LayerDREI

EDV-Schulungen

Windows-Welt

World‘s Best-
Managed Platform

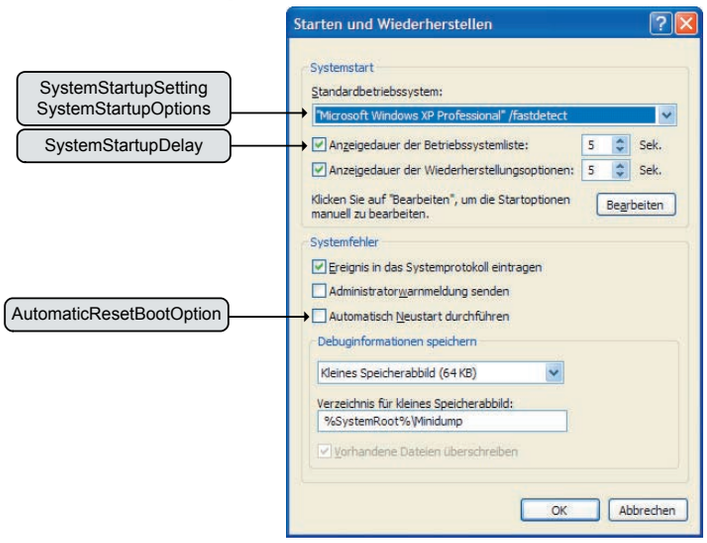
Automatisierung von
Windows NT4 /2000
/2003 mit Visual
Basic Script und
WMI

Ein ***LayerDREI***
Kompetenzabend mit
Dr. Tobias Weltner

Hamburger Straße 273c
Gebäude C4
38114 Braunschweig

fon.: 0531 / 380 80 95 - 0
fax: 0531 / 380 80 95 - 9
info@LayerDREI.de
www.LayerDREI.de

Computersystem und Verwandte



Bootmenü-Anzeigedauer setzen

```
WMIC ComputerSystem SET SystemStartupDelay=5
```

Bei Systemfehler neu starten

```
WMIC ComputerSystem SET AutomaticResetBootOption=True
```

Startmodus feststellen

```
WMIC ComputerSystem GET BootupState
```

Angemeldeten Benutzer bestimmen

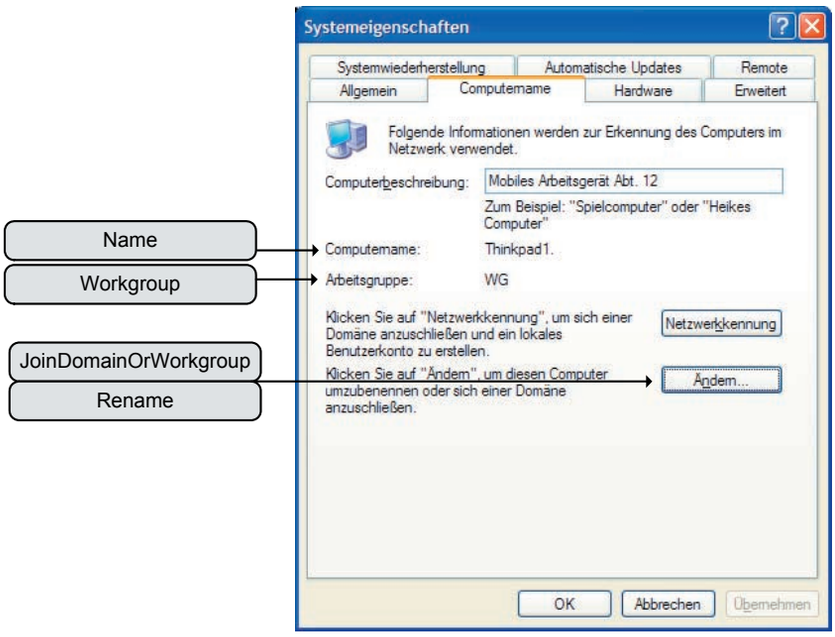
```
WMIC /USER:Administrator /PASSWORD:password /NODE:srs1 ComputerSystem GET UserName
```

Domäne feststellen

```
WMIC ComputerSystem WHERE "partofdomain=True" GET Domain, DomainRole
```

Netzwerkdienste bestimmen

```
WMIC ComputerSystem GET Roles
```



Computernamen ändern

```
WMIC ComputerSystem WHERE name!=NULL CALL Rename "WS23", "password", "Administrator"
```

Computernamen remote ändern

```
WMIC /AUTHLEVEL:Pktprivacy /USER:Administrator /PASSWORD:password /NODE:srs1 ComputerSystem WHERE name!=null call
rename "NEUERNAME", "password", "Administrator"
```

Computer in Arbeitsgruppe aufnehmen

```
WMIC ComputerSystem WHERE name!=NULL CALL JoinDomainOrWorkgroup "", 0, "AG2", "Administrator", "password"
```

Computer remote in Arbeitsgruppe aufnehmen

```
WMIC /AUTHLEVEL:Pktprivacy /USER:Administrator /PASSWORD:password /NODE:srs1 ComputerSystem WHERE name!=NULL CALL
JoinDomainOrWorkgroup "", 0, "AG2", "password", "Administrator"
```

Computer in Domäne aufnehmen

```
WMIC ComputerSystem WHERE name!=NULL CALL JoinDomainOrWorkgroup "", 3, "scriptinternals.de", "password",
"scriptinternals\Administrator"
```

Computer remote in Domäne aufnehmen

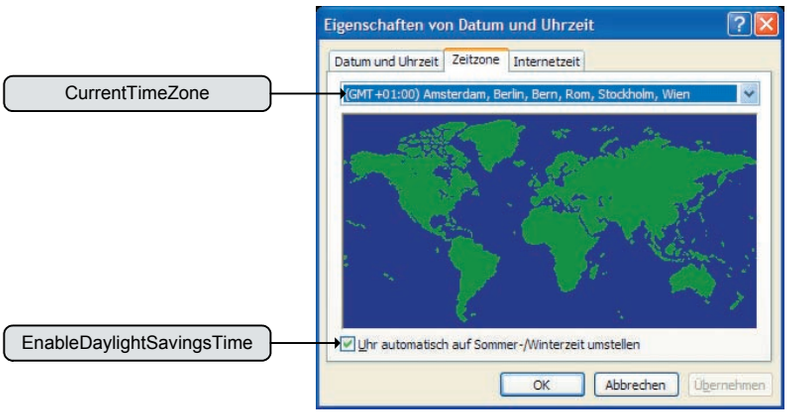
```
WMIC /AUTHLEVEL:Pktprivacy /USER:Administrator /PASSWORD:password /NODE:srs1 computersystem WHERE name!=NULL CALL
JoinDomainOrWorkgroup "", 3, "scriptinternals.de", "password", "scriptinternals\Administrator"
```

Computer aus Domäne entfernen, Computerkonto aktiviert lassen

```
WMIC ComputerSystem WHERE name!=NULL CALL UnjoinDomainOrWorkgroup 0, "password", "scriptinternals\Administrator"
```

Computer aus Domäne entfernen, Computerkonto sperren

```
WMIC ComputerSystem WHERE name!=NULL CALL UnjoinDomainOrWorkgroup 4, "password", "scriptinternals\Administrator"
```



Zeitzoneninformationen ermitteln

```
WMIC ComputerSystem GET CurrentTimeZone, DaylightInEffect, EnableDaylightSavingsTime
```

Zeitzone setzen

```
WMIC ComputerSystem SET CurrentTimezone=60
```

Sommerzeitumschaltung aktivieren

```
WMIC ComputerSystem SET EnableDaylightSavingsTime=True
```

