Prozent abgeschlossen (58/111) Bereich Registry Keys verarbeiten
59 Prozent abgeschlossen (59/111) Bereich Registry Keys verarbeiten
60 Prozent abgeschlossen (60/111) Bereich Registry Keys verarbeiten
61 Prozent abgeschlossen (61/111) Bereich File Security verarbeiten
62 Prozent abgeschlossen (62/111) Bereich File Security verarbeiten
63 Prozent abgeschlossen (63/111) Bereich File Security verarbeiten
64 Prozent abgeschlossen (64/111) Bereich File Security verarbeiten
65 Prozent abgeschlossen (65/111) Bereich File Security verarbeiten
66 Prozent abgeschlossen (66/111) Bereich File Security verarbeiten
67 Prozent abgeschlossen (67/111) Bereich File Security verarbeiten
68 Prozent abgeschlossen (68/111) Bereich File Security verarbeiten
69 Prozent abgeschlossen (69/111) Bereich File Security verarbeiten
70 Prozent abgeschlossen (70/111) Bereich File Security verarbeiten
71 Prozent abgeschlossen (71/111) Bereich File Security verarbeiten
72 Prozent abgeschlossen (72/111) Bereich File Security verarbeiten
73 Prozent abgeschlossen (73/111) Bereich File Security verarbeiten
74 Prozent abgeschlossen (74/111) Bereich File Security verarbeiten
75 Prozent abgeschlossen (75/111) Bereich File Security verarbeiten
76 Prozent abgeschlossen (76/111) Bereich File Security verarbeiten
77 Prozent abgeschlossen (77/111) Bereich File Security verarbeiten
78 Prozent abgeschlossen (78/111) Bereich File Security verarbeiten
79 Prozent abgeschlossen (79/111) Bereich File Security verarbeiten
80 Prozent abgeschlossen (80/111) Bereich File Security verarbeiten
81 Prozent abgeschlossen (81/111) Bereich File Security verarbeiten
82 Prozent abgeschlossen (82/111) Bereich File Security verarbeiten
83 Prozent abgeschlossen (83/111) Bereich File Security verarbeiten
84 Prozent abgeschlossen (84/111) Bereich File Security verarbeiten
85 Prozent abgeschlossen (85/111) Bereich File Security verarbeiten
86 Prozent abgeschlossen (86/111) Bereich File Security verarbeiten
87 Prozent abgeschlossen (87/111) Bereich File Security verarbeiten
88 Prozent abgeschlossen (88/111) Bereich File Security verarbeiten
89 Prozent abgeschlossen (89/111) Bereich File Security verarbeiten
90 Prozent abgeschlossen (90/111) Bereich File Security verarbeiten
91 Prozent abgeschlossen (91/111) Bereich File Security verarbeiten
92 Prozent abgeschlossen (92/111) Bereich File Security verarbeiten
93 Prozent abgeschlossen (93/111) Bereich File Security verarbeiten
94 Prozent abgeschlossen (94/111) Bereich File Security verarbeiten
95 Prozent abgeschlossen (95/111) Bereich File Security verarbeiten
96 Prozent abgeschlossen (96/111) Bereich File Security verarbeiten
97 Prozent abgeschlossen (97/111) Bereich File Security verarbeiten
98 Prozent abgeschlossen (98/111) Bereich File Security verarbeiten
99 Prozent abgeschlossen (99/111) Bereich File Security verarbeiten
100 Prozent abgeschlossen (100/111) Bereich File Security verarbeiten

Der Auftrag wurde abgeschlossen. Während dieses Vorgangs wurden für einige Attribute Warnungen gemeldet. Die Warnung kann ignoriert werden.
Detaillierte Informationen befinden sich in der Protokolldatei %windir%\security\logs\scsccsrp.log.
```

Diese Methode kann angewendet werden, wenn z.B. eine Fehlermeldung/Laufzeitfehler etc. auftrat in Zusammenhang mit der defltbase.sdb. Natürlich auch bei einer Fehlkonfiguration des Dateisystems, der Registry usw.



Standard Sicherheitsrichtlinien zurücksetzen

Alle Änderungen werden in diese Log-Datei geschrieben:

C:\Windows\security\logs

```
scesrv.log - Editor
Datei Bearbeiten Format Ansicht ?

----Sicherheitsrichtlinien werden konfiguriert...
Konfigurieren der Kennwortinformationen.
Das Administratorkonto ist deaktiviert.
Das Gastkonto ist deaktiviert.

