

Musterlösung für
Schulen in
Baden-Württemberg

Windows 2003

Lokale Administratoren

Eine kleine Übersicht

Stand: 20.02.08



Impressum

Herausgeber

Zentrale Planungsgruppe Netze (ZPN)
am Kultusministerium Baden-Württemberg

Autoren

Andreas Mayer
Martin Resch

Endredaktion

Martin Resch

Weitere Informationen

<http://www.lehrerfortbildung-bw.de/netz/>

Veröffentlicht: 2008

© Zentrale Planungsgruppe Netze (ZPN)

Inhaltsverzeichnis

1. Lokale Administratoren.....	4
1.1. Was ist ein Administrator?.....	4
1.2. Netzwerk- und lokale Administratoren.....	4
1.3. Weitere lokale Administratoren per Gruppenrichtlinie ermöglichen.....	5
1.4. Lokal einen Administrator hinzufügen.....	10

1. Lokale Administratoren

1.1. Was ist ein Administrator?

In Netzwerken wie an Standalone-Rechnern gibt es Benutzer mit unterschiedlichen Berechtigungen. Während ein *Anwender* möglichst auf die Benutzung der ihm zugeordneten Programme beschränkt sein soll, muss der *Systemadministrator* die komplette Kontrolle über alle Einstellungen des Systems übertragen bekommen.

Unter Windows existiert für diese Rolle der vorgefertigte Benutzer *Administrator*. Er ist ein so genannter build-in-user, wird also beim Aufsetzen des Systems automatisch angelegt.

Sie können jederzeit weitere Benutzer mit den selben Rechten versehen, indem Sie sie in die Gruppe der *Administratoren* aufnehmen.

Administrator zu sein, macht das Arbeiten auf einem PC sehr einfach, denn jeder Zugriff und jeder Konfigurationsänderung ist erlaubt. Trotzdem hat es gewaltige Nachteile, ständig mit Administratorberechtigungen zu arbeiten:

- Unerfahrene Benutzer verstellen Einstellungen oder löschen gar Systemdateien; sie können diese Änderungen nicht rückgängig machen.
- Destruktive Benutzer zerstören die Systemintegrität, der Computer ist anschließend durch andere nicht mehr nutzbar.
- Absichtlich oder unabsichtlich kommen Schädlinge wie Spionageprogramme, Viren, Würmer u. dgl. auf das System.

Benutzer sollten daher normalerweise keine Administratorberechtigungen haben.

Schüler und Lehrer sind deshalb als *Benutzer* eingerichtet, die nur wenige Änderungen am System vornehmen können. Diese Änderungen werden zudem nach dem Abmelden verworfen.

Als Administrator sollte man sich nur anmelden, wenn dies unumgänglich ist. Z.B. weil man Software installieren möchte oder das System konfigurieren will.

Als Administrator sollte man möglichst nicht im Internet surfen, da sonst möglicherweise eingefangene Schadprogramme mit dessen Rechten sich im System einnisten könnten. Das neue Betriebssystem "Microsoft Vista" beachtet diese Grundregeln.

1.2. Netzwerk- und lokale Administratoren

Administrator ist nicht unbedingt gleich Administrator, denn trotz des gleichen Namens gibt es im Netzwerk der PaedML zwei völlig verschiedene Benutzer.

- Der **Netzwerkadministrator** ist derjenige, mit dem Sie sich am Server anmelden. Er hat auf jedem einzelnen Rechner der Domäne (des Netzwerks also) Administratorrechte und kann darüber hinaus auch Konfigurationen im ganzen Netz än-

dem. Mit diesem Konto können Sie sich auf jedem Rechner anmelden, der mit dem Server verbunden ist. Sie melden sich dann an der *Domäne* an. Entsprechend ist dieser Administrator in der Gruppe der *Domänenadministratoren*, zusammen mit *aprofschueler* und *aproflehrer*. Es ist sehr wichtig, für diese Benutzer ein sicheres Passwort zu verwenden. Dieses sollte niemand anderem mitgeteilt werden, aber in einem verschlossenen Umschlag sicher verwahrt für Notfälle hinterlegt werden.

- Den **lokalen Administrator** gibt es auf jedem Clientrechner. Sie können sich mit diesem Konto lokal anmelden und diesen einen Rechner betreuen. Auf das Netzwerk haben Sie dann keine Zugriffsberechtigung. Das Konto ist aber auch dann verfügbar, wenn die Verbindung zum Server ausgefallen ist oder der Rechner neu in die Domäne aufgenommen werden muss.

