# SuRun (Super User Run)

Gebruikershandleiding

SuRun versie 1.2.0.0

# Inhoudsopgave

Wat is SuRun?	3
Waarom SuRun?	3
Hoe werkt SuRun?	4
Waarom niet de standaard Windows functionaliteit?	5
Installatie	7
Deïnstallatie	9
Configuratie	10
SuRun Instellingen "Algemene instellingen"	10
SuRun instellingen "SuRunners gebruikersgroep"	13
SuRun instellingen "Programma-uitvoering"	16
SuRun instellingen "Geavanceerd"	18
Gebruik	21
"SuRunner" worden	21
Programma's als Administrator starten	22
Automatisch en op verzoek	24
Het Windows context-menu	25
Integratie in het systeem-menu	
Informatie pop-up bij automatische starts	27
"Uitvoeren als" door SuRun	
De waakhond	28
Licentie, garantie en aansprakelijkheid	29

# Wat is SuRun?



SuRun is een gratis, Open Source programma dat het dagelijks gebruik van Windows 2000, XP, Server 2003 en Vista vereenvoudigd.

SuRun maakt het mogelijk programma's te starten met Administrator/Computerbeheerderrechten zonder daarbij wachtwoorden te hoeven invoeren, van gebruiker te wisselen, opnieuw aan te melden, of Windows registeren omgevingsvariabelen te veranderen.

SuRun werkt niet op systemen met Windows 95/98/ME.

SuRun werkt prima samen met Windows Vista's "User Account Control" (UAC).

# Waarom SuRun?

In Windows NT en zijn afgeleiden (2000, XP, 2003, Vista...) heeft Microsoft een systeem voor gebruikersrechten ingebouwd. Aan de hand van toegangscontrole-lijsten bepaalt Windows of en in welke mate toegang verleend wordt tot bestanden, programma's, apparaten of het register.

Standaard wordt elk Windows programma uitgevoerd met de rechten van het programma dat het gestart heeft. Zo erft bijvoorbeeld Notepad de rechten van de Windows Verkenner waarmee we een txt-bestand hebben geopend.

Ook kwaadaardige software ontleent zijn toegangsrechten aan het programma dat het heeft gestart. Zo erft een virus of trojan de rechten van Internet Explorer, die zijn rechten weer heeft verkregen van de Windows Verkenner, die op zijn beurt de rechten kreeg van de aangemelde gebruiker.

# Als men het dagelijks computerwerk als Administrator/Computerbeheerder uitvoert kan een virus de PC dus ongehinderd overnemen, zombie-netwerk software installeren of onklaar maken.

Door de geïntegreerde ondersteuning voor virtualisatie in de hedendaagse processoren is het zelfs mogelijk de gehele Windows-omgeving ongemerkt naar een virtuele omgeving te verbannen en vervolgens diepgaande wijzigingen in het systeem aanbrengen.

(Zie Joanna Rutkowska (http://InvisibleThings.org) met BluePill (http://bluepillproject.org/))

### Het is dus raadzaam het reguliere computerwerk als gebruiker met beperkte rechten te doen, zodat een virus in principe weinig kwaad kan aanrichten omdat het daarvoor, net als de aangemelde gebruiker, de rechten niet heeft.

In Windows is het zonder extra's niet eenvoudig met beperkte rechten te werken. Zelfs voor simpele taken als het bijstellen van de datum of tijd zijn al administrator-rechten nodig. Programma's mogen niet geïnstalleerd worden en hardware al helemaal niet.

SuRun maakt het mogelijk het dagelijks computerwerk met beperkte gebruikersrechten verrichten, door daar en wanneer het nodig is uw toegangsrechten te verhogen.

# Hoe werkt SuRun?

SuRun stelt een gebruiker in staat een programma naar believen met verhoogde rechten uit te voeren. Waar men in het verleden een "administrator"-taak binnen een beschermde omgeving moest uitvoeren, beschikt SuRun over eigen "Service" die programma's met administrator-rechten start binnen de context van de aangemelde gebruiker.

Hoe dit werkt is in onderstaand schema weergegeven:

Logon Session 0 "Goml Window Station "WinS Desktop "Default" Windows Explorer	bjuder\Oddo" ta0"
Window Station "Servi Desktop "Default" SuRun Dienst Unsich	ce-0x0-3e7\$" Zugriff nur "System" tbar! Zugriff nur "System"
Logon Session 1 "Gom Window Station "WinS Desktop "Default" Windows Explorer SuRun.exe "Notepad" Notepad.exe Marieschn als Admin	bjuder\Marieschn" ita0" Desktop " < UID > " SuRun.exe "NotePad als Admin?" OK Zugriff nur "System"

Op de computer zijn, dankzij Windows' snelle gebruikerswissel, twee gebruikers aangemeld. Oddo had de computer het eerst in gebruik voor een spel. Vervolgens tikte Marie hem op de schouders, omdat ze nog even snel een e-mail moest versturen. Dus liet Oddo haar m.b.v. [WIN] + "L" snel aanmelden om haar dat bericht te laten schrijven.

Marie wil haar PC-omgeving graag vrijhouden van virussen en andere kwalijke software, dus haar gebruikersrechten zijn zoals dat hoort "beperkt".

Omdat het een nieuwe veiligheidsupdate wil installeren en daarvoor administrator-rechten nodig heeft, weigert het e-mailprogramma van Marie echter dienst. Zij klikt nu met de rechtermuisknop op de bovenbalk van haar e-mailprogramma en selecteert de SuRun optie "Opnieuw starten als Administrator". Hiermee start SuRun het e-mailprogramma opnieuw, maar nu als Marie met Administrator-rechten.

Voor de SuRun service is het niet duidelijk of Marie of wellicht een virus de opdracht heeft gegeven. Daarom creëert het een beveiligde omgeving waarin alleen Windows Services mogen draaien. In deze beschermde omgeving wordt Marie nog een keer gevraagd of het inderdaad de bedoeling is het e-mailprogramma met verhoogde rechten uit te voeren.

🛠 Toestemming vereist
De opdracht:
"C:\Program Files\Revo Uninstaller\revouninstaller.exe"
wordt met verhoogde rechten uitgevoerd.
Moet dit programma met verhoogde rechten worden uitgevoerd? Zo niet, druk dan 'Annuleren'!
Gebruikersnaam: MAXDATA\Stephan Wachtwoord: ****** Deze vraag niet meer stellen voor dit programma Dit programma automatisch met verhoogde rechten uitvoeren.

Een virus kan in dit venster geen muisklik simuleren, maar voor Marie is het eenvoudig de "OK" knop te drukken waarna SuRun het e-mailprogramma daadwerkelijk opnieuw start met dezelfde rechten als van een Administrator/Computerbeheerder.

Na enkele ogenblikken heeft het e-mailprogramma zijn updates verwerkt, kan Marie snel haar e-mail afmaken en kan Oddo vervolgens weer verder met zijn game.

Iedereen gelukkig.

# Waarom niet de standaard Windows functionaliteit?

Maar de Windows Verkenner biedt toch "Uitvoeren als..."?

Deze standaard functionaliteit van Windows heeft echter twee wezenlijke bezwaren!

