

# 1.

## Inhaltsverzeichnis

<b>1. Inhaltsverzeichnis .....</b>	<b>2</b>
<b>2. Zentrale Vergabe von Berechtigungen .....</b>	<b>3</b>
2.1. Rechte für ein Verzeichnis oder eine Datei .....	3
2.1.1. Schritt 1: Anlegen einer neuen Gruppenrichtlinie.....	3
2.1.2. Schritt 2: Hinzufügen der Berechtigung .....	4
2.2. Hinweis zur Übernahme.....	6
2.3. Schreibrechte in der Registry .....	7
2.4. Übernahme durch die Clients .....	7
2.5. Entzug der Berechtigungen.....	7
<b>3. Ermitteln der notwendigen Berechtigungen .....</b>	<b>8</b>

## 2. Zentrale Vergabe von Berechtigungen

Für manche Programme benötigt ein Benutzer Schreibrechte auf ein Verzeichnis oder eine Datei auf dem lokalen Laufwerk, z.B. um temporäre Daten abzulegen oder um Konfigurationsdaten abzuändern. Ebenso können Schreibrechte auf einen Zweig in der Registry benötigt werden.

Eigentlich ist das in den meisten Fällen ein Programmierfehler und tritt deshalb in der Regel bei älteren Programmen auf, die noch zu Zeiten von Windows 98 erstellt wurden. Trotzdem gibt es hier mitunter Programme, die für unterrichtliche Zwecke nicht ersetzbar sind

Damit das Programm auch von Schülern bzw. Lehrern (also Benutzern ohne Administratorrechte) ausgeführt werden können, müssen Sie diese Rechte nach der Installation vergeben. Das kann zentral über eine Gruppenrichtlinie geschehen.

Im Folgenden wird beschrieben, wie Programme installiert werden müssen, die solche Berechtigungen benötigen.

### 2.1. Rechte für ein Verzeichnis oder eine Datei

Das ist der Fall, der häufiger auftritt. Das Programm benötigt nach dem Start den Schreibzugriff auf eine Datei (z.B. eine Konfigurationsdatei) oder ein Verzeichnis (z.B. für temporäre Daten, oder es versucht im Programmverzeichnis eine neue Datei zu erstellen).

Ist das nicht möglich, so bricht die Programmausführung entweder ab oder es lassen sich nicht alle Funktionalitäten nutzen.

#### 2.1.1. Schritt 1: Anlegen einer neuen Gruppenrichtlinie

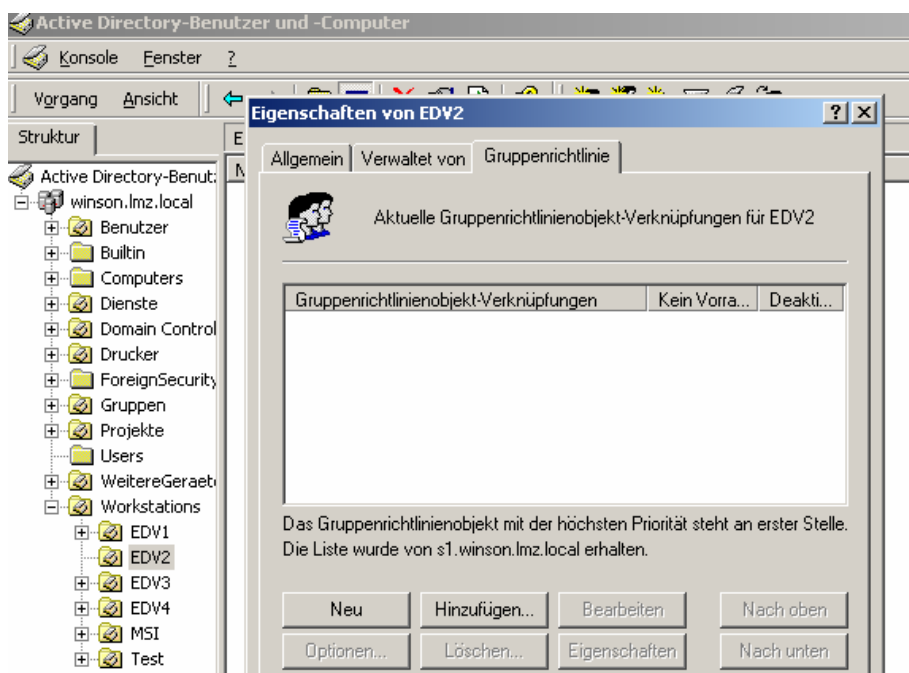
Der Übersicht halber sollten Sie solche Softwarepakete unbedingt über eine eigene Gruppenrichtlinie zuweisen.

