



# DpuScan

Janich & Klass  
Computertechnik GmbH



## DpuScan 7

Referenzhandbuch

Modul Rechteverwaltung



## Copyrights

© 1997 bis 2024 Janich & Klass Computertechnik GmbH. Alle Rechte vorbehalten. Gedruckt in Deutschland. Die in dieser Dokumentation enthaltenen Informationen sind Eigentum der Janich & Klass Computertechnik GmbH. Ohne schriftliche Genehmigung der Janich & Klass Computertechnik GmbH begründen weder der Empfang noch der Besitz dieser Informationen irgendein Recht auf Reproduktion oder Veröffentlichung irgendwelcher Teile davon.

## Warenzeichen

Alle Produktnamen und Logos sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Eigentümer.

## Haftungsausschluss

Die Anweisungen und Beschreibungen in diesem Handbuch waren zum Druckzeitpunkt zutreffend. Wir behalten uns jedoch das Recht vor, sowohl Beschreibung als auch Produkt jederzeit ohne Benachrichtigung zu ändern. Nach dem derzeitigen Stand der Softwaretechnik ist es nicht möglich, Programme zu entwickeln, die unter allen Bedingungen in jeder Konfiguration fehlerfrei arbeiten. Die Janich & Klass Computertechnik GmbH übernimmt keinerlei Haftung für Defekte, die direkt oder indirekt durch Fehler dieses Handbuches, Weglassen von Informationen oder durch Unstimmigkeiten zwischen diesem Referenzhandbuch und dem Produkt entstanden sind.

## Aktualität

Es ist möglich, dass im Internet eine neuere Version dieses Handbuches verfügbar ist. Wir empfehlen deshalb, die Version anhand des auf dieser Seite abgedruckten Datums mit der Version auf dem Internet zu vergleichen. Falls die Version im Internet neueren Datums ist, sollten Sie diese herunterladen und ggf. selbst ausdrucken.

Die aktuelle Version des DpuScan Referenzhandbuch finden Sie im Web unter:

[https://www.dpuscan.com/pdf/de\\_manual/DpuScan-Referenzhandbuch.pdf](https://www.dpuscan.com/pdf/de_manual/DpuScan-Referenzhandbuch.pdf)



## Inhaltsverzeichnis

<b>1 Benutzerrechte</b>	<b>6</b>
1.1 Übersicht Benutzerrechte .....	6
1.2 Konfiguration .....	7
1.2.1 Benutzer hinzufügen .....	8
1.2.2 Einstellungen .....	9
1.2.3 Rechte .....	9
1.3 Beispiel .....	10
1.4 Verwendung auf anderen Stationen .....	11

## 1 Benutzerrechte

Das Programm bietet die Möglichkeit, den Zugriff auf bestimmte Funktionen oder bestimmte Tasks einzuschränken. Es verwendet dabei die im Betriebssystem hinterlegten Gruppen und Benutzer.

[Benutzerrechte](#)

[Konfiguration](#)

[Benutzer hinzufügen oder entfernen](#)

[Einstellungen](#)

[Rechte](#)

[Beispiel](#)

[Verwendung bereits erstellter Berechtigungsdefinitionen auf anderen Stationen](#)

### 1.1 Übersicht Benutzerrechte

Microsoft-Windows verwaltet Benutzer und Gruppen. Gruppen sind Zusammenfassungen von Benutzern. Benutzer können gleichzeitig Mitglieder in mehreren Gruppen sein. Auf der Basis dieser Informationen werden in Windows-Systemen Berechtigungen geregelt. Das sind zum Beispiel Zugriffsberechtigungen für Dateien des Computers oder Ausführungsberechtigungen für Programme.

Die Verwaltung der Benutzer und Gruppen sowie der Zuordnung von Benutzern zu Gruppen wird mit den Mitteln des Betriebssystems durchgeführt.