Het eerste en meest schadelijke bezwaar: kwalijke software kan u met behulp van "Uitvoeren als..." eenvoudig het Administrator-wachtwoord ontfutselen.

Dit is met AutoHotkey te demonstreren.

AutoHotkey is een programmaatje dat alle toetsaanslagen onderschept en opslaat in een LOG bestand, waaruit het paswoord eenvoudig valt af te lezen.

Ausführen als	Đ							
Welches Benu verwendet we	tzerkonto soll zum Ausführen dieses Programms rden?		H C:\Prog <u>F</u> ile <u>V</u> iew	ramme\ <u>H</u> elp	AutoH	otkey\AutoH	otkey	
	BRUNS (Kay)		49 017 49 017		d u	0.03 0.06	l l	[
schützen	aten vor nicht autonsierter Programmaktivität		4E 031 4E 031 50 019		d U d	0.11 0.09 0.16	N N P	
Mit dieser Optio den Computer o auch dazu führe	n konnen Computerviren davon abgehalten werden der persönliche Daten zu schädigen. Sie kann aber m, dass ein Programm nicht korrekt ausgeführt	1	50 019 41 01E		u d	0.08	Р А	
werden kann.	:		41 01E 43 02E		u d	0.11 0.03	A C	
<u>B</u> enutzername:	😰 SuperUser 💌 📰		43 02E 4B 025 4B 025		u d u	0.09 0.11 0.08	K K	
<u>K</u> ennwort:			45 012 45 012		d u	0.02 0.11	E E	
	Abbrechen		4E 031		d	0.05	N	

Met het Windows commando "*RunAs*" of het *MakeMeAdmin* Script gaat het al niet veel anders. Ook al werkt een eenvoudige keylogger hier niet, deze methoden kunnen nog steeds misbruikt worden om ongemerkt een Administrator-wachtwoord te bemachtigen.

Hoe dit gaat, demonstreert bijv. mijn demo "IAT-Hook".

Wanneer iemand, zelfs als Gast, deze demo uitvoert en nieuwe hardware aansluit of RunAs gebruikt en het wachtwoord van de Administrator/Computerbeheerder invoert, wordt het rode commandovenster geopend met een bijzonder onthullende tekst.



Waarom Microsoft dit deel van de beveiliging zo kort-door-de-bocht heeft uitgevoerd, is onduidelijk. Al in Windows NT 3.1 had dit aangepakt kunnen worden en tot aan Windows XP is hieraan niets verbeterd.

Het tweede probleem met het Windows commando "*Uitvoeren als*..." is dat het programma gestart wordt in een andere context als die van de aangemelde gebruiker.

Bijvoorbeeld:

Ik ben als beperkte-rechten-gebruiker "Oddo" aangemeld en wil SuperApp installeren.

Het setup-programma klaagt dat het niet voldoende rechten heeft om de installatie uit te voeren. Dus gebruikt "Oddo" het commando "*Uitvoeren als...*" om de software als Administrator "SubberUhser" te installeren.

SuperApp is een bijzonder duur programma dat maar door één gebruiker mag worden gebruikt en slaat de licentie en instellingen, waaronder de werk-directory

"C:\Documents and Settings\SubberUhser", op in de register-sleutel

HKEY\_CURRENT\_USER\Software\SuperApp.

Het stomme is dat precies dit soort essentiële parameters tijdens een installatie m.b.v. "Uitvoeren als..." naar de verkeerde plek verwijzen. Gebruiker "Oddo" heeft zijn bestanden en instellingen opgeslagen in "C:\Documents and Settings\Oddo", maar SuperApp slaat het licentiebestand op in "C:\Documents and Settings\SubberUhser".

Wanneer "Oddo" SuperApp gebruiken wil, krijgt hij een melding "Licentie niet gevonden", omdat "Oddo" de folder "*C:\Documents and Settings\SubberUhser*" niet kan lezen. Met de vermeldingen in het Windows register is het precies hetzelfde!

# Installatie

**BELANGRIJK!:** Behoud altijd een Administrator-account waarmee u zich kunt aanmelden voor het geval dat SuRun (of een ander programma) iets onverwachts doet!

Om SuRun te installeren pakt u de gedownloade installatie-ZIP uit in een folder en start u *"InstallSuRun.exe"*. Bent u tijdens de installatie niet aangemeld als Administrator dan vraagt SuRun u om het Administrator wachtwoord.

량 Toestemn	ning vereist		×		
	Administrator-re	chten zijn nodig om SuRi	un te installeren.		
$\mathbf{O}$	Voer de naam en het wachtwoord van de computerbeheerder in:				
	Kies 'Annuleren' ind	dien u niet zeker weet wat dit in	houdt!		
New York	Gebruikersnaam:	MAXDATA\Administrator	~		
ALEX	Wachtwoord:	*****			
			OK Annuleren		

**WAARSCHUWING:** Tijdens de installatie kan het wachtwoord niet in een beveiligde omgeving worden opgevraagd. Een password-sniffer die mogelijk al op uw systeem actief is, kan het wachtwoord dan onderscheppen!

U kunt SuRun het beste installeren door u op de computer aan te melden als Administrator/Computerbeheerder en de verbindingen met het (draadloos) netwerk te verbreken.

SuRun 1.2.0.0 - Installatie					
Wilt u SuRun installeren?					
☑ Na installatie 'SuRun instellingen' openen					
Het volgende veiligheidsbeleid moet worden ingesteld:					
Markeer 'Administrators' i.p.v. 'Maker' als eigenaar van Administrators-bestanden. WAARSCHUWING: Indien niet geactiveerd, kunnen gebruikers bestanden en registersleutels van SuRun Administrators wijzigen!!					
<u>Annuleren</u> Installeren >>					

Tijdens de installatie van SuRun worden twee keuze-opties geboden.

Het is van het grootste belang dat u het vinkje bij de optie "Markeer 'Administrators' i.p.v. 'Maker' als eigenaar van Administrators bestanden." laat staan!

Is SuRun al op de PC geïnstalleerd, dan zal "InstallSuRun.exe" voorstellen een update naar de nieuwere versie uit te voeren.



De instellingen van SuRun worden bij een update niet veranderd. Alleen de "Start als Administrator..."-koppelingen worden opnieuw aangemaakt. Wanneer u de optie "SuRun snelkoppelingen behouden zoals ze zijn" aanvinkt, worden ook deze niet aangepast.

Tijdens de installatie toont SuRun een voortgangslijst.



Om de installatie te voltooien, moet u zich van Windows afmelden en weer aanmelden.

# Deïnstallatie

SuRun kan op de reguliere wijze, met behulp van "Software" in het Configuratiescherm worden verwijderd.



Vinkt u de optie **"SuRun instellingen behouden"** aan, dan zal SuRun alle instellingen, net als de gebruikersgroep *"SuRunners"*, op de PC laten staan.

Gegevens die niet direct gewist kunnen worden, zullen bij de eerstvolgende systeemstart worden verwijderd.

# Configuratie

Met de commando-regel "surun /setup" of via "SuRun instellingen" in het Configuratiescherm wordt het SuRun Instellingenvenster in een beveiligde omgeving geopend.