Im folgenden Beispiel soll das Paket „Minixampp“ auf allen Rechnern des Raums EDV2 installiert werden.

Starten Sie die Verwaltung des *Active Directory für Benutzer und Computer* und navigieren Sie zu *Workstations-EDV2*.

Klicken Sie mit der rechten Maustaste auf *EDV2* und wählen Sie *Eigenschaften*, anschließend den Reiter *Gruppenrichtlinie*.

Erstellen Sie über „*Neu*“ eine neue Gruppenrichtlinie mit dem Name der Anwendung, wählen Sie anschließend *Bearbeiten*.

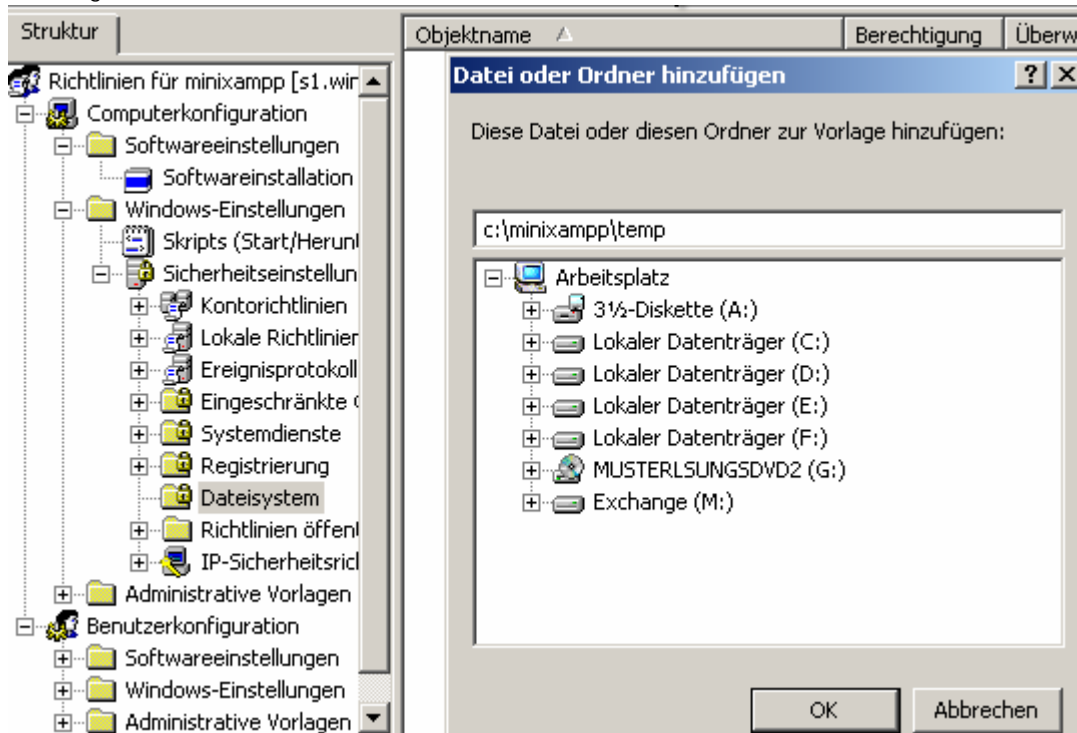


Nun fügen Sie wie gewohnt unter *Computereinstellungen-Softwareeinstellungen-Softwareinstallation* das MSI-Paket hinzu (wichtig: über die Netzwerkumgebung browsen).

## 2.1.2. Schritt 2: Hinzufügen der Berechtigung

Wechseln Sie nun auf [Computerkonfiguration] Windows-Einstellungen-Sicherheitseinstellungen-Dateisystem.

Klicken Sie mit der rechten Maustaste in die rechte, weiße Fläche und wählen Sie „Neu“ bzw. Datei hinzufügen.