Das Passwort des lokalen Administrators muss mit dem des Netzwerkadministrators nicht übereinstimmen und kann sogar auf jedem Rechner unterschiedlich sein. Es wird bei der RIS-Installation durch einen Eintrag in der Datei `ristndrd.sif` festgelegt, kann aber danach geändert werden¹.

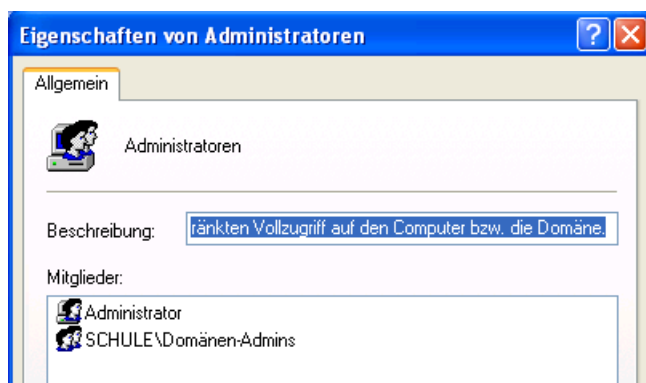
```
[GuiUnattended]
OemSkipWelcome = 1
OemSkipRegional = 1
TimeZone = %TIMEZONE%
AdminPassword = muster
```

Achten Sie möglichst darauf, wirklich verschiedene Passwörter zu verwenden, denn das des lokalen Administrators ist sehr viel einfacher anzugreifen als das des Netzwerkadministrators.

- Weitere Benutzer mit lokalen Administratorenrechten sind alle Domänenadministratoren (wiederum Systemstandard) und in der `paedML` der *PGMAdmin*.

1.3. Weitere lokale Administratoren per Gruppenrichtlinie ermöglichen

Betrachtet man die Mitglieder der Gruppe Administratoren auf einem Client in einer Domäne, so sieht das im Regelfall so aus:



- 1 Wie Sie das am einfachsten für alle Clients machen, erfahren Sie unter <http://lehrerfortbildung-bw.de/netz/muster/win2000/material/tipps/startup/lokalespasswort/index.html>

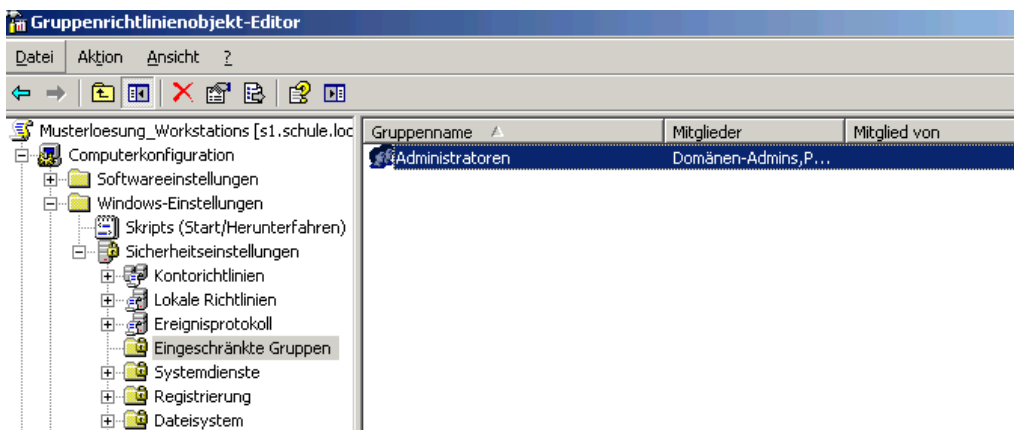
Die lokale Gruppe Administratoren besteht aus dem lokalen Administrator und der Gruppe der Domänen-Administratoren. Manuell können dieser Gruppe weitere Mitglieder hinzugefügt werden.

Nun soll in der paedML der PGMAdmin auf allen Workstations über Administratorrechte verfügen, nicht jedoch in der Domäne. Daher muss der PGMAdmin Mitglied der lokalen Gruppe Administratoren werden.

Dies wurde über eine sogenannte *Eingeschränkte Gruppe* in der Gruppenrichtlinie *Musterloesung_Workstations* umgesetzt.

