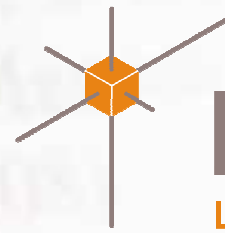


wei|se (klug); 'Weise, der  
-n, -n; ↑ R 5 ff. (kluger Ma  
weisen (↑ R 10)



**Netz-Weise**  
Lernen von den Besten.

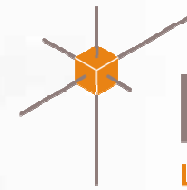
# Gruppenrichtlinien Troubleshooting

wei|se (klug); 'Weise, der  
-n, -n; ↑ R 5 ff. (kluger Mann)  
weisen (↑ R 108)



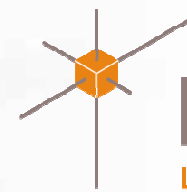
**Netz-Weise**  
Lernen von den Besten.

**Netz-Weise**  
**Holger Voges**  
**Walkürenring 17**  
**38106 Braunschweig**  
**[www.netz-weise.de](http://www.netz-weise.de)**



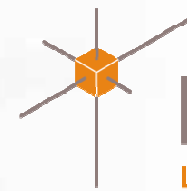
## Überblick

- Funktionsweise von Gruppenrichtlinien
- Verwalten mit der Group Policy Management Console
- Erweitern von Gruppenrichtlinien
- Fremdhersteller-Erweiterungen
- Troubleshooting mit Bordmitteln
- Probleme und Lösungen



## Was sind Gruppenrichtlinien

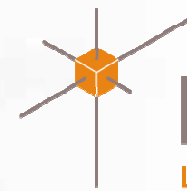
- Gruppenrichtlinien sind mit Windows 2000 eingeführt worden
- Gruppenrichtlinien ersetzen die NT4 Policies
- Grundlage ist Active Directory!
- Der empfangende PC benötigt als Win2k, Win XP oder Win2k3
- Mit jedem Windows-Servicepack wachsen die Funktionen von Gruppenrichtlinien
- Gruppenrichtlinien sind ein extrem mächtiges Werkzeug zur Konfiguration von Clients und Benutzerumgebungen



## Neue Funktionen seit Win XP

- Resultant Set of Policies (RSOP) zeigen die auf einem Client angewendeten Richtlinien an
- Software Restriction Policies ermöglichen die Kontrolle über ausführbare Software
- WMI-Filter ermöglichen das bedingte Ausführen von Gruppenrichtlinien anhand von WMI-Abfragen (z.B. Service-Pack Version)
- Es sind viele neue Einstellungen per Richtlinien möglich

weise (klug); Weise, der  
-n, -n; ↑ R 5 ff. (kluger Mann)  
weisen (↑ R 108)



**Netz-Weise**  
Lernen von den Besten.

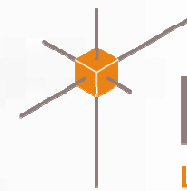
## Typen von Richtlinien

- Lokale Richtlinien (nur Sicherheitseinstellungen)
- Richtlinien auf Standort-Ebene
- Richtlinien auf Domänen-Ebene
- Richtlinien auf OU-Ebene

niedrig

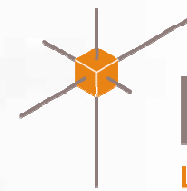


hoch



## Lokale vs. Domänenrichtlinien

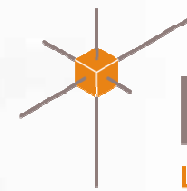
- Lokale Richtlinien
  - liegen im Dateisystem (system32\GroupPolicy)
  - Ermöglichen keine benutzerspezifische Konfiguration
  - Können nur 1 mal pro PC eingerichtet werden
- Domänenrichtlinien
  - Liegen im AD und auf dem DC
  - Erlauben die Konfiguration pro Computer / pro Benutzer
  - Max. 999 Richtlinien pro Objekt – sind auf ein Objekt mehr Richtlinien angewendet, werden keine Richtlinien angewandt!



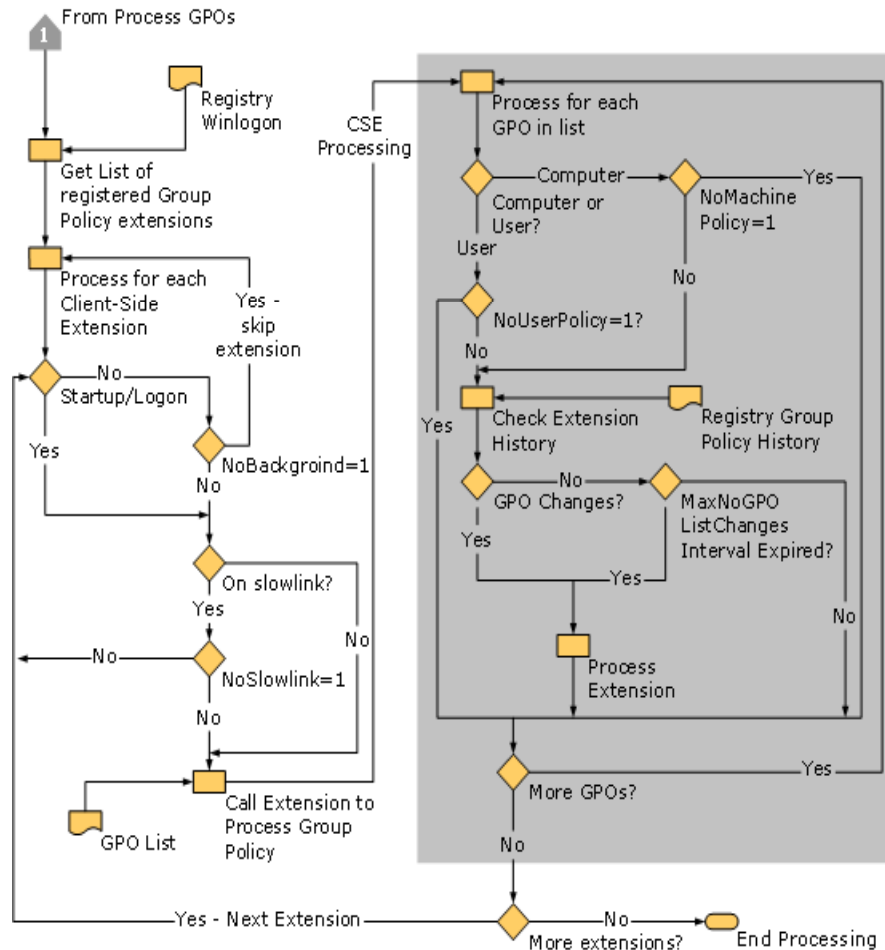
## So funktionieren Gruppenrichtlinien

- Gruppenrichtlinien haben 3 Bestandteile:
  - Den AD-Container Policies
  - Den Ordner Sysvol\Policies auf Domänencontrollern
  - Die Client Side Extensions auf dem PC (führen die Konfiguration auf den Clients durch)
- Gruppenrichtlinien können auf Benutzer- und Computer-Objekte angewendet werden

wei|se (klug); We|ise, die  
-n, -n; ↑ R 5 ff. (kluger Man  
Weisen (↑ R 108)

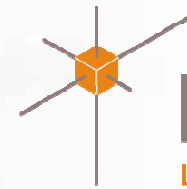


# Ablauf einer Anmeldung



## ADM-Dateien

- ADM-Dateien sind die Konfigurationsdateien für den Knoten „Administrative Vorlagen“
- Sie beinhalten Einstellungen, die auf dem Client über Registry-Keys angepasst werden
- Sie können manuell erzeugt werden
- Sie werden vom Gruppenrichtlinieneditor gpedit.msc geladen
- Sie werden standardmäßig in Sysvol abgelegt
- Sie sind für die Konfiguration des Clients nicht notwendig



