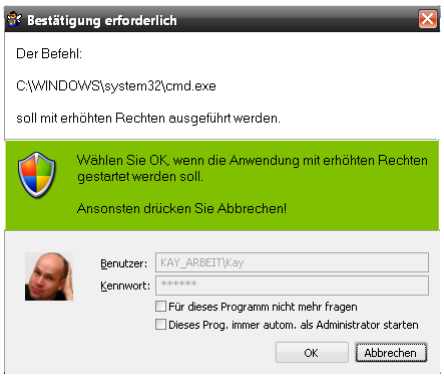
SuRun
„Benutzerhandbuch“
(ein Versuch)

Stand SuRun Version 1.2.0.9

Inhaltsverzeichnis

Was ist SuRun?



SuRun ist eine kostenlose Software mit frei verfügbarem Quelltext, die das Arbeiten mit eingeschränkten Rechten unter Windows 2000, XP, Server 2003, Vista und Windows 7 erleichtert.

SuRun ermöglicht es, bestimmte Programme mit administrativen Rechten zu starten, ohne ein Kennwort anzugeben, ohne die Registry des Benutzers zu wechseln oder Umgebungsvariablen zu verändern.

SuRun läuft nicht in Windows 95/98/ME.

Warum braucht man SuRun?

In Windows NT und dessen Nachfolgern (2000, XP, 2003, Vista...) hat Microsoft eine Rechteverwaltung integriert. Anhand von Zugriffskontrollisten legt Windows fest, ob und wie auf Objekte (z.B. Dateien, Geräte, Registryschlüssel) zugegriffen werden darf oder nicht.

Jedes Programm wird standardmäßig mit den Rechten des Programms ausgeführt, das es startet. So *z.B. erbt Notepad* üblicher Weise die Rechte von *Explorer*.

Auch schadhafte Software, die ausgeführt wird, hat die Rechte des ausführenden Programms. So würde ein Virus die Rechte des *Internet Explorer*s bekommen der die Rechte von *Explorer* bekam der die Rechte des angemeldeten Benutzers hat.

Wenn man immer als Administrator arbeitet kann ein Virus den PC unbemerkt komplett übernehmen und das System unbrauchbar machen.

Durch die integrierte Unterstützung für Virtualisierung in allen aktuellen Prozessoren und deren Chipsätzen kann man sogar das ganze Windows im laufenden Betrieb in eine virtuelle Maschine verbannen. Ein experimentelles Beispiel dafür hat 2007 *Joanna Rutkowska* (http://InvisibleThings.org) mit BluePill geliefert. Es packt das System „zurück in die *Matrix*“, während Windows weiterhin meint die Kontrolle zu haben. Doch auch BluePill braucht Administratoren-Rechte (oder eine Lücke im System). Sonst kann es sich nicht installieren.

Arbeitet man mit eingeschränkten Rechten, kann ein Virus das System prinzipiell nicht angreifen, da ihm, wie dem angemeldeten Benutzer, die Rechte dazu fehlen.

In Windows, vor Windows Vista, **ist es** mit Bordmitteln **nicht leicht, mit eingeschränkten Rechten zu arbeiten**. Selbst für einfache Sachen, wie das Stellen der Systemuhr oder das Anpassen der Energieverwaltung, braucht Windows einen Administrator. Software darf man normalerweise gar nicht installieren, Hardware auch nicht. Erst ab Windows Vista ist mit der Benutzerkontensteuerung (UAC) eine Verbesserung zu verzeichnen.

Historisch gewachsene Windows Programme benutzen INI-Dateien im Windows-Verzeichnis um deren Einstellungen zu speichern. All diese Programme laufen nicht mit eingeschränkten Rechten. Man muss die Berechtigungen für jede INI-Datei anpassen, damit eingeschränkte Benutzer darin schreiben dürfen.

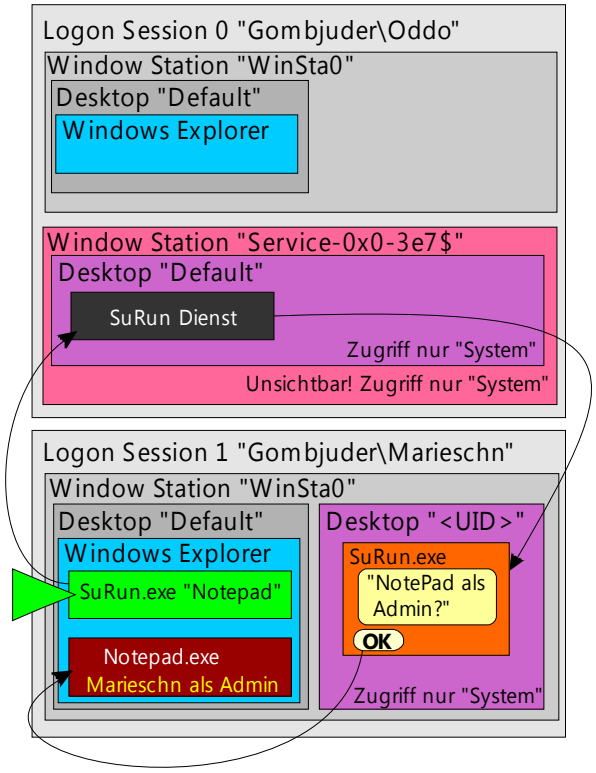
Wie funktioniert SuRun?

SuRun lässt bestimmte Benutzer auf Anfrage eine Anwendung mit administrativen Rechten ausführen. Es hat einen eigenen Windows Dienst, der das gewünschte Programm mit Administratorrechten, aber im Kontext des eingeschränkten Benutzers startet. Vorher muss der Benutzer auf einem abgesicherten Desktop den Start der Anwendung bestätigen.

Dadurch kann man administrative Aufgaben erledigen, ohne Administrator zu sein und ohne ein Administratoren-Kennwort zu kennen.

Im Gegensatz zur Benutzerkontensteuerung (UAC) von Windows Vista und Nachfolgern startet SuRun Programme immer im Kontext des Benutzers und nicht im Kontext eines Systemadministrators.

Das Ganze funktioniert prinzipiell so:



Informelle Beschreibung:

An Gombuter sind (Dank schneller Benutzerumschaltung) zwei Benutzer angemeldet. Zuerst kam Oddo, der wollte noch schnell ein Spiel spühlen.

Dann kam Marieschn, die noch eine Email schreiben muss.

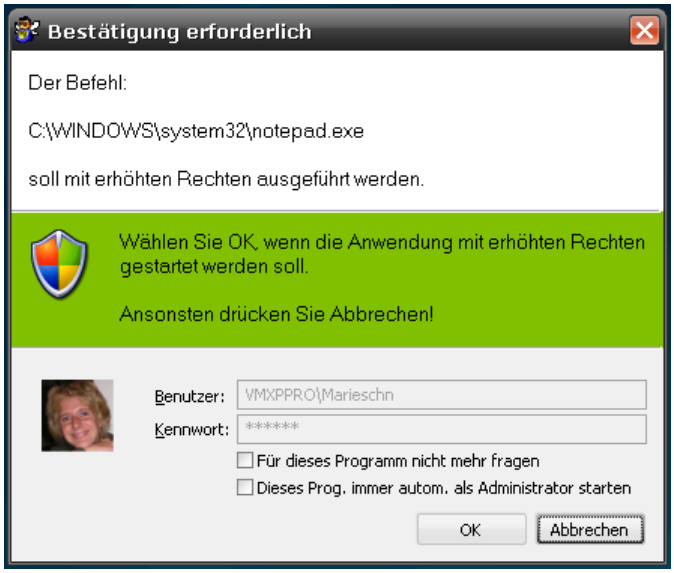
Also drückte Oddo kurz [WIN]+”L” und ließ Marie sich anmelden und ihre Email schreiben.

Marie will weder Virenscanner noch Viren haben und arbeitet deshalb vorbildlich mit eingeschränkten Rechten.

Das Email Programm “Notepad” verweigert aber den Dienst, weil es noch einige hundert Megabyte Sicherheitsupdates aus dem Internet nachinstallieren muss und dafür administrative Rechte braucht.

Also klickt die Goldmarie mit der rechten Maustaste auf Notepad.exe und dann auf SuRuns Eintrag “Starte als Administrator“. Damit wird “SuRun.exe Notepad.exe” gestartet. SuRun.exe kontaktiert den Dienst und teilt ihm mit, dass die Marie in Logon Session 2 ein Notepad.exe mit administrative Rechten braucht.

Der Dienst ist sich nicht ganz sicher, ob die Marie das wirklich will oder ein Virus in ihrem Namen zu handeln versucht. Also macht er erst mal einen neuen Desktop in Marieschns “Window Station” auf. Auf diesen neuen Desktop dürfen als Programme nur Dienste zugreifen. Dort wird die Marie nochmal gefragt, ob sie wirklich Notepad administrativ ausführen wollte.



Ein Virus könnte hier keinen Klick simulieren, aber die Marie findet leicht den “OK” Knopf und drückt ihn. Das macht den SuRun Dienst nun sicher und er startet “Notepad.exe” als Benutzer “Marieschn” aber mit den Rechten eines Administrators.

Nach ein paar Sekunden hat sich Notepad die Updates einverleibt, Marie kann schnell ihre Email schreiben und Oddo bricht den Streckenrekord im Geschirrspühler.

Alle sind glücklich.

Was ist SuRuns sicherer Desktop?

Ein Desktop ist der Teil in Windows, den der Benutzer auf seinen Bildschirmen sieht. Der Desktop empfängt exklusiv alle Tastatur- und Mauseingaben.

Ein Desktop ist auch ein Objekt, das mit einer Zugriffskontrollliste geschützt ist. Will ein Programm auf einen Desktop zugreifen, also z.B. ein Fenster anzeigen, ist dazu die entsprechende Berechtigung in der Zugriffskontrollliste des Desktop erforderlich.

Muss der SuRun Dienst mit dem Benutzer interagieren, verwendet er den WinLogon Desktop oder erstellt einen neuen Desktop über den er mit dem Benutzer kommuniziert. Die Zugriffskontrollisten dieser Desktops verwehren den Programmen des Benutzers jeglichen Zugriff.

So kann der Benutzer nur mit Tastatur und Maus mit SuRun interagieren und laufende

Programme sind nicht in der Lage, SuRun fernzusteuern.

TIPPS:

Ist das Verwenden des WinLogon-Desktop deaktiviert, wird auf manchen Systemen ab und zu die Fehlermeldung „Abbruch! **Sicherer Desktop konnte nicht erstellt werden**!“ angezeigt.

Das ist kein Fehler in SuRun: SuRun versucht, einen Desktop zu erstellen, Windows verweigert das und SuRun zeigt dann die Meldung.

Seltsamer Weise berichten Leute diesen Fehler, die enorme Hardware-Ressourcen haben, jedoch niemand, der ein Windows XP mit nur 256MB RAM betreibt.

