

# AdminsRobot 4.0

## Installationsanleitung



DIESE DOKUMENTATION UND DAS ZUGEHÖRIGE COMPUTER-SOFTWAREPROGRAMM SIND IM RAHMEN DES URHEBERRECHTS INTERNATIONAL GESCHÜTZT. DIE DOKUMENTATION UND DAS ZUGEHÖRIGE COMPUTER-SOFTWAREPROGRAMM UNTERLIEGEN RECHTLICH DEN JEWEILS GÜLTIGEN LIZENZVERTRÄGEN DES ENDBENUTZERS (s. EULA.TXT).

© 2017 Lugin Software GmbH. Alle genannten Unternehmens- und Markennamen sowie Dienstmarken sind das Eigentum der jeweiligen Unternehmen. Alle Rechte vorbehalten.

Windows ist ein eingetragenes Warenzeichen der Microsoft Corporation.

## Installationsanleitung

### Inhalt

Funktionsweise .....	3
Systemvoraussetzungen .....	3
Installation.....	3
AdminsRobot-Freigabe ArShare\$.....	4
Silent Installation / Installation per Softwareverteilung .....	5
Bereitstellen der globalen Objekte .....	5
PCs aus DHCP-Server extrahieren .....	5
GlobalObjects.txt mit Benutzerinformationen erzeugen .....	6
Erstellen einer Textdatei bei jeder Anmeldung eines Benutzers.....	6
Als Administrator ausführen .....	7
Dienste und Ports .....	8
PowerShell-Skripte .....	8

## Funktionsweise

AdminsRobot ist eine grafische Oberfläche, die es Ihnen ermöglicht, Kommandozeilenbefehle und Skripte auf einem oder mehreren entfernten Windows-Rechnern gleichzeitig und automatisiert auszuführen. AdminsRobot enthält im Lieferumfang bereits viele häufig verwendete und weniger bekannte Kommandozeilenbefehle und nützliche Skripte für Administratoren. AdminsRobot ist erweiterbar – eigene Aktionen und Skripte können in Batchprogrammierung, VBS oder PowerShell erstellt und problemlos weitergegeben werden. Alle Aktionen können zeitgesteuert ausgeführt werden, um beispielsweise nachts eine Reihe von Rechnern aufzuwecken, bestimmte Aktionen durchzuführen und dann wieder schlafen zu legen.

### Zusätzliche Tools, die benötigt werden

Um den vollen Funktionsumfang der Software nutzen zu können, werden die kostenlosen Microsoft Kommandozeilen-Tools psexec.exe (Download-Link: <http://technet.microsoft.com/en-us/sysinternals/bb897553>) und pslist.exe (Download-Link: <http://technet.microsoft.com/en-us/sysinternals/bb896682.aspx>) benötigt.

Beide Dateien befinden sich in den Sysinternals PsTools. Sie müssen nicht installiert, sondern nur in das AdminsRobot-Verzeichnis kopiert werden (C:\Program Files\AdminsRobot oder C:\Program Files (x86)\AdminsRobot).

## Systemvoraussetzungen

AdminsRobot benötigt keinen Server, keine Datenbank und keine Agenten auf den Clients. Installieren Sie die Software einfach auf Ihrem Arbeitsplatzrechner.

Folgende Systemvoraussetzungen sind notwendig:

- Windows Vista, Windows 7, Windows 8, Windows 8.1 oder Windows 10 (jeweils 32 oder 64 Bit-Version)
- .NET-Framework 4 oder höher

## Installation

1. Starten Sie die Datei AdminsRobot.msi mit Administrator-Rechten. Während der Installation werden der AdminsRobot-Zielpfad, der Lizenzschlüssel und der UNC-Pfad zu den globalen Objekten abgefragt.

**Zielpfad** (notwendig): Der Pfad, in dem AdminsRobot installiert werden soll.

**Lizenzschlüssel** (notwendig): ein Lizenzschlüssel für die kostenlose 50-PC-Lizenz ist während der Installation bereits eingeblendet.