Anzahl Prozessoren bestimmen

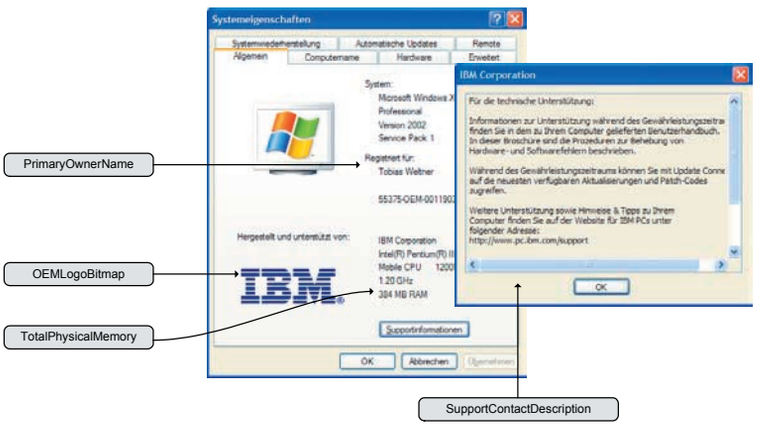
```
WMIC ComputerSystem GET NumberOfProcessors
```

Gesamten physikalischen Speicher bestimmen

```
WMIC ComputerSystem GET TotalPhysicalMemory
```

Besitzer des Systems ermitteln

```
WMIC ComputerSystem GET PrimaryOwnerName, PrimaryOwnerContact
```



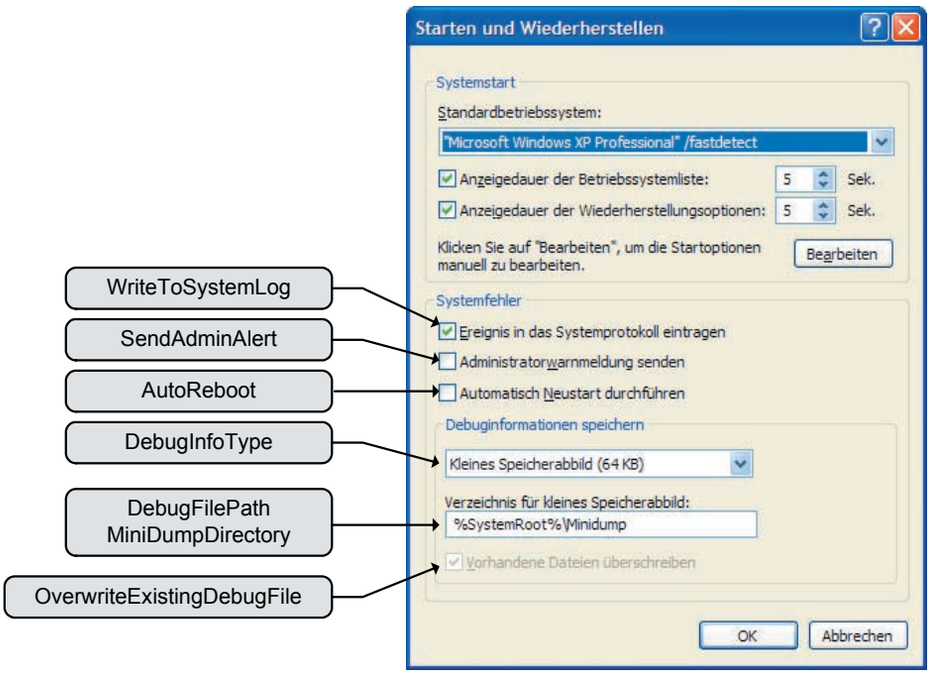
Systemfehler

Alle Informationen als HTML-Report ausgeben

```
WMIC /OUTPUT:%temp%\info.htm RecoverOS GET /FORMAT:hform
%temp%\info.htm
```

Restart-Optionen konfigurieren

```
WMIC RecoverOS SET DebugFilePath="%systemroot%\KERNERR.DMP", DebugInfoType=2, OverwriteExistingDebugFile=True,
AutoReboot=True, SendAdminAlert=True, WriteToSystemLog=True
```



Inventarinformationen

Alle Informationen als HTML-Report

```
WMIC /OUTPUT:%temp%\info.htm CSProduct GET /FORMAT:hform
%temp%\info.htm
```

UUID auflisten

```
WMIC csproduct GET uuid
```

Betriebssystem

Alle Informationen als HTML-Report

```
WMIC /OUTPUT:%temp%\info.htm OS GET /FORMAT:hform
%temp%\info.htm
```

Beschreibung setzen

```
WMIC OS SET Description="CAD/CAM-Arbeitsstation Gebäude 12"
```

Systemneustart

```
WMIC OS WHERE Primary=True CALL Reboot
```

Systemneustart remote

```
WMIC /USER:Administrator /PASSWORD:password /NODE:srs1 OS WHERE Primary=True CALL Reboot
```

Systemneustart remote trotz hängender Programme/Speicherabfragen

```
WMIC /USER:Administrator /PASSWORD:password /NODE:srs1 OS WHERE Primary=True CALL Win32Shutdown 6
```

System herunterfahren

```
WMIC OS WHERE Primary=True CALL Shutdown
```

System remote herunterfahren trotz hängender Programme

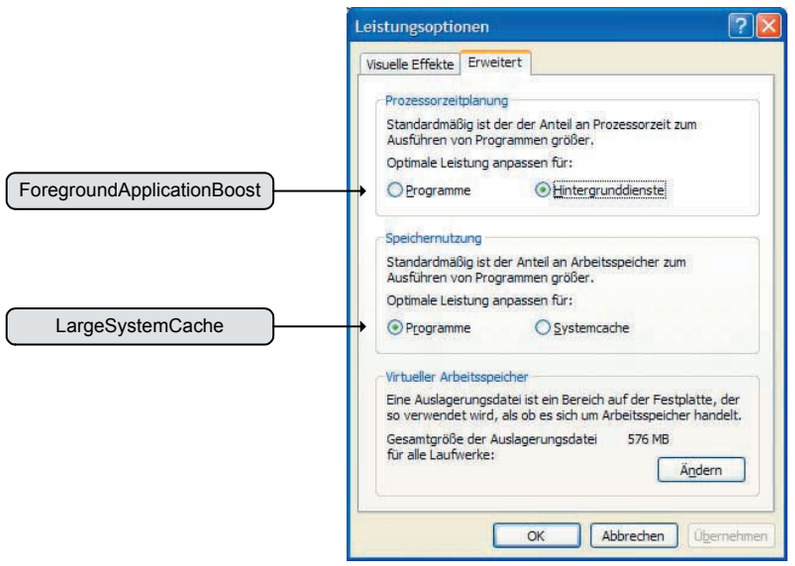
```
WMIC /USER:Administrator /PASSWORD:password /NODE:srs1 OS WHERE Primary=True CALL Win32Shutdown 5
```

System abschalten

```
WMIC OS WHERE Primary=True CALL Win32Shutdown 8
```

Benutzer abmelden

```
WMIC OS WHERE Primary=True CALL Win32Shutdown 0
```



Prozessorzeitplanung ändern

```
wmic OS SET ForegroundApplicationBoost=2
wmic OS SET ForegroundApplicationBoost=0
```

Lokale Systemzeit ermitteln

```
WMIC OS GET LocalDateTime
```

Zeitzone einstellen

```
WMIC OS SET CurrentTimeZone=60
```

Letzte Bootup-Zeit ermitteln

```
WMIC OS GET LastBootUpTime
```

Freien RAM-Speicher ermitteln

```
WMIC OS GET FreePhysicalMemory
```

Service-Pack-Informationen ermitteln

```
WMIC OS GET CSDVersion
```

Computernamen ermitteln

```
WMIC OS GET CSName
```

Verschlüsselungsstärke ermitteln

```
WMIC OS GET EncryptionLevel
```

Produkttyp ermitteln

```
WMIC OS GET ProductType
```

```
arrBits = Array("Small Business","Enterprise","Backoffice","Kommunikationen" _
, "Terminal","SmallBusiness (eingeschränkt)","Eingebettetes NT" _
```