Wenn Sie diese Meldung sehen, sollte SysInternals Desktops in der selben Situation eine ähnliche Meldung zeigen. Dann hilft es häufig, in der Registry die Werte für die Windows-Desktop-Verwaltung zu erhöhen, indem man folgendes in die Registry importiert und den PC neu startet:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management]
"SessionPoolSize"=dword:00000040
"SessionViewSize"=dword:00000068
```

Die genauen technischen Details sind sporadisch im Internet beschrieben. Man kann sie dort finden, wenn man nach "SessionPoolSize" und "SessionViewSize“ sucht.

Warum keine Windows Bordmittel?

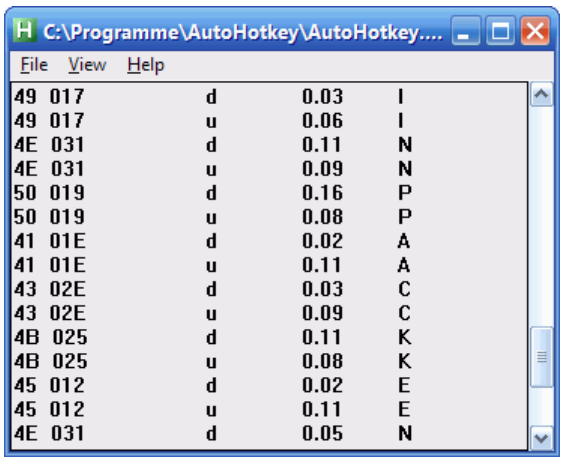
Der Windows Explorer hat einen “*Ausführen als…*” Befehl.

Der hat allerdings zwei entscheidende Nachteile!

Der erste und fatale Nachteil: Schadsoftware kann sich durch „Ausführen als...“ mit einfachsten Mitteln ein Administratoren-Kennwort besorgen.

Als Demonstration dafür kann man einfach AutoHotkey benutzen.

AutoHotkey schneidet alle Tastendrücke mit und man kann sich das Passwort im LOG ansehen.



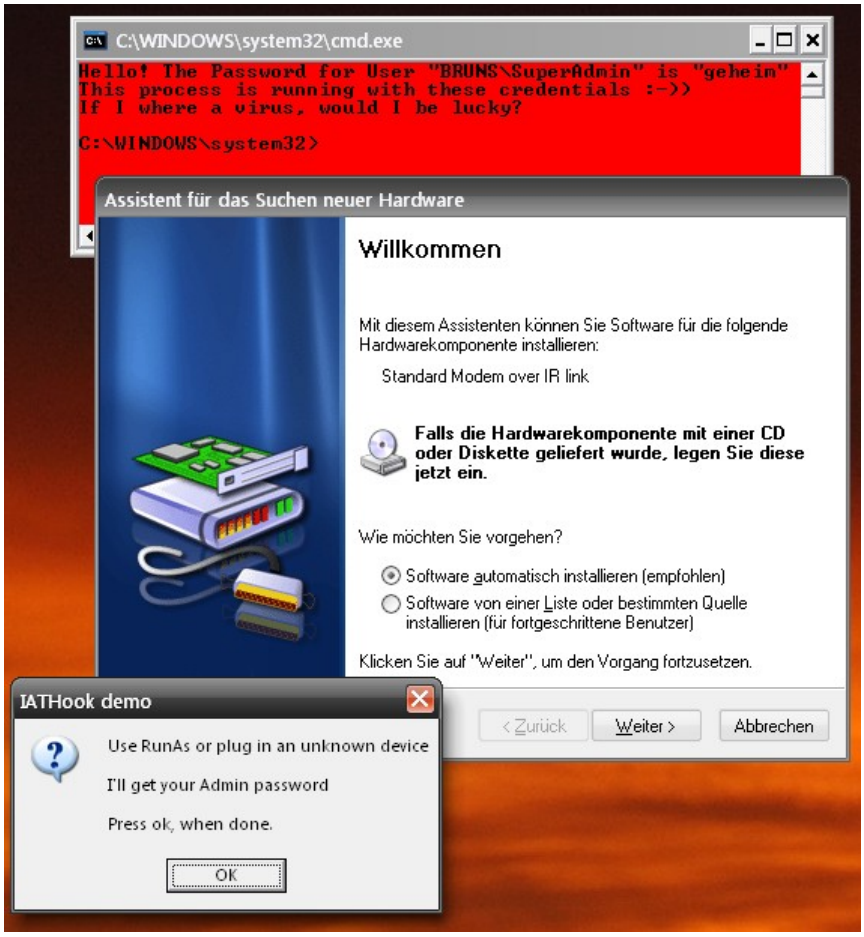
Mit dem Windows Kommandozeilenprogramm „*RunAs“, oder dem MachMichadmin Script*

ist es nicht viel anders. Auch wenn da ein normaler Keylogger nicht reicht, kann man diese Programme missbrauchen, um unbemerkt an ein Administrator-Kennwort zu gelangen.

Wie das geht, demonstriert z.B. meine Demo **„*IAT-Hook*“**.

Wenn man, selbst als Gast, die Demo startet, neue Hardware ansteckt oder RunAs benutzt und die Daten eines Administrators eingibt,

startet diese Demo eine cmd-Konsole mit diesen Berechtigungen.



Das Microsoft dieses Thema so nachlässig behandelt hat, ist mir unverständlich. Schon in Windows NT 3.1 hätte man das Sicherheitsloch stopfen können. An der Rechteverwaltung hat sich bis einschließlich Windows XP nichts geändert.

Das zweite Problem des „Ausführen als...“ Befehls von Windows ist, dass das gestartete Programm im Kontext eines anderen Benutzers läuft. Das Benutzer-Verzeichnis und HKEY_CURRENT_USER in der Registry zeigen auf die Orte des Benutzers, der in „Ausführen als...“ angegeben wurde. Dieses Problem besteht übrigens auch für eingeschränkte Benutzer in Windows Vista.

Ein Beispiel:

Ich bin als eingeschränkter Benutzer “Oddo” angemeldet und will SuperApp installieren.

Das Installationsprogramm meckert, dass es keine ausreichenden Rechte hat. Also benutzt “Oddo” “Ausführen als…“, um die Software als Administrator “SubberUhser” zu installieren.

SuperApp ist wahnsinnig teuer, darf nur von einem Benutzer ausgeführt werden und speichert den Lizenzschlüssel und Einstellungen in HKEY_CURRENT_USER\Software\SuperApp bzw. dem Benutzerverzeichnis “C:\Dokumente und Einstellungen\SubberUhser” ab.

Das Dumme ist, das genau diese Orte während der Installation auf den falschen Ort

verweisen.

Der Benutzer “Oddo” hat seine Einstellungen in “C:\Dokumente und Einstellungen\Oddo” gespeichert, SuperApp legt den Lizenzschlüssel aber in “C:\Dokumente und Einstellungen\SubberUhser” ab.

Will “Oddo” nun SuperApp benutzen, guckt er in eine “Sie haben keine Lizenz” Meldung, denn “Oddo” darf in “C:\Dokumente und Einstellungen\SubberUhser” Dateien weder lesen noch schreiben. [Mit der Registry ist das analog!]

Installation

GANZ WICHTIG!: Behalten Sie immer ein Administrator-Konto, an das Sie sich anmelden können, falls SuRun Unerwartetes tut!

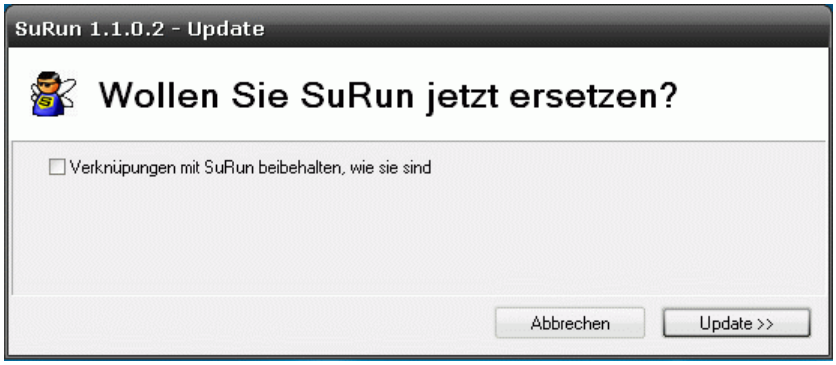
Um SuRun zu installieren muss man einfach das Installations-ZIP in einen Ordner auspacken und “*InstallSuRun.exe*” ausführen. Ist man während der Installation kein Administrator, fragt SuRun nach einem Administrator Passwort.

WARNUNG: Das Passwort für die Installation wird in einer nicht gesicherten Umgebung abgefragt. Schon vorhandene Passwortschnüffler würden es herausfinden! Sicher ist, den Netzwerkstecker zu ziehen, sich als Administrator anzumelden und SuRun zu installieren.

Der Dialog für die Installation beinhaltet zwei Checkboxen.

Sie sollten auf jeden Fall den Haken in **"'Administratoren' statt 'Ersteller' als Standard-Besitzer für von Administratoren erstellte Objekte."** aktiviert lassen!

Ist SuRun bereits installiert, wird *„InstallSuRun.exe“* ein Update vorschlagen.



SuRuns Einstellungen werden bei einem Update nicht verändert. Lediglich die **„Starte als Administrator...“**-Verknüpfungen werden neu angelegt. Ist jedoch **„Verknüpfungen mit SuRun beibehalten, wie sie sind“** aktiviert, werden auch diese nicht verändert.

Während der Installation zeigt SuRun durchgeführte Aktionen in einer Liste an.

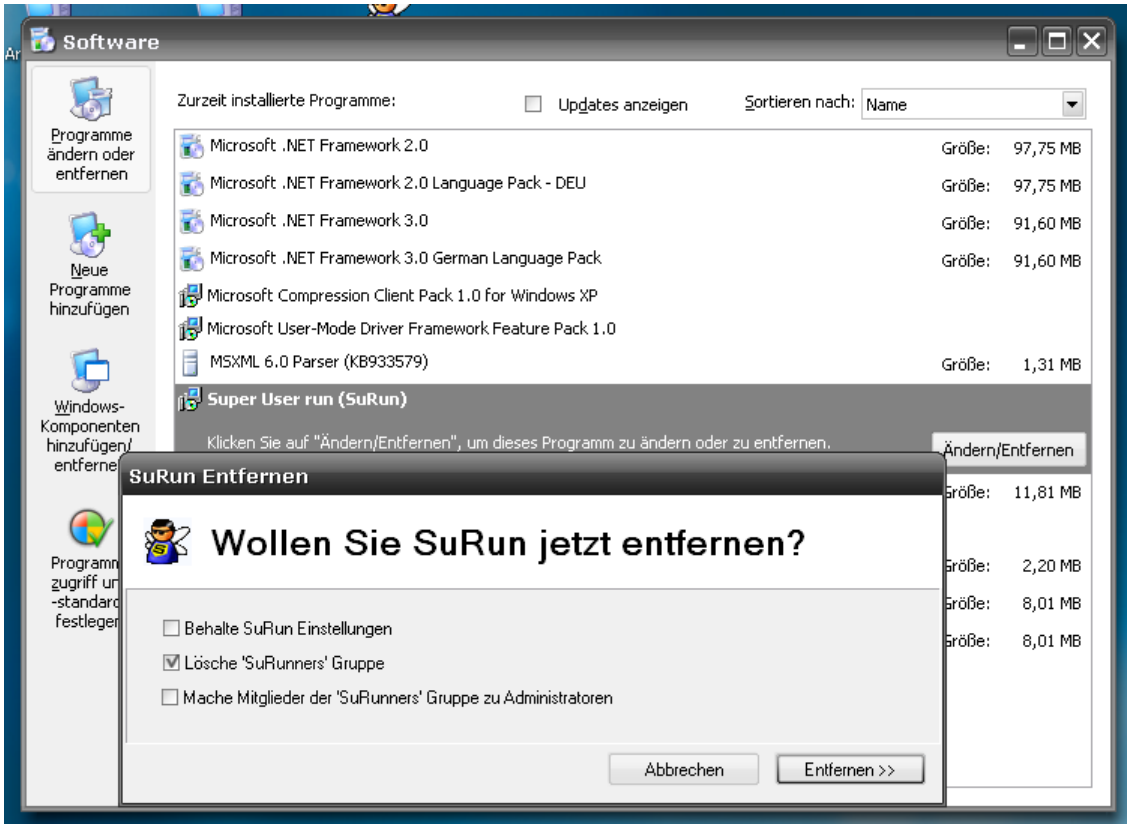
Um die Installation abzuschließen **müssen Sie sich von Windows Vista (und neuer) ab**- und wieder an**melden**. Unter **Windows 2003** und älter ist ein **Neustart erforderlich**.

Hinweis:

Wenn Sie SuRun auf einem System **unbeaufsichtigt installieren** wollen, können Sie das mit dem Befehl „InstallSuRun.exe /INSTALL“ tun. Sollen bei der Installation zuvor gesicherte SuRun **Einstellungen wiederhergestellt** werden, lautet die Befehlszeile „InstallSuRun.exe /INSTALL <PfadUndDateiMitSuRunEinstellungen>“.

Deinstallation

SuRun kann über „Software“ in der Systemsteuerung entfernt werden.



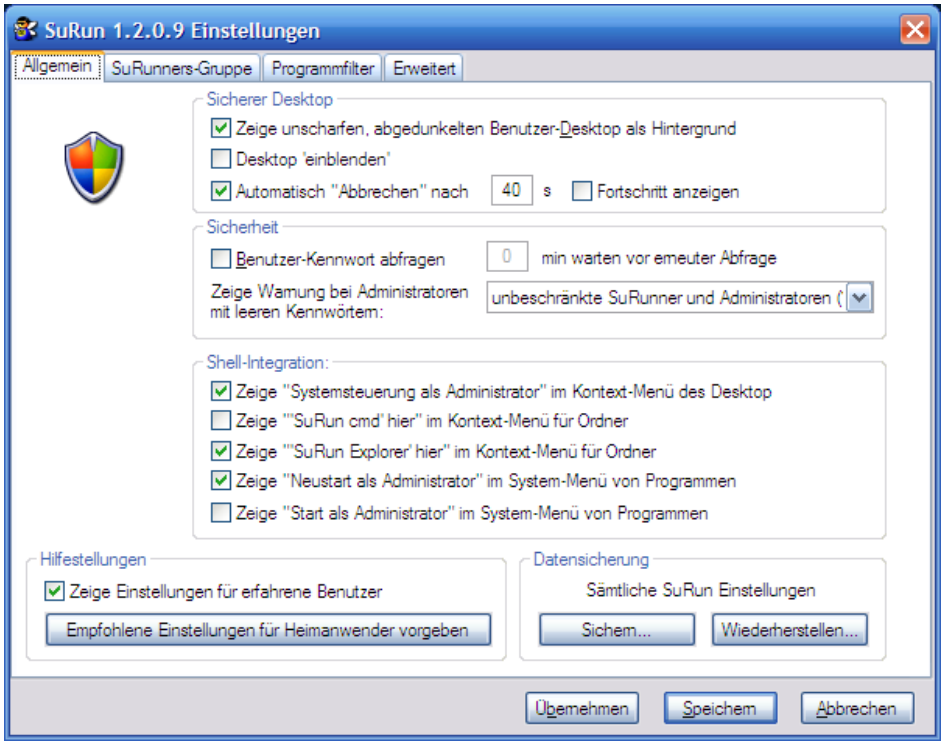
Ist die Option **„Behalte SuRun Einstellungen“** aktiviert, wird SuRun alle Einstellungen belassen, wie sie sind und, die Gruppe *„SuRunners“* nicht löschen.

Dateien, die nicht sofort gelöscht werden können, werden beim nächsten Systemstart gelöscht.

Konfiguration

Über die Kommandozeile “**surun /setup**” oder „*SuRun Einstellungen*“ in der Systemsteuerung erscheint SuRuns Konfigurationsdialog auf einem abgesicherten Desktop.

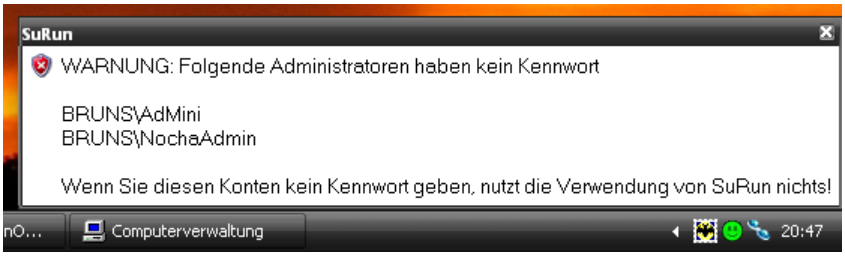
SuRun Einstellungen „Allgemein“



- **Zeige unscharfen, abgedunkelten Benutzer-Desktop als Hintergrund**
  Ist diese Option aktiviert, wird vor dem Umschalten auf den abgesicherten Desktop ein Schnappschuss des Benutzer-Desktops gemacht, verwaschen und abgedunkelt und dann als Hintergrundbild im abgesicherten Desktop dargestellt. (Das kostet auf meinem System (PIV 3.2GHz, 2800×1050 Pixel) ca. 0.5s, sieht aber schön aus)
