



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:

The screenshot shows the 'Editor für lokale Gruppenrichtlinien' window. The left pane displays a tree view of policy settings under 'Richtlinien für Lokaler Computer'. The right pane lists policy settings with their security configurations. One specific entry, 'Anmelden als Dienst' (Log on as a service), is highlighted with a red arrow pointing to its security configuration, which is set to 'WIN81\Joern, NT SERVICE\ALL SERVICES'. Other entries include 'Ändern der Systemzeit' (Change system time) and 'Ändern der Zeitzone' (Change time zone).

Richtlinie	Sicherheitseinstellung
Ändern der Systemzeit	Lokaler Dienst, Administratoren
Ändern der Zeitzone	Lokaler Dienst, Administratoren, Benutzer
Anheben der Zeitplanungspriorität	Administratoren
Anmelden als Batchaufrag verweigern	
Anmelden als Dienst	WIN81\Joern, NT SERVICE\ALL SERVICES
Anmelden als Dienst verweigern	
Anmelden als Stapelverarbeitungsauftrag	
Anmelden über Remotedesktopdienste verweigern	
Anmelden über Remotedesktopdienste zulassen	
Annehmen der Clientidentität nach Authentifizierung	
Anpassen von Speicherkontingenzen für einen Prozess	
Arbeitssatz eines Prozesses vergrößern	
Auf Anmeldeinformations-Manager als vertrauenswürdige...	Jeder, Administratoren, Benutzer, Sicherungs-Operat...
Auf diesen Computer vom Netzwerk aus zugreifen	Jeder, Administratoren, Benutzer, Sicherungs-Operat...
Auslassen der durchsuchenden Überprüfung	Jeder, Lokaler Dienst, Netzwerkdienst, Administrat...
Debuggen von Programmen	Administratoren
Durchführen von Volumenwartungsaufgaben	Administratoren
Einsetzen als Teil des Betriebssystems	Administratoren
Entfernen des Computers von der Dockingstation	Administratoren, Benutzer
Ermöglichen, dass Computer- und Benutzerkonten für Dele...	Lokaler Dienst, Netzwerkdienst
Ersetzen eines Tokens auf Prozessebene	Administratoren
Erstellen einer Auslagerungsdatei	Administratoren
Erstellen eines Profils der Systemleistung	Administratoren, NT SERVICE\WdiServiceHost
Erstellen eines Profils für einen Einzelprozess	Administratoren
Erstellen eines Tokenobjekts	Administratoren

Konfigurierte Überwachungsrichtlinie als Beispiel:

The screenshot shows the 'Editor für lokale Gruppenrichtlinien' window. The left pane displays a tree view of policy settings under 'Richtlinien für Lokaler Computer'. The right pane lists policy settings with their monitoring configurations. Two specific entries, 'Anmeldeereignisse überwachen' and 'Objektzugriffsversuche überwachen', are highlighted with red arrows pointing to their monitoring configurations, both set to 'Erfolgreich'. Other entries include 'Kontenverwaltung überwachen' and 'Rechteverwendung überwachen'.

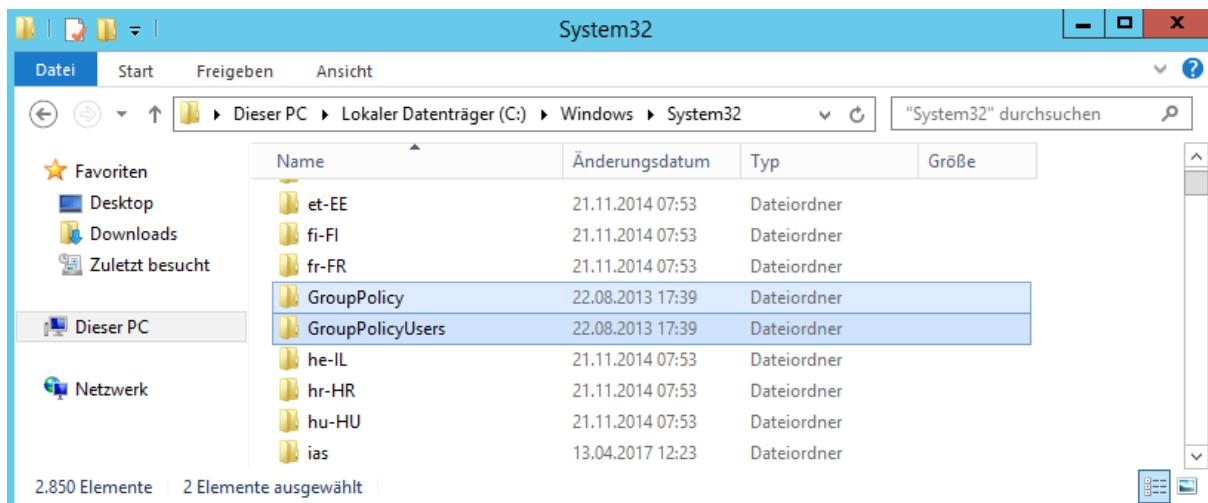
Richtlinie	Sicherheitseinstellung
Anmeldeereignisse überwachen	Erfolgreich
Anmeldeversuche überwachen	Keine Überwachung
Kontenverwaltung überwachen	Keine Überwachung
Objektzugriffsversuche überwachen	Erfolgreich
Prozessnachverfolgung überwachen	Keine Überwachung
Rechteverwendung überwachen	Keine Überwachung
Richtliniänderungen überwachen	Keine Überwachung
Systemereignisse überwachen	Keine Überwachung
Verzeichnisdienstzugriff überwachen	Keine Überwachung