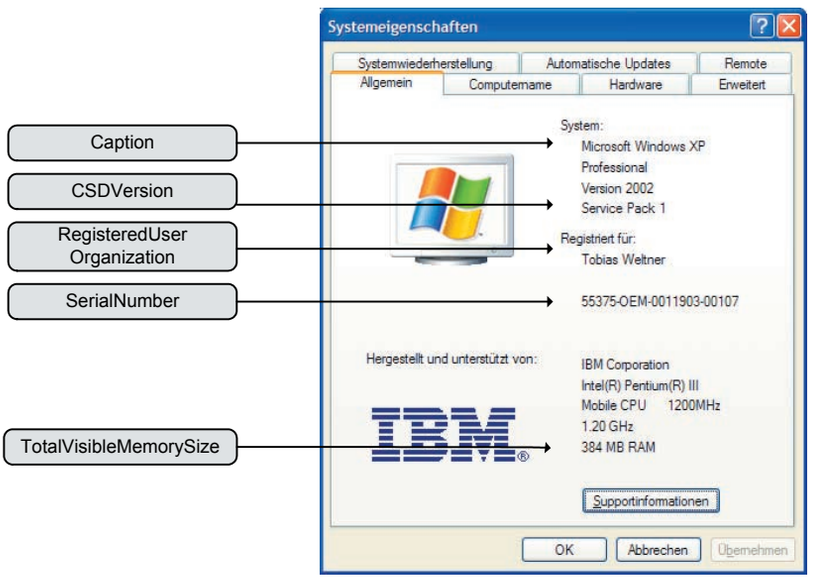
```
, "Data Center","Einzelner Benutzer","Personal","Blade","11","12","13" _
, "14", "15", "16", "17", "18", "19", "20", "21", "22", "23", "24", "25" _
, "26", "27", "28", "29", "NT-Arbeitsstation", "NT Server")
```

Seriennummer ermitteln

```
WMIC OS GET SerialNumber
```

Leistungsstatistik

```
WMIC OS GET NumberOfUsers
WMIC OS GET NumberOfProcesses
```



Registrierten Benutzer ermitteln

```
WMIC OS GET RegisteredUser
```

BIOS

Alle Informationen als HTML-Datei

```
wmic /output:%temp%\info.htm bios get /format:hform
%temp%\info.htm
```

Release-Datum und andere Informationen erfragen

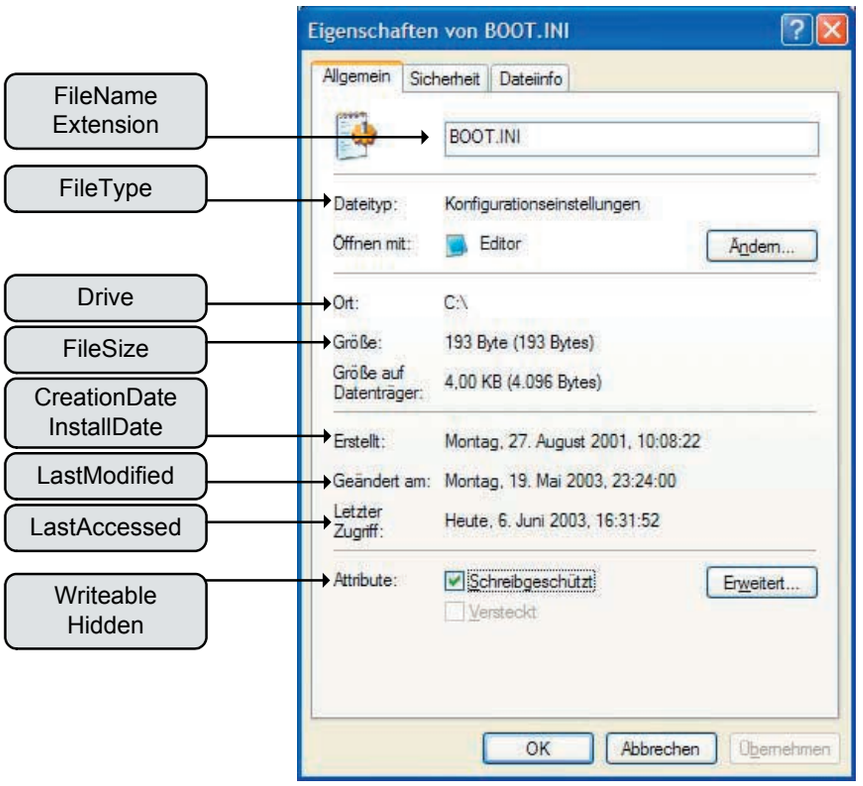
```
WMIC Bios GET ReleaseDate, Manufacturer, SMBIOSBIOSVersion
```

Boot-Konfiguration

Informationen in Konsole ausgeben

```
WMIC BootConfig GET /VALUE
```

Dateisystem



Alle Eigenschaften einer bestimmten Datei als HTML-Report

```
WMIC /OUTPUT:%temp%\ergebnis.htm DataFile "c:\\boot.ini" GET /FORMAT:hform
%temp\ergebnis.htm
```

Alle INF-Dateien im INF-Ordner, die mindestens 10.000 Byte groß sind

```
WMIC DataFile WHERE "Drive='C:' AND Path='\\WINDOWS\\INF\\' AND Extension='inf' AND FileSize>10000" GET /VALUE
```

Überforderung: alle EXE-Dateien irgendwo im Dateisystem

```
WMIC DataFile WHERE extension=exe" GET
```

Alle Dateien im Stammordner

```
WMIC DataFile WHERE "Path='\\'"
```

Alle Dateien im Ordner C:

```
WMIC DataFile WHERE "Path='\\' AND Drive='C:'"
```

Dateien kopieren

```
WMIC DataFile "c:\\boot.ini" CALL copy "c:\\boot.ini.bak"
```

Dateien löschen

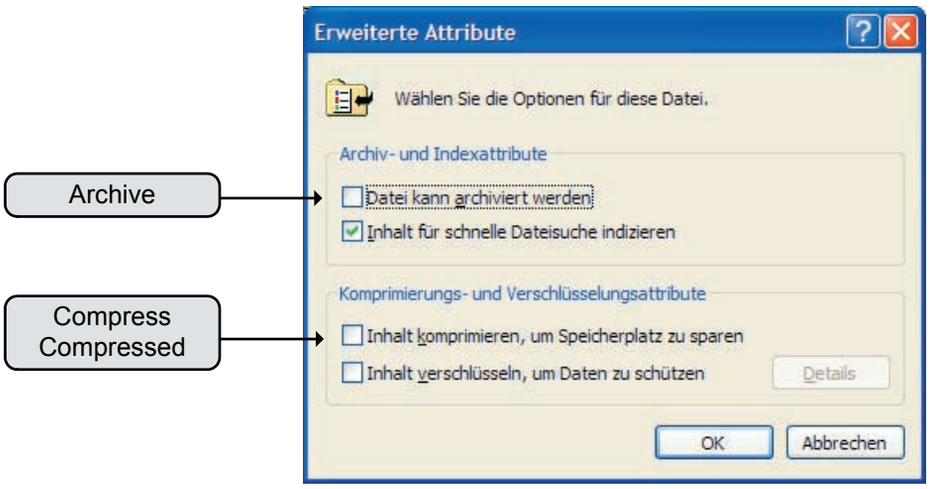
```
WMIC DataFile "c:\\boot.ini.bak" CALL Delete
```

Dateien umbenennen

```
WMIC DataFile "c:\\boot.ini.tmp" CALL Rename "c:\\boot.ini.bak"
```

Dateien komprimieren

```
WMIC DataFile WHERE "Drive='C:' AND Path='\\windows\\' AND Extension='vbs' AND Compressed=false" CALL Compress
```



Besitzrechte übernehmen

```
WMIC DataFile "c:\\boot.ini" CALL TakeOwnership
```

Zugriffsberechtigungen prüfen

```
WMIC DataFile "c:\\boot.ini" CALL GetEffectivePermission 1
```

