

MultiCash[®] 3.23

System Administrators Quick Reference

November 2012

Omikron Systemhaus GmbH & Co. KG
Von-Hünefeld-Str. 55
D-50829 Köln

Tel.: +49 (0)221 -59 56 99 -0
Fax: +49 (0)221 -59 56 99 -7

info@omikron.de
www.omikron.de

Table of Contents:

1	PRELIMINARY REMARKS.....	3
2	LOCAL INSTALLATION.....	4
3	NETWORK INSTALLATION.....	8
3.1	Preparations on the file server	8
3.2	Preparations on all workstations	15
3.3	Installation of the software on other workstations	17
4	UPDATE OVER AN OLDER VERSION.....	19
4.1	Prior to the update installation	20
4.2	Installation	21
4.3	After the update installation	21
5	GETTING STARTED	23
5.1	What to do next ... / Configuration Wizard	26
5.2	New entry of a user with the wizard	36
5.3	User groups and access class for confidential payments	43
6	HOW TO MAKE CHM FILES ACCESSIBLE VIA NETWORK	60
6.1	Zone modification	61
6.2	Allow URL	65

1 Preliminary remarks

This manual is addressed to consultants for Electronic Banking and system administrators who install and configure the application.

In **Chapter 2** the **installation** of the software is described.

In general, the software is network-compatible. For this reason, a standalone installation only differs from the network version concerning the type of configuration. If you want to install in a network, read for this reason first **Chapter 3** with notes on the **network installation**.

If you want to execute an **update** of an older version, please read first **Chapter 4**.

In **Chapter 5** you can read how the application is **configured** after the first logon.

Chapter 6 tells you, how to re-enable the remote access on **HTML Help files**.

2 Local installation

To install the program as single-user application, please follow the steps given below:

If you want to execute a network installation, please make sure that you have created the prerequisites according to **Chapter 3**.

1 Switch on the computer

Switch on your computer and wait until the memory test is done and Windows has been loaded.

2 Insert the CD-ROM

Place the Installation CD-ROM in the CD-ROM drive.

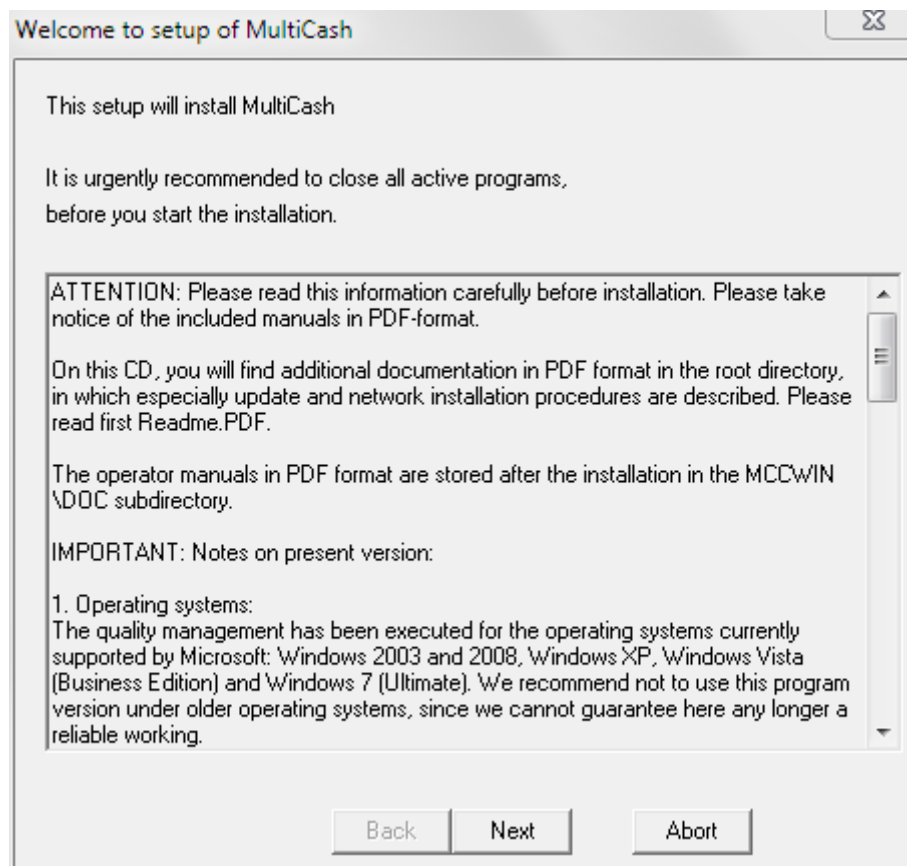
3 Start the Setup program

Open with the Windows Explorer the installation directory on the CD-ROM and start the program