- **Desktop 'einblenden'**
  Der Hintergrund des abgesicherten Desktops wird ein- und ausgeblendet. Ist diese Option aktiv, werden erhebliche Ressourcen und ein schnelles System benötigt.
- **Automatisch 'Abbrechen' nach**
  Fragt SuRun den Benutzer um Erlaubnis und ist dies Option aktiv, wird nach der eingestellten Zeit automatisch die Taste „Abbrechen“ gedrückt. Man kann das Zeitlimit zusätzlich als **Fortschritt**sbalken **anzeigen** lassen.
- **Benutzer Kennwort abfragen, X min warten vor erneuter Abfrage**
  Ist diese Option aktiv, fragt SuRun vor dem administrativen Start eines Programms nach dem Benutzerkennwort.
  Ist eine Zeit verschieden von NULL angegeben wird SuRun erneut nach dem Kennwort fragen, wenn man SuRun länger als diese Zeit nicht zum starten eines Programms benutzt. Das ist Sinnvoll für Situationen, in denen man häufig

Programme als Administrator starten muss aber den Rechner regelmäßig unbeaufsichtigt lässt. So können andere Benutzer SuRun nur schwer missbrauchen.

- **Zeige Warnung bei Administratoren mit leeren Kennwörtern**
  SuRun kann beim Anmelden eines Benutzers prüfen, ob im System lokale Administratoren existieren, die kein Kennwort haben.
  Standardmäßig legt Microsoft bei der Installation genau so ein Konto, den vordefinierten „Administrator“ ohne Kennwort an. Das ist ein erhebliches Sicherheitsrisiko! SuRun kann in solchen Fällen warnen:



  Das Hinweisfenster verschwindet nicht von selbst und muss manuell geschlossen werden.
  Als Standard werden Administratoren und nicht eingeschränkte Mitglieder der Gruppe SuRunners gewarnt, es gibt jedoch fünf Optionen, welche Benutzer gewarnt werden: "Alle Benutzer", "SuRunner und Administratoren", "unbeschränkte SuRunner und Administratoren", "Administratoren" und "Niemanden".

Shell Integration:

SuRun kann sich in das Kontextmenü und das Systemmenü der Windows Oberfläche integrieren. Ein Kontext-Menü für ein Objekt erscheint, wenn man mit der rechten Maustaste auf ein Objekt klickt bzw. die Menü-Taste drückt.

Das System-Menü erscheint, wenn man auf das Symbol in der Titelleiste einer Anwendung klickt, wenn man auf die Titelleiste der Anwendung mit der rechten

Maustaste klickt oder wenn man [ALT]+[Leerzeichen] drückt:

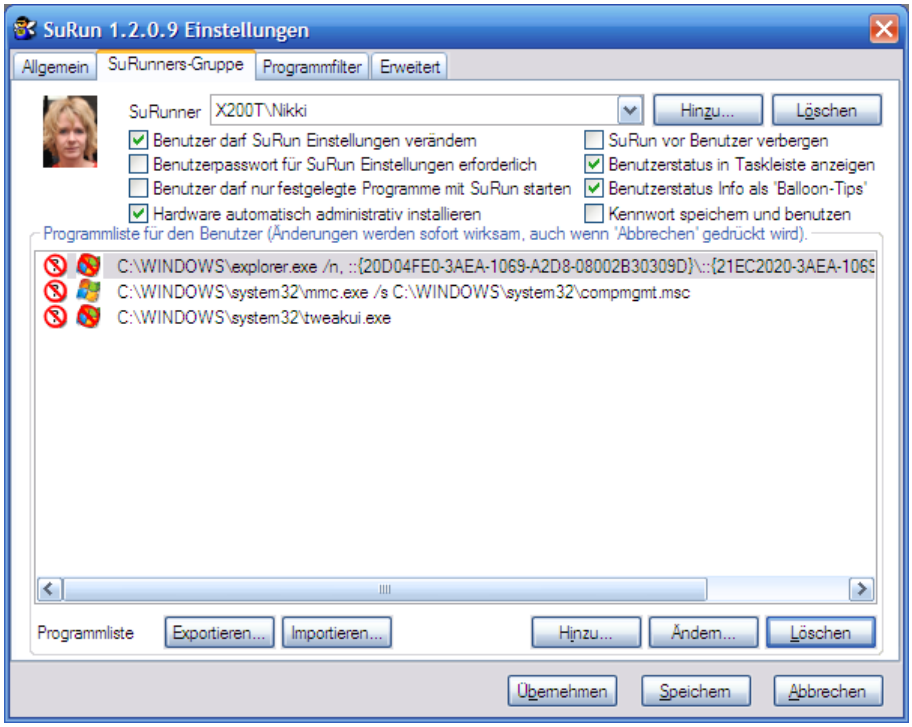
- **Zeige "Systemsteuerung als Administrator" im Kontext-Menü des Desktop**
  Systemsteuerung als Administrator wird im Kontext-Menü des Desktops eingeblendet. Klickt man auf den Befehl, wird die Systemsteuerung mit erhöhten Rechten gestartet.
- **Zeige "'SuRun cmd' hier" im Kontext-Menü für Ordner**
  'SuRun cmd' hier wird im Kontext-Menü für Ordner eingeblendet.
  Klickt man auf den Befehl, wird die Eingabeaufforderung (cmd) im gewählten Ordner mit erhöhten Rechten gestartet.
- **Zeige "'SuRun Explorer' hier" im Kontext-Menü für Ordner**
  'SuRun Explorer' hier wird im Kontext-Menü für Ordner eingeblendet.
  Klickt man auf den Befehl, wird Explorer im gewählten Ordner mit erhöhten Rechten gestartet.
- **Zeige "Neustart als Administrator" im System-Menü von Programmen**
  Neustart als Administrator wird im Systemmenü von Programmen eingeblendet. Klickt man darauf, fragt SuRun, ob das wirklich gewünscht ist. Wenn ja, beendet SuRun das laufende Programm und startet es erneut als Administrator.
- **Zeige "Start als Administrator" im System-Menü von Programmen**
  Start als Administrator wird im Systemmenü von Programmen eingeblendet. Klickt man darauf, fragt SuRun, ob das wirklich gewünscht ist. Wenn ja, startet SuRun das laufende Programm erneut als Administrator.

- **Zeige Einstellungen für erfahrene Benutzer**
  Ist diese Option aktiviert, werden die Seiten **„Programmfilter“** und **„Erweitert“** der SuRun-Einstellungen angezeigt. Versteht man die Einstellungen auf diesen Seiten nicht, sollte **„Zeige Einstellungen für erfahrene Benutzer“** deaktiviert werden.
- **Empfohlene Einstellungen für Heimanwender vorgeben**
  Mit diesem Befehl werden alle SuRun Einstellungen und die Optionen aller „SuRunners“ auf Werte gesetzt, die für den normalen Heimnutzer in Ordnung sein sollten. Sollten Sie Probleme auf Ihrem Computer feststellen, von denen Sie glauben, dass sie mit den SuRun-Einstellungen zusammen hängen könnten, sollten Sie die empfohlenen Einstellungen wählen.

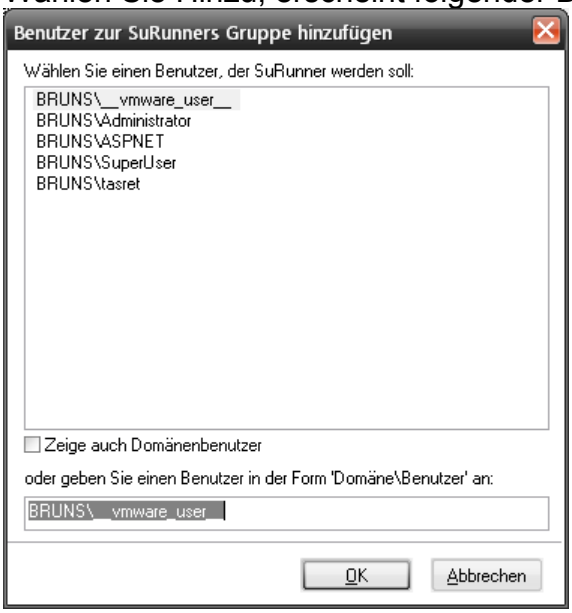
Tipp: Damit Sie später wieder einfach zu Ihren persönlichen Einstellungen zurückkehren können, sollten sie diese zuvor sichern (siehe folgende Punkte).
Hinweis: Auch wenn die Seiten **„Programmfilter“** und **„Erweitert“** der SuRun-Einstellungen ausgeblendet sind, werden deren Einstellungen auf Standards gesetzt. Die Windows Optionen, die man auf der Seite **„Erweitert“** mit SuRun verändern kann, werden jedoch nicht angetastet

- **Sichern...**
  Mit diesem Befehl werden alle SuRun Einstellungen und die Optionen aller „SuRunners“ in einer Datei gespeichert.
  Hinweis: Auch wenn die Seiten **„Programmfilter“** und **„Erweitert“** der SuRun-Einstellungen ausgeblendet sind, werden die dort aktiven Einstellungen gespeichert. Die Windows Optionen, die man auf der Seite **„Erweitert“** mit SuRun verändern kann, werden jedoch nicht gesichert.
- **Wiederherstellen...**
  Mit diesem Befehl werden alle SuRun Einstellungen und die Optionen aller „SuRunners“ aus einer Datei geladen. Auch wenn die Seiten **„Programmfilter“** und **„Erweitert“** der SuRun-Einstellungen ausgeblendet sind, werden die dort aktiven Einstellungen gesetzt. Die Windows Optionen, die man auf der Seite **„Erweitert“** mit SuRun verändern kann, werden jedoch nicht verändert.

SuRun Einstellungen „SuRunners-Gruppe“



- **SuRunner <Name>, Hinzu, Löschen**
  In der Liste stehen alle Mitglieder der lokalen Benutzergruppe „SuRunners“.
  Die Optionen des ausgewählten Benutzers werden auf dieser Seite dargestellt.
  Wählen Sie Hinzu, erscheint folgender Dialog:



  Hier können Sie einen Benutzer, der nicht Mitglied der lokalen Benutzergruppe „SuRunners“ ist, in die Gemeinde der SuRunners aufnehmen.