Access Control Lists sichtbar machen

```
WMIC PATH Win32_LogicalFileSecuritySetting WHERE "Path='c:\\boot.ini'" CALL GetSecurityDescriptor
```

Ordner

Eigenschaften des Windows-Ordners ermitteln

```
WMIC FSDir "c:\\windows" GET /VALUE
WMIC /OUTPUT:%temp%\info.htm FSDir "C:\\WINDOWS" GET /FORMAT:hform
```

Unterordner eines Ordners auflisten

```
WMIC FSDir WHERE "Drive='C:' AND Path='\\Windows\\'" GET CSName, EightDotThreeFileName
```

Dateien auflisten, die in einem Ordner enthalten sind

```
WMIC DataFile WHERE "Drive='C:' AND Path='\\Windows\\'" GET CSName, EightDotThreeFileName
```

CD-ROM-Laufwerke

HTML-Report

```
WMIC /OUTPUT:%temp%\info.htm CDROM GET /FORMAT:hform
%temp%\info.htm
```

Alle CD-ROM-Laufwerke auflisten

```
WMIC CDROM GET Name
```

Bestimmtes Laufwerk abfragen

```
WMIC CDROM "d:" GET MediaLoaded, VolumeName
```

Festplatten

HTML-Report

```
WMIC /OUTPUT:%temp%\info.htm DiskDrive GET /FORMAT:hform
%temp%\info.htm
```

Bestimmtes Laufwerk ansprechen

```
WMIC DiskDrive 0 GET /VALUE
```

Logische Laufwerke

Laufwerksinventarisierung

```
WMIC /OUTPUT:%temp%\info.htm LogicalDisk GET Name, Description, FileSystem,FreeSpace, Size /FORMAT:htable
```

Freier Speicherplatz

```
WMIC LogicalDisk "c:" GET FreeSpace
```

Laufwerk überprüfen

```
WMIC LogicalDisk "c:" CALL chkdsk
```

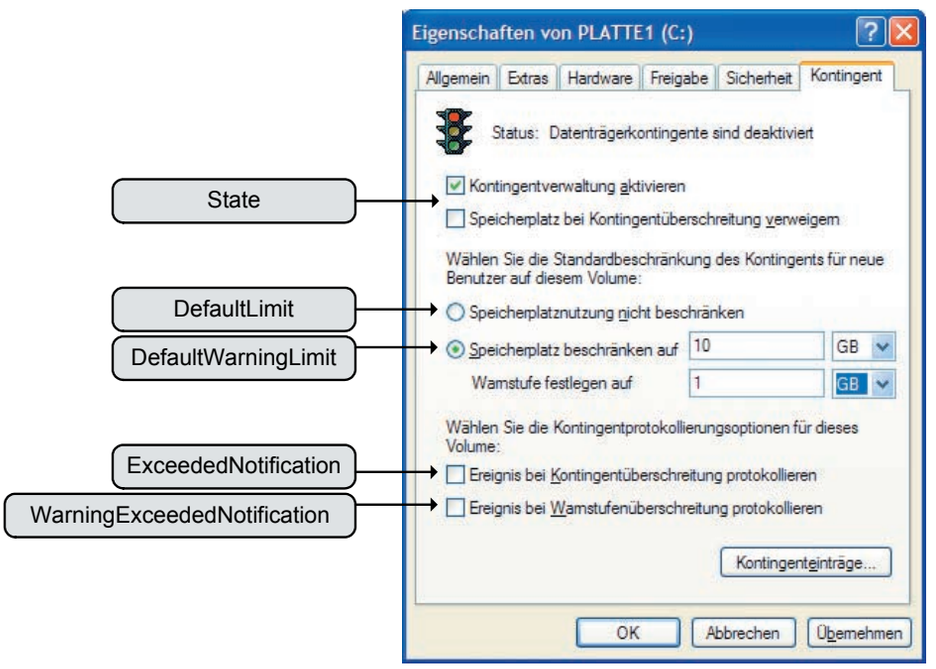
Kontingentverwaltung

HTML-Report

```
WMIC /OUTPUT:%temp%\info.htm QuotaSetting GET /FORMAT:hform
%temp%\info.htm
```

Laufwerke mit Kontingentverwaltung

```
WMIC QuotaSetting GET VolumePath, State
```



Laufwerke mit abgeschalteter Kontingentierung

```
WMIC QuotaSetting WHERE "state=0" GET VolumePath
```

Kontingentverwaltung auf allen Laufwerken aktivieren

```
WMIC QuotaSetting SET State=1
```

Kontingentverwaltung auf C: aktivieren

```
WMIC QuotaSetting WHERE "VolumePath='C:\\'" SET State=1
```

Warn- und Kontingentgrenzen festlegen

```
WMIC QuotaSetting WHERE "State=1 OR State=2" SET DefaultLimit=10737418240
WMIC QuotaSetting WHERE "State=1 OR State=2" SET DefaultWarningLimit=8589934592
```

Grenzwerte auf bestimmten Laufwerken festlegen

```
WMIC QuotaSetting WHERE "VolumePath='C:\\' AND (State=1 OR State=2)" SET DefaultLimit=10737418240
WMIC QuotaSetting WHERE " VolumePath='C:\\' AND (State=1 OR State=2)" SET DefaultWarningLimit=8589934592
```

Kontingentgrenzen entfernen

```
WMIC QuotaSetting WHERE "VolumePath='C:\\'" SET DefaultLimit=18446744073709551615
WMIC QuotaSetting WHERE "VolumePath='C:\\'" SET DefaultWarningLimit=18446744073709551615
```

Ereignislogbuch-Protokollierung

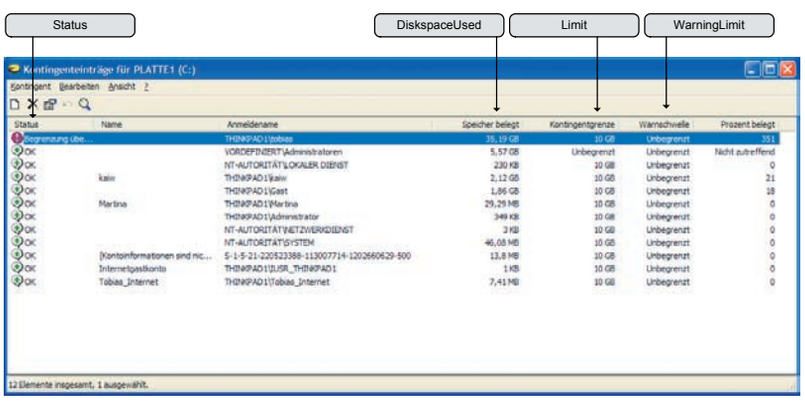
```
WMIC QuotaSetting SET ExceededNotification=True
WMIC QuotaSetting SET WarningExceededNotification=True
```

Kontingenteinträge

Benutzer mit überschrittenem Kontingent

```
WMIC DiskQuota WHERE Status=2 GET User, VolumePath
```

```
WMIC /OUTPUT:%temp%\info.htm DiskQuota WHERE Status=2 GET User, VolumePath /FORMAT:htable
%temp%\info.htm
```



Bildschirm

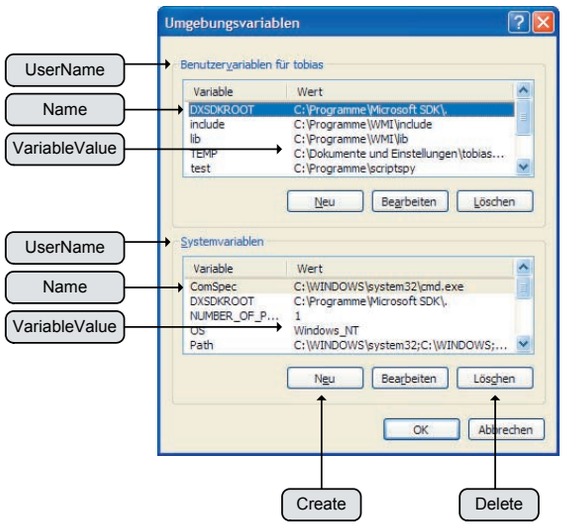
Hintergrundbilder aller Benutzer

```
WMIC Desktop GET Wallpaper, Name
```