In DpuScan besteht die Möglichkeit, Berechtigungen zum Ausführen von Tasks und auch von einzelnen Kommandos einzurichten. DpuScan nutzt hierzu die Informationen über Benutzer und Gruppen des Windows-Systems, auf dem die Anwendung betrieben wird. Sowohl für Benutzer als auch für Gruppen können Rechte vergeben werden. Der Administrator kann dabei Rechte zuweisen oder auch ausdrücklich entziehen. Für jede Benutzergruppe oder auch einzelne Benutzer wird ein kompletter Satz von Berechtigungseinstellungen abgelegt.

Die nachfolgende Beschreibung hebt auf die Rechteverwaltung in DpuScan ab. Im Programmpaket von DpuScan gibt es darüber hinaus noch weitere Module, die die Rechteverwaltung nutzen. Hierbei unterscheiden sich lediglich die Listen der Objekte, denen Rechte zugewiesen werden können.

Siehe auch: [Konfiguration](#)

[Benutzer hinzufügen oder entfernen](#)

[Einstellungen](#)

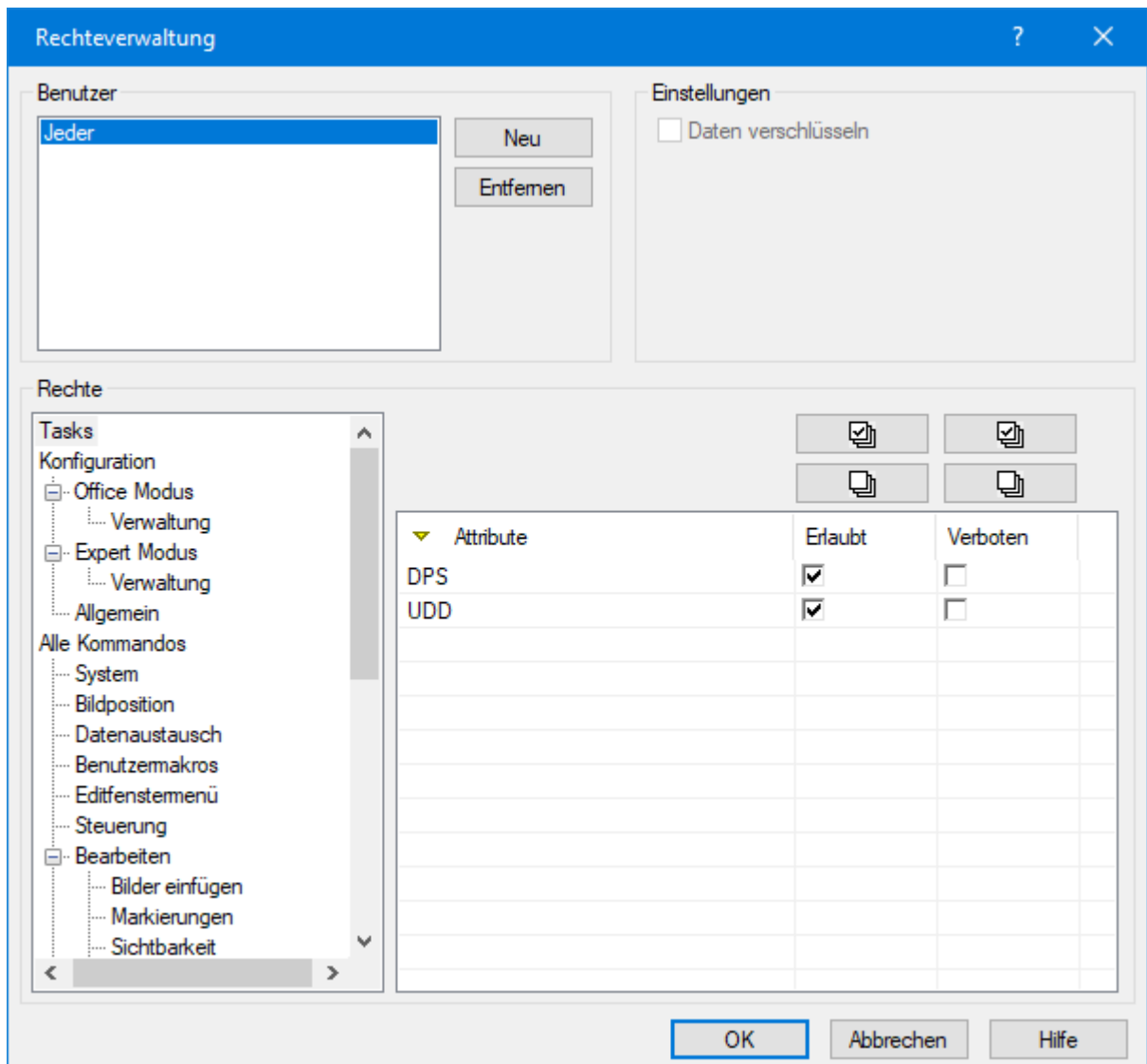
[Rechte](#)

