



DpuScan

Janich & Klass
Computertechnik GmbH



DpuScan 7

Reference Manual

Module User Privilege Administration

Copyrights

© 1997 to 2024 © Janich und Klass Computertechnik GmbH. All rights reserved.
Printed in Germany. The information contained in this documentation is the property of © Janich und Klass Computertechnik GmbH, Wuppertal. Neither receipt nor possession hereof confers or transfers any right to reproduce or disclose any part of the contents hereof, without the prior written consent of Janich & Klass, Wuppertal

Trademarks

The DPU logo is a registered trademark of © Janich und Klass Computertechnik GmbH. All other product names and logos are trademarks or registered trademarks of their representative companies.

Disclaimer

The instructions and descriptions in this manual were accurate at the time of this manual's printing. However, we reserve the right to alter the description and/or the product at anytime without prior notice. As per the actual state of software technique it is not possible to develop programs that will work trouble-free under all conditions and in any configuration. © Janich und Klass Computertechnik GmbH assume no liability for damages incurred directly or indirectly from errors, omissions, or discrepancies between this manual and the product.

Actuality

It may happen that a more recent version of this manual for DpuScan is available for download from the Internet. Therefore, it is recommended that you should compare the version by means of the date printed on this page with the version on the Internet. You should please use the most up-to-date version of the manual. The actual version of this First Steps Manual is found on the Web at the following address:

https://www.dpuscan.com/pdf/en_manual/DpuScan-Reference-Manual.pdf

Table of Contents

1 Overview User Rights	6
1.1 User Rights	6
1.2 Configuration	6
1.3 Example	8
1.4 Re-Use of defined User Privileges on other Computers	9

1 Overview User Rights

User Privileges

Configuration

How to Add or Remove Users

Options

Privilege

Example

Re-Use of defined User Privileges on other Computers

1.1 User Rights

Microsoft-Windows administers Users and Groups. Groups are combinations of Users. User may be members of several Groups, in parallel. Basing on this information, privileges are handled in Windows systems. This may be, for example, access privileges for files on the computer, or privileges to execute programs.

The administration of Users and Groups as well as the arrangement of Users to Groups is executed by means of the operating system.

In DpuScan it is possible to define privileges for executing Tasks and even individual commands. For doing so, DpuScan uses information about User and Groups on the Windows system where the application is in use. Privileges can be assigned to Users as also to Groups. The administrator can assign Privileges, or expressively forbid them. A complete set of privilege settings is saved for each User Group or also for individual Users.

The following description yields to the User Attributes Administration in DpuScan. The program package of DpuScan still contains further modules that use the User Attributes Administration. Here, only the lists of objects differ to which privileges can be assigned.