Geben Sie anschließend den Pfad auf den Ordner bzw. die einzelne Datei ein, und zwar so, wie sie später auf dem Client vorhanden ist. Sie können diesen Pfad nicht durch Browsen aussuchen, weil das Programm ja nicht auf dem Server installiert ist.

Lassen Sie sich nicht davon verwirren, dass *c:* später durch „%systemdrive%“ ersetzt wird, das hat seine Richtigkeit.

Sie müssen nun die Benutzer eintragen, die Berechtigungen erhalten sollen.

- **Tragen Sie immer *Administratoren* und *System* mit Vollzugriff ein**
- *G\_Benutzer* bedeutet Schüler und Lehrer und ist etwas sicherer als „*jeder*“ (hier sind auch lokal angemeldete Benutzer eingeschlossen)
- *G\_lehrer* sind nur die Lehrer
- *G\_schueler* alle Schüler
- *Vorsicht:* In *G\_schueler* sind die Klassenarbeitsbenutzer nicht enthalten!

Es können auch dezidiertere Rechte auf einzelne Gruppen wie Klassen oder Projektgruppen, einzelne Personen usw. vergeben oder verweigert werden. So könnte man z.B. der Gruppe der Klassenarbeitsbenutzer das Leserecht auf alle nicht benötigte Verzeichnisse entziehen.

Gehen Sie nun wie folgt vor:

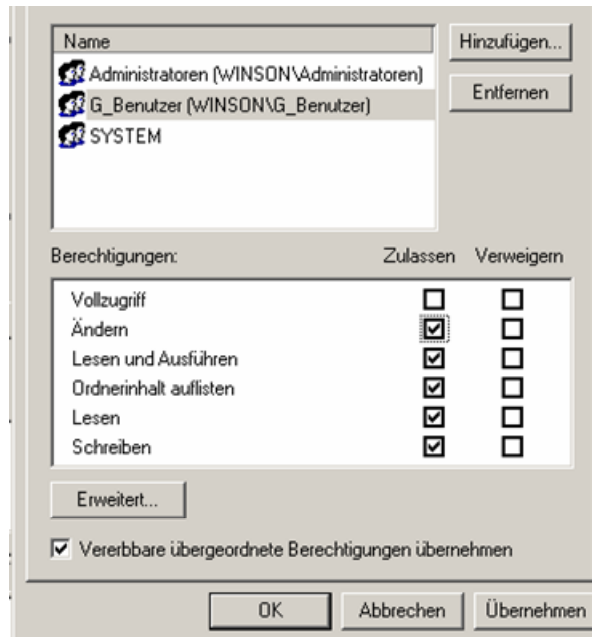
Löschen Sie zunächst den Eintrag „*jeder*“ oder „*Benutzer*“. Klicken Sie anschließend auf „Hinzufügen“ und wählen Sie ganz oben die *Administratoren* aus. Erteilen Sie diesen Vollzugriff.

Nach OK erscheint ein weiteres Fenster, dessen Einstellungen Sie übernehmen (s.u.)

Wählen Sie „Sicherheit bearbeiten“ um weitere Eintragungen vorzunehmen.

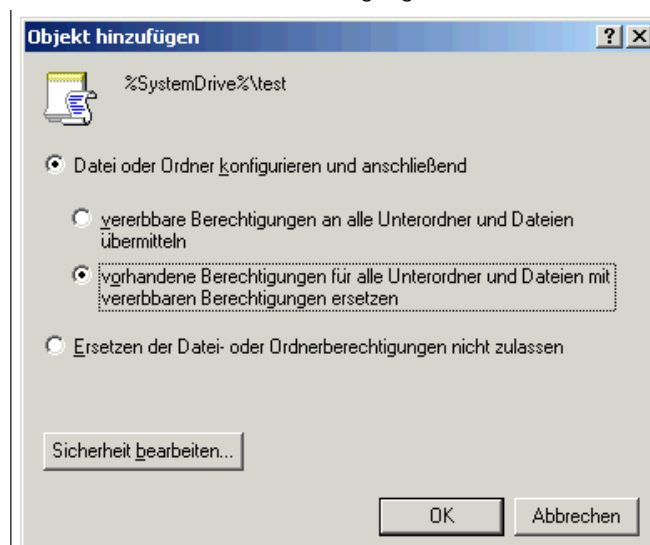
Diesmal tragen Sie im unteren Teil des Fensters „system“ ein und klicken nach Bestätigen durch OK auf den dann angezeigten Benutzer System.  
Nach einem weiteren OK und der Auswahl Vollzugriff wiederholen Sie diese Aktion für die Gruppe G\_Benutzer.