Umgebungsvariablen

HTML-Report

```
WMIC /OUTPUT:%temp%\info.htm Environment GET /FORMAT:hform
%temp%\info.htm
```



Umgebungsvariable lesen

```
WMIC Environment WHERE Name="temp" GET VariableValue, Name, UserName
```

Umgebungsvariable eines Users lesen

```
WMIC Environment WHERE "Name='temp' AND UserName='ws82\\tobias'" GET VariableValue, Name, UserName
```

Umgebungsvariable ändern

```
WMIC Environment WHERE "UserName='ws20\\martina' AND Name='temp'" SET VariableValue="c:\specialtemp"
```

Neue Umgebungsvariable

```
wmic environment create name="folder", username="ws02\Tobias",variablevalue= "%programfiles%\Scriptspy"
```

Umgebungsvariable löschen

```
WMIC Environment WHERE Name="folder" delete
```

Auslagerungsdatei-Einstellungen

Maximalgröße ändern

```
C:\>WMIC PageFileSet WHERE Name="C:\\pagefile.sys" SET MaximumSize=1300
```

Auslagerungsdatei

Auslagerungsdateien ermitteln

```
WMIC PageFile GET Name, AllocatedBaseSize, CurrentUsage
```

Drucker

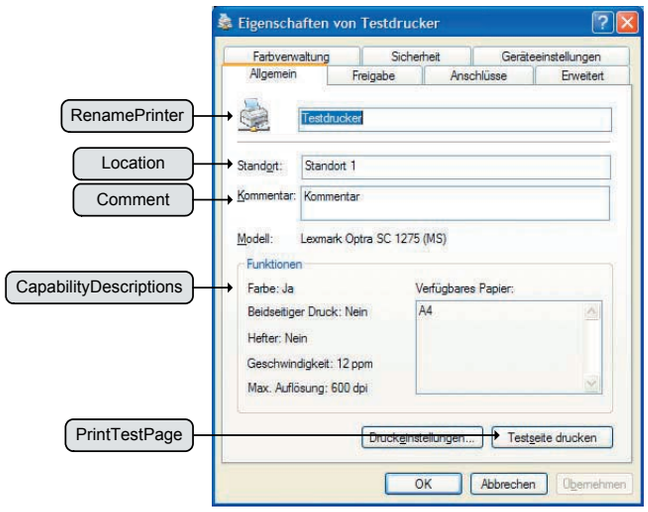
Alle Drucker auflisten

```
WMIC Printer GET Name
```

Detailinformationen zu einem bestimmten Drucker

```
WMIC Printer "Test1" GET /VALUE
```

```
WMIC /OUTPUT:%temp%\drucker.htm Printer "Test1" GET /FORMAT:hform
%temp%\drucker.htm
```



Alle Aufträge löschen

```
WMIC Printer "Test1" CancelAllJobs
```

Standortangaben

```
WMIC Printer Testdrucker SET Location="Standort 1", Comment="Farbdrucker"
```

Drucker umbenennen

```
WMIC Printer "Test1" RenamePrinter "Testdrucker"
```

Standarddrucker festlegen

```
WMIC Printer "Lexmark Optra SC 1275 PS" SetDefaultPrinter
```

Drucker anhalten

```
WMIC Printer "Testdrucker" Pause
```

Druckerpriorität festlegen

```
WMIC Printer "Testdrucker" SET Priority=5
```

Spooler abschalten

```
WMIC Printer "Testdrucker" SET Direct=True
```

Spooler einschalten

```
WMIC Printer "Testdrucker" SET Queued=True
```

Drucker entfernen

```
WMIC Printer Test2 Delete
```

```
wmic printer where name!=null delete
```

Druckaufträge

Druckaufträge auflisten

```
WMIC PrintJob GET /VALUE
```

Druckaufträge eines bestimmten Druckers auflisten

```
WMIC PrintJob WHERE "Name LIKE '%Testdrucker,%'" GET Document, Owner
```

```
WMIC /OUTPUT:%temp%\print.htm PrintJob WHERE "Name LIKE '%Testdrucker,%'" GET Document, Owner, ElapsedTime,
PagesPrinted /FORMAT:htable:"sortby=Owner"
%temp%\print.htm
```

Druckauftrag anhalten

```
WMIC PrintJob WHERE "Name LIKE '%Testdrucker,%'" GET Document, Owner, JobId
```

Alle Druckaufträge eines Druckers anhalten

```
WMIC PrintJob WHERE "Name LIKE '%Testdrucker,%'" Pause
```

Alle Druckaufträge eines Printservers anhalten

```
WMIC PrintJob WHERE JobId!=NULL Pause
```

Netzwerkkarten

HTML-Report

```
WMIC /OUTPUT:%temp%\info.htm NIC GET /FORMAT:hform
%temp%\info.htm
```

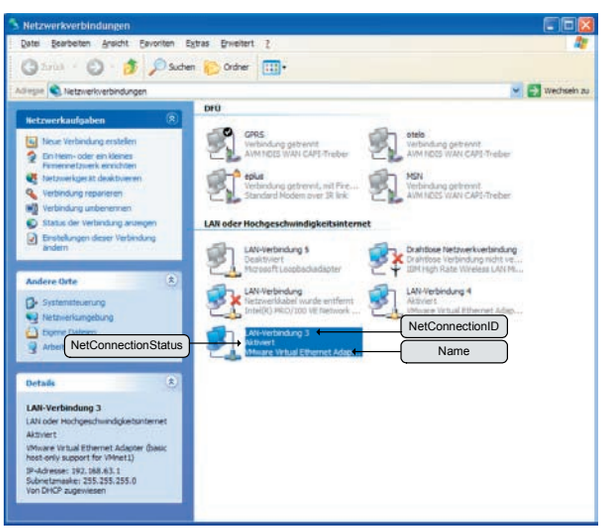
MAC-Adresse bestimmen

```
WMIC NIC GET Name, MACAddress /VALUE
WMIC NIC WHERE MACAddress!=NULL GET Name, MACAddress /VALUE

WMIC /OUTPUT:%temp%\ergebnis.htm NIC WHERE macaddress!=NULL GET Name, MACAddress /FORMAT:htable:"sortby=MACAddress"
%temp%\ergebnis.htm
```

Bestimmte Netzwerkkarte ansprechen

```
WMIC NIC WHERE AdapterTypeId=0 GET Name
```



Netzwerkverbindung ermitteln

```
WMIC NIC WHERE "NetConnectionId!=NULL" GET /VALUE
```

Verbundene Netzwerkkarten finden

```
WMIC NIC WHERE "NetConnectionId!=NULL AND netconnectionstatus=2" GET Name
```

Netzwerkkarten listen, die in Netzwerkverbindungen aufgeführt sind

```
WMIC NIC WHERE "NetConnectionId=NULL" GET Name
```

Netzwerkkarten-Konfiguration

HTML-Report

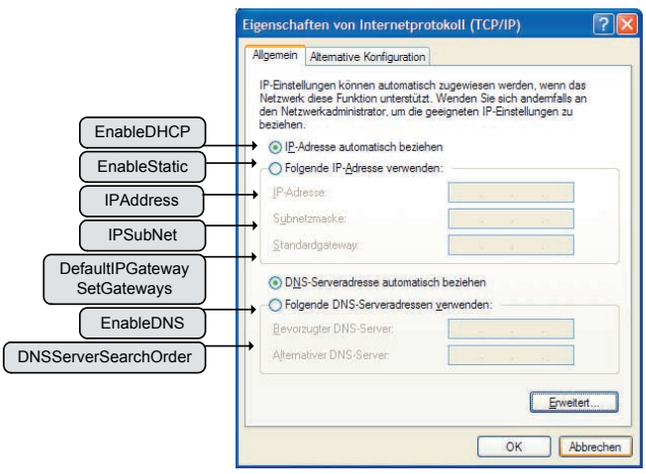
```
WMIC /OUTPUT:%temp%\info.htm NICConfig GET /FORMAT:hform
%temp%\info.htm
```