# SuRun Instellingen "Algemene instellingen"

💕 SuRun 1.2.0.0 Inst	ellingen 🔀				
Algemene instellingen	SuRunners groep				
	Beveiligd Bureaublad				
	Scherm vervagen en Bureaublad in de achtergrond 'dimmen'				
	Bureaublad 'in- en uitvloeien'				
	Beveiliging				
	Gebruikerswachtwoord vragen 0 min. niet meer om wachtwoord vragen				
	Toon waarschuwing bij Administrators zonder wachtwoord				
	Systeem-Integratie:				
	Toon "Configuratiescherm als Administrator" in het Bureaublad context-menu				
	Toon "SuRun cmd' hier" in folder context-menu's				
	✓ Toon "SuRun Verkenner' hier" in folder context-menu's				
	V Toon "Opnieuw starten als Administrator" in programma systeem-menu's				
	Toon "Start als Administrator" in programma systeem-menu's				
-Standaard/geavance	eerd Backup				
Toon geavanceerde instellingen voor ervaren gebruiker Alle SuRun Instellingen					
Aanbevolen instellingen voor regulier gebruik Opslaan Laden					
	Toepassen OK Annuleren				

### **Beveiligd Bureaublad**

SuRun maakt veelvuldig gebruik van een zogenaamd "beveiligd Bureaublad". Hierbij wordt een nieuwe Bureaublad-omgeving opgeworpen waar alle communicatie (muiskliks, gebruikersgegevens) op een veilige, versleutelde wijze wordt afgehandeld. Wanneer SuRun een beveiligd Bureaublad heeft gecreëerd, is het reguliere bureaublad (en de rest van de PC) niet toegankelijk. Maar belangrijker is dat andere programma's geen toegang kunnen krijgen tot de gegevens die de gebruiker in de beveiligde omgeving met SuRun uitwisselt. Kwalijke software, zoals bijv. keyloggers, kunnen tijdens het beveiligd bureaublad dus geen wachtwoorden onderscheppen.

### Scherm vervagen en Bureaublad in de achtergrond 'dimmen'

Met deze optie wordt bij het overschakelen naar de beveiligde omgeving een 'foto' van het actieve Bureaublad gemaakt. Dit beeld wordt vervaagd en gedimd en vervolgens als achtergrond in de beveiligde omgeving geprojecteerd. De snelheid waarmee dit gebeurt is afhankelijk van de prestaties van uw PC, maar het ziet er wel fraai uit.

### Bureaublad 'in- en uitvloeien'

De achtergrond van het beveiligde Bureaublad wordt hierbij in- en uitgevloeid; een fade-in, fade-out effect. De snelheid waarmee dit gebeurt is in sterke mate afhankelijk van de prestaties van uw PC.

### Beveiliging

### Gebruikerswachtwoord vragen, X min. niet meer om wachtwoord vragen

Met deze optie geactiveerd, vraagt SuRun om een wachtwoord alvorens een programma met Administrator-rechten te starten. Door hier een waarde in te voeren bewaart SuRun het ingevoerde wachtwoord zodat een reeks acties ongehinderd kan worden uitgevoerd.

### Toon waarschuwing bij Administrators zonder wachtwoord

SuRun kan bij het aanmelden van een gebruiker testen of er op het systeem Administrator-accounts zijn die niet met een wachtwoord zijn beveiligd.

Bij de installatie van Windows wordt precies zo'n account "Administrator" zonder wachtwoord aangemaakt. Dit is een serieus veiligheidsrisico waarvoor SuRun een waarschuwing kan geven:

SuRun 🗙
😻 WAARSCHUWING: De volgende Administrator gebruikers hebben geen wachtwoord:
MAXDATA\Admin2
Dit is een groot veiligheidsrisico!

Deze waarschuwing verdwijnt niet vanzelf, maar moet handmatig gesloten worden. Standaard wordt deze waarschuwing getoond aan Administrators en niet de beperkte-rechten gebruikers. Met het naastgelegen pull-down menu kunt u aangeven of deze waarschuwing moet worden getoond aan "Alle gebruikers", "SuRunners en Administrators", "onbeperkte SuRunners en Administrators", "Administrators" of "Niemand".

### Systeem-integratie

SuRun kan zich in de Windows context- en systeem-menu's integreren.

Een context-menu verschijnt wanneer men met de rechtermuis-knop op een object klikt, of op de menu-toets op het toetsenbord drukt.

Pictogrammen schikken op 🔹 🕨 Vernieuwen
Plakken Snelkoppeling plakken
Grafische eigenschappen Grafische opties
Configuratiescherm als Administrator
Nieuw 🕨
Eigenschappen

Het systeem-menu verschijnt wanneer men met de rechtermuis-knop op titelbalk van een programma klikt of [ALT]+[Spatie] op het toetsenbord indrukt:

×	Sluiten	Alt+F4
	Opnieuw starten als Administrator	
	Maximaliseren	
-	Minimaliseren	
	Formaat wijzigen	
	Verplaatsen	
5	Vorig formaat	

### Toon "Configuratiescherm als Administrator" in het Bureaublad context-menu

Het commando Configuratiescherm als Administrator wordt aan het context-menu van het Bureaublad toegevoegd. Met dit commando wordt het Windows Configuratiescherm met verhoogde rechten geopend.

### Toon "'SuRun cmd' hier" in folder context-menu's

'SuRun cmd' hier wordt aan het context-menu van folders toegevoegd. Selecteert men dit commando dan wordt in deze folder-locatie een Commando-prompt met verhoogde rechten geopend.

### Toon "'SuRun Verkenner' hier" in folder context-menu's

'SuRun Verkenner' hier wordt aan het context-menu van folders toegevoegd. Kiest men dit commando, dan wordt de Windows Verkenner met verhoogde rechten gestart in de aangewezen folder-locatie.

### Toon "'Opnieuw starten als Administrator' in programma systeem-menu's

Opnieuw starten als Administrator wordt aan het systeem-menu van programma's toegevoegd. Selecteert men dit commando, dan vraagt SuRun of dit inderdaad gewenst is. Zo ja, dan sluit SuRun het lopende programma en start het weer opnieuw op met verhoogde rechten.

### Toon "'Start als Administrator' in programma systeem-menu's

Start als Administrator wordt aan het systeem-menu van programma's toegevoegd. Kiest men dit commando, dan vraagt SuRun of dit daadwerkelijk gewenst is. Zo ja, dan start SuRun het lopende programma opnieuw op met verhoogde rechten.

### Toon geavanceerde instellingen voor ervaren gebruikers

Met deze optie geselecteerd, worden de tabs "Programma uitvoering" en "Geavanceerd" in de SuRun Instellingen beschikbaar gesteld. Wie geen begrip heeft van de op deze pagina's gebruikte termen, doet er verstandig aan deze optie uit te schakelen.

### Standaard/geavanceerd

### Aanbevolen instellingen voor regulier gebruik

Met deze knop worden alle SuRun instellingen en opties voor alle "SuRunners" op waarden gezet die toereikend zijn voor normaal thuisgebruik. Mocht u een vermoeden hebben van problemen met SuRun, dan kunnen de aanbevolen instellingen met een simpele klik worden ingesteld. **Tip:** Maak een backup van de persoonlijke instellingen zodat je ze later weer eenvoudig kunt inlezen. Zie volgende punt.