**UNC-Pfad zu den globalen Objekten** (optional): Der Pfad, in dem sich die Textdatei mit den globalen Objekten befindet. Dabei handelt es sich um eine Datei, die die Namen von Objekten wie Workstations, Server, Drucker und Netzwerkkomponenten und deren Mac- und IP-Adressen enthält. Lesen Sie in dieser Anleitung oder unter [www.AdminsRobot.de](http://www.AdminsRobot.de) → „Datenbasis erzeugen“ (aktueller), wie sie diese Datei erzeugen. Dieses Feld kann leer gelassen und später eingetragen werden.

2. Kopieren Sie die Dateien psexec.exe und pslist.exe ins AdminsRobot-Verzeichnis (normalerweise C:\Program Files\AdminsRobot bzw. C:\Program Files (x86)\AdminsRobot).

Die Dateien können kostenlos von <http://technet.microsoft.com/en-us/sysinternals/bb897553> heruntergeladen werden. Sie befinden sich in den **Sysinternals PsTools**.

## Erster Start der Software

1. Starten Sie AdminsRobot mit administrativen Rechten. Klicken Sie dazu mit rechter Maustaste im Startmenü → Alle Programme → AdminsRobot auf das AdminsRobot-Icon und wählen Sie „Als Administrator ausführen“. Geben Sie Zugangsdaten an, mit denen Sie lokale Administratorenrechte auf Ihrem Computer haben.  
Um alle Aktionen verwenden zu können, benötigen Sie einen Account, der auch auf den entfernten zu administrierenden Computern Administratorrechte besitzt.
2. Es erscheint ein Hinweis, dass die Ersteinrichtung durchgeführt wird. Dabei werden die Benutzer bezogenen Dateien unter %APPDATA%\AdminsRobot abgelegt. Bestätigen Sie den Hinweis mit OK.
3. Im Objekte-Bereich befindet sich zu diesem Zeitpunkt zumindest ein Objekt: Localhost. Markieren Sie das Objekt und fügen Sie es mit der rechten Maustaste oder dem „Pfeil nach rechts“-Button der Auswahl hinzu.
4. Klicken Sie im Aktionen-Bereich mit der rechten Maustaste auf die Aktion „Ping“ und wählen Sie „Anwenden auf markierte Objekte“. Daraufhin öffnet sich ein Fenster, in dem der Ping-Befehl ausgeführt wird.

Um Ihrer neuen AdminsRobot-Installation weitere Objekte hinzuzufügen, klicken Sie bitte auf **Bearbeiten → Objekte discovern** oder auf **Datei → Neues Objekt**.

Lesen Sie im Abschnitt „Bereitstellen der globalen Objekte“, wie Sie den Objekte-Bereich mit Ihren Client-Computern füllen und dauerhaft aktuell halten.

Während der Installation werden zusätzlich ein Geplanter Task und eine Freigabe auf Ihrem Computer eingerichtet. Um die Installation des Geplanten Tasks abzuschließen, gehen Sie bitte folgendermaßen vor: Öffnen Sie die Computerverwaltung → Aufgabenplanung → Aufgabenplanungsbibliothek. Tragen Sie in der Aufgabe „AdminsRobot“ unter Allgemein → Sicherheitsoptionen einen Benutzer ein, der Administrator-Rechte auf den Rechnern besitzt, die Sie mit AdminsRobot administrieren möchten. Der Geplante Task ist nur für die zeitgesteuerte Ausführung von Aktionen notwendig und kann auch später noch konfiguriert werden.

Die Installation des Geplanten Tasks lässt sich über die Silent Installation (s.u.) vermeiden. Dadurch ist die zeitgesteuerte Ausführung von Aktionen nicht möglich.