## Funktionsweise von ADMs

- Es gibt 5 Standard-ADM-Dateien:
  - Conf.amd, inetres.adm, system.adm, Wmplayer.adm, Wuau.adm
  - Die Original-ADMs sollten niemals editiert werden!
- ADM-Vorlagen zur Konfiguration von MS Office stehen im Office Resource Kit zur Verfügung
- Viele ADM-Vorlagen sind im Internet verfügbar
- Tattooing bezeichnet den Vorgang, bei dem Registry-Einstellungen aus Richtlinien nach dem Entfernen der Richtlinie in der Registry verbleiben

weise (klug); 'Weise, der  
-n, -n; ↑ R 5 ff. (kluger Man  
weisen (↑ R 108)



**Netz-Weise**  
Lernen von den Besten.

# Aufbau einer ADM-Datei

```
CATEGORY !!AdministrativeServices
```

```
    POLICY !!DisableCMD
```

```
        KEYNAME "Software\Policies\Microsoft\Windows\System"
```

```
        #if version >= 4
```

```
        SUPPORTED !!SUPPORTED_Win2k
```

```
        #endif
```

```
    EXPLAIN !!DisableCMD_Help
```

```
    PART !!DisableCMDScripts      DROPDOWNLIST  NOSORT
```

```
        VALUENAME "DisableCMD"
```

```
        ITEMLIST
```

```
            NAME !!DisableCMD_YES      VALUE NUMERIC  1
```

```
            NAME !!DisableCMD_NO      VALUE NUMERIC  2 DEFAULT
```

```
        END ITEMLIST
```

```
    END PART
```

```
END POLICY
```

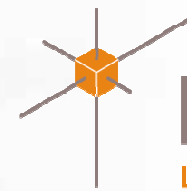
```
END CATEGORY ; AdministrativeServices
```

Die Keys in der Registry und die Anzeige in gpedit

Textvariablen aus dem oberen Bereich werden hier definiert

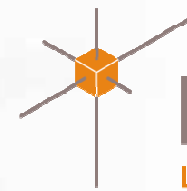
```
[strings]
```

```
DisableCMD_Help="Verhindert, dass Benutzer die interaktive [...] werden.."
```



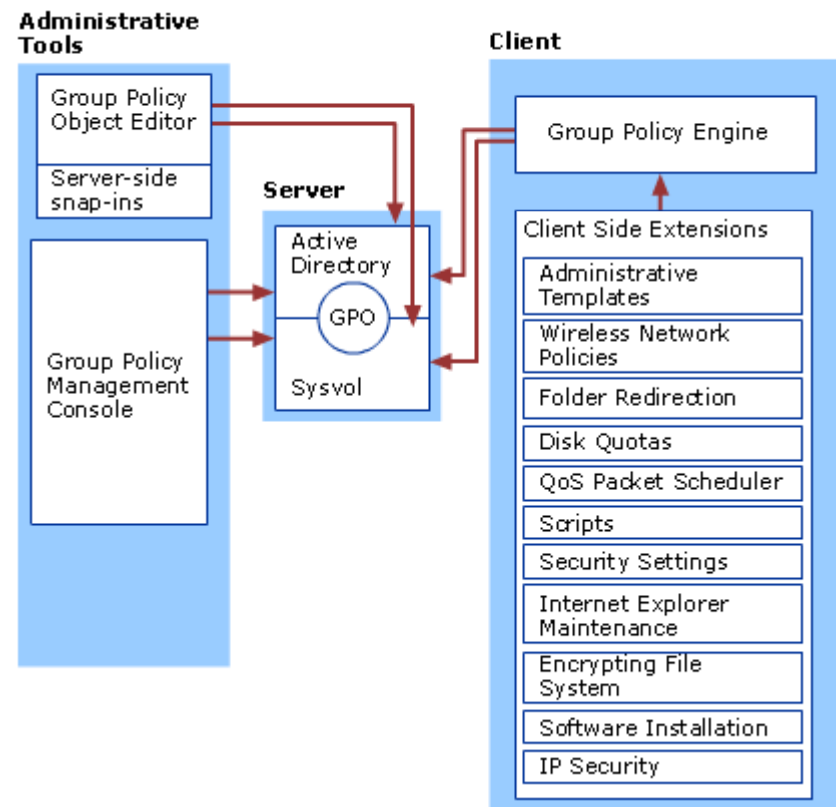
## Tools zum Bearbeiten von ADMs

- ADMX aus den Support-Tools
- Reg2ADM speichert Registry Keys als ADM-Dateien
- Editoren zum einfachen Erstellen von ADM-Dateien:
  - ADM Template Editor von Syprosoft
  - Policy Template File Editor
  - ADM Utils (Perl-Scripte)



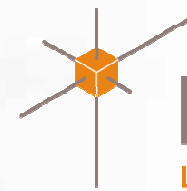
# Funktion von Client Side Extensions

- Die Änderungen auf dem Client werden durch Clientseitige Software (CSE's) durchgeführt



# Group Policy Management Console

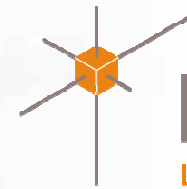
- Die Group Policy Management Console:
  - Ist ein kostenloses Tool von Microsoft
  - Enthält etliche nützlicher Zusatzfunktionen zur Verwaltung von Gruppenrichtlinien
  - Eignet sich auch zur Verwaltung von Gruppenrichtlinien in W2k-basierten Domänen
  - Installationsvoraussetzungen:
    - Windows XP SP1
    - .NET-Framework 1.1



## Funktionalitäten der GPMC

- Übersichtlichere Verwaltung der Richtlinien
- Gruppenrichtlinien-Berichte zeigen nur die konfigurierten Einstellungen von Richtlinien
- Die GPMC bietet ein Interface für die RSOP's
- Gruppenrichtlinienmodellierung ermöglicht das Planen neuer Richtlinien
- Die GPMC stellt ermöglicht die Sicherung und Wiederherstellung von Richtlinien
- Gruppenrichtlinien Import erlaubt das transferieren von Richtlinien über Domänen
- Die GPMC erlaubt das Scripten von Richtlinien

wei|se (klug); 'Weise,  
-n, -n; ↑ R 5 ff. (kluger Men  
weisen (↑ R 10)



**Netz-Weise**  
Lernen von den Besten.

# Berichterstellung

- Die GPMC erzeugt Berichte, die nur die konfigurierten Einstellungen einer Richtlinie anzeigen
- Berichte können im Format HTML und XML gespeichert werden
- Die Dokumentation von Richtlinien wird so stark vereinfacht

The screenshot shows the Group Policy Management console for the domain 'nwtraders.net'. The left pane shows the hierarchy: Group Policy Management > Gesamtstruktur: nwtraders.net > Domänen > nwtraders.net > Default Domain Policy > Windows Update. The right pane displays the 'Windows Update' policy configuration. The policy is 'Aktiviert' (Enabled). The configuration includes several settings under 'Administrative Vorlagen' and 'Windows-Komponenten/Windows Update'.