Konfiguration des Systemzugriffs wurde erfolgreich abgeschlossen.
LSA-Anonymous-Lookupnameeinstellung: vorhandenes SD = D:(D;;0x800;;;AN)(A;;0xf1fff;;;BA)(A;;0x20801;;;WD)(A;;0x801;;;AN)(A;;0x1000;;;LS)(A;;0x1000;;;NS)(A;;0x1000;;;S-1-5-17).
Konfiguration der LSA-Anonymous-Lookupeinstellung.
Konfigurieren von machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\securitylevel.
Konfigurieren von machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\setcommand.
Konfigurieren von machine\software\microsoft\windows nt\currentversion\winlogon\scremoveoption.
Konfigurieren von machine\software\microsoft\windows\currentversion\policies\system\dontdisplaylastusername.
Konfigurieren von machine\software\microsoft\windows\currentversion\policies\system\legalnoticecaption.
Konfigurieren von machine\software\microsoft\windows\currentversion\policies\system\legalnoticetext.
Konfigurieren von machine\software\microsoft\windows\currentversion\policies\system\shutdownwithoutlogon.
Konfigurieren von machine\software\microsoft\windows\currentversion\policies\system\undockwithoutlogon.
Konfigurieren von machine\software\policies\microsoft\windows\safer\codeidentifiers\authenticodeenabled.
Konfigurieren von machine\system\currentcontrolset\control\lsa\auditbaseobjects.
Konfigurieren von machine\system\currentcontrolset\control\lsa\crashonauditfail.
Konfigurieren von machine\system\currentcontrolset\control\lsa\disabledomaincreds.
Konfigurieren von machine\system\currentcontrolset\control\lsa\everyoneincludesanonymous.
Konfigurieren von machine\system\currentcontrolset\control\lsa\fpalgorithmpolicy\enabled.
Konfigurieren von machine\system\currentcontrolset\control\lsa\forceguest.
Konfigurieren von machine\system\currentcontrolset\control\lsa\fullprivilegeauditing.
Konfigurieren von machine\system\currentcontrolset\control\lsa\lmhash.
Konfigurieren von machine\system\currentcontrolset\control\lsa\restrictanonymous.
Konfigurieren von machine\system\currentcontrolset\control\lsa\restrictanonymoussam.
Konfigurieren von machine\system\currentcontrolset\control\print\providers\lanman print services\servers
\addprinterdrivers.
Konfigurieren von machine\system\currentcontrolset\control\session manager\kernel\obcaseinsensitive.
\clearpagefileatshutdown.
Konfigurieren von machine\system\currentcontrolset\control\session manager\protectionmode.
Konfigurieren von machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect.
Konfigurieren von machine\system\currentcontrolset\services\lanmanserver\parameters\enableforcedlogoff.
Konfigurieren von machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature.
Konfigurieren von machine\system\currentcontrolset\services\lanmanserver\parameters\requiresecuritysignature.
Konfigurieren von machine\system\currentcontrolset\services\lanmanserver\parameters\restrictnullsessaccess.
\enableplaintextpassword.
Konfigurieren von machine\system\currentcontrolset\services\lanmanworkstation\parameters
\enablesecuritysignature.
Konfigurieren von machine\system\currentcontrolset\services\lanmanworkstation\parameters
\requiresecuritysignature.
Konfigurieren von machine\system\currentcontrolset\services\ldap\ldapclientintegrity.

Die Konfiguration der Registrierungswerte wurde erfolgreich abgeschlossen.
Konfigurieren der Protokolleinstellungen.

Konfiguration des Überwachungsprotokolls wurde erfolgreich abgeschlossen.
```

Optional:

GPOs per Powershell sichern:

Get-GPO -All | where CreationTime -gt 01.01.2015 | Backup-GPO -Path C:\backup\GPO

GPOs per Powershell wiederherstellen:

Restore-GPO -All -Path C:\backup\GPO

Leere GPOs ermitteln:

```
$AllGPOs = Get-GPO -all
foreach($GP in $AllGPOs){if($GP.User.DSVersion -eq 0 -and $GP.Computer.DSVersion -eq 0)
{Write-Host "Leere GPOs:" $GP.DisplayName}}
```

GPO report XML:

Get-GPOReport -All -ReportType XML

Nicht zugewiesene GPOs ermitteln:

```
Get-GPO -All | %{$XML} $GPOs = Get-GPOReport -Name $_.DisplayName -ReportType XML; $GPOs.GPO.Name + ";" + $GPOs.GPO.LinksTo.SOMName}
```