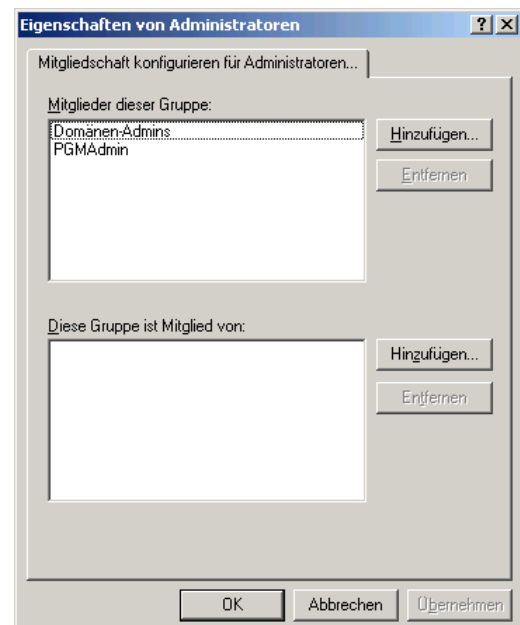
Mit Hilfe von Eingeschränkten Gruppen können Domänenbenutzer automatisch in eine lokale Gruppen auf den Clients aufgenommen werden.

Wichtig ist noch der Hinweis, dass durch die Einstellungen für die Eingeschränkte Gruppe lokal vorhandene Einstellungen **ersetzt** werden.



In der Abbildung wurde eine neue Eingeschränkte Gruppe *Administratoren* angelegt². Wichtig ist, dass der Gruppennamen der gleiche ist, die die Gruppe auch auf dem lokalen Client besitzt.

Blickt man in die Eingeschränkte Gruppe *Administratoren*, so erkennt man, dass hier die Domänen Administratoren und der PGMAdmin Mitglied sind.



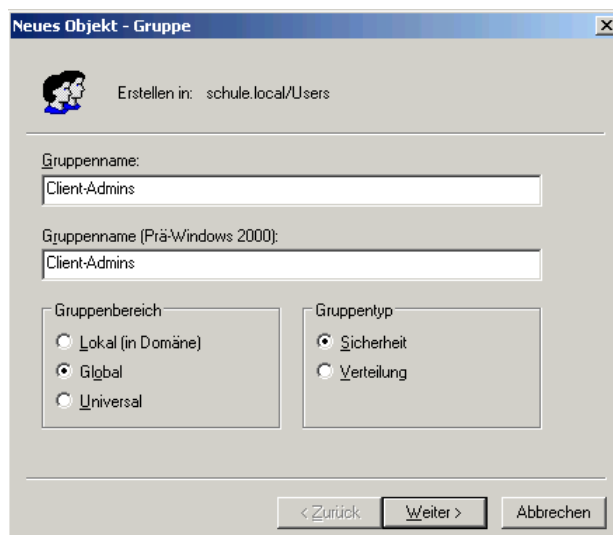
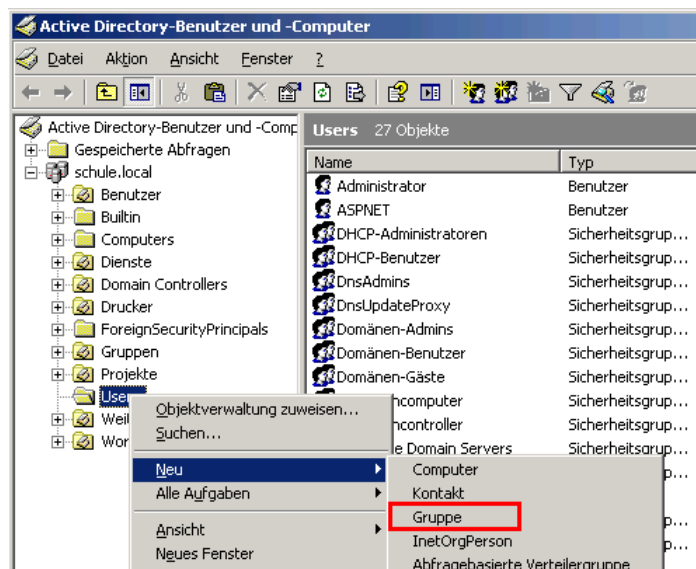
² Diese Einstellung gilt in der paedML 2.1

Diese Einstellung bewirkt, dass spätestens bei jedem Neustart eines Clients bis auf den lokalen Administrator alle weiteren Mitglieder der lokalen Gruppe Administratoren durch die der Eingeschränkten Gruppe ersetzt werden.

Die paedML ist also durch diese Einstellung so konfiguriert, dass weitere lokale Administratoren nicht vorgesehen sind. Konkret bedeutet das, dass wenn andere lokale oder Netzwerkbenutzer auf einer Arbeitsstation als lokaler Administrator eingerichtet werden, diese die Berechtigungen nach einen Neustart wieder verlieren.