[Beispiel](#)

Weitere Informationen finden Sie im [Inhalt](#).

## 1.2 Konfiguration

Über **Datei | Konfiguration: Benutzerrechte** gelangt man in den Dialog zur Verwaltung der Benutzerrechte.



## Rechteverwaltung

Der Dialog ist in die Bereiche **Benutzer**, **Einstellungen** und **Rechte** unterteilt.

Der Bereich [Benutzer](#) erlaubt das Hinzufügen oder Entfernen von Benutzern und Gruppen, für die anschließend Rechte vergeben werden.

Über die [Einstellungen](#) wird festgelegt, ob die Ablage der Rechte verschlüsselt erfolgt.

Die Elemente im Bereich **Rechte** erlauben die Vergabe der Rechte für einzelne Objekte. Die Eingabe bezieht sich auf den aktuell ausgewählten Eintrag aus der Liste der Benutzer bzw. Gruppen.

Am unteren Rand des Fensters befinden sich die drei Schaltflächen:

<b>OK</b>	Schließt den Dialog und speichert alle Definitionen auf Festplatte.
<b>Abbrechen</b>	Schließt den Dialog, ohne zu speichern.
<b>Hilfe</b>	Öffnet den Hilfebildschirm.

Siehe auch: [Benutzer hinzufügen oder entfernen](#)

[Einstellungen](#)

[Rechte](#)

Weitere Informationen finden Sie im [Inhalt](#).

### 1.2.1 Benutzer hinzufügen

Nach der Installation von DpuScan ist hier der Eintrag "Jeder" vorhanden, für den im Standard die Ausführung aller Kommandos und Tasks erlaubt ist.

Über die Schaltfläche **Neu** gelangt man zu einem Dialog, der das Hinzufügen von Benutzern und/oder Gruppen erlaubt.

Die Dialoge zur Auswahl von Benutzern und Gruppen sind je nach verwendeter Windows-Version unterschiedlich und werden in diesem Handbuch nicht im Einzelnen erläutert.

Verwenden Sie für weitergehende Informationen über die Benutzerverwaltung Ihrer verwendeten Windows-Version bitte die Dokumentation des Betriebssystems.

Unterschiedliche Darstellungen haben keine Auswirkungen auf die Funktionalität innerhalb von DpuScan.

Abhängig von der Windows-Version werden nun die Benutzer und Gruppen zur Auswahl angeboten.

Jeder neu hinzugefügte Benutzer bzw. jede neu hinzugefügte Gruppe hat zunächst alle Rechte.

Entsprechend dem Berechtigungskonzept sind dann die Rechte einzuschränken.

Die Schaltfläche **Entfernen** löscht den aktuell selektierten Eintrag aus der Liste.

Anmerkung:

Obwohl DpuScan die Vergabe von Rechten für einzelne Benutzer zulässt, ist bei der Erstellung des Berechtigungskonzeptes die Vergabe auf Gruppenebene zu bevorzugen, soweit das zugrunde liegende Betriebssystem dieses ermöglicht. Die Verwendung von Gruppen erleichtert die Abbildung von Rollen und Funktionen. Im Falle von Änderungen sind dann lediglich wenige Gruppen zu ändern bzw. ggf. die Gruppenzugehörigkeit der Benutzer anzupassen.

Siehe [Konfiguration](#)  
auch

[Einstellungen](#)

[Rechte](#)

Weitere Informationen finden Sie im [Inhalt](#).