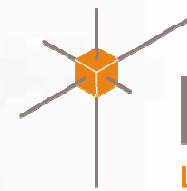
Richtlinie	Einstellung
Automatische Updates sofort installieren	Deaktiviert
Clientsseitige Zielzuordnung aktivieren	Aktiviert
Zielgruppenname für diesen Computer	Server
Erneut zu einem Neustart für geplante Installationen auffordern	Aktiviert
Folgender Zeitraum (in Minuten) warten, bevor zu einem Neustart aufgefordert wird:	10
Internen Pfad für den Microsoft Updatedienst angeben	Aktiviert
Interner Updatedienst zum Ermitteln von Updates:	http://WUSServer1
Intranetserver für die Statistiken: (Beispiel: http://IntranetUpd01)	http://WUSSERVER1
Neustart für geplante Installationen verzögern	Aktiviert
Folgender Zeitraum (in Minuten) warten, bevor ein geplanter Neustart ausgeführt wird:	5
Nicht-Administratoren gestatten, Updatebenachrichtigungen zu erhalten	Deaktiviert
Zeitplan für geplante Installationen neu erstellen	Aktiviert
Wartezeit nach Systemstart (Minuten):	1

Below the table, there is a section for 'Benutzerkonfiguration (Aktiviert)' which shows 'Keine Einstellungen definiert'.

## Richtlinienergebnissätze

- Mit Windows XP kommt das neue Feature Richtlinienergebnissätze (Resultant Set of Policies oder RSOP)
- RSOP listet die Einstellungen auf, die auf einem Client für einen Benutzer gültig werden
- Der Ergebnissatz wird vom Client (!) erzeugt
- Es werden alle Einstellungen und die jeweils ausschlaggebende Richtlinie angezeigt
- Dank RSOP wird eine einfache Fehleranalyse möglich
- RSOP ist ein Feature ab Windows XP und funktioniert nicht mit W2k!

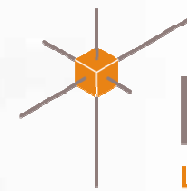




# Gruppenrichtlinienmodellierung

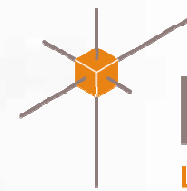
## Gruppenrichtlinienmodellierung...

- ähnelt von der Funktionalität RSOP
- vereinfacht das Planen von Richtlinien
- benötigt einen Domänencontroller mit W2k3
- simuliert die Abarbeitung der Richtlinien auf dem Client
- kann auch zum Troubleshooting für W2k verwendet werden



## Sichern und Wiederherstellen

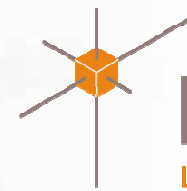
- Mit der GPMC können Sicherungen von Gruppenrichtlinien angelegt werden
- Das Backup enthält alle Daten aus dem Sysvol-Ordner und zusätzliche Verwaltungsinformationen in Form von XML-Dateien
- Mit einer Richtliniensicherung können zerstörte Richtlinien und alte Stände wiederhergestellt werden
- Eine Sicherung kann auch zum Richtlinienexport genutzt werden
- Nicht gesichert werden IPSEC-Einstellungen und WMI-Filter (liegen im AD)



## Import von Richtlinien

- Die GPMC erlaubt den Import von Richtlinien
- Der Import erfolgt immer in eine bestehende Richtlinie
- Die Vorlage für den Import ist die Sicherung einer bestehenden Richtlinie
- Beim Import werden Daten in eine neue Richtlinie geladen. Evtl. Bestehende Einstellungen werden dabei überschrieben
- Importtabellen unterstützen den Import von Berechtigungen, indem die SID's der Original-Domäne in die SID's der Zieldomäne übersetzt werden

wei|se (klug); 'Weise, der  
-n, -n; ↑ R 5 ff. (kluger Mann)  
Weisen (↑ R 103)



**Netz-Weise**  
Lernen von den Besten.

# Sichern und Importieren

The screenshot shows the Group Policy Management console. The left pane displays the hierarchy: Group Policy Management > Gesamtstruktur: nwtraders.net > Domänen > nwtraders.net > Firewall-Konfiguration. The right pane shows the 'Firewall-Konfiguration' window with the 'Verknüpfungen' tab selected. A context menu is open over the 'Firewall-Konfiguration' object in the left pane, with 'Sichern...' and 'Einstellungen importieren...' highlighted in red. The 'Verknüpfungen' table in the right pane is as follows:

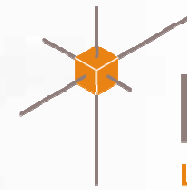
Pfad	Erzungen	Verknüpfung aktiviert	Pfad
<input checked="" type="checkbox"/> Workstations	Nein	Ja	nwtraders.net/Braunschweig/Workstations

## Scriptfähiges Interface

- Mit der GPMC stellt Microsoft eine Schnittstelle zum Scripten von Richtlinien zur Verfügung
- Eine Reihe von Beispielskripten liegen der GPMC im Order `%Programfiles%\GPMC\Scripts` bei

Name	Größe	Typ	Geändert am	Attri
BackupAllGPOs.wsf	7 KB	Windows-Skriptdatei	19.05.2004 10:26	A
BackupGPO.wsf	7 KB	Windows-Skriptdatei	19.05.2004 10:26	A
CopyGPO.wsf	9 KB	Windows-Skriptdatei	19.05.2004 10:26	A
CreateEnvironmentFromXML...	86 KB	Windows-Skriptdatei	19.05.2004 10:26	A
CreateGPO.wsf	4 KB	Windows-Skriptdatei	19.05.2004 10:26	A
CreateMigrationTable.wsf	14 KB	Windows-Skriptdatei	19.05.2004 10:26	A
CreateXMLFromEnvironment...	42 KB	Windows-Skriptdatei	19.05.2004 10:26	A
DeleteGPO.wsf	8 KB	Windows-Skriptdatei	19.05.2004 10:26	A
DumpGPOInfo.wsf	10 KB	Windows-Skriptdatei	19.05.2004 10:26	A
DumpSOMInfo.wsf	9 KB	Windows-Skriptdatei	19.05.2004 10:26	A
FindDisabledGPOs.wsf	4 KB	Windows-Skriptdatei	19.05.2004 10:26	A
FindDuplicateNamedGPOs.wsf	5 KB	Windows-Skriptdatei	19.05.2004 10:26	A
FindGPOsByPolicyExtension.wsf	7 KB	Windows-Skriptdatei	19.05.2004 10:26	A
FindGPOsBySecurityGroup.wsf	8 KB	Windows-Skriptdatei	19.05.2004 10:26	A
FindGPOsWithNoSecurityFilter...	4 KB	Windows-Skriptdatei	19.05.2004 10:26	A
FindOrphanedGPOsInSYSVOL...	4 KB	Windows-Skriptdatei	19.05.2004 10:26	A
FindSOMsWithExternalGPOLin...	6 KB	Windows-Skriptdatei	19.05.2004 10:26	A
FindUnlinkedGPOs.wsf	4 KB	Windows-Skriptdatei	19.05.2004 10:26	A
GetReportsForAllGPOs.wsf	8 KB	Windows-Skriptdatei	19.05.2004 10:26	A
GetReportsForGPO.wsf	8 KB	Windows-Skriptdatei	19.05.2004 10:26	A
gpmc.chm	282 KB	Kompilierte HTML-Hilf...	19.05.2004 10:26	A
GrantPermissionOnAllGPOs.wsf	9 KB	Windows-Skriptdatei	19.05.2004 10:26	A
ImportAllGPOs.wsf	9 KB	Windows-Skriptdatei	19.05.2004 10:26	A
ImportGPO.wsf	10 KB	Windows-Skriptdatei	19.05.2004 10:26	A
Lib_CommonGPMCFuctions.js	14 KB	JScript-Skriptdatei	19.05.2004 10:26	A
ListAllGPOs.wsf	9 KB	Windows-Skriptdatei	19.05.2004 10:26	A
ListSOMPOLICYTree.wsf	9 KB	Windows-Skriptdatei	19.05.2004 10:26	A
QueryBackupLocation.wsf	6 KB	Windows-Skriptdatei	19.05.2004 10:26	A
RestoreAllGPOs.wsf	6 KB	Windows-Skriptdatei	19.05.2004 10:26	A
RestoreGPO.wsf	6 KB	Windows-Skriptdatei	19.05.2004 10:26	A
SampleEnvironment.xml	5 KB	XML-Dokument	19.05.2004 10:26	A
SampleMigrationTable.migttable	16 KB	MIGTABLE-Datei	19.05.2004 10:26	A
ScriptingReadme.rtf	8 KB	RTF-Dokument	19.05.2004 10:26	A
SetGPOCreationPermissions.wsf	5 KB	Windows-Skriptdatei	19.05.2004 10:26	A
SetGPOPermissions.wsf	7 KB	Windows-Skriptdatei	19.05.2004 10:26	A
SetGPOPermissionsBySOM.wsf	14 KB	Windows-Skriptdatei	19.05.2004 10:26	A
SetSOMPermissions.wsf	15 KB	Windows-Skriptdatei	19.05.2004 10:26	A