Let op: Ook wanneer de tabs "**Programma uitvoering**" en "Geavanceerd" niet zichtbaar zijn, worden hun instellingen op standaardwaarden gezet. De Windows-opties op de tab "Geavanceerd" worden niet aangepast.

### Backup

### Backup opslaan...

Met deze functie worden alle SuRun instellingen en de persoonlijke opties van de "SuRunners" in een bestand opgeslagen.

Let op: Ook wanneer de tabs "Programma uitvoering" en "Geavanceerd" niet zichtbaar zijn, worden hun instellingen in een backup-bestand opgeslagen. De Windows-opties in de tab "Geavanceerd" worden niet opgeslagen.

### Backup laden...

Met deze functie worden alle SuRun instellingen en de persoonlijke opties van de "SuRunners" uit een bestand ingelezen.

Let op: Ook wanneer de tabs "Programma uitvoering" en "Geavanceerd" niet zichtbaar zijn, worden hun instellingen met de informatie uit het backup-bestand overschreven. De Windowsopties in de tab "Geavanceerd" worden niet aangepast.

### SuRun instellingen "SuRunners gebruikersgroep"

😻 SuRun 1	.2.0.0 Instellingen
Algemene in	stellingen SuRunners groep Programma uitvoering Geavanceerd
Algemene in Programm S # S # S # S # S # S # S # S # S # S #	stellingen       SuRunners groep       Programma uitvoering       Geavanceerd         SuRunner       MAXDATA\Stephan       Ioevoegen       Verwijderen         Image: Surger Surg
Programm	alijst Exporteren Importeren Toevoegen Bewerken Verwijderen Toepassen OK Annuleren

### SuRunner <Naam>, Toevoegen, Verwijderen

In de drop-down lijst staan alle leden van de lokale gebruikersgroep "SuRunners" vermeld. De specifieke opties van de geselecteerde gebruiker worden in hier weergegeven. Klikt u op "Toevoegen" dan verschijnt er een venster met een lijst:

Gebruiker toevoegen aan SuRunners groep	<
Selecteer een gebruiker die aan de groep 'SuRunners' moet worden MAXDATA\Administrator MAXDATA\Gast MAXDATA\Jasper MAXDATA\Rutger MAXDATA\SUPPORT_388945a0	
Toon gebruikers in het domein of voer een gebruikersnaam in als 'domein\gebruiker':	
MAXDATA\Jasper	]

Hier kunt u gebruikers-accounts die nog geen lid zijn aan de groep SuRunners toevoegen. Gebruikers-accounts met Administrator-rechten worden hierbij gedegradeerd tot normale gebruikers met beperkte rechten. Met "Verwijderen" kunt u de geselecteerde gebruiker uit de groep SuRunners wegnemen. SuRun zal hierbij voorstellen de 'verbannen' gebruiker Administrator-rechten te verlenen.

### Gebruiker kan SuRun instellingen wijzigen

Is deze optie niet aangevinkt, dan kan de geselecteerde gebruiker de SuRun Instellingen zien noch veranderen.

### Wachtwoord vereist voor SuRun instellingen

Met deze optie geactiveerd, vraagt SuRun om het gebruikerswachtwoord voordat het venster SuRun Instellingen geopend wordt. Het wachtwoord wordt alleen geverifieerd en direct weer vergeten.

### Alleen bepaalde programma's met SuRun starten

Programma's die niet in de lijst staan worden voor deze SuRunner niet met verhoogde rechten gestart.

### SuRun voor deze gebruiker verbergen

Is deze optie geactiveerd dan worden de instellingen "Gebruiker kan SuRun instellingen wijzigen" en "Status op taakbalk tonen" non-actief gemaakt en de instelling "Alleen bepaalde programma's met SuRun starten" geactiveerd. De gebruiker krijgt tevens geen meldingen van SuRun en alleen vooraf gespecificeerde programma's kunnen met verhoogde rechten worden gestart. Deze optie is met name interessant voor bedrijfsomgevingen of ouder-kind situaties wanneer bepaalde programma's Administrator-rechten nodig hebben, maar de gebruiker dit niet hoeft te weten.

#### Status op taakbalk tonen

SuRun kan rechts-onderin het systeemvak van de taakbalk een pictogram plaatsen dat aangeeft welke rechten het actieve venster heeft. Hiervoor worden vijf verschillende symbolen gebruikt:

- Het actieve venster heeft standaard-rechten, evenals de Windows Verkenner
- Het actieve venster is door SuRun met verhoogde rechten gestart
- Geen actief venster
- Het actieve venster en de Windows Verkenner draaien als Administrator
  - Het actieve venster draait als Administrator, de Windows Verkenner niet

Met deze optie kunt u voor iedere gebruiker apart vastleggen of het pictogram in de taakbalk wordt weergegeven of niet.

#### Status m.b.v. 'Balloon-Tips' tonen

Heeft het actieve venster een andere gebruiker dan degene die op het moment is aangemeld, dan kan SuRun dat door middel van een "Balloon-Tip" boven de taakbalk melden:



# Programmalijst voor de gebruiker, Exporteren, Importeren, Toevoegen, Bewerken, Verwijderen

In dit venster staan alle programma's die SuRun op een speciale manier behandeld. De betekenis van de symbolen in de lijst wordt duidelijk als men "Toevoegen" of "Bewerken" klikt:



De symbolen voor de automatische start zijn alleen zichtbaar wanneer de optie "**Probeer bepaalde programma's automatisch met verhoogde rechten te starten**" op de tab "**Geavanceerd**" van de SuRun Instellingen geactiveerd is. De betekenis van de knop is vanzelfsprekend. Om meerdere programma's in de lijst te wissen kunt u deze opde standaard-Windows wijze eenvoor-een met de [Ctrl] toets selecteren, of een bereik met de [Shift]-toets selecteren. De programmalijst vult zich vanzelf op basis van de opties "Deze vraag niet meer stellen voor dit programma" of "Dit programma automatisch met verhoogde rechten uitvoeren" in SuRun's bevestigings-dialoog.

Moet dit prograr uitgevoerd?	nma met verhoogde rechten worden
Zo niet, druk dan	'Annuleren'!
Gebruikersnaam:	MAXDATA\Stephan
Wachtwoord:	*****
🗌 Deze vraag	niet meer stellen voor dit programma
📃 Dit program	nma automatisch met verhoogde rechten uitvoeren.
	OK Annuleren

Met "Exporteren..." kunt u de programmalijst van de geselecteerde SuRunner opslaan. Met "Importeren" kan een eerder opgeslagen programmalijst weer worden ingelezen. Met de Export/Import-functie kunt u eenvoudig een standaard-programmalijst op alle gebruikers van toepassing maken. Andere instellingen van de SuRunner(s) worden bij deze import van de programmalijst niet aangepast. Reeds aanwezige vermeldingen in de programmalijst blijven bij een import behouden. Bij programma's die al in de programmalijst vermeld staan en zich ook in de import bevinden, blijven de instellingen onveranderd. Om voor een SuRunner de gehele programmalijst te vervangen voor een geïmporteerde lijst, moeten de programma's in de bestaande lijst eerst gewist worden.