Dieser erteilen Sie das Recht „Ändern“, damit sind automatisch weitere Berechtigungen richtig gesetzt. Vollzugriff sollten Sie außer Administratoren und System niemals erteilen – dadurch könnten die Benutzer selbst wieder Berechtigungen verändern.



Ihr Berechtigungsfeld sollte am Ende wie hier angezeigt aussehen, Sie können jetzt mit OK abschließen und diesmal die Bearbeitung wiederum durch OK abschließen.

Wählen Sie im abschließenden Bildschirm die Optionen „Datei oder Ordner konfigurieren und anschließend“ sowie „vorhandene Berechtigungen ... ersetzen“.



Die Vergabe der Berechtigungen ist dadurch abgeschlossen.

---

## 2.2. Hinweis zur Übernahme der Berechtigungen

Gruppenrichtlinien können nur Berechtigungen auf Ordner/Dateien setzen, die bereits existieren.

Legen Sie also einen Ordner, auf den eine Berechtigung gesetzt werden soll, neu an oder wird er durch eine Softwareinstallation (MSI-Paket) erstellt, so wirkt sich die entsprechende Richtlinie zunächst nicht aus. Auch ein Neustart hilft hier nicht.

Grund dafür ist, dass Sicherheitsrichtlinien aus Performancegründen nur bei Veränderungen oder alle 16 Stunden neu angewendet werden. Spätestens nach dieser Zeit sollten die Sicherheitseinstellungen also wie gewünscht umgesetzt werden (Neustart vorausgesetzt).

Zur Überprüfung können Sie aber auch eine Durchsetzung der Richtlinie am Client erzwingen.

Melden Sie sich hierzu als Administrator am Client an und geben Sie unter Start| Ausführen die folgende Zeile ein:

```
Secedit /refreshpolicy machine_policy /enforce (Windows 2000) bzw.  
gpupdate /force (Windows XP)
```

## 2.3. Schreibrechte in der Registry

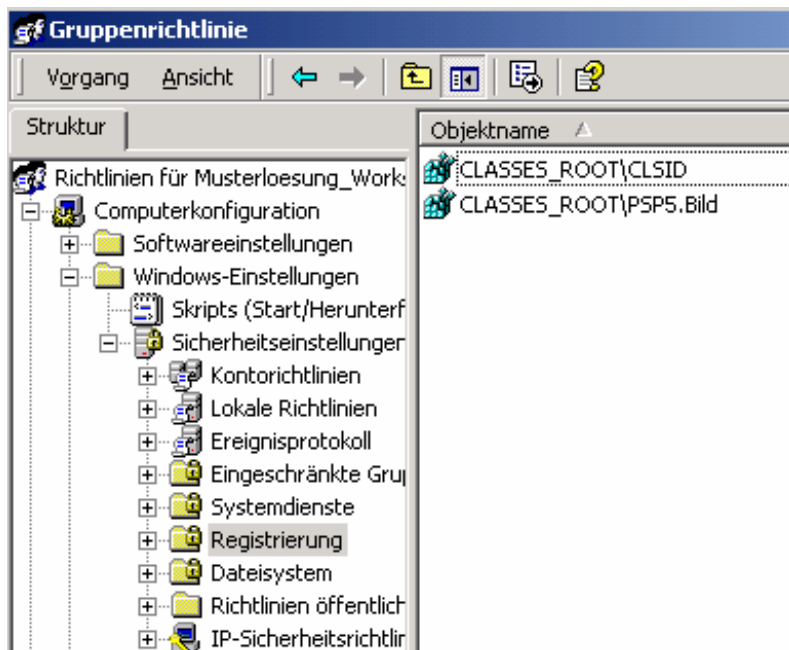
Fast analog sind Schreibrechte auf Registryschlüssel oder Zweige zu setzen. Auch hier empfiehlt sich die Vorgehensweise, dies in der gleichen Gruppenrichtlinie wie die Softwarezuweisung vorzunehmen.