Die mitgelieferten Skripte der GPMC



## Kostenlose Erweiterungen

- Einige Tools zum Erweitern von Gruppenrichtlinien
  - EZ GPO Software (Energiesparmodus per gpo)
  - Office Resource Kit (ORK)
  - Policy Maker Registry Extensions
  - Gpovault
  - True control Template (ADM für TS und Citrix)

## EZ GPO Software

- EZ GPO Software konfiguriert den Energiesparmodus per Richtlinien
- Die Erweiterung besteht aus einem Client und einer ADM-Datei
- Die Erweiterung ist kostenlos
- Durch Stromeinsparungen z.B. in Verbindung mit AMD's Cool'n Quiet kann viel Geld eingespart werden, da cool'n Quiet nur in Verbindung mit Energiespar-Profilen aktiv wird

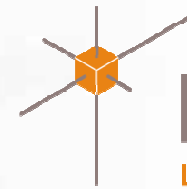
([http://www.energystar.gov/index.cfm?c=power\\_mgt.pr\\_pm\\_ez\\_gpo](http://www.energystar.gov/index.cfm?c=power_mgt.pr_pm_ez_gpo))

## Office Resource Kit (ORK)

- Das ORK stellt ab Office 2000 ADM-Dateien zur Office-Konfiguration bereit
- Fast alle Office-Einstellungen lassen sich per Richtlinie vorgeben
- Komplette Office-Menüs können vollständig deaktiviert werden
- Download:

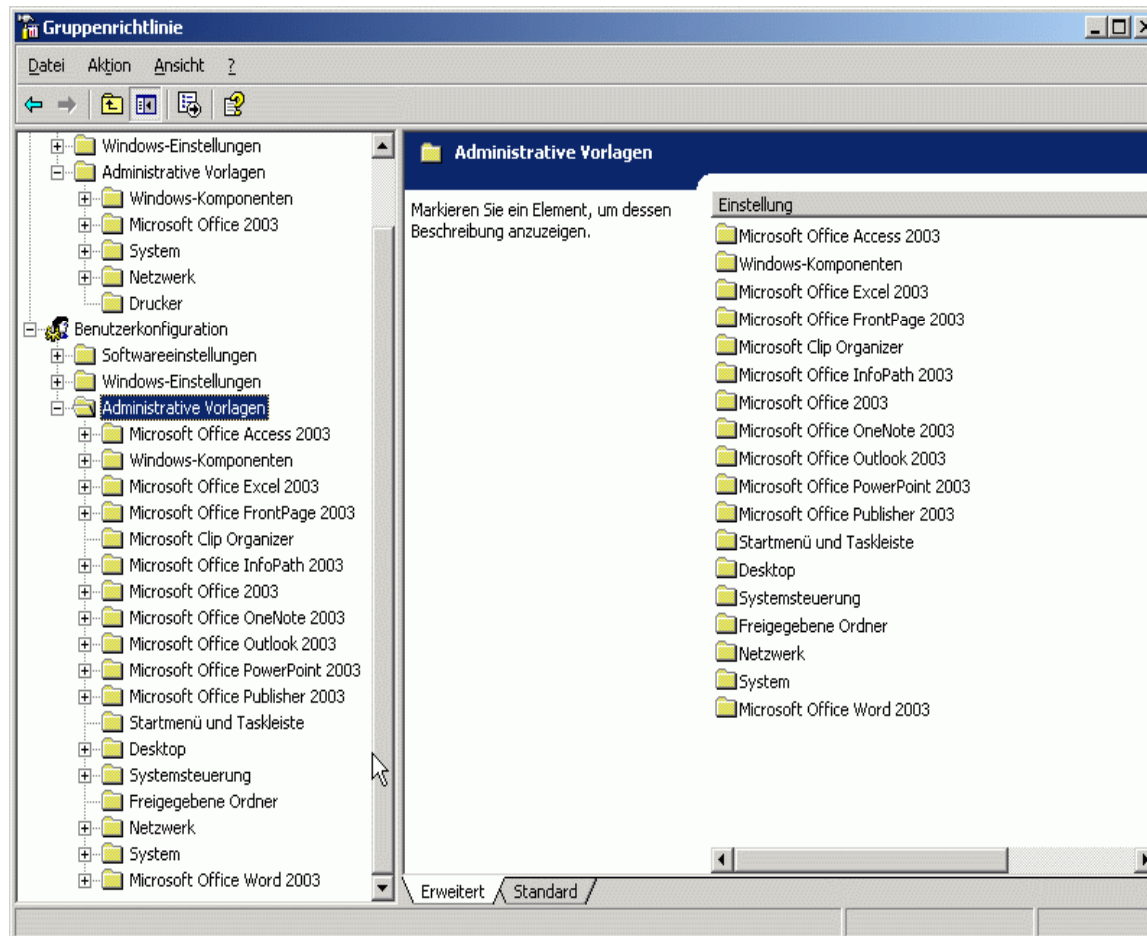
<http://www.microsoft.com/office/orkarchive/2003ddl.htm>

wei|se (klug); 'Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Man  
Weisen (↑ R 103)