# SuRun instellingen "Programma-uitvoering"



### Probeer programma's automatisch met verhoogde rechten te starten

SuRun kan proberen de start van programma's af te vangen en te controleren. Wanneer een programma (volgens Windows, of het programma zelf) met verhoogde rechten gestart moet worden, zal SuRun voorstellen het te starten met verhoogde rechten. Zo kunnen programma's ook zonder "SuRun <programma>" commando of "Start als Administrator" automatisch met verhoogde rechten worden gestart.

In Windows kunnen programma's op verscheidene manieren in het geheugen worden geladen en uitgevoerd.

De eerste methode is bijv. met behulp van de functie "CreateProcess". Deze heeft als belangrijkste nadeel dat ze alleen voor .EXE bestanden werkt.

De tweede methode is d.m.v. de functie "ShellExecute(Ex)". Deze kan bestanden en snelkoppelingen "uitvoeren", afdrukken en veel meer.

Zo start bijv. de Windows Verkenner *ShellExecute(Ex)* IrfanView wanneer ik op mijn systeem een JPG-bestand dubbelklik. Omdat dit zo goed functioneert, gebruiken bijna alle programma's ShellExecute wanneer ze iets uit te voeren hebben. In Windows 2000/2003/XP/Vista is het mogelijk op deze functie in te haken m.b.v. Een zogenamde COM-interface genaamd *"IShellExecuteHook"*. Als de optie **"Filter programma's die door Windows worden gestart"** geactiveerd is, past SuRun deze interface toe om op de hoogte gesteld te worden wanneer een programma *"ShellExecute(Ex)"* aanroept.

### Dit dekt helaas niet alles af.

Wanneer een programma niet "ShellExecute(Ex)", maar CreateProcess gebruikt, krijgt SuRun dat niet mee en kan het programma niet met verhoogde rechten starten. Ook wanneer een ander programma hoger in de lijst van "IshellExecuteHook"-programma's vermeld staat, zal SuRun in het ongewisse blijven. De Verkenner van Windows Vista start bijv. haast niets op met de functie

*"ShellExecute(Ex)"*. Dientengevolge zal de optie **"Filter programma's die door Windows worden gestart"** in een Vista omgeving weinig successvol zijn.

De tweede en meest gebruikte Windows functie om programma's te starten is "*CreateProcess*". Zelfs "*ShellExecute(Ex)*" gebruikt onderhuids meestal "*CreateProcess*" om een programma te starten.

Helaas biedt Windows officieel geen mogelijkheden om op "CreateProcess" in te haken.

Met de optie **"SuRun direct koppelen aan het starten van programma's."** gebruikt SuRun een inofficiële, maar vaak gebruikte methode om o.a. *"Createprocess"* af te vangen.

In Windows processen worden tabellen van functies die zich in DLL's bevinden bijgehouden. De betreffende DLL wordt in het geheugen van het proces geladen. Vervolgens worden de tabellen met de geïmporteerde functies op de geladen DLL afgestemd en alles loopt zoals het hoort. Er bestaan ook tabellen met de adressen van geïmporteerde DLL-functies, oftewel Import Address Tables (IAT).

Door de IAT van alle geladen modulen dusdanig aan te passen dat in plaats van *"CreateProcess"* een eigen functie aangeroepen wordt, kan je de controle overnemen op het starten van processen.

Maar ook dit heeft nadelen! Aangezien IAT-hooking niet officieel untdersteund wordt, kan het gebeuren dat het op een gegeven moment niet meer werkt. Tot nu toe gaat het in ieder geval prima, zelfs onder Windows Vista en Vista x64.

Het tweede nadeel: Wanneer bijv. een systeem-module zoals ncpa.cpl, gestart wordt, wordt "IShellExecuteHook" en niet "CreateProcess" door de Verkenner aangeroepen.

Daarom moeten beide opties actief zijn, opdat de start van zoveel mogelijk processen door SuRun gecontroleerd kan worden.

Wanneer een bepaald programma niet meer normaal functioneren, dan kan het in de "**Uitsluitingen...**" lijst worden opgenomen. In dat geval zal SuRun zich niet meer bemoeien met dat programma en zou het weer naar behoren functioneren.

### Probeer te ontdekken of onbekende programma's verhoogde rechten nodig hebben.

Met deze optie probeert SuRun uit te vinden of een programma dat niet in de lijst van bekende programma's voorkomt, Administrator-rechten nodig heeft. Zo ja, dan zal SuRun voorstellen het met verhoogde rechten te starten.

### Informatievenster tonen wanneer SuRun een programma met verhoogde rechten start

Met deze optie vertoont SuRun een venster met informatie over het programma dat zojuist met verhoogde rechten is gestart.



# SuRun instellingen "Geavanceerd"



### Toon gebruikersstatus voor actieve processen

SuRun kan in het systeemvak van de taakbalk een pictogram plaatsen dat aangeeft welke rechten het actieve venster bezit. Hiervoor worden vijf verschillende symbolen gebruikt:

- Het actieve venster heeft standaard-rechten, evenals de Windows Verkenner
  - Het actieve venster is door SuRun met verhoogde rechten gestart
- Geen actief venster
  - Het actieve venster en de Windows Verkenner draaien als Administrator
- **\*\*** 
  - Het actieve venster draait als Administrator, de Windows Verkenner niet

Door middel van deze optie kan worden bepaald voor welke gebruikers deze informatie getoond wordt ("Administrators", "alle gebruikers", "Niemand").

Standaard is het gebruikersstatus-pictogram uitgeschakeld. In de tab **"SuRunners-groep"** van de SuRun-Instellingen kan deze optie voor leden van de SuRunners-groep specifiek worden ingesteld.

### Toon Balloon-Tips voor programma's die niet door de huidige gebruiker gestart zijn

Behoort het actieve venster toe aan een andere gebruiker dan degene die op het moment is aangemeld, dan kan SuRun dit middels een "Balloon-Tip" boven de taakbalk weergeven:



### Administrators nooit vragen om aan de groep 'SuRunners' toegevoegd te worden

Met deze optie wordt Administrators niet gevraagd of ze lid willen worden van de groep SuRunners, wanneer ze in het context-menu de opdracht "Start als Administrator..." kiezen. (Het programma wordt dan op normale wijze gestart.)

### Niemand vragen of hij aan de groep 'SuRunners' toegevoegd moet worden

Wanneer iemand die geen lid is van de groep SuRunners, SuRun wil gebruiken, wordt er een foutmelding gegeven en de gebruiker wordt niet (automatisch) in de groep SuRunners opgenomen.

### SuRun verbergen voor alle gebruikers die geen lid zijn van de groep 'SuRunners'

Met deze optie geactiveerd, krijgen gebruikers die geen lid van de groep SuRunners zijn, geen meldingen van SuRun en kunnen ook geen programma's (door SuRun) met verhoogde rechten (laten) starten.

Met de instellingen in het kader "Vereenvoudigde bediening" kunnen enkele Windowsonhebbelijkheden, die eigenlijk niets met SuRun te maken hebben, aangepast worden.