  Administratoren werden dabei automatisch zu normalen Benutzern degradiert.
  Mit „Löschen“ können Sie einen SuRunner aus der Gemeinde verbannen. Wenn Sie das tun wird SuRun fragen, ob der verbannte zum Administrator gemacht werden soll.

- **Benutzer darf SuRun Einstellungen verändern**
  Entfernt man den Haken, kann der gewählte Benutzer zukünftig die SuRun Einstellungen weder sehen noch ändern.

- **Benutzerpasswort für SuRun Einstellungen erforderlich**
  Ist diese Option aktiv, fragt SuRun jedes mal nach dem Benutzerkennwort, wenn die SuRun Einstellungen gestartet werden.
  Das Kennwort wird nur überprüft und dann sofort verworfen.

- **Benutzer darf nur festgelegte Programme mit SuRun starten**
  Für Programmen, die nicht in der Liste stehen, verweigert SuRun den administrativen Start für diesen Benutzer.

- **Hardware automatisch administrativ installieren**
  Dies Option ist nur unter Windows 2000, XP und 2003 und nur bei aktiviertem "Direkt in Programme einhängen, die andere Programme ausführen." verfügbar.
  Ist die Option aktiv, fängt SuRun bei dem aktiven Benutzer den „Neue Hardware gefunden“-Dialog von Windows ab und startet ihn immer als Administrator. So kann der Benutzer Hardware installieren, ohne ein Administratoren-Kennwort preisgeben zu müssen.

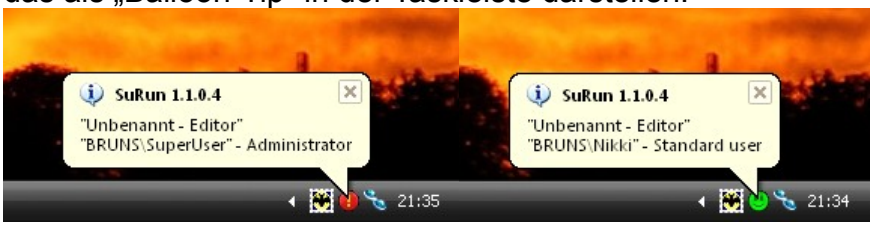
- **SuRun vor Benutzer verbergen**
  Ist diese Option aktiv, werden die Optionen „Benutzer darf SuRun Einstellungen verändern“ und „Benutzerstatus in Taskleiste anzeigen“ deaktiviert und die Option

„Benutzer darf nur festgelegte Programme mit SuRun starten“ aktiviert.
Der Benutzer bekommt zusätzlich keine Meldungen von SuRun zu sehen und kann auch nur Programme administrativ starten, die in der Programmliste festgelegt sind. Das ist in Firmenumgebungen und Eltern/Kind-Szenarien sinnvoll, wenn Programme Administratorrechte erfordern, der Benutzer aber nicht merken darf, dass er Programme mit gehobenen Rechten starten darf.

- **Benutzerstatus in Taskleiste anzeigen**
  SuRun kann im Infobereich der Taskleiste ein Symbol einblenden, dass anzeigt, welche Rechte das aktive Fenster hat. Fünf verschiedene Symbole werden dargestellt:
  - Aktives Fenster hat Standard-Rechte, Explorer auch
  - Aktives Programm wurde von SuRun mit gehobenen Rechten gestartet
  - Kein aktives Fenster
  - Explorer läuft als Administrator, das aktive Fenster auch
  - Aktives Fenster läuft als Administrator, Explorer nicht

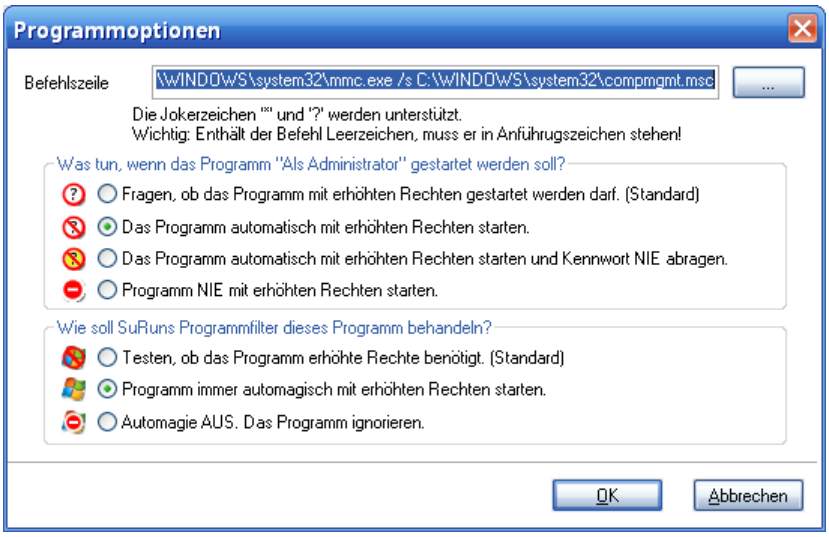
  Mit dieser Option kann man für jeden SuRunner getrennt festlegen, ob er das Symbol sehen (Haken gesetzt) oder nicht sehen soll (Haken gelöscht).

- **Benutzerstatus Info als 'Balloon-Tips'**
  Hat das aktive Fenster einen anderen Benutzer als den angemeldeten, kann SuRun das als „Balloon-Tip“ in der Taskleiste darstellen:

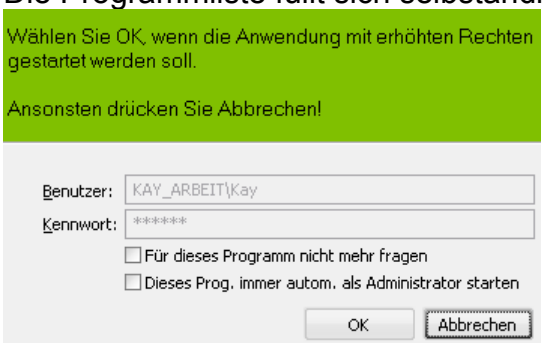


- **Kennwort speichern und benutzen**
  Ist diese Option aktiv, fragt SuRun einmalig das Kennwort des Benutzers ab, speichert und verwendet es, um Programme mit gehobenen Rechten zu starten. Diese Option ist vor Allem dann sinnvoll, wenn man mit SuRun Probleme beim Zugriff auf Ressourcen in Netzwerken hat.
  Sicherheit: Das Kennwort wird mit der Windows-Funktion *CryptProtectData* verschlüsselt in einem nur für „SYSTEM“ zugreifbaren Zweig der Registry gespeichert. Die Funktion *CryptProtectData* benutzt einen Master-Key, der aus dem eigentlichen Benutzer-Kennwort erzeugt wird. Damit ist es sehr schwer möglich, aus den verschlüsselten Daten das Benutzerkennwort zurück zu gewinnen.

- **Programmliste für den Benutzer, Export, Import, Hinzu, Bearbeiten, Löschen**
  In dieser Liste stehen alle Programme, die SuRun besonders behandelt.
  Die Bedeutung der Symbole in der Liste sieht man, wenn man „Hinzu“ oder „Ändern“ drückt:



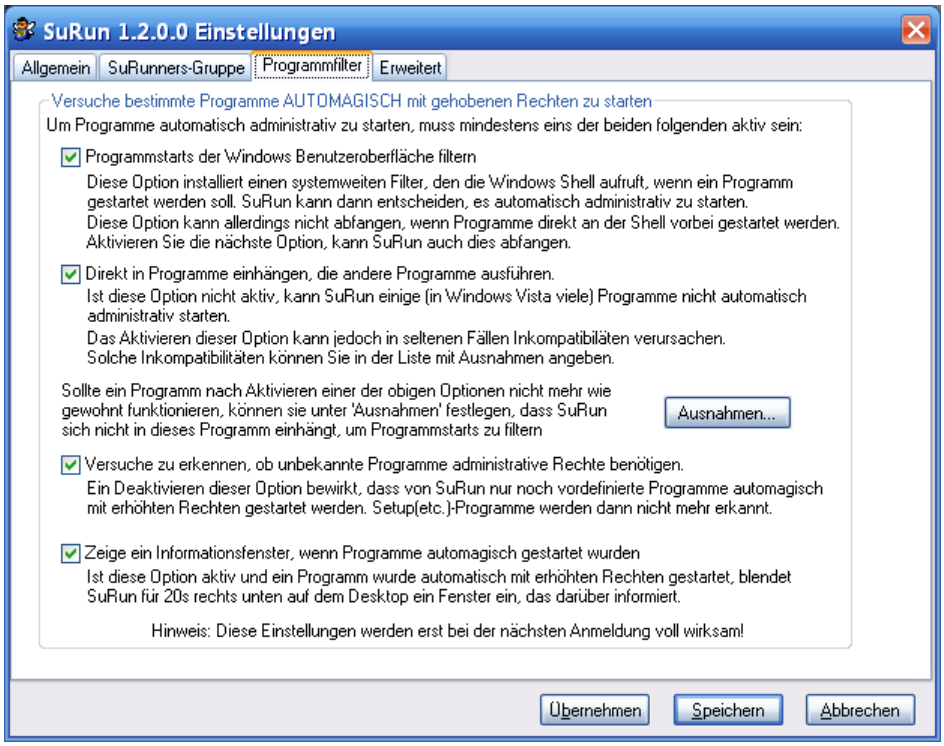
Die Symbole für den automatischen Start sind nur aktiv, wenn SuRun **"Versuche bestimmte Programme AUTOMAGISCH mit gehobenen Rechten zu starten"** auf der Seite **„Erweitert“** der SuRun Einstellungen aktiviert ist.
Die Bedeutung der Knöpfe ist selbsterklärend.
HINWEIS: Sind „Programm NIE mit erhöhten Rechten starten“ und „Programm immer automagisch mit erhöhten Rechten starten“ beide aktiviert, wird das Programm direkt von SuRun immer ohne gehobene Rechte gestartet.
Um mehrere Programme aus der Liste zu löschen, können Sie (wie in Windows allgemein üblich) mehr als einen Eintrag in der Liste markieren, indem Sie gleichzeitig die Strg-Taste festhalten. Um die gesamte Liste zu löschen, markieren Sie sie, indem Sie Strg+“A“ drücken oder zunächst den ersten Eintrag anklicken und anschließend den letzten mit festgehaltener Umschalttaste. Zum Löschen können Sie statt der Schaltfläche auch die Taste Entf verwenden. Diese Funktionen sind insbesondere zum vollständigen Importieren (siehe im Folgenden) hilfreich.
Die Programmliste füllt sich selbständig, wenn Sie in SuRuns Bestätigungsdialog:



"Für dieses Programm nicht mehr fragen" oder "Dieses Prog. immer autom. als Administrator starten" aktiviert haben.
Mit „**Exportieren...**“ der Programmliste exportieren Sie die Programmliste des oben ausgewählten SuRunners; entsprechend wird bei „**Importieren...**“ eine exportierte zu dem oben ausgewählten SuRunner importiert. Mit diesen Export / Import-Funktionen können Sie also ganz einfach die Programmlisten eines SuRunners auf andere SuRunner verteilen. Andere Einstellungen zu den SuRunnern (oberhalb der Programmliste) werden bei diesen Exporten nicht berücksichtigt und bleiben folglich nach einem Import von einem anderen SuRunner unverändert. Einträge in der Programmliste des SuRunners, zu dem der Import erfolgt, bleiben erhalten, bei

Programmen, die sich sowohl in der Liste des gewählten SuRunners und im Import befinden, bleiben die Einstellungen des gewählten SuRunners erhalten. Um für einen SuRunner die Programmliste vollständig durch die importierte Liste zu ersetzen, müssen Sie die vorhandene Liste zuvor löschen (siehe oben).

SuRun Einstellungen, „Programmfilter“



Versuche bestimmte Programme AUTOMAGISCH mit gehobenen Rechten zu starten