### 1.2.2 Einstellungen

	Das Kontrollkästchen <b>Daten verschlüsseln</b> legt fest, dass die Einstellungen verschlüsselt auf der Festplatte abgelegt werden.
---	---

Die verschlüsselte Ablage der Rechteverwaltung auf der Festplatte allein stellt jedoch noch keinen Manipulationsschutz dar. Bei entsprechenden Sicherheitsanforderungen wird empfohlen, neben der Sperrung des Berechtigungsdialoges für Scan-Operatoren auch auf Betriebssystem-Ebene die Rechte für Dateien mit den Endungen ".rgi" auf "nur lesen" zu reduzieren. Diese Dateien sind bei Standard-Installationen im jeweiligen Programmverzeichnis abgelegt.

Siehe auch [Konfiguration](#)

[Benutzer hinzufügen oder entfernen](#)

[Rechte](#)

Weitere Informationen finden Sie im [Inhalt](#).

### 1.2.3 Rechte

Dieser Rahmen enthält am linken Rand eine Baumdarstellung zur Auswahl des funktionalen Kontextes, für den die Rechte vergeben werden sollen. In DpuScan wird auf der obersten Ebene zwischen **Tasks** und **Alle Kommandos** unterschieden.

Wählt man **Tasks**, so werden in der Liste rechts neben der Baumdarstellung die Tasks angezeigt, die auf dem System definiert sind.

Die Auswahl der **Kommandos** ist nach funktionellen Gesichtspunkten unterteilt, so dass die Anzahl der Elemente in der Liste klein gehalten werden kann.

Über die beiden Kontrollkästchen **Erlaubt** und **Verboten** sind drei verschiedene Zustände einzustellen:

Erlaubt	Verboten
<input checked="" type="checkbox"/>	<input type="checkbox"/>

Gibt an, dass die Ausführung des Tasks oder Kommandos erlaubt ist. Der Benutzer kann gleichzeitig in mehreren Gruppen Mitglied sein. Ist in einer dieser anderen Gruppenkonfiguration keines der Kontrollkästchen angekreuzt, wird die Ausführung durch diese Einstellung erlaubt. Sollte jedoch eine andere Gruppenmitgliedschaft die Ausführung verbieten, greift das ausdrückliche Verbot.

Erlaubt	Verboten
<input type="checkbox"/>	<input checked="" type="checkbox"/>

Mit dieser Einstellung ist die Ausführung des Kommandos oder Tasks verboten, unabhängig von weiteren Einstellungen. Das **ausdrückliche Verbot** hat die höchste Priorität und gilt vor allen anderen Einstellungen.

Erlaubt	Verboten
<input type="checkbox"/>	<input type="checkbox"/>

Diese Einstellung entspricht einem "nicht erlaubt". Im Gegensatz zur Einstellung "Verboten" kann in diesem Fall die Ausführung durch die Einstellung einer anderen Gruppenmitgliedschaft implizit erlaubt sein.

Systemseitig wird der Zustand ausgeschlossen, dass beide Kontrollkästchen aktiviert sind. Ist eines der Kästchen aktiv und man aktiviert das jeweils Andere, so wird das erste Kästchen deaktiviert.

Bitte beachten Sie, dass ausdrücklich erteilte, personenbezogene Rechte eines Benutzers ihre Gültigkeit durch den Beitritt zu einer Gruppe verlieren können, sofern in dieser Gruppe entsprechende Verbote gesetzt sind.

Aus diesem Grund wird empfohlen, Benutzer mit Administrationsaufgaben nicht einer Gruppe zuzuordnen.

Weiterhin ist darauf zu achten, ggfs. den Eintrag "Jeder" zu entfernen, um Seiteneffekte durch indirekte Erlaubnis zu verhindern.

Die Schaltflächen **Setze alle** und **Lösche alle** setzen bzw. löschen alle Häkchen in der Spalte unterhalb der jeweiligen Schaltfläche.

Siehe auch [Konfiguration](#)

[Benutzer hinzufügen oder entfernen](#)

[Einstellungen](#)

Weiter zum [Beispiel](#)

Weitere Informationen finden Sie im [Inhalt](#).