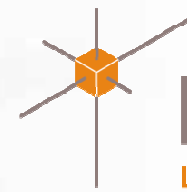


**Netz-Weise**  
Lernen von den Besten.

# Die Office Richtlinien



Alle Office-Richtlinien des Benutzers auf einen Blick



## Policy Maker Registry Extensions

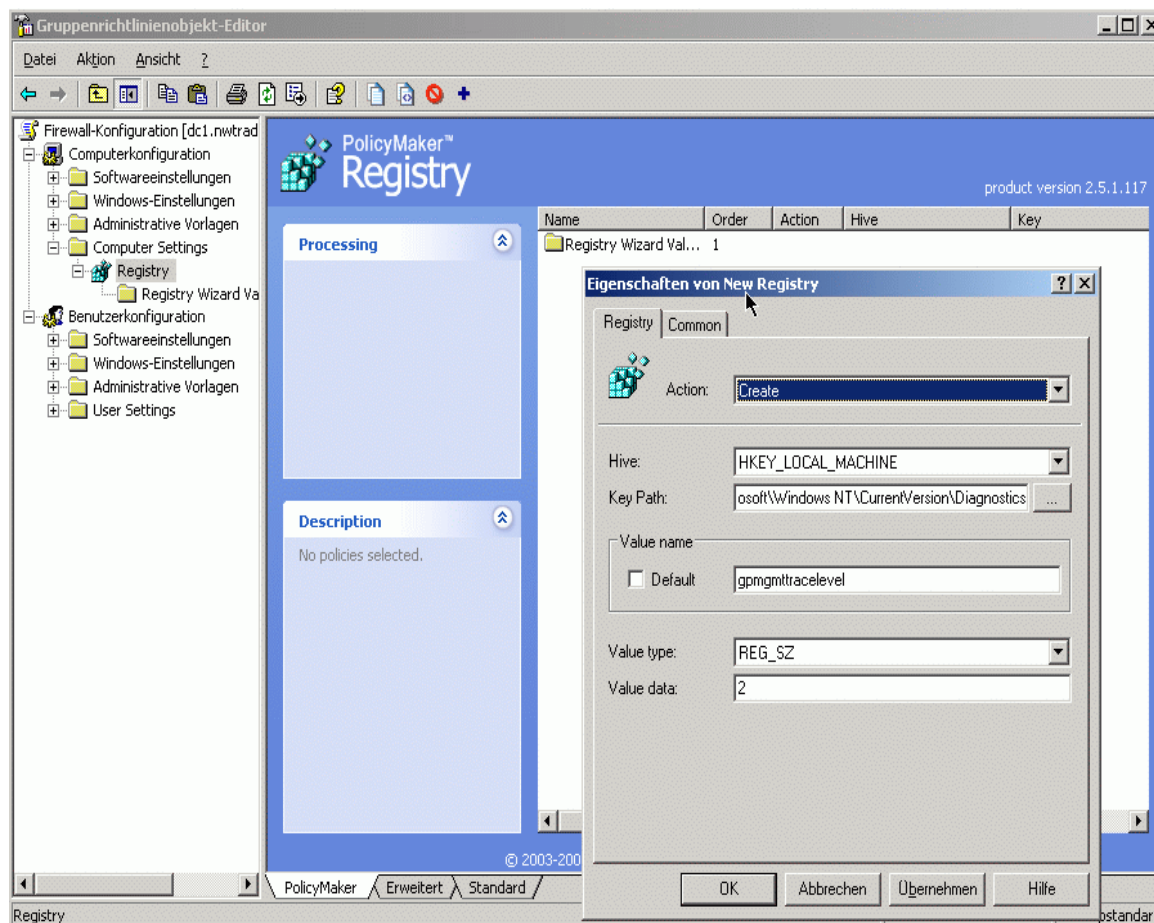
- Policy Maker Registry Extensions erweitert die Gruppenrichtlinien um ein Funktion zum erstellen und Löschen von Registry-Keys
- Registry Extensions integriert sich nahtlos in die Gruppenrichtlinien
- Kostenlos

wei|se (klug); 'Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Man...  
Weisen (↑ R 103)

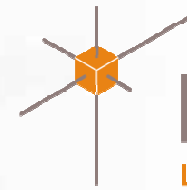


**Netz-Weise**  
Lernen von den Besten.

# Policy Maker Registry Extensions



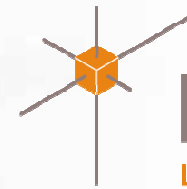
Einen Schlüssel zur Registry hinzufügen



## Desktop Standards GPO Vault

- GPO-Vault erweitert die GPMC um Funktionen zur Verwaltung von Gruppenrichtlinien
- GPO Vault ist kostenlos, während GPO Vault Enterprise kostenpflichtig ist
- Funktionalität:
  - Offline-Bearbeitung von Gruppenrichtlinien
  - Versionkontrolle von Gruppenrichtlinien
  - Rollenbasierte Delegation (Enterprise)
  - Check-In und Check-Out von Richtlinien (Enterprise)
  - Differenz-Reporting
  - GPO-Vorlagen

wei|se (klug); 'Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Man  
Weisen (↑ R 103)



**Netz-Weise**  
Lernen von den Besten.

# GPOvault

**Group Policy Management**

Change Control for nwtraders.net

Contents | Domain Delegation | Archive Location

Controlled | Uncontrolled | Pending | Templates | Recycle Bin

Group Policy Objects:

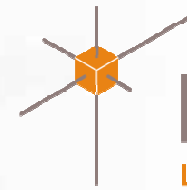
Name	Comp.	User	State	GPO Status	WMI Filter	Modified	Owner
Firewall-Konfiguration	8	0	Checked Out	Enabled	nur XP_SP2	22.03.2006 16:22:40	Holger V

These groups and users have the specified vault permissions for the selected GPO:

Name	Allowed Permission
Holger Voges (hvoges@nwtraders.net)	Full Control

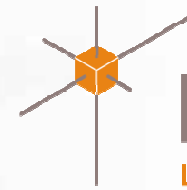
Buttons: Add... Remove Properties Advanced...

GPO-Vault als Erweiterung der GPMC



## True control template

- True Control Template ist eine Sammlung von Registry Einstellungen, die in eine ADM-Datei verpackt sind
- Das Template ist speziell für den Einsatz mit Terminal-Server- und Citrix-Umgebungen konzipiert
- Der Download ist kostenlos unter [www.loginconsultants.com](http://www.loginconsultants.com) möglich



## Tools von Fremdherstellern

- Kostenpflichtige Erweiterungen für Gruppenrichtlinien
  - Policy Maker von Desktop Standard
  - Specops Deploy (vereinfacht die Softwareverteilung)
  - NetIQ Group Policy Administrator (FAZAM 2000)

# Policy Maker

- Policy Maker Standard Edition integriert sich nahtlos in die Microsoft Verwaltungstools
- Mit Hilfe von zusätzlichen Client Side Extensions werden die Möglichkeiten der Richtlinien enorm erweitert
- Eine kleine Auswahl von Funktionen:
  - Ini/inf-Datei-Einstellungen konfigurieren
  - Outlook-Mailprofile konfigurieren
  - Dateien/Ordner anlegen/löschen
  - Laufwerke verbinden
  - Anzeigeeigenschaften einstellen
  - Energieoptionen konfigurieren
  - Geplante Tasks verwalten ...
- <http://www.desktopstandard.com/PolicyMakerStandard.aspx>

## Specops Deploy

- Specops Deploy ist eine Erweiterung der AD-Software-Bereitstellung
- Specops Deploy integriert sich nahtlos in den Group Policy Editor
- Mit Specops-Deploy ist ein zeitgesteuertes Bereitstellen von Software möglich
- Das Gruppieren von Software-Paketen mit einer Installations-Rangfolge wird möglich
- Mit Abhängigkeiten können Abhängigkeiten von Programmen bestimmt werden (GPMC benötigt .NET-Framework usw)
- <http://www.specopssoft.com/products/specopsdeploy/Default.asp>

# Group Policy Manager (GPM)

- Group Policy Manager ist die neueste Version von FAZAM 2000, das als eingeschränkte Version schon dem Windows 2000 Reskit beilag
- GPM erlaubt das Offline-editieren von Richtlinien
- GPM ermöglicht das Versionieren von Richtlinien
- Über das Ein-und Auschecken von Richtlinien ist es möglich, das zeitgleiche Bearbeiten von Richtlinien durch mehrere Administratoren zu verhindern
- Eine Änderungs-Protokollierung ermöglicht eine Gruppenrichtlinien-Historie
- GPM ermöglicht das systematische dokumentieren aller Änderungen
- [http://www.quest.com/group\\_policy\\_manager/](http://www.quest.com/group_policy_manager/)

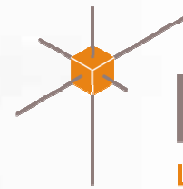
wei|se (klug); 'Weise, der  
-n, -n; ↑ R 5 ff. (kluger Man  
weisen (↑ R 108)



**Netz-Weise**  
Lernen von den Besten.

## Troubleshooting-Tools

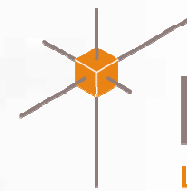
- RSOP
- Gpotool
- DCDiag
- GPRresult
- Group Policy Monitor
- Policy Reporter
- GP Inventory
- Windows Hilfe
- Policyspy
- GPO Logging ADM Template
- Registry.pol Viewer
- gpupdate
- Command Line GPO Refresh
- GPDisable
- Killpol
- gptime