SuRun kann versuchen, das Ausführen von Programmen abzufangen. Wenn ein Programm mit administrativen Rechten ausgeführt werden muss, schlägt SuRun vor, dieses Programm gleich mit erhöhten Rechten zu starten.
So kann man auch ohne Eingabe einer „SuRun <Programm>“ Befehlszeile und ohne „Starte als Administrator“, Programme automatisch administrativ ausführen lassen.

> *Unter Windows kann man Programme auf verschiedene Weise in den Speicher Laden und ausführen.*
>
> *Eine Methode ist z.B. die Funktion "CreateProcess", die hat aber für viele den Nachteil, dass man damit wirklich nur EXE-Dateien ausführen kann.*
>
> *Eine zweite Funktion ist "ShellExecute(Ex)".*
>
> *Damit kann man Dateien und Verknüpfungen "ausführen", Drucken und vieles mehr.*

So z.B. startet Explorer -die Windows Shell- bei mir, wenn ich auf ein JPG-File Doppelklicke mit *ShellExecute(Ex)* IrfanView.
Weil das so schön geht, benutzen fast alle Programme ShellExecute, wenn sie etwas ausführen müssen.
In Windows 2000/2003/XP/Vista kann man sich in diese Funktion einklinken.

Das macht man mittels eines COM-Interfaces Namens "*IShellExecuteHook*".
Wenn Sie **"Programmstarts der Windows Benutzeroberfläche filtern"** aktiviert haben, implementiert SuRun dieses Interface und bekommt so mit, wenn ein Programm „*ShellExecute(Ex)*“ aufruft.

Das hat aber auch Nachteile.

Wenn ein Programm nicht „*ShellExecute(Ex)*“, sondern CreateProcess benutzt, bekommt SuRun das nicht mit und kann das Programm nicht starten. Falls ein anderes Programm vor SuRun in der Liste der „*IShellExecuteHook“*-Programme aufgerufen wird, bekommt SuRun das auch nicht mit.
Der Explorer von Windows Vista führt z.B. fast nichts per „*ShellExecute(Ex)*“ aus. Deshalb wird ein aktives **"Programmstarts der Windows Benutzeroberfläche filtern"** in Vista nicht sehr Erfolgreich sein.

Die zweite, am häufigsten benutzte Windows Funktion um ein Programm zu starten ist „*CreateProcess*“. Selbst „*ShellExecute(Ex)*“ benutzt meistens „*CreateProcess*“, um ein Programm zu starten.

Dumm nur, dass es keine offizielle Möglichkeit gibt, sich in „*CreateProcess“* einzuhängen.

Wenn die Option **"Direkt in Programme einhängen, die andere Programme ausführen."** aktiviert ist, benutzt SuRun eine nicht offizielle, aber gebräuchliche Methode, um unter anderen „*CreateProcess*“ abzufangen.

> *Innerhalb eines Windows Prozesses werden Aufrufe von Funktionen, die in DLLs implementiert sind (Importe) über Tabellen gehandhabt. Die jeweilige DLL wird in den Speicher des Prozesses geladen. Dann werden die Tabellen mit den Importierten Funktionen des Moduls auf die geladene DLL “verbogen” und alles läuft prima. Es gibt also Tabellen mit den Adressen importierter DLL Funktionen, kurz Import Address Tabellen oder IAT.*

Wenn man die IAT aller geladenen Module so modifiziert, dass anstatt „*CreateProcess*“ eine eigene Funktion aufgerufen wird, kann man so kontrollieren, was wie gestartet wird.

Aber auch das hat Nachteile! Da IAT-Hooking nicht offiziell unterstützt ist, kann es sein, das das irgendwann nicht mehr funktioniert. Bisher geht es allerdings prima, selbst in Windows Vista und Vista x64.
Der zweite Nachteil: Wenn z.B. ein Systemsteuerungs-Modul (wie ncpa.cpl) gestartet werden soll, wird zwar der „*IShellExecuteHook*“ aber nicht „*CreateProcess*“ aufgerufen, denn Explorer handhabt das selbst.

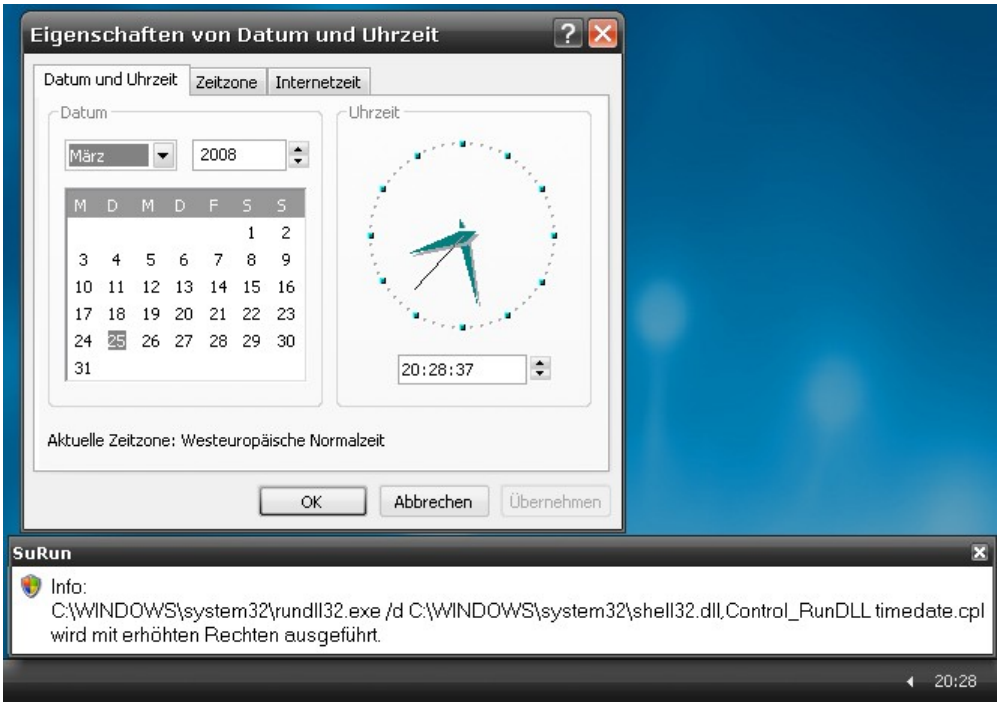
Es sollten also beide Optionen aktiviert werden, damit möglichst kein administrativ zu startender Prozess von SuRun verpasst wird.

Sollte ein Programm nicht mehr, wie gewohnt, funktionieren, wenn eine der beiden o.g. Optionen aktiv ist, kann dieses Programm in die **„Ausnahmen...“** Liste aufgenommen werden. Dann wird SuRun sich in dieses Programm nicht mehr einhängen und es sollte dann wieder funktionieren.

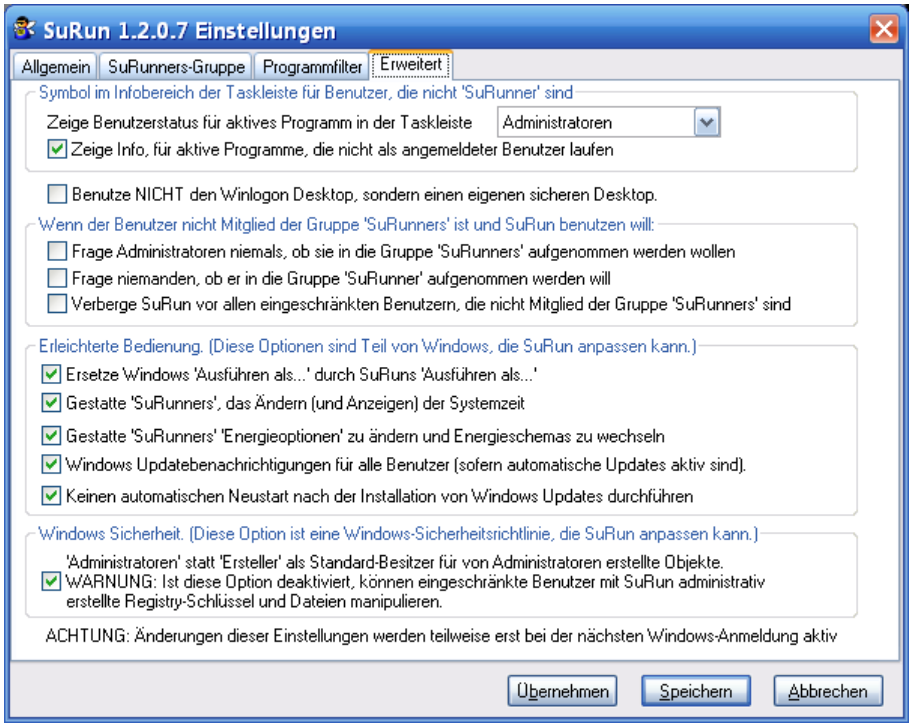
- **Versuche zu erkennen, ob unbekannte Programme administrative Rechte benötigen.**
  Ist diese Option aktiv, und ein Programm soll gestartet werden, prüft SuRun wenn es nicht in der Programmliste des Benutzers steht, ob dieses Programm

administrative Rechte zum Ausführen benötigt. Wenn ja, wird vorgeschlagen, dieses unbekannte Programm gleich mit gehobenen Rechten zu starten.

- **Zeige ein Informationsfenster, wenn Programme automagisch gestartet wurden**
  Startet SuRun ein Programm automatisch mit gehobenen Rechten und diese Option ist aktiv, informiert ein kleines Fenster rechts unten am Bildschirm über diesen automatischen Start.

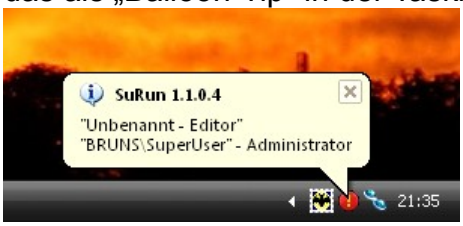


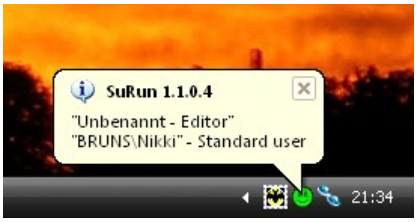
SuRun Einstellungen, „Erweitert“



- **Zeige Benutzerstatus für aktives Programm in der Taskleiste**
  SuRun kann im Infobereich der Taskleiste ein Symbol einblenden, dass anzeigt, welche Rechte das aktive Fenster hat. Fünf verschiedene Symbole werden dargestellt:
  - :Aktives Fenster hat Standard-Rechte, Explorer auch
  - :Aktives Programm wurde von SuRun mit gehobenen Rechten gestartet
  - :Kein aktives Fenster
  - :Explorer läuft als Administrator, das aktive Fenster auch
  - : Aktives Fenster läuft als Administrator, Explorer nicht

  Mit dieser Option kann man Festlegen welchen Benutzern des PC das Symbol gezeigt werden soll („Administratoren“, „allen Benutzern“, „Niemanden“). Standardmäßig ist das Symbol abgeschaltet.
  Für Mitglieder der SuRunners-Gruppe kann diese Option auf der Seite **„SuRunners-Gruppe“** der SuRun-Einstellungen überschrieben werden.
- **Zeige Info, für aktive Programme, die nicht als angemeldeter Benutzer laufen**
  Hat das aktive Fenster einen anderen Benutzer als den angemeldeten, kann SuRun das als „Balloon-Tip“ in der Taskleiste darstellen:



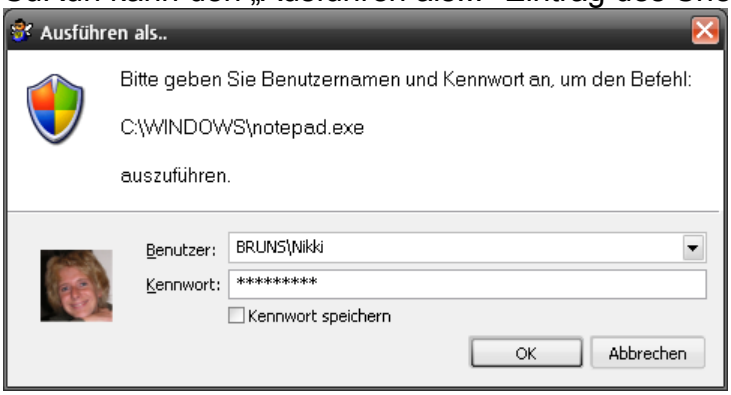


- **Benutze NICHT den WinLogon Desktop, sondern einen eigenen sicheren Desktop.**

SuRun verwendet als sicheren Desktop, den bereits von WinLogon.exe erstellten. Er ist immer vorhanden und für Benutzer unzugänglich. Sollte es dennoch zu Seltsamkeiten kommen, kann man diese Option aktivieren. Allerdings braucht das deutlich mehr Systemressourcen, da jedes Mal, wenn SuRun mit dem Benutzer interagiert, ein neuer Desktop angelegt und danach wieder freigegeben wird.