## AdminsRobot-Freigabe ArShare\$

Die AdminsRobot-Freigabe ArShare\$ ist notwendig, um bestimmte Aktionen durchführen zu können. Immer dann, wenn eine Aktion auf einem Client ausgeführt wird (mit Psexec oder WinRM) und auf eine Batch-, VBS- oder PowerShell-Datei zugegriffen werden muss oder Ergebnisse zurück geschrieben werden, wird auf die Freigabe \\IhrComputer\ArShare\$ zugegriffen. Da das Psexec-Kommando unter dem System-Account läuft, benötigt die ArShare-Freigabe Schreibrechte für "Jeder" (Everyone). Für Aktionen, die ausschließlich auf Ihrem Rechner stattfinden (z.B. Ping, Computerverwaltung, Remotedesktopverbindung) und nur über das Netzwerk auf andere Rechner zugreifen, wird die Freigabe nicht benötigt.

Wenngleich es sich dabei um eine versteckte Freigabe handelt, könnte ein Angreifer, der die Existenz der Freigabe kennt, auf Ergebnisdateien zugreifen, die von AdminsRobot erzeugt wurden. Auf Batch-, VBS- oder PowerShell-Dateien könnte er in jedem Fall nur lesend zugreifen, da auf das Unterverzeichnis 'Files' keine Schreibrechte für Everyone eingerichtet sind.

Unter **Optionen → Sicherheit** können Sie konfigurieren, dass die AdminsRobot-Freigabe nur dann erstellt wird, wenn Sie für eine Aktion benötigt wird. Danach wird sie nach einer frei wählbaren Zeitspanne wieder gelöscht.

## Silent Installation / Installation per Softwareverteilung

Die Installation ohne Benutzereingriff können Sie folgendermaßen durchführen:

```
msiexec /i AdminsRobot.msi /qr CREATE_ARSHARE="YES" CREATE_TASK="YES"
GLOBALOBJECTSDIR="//server\share$" SUBNETMASK="255.255.0.0" LICENSEKEY="AK14F-
LN960-B1C72-7BU7J-34N37"
```

Geben Sie bei **LICENSEKEY** Ihren Lizenzschlüssel an. Den Lizenzschlüssel für die kostenlose 50-PC-Version finden Sie als Textdatei im Download.

Der Pfad für die globalen Objekte wird unter **GLOBALOBJECTSDIR=** angegeben. Zusätzlich können Sie bei der unbeaufsichtigten Installation die für Sie gültige Subnet-Maske angeben und bestimmen, ob der AdminsRobot-Share bzw. der AdminsRobot-Task während der Installation erstellt werden. Der AdminsRobot-Share wird für einige Aktionen benötigt, um Ergebnisse zurückzuschreiben. Der AdminsRobot-Task ist für die zeitgesteuerte Ausführung von Aktionen notwendig.

Die Deinstallation erfolgt mit

```
msiexec /x AdminsRobot.msi /qb
```

## Bereitstellen der globalen Objekte

AdminsRobot kann mit einem zentralen Objekt-Datenpool betrieben werden. Das hat den Vorteil, dass alle AdminsRobot-Benutzer immer die gleichen, aktuellen Objekte zur Verfügung haben. Der zentrale Datenpool besteht aus der Datei GlobalObjects.txt. Jeder Benutzer hat die Möglichkeit, sich zusätzlich individuelle Objekte zu erstellen. Diese werden automatisch in der Datei PersonalObjects.txt gespeichert und sind für andere AdminsRobot-Benutzer nicht sichtbar.

## PCs aus DHCP-Server extrahieren

Die einfachste Möglichkeit, an PC-Namen, IP-Adressen und Mac-Adressen zu gelangen, ist der Export aus Ihrer DHCP-Datenbank. Im folgenden sind zwei Skripte und deren Einrichtung beschrieben, die den zentralen Datenpool **GlobalObjects.txt** generieren. Das erste Skript **ExportDhcp.vbs** exportiert nur die Hostnamen, Mac-Adressen und IP-Adressen aus einer Microsoft DHCP-Datenbank und erzeugt daraus den zentralen Datenpool, das zweite Skript **CreateGlobalObjects.vbs** erweitert die Objekte noch um die Namen der angemeldeten Benutzer. Die beiden Skripte können alternativ eingesetzt werden - beim Einsatz von CreateGlobalObjects.vbs wird ExportDhcp.vbs nicht benötigt. Sie finden die beiden Skripte im AdminsRobot-Download.