Setup.exe

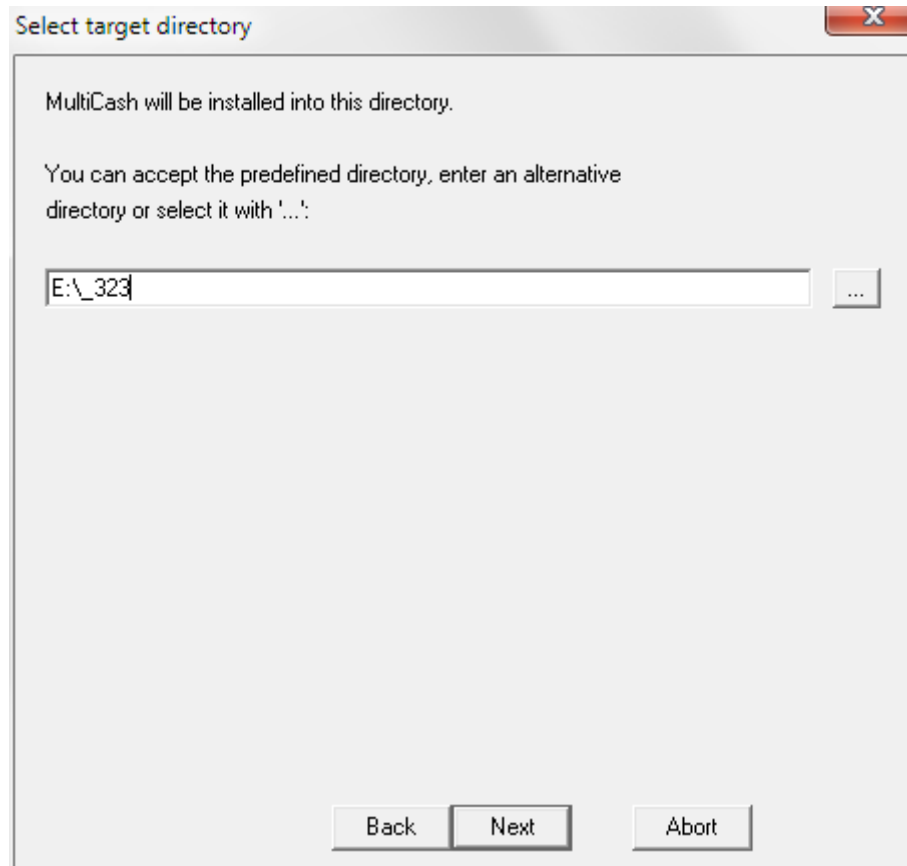
4 Welcome Screen

It is urgently recommended to close a still opened Core module before running **Setup**. After closing a possibly still opened module, you click on the **[Next]** button afterwards.



5 Selecting the target directory

When performing a new installation, the installation program suggests a default installation directory.



You can confirm the suggested drive and directory or browse to any other drive and directory of your choice using the [...] button.

If a version of the program is already installed, the installation program will now suggest the basic path, where the ..\MCCWIN directory has been installed. Via [...] button you can search for another basic installation directory.

If need be, a new directory can be created using the [**Make new folder**] button.



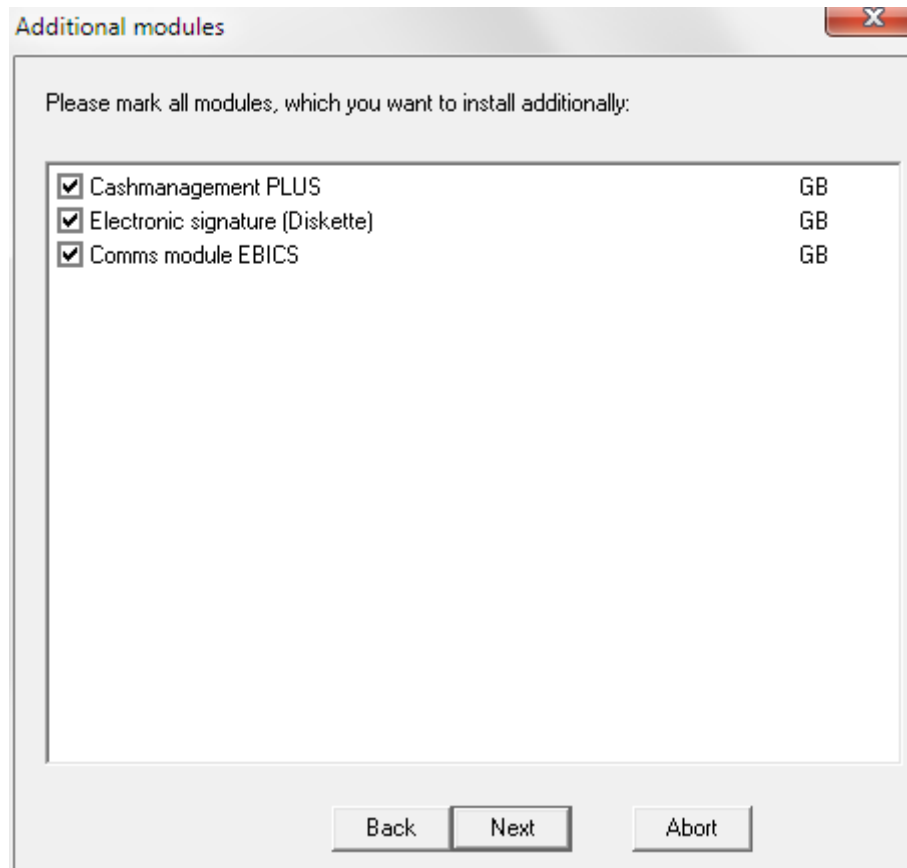
Please note...