- **Frage Administratoren niemals, ob sie in die Gruppe 'SuRunners' aufgenommen werden wollen**
  Ist diese Option aktiv, werden Administratoren nicht gefragt, ob sie Mitglieder der Gruppe der SuRunners werden wollen, wenn sie im Kontextmenü den Befehl "**Starte als Adminsitrator...**" aufrufen. (Das Programm wird ganz normal gestartet.)
- **Frage niemanden, ob er in die Gruppe 'SuRunner' aufgenommen werden will**
  Falls Sie SuRun benutzen aber kein Mitglied der lokalen Benutzergruppe „SuRunners“ sind, wird SuRun einen Fehler zurückgeben und nicht versuchen Sie in die „SuRunners“ Gemeinde aufzunehmen.
- **Verberge SuRun vor allen eingeschränkten Benutzern, die nicht Mitglied der Gruppe 'SuRunners' sind**
  Ist diese Option aktiv, bekommen Benutzer, die keine Administratoren sind, keine Meldungen von SuRun zu sehen und können auch keine Programme administrativ starten.

Mit Einstellungen im Feld **"Erleichterte Bedienung"** kann man einige Windows Unannehmlichkeiten umgehen, die im Eigentlichen nichts mit SuRun zu tun haben.

- **Ersetze Windows 'Ausführen als...' durch SuRuns 'Ausführen als...'**
  Das Benutzen des eingebauten „Ausführen als...“ von Windows ist sehr unsicher! Selbst Programme mit Gast-Rechten können die eingegebenen Daten abfangen und das System übernehmen.
  SuRun kann den „Ausführen als...“-Eintrag des Shell Kontext-Menüs ersetzen:
  

  Das hat den großen Vorteil, dass das Benutzerkennwort auf einem abgesicherten Desktop abgefragt wird und nicht ausgespäht werden kann. Das Kennwort für den Benutzer kann gespeichert werden. Es wird leicht verschlüsselt in der Registry unter „HKEY_LOCAL_MACHINE\SECURITY\SuRun\RunAs\<username>\Cache“ gespeichert.
- **Gestatte 'SuRunners', das Ändern (und Anzeigen) der Systemzeit**
  Eingeschränkte Benutzer dürfen in Windows NT die Uhrzeit des Systems **nicht** verändern. Das ist ganz besonders wichtig, wenn der Rechner Domänenmitglied ist, aber auch für Heimbenutzer aus Sicherheitsgründen zu empfehlen. Wenn es

Sie allerdings stört, dass Sie nicht unmittelbar auf den Datumsdialog zugreifen können, aktivieren Sie diese Option. Sie können dann mit einem Doppelklick auf die Uhrzeit im Infobereich der Taskleiste den Dialog öffnen.
Aktivieren Sie diese Option, bekommen Mitglieder der Gruppe SuRunners das Privileg “**SeSystemtimePrivilege**” und dürfen ab der nächsten Anmeldung die Systemzeit verändern.

- **Gestatte 'SuRunners' 'Energieoptionen' zu ändern und Energieschemas zu wechseln**
  Eingeschränkte Benutzer dürfen nicht per Klick auf das Akku-Symbol in der Taskleiste einstellen, ob Windows Energie oder Zeit sparen soll. Das liegt daran, das eingeschränkte Benutzer keinen Schreibzugriff auf die Energie-Einstellungen in der Registry (HKLM\ Software\ Microsoft\ Windows\ CurrentVersion\ Controls Folder\ PowerCfg) haben.
  Aktivieren Sie diese Option, wird den Berechtigungen für den Registry-Zweig Vollzugriff für die SuRunners gesetzt. Wenn Sie die Option deaktivieren, werden die SuRunners wieder aus den Registry-Berechtigungen entfernt.
- **Windows Updatebenachrichtigungen für alle Benutzer (sofern automatische Updates aktiv sind).**
  Eingeschränkte Benutzer werden standardmäßig nicht über Updates informiert. In Windows XP Professional kann man das mit dem Gruppenrichtlinien-Editor ändern. In Windows XP Home geht das mit Windows-Mitteln nicht zu ändern.
  Aktivieren Sie diese Option um die gewohnten Balloon-Tips und Schild-Symbole des Windows Update Clients in der Taskleiste zu sehen.
- **Keinen automatischen Neustart nach der Installation von Windows Updates durchführen**
  Sind automatische Updates aktiviert und ein eingeschränkter Benutzer angemeldet, werden Updates installiert und der PC dann neu gestartet. Ob ein nicht gespeichertes Dokument offen ist, oder nicht. Auch das kann man nicht mit Bordmitteln von Windows XP Home verändern.
  Aktivieren Sie diese Option, können Sie wählen, ob Sie *nach einem Update jetzt* oder *später* den PC neu starten wollen.

- **'Administratoren' statt 'Ersteller' als Standard-Besitzer für von Administratoren erstellte Objekte.**
  Standardmäßig ist der Ersteller eines Objektes, z.B. einer Datei, eines Ordners oder eines Registry Schlüssels, dann auch dessen Besitzer. Besitzer von Objekten dürfen sich darauf Vollzugriff verschaffen. Wenn zum Beispiel ein mit SuRun gestarteter, als Administrator laufender Prozess, einen Registry Schlüssel unter HKEY_LOCAL_MACHINE anlegt, kann der eingeschränkte Benutzer, der SuRun benutzt hat, diesen Registry Schlüssel jederzeit manipulieren, indem er sich mit Vollzugriff in die Zugriffskontrollliste des Registry Schlüssels einträgt und dann damit macht, was er will. Das Gleiche geht mit Dateien.
  Ist diese Option aktiviert, sind Objekte, die ein Administrator erstellt im Besitz der Gruppe “Administratoren” und **nicht** im Besitz des Benutzers. Das verhindert, dass diese Objekte später von dem selben aber dann eingeschränkten Benutzer manipuliert werden können.

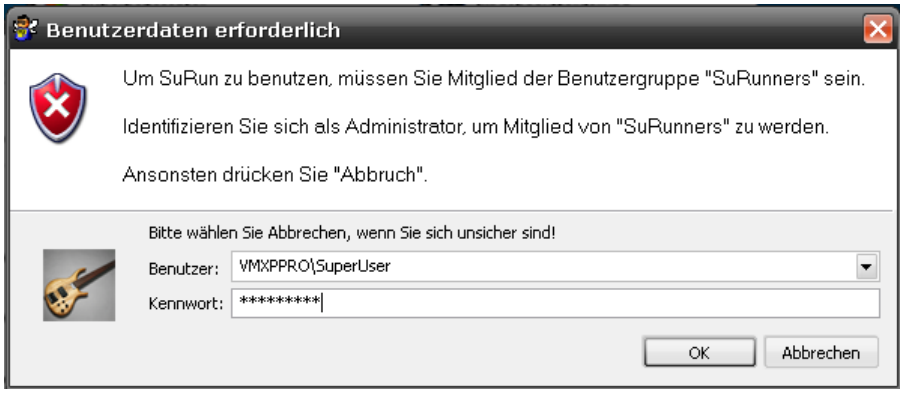
HINWEIS: Diese Option sollte unbedingt aktiviert sein!

Betrieb

„SuRunner“ werden

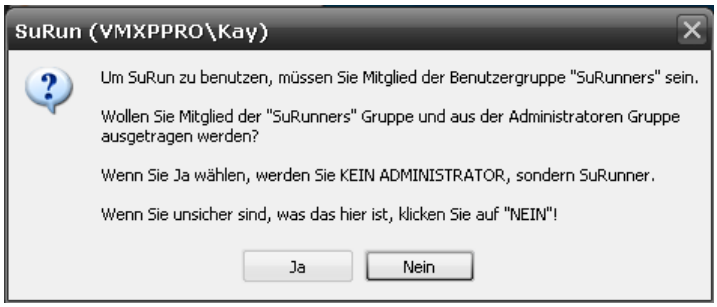
Sind Sie kein Mitglied der Benutzergruppe “**SuRunners**“ und versuchen ein Programm als Administrator zu starten oder die **„SuRun Einstellungen“** mit der Systemsteuerung aufzurufen, bietet Ihnen SuRun an, beizutreten.

Sind sie kein Administrator, müssen Sie durch Eingabe des Passwortes eines Administrators als berechtigt ausweisen, damit SuRun Sie in die “**SuRunners**” aufnimmt.



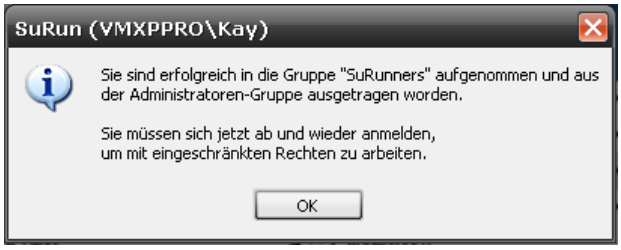
Das Kennwort wird in einer gesicherten Umgebung abgefragt, überprüft, sofort verworfen und kann nach meiner Kenntnis nicht erhascht werden.

Sind Sie ein Administrator, dann wird SuRun Sie bei der ersten Benutzung fragen, ob Sie Mitglied der Benutzergruppe “**SuRunners**” und Ex-Mitglied der “**Administratoren**” werden wollen.



Sie müssen sich danach von Windows ab- und wieder anmelden.