Eine pragmatische Möglichkeit bestünde nun darin, das Passwort des lokalen Administrators an besagtem Computer zu ändern und dieses dann dem Kollegen mitzuteilen. Sie können jedoch mit einer Änderung der Eingeschränkten Gruppe wieder einen normalen Benutzer auf einem Computer in die Gruppe der lokalen Administratoren aufnehmen.

Hierfür müssen Sie zunächst eine neue Gruppe *Client-Admins erstellen*. Öffnen Sie das Active-Directory. Erstellen Sie in der OU *Users* eine neue Gruppe und nennen Sie diese *Client-Admins*.

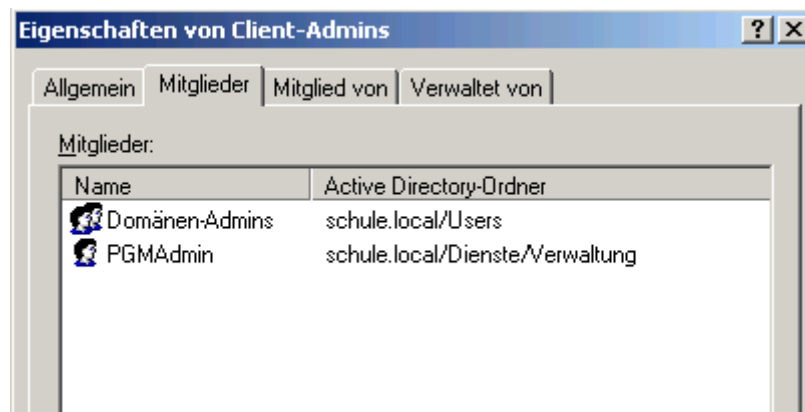


Stellen Sie den Assistenten ohne weitere Änderungen fertig.

Öffnen Sie nun die gerade angelegte Gruppe per Doppelklick. Vergeben Sie eine Beschreibung für die Gruppe.



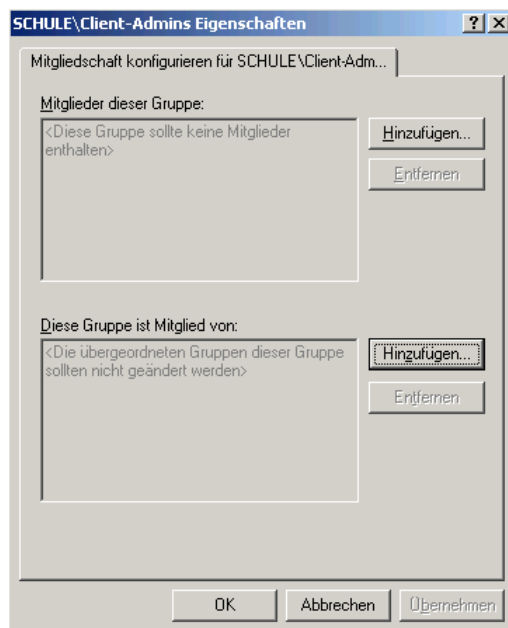
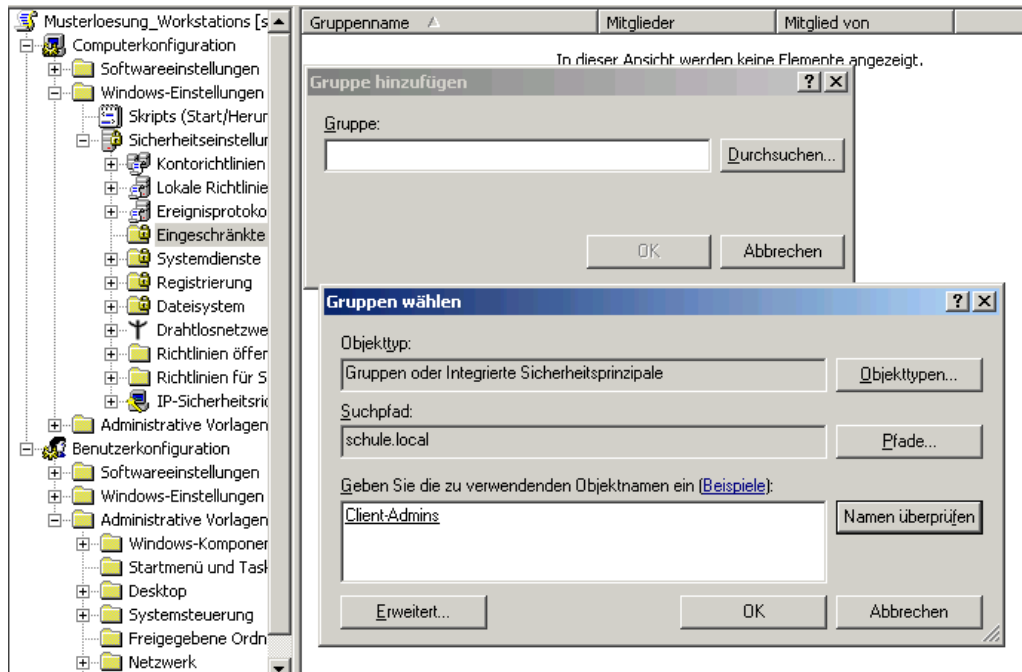
Wechseln Sie zur Registerkarte *Mitglieder* und fügen Sie *Domänen-Admins* und den *PGMAdmin* hinzu³.