## Troubleshooting mit RSOP's

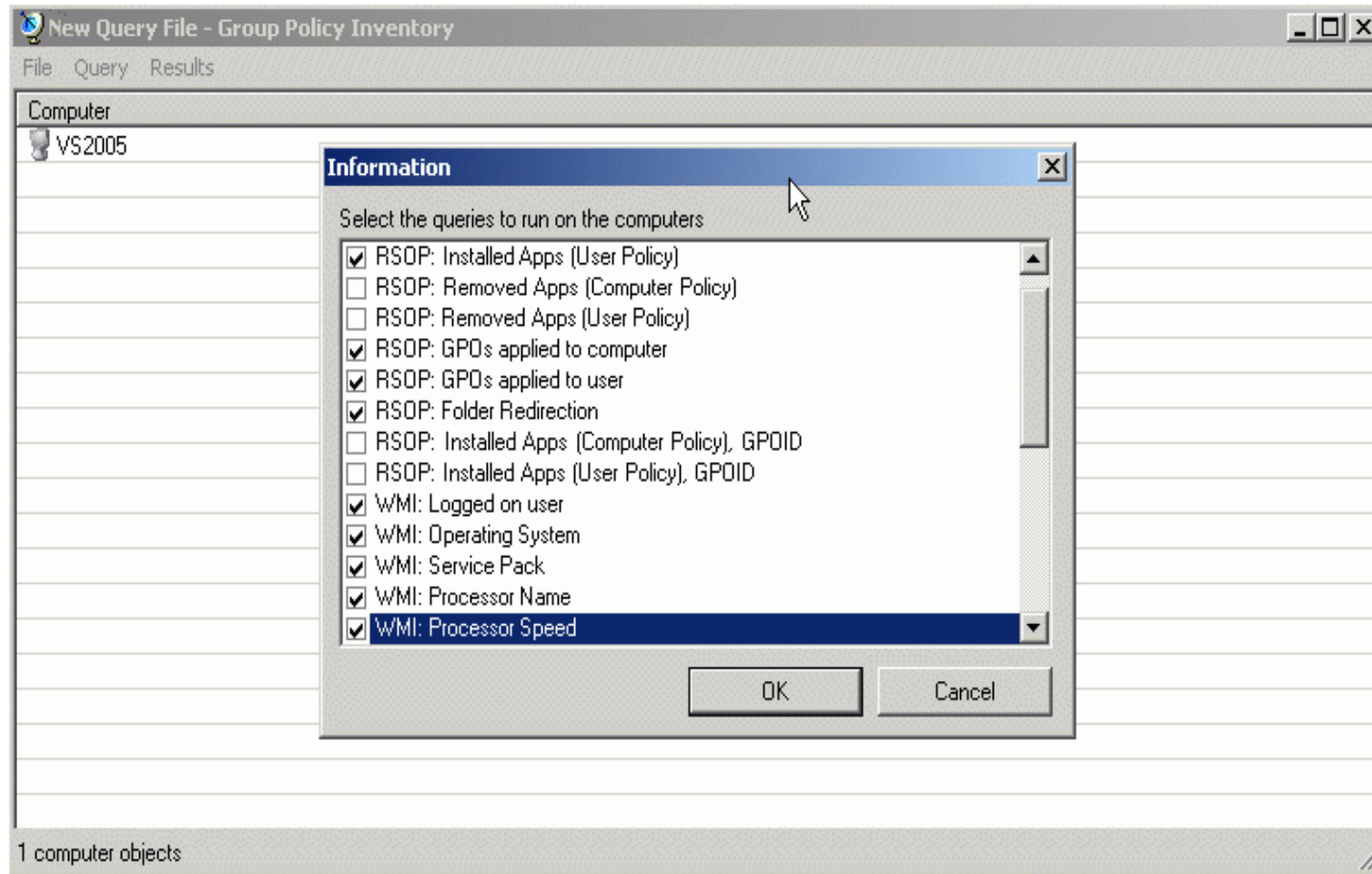
- GPRresult, Group Policy Monitor, GPMC, Policyspy und die Windows Hilfe nutzen RSOP
- GPRresult gehört bei XP zur Standard-Ausstattung, während es bei W2k installiert werden muß (Windows Support Tools)
- Der Group Policy Monitor (Dienst und Viewer) soll zentral die Gruppenrichtlinienabarbeitung protokollieren. Leider hat er Probleme mit Umlauten und ist daher auf deutschen Systemen nicht sauber lauffähig
- Der GPMonitor ist Teil des Windows Resource Kits
- Policyspy ist ebenfalls ein Reskit-Tool und kann RSOP's und andere Daten Fernabfragen

wei|se (klug); 'Weise, der  
-n, -n; ↑ R 5 ff. (kluger Man  
Weisen (↑ R 108)

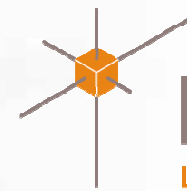


**Netz-Weise**  
Lernen von den Besten.

# Policspsy



Das Abfragefenster von Policspsy



## Gpotool

- GPOtool ist Teil des Windows Resource Kits
- Gpotool
  - überprüft die Richtlinien-Konsistenz
  - überprüft die Richtlinien-Replikation
  - zeigt Informationen über die einzelnen Gruppenrichtlinien-Objekte an
  - startet mit dem Parameter /v im ausführlichen Modus

weise (klug); Weisheit, Weisheit  
-n, -n; ↑ R 5 ff. (kluger Mensch)  
Weisheit R 105