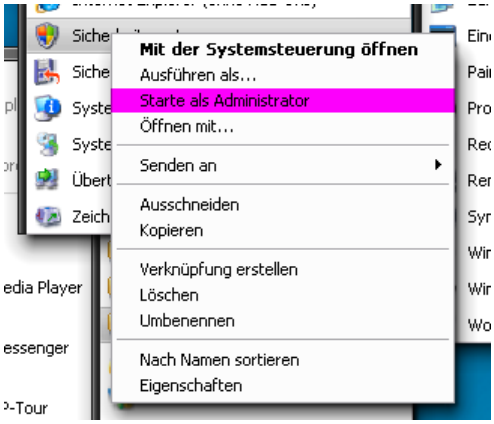
Ist in den SuRun Einstellungen **"Frage niemanden, ob er in die Gruppe 'SuRunner' aufgenommen werden will"** bzw. **"Frage Administratoren niemals, ob sie in die Gruppe 'SuRunners' aufgenommen werden wollen"** aktiviert, wird SuRun Sie natürlich nicht nerven und Sie „dürfen“ sich selbst in die SuRunners Gruppe ein- und aus der Administratoren-Gruppe austragen.



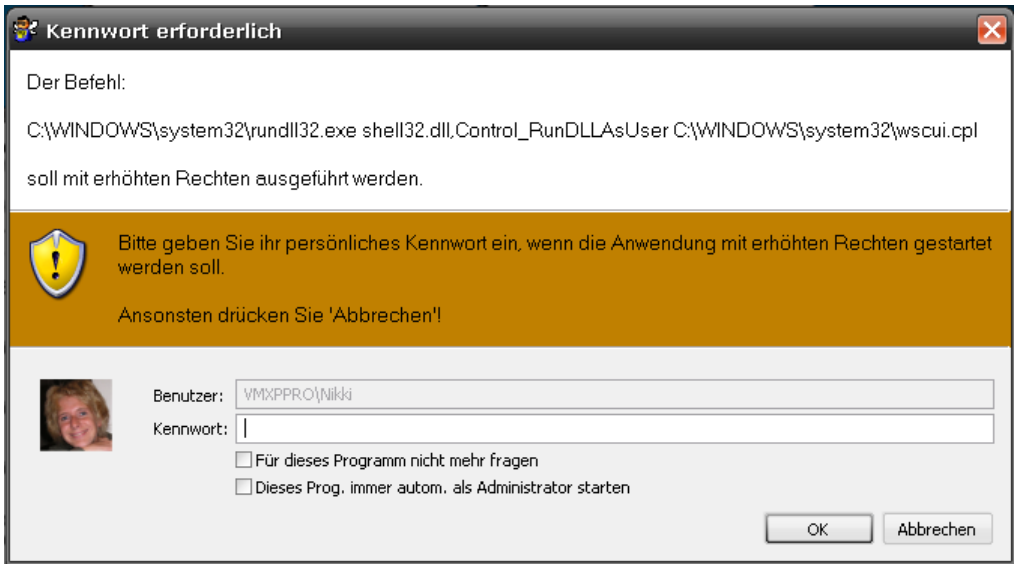
Jetzt sind Sie SuRunner und dürfen komfortabel eingeschränkt arbeiten.

Starte als Administrator

Wenn Sie ein Programm mit administrativen Rechten starten wollen dann klicken Sie mit der rechten Maustaste darauf und wählen Sie „*Starte als Administrator*“ im Kontextmenü.



SuRun benötigt kein Passwort, um Programme mit gehobenen Rechten zu starten. Haben Sie jedoch die Option **"Benutzer-Kennwort abfragen"** aktiviert, fragt SuRun nach dem persönlichen Kennwort des angemeldeten Benutzers.

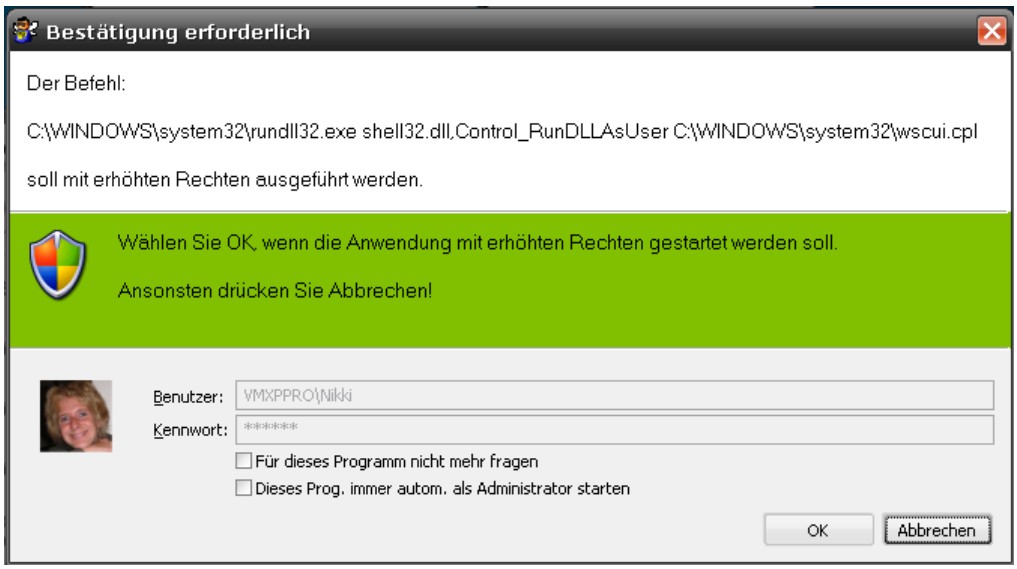


Das Passwort wird überprüft, sofort verworfen und nicht gespeichert.

Ausnahmen:

- Bei Domänen-Benutzern benötigt und speichert SuRun das Benutzerkennwort verschlüsselt an einer unzugänglichen Stelle der lokalen Registry.
- Ist die Benutzer-Option „Kennwort speichern und benutzen“ aktiv, wird das Benutzerkennwort gespeichert. (siehe "Kennwort speichern und benutzen")

Ist die Option "Benutzer-Kennwort abfragen" nicht aktiv, fragt SuRun nur nach Bestätigung:



Automagie und Fragefreiheit

Aktivieren Sie das Kästchen **„Für dieses Programm nicht mehr fragen“**, so wird SuRun für dieses Programm bei allen folgenden Aufrufen mit SuRun automatisch die von Ihnen gewählte „Antwort geben“.

Im obigen Beispiel würde SuRun nicht mehr fragen, ob das Sicherheitscenter mit erhöhten

Rechten gestartet werden darf. Klicken Sie „OK“, wird es ohne Nachfragen gestartet. Klicken Sie „Abbrechen“, wird SuRun das Sicherheitscenter auch in Zukunft automatisch nicht starten.

Diese Option ist sinnvoll, um z.B. Windows-Autostart Programme zu starten, die administrative Rechte benötigen.

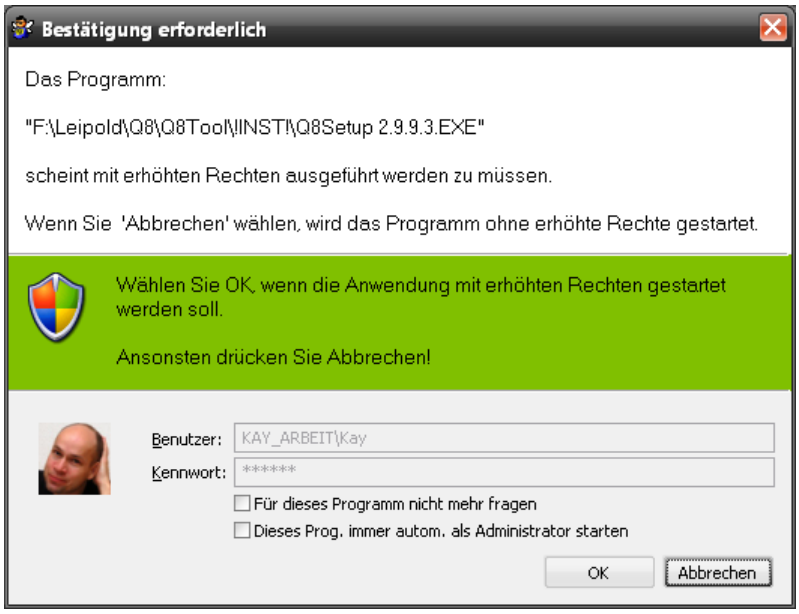
Es ist auch möglich, das SuRun fälschlicher Weise ein Programm administrativ starten will. Ein fiktives Programm „PlinseTupper.exe“ z.B. beinhaltet „setUp“. Deshalb wird SuRun fragen, ob das Programm als Administrator gestartet werden soll. Aktivieren Sie das Kästchen **„Für dieses Programm nicht mehr fragen“** und drücken Sie „**Abbrechen**“, um die Nerverei zu beenden.

Ist **„Dieses Prog. immer autom. als Administrator starten“** aktiv, wird SuRun versuchen, dieses Programm auch ohne **„Starte als Administrator“** immer mit erhöhten Rechten zu starten.

Scheint ein Programm gehobene Rechte zu benötigen, wird SuRun fragen, ob es damit gestartet werden soll. Dass ein Programm gehobene Rechte braucht, erkennt SuRun so:

- Das Programm steht als **“immer mit gehobenen Rechten starten”** in der Programmliste des Benutzers
- Die Option **"Versuche zu erkennen, ob unbekannte Programme administrative Rechte benötigen."** ist aktiv **und**
  - Das Programm hat als Endung exe, cmd, lnk, com, pif, bat und der Dateiname enthält eine der Zeichenfolgen „install“, „setup“, „upgrade“ oder „update“
  - Das Programm hat eine interne oder externe Kennung (Manifest Ressource oder eine externe Manifest Datei die <*trustInfo>-> <*security>-> <*requestedPrivileges>-> <*requestedExecutionLevel level=”requireAdministrator”> enthält)

Soll ein Programm ausgeführt werden und eine der Bedingungen ist erfüllt, wird SuRun folgendes fragen:

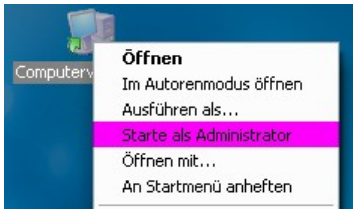


Wie SuRun versucht, den Start eines Programms in Windows abzufangen um es selbst eventuell automagisch mit gehobenen Rechten zu starten, steht hier.

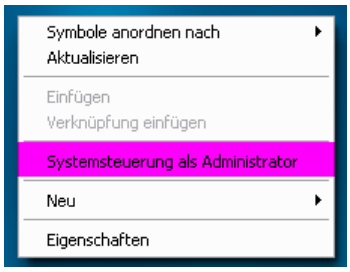
Das Kontext-Menü der Windows Benutzeroberfläche

Zum erleichterten Ausführen von Programmen integriert sich SuRun in das Kontextmenü des Windows Explorers.

Es fügt dem Kontextmenü von Dateien mit der Endung bat, cmd, cpl, exe, lnk, msi, msp und reg einen "**Starte als Administrator**" Befehl hinzu.



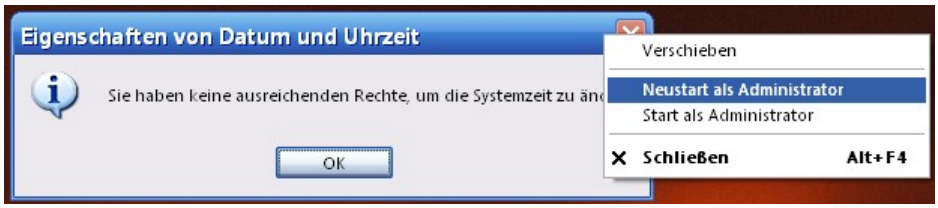
Dem Kontextmenü für den Desktop-Hintergrund fügt SuRun (wie auch SuDown) einen "**Systemsteuerung als Administrator**" Befehl hinzu.



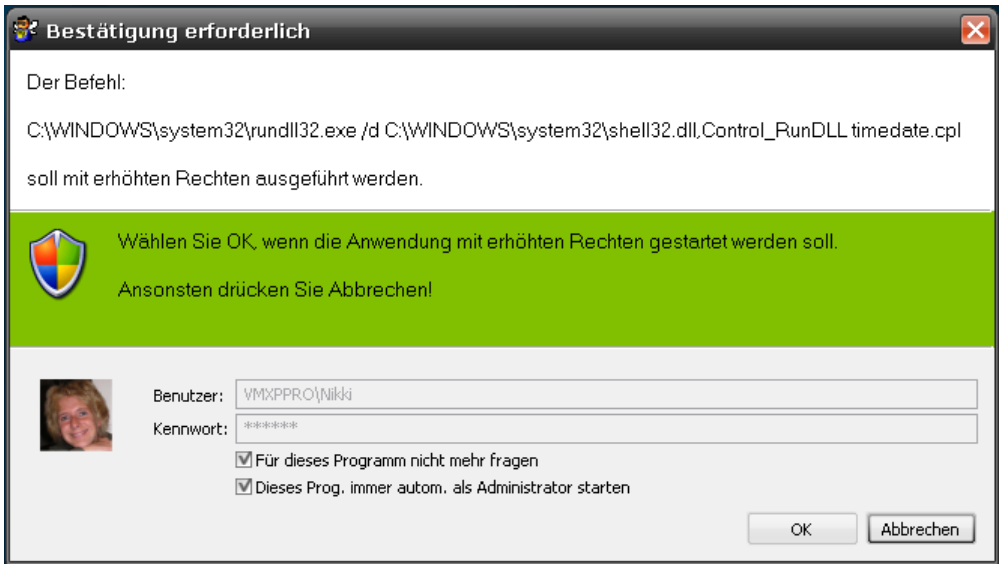
Integration in das System-Menü

Manche Programme erfordern administrative Rechte, z.B. um installiert zu werden, erzählen davon aber erst, wenn sie sich beenden. Wie die Befehlszeile für ein solches Programm genau aussieht ist nur schwer zu erraten.

Um diese Programme komfortabel nutzen zu können integriert sich SuRun in das Windows-Systemmenü:

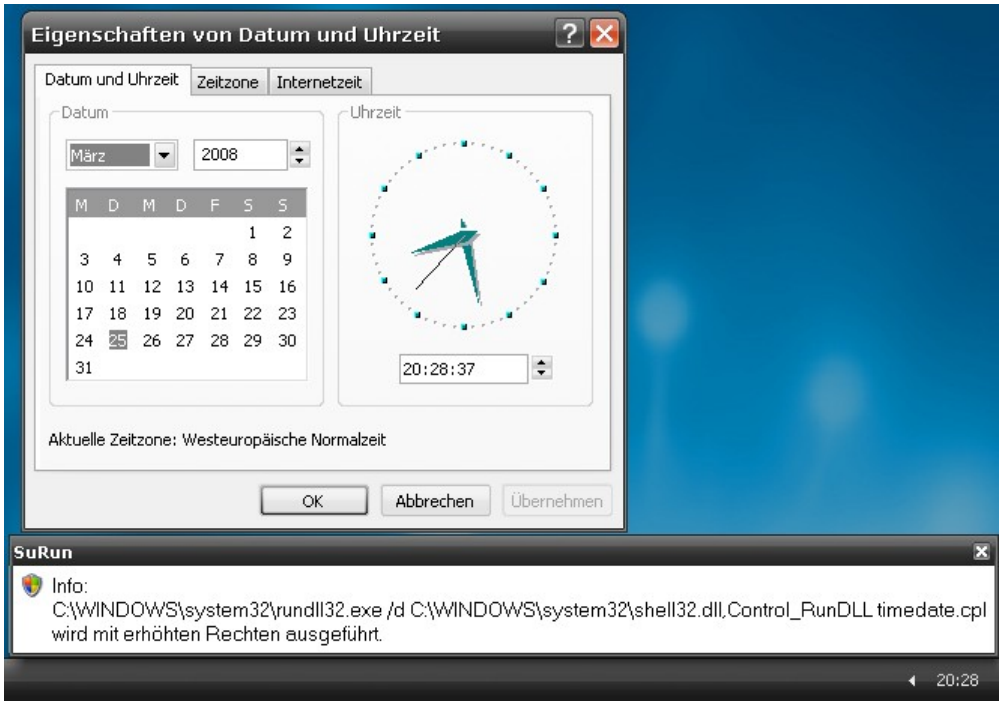


Mit einem Klick mit der rechten Maustaste auf die Titelleiste eines Fensters und den Befehlen "**Neustart als Administrator**" oder "**Start als Administrator**" kann man so des Problemchens Herr werden.



Falls Sie in obigem Beispiel (Doppelklick auf die Uhrzeit im „Tray“) beide Optionen aktivieren und „OK“ drücken, werden beim nächsten Doppelklick darauf die **„Eigenschaften von Datum und Uhrzeit“** mit administrativen Rechten gestartet.

Hinweisfenster für automagische Starts



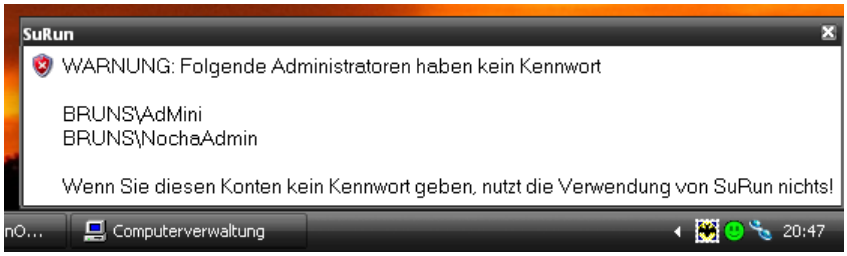
Bei solchen automatischen administrativen Starts zeigt SuRun das optional in einem kleinen Fenster 20 Sekunden lang an.

Hinweisfenster für Administrator-Konten ohne Kennwort

Standardmäßig legt Microsoft bei der Installation genau so ein Konto, den vordefinierten „Administrator“ ohne Kennwort an.

Das ist ein erhebliches Sicherheitsrisiko! Wenn man Windows in den abgesicherten Modus startet, kann so jeder das System als Administrator benutzen.

SuRun kann beim Anmelden eines Benutzers prüfen, ob im System lokale Administratoren existieren, die kein Kennwort haben und dann folgendes zeigen:



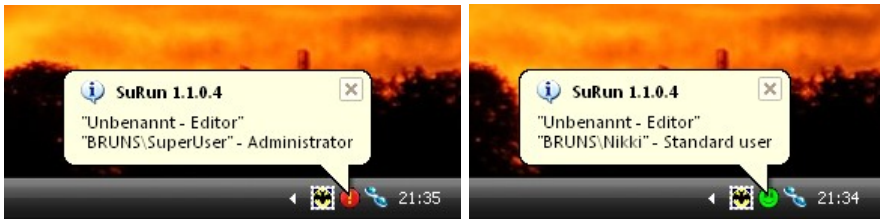
Das Hinweisfenster verschwindet nicht von selbst und muss manuell geschlossen werden. Als Standard werden Administratoren und nicht eingeschränkte Mitglieder der Gruppe SuRunners gewarnt, es gibt jedoch fünf Optionen, welche Benutzer gewarnt werden: „Alle Benutzer", "SuRunner und Administratoren", "unbeschränkte SuRunner und Administratoren", "Administratoren" und "Niemanden".