### Vervang Windows 'Uitvoeren als...' voor SuRun's 'Uitvoeren als...'

Het gebruik van Windows ingebouwde "Uitvoeren als..." is onveilig! Zelfs programma's met Gastrechten kunnen bij "Uitvoeren als..." ingevoerde wachtwoorden onderscheppen en vervolgens het systeem overnemen.

SuRun kan het commando "Uitvoeren als..." van de context-menu's vervangen:

💕 Uitvoerer	1 als	$\mathbf{X}$
	Voer uw gebruik	ersnaam en wachtwoord in om de opdracht:
	"C:\Program File	s\Notepad2\Notepad2.exe"
	uit te voeren.	
. Aller	Gebruikersnaam:	MAXDATA\Administrator
- BRE	Wachtwoord:	*****
A. Maria		wachtwoord onthouden
		OK Annuleren

Het grote voordeel is dat het gebruikerswachtwoord in een beveiligde omgeving wordt opgevraagd en niet onderschept kan worden. Het gebruikerswachtwoord kan worden opgeslagen. Het wordt met versleuteling opgeslagen in het Windows register onder

"HKEY\_LOCAL\_MACHINE\SECURITY\SuRun\RunAs\<username>\Cache".

### 'SuRunners' mogen de systeemtijd aanpassen

Gebruikers met beperkte rechten mogen onders Windows NT de klok niet aanpassen. Dit is vanzelfsprekend belangrijk wanneer een computer deel is van een server-netwerk, maar ook voor thuisgebruik uit veiligheidsoverwegingen aan te bevelen. Wanneer het u evenwel stoort dat u niet zomaar de systeemtijd kunt aanpassen, dan kunt u deze optie activeren. Met deze optie krijgen de leden van de groep SuRunners het privilege "SeSystemtimePrivilege" en kunnen (na af- en weer opnieuw aanmelden) de systeemtijd aanpassen.

### 'SuRunners' mogen instellingen van Energiebeheer en Energieschemas aanpassen

Gebruikers met beperkte rechten mogen standaard niet met een klik op het accu-symbool op de taakbalk het toe te passen energieschema instellen. Dit is het gevolg van het feit dat beperkterechten gebruikers geen toegang hebben tot de energie-instellingen in het Windows register (HKLM\ Software\Microsoft\Windows\CurrentVersion\ControlsFolder\PowerCfg).

Met deze optie krijgen de SuRunners volledig toegang tot dit deel van het Windows register en de Energiebeheer-opties. Bij het deactiveren van deze optie wordt leden van de groep SuRunners deze toegangsrechten weer ontnomen.

### Windows Update berichten aan alle gebruikers doorgeven

Standaard worden beperkte-rechten gebruikers niet geïnformeerd over beschikbare Windows updates. In Windows XP Professional kan dit met de Lokale beveiligingsinstellingen aangepast worden, maar Windows XP Home biedt deze mogelijkheid niet. Met deze optie worden de Windows Updates Balloon-Tips voor alle gebruikers zichtbaar gemaakt.

### Niet automatisch opnieuw starten na installatie van Windows Updates

Wanneer Automatische Updates in Windows geactiveerd is en een gebruiker met beperkte rechten is aangemeld, dan worden Windows Updates automatisch geïnstalleerd en wordt de computer automatisch opnieuw gestart. Dit gebeurt ongeacht nog lopende programma's en nog niet opgeslagen bestanden. Ook dit is in Windows XP Home niet zomaar aan te passen. Met deze optie krijgt u de keuze of u de PC na het downloaden van de update direct of later opnieuw wilt starten.

### Markeer 'Administrators' i.p.v. 'Maker' als eigenaar van Administrators-bestanden.

Onder normale omstandigheden is de maker van een object, zoals bijv. een bestand, een folder of een register-sleutel, ook de "eigenaar". Eigenaars van objecten krijgen uiteraard volledig toegang tot deze objecten. Wanneer bijv. een met SuRun gestart en met Administrator-rechten lopend proces een register-sleutel onder HKEY\_LOCAL\_MACHINE aanmaakt, dan kan de beperkte-rechtengebruiker die SuRun gebruikte, deze registersleutel ten alle tijden aanpassen. Hetzelfde geldt met bestanden.

Met deze optie worden objecten die onder Administrator-rechten worden aangemaakt, toegekend aan de gebruikersgroep "Administrators" en niet de gebruiker wiens rechten zojuist even zijn verhoogd. Dit voorkomt dat deze objecten later door dezelfde gebruiker, maar dan niet met verhoogde-rechten, aangepast kunnen worden.

### LET OP: Deze optie moet ten alle tijden geactiveerd blijven!

# Gebruik

### "SuRunner" worden

Bent u geen lid van de gebruikersgroep "SuRunners" en u probeert een programma m.b.v. SuRun als Administrator te starten of de "SuRun Instellingen" vanuit het configuratiemenu te openen, dan biedt SuRun u aan u bij de groep aan te sluiten.

Bent u geen Administrator, dan moet deze actie met de invoer van een Administrator-wachtwoord bevestigd worden, waarna u aan de gebruikersgroep **"SuRunners"** wordt toegevoegd.

량 Benut	zerdaten ei	forderlich 🛛 🔀
	Um SuRun z	u benutzen, müssen Sie Mitglied der Benutzergruppe "SuRunners" sein.
V	Identifizieren	Sie sich als Administrator, um Mitglied von "SuRunners" zu werden.
	Ansonsten d	rücken Sie "Abbruch".
	Bitte wähler	i Sie Abbrechen, wenn Sie sich unsicher sind!
	Benutzer:	VMXPPRO\SuperUser
80-	Kennwort:	*****
		OK Abbrechen

(Het wachtwoord wordt in een beveiligde omgeving opgevraagd en gecontroleerd opdat het niet onrechtmatig kan worden onderschept.)

Bent u wel een gebruiker met Administrator-rechten, dan zal SuRun bij eerste gebruik de vraag stellen of u lid van de gebruikersgroep "**SuRunners**" wilt worden en geschrapt kan worden als lid van de groep "**Administrators**".

SuRun	(VMXPPRO\Kay)
?	Um SuRun zu benutzen, müssen Sie Mitglied der Benutzergruppe "SuRunners" sein. Wollen Sie Mitglied der "SuRunners" Gruppe und aus der Administratoren Gruppe ausgetragen werden? Wenn Sie Ja wählen, werden Sie KEIN ADMINISTRATOR, sondern SuRunner. Wenn Sie unsicher sind, was das hier ist, klicken Sie auf "NEIN"! Ja Nein

U moet hierna van Windows afmelden en weer aanmelden om deze actie te voltooien.

Is in de SuRun instellingen "Niemand vragen of hij aan de groep 'SuRunners' toegevoegd moet worden" of "Administrators nooit vragen om aan de groep 'SuRunners' toegevoegd te worden" geactiveerd, dan zal SuRun uiteraard niets voorstellen.