Standard Sicherheitsrichtlinien zurücksetzen

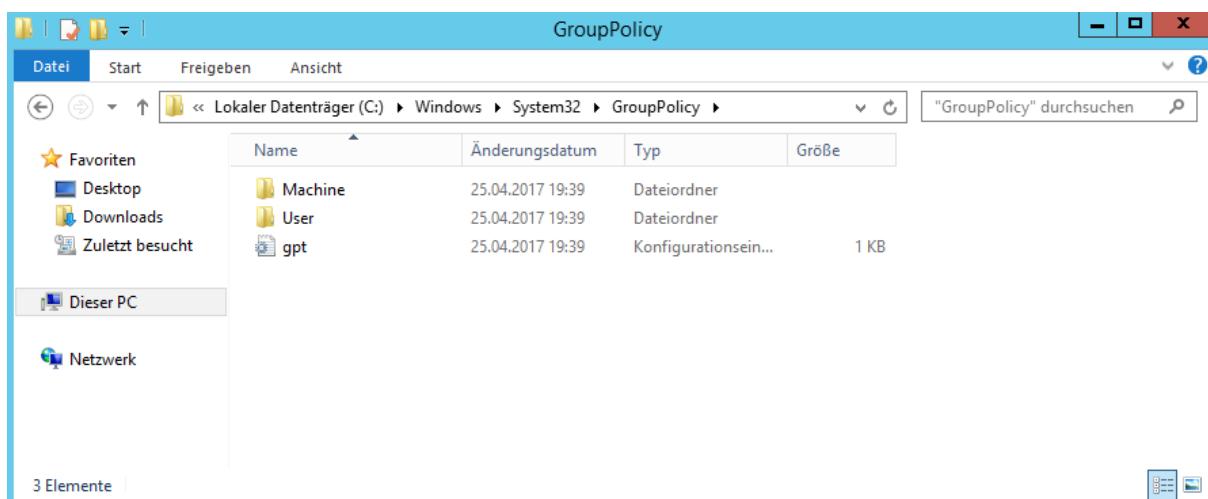
Der Speicherort der Einstellungen im Dateisystem ist:

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:

Lokale Sicherheitsrichtlinie

Richtlinie	Sicherheitseinstellung
Ändern der Systemzeit	Lokaler Dienst,Administratoren
Ändern der Zeitzone	Lokaler Dienst,Administratoren,Benutzer
Anheben der Zeitplanungspriorität	Administratoren
Anmelden als Batchauftrag verweigern	
Anmelden als Dienst	WIN81\Jörn,NT SERVICE\ALL SERVICES
Anmelden als Dienst verweigern	
Anmelden als Stapelverarbeitungsauftrag	
Anmelden über Remotedesktopdienste verweigern	
Anmelden über Remotedesktopdienste zulassen	Administratoren,Remotedesktopbenutzer
Annehmen der Clientidentität nach Authentifizierung	Lokaler Dienst,Netzwerkdienst,Administ...
Anpassen von Speicherkontingenten für einen Prozess	Lokaler Dienst,Netzwerkdienst,Administ...
Arbeitssatz eines Prozesses vergrößern	Benutzer
Auf Anmeldeinformations-Manager als vertrauenswürdige...	Jeder,Administratoren,Benutzer,Sicheru...
Auf diesen Computer vom Netzwerk aus zugreifen	Jeder,Lokaler Dienst,Netzwerkdienst,Ad...
Auslassen der durchsuchenden Überprüfung	Administratoren
Debuggen von Programmen	Administratoren
Durchführen von Volumewartungsaufgaben	
Einsetzen als Teil des Betriebssystems	
Entfernen des Computers von der Dockingstation	Administratoren,Benutzer
Ermöglichen, dass Computer- und Benutzerkonten für Dele...	
Ersetzen eines Tokens auf Prozessebene	Lokaler Dienst,Netzwerkdienst
Erstellen einer Auslagerungsdatei	Administratoren
Festlegen eines Profils der Systemleistung	Administratoren NT SERVIC\ICE\WtService