Taskleistensymbol

SuRun kann im Infobereich der Taskleiste ein Symbol einblenden, dass anzeigt, welche Rechte das aktive Fenster hat. Fünf verschiedene Symbole werden dargestellt:

Aktives Fenster hat Standard-Rechte, Explorer auch
Aktives Programm wurde von SuRun mit gehobenen Rechten gestartet
Kein aktives Fenster
Explorer läuft als Administrator, das aktive Fenster auch
Aktives Fenster läuft als Administrator, Explorer nicht

Hat das aktive Fenster einen anderen Benutzer als den angemeldeten, kann SuRun das optional als „Balloon-Tip“ in der Taskleiste darstellen:



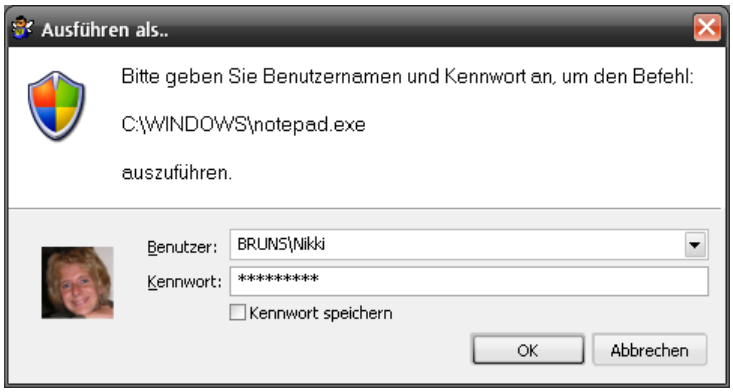
Die Darstellung des Symbols kann für alle Benutzer des Systems festgelegt und für jeden SuRunner einzeln überschrieben werden.

„Ausführen als...“ durch SuRun ersetzen

Das Benutzen des eingebauten „Ausführen als...“ von Windows ist sehr gefährlich!

Selbst Programme mit Gast-Rechten können die eingegebenen Daten mitlesen, so ein Administratorenkennwort erhaschen und das System übernehmen.

SuRun kann den „Ausführen als...“-Eintrag des Explorer Kontext-Menüs ersetzen:



Das hat den großen Vorteil, dass das Benutzerkennwort auf einem abgesicherten Desktop abgefragt wird und nicht ausgespäht werden kann.

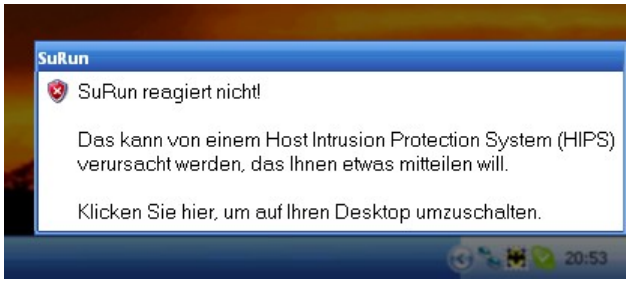
Für jeden Benutzer von „Ausführen als...“ können die eingegebenen Kennworte gespeichert werden. Sie werden verschlüsselt in der Registry unter „HKEY_LOCAL_MACHINE\SECURITY\SuRun\RunAs\<username>\Cache“ gespeichert. Auf diesen Registry-Zweig haben normalerweise nur Dienste Zugriff. Die Verschlüsselung erfolgt **spezifisch** für jeden Benutzer. Die Speicherung erfolgt **getrennt** für jeden Benutzer der „Ausführen als...“ benutzt. Wenn also ein Benutzer Kennworte für „Ausführen als..“ speichert, kann **kein** anderer Benutzer darauf zugreifen.

Der WatchDog

Falls auf dem System ein HIPS (Host Intrusion Protection System) installiert ist -Das ist Software die ungewöhnliches Verhalten von Programmen analysiert und den Benutzer warnt-, kann es sein, dass es Aktionen von SuRun als ungewöhnlich einstuft. Versucht das HIPS dann den Benutzer zu warnen, funktioniert das nicht, denn der sichere Desktop von SuRun ist aktiv. Das ergibt eine typische Patt-Situation:

- SuRun ist durch das HIPS blockiert und kann keine Eingaben verarbeiten
- Das HIPS kann keine Eingaben empfangen, weil SuRuns Desktop aktiv ist

Mit SuRun 1.1.0.6 wurde deshalb ein „WatchDog“ eingeführt. Setzt SuRun für länger als zwei Sekunden ein Signal nicht, ist es scheinbar blockiert. Dann zeigt der WatchDog ein Fenster auf dem Benutzerbildschirm an:



Klickt man auf das Fenster, wird auf den Benutzer-Desktop umgeschaltet. Hier kann man jetzt die Fragen des HIPS beantworten.

Auf dem Benutzer-Desktop wird vom WatchDog ein Fenster eingeblendet:

Klickt man darauf, kann man mit SuRun weiter arbeiten.

Kommandozeilenoptionen und Tipps

SuRun ist ein Programm, dass seine Befehle per Kommandozeile entgegen nimmt. Man kann so z.B. über „Start > Ausführen“ (ohne Anführungszeichen Tippen:) „SuRun control“ <ENTER>. Die Systemsteuerung als Administrator starten.

Sinnvolle Kommandozeilenoptionen von SuRun sind

- /QUIET — Keine Meldungen ausgeben
- /RUNAS <Programm> — Programm als anderer Benutzer ausführen
- /RESTORE <Datei> — „SuRun Einstellungen“ aus <Datei> wiederherstellen <Datei> ist der volle Pfad plus Dateinamen!
- /SETUP — „SuRun Einstellungen“ starten
- /SWITCHTO <user> — Auf den Desktop von „user“ umschalten
- /SWITCHTO <sitzung> — Auf den Desktop der Logon-Sitzung [0,1,2...] umschalten
- /INSTALL — SuRun installieren
- /INSTALL <Datei> — SuRun installieren und „/RESTORE <Datei>“ ausführen <Datei> ist der volle Pfad plus Dateinamen!
- /UNINSTALL — SuRun deinstallieren

Wenn Sie also den Gruppenrichtlinien-Editor als echter Systemadministrator starten müssen, können Sie einfach „SuRun /RUNAS gpedit.msc“ eingeben, Benutzernamen und Kennwort des Systemadministrators eingeben und fertig.

Um unter Windows XP direkt Elemente der Systemsteuerung zu starten., können Sie z.B. folgende Kommandozeilen verwenden:

Automatische Updates:	„surun wuaucpl.cpl“
Computerverwaltung:	„surun compmgmt.msc“
Datum und Uhrzeit:	„surun timedate.cpl“
Netzwerkverbindungen:	„surun ncpa.cpl“
Sicherheitscenter:	„surun wscui.cpl“
Software:	„surun appwiz.cpl“
Systemeigenschaften:	„surun sysdm.cpl“

Einige Programme funktionieren leider nicht korrekt, wenn sie mit SuRun im Kontext des angemeldeten Benutzers mit gehobenen Rechten gestartet werden. Solche Programme müssen Sie leider im Kontext eines echten Systemadministrators (surun /runas ...) starten. Zu solchen Programmen zählen u.A. in Windows XP folgende Komponenten:

Benutzerkonten:	„surun /runas nusrmgr.cpl“

Gruppenrichtlinie:	„surun /runas gpedit.msc“
Lokale Sicherheitsrichtlinie:	„surun secpol.msc“
Windows Update:	„surun /runas wupdmgr.exe“

Lizenz, Garantie und Haftung

...gibt es nicht! Dieses Kapitel hilft hoffentlich, mir ökonomisch orientierte Rechtsverdreher vom Hals zu halten. SuRun hat mit Geld nichts zu tun!

Ich habe SuRun in der verfügbaren Zeit so gut ich konnte programmiert. Ziel war ursprünglich, selbst nicht mehr als Administrator zu arbeiten ohne die üblichen Unannehmlichkeiten in Kauf nehmen oder das System unsicherer machen zu müssen.

Das ist mir meiner Meinung nach gelungen.

Ich setze SuRun selbst auf all meinen PC ohne Probleme ein.

Sollte SuRun jedoch für Schäden irgendwelcher Art verantwortlich gemacht werden, übernehme ich dafür keine Haftung.

Schauen Sie in die Quelltexte bevor Sie SuRun installieren.

Nutzt Ihnen das nichts, und Sie sind sich nicht sicher, ob SuRun Ihnen schadet, benutzen Sie es einfach nicht!

Die Quelltexte sind wie die Software frei verfügbar. Jeder darf damit machen, was er will. Baut jemand SuRun oder Teile davon in sein eigenes Produkt ein und verschweigt die Herkunft, so ist das gestattet, wenn auch nicht erwünscht.