- Mutated vowels (ä, ö, ü) in directory names are not allowed!
- For standalone installations under operating systems of the generation starting from Windows Vista / Windows 7 , please do not make any installation in the default path C:\Programs, since the default user has no write-access any longer.

After having defined the directory, click on the [**Next**] button.

6 Additional modules

If you have purchased **additional modules** and wish to install it immediately, please click on the desired module. If you wish, you can also wait to install this supplemental module separately at a later time. Install the supplementary modules in exactly the same manner as you installed the Core module.



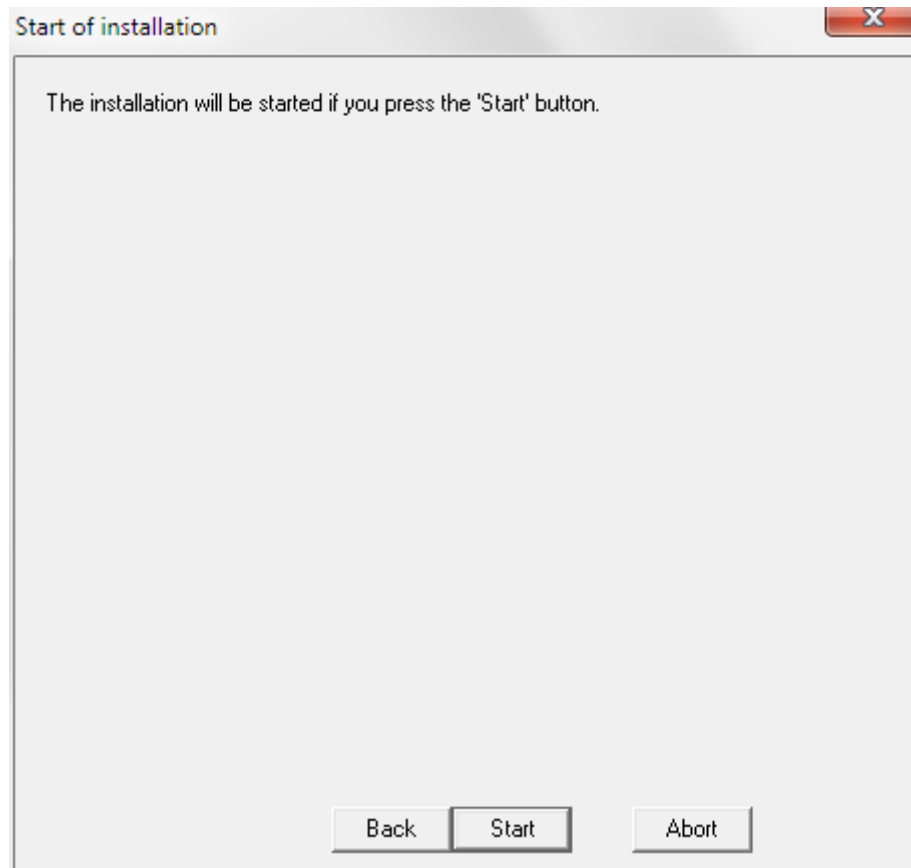
After selecting the additional module to be installed, click on the **[Next]** button.

7 Starting the Installation

Click on the **[Start]** button to start the installation process.

During the installation, a display at the lower edge of the installation screen will keep you informed regarding the progress of the copy routine. In the "Installation Progress" dialog box, each of the "Completed tasks" will be check marked.

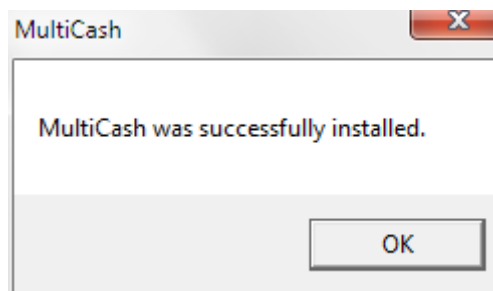
If you experience problems during installation or you cannot install the system properly, please contact your **bank's systems consultant or your Omikron partner**.