Das folgende Skript ExportDhcp.vbs exportiert die Hostnamen, Mac-Adressen und IP-Adressen aus einer Microsoft DHCP-Datenbank in die Datei GlobalObjects.txt, die dann als Datenquelle für AdminsRobot verwendet werden kann. Aber Schritt für Schritt:

1. Speichern Sie die Datei ExportDhcp.vbs in einem Verzeichnis auf Ihrem DHCP-Server, z.B. in C:\Program Files (x86)\DhcpExport. (Kann auch ein anderer Server sein. Entscheidend ist der Benutzeraccount, unter dem das Skript ausgeführt wird.)
2. Ändern Sie in der Datei ExportDhcp.vbs nach "dhcpserver =" den Wert auf den Namen Ihres DHCP-Servers und nach "domainsuffix =" den Wert auf den Namen Ihrer Domäne, z.B. ".domain.de"

3. Starten Sie die Datei ExportDhcp.vbs. Wichtig ist, dass Sie über ausreichend Rechte verfügen, um einen Export der DHCP-Leases durchführen zu können. Im Zweifelsfall starten Sie eine Eingabeaufforderung (als Administrator ausführen), navigieren in das richtige Verzeichnis und setzen den Befehl "wscript ExportDhcp.vbs" ab. Nach einigen Sekunden ist die Erstellung der Datei GlobalObjects.txt abgeschlossen.
4. Die Datei GlobalObjects.txt eignet sich als AdminsRobot-Datenquelle. Speichern Sie sie in eine zentrale Freigabe. Der Kopierbefehl ist am Ende des Skriptes bereits vorhanden. Geben Sie in AdminsRobot unter Extras / Optionen / Allgemein / Globale Objekte den Pfad zu dieser Datei an.
5. Starten Sie AdminsRobot neu. In der Objekt-Liste erscheinen nun die aus der DHCP-Datenbank generierten Objekte.

Das Wichtigste fehlt allerdings noch: die Information, welcher Benutzer sich an welchem PC anmeldet. Es gibt verschiedene Möglichkeiten, diese Information zu erhalten.

## GlobalObjects.txt mit Benutzerinformationen erzeugen

Im Folgenden ist beschrieben, wie man mit Bordmitteln die Zuordnung PC – Benutzer erhält. Dabei wird auch berücksichtigt, dass sich mehrere Benutzer an einem PC anmelden können.

### Erstellen einer Textdatei bei jeder Anmeldung eines Benutzers

Über die Gruppenrichtlinien im Active Directory lässt sich konfigurieren, dass bei jeder Anmeldung ein Skript ausgeführt wird. Das nutzen wir, um bei jedem Anmeldevorgang eine Textdatei mit dem Dateinamen %COMPUTERNAME%\_%USERNAME%.txt zu erzeugen (z.B. mueller\_pc04711.txt), die in eine zentrale Freigabe geschrieben wird.

Schritt für Schritt:

1. Erstellen Sie auf einem Fileserver eine Windows-Freigabe mit Namen pc\$. Sowohl bei den Freigaberechten als auch bei den NTFS-Berechtigungen ist es wichtig, dass alle Domänenbenutzer (Domain Users) Ändern-Rechte (Modify) besitzen. Sie können den Domänenbenutzern die Leserechte auch noch entziehen – ist aber im ersten Schritt nicht wichtig.
2. Erstellen Sie eine neue Gruppenrichtlinie oder erweitern Sie eine vorhandene. Navigieren Sie zu Benutzerkonfiguration → Richtlinien → Windows-Einstellungen → Skripts (Anmelden/Abmelden) → Anmelden. Klicken Sie auf "Dateien anzeigen" und erstellen Sie eine Datei mit dem Namen "UserNames.cmd" mit folgendem Inhalt:

```
@echo off
```

```
echo Computername: %COMPUTERNAME%
>\\MyFileServer\pc$\%COMPUTERNAME%_%USERNAME%.txt
```

Ersetzen Sie MyFileServer durch den Namen Ihres Fileservers.