Indexzahlen der Netzwerkkarten listen

```
WMIC NIC WHERE NetConnectionID!=NULL GET Index, NetConnectionID
```

Netzwerkkarten-Konfiguration über Indexzahl ansprechen

```
WMIC NICConfig WHERE DeviceID=5 GET /VALUE
```



IPAdresse ermitteln

```
WMIC NICConfig 1 GET IPAddress, IPSubnet
```

DHCP verwenden

```
WMIC NICCONFIG 1 CALL EnableDHCP
```

IP-Adresse zuweisen

```
WMIC NICCONFIG 1 CALL EnableStatic ("10.10.10.252", "10.10.10.253"), ("255.255.0.0","255.255.0.0)
```

Gateways ermitteln

```
WMIC NICCONFIG 1 GET DefaultIPGateway
```

Gateways setzen

```
WMIC NICCONFIG 1 CALL SetGateways ("10.10.10.250")
```

Freigaben

Shares auflisten

```
WMIC /OUTPUT:%temp%\info.htm Share GET /FORMAT:hform
%temp%\info.htm
```

Shareinformationen anzeigen

```
WMIC share "C$" GET /VALUE
```

Neue Freigabe anlegen

```
WMIC share CALL create "","WMIC-Share",5,"PUBLIC","","C:\TEST",0
```

Freigabe löschen

```
WMIC share "PUBLIC" CALL Delete
```

Netzlaufwerke

Übersicht über Netzlaufwerke

```
WMIC netuse GET caption, Name

WMIC netuse GET localname, remotepath

WMIC /OUTPUT:%temp%\info.htm NetUse GET /FORMAT:hform
%temp%\info.htm
```

Laufende Prozesse

Alle laufenden Prozesse

```
WMIC /OUTPUT:%temp%\liste.htm Process GET Name, CommandLine, Handle /FORMAT:htable:"sortby=Name"
%temp%\liste.htm
```

Bestimmten Prozess finden

```
WMIC Process WHERE Name="notepad.exe" GET Name, Handle /VALUE
```

Ähnliche Prozesse finden

```
WMIC Process WHERE "CommandLine LIKE '%svchost%'" GET
```

Bestimmte Prozesse killen

```
WMIC Process WHERE Name="notepad.exe" CALL Terminate 0
WMIC Process 3968 Terminate 0
```

Prozesse killen, die bestimmte Datei geöffnet haben

```
WMIC Process WHERE "commandline like '%c:\\temp.txt%'" CALL Terminate 0
```

Neuen Prozess starten

```
WMIC Process CALL Create "regedit.exe"
```

Prozessinformationen über Handle erfragen

```
WMIC Process 1768 GET /VALUE
```

Priorität ändern

```
WMIC Process 1768 SetPriority 128
WMIC Process WHERE Name="explorer.exe" setpriority 64
```

Geplante Tasks

Alle Jobs auflisten

```
WMIC /OUTPUT:%temp%\info.htm Job GET /FORMAT:hform
%temp%\info.htm
```

Bestimmte Jobs auflisten

```
WMIC job WHERE "Command LIKE '%defrag%'" GET JobId, StartTime
```

Auftrag für einmalige Ausführung einrichten

```
WMIC job CALL Create "defrag c:",0 ,0 , False, False, "********183000.000000+120"
```

Autostart-Programme

Alle Autostartprogramme zeigen

```
WMIC /OUTPUT:%temp%\info.htm StartUp GET /FORMAT:hform
%temp%\info.htm
```

Autostartprogramme für alle Benutzer

```
WMIC startup WHERE user="All Users" GET command, location
```

Autostartprogramme für spezifische Benutzer

```
WMIC startup WHERE user="scriptinternals\\TobiasW" GET command, location
```

Informationen zu Autostartprogrammen finden

```
WMIC startup "McAfee Guardian" GET /VALUE
WMIC startup WHERE "command like '%rulaunch%'" GET /VALUE
```

Dienste

Lokalisierte und allgemeine Dienstnamen auflisten

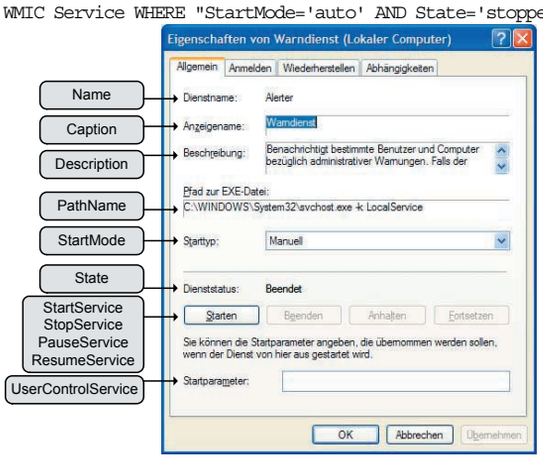
```
WMIC /OUTPUT:%temp%\dienste.htm Service GET Name, Caption /FORMAT:htable:"sortby=Caption"
%temp%\dienste.htm
```

Informationen zu einem bestimmten Dienst

```
WMIC Service WHERE Caption="Warndienst" GET /VALUE
WMIC Service WHERE "Name='Alerter'" GET /VALUE
WMIC Service "Alerter" GET /VALUE
```

Kritische Dienste finden

```
WMIC Service WHERE "StartMode='auto' AND State='stopped'" GET Caption
```



Spezifische Informationen eines Dienstes

```
WMIC Service Alerter GET PathName
```

Dienst stoppen

```
WMIC Service "Alerter" CALL StopService
```

Dienst killen

```
C:\>WMIC Service "Alerter" GET ProcessId
ProcessId
1392
C:\>wmic process 1392 terminate
```

Dienst starten

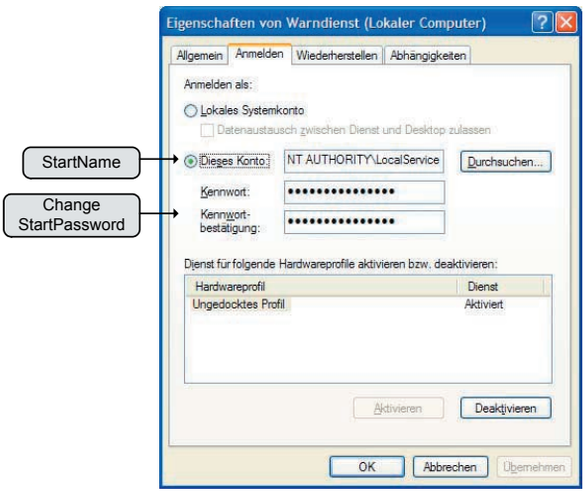
```
WMIC Service tlntsvr StartService
```

Deaktivierte Dienste aktivieren

```
WMIC Service tlntsvr ChangeStartMode "Manual"
```

Dienste unwiderruflich löschen

```
WMIC Service tlntsvr Call Delete
```



Ungewöhnliche Dienstkonten finden

```
C:\>WMIC Service WHERE "NOT (StartName LIKE '%LocalService%' OR StartName LIKE '%LocalSystem%' OR StartName LIKE
'%NetworkService%')" GET Caption, Name, StartName
```

Softwarepakete

Installierte MSI-Pakete auflisten

```
WMIC Product GET Name, Version
```

```
WMIC /OUTPUT:%temp%\software.htm Product GET Name, Version /FORMAT:htable:"sortby=Name"
```