**Netz-Weise**  
Lernen von den Besten.

# Gpresult und gpoutil

```
C:\WINDOWS\system32\cmd.exe
An 22.03.2006 um 17:06:05 erstellt

RSOP-Ergebnisse für NUTRADERS\hvoiges auf US2005 : Protokollierungsmodus

Betriebssystemtyp: Microsoft Windows XP Professional
Betriebssystemkonfiguration: Mitglied der Domäne/Arbeitsgruppe
Betriebssystemversion: 5.1.2600
Domänenname: NUTRADERS
Domänentyp: Windows 2000
Standortname: Standardname-des-ersten-Standorts
Zwischengespeichertes Profil: 
Lokales Profil: C:\Dokumente und Einstellungen\HVOIGES
Langsame Verbindung? Nein

COMPUTEREINSTELLUNGEN

CN=US2005,OU=Workstations,OU=Braunschweig_DC=nutraders_DC=net
Zeit der letzten Gruppenrichtlinienanwendung: 22.03.2006 at 17:05:18
Gruppenrichtlinie wurde angewendet von: dcl.nutraders.net
Gruppenrichtlinienschwellexwert für langsame Verbindung: 500 kbps

Angewendete Gruppenrichtlinienobjekte
-----
Windows Update
Firewall-Konfiguration
Default Domain Policy

Die folgenden Gruppenrichtlinie werden nicht angewendet, da sie herausgefiltert wurden.

Richtlinien der lokalen Gruppe
Filterung: Nicht angewendet <Leer>

Der Computer ist Mitglied der folgenden Sicherheitsgruppen:
-----
Administratoren
Jeder
Benutzer
US2005$
Domänencomputer
NETZWERK
Authentifizierte Benutzer

BENUTZEREINSTELLUNGEN

CN=Holger Voges,OU=Benutzer,OU=Braunschweig_DC=nutraders_DC=net
Zeit der letzten Gruppenrichtlinienanwendung: 22.03.2006 at 16:19:19
Gruppenrichtlinie wurde angewendet von: dcl.nutraders.net
Gruppenrichtlinienschwellexwert für langsame Verbindung: 500 kbps

Angewendete Gruppenrichtlinienobjekte
-----
Default Domain Policy

Die folgenden Gruppenrichtlinie werden nicht angewendet, da sie herausgefiltert wurden.

Richtlinien der lokalen Gruppe
Filterung: Nicht angewendet <Leer>

Der Benutzer ist Mitglied der folgenden Sicherheitsgruppen:
-----
Domänen-Benutzer
Jeder
Benutzer
Administratoren
INTERAKTIV
Authentifizierte Benutzer
LOKAL
Domänen-Admins
```

```
C:\Programme\Windows Resource Kits\Tools>gpoutil /v
Validating DCs...
Available DCs:
dcl.nutraders.net
Searching for policies...
Found 5 policies
=====
Policy {09F72725-FD85-4C8D-83B4-344C0575BFEE}
Friendly name: [Checked Out] Firewall-Konfiguration
Policy OK
=====
Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
Friendly name: Default Domain Policy
Policy OK
=====
Policy {525AF7C4-CB8E-49AE-A0CF-3F7884F28752}
Friendly name: Firewall-Konfiguration
Policy OK
=====
Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Friendly name: Default Domain Controllers Policy
Policy OK
=====
Policy {70754213-E6C1-4E90-8DD6-45B86563DDC6}
Friendly name: Windows Update
Policy OK
=====
Policies OK

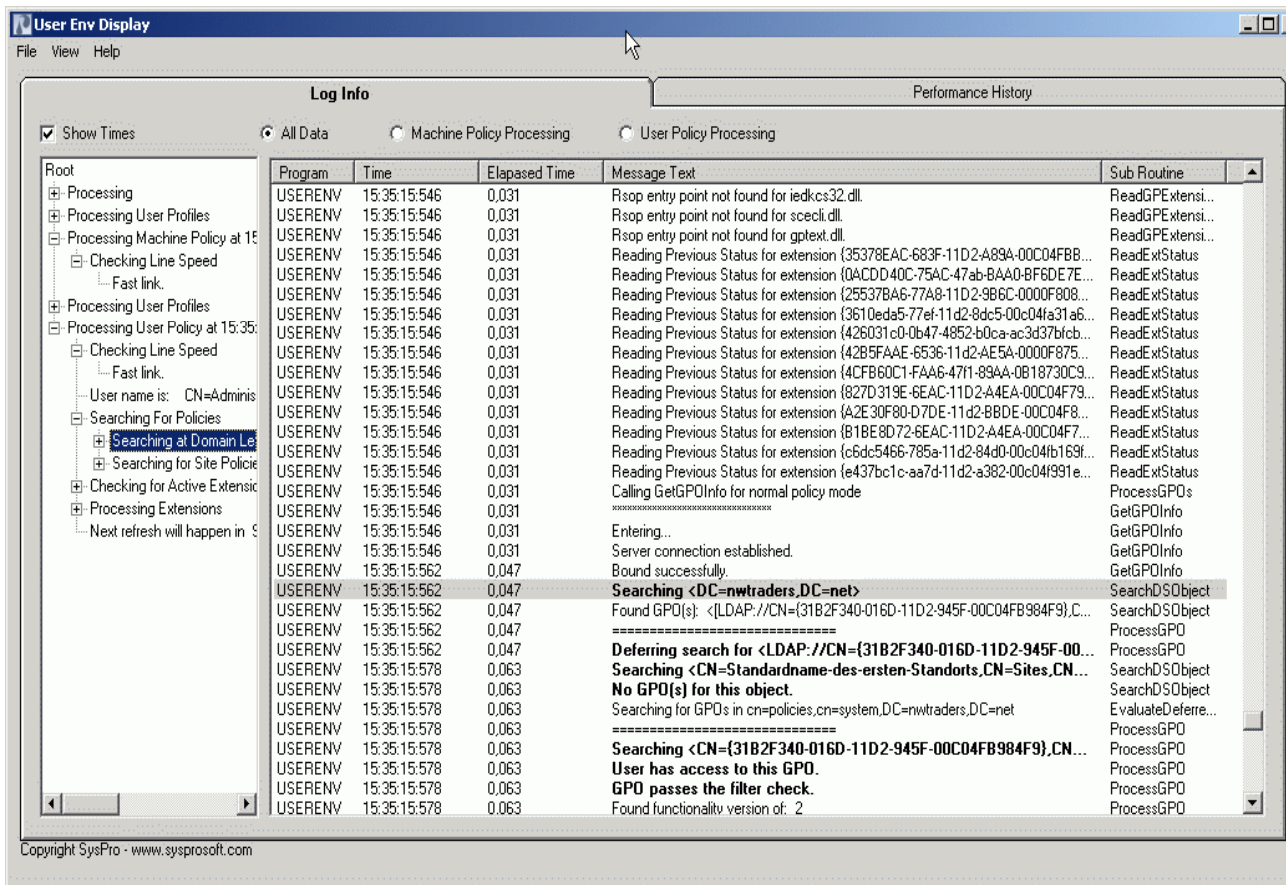
C:\Programme\Windows Resource Kits\Tools>
```

# Troubleshooting mit Logfiles

- Die Protokollierung der Gpo-Abarbeitung kann in der Registry aktiviert werden
- Policy Reporter formatiert die Log-Datei userenv.log lesbar  
<http://www.sysprosoft.com>
- Das GPO Logging Template aktiviert Protokollierung per gpo  
<http://www.gpoguy.com>

Gruppenrichtlinien-Kern und Registry CSE	%windir%\debug\usermode\userenv.log
Sicherheit CSE	%windir%\security\logs\winlogon.log
Ordnerumleitung	%windir%\debug\usermode\fddeploy.log
Software-Verteilung	%windir%\debug\usermode\apppgmt.log
Windows Installer (Softwareverteilung)	%windir%\temp\msi*.log
Windows Installer (benutzerinitiiert)	%temp%\msi*.log

# Policy Log Analyzer



**User Env Display**  
File View Help

**Log Info** Performance History

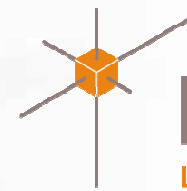
Show Times  All Data  Machine Policy Processing  User Policy Processing

Program	Time	Elapsed Time	Message Text	Sub Routine
USERENV	15:35:15:546	0,031	Rsoop entry point not found for iedkcs32.dll	ReadGPExtensi...
USERENV	15:35:15:546	0,031	Rsoop entry point not found for scecli.dll	ReadGPExtensi...
USERENV	15:35:15:546	0,031	Rsoop entry point not found for gptext.dll	ReadGPExtensi...
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {35378EAC-683F-11D2-A89A-00C04FBB...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {0ACDD40C-75AC-47ab-BAA0-BF6DE7E...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {25537BA6-77A8-11D2-9B6C-0000F808...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {3610eda5-77ef-11d2-9dc5-00c04fa31a6...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {42B031c0-0b47-4852-b0ca-ac3d37bfc...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {42B5FAAE-6536-11d2-AE5A-0000F875...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {4CFB60C1-FAA6-4711-89AA-0B18730C9...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {827D319E-6EAC-11D2-A4EA-00C04F79...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {A2E30F80-D7DE-11d2-BBDE-00C04F8...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {B1BE8D72-6EAC-11D2-A4EA-00C04F7...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {c6dc5466-785a-11d2-84d0-00c04fb169f...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {e437bc1c-aa7d-11d2-a382-00c04f91e...	ReadExtStatus
USERENV	15:35:15:546	0,031	Calling GetGPOInfo for normal policy mode	ProcessGPOs
USERENV	15:35:15:546	0,031	Entering...	GetGPOInfo
USERENV	15:35:15:546	0,031	Server connection established.	GetGPOInfo
USERENV	15:35:15:546	0,031	Bound successfully.	GetGPOInfo
USERENV	15:35:15:562	0,047	<b>Searching &lt;DC=nwtraders.DC-net&gt;</b>	SearchDSObject
USERENV	15:35:15:562	0,047	Found GPO(s): <LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},C...	SearchDSObject
USERENV	15:35:15:562	0,047	Deferring search for <LDAP://CN={31B2F340-016D-11D2-945F-00...	ProcessGPO
USERENV	15:35:15:578	0,063	<b>Searching &lt;CN=Standardname-des-ersten-Standorts,CN=Sites,CN=...</b>	SearchDSObject
USERENV	15:35:15:578	0,063	<b>No GPO(s) for this object.</b>	SearchDSObject
USERENV	15:35:15:578	0,063	Searching for GPOs in cn=policies,cn=system,DC=nwtraders.DC-net	EvaluateDeferre...
USERENV	15:35:15:578	0,063	<b>Searching &lt;CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=...</b>	ProcessGPO
USERENV	15:35:15:578	0,063	<b>User has access to this GPO.</b>	ProcessGPO
USERENV	15:35:15:578	0,063	<b>GPO passes the filter check.</b>	ProcessGPO
USERENV	15:35:15:578	0,063	Found functionality version of: 2	ProcessGPO