3. Klicken Sie auf "Hinzufügen" und "Durchsuchen" und wählen Sie die gerade erstellte Datei aus.
4. Melden Sie sich mit einem Benutzer, für den die neu erstellte Gruppenrichtlinie Gültigkeit besitzt, an und vergewissern Sie sich, dass bei jeder Anmeldung in der Freigabe pc\$ eine Textdatei erstellt wird.
5. Speichern Sie die CreateGlobalObjects.vbs in einem Verzeichnis auf Ihrem DHCP-Server, z.B. in C:\Program Files (x86)\DhcpExport. (Kann auch ein anderer Server sein. Entscheidend ist der Benutzeraccount, unter dem das Skript ausgeführt wird.)
6. Ändern Sie in der Datei CreateGlobalObjects.vbs nach "dhcpserver =" den Wert auf den Namen Ihres DHCP-Servers, nach "share =" den Wert auf den UNC-Pfad der in 1. erstellten

Freigabe und nach "domainsuffix = " den Wert auf den Namen Ihrer Domäne, z.B. ".domain.de".

7. Starten Sie die Datei CreateGlobalObjects.vbs. Wichtig ist, dass Sie über ausreichend Rechte verfügen, um einen Export der DHCP-Leases durchführen zu können. Im Zweifelsfall starten Sie eine Eingabeaufforderung (als Administrator ausführen), navigieren in das richtige Verzeichnis und setzen den Befehl "wscript CreateGlobalObjects.vbs" ab. Nach einigen Sekunden oder wenigen Minuten ist die Erstellung der Datei GlobalObjects.txt abgeschlossen.
8. Die Datei GlobalObjects.txt eignet sich als AdminsRobot-Datenquelle. Speichern Sie sie in eine zentrale Freigabe. Der Kopierbefehl ist am Ende des Skriptes bereits vorhanden. Geben Sie in AdminsRobot unter Extras / Optionen / Allgemein / Globale Objekte den Pfad zu dieser Datei an.
9. Starten Sie AdminsRobot neu. In der Objekt-Liste erscheinen nun die aus der DHCP-Datenbank generierten Objekte mit Benutzerinformationen.

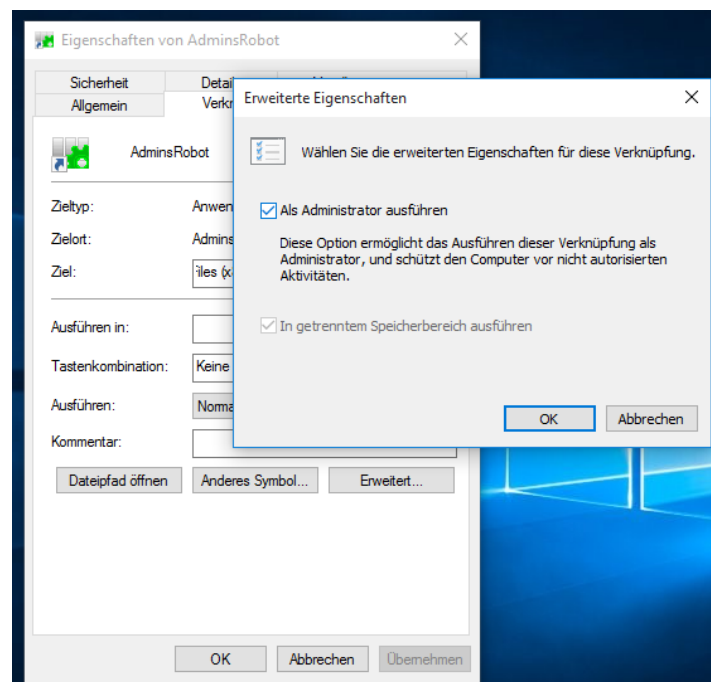
Die Datei GlobalObjects.txt enthält alle wichtigen Informationen in folgendem Format:

*Hostname,Mac-Adresse1,Mac-Adresse2,Mac-Adresse3,Anmeldedatum,Benutzer,IP-Adresse,Typ*

Das Anmeldedatum ist das Datum der Anmeldung des zuletzt angemeldeten Benutzers. Alle angemeldeten Benutzer stehen im Feld "Benutzer" durch Leerzeichen getrennt. Der zuletzt angemeldete Benutzer steht an erster Position.

## Als Administrator ausführen

AdminsRobot wird in den meisten Fällen als Administrator gestartet. Der Start lässt sich über die rechte Maustaste --> „Als Administrator ausführen“ realisieren. Über die Eigenschaften der AdminsRobot-Verknüpfung (Desktop, Startmenü oder Taskleiste) lässt sich konfigurieren, dass AdminsRobot immer als Administrator ausgeführt wird. Klicken Sie dazu mit rechter Maustaste (evtl. mit gedrückter Shift-Taste) auf das AdminsRobot-Symbol, dann auf **Eigenschaften** und **Erweitert**:



## Dienste und Ports

Um entfernte Windows-Rechner administrieren zu können (Computerverwaltung, c\$-Freigabe öffnen, Eventlogs ansehen usw.), ist es notwendig, einige Standard-Administrationsdienste und -ports auf den zu verwaltenden Clients zu aktivieren

### Dienste

Der Dienst **Remoteregistrierung** sollte auf allen Clients, die mit AdminsRobot verwaltet werden, gestartet sein. Der Dienst kann auch auf „Trigger Start“ (Start durch Auslöser) stehen. Dieser Dienst wird beispielsweise von der Aktion „PC-Check“ angesprochen.

Einige Aktionen enthalten den Befehl `wmic.exe` und benötigen dafür den Dienst **Windows-Verwaltungsinstrumentation**.

### Ports

Folgende TCP-Ports sollten auf allen durch AdminsRobot administrierten Rechnern in der Windows-Firewall geöffnet sein:

1. **ICMPv4 (Ping) - eingehend:** Diese Windows Firewall-Regel sollte auf allen Clients aktiviert sein, um feststellen zu können, ob ein Rechner im Netzwerk antwortet.
2. **TCP - Port 445 - eingehend:** Dieser Port sollte als eingehender Port in der Windows-Firewall freigeschaltet sein. Der Port wird benötigt, um eine Freigabe auf dem entfernten Rechner zu verbinden (z.B. c\$-Freigabe) und um mit dem PSEXEC-Tool Befehle auf dem entfernten Rechner ausführen zu können.
3. **TCP - RPC Dynamic Ports - eingehend:** Dieser Port sollte als eingehender Port in der Windows-Firewall freigeschaltet sein. Das Öffnen dieses Ports beschleunigt das Öffnen der Computerverwaltung und die Ausführung von PSEXEC-Befehlen.

Die Freischaltung der Ports kann natürlich per Gruppenrichtlinie erfolgen.

**Hinweis:** Die unter Punkt 2. und 3. aufgeführten Firewall-Einstellungen können auf die IP-Adressen der AdminsRobot-Rechner beschränkt werden. Tragen Sie dazu in der Registerkarte **Scope** (Bereich) die IP-Adressen der AdminsRobot-Rechner ein.

## PowerShell-Skripte

Einige AdminsRobot-Aktionen verwenden PowerShell-Skripte. Die Ausführung von unsignierten PowerShell-Skripten ist standardmäßig unter Windows verboten und muss zunächst erlaubt werden. Einen ganz vernünftigen Kompromiss zwischen Sicherheit und Praxistauglichkeit bietet die Einstellung "RemoteSigned". Der Befehl dafür lautet (innerhalb einer PowerShell-Console): **Set-ExecutionPolicy RemoteSigned**.