Öffnen Sie nun im Gruppenrichtlinienditor die Richtlinie *Musterloesung_Workstations / Computerkonfiguration / Windows-Einstellungen / Sicherheitseinstellungen / Eingeschränkte Gruppen*

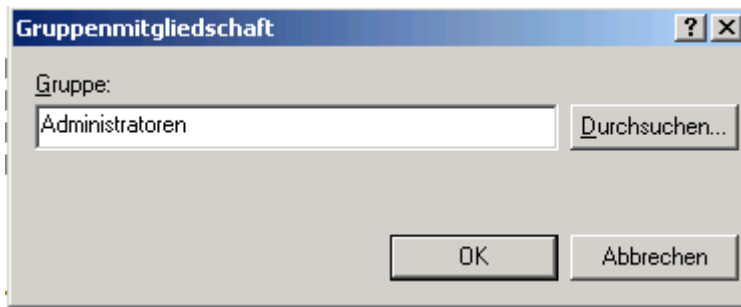
Löschen Sie die Gruppe *Administratoren* und fügen Sie per Rechtsklick eine neue Gruppe hinzu. Über Durchsuchen wählen Sie die vorher erstellte Gruppe *Client-Admins*.

³ Alle Mitglieder, die Sie hier hinzufügen, haben später Administratorrechte auf *allen* Clients.



Nun müssen Sie noch Festlegen, dass die Gruppe zur Gruppe der lokalen Administratoren gehören soll. Klicken Sie hierzu bei *Diese Gruppe ist Mitglied von:* auf *Hinzufügen*.

Geben Sie im nächsten Fenster *Administratoren* ein.

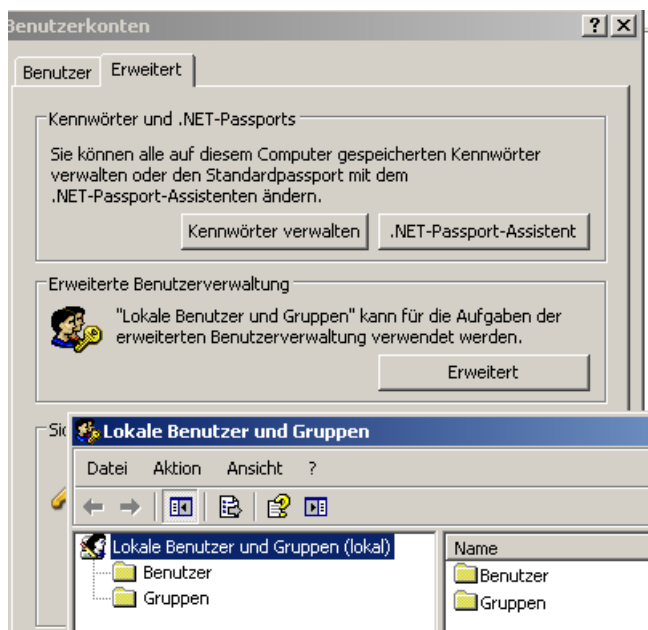


Die nun vorgenommenen Einstellungen bewirken, dass die lokalen Einstellungen nicht mehr **ersetzt**, sondern **ergänzt** werden.

Nun können Sie an einem Computer einen Benutzer wieder in die Gruppe der lokalen Administratoren aufnehmen.

1.4. Lokal einen Administrator hinzufügen

Auf dem Client verändern Sie die lokale Administratorengruppe über *Systemsteuerung / Benutzerkonten*. Am einfachsten verwenden Sie hier den Reiter *Erweitert*.



Klicken Sie hier nochmal auf den Button erweitert. Nun können Sie in den "Ordnern" der Benutzer mit der rechten Maustaste neue Benutzer hinzufügen etc. Ein Drücken der [F1]-Taste bringt Ihnen die Onlinehilfe zu diesem Thema.