Verwenden Sie diesmal dem Punkt „Registrierung“ und fügen Sie dort einen Schlüssel hinzu.

Die nebenstehende Abbildung zeigt als Beispiel die notwendigen Ergänzungen

für das Programm „Paintshop Pro 5“.

Wichtigster Unterschied zu den Dateirechten: ein Änderungsrecht gibt es bei den Registry-Einstellungen nicht, Sie müssen den Benutzern also „Vollzugriff“ erteilen. (Oder Sie wählen Erweitert – Bearbeiten, um ganz präzise Berechtigungen vorzugeben).



Der Rest funktioniert ganz genauso wie bei den Datei- und Ordnerrechten beschrieben.

## 2.4. Übernahme durch die Clients

Wichtig ist noch die folgende Anmerkung: die neuen Berechtigungen greifen erst nach einem Neustart des Clients. Ein Abmelden und Neuanmelden des Benutzers genügt also nicht.

Sie können Sie als Administrator an einem Client anmelden und über Eigenschaften-Sicherheitseinstellungen im Dateisystem oder per Aufruf des Programms regedt32 über Start-Ausführen in der Registry die Übernahme Ihrer Einstellungen überprüfen.

## 2.5. Entzug der Berechtigungen

Ein wichtiger Hinweis: über die Gruppenrichtlinie wird die Sicherheitseinstellung der Objekte dauerhaft geändert. Das bedeutet insbesondere, dass nach dem Deaktivieren oder Löschen der zugehörigen Gruppenrichtlinie die Schreibrechte nicht automatisch wieder entzogen werden! Wird durch Deinstallation der Software der entsprechende Ordner gelöscht, so sind natürlich die Sicherheitseinstellungen irrelevant geworden.

Anderenfalls muss durch eine neue Gruppenrichtlinie der originale Zustand wiederhergestellt werden. Benötigte z.B. eine Software Schreibrechte auf *C:\winnt\temp*, und benötigen Sie diese Einstellung nach der Deinstallation der Software nicht mehr, so müssen Sie wie oben beschrieben die Sicherheit zurücksetzen. In der Regel bedeutet das Administratoren, system mit Vollzugriff und jeder oder Benutzer mit Lesen.

---

### 3.

## Ermitteln der notwendigen Berechtigungen

Leider sind die notwendigen Berechtigungen in den Installationsanleitungen so gut wie nie dokumentiert, ja oft ist sich der Autor des Programms nicht bewusst, dass er hier ein Problem geschaffen hat.

Manchmal findet man nur einen wenig hilfreichen Hinweis „das Programm kann nur mit Hauptbenutzer- oder Administratorberechtigungen ausgeführt werden“.

Fragen Sie trotzdem bei der angegebenen Hotline an, ob etwas über notwendige Sicherheitseinstellungen bekannt ist.

Da, aufgeschreckt durch die Welle von Viren und andere Malware, inzwischen auch bei privaten Benutzern die Einsicht wächst, dass das normale Arbeiten am PC, insbesondere wenn man eine Verbindung zum Internet eingestellt hat, eher als Benutzer denn als Administrator durchgeführt werden soll, beschäftigen sich mehr und mehr Anwender damit, die notwendigen Berechtigungen herauszufinden.

(D.h. Software wird zwar als Administrator installiert, dann aber als Benutzer aufgeführt – genau der in der Musterlösung vorgesehene Zustand).

Eine sehr gute Informationsquelle ist die Internetseite

<http://www.noadmin.de>

Sie finden hier ein Forum mit sehr vielen bereits durchleuchteten Programmen, und Sie können nach einer kostenlosen Anmeldung auch selbst Fragen stellen.

Wollen Sie selbst notwendige Berechtigungen herausfinden, so finden Sie unter

[http://www.grurili.de/HowTo/MusicMatch\\_als\\_Benutzer\\_ausfuehren.htm](http://www.grurili.de/HowTo/MusicMatch_als_Benutzer_ausfuehren.htm)

eine gute Anleitung (nicht für Anfänger geeignet).