Lokale Sicherheitsrichtlinie

Richtlinie	Sicherheitseinstellung
Anmeldeereignisse überwachen	Erfolgreich
Anmeldeversuche überwachen	Keine Überwachung
Kontenverwaltung überwachen	Keine Überwachung
Objektzugriffsversuche überwachen	Erfolgreich
Prozessnachverfolgung überwachen	Keine Überwachung
Rechteverwendung überwachen	Keine Überwachung
Richtlinienänderungen überwachen	Keine Überwachung
Systemereignisse überwachen	Keine Überwachung
Verzeichnisdienstzugriff überwachen	Keine Überwachung



Standard Sicherheitsrichtlinien zurücksetzen

Reset-Befehl:

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

The screenshot shows the Windows Security Configuration Editor window titled "defltbase - Editor". The file path is "C:\Windows\Inf\defltbase.inf". The content of the file is as follows:

```
; Copyright (c) Microsoft Corporation. All rights reserved.  
;  
; Security Configuration Template for Security Configuration Editor  
;  
; Template Name: DefltWK.INF  
; Template Version: 05.10.DW.0000  
;  
; Default Security for Vista  
  
[Profile Description]  
%SCEDefltWKProfileDescription%  
  
[version]  
signature="$CHICAGO$"  
revision=1  
DriverVer=06/21/2006,6.3.9600.16384  
  
[System Access]  
-----  
;Account Policies - Password Policy  
-----  
MinimumPasswordAge = 0  
MaximumPasswordAge = 42  
MinimumPasswordLength = 0
```

At the bottom of the editor window, it says "749 Elemente 1 Element ausgewählt (28,6 KB)". Below the window, the status bar displays "Typ: Setup-Informationen, Größe: 28,6 KB, Änderungsdatum: 22.08.2013 09:00" and "28,6 KB Computer".



Standard Sicherheitsrichtlinien zurücksetzen

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

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

The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\System32\cmd.exe". The window displays the output of the "secedit /configure" command. The output lists numerous security settings (e.g., Privilege Rights, Group Membership, Registry Keys) and their status as "abgeschlossen" (closed) or "verarbeiten" (processing). The process continues sequentially from index 0 to 110. A warning message at the bottom states: "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\klog\scscev.log." (The task was completed. During this process, warnings were issued for some attributes. The warning can be ignored. Detailed information is located in the log file %windir%\security\klog\scscev.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

```
scserv.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-Lookupnameneinstellung: 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).
Konfigurieren 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\legalnoticetextcaption.
Konfigurieren von machine\software\microsoft\windows\currentversion\policies\system\legalnoticetext.
Konfigurieren von machine\software\microsoft\windows\currentversion\policies\system\scforceoption.
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\fipsalgorithmpolicy\enabled.
Konfigurieren von machine\system\currentcontrolset\control\lsa\forceguest.
Konfigurieren von machine\system\currentcontrolset\control\lsa\fullprivilegeauditing.
Konfigurieren von machine\system\currentcontrolset\control\lsa\nolmhash.
Konfigurieren von machine\system\currentcontrolset\control\lsa\restrictanonymous.
Konfigurieren von machine\system\currentcontrolset\control\lsa\restrictanonymousmousam.
Konfigurieren von machine\system\currentcontrolset\control\print\providers\lanman print services\servers
\addprinterdrives.
Konfigurieren von machine\system\currentcontrolset\control\session manager\kernel\obcaseinsensitive.
Konfigurieren von machine\system\currentcontrolset\control\session manager\memory management
\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.
Konfigurieren von machine\system\currentcontrolset\services\lanmanworkstation\parameters
\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-GPReport -All -ReportType XML
```

Nicht zugewiesene GPOs ermitteln:

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