SuRun	(VMXPPRO\Nikki)	
٩	Sie sind erfolgreich als Mitglied in die Gruppe "SuRunners" aufgenommer	n worden.
	ОК	
SuRun	(VMXPPRO\Kay) 🛛 🔀	
(į)	Sie sind erfolgreich in die Gruppe "SuRunners" aufgenommen und aus der Administratoren-Gruppe ausgetragen worden.	
	Sie müssen sich jetzt ab und wieder anmelden, um mit eingeschränkten Rechten zu arbeiten.	
	ОК	

Nu bent u SuRunner en kunt u comfortabel als beperkte-rechten account werken.

### Programma's als Administrator starten

Wanneer u een programma met verhoogde rechten starten wil, klikt u het met de rechtermuisknop en kiest u eenvoudig "Start als Administrator" in het context-menu.

TaskSwitchXF	Openen	
	Uitvoeren als	
m TreeSize	Start als Administrator	
🛗 WD Diagnosti	tics 7-Zip	•
🚔 Ulia Cuntania	Scan rstrui.exe	
wincustomize	e Aan het menu Start vastmaken	
🌷 Beveiligingsca	entrum Kopiëren naar	•
🙆 Geplande tak	ken Knippen	
💫 Hulp op afsta	and Kopiëren	
📇 JkDefrag	Snelkoppeling maken	
🚯 Schijfdefragn	mentatie Verwijderen	
💰 Schijfopruimir		
🐻 Software	Sorteren op naam Eigenschannen	
3 Systeemhers	stel	
🤨 Systeeminfo		

SuRun heeft geen wachtwoord nodig om een programma met verhoogde rechten te starten. Is echter de optie **"Gebruikerswachtwoord vragen"** geactiveerd, dan vraagt SuRun naar het wachtwoord van de aangemelde gebruiker.

😽 Wachtw	oord vereist 🛛 🔀
De opdr	acht:
"C:\Prog	gram Files\Notepad2\Notepad2.exe''
wordt m	et verhoogde rechten uitgevoerd.
1	Moet dit programma met verhoogde rechten worden uitgevoerd? Zo niet, druk dan 'Annuleren'!
	Gebruikersnaam: MAXDATA\Stephan Wachtwoord: ******* Deze vraag niet meer stellen voor dit programma Dit programma automatisch met verhoogde rechten uitvoeren. OK Annuleren

Dit wachtwoord wordt gecontroleerd en direct gewist. Het wordt nergens opgeslagen waar het weer zou kunnen worden opgevraagd of op andere wijze ontfutseld.

Is de optie "Gebruikerswachtwoord vragen" niet geactiveerd, dan vraagt SuRun alleen maar om een eenvoudige bevestiging:

### Gebruik



### Automatisch en op verzoek

Wanneer u "**Deze vraag niet meer stellen voor dit programma**" aanvinkt, dan zal SuRun het gekozen antwoord (OK, Annuleren) onthouden en toepassen bij de volgende keren dat dit programma wordt aangeroepen. Deze optie komt goed van pas bij Windows-Autostart programma's die Administrator-rechten nodig hebben.

Het is ook mogelijk dat SuRun ten onrechte een programma met verhoogde rechten wil starten. Bijv. het fictieve programma "PlinseTupper.exe" bevat het woord "setUp", op basis waarvan SuRun meent dat het mogelijk wel Administrator-rechten nodig heeft. In zo'n geval vinkt u de optie "**Deze vraag niet meer stellen voor dit programma**" aan en vervolgens "**Annuleren**" en u bent voor altijd van het gezeur af.

Met een vinkje bij **"Dit programma automatisch met verhoogde rechten uitvoeren."** zal SuRun proberen het programma ook zonder **"Start als Administrator"** altijd met verhoogde rechten te starten.

Wanneer een programma verhoogde rechten nodig lijkt te hebben, zal SuRun vragen of het daarmee gestart moet worden. Of een programma met verhoogde rechten gestart moet worden herkent SuRun zo:

- Het programma staat als **"altijd met verhoogde rechten starten"** in de gebruiker's programmalijst
- De optie "Probeer te ontdekken of onbekende programma's verhoogde rechten nodig hebben." is geactiveerd en
  - Het programma heeft als extensie exe, cmd, lnk, com, pif, bat en de bestandsnaam bevat een van de woorden "install", "setup" of "update"
  - Het programma bevat een interne of externe kenmerk (Manifest Resource of een externe Manifest bestand dat <\*trustInfo>-> <\*security>-> <\*requestedPrivileges>-> <\*requestedExecutionLevel level= "requireAdministrator"> bevat)

Wanneer een programma gestart moet worden en een van de condities is vervuld, dan zal SuRun de volgende vraag stellen:

🚏 Toestemming vereist	
De opdracht:	
C:\WINDOWS\system32\rundll.exe C:\system32\shell32.DLL, Control_RunDLL "C:\WINDOWS\system32\firewall.cpl",Windows Firewall wordt met verhoogde rechten uitgevoerd	
Moet dit programma met verhoogde rechten worden uitgevoerd? Zo niet, druk dan 'Annuleren'!	
Gebruikersnaam: MAXDATA\Stephan Wachtwoord: ****** Deze vraag niet meer stellen voor dit programma Dit programma automatisch met verhoogde rechten uitvoeren.	OK Annuleren

### Het Windows context-menu

Om programma's eenvoudig te kunnen opstarten, heeft SuRun zich geïntegreerd in het contextmenu van de Windows Verkenner.

Voor bestanden met de extensie bat, cmd, cpl, exe, lnk en msi voegt het de opdracht "Start als Administrator" aan het context-menu toe.

Openen
Uitvoeren als
Start als Administrator
7-Zip
Aan het menu Start vastmaken
Kopiëren naar 🕨
Knippen
Kopiëren
Snelkoppeling maken
Verwijderen
Naam wijzigen
Sorteren op naam
Eigenschappen

In het context-menu voor de Bureaublad-achtergrond voegt SuRun de opdracht "configuratiescherm als Administrator" toe.

Pictogrammen schikken op Vernieuwen	×
Plakken Snelkoppeling plakken	
Grafische eigenschappen Grafische opties	•
Configuratiescherm als Administrator	΄ Ν
Nieuw	1
Eigenschappen	

### Integratie in het systeem-menu

Veel programma's behoeven Administrator-rechten bijv. bij installatie, vertellen u dit pas wanneer zij afsluiten. Om dit soort programma's comfortabel te gebruiken heeft SuRun zichzelf ook geïntegreerd in het Windows systeem-menu:



Met een klik van de rechtermuisknop op titelbalk van een venster, kunt u zo'n probleem-programma eenvoudig **"Opnieuw starten als Administrator"** of **"Starten als Administrator"**.

😵 Toestemming vereist	×
De opdracht:	
C:\WINDOWS\system32\rundll.exe C:\system32\shell32.DLL, Control_RunDLL "C:\WINDOWS\system32\firewall.cpl",Windows Firewall wordt met verhoogde rechten uitgevoerd	
Moet dit programma met verhoogde rechten worden uitgevoerd? Zo niet, druk dan 'Annuleren'!	
Gebruikersnaam: MAXDATA\Stephan Wachtwoord: ****** Deze vraag niet meer stellen voor dit programma Dit programma automatisch met verhoogde rechten uitvoeren.	
	uleren

Wanneer in het bovenstaande voorbeeld (Dubbelklik op de klok in het systeemvak van de taakbalk) beide opties aangevinkt zijn en "OK" gedrukt, dan wordt **"Windows Firewall"** de volgende keren als Administrator gestart.