Also refer: Configuration

How to Add or Remove Users

Options

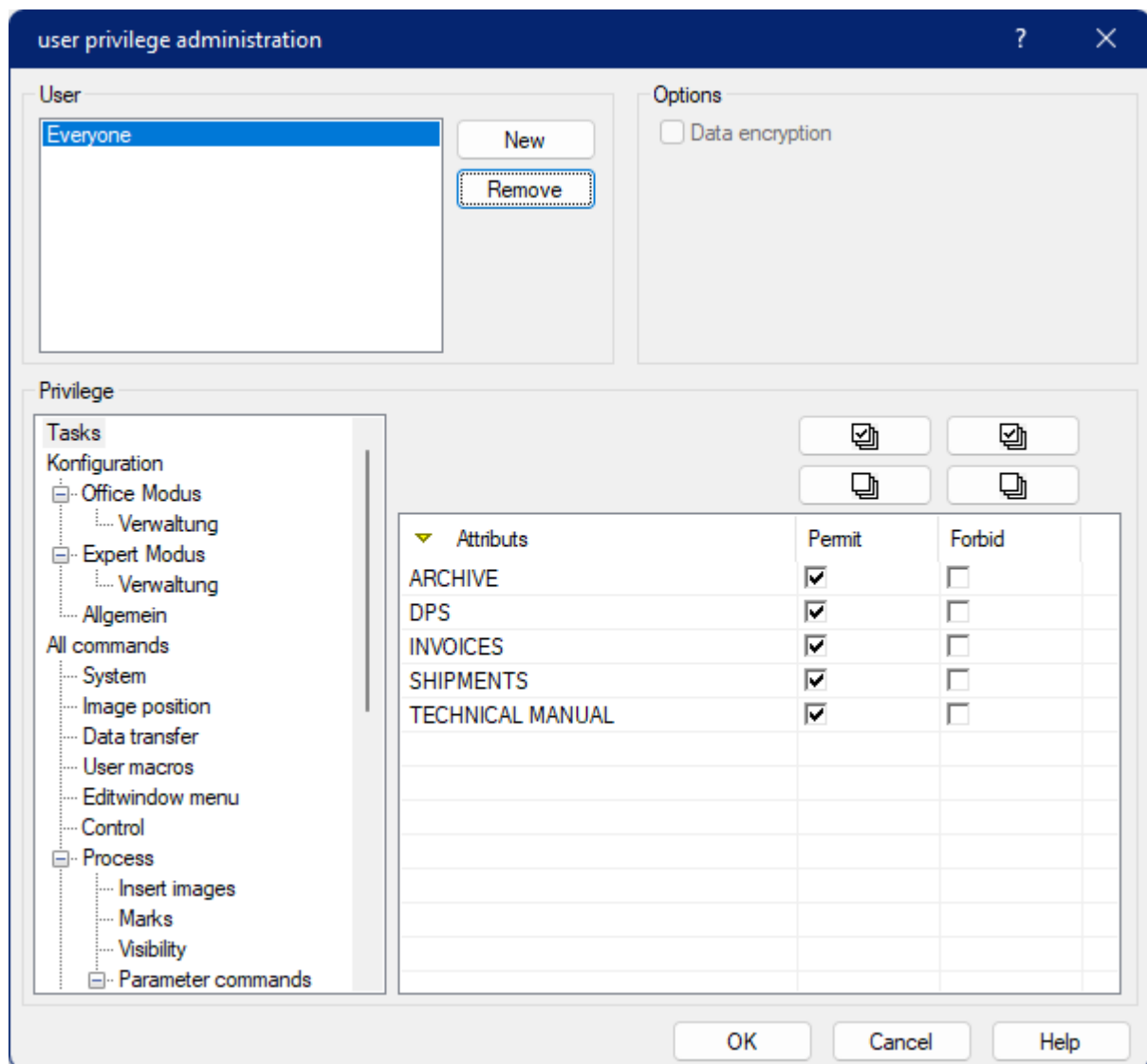
Privilege

Example

More information is found at Content.

1.2 Configuration

Click File | Configuration: User Attributes to enter the dialog for administering the user privileges.



Rights Management

The dialog is composed of the areas User, Options, and Privilege.

The User area allows to add or remove Users and Groups; later their Privileges are assigned. At Options you determine whether the data are stored in encrypted form, or not.

The elements in the Privilege area allow to assign privileges for individual objects. The entry relates to the actually selected entry in the list of Users or Groups.

Placed at the bottom of the window, you can find the three usual buttons:

- OK Closes the dialog and saves all definitions to disk.
- Cancel Closes the dialog without saving.
- Help Opens the Help screen.

Also refer: How to Add or Remove Users

Options

Privilege

More information is found at Content.

1.3 Example

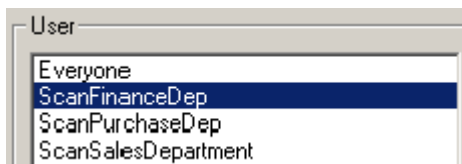
In the context of privilege assignment, some dialogs depend on the operating system in use. In the below described example, the workstation is driven under Windows XP.

On this scan station, the Group "ScanFinanceDep" is administered. To this Group, the Privileges for the Task "SCAN1" shall be assigned, and those for the Task "INDEX1" shall be expressively forbidden.

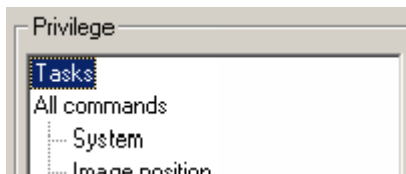
Initially, the Group must be added to the list of Users. For it, just click the New button. The next dialog that opens offers the functions of the basing operating systems. You can now enter a User or a Group name in the active input field.

In order to ease the input, you can display a list of available entries. Just click the Advanced button. In the following dialog, you can select the Users and/or Groups. When you confirm the dialog, these Users / Groups will be added to the list in DpuScan.

For assigning the Privilege, you must select the list entry "ScanFinanceDep".



The next step is to highlight the "Tasks" branch in the tree view.



In the list of Tasks, initially all Tasks are marked as Permit, for any new Group. For the Task "INDEX1", now please activate the Forbid box.

Attributes	Permit	Forbid
DEFAULT	<input checked="" type="checkbox"/>	<input type="checkbox"/>
INDEX1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SCAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The Privilege configuration is completed by clicking the OK button. For all members of the Group "ScanFinanceDep" it is now forbidden to execute the Task "INDEX1". This prohibition also becomes effective if a User is additional a member of, for example, the Group "ScanPurchaseDep" who may execute this Task.

[Return to Content.](#)

1.4 Re-Use of defined User Privileges on other Computers

When several workstations are in use, the Privileges must not always be newly entered on every station: The Privileges can be transferred to other computers. For doing so, an administrator will set the Privileges only once on a source computer. Then, the files with the extension ".rgi" are copied to the target PC and are there eventually secured against modification / removal by means of the operating system.

When you do so, please make sure that the Users/Groups stated in the Privilege definition do also exist on the target computers.

[Return to Content.](#)

Index

- C -

configuration 6

- D -

deployment of defined user privileges on other
computers 9

- E -

example 8

- G -

group rights 6

- R -

re-use of defined user privileges on other computers
9

- T -

transport of defined user privileges on other
computers 9

- U -

user rights 6