Informationen zu bestimmtem Produkt

```
WMIC Product "Microsoft Office XP Professional" GET /value
```

Softwarepaket lokal installieren

```
WMIC Product CALL Install True, "", "\\srs1\software\spy.msi"
```

Softwarepaket remote installieren

```
WMIC /NODE:srs1 Product CALL Install True, "", c:\software\spy.msi"
```

Softwarepaket deinstallieren

```
WMIC Product "Scripting Spy Trial" CALL Uninstall
```

Softwarepaket remote deinstallieren

```
C:> WMIC /USER:scriptinternals\Administrator /NODE:srs1 Product "Scripting Spy Trial" CALL Uninstall
```

Hotfixes

Alle Hotfixes auflisten

```
WMIC qfe GET /value
```

```
WMIC /OUTPUT:%temp%\qfe.htm qfe GET /FORMAT:htable:"sortby=HotFixID"
%temp%\qfe.htm
```

Konten

SID des Administrator-Kontos ermitteln

```
WMIC PATH Win32_Account WHERE Name="Administrator" GET Sid
```

SID-Liste generieren

```
WMIC /output:%temp%\ergebnis.htm PATH Win32_Account GET Sid, Name /FORMAT:htable:"sortby=SID"
```

Lokale Konten auflisten

```
WMIC PATH Win32_Account WHERE LocalAccount=True GET Name
```

Domänenkonten auflisten

```
WMIC PATH Win32_Account WHERE LocalAccount=False GET Name, Domain
```

Benutzerkonten

Konten, bei denen Kennwort nie abläuft

```
WMIC UserAccount  WHERE passwordexpires=False GET domain, Name
```

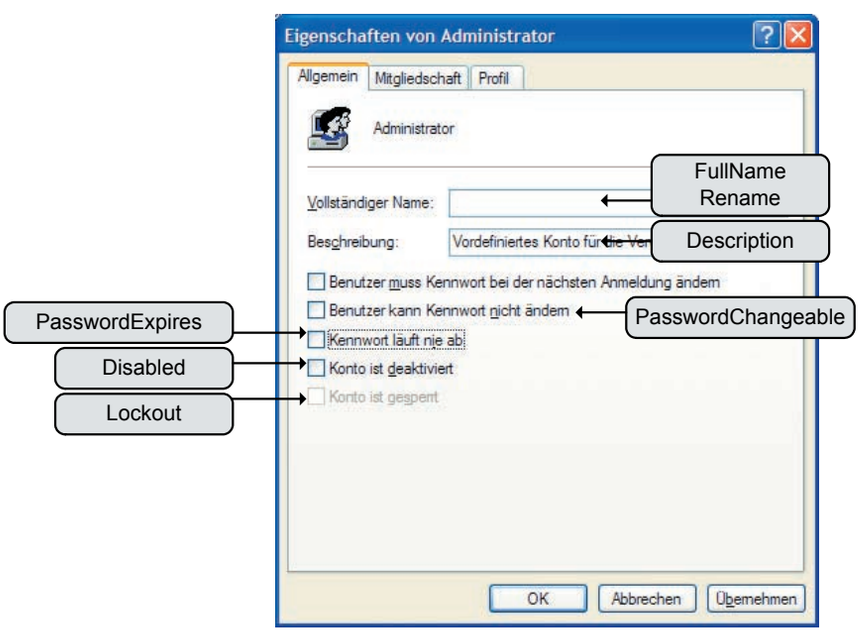
```
WMIC /output:%temp%\ergebnis.htm UserAccount  WHERE passwordexpires=False GET domain, Name /FORMAT:htable:"sortby=Name"
```

Kennwort mit zeitlicher Begrenzung

```
WMIC UserAccount WHERE Name="test" SET PasswordExpires=True
```

Nicht betriebsbereite Konten finden (gesperrt/disabled)

```
WMIC UserAccount  WHERE status!="OK" GET Name, lockout, disabled
```



Konto deaktivieren

```
WMIC UserAccount  WHERE Name="test" SET Disabled=True
```

Gesperrtes Konto entsperren

```
WMIC UserAccount  WHERE Name="test" SET Lockout=False
```

Konto umbenennen

```
WMIC UserAccount WHERE Name="test" CALL Rename "KMeier"
```

Gruppen

Gruppe umbenennen

```
WMIC Group WHERE Name="AlterName" CALL Rename "NeuerName"
```

Systemkonten

Systemkonten auflisten

```
WMIC SysAccount GET Name
```

Ereignislogbuch

Ereignislogbuch sichern

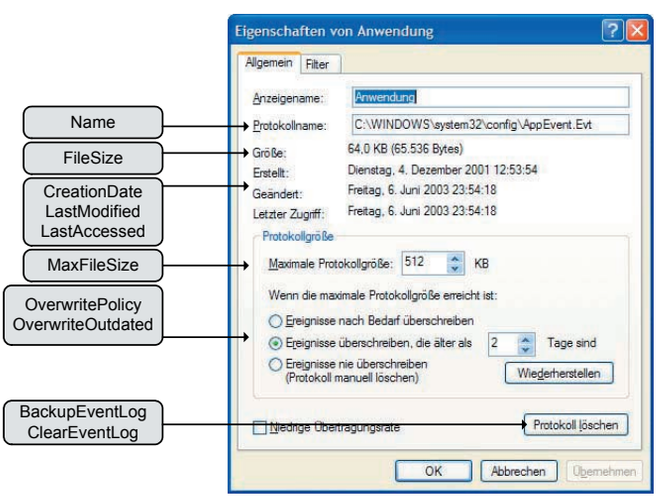
```
WMIC NTEventLog "Application" CALL BackupEventLog "c:\\appevent.evt"
```

Ereignislogbuch löschen

```
WMIC NTEventLog "Application" CALL ClearEventLog "c:\\appevent.evt"
```

Maximale Größe festlegen

```
WMIC NTEventLog "Application" SET MaxFileSize=512000
```



Überschreibungsrichtlinie festlegen

```
WMIC NTEventLog Application SET OverwriteOutdated=2
```

Ereignislogbuch-Einträge

Kritische Events anzeigen

```
WMIC NTEvent WHERE "logfile='System' AND EventType=1" GET TimeGenerated, Message
```

```
WMIC /OUTPUT:%temp%\events.htm NTEvent WHERE "Logfile='System' AND EventType=1" GET TimeGenerated, Message
/FORMAT:htable:"sortby=TimeGenerated"
```

```
%temp%\events.htm
```

TCP/IP-bezogene Events anzeigen

```
WMIC /OUTPUT:%temp%\net.htm NTEvent WHERE SourceName="Tcpip" GET Message,timegenerated
/FORMAT:htable:"sortby=TimeGenerated"
```

```
%temp%\net.htm
```

Nach EventTyp sortierte Ausgabe

```
WMIC /OUTPUT:%temp%\evt.htm NTEvent WHERE "EventType<3 AND LogFile!='System' AND LogFile!='Security'" GET
LogFile,SourceName,EventType,Message,TimeGenerated /FORMAT:htable:"datatype=number":"sortby=EventType"
```

```
%temp%\evt.htm
```

EventCodes finden

```
WMIC /OUTPUT:%temp%\evt.htm NTEvent WHERE "EventCode=1000 AND LogFile='System'" GET
LogFile,SourceName,EventType,Message,TimeGenerated /FORMAT:htable:"sortby=TimeGenerated"
```

```
%temp%\evt.htm
```

Zeiträume durchsuchen

```
WMIC /OUTPUT:%temp%\event.htm" NTEvent WHERE "Logfile='System' AND TimeGenerated>'2003.05.06' AND
TimeGenerated<'2003.07.06'" GET /FORMAT:htable
```