Dat	tum (	und L	Ihrze	it ;	Zeitzo	one	Internetze	it it is a second s
é E	Datur	n —					C	Uhrzeit
	Mär:	2			2008	3		a sector and the sector of the
	Million			-				
	М	D	М	D	F	S	S	
						1	2	
	3	4	5	6	7	8	9	
	10	11	12	13	14	15	16	
	17	18	19	20	21	22	23	
	24	25	26	27	28	29	30	
	31							20:28:37
Ak	tuelle	e Zeit	zone	e: Wi	esteu	iropä	ische Norma	alzeit
						1	OK	Abbrechen Übernehmen
							-	
ur	1							
In	fo							
	10.			-				ava /d C\\\//NDO\\//S\austam2?\aball?? dll Cantral, DupDLL timadata

### Informatie pop-up bij automatische starts

Wanneer een programma door SuRun met verhoogde rechten gestart wordt, kan het voor 20 seconden een informatievenster boven het systeemvak van de taakbalk tonen.

### Waarschuwing bij Administrators zonder wachtwoord

Bij de installatie van Windows wordt automatisch een voorgedefinieerd Administrator-account zonder wachtwoord aangemaakt. Dit is een aanzienlijk veiligheidsrisico!

SuRun kan bij de aanmelding van gebruikers controleren of er op het systeem lokale gebruikers bestaan die Administrator-rechten hebben en niet met een wachtwoord zijn beveiligd. In dat geval wordt de volgende mededeling getoond:



Deze waarschuwing verdwijnt niet vanzelf, maar moet handmatig gesloten worden. Standaard worden Administrators en niet-beperkte leden van de gebruikersgroep "SuRunners" op deze wijze gewaarschuwd, maar deze melding is ook weer te geven voor "Alle gebruikers", "SuRunners en Administrators", "Onbeperkte gebruikers en Administrators", "Administrators" en "Niemand".

### Taakbalk-pictogram

SuRun kan rechts-onderin het systeemvak van de taakbalk een pictogram plaatsen dat aangeeft welke rechten het actieve venster heeft. Hiervoor worden vijf verschillende symbolen gebruikt:



Het actieve venster heeft standaard-rechten, evenals de Windows Verkenner

Het actieve venster is door SuRun met verhoogde rechten gestart

Geen actief venster

<del>...</del>

?

Het actieve venster en de Windows Verkenner draaien als Administrator

Het actieve venster draait als Administrator, de Windows Verkenner niet

Behoort het actieve venster toe aan een andere gebruiker dan degene die op het moment is aangemeld, dan kan SuRun dit middels een "Balloon-Tip" boven de taakbalk weergeven:



In de tab "SuRunners-groep" van de SuRun-Instellingen kan de weergave van het taakbalkpictogram en de Balloon-Tips voor leden van de SuRunners-groep specifiek worden ingesteld.

# "Uitvoeren als..." door SuRun

Het gebruik van Windows ingebouwde "Uitvoeren als..." is onveilig! Zelfs programma's met Gastrechten kunnen bij "Uitvoeren als..." ingevoerde wachtwoorden onderscheppen en vervolgens het systeem overnemen.

SuRun kan het commando "Uitvoeren als..." van de context-menu's vervangen:

💱 Uitvoeren als 🔀	
۲	Voer uw gebruikersnaam en wachtwoord in om de opdracht:
	"C:\Program Files\Notepad2\Notepad2.exe"
	uit te voeren.
*	Gebruikersnaam: MAXDATA\Administrator  Wachtwoord: ******  Wachtwoord onthouden  K Annuleren

Het grote voordeel is dat het gebruikerswachtwoord in een beveiligde omgeving wordt opgevraagd en niet onderschept kan worden.

Het gebruikerswachtwoord kan voor iedere gebruiker van "Uitvoeren als..." worden opgeslagen. Het wordt met versleuteling opgeslagen in een deel van het Windows register onder "HKEY\_LOCAL\_MACHINE\SECURITY\SuRun\RunAs\<username>\Cache" dat alleen toegankelijk is voor Services. De wachtwoorden van alle gebruikers worden **gescheiden en met** versleuteling opgeslagen om te voorkomen dat een gebruiker eenvoudig het wachtwoord van een andere gebruiker kan achterhalen.

### De waakhond

Wanneer een systeem is voorzien van een zgn. Host Intrusion Protection System (HIPS), die het gedrag van programma's analyseert en de gebruiker waarschuwt voor evt. gevaren, kan dit tot problemen leiden met SuRun. Als de HIPS bijv. de gebruiker probeert te waarschuwen ontstaat er een PAT-stelling, omdat SuRun al een beveiligde Bureaublad-omgeving heeft gecreëerd.

- SuRun wordt door de HIPS geblokkeerd en kan niet verder werken
- De HIPS kan geen meldingen geven of invoer verwerken, omdat SuRun's beveiligde Bureaublad-omgeving actief is

Vanaf versie 1.1.0.6 is SuRun voorzien van een "WatchDog" die hierin moet voorzien. Wanneer SuRun langer dan twee seconden zichzelf niet kan voorzien van een levensteken, dan wordt het waarschijnlijk (door een HIPS) geblokkeerd. In dat geval grijpt de WatchDog in met de volgende melding op het scherm:



Met een muisklik op het venster wordt overgeschakeld naar de normale (onbeveiligde) Bureaubladomgeving. Hier kan men de vragen van de HIPS beantwoorden.

Op de Bureaublad-omgeving wordt door de Watchdog een venster geopend:



Met een muisklik in dit venster kan men weer terugkeren naar de SuRun beveiligde omgeving en verder werken.

# Licentie, garantie en aansprakelijkheid

... is er niet! Deze paragraaf draagt er hopelijk toe bij duidelijk te maken dat SuRun niets met geld te maken heeft!

Ik heb SuRun zo goed mogelijk geprogrammeerd in mijn vrije tijd. Mijn oorspronkelijk doel was zelf niet meer als Administrator te hoeven werken zonder de bijkomende onhebbelijkheden op de koop te hoeven nemen, of de beveiliging van mijn PC te reduceren.

Ik ben van mening dat dit gelukt is en ik gebruik SuRun zelf zonder problemen op al mijn PC's.

Mocht er door toedoen van SuRun toch bepaalde schade ontstaan, verschoon ik mij van alle mogelijke aansprakelijkheid. Het gebruik van SuRun is op eigen risico.

De gehele broncode van SuRun is beschikbaar en kan voor het in gebruik nemen van het programma worden geïnspecteerd. Indien u dan nog twijfels hebt over de evt. schade die SuRun zou kunnen aanrichten, dan ben u vrij het niet te installeren!

De broncode tezamen met het programma vrij beschikbaar. Iedereen mag ermee doen wat hij/zij wil. Indien SuRun of delen daarvan in een eigen product worden opgenomen, dan is men verplicht duidelijke vermelding te maken van de herkomst van de code.

Kay Bruns