Copyright SysPro - www.sysprosoft.com

Der Policy Log Reporter von Sysprosoft zeigt die Userenv.log in lesbarer Form an

wei|se (klug); 'Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Man  
Weisen (↑ R 108)



**Netz-Weise**  
Lernen von den Besten.

# Ablaufzeit-Analyse

- Gptime zeigt die Zeit an, die eine einzelne Gruppenrichtlinie bis zum Beenden der Abarbeitung gebraucht hat
- Mit GPTIME kann die Anmeldezeit für Benutzer optimiert werden

<http://www.gpoguy.com>

```
C:\WINDOWS\system32\cmd.exe

C:\>gptime

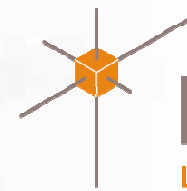
Computer Group Policy processing cycle:
STARTED: 17:10:21 on 3/22/2006
FINISHED: 17:10:22 on 3/22/2006
Total elapsed processing time: 0 hours, 0 minutes, 0 seconds and 953 msec.

User Account: Holger Group Policy processing cycle:
STARTED: 16:6:1 on 1/22/2006
FINISHED: 16:6:1 on 1/22/2006
Total elapsed processing time: 0 hours, 0 minutes, 0 seconds and 16 msec.

User Account: HVOGES Group Policy processing cycle:
STARTED: 17:11:20 on 3/22/2006
FINISHED: 17:11:20 on 3/22/2006
Total elapsed processing time: 0 hours, 0 minutes, 0 seconds and 268 msec.

User Account: administrator Group Policy processing cycle:
STARTED: 15:35:15 on 3/22/2006
FINISHED: 15:35:15 on 3/22/2006
Total elapsed processing time: 0 hours, 0 minutes, 0 seconds and 110 msec.

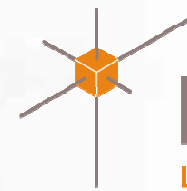
C:\>_
```



## Aktualisieren der Richtlinien

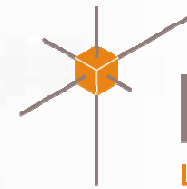
- GPupdate erzwingt unter Windows XP das Überprüfen auf neue Richtlinien
- GPupdate /force aktualisiert alle Richtlinieneinstellungen. Sonst werden nur neue oder geänderte Richtlinien angewendet.
- Specops GPUpdate ermöglicht eine Aktualisierung der Gruppenrichtlinien auf allen Clients zu erzwingen
- Specops GPupdate ist kostenlos!
- Download:

<http://www.specopssoft.com/products/specopsgpupdate/default.asp>



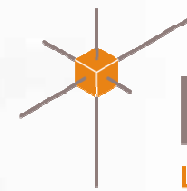
## Deaktivieren von Richtlinien

- Die Abarbeitung bestimmter Richtlinien wie Softwareeinschränkungen kann von einem Benutzer verhindert werden
- Hierfür sind KEINE Adminrechte erforderlich – ein kleines Tool (GPdisable) reicht
- Ein ausführliche Beschreibung inkl. GPdisable gibt es bei Sysinternals:  
<http://www.sysinternals.com/blog/2005/12/circumventing-group-policy-as-limited.html#113447773217906873>
- Killpol ist als Supporttool gedacht und braucht Adminrecht  
<http://www.petri.co.il/killpol.htm>



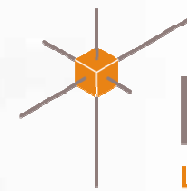
## Bekannte Probleme

- **Fehlermeldung:** “The following entry in the [strings] section is too long and has been truncated”  
(<http://support.microsoft.com/default.aspx?kbid=842933> )
- Richtlinien sind deaktivierbar (gpdisable)
- Zu große Sysvol-Ordner können sehr starken Replikationsverkehr erzeugen  
Lösung: Lokales Speichern der ADM´s  
(<http://support.microsoft.com/?id=816662#XSLTH4236121121120121120120>)



# Weiterführende Quellen bei MS

- Microsoft Group Policy Website  
<http://www.microsoft.com/windowsserver2003/technologies/management/grouppolicy/default.mspx>
- Technet Group Policy Center  
<http://technet2.microsoft.com/windowsserver/en/technologies/featured/gp/default.mspx>
- Implementing Common Desktop Management Scenarios with the Group Policy Management Console  
<http://technet2.microsoft.com/WindowsServer/en/Library/7b33dcd6-0ad2-44e8-82f8-962425b6cf8e1033.mspx>
- Enterprise Management with the Group Policy Management Console  
<http://www.microsoft.com/windowsserver2003/gpmc/default.mspx>
- Whitepaper: Introduction to Group Policy in Windows Server 2003  
<http://www.microsoft.com/windowsserver2003/techinfo/overview/gpintro.mspx>
- Whitepaper: Administering Group Policy with the GPMC  
<http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.mspx>
- MS Technet: Step-by-Step Guide to Understanding the Group Policy Feature Set  
<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/stepbystep/gpfeat.mspx>
- Technet – Group Policy Troubleshooting  
<http://technet2.microsoft.com/WindowsServer/en/Library/0c627456-5dfa-44db-b43a-e41c8f4f09231033.mspx>
- TechNet Support WebCast: Behandeln von Problemen mit Gruppenrichtlinien und Profilprobleme in einer Domäne-Umgebung, indem der Protokollierung von Userenv verwendet  
<http://support.microsoft.com/default.aspx?kbid=835302>
- MS KB: Troubleshooting Group Policy application problems  
<http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B250842>
- SO WIRD'S GEMACHT: Festlegen erweiterter Einstellungen in Internet Explorer mit Hilfe von Gruppenrichtlinienobjekten  
<http://support.microsoft.com/?kbid=274846>
- Group Policy Settings Reference  
<http://www.microsoft.com/downloads/details.aspx?FamilyID=7821C32F-DA15-438D-8E48-45915CD2BC14&displaylang=en>



## Andere Quellen

- Group Policy Wiki  
<http://grouppolicy.editme.com/>
- GPO-Guy  
<http://www.gpoguy.com/>
- Website von Mark Heitbrink (MVP) zum Thema Gruppenrichtlinien  
[www.gruppenrichtlinien.de](http://www.gruppenrichtlinien.de)
- Marks Sysinternals Blog: Circumventing Group Policy as a Limited User  
<http://www.sysinternals.com/blog/2005/12/circumventing-group-policy-as-limited.html>