Remote Desktop

Remote Desktop Verbindungen zulassen

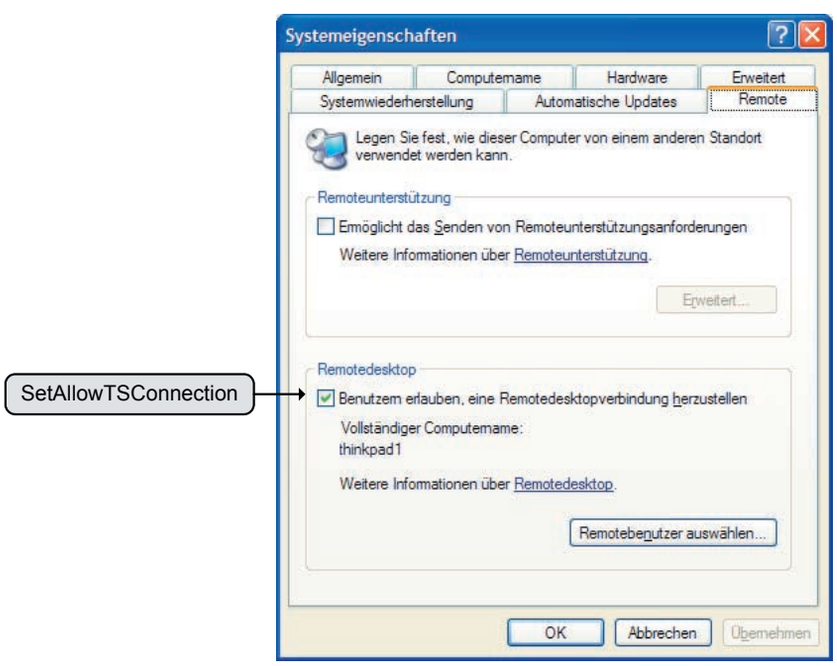
```
WMIC /USER:Administrator /NODE:ws2003 PATH Win32_TerminalServiceSetting WHERE ServerName!=NULL CALL
SetAllowTSConnections 1
```

Remote Desktop auf allen Computern abschalten

```
WMIC /NODE:@"C:\computer.txt" /FAILFAST:ON RDTOGGLE WHERE AllowTSConnections=1 CALL SetAllowTSConnections 0
```

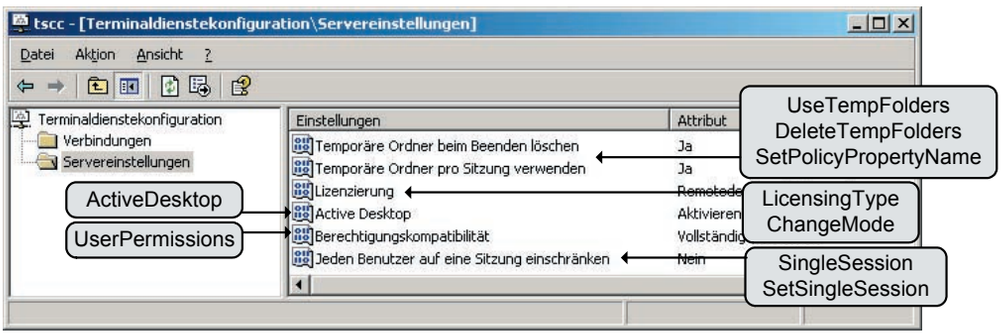
Remote Desktop auf allen Computern abschalten (XP)

```
WMIC /NODE:@"C:\computer.txt" /FAILFAST:ON PATH Win32_TerminalServiceSetting WHERE AllowTSConnections=1 CALL
SetAllowTSConnections 0
```



ActiveDesktop abschalten

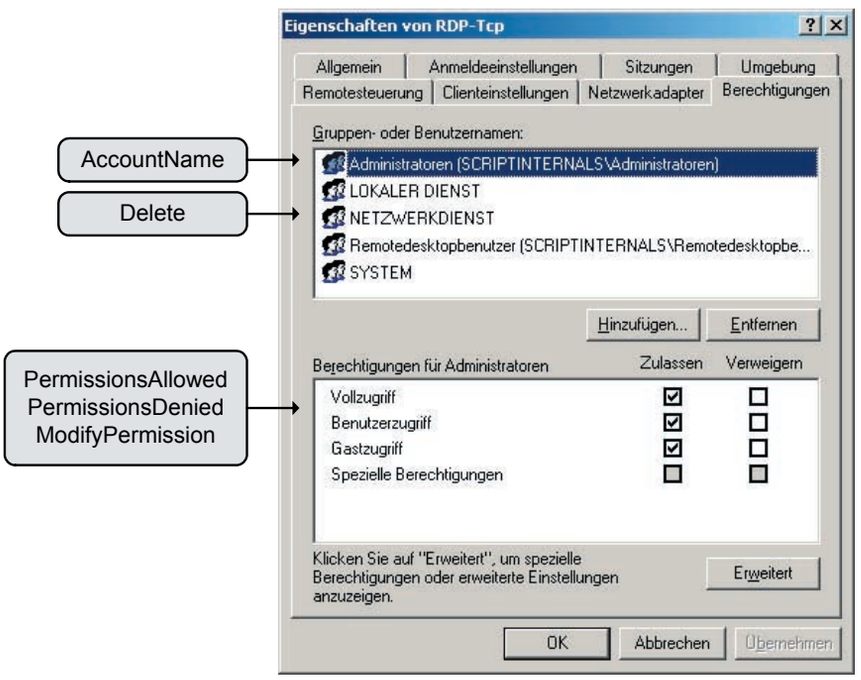
```
C:\>WMIC RDTOGGLE SET ActiveDesktop=0
```



TS Konten

Konten auflisten

```
WMIC RDAccount GET accountname
```



Konsolenkonten auflisten

```
WMIC RDAccount WHERE TerminalName="Console" GET AccountName
```

Sessionkonten auflisten

```
WMIC RDAccount WHERE TerminalName="RDP-tcp" GET AccountName
```

```
1    Informationen abfragen
2    Informationen festlegen
4    Abmelden
8    Virtuelle Kanäle
16   Remoteüberwachung
32   Anmelden
64   Session zurücksetzen oder beenden
128  Nachricht
256  Verbinden
512  Verbindung trennen
```

Berechtigungen eines Kontos lesen

```
WMIC RDAccount WHERE accountname="vordefiniert\\Administratoren" GET PermissionsAllowed
WMIC RDAccount "vordefiniert\\Administratoren" "Console" GET PermissionsAllowed
WMIC RDAccount "vordefiniert\\Administratoren" "RDP-tcp" GET PermissionsAllowed
WMIC RDAccount WHERE "accountname LIKE '%\\Administratoren' AND TerminalName='Console'" GET PermissionsAllowed
```

Berechtigungen ändern

```
0    Informationen abfragen
1    Informationen festlegen
2    Abmelden
3    Virtuelle Kanäle
4    Remoteüberwachung
5    Anmelden
6    Session zurücksetzen oder beenden
7    Nachricht
8    Verbinden
9    Verbindung trennen
```

```
WMIC RDAccount "scriptinternals\\Tobias" "RDP-tcp" CALL ModifyPermissions true, 0
WMIC RDAccount "scriptinternals\\Tobias" "RDP-tcp" CALL ModifyPermissions true, 5
WMIC RDAccount "scriptinternals\\Tobias" "RDP-tcp" CALL ModifyPermissions true, 8
WMIC RDAccount "scriptinternals\\Tobias" "RDP-tcp" CALL ModifyPermissions false, 4
```

Konto löschen

```
WMIC RDAccount "scriptinternals\\Tobias" "RDP-tcp" CALL Delete
```

Standardberechtigungen

Neues Konto mit Standard-Benutzerberechtigungen anlegen

```
WMIC RDPermissions "Console" CALL addaccount "scriptinternals\Tobias", 1
```

Standardberechtigungen wiederherstellen

```
WMIC RDPermissions "RDP-tcp" CALL RestoreDefaults
```