## 1.3 Beispiel

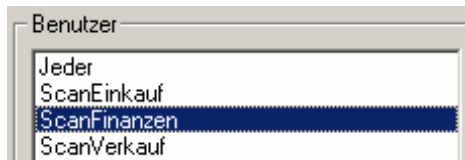
Im Rahmen der Rechtevergabe sind einige Dialoge abhängig vom verwendeten Betriebssystem. In dem nachfolgend beschriebenen Beispiel wird die Station unter Windows XP betrieben.

Auf der Scan-Station ist die Gruppe "ScanFinanzen" administriert. Dieser Gruppe sollen Rechte für die Task "SCAN1" zugewiesen und für die Task "INDEX1" ausdrücklich entzogen werden.

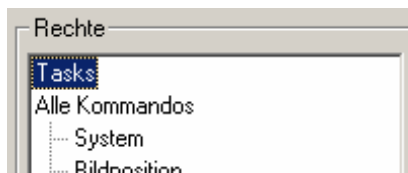
Zunächst ist die Gruppe zur Liste der Benutzer hinzuzufügen. Dazu ist die Schaltfläche **Neu** zu betätigen. Es öffnet sich ein weiterer Dialog, der Funktionen des zugrundeliegenden Betriebssystems anbietet. In das aktive Eingabefeld kann nun ein Benutzer oder Gruppenname eingegeben werden.

Um die Eingabe zu vereinfachen, kann eine Liste der verfügbaren Einträge angezeigt werden. Dazu ist die Schaltfläche **Erweitert** zu betätigen. In dem dann folgenden Dialog lassen sich Benutzer und/oder Gruppen auswählen, die mit Bestätigung der Dialoge der Liste in DpuScan hinzugefügt werden.

Zur Vergabe der Rechte ist der Listeneintrag "ScanFinanzen" auszuwählen.



Dann ist in der Baumansicht der Zweig "Tasks" zu markieren.



In der Liste der Tasks sind für die neue Gruppe zunächst alle Tasks als **Erlaubt** gekennzeichnet. Für die Task "INDEX1" ist das Kontrollkästchen **Verboten** zu aktivieren.

Attribute	Erlaubt	Verboten
DEFAULT	<input checked="" type="checkbox"/>	<input type="checkbox"/>
INDEX1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SCAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Die Konfiguration der Berechtigung wird mit Betätigen der Schaltfläche **OK** abgeschlossen. Allen Mitgliedern der Gruppe "ScanFinanzen" ist nun das Ausführen der Task "INDEX1" verboten. Das Verbot greift auch dann, wenn ein Benutzer beispielsweise zusätzlich Mitglied der Gruppe "ScanEinkauf" ist, die diese Task ausführen darf.

Zurück zum [Inhalt](#).

## 1.4 Verwendung auf anderen Stationen

Um bei Verwendung mehrerer Scan-Stationen die Berechtigungen nicht auf jeder Station erneut eingeben zu müssen, können die Berechtigungen auf andere Rechner übertragen werden. Hierzu werden durch einen Administrator auf einem Quellrechner die Berechtigungen gesetzt. Dann werden die Dateien mit der Endung ".rgi" auf die Zielrechner kopiert und dort ggfs. mit Mitteln des Betriebssystems gegen Verändern/Löschen gesichert.

Bei einem solchen Vorgehen ist zu beachten, dass die in der Berechtigungsdefinition genannten Benutzer/Gruppen sowohl auf dem Quellrechner als auch auf den Zielrechnern verfügbar sind.

Zurück zum [Inhalt](#).

# Index

## - A -

Ausführungsrechte 9

## - B -

Beispiel 10

Benutzer 8

Benutzer hinzufügen 8

Benutzerrechte 6

Berechtigungen 9

## - E -

Einstellungen 9

## - G -

Gruppen 8

Gruppenrechte 6

## - K -

Konfiguration 7

## - R -

Rechte 9

## - T -

Transport von Rechtedefinitionen 11

## - V -

Verschlüsselung 9

Verteilung von Rechtedefinitionen auf andere  
Stationen 11

## - W -

Wiederverwendung von Rechtedefinitionen 11