8 Quitting the Installation

Once the installation has been successfully completed, the installer will quit with an appropriate message.

Click on the [**OK**] button to return to the Windows screen. The Core module has now been successfully installed on the drive you selected.



The Start menu now contains a new entry from which you can start the program that you have just installed.

3 Network Installation

In principle, the installation of a network version is made in the following steps:

1. Configuration of the network resource on the file server
2. Installation of the software on the file server
3. Starting the software on the computer to be used as database server (recommended: file server) and configuration of the program parameters
4. If required: Configuration of the database service
5. If required: Definition of the user groups with their rights in the network domain
6. Configuration of the access paths for the workstations
7. Call of the Setup program from the central resource on each workstation

For the use of the system within a network environment, please make the following steps during installation :

Requirements:

1. TCP / IP protocol
2. A DNS – Name for addressing the database



Please note ...

For network installations with drive linkage you should use necessarily a **path without blanks**, because otherwise starting with Windows Vista / Windows 7 the program shortcuts on the workstations cannot be made correctly.

3.1 Preparations on the file server

On the file server, the administrator has to create a new directory and to release it in the network or a directory already released in the network can be used for the installation of the program.

Alternatively, a drive partition can also be used. This is recommended for larger databases, since the data accesses are directly made to the hard disk and not using the network subsystem.

On the directory released for the program, the access right 'Change' or 'Full access' must be assigned to all users.

Example:

The directory 'EB' on the computer 'fileserv' is made accessible to its user as network resource 'ElectronicBanking'.



Please note ...

The access to the directory need be accomplished for the database server and the clients in the same way! If you want to select the installation from the workstations using the UNC path, you also have to make the installation on the server using the UNC path. If you install on a partition, on the clients the chosen drive letter must be connected to the network resource.

3.1.1 Installing the software

For this, proceed as described in **Chapter 2** .



Please note ...

The database addressing is automatically configured at first logon. For this reason, execute the first logon on the computer which should be used later as database server.

3.1.2 First start of the software

Even if the file server is used to serve as database server, start here the software now. If the data base engine should run on another computer, accomplish there first the configuration as workstation, as described in the next chapter.

Here you should accomplish the configuration of the system as described in **Chapter 5** .

3.1.3 Setup database server as service

Requirements:

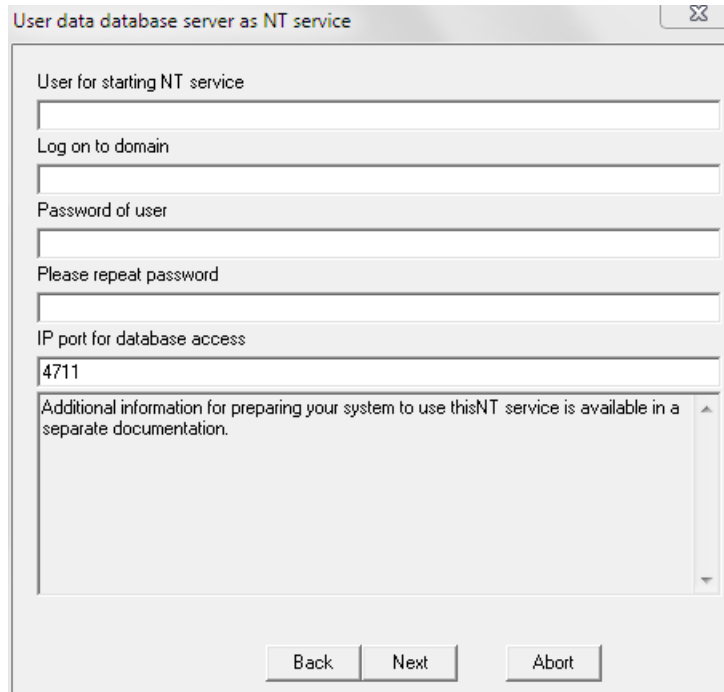
For using the database as Windows service, the following prerequisites must be fulfilled:

The user of the database service must, as all other users which wish to use the program, have full access to the network resource.

For this user, the permission "Logon as Service" must also be switched on under "Local security guidelines". You can check the status of the database service, as for other NT-services, in the display of services. The database is started without a window being opened, i.e. the status can only be seen in the service settings. In addition, the files ZBASE32.LOG and B30SVC.LOG are written to the Windows system directory, in which the messages of the database services are logged.

You can configure the database server so that the database is started directly on booting the PC as service under NT, without a user having to log on. The database server is then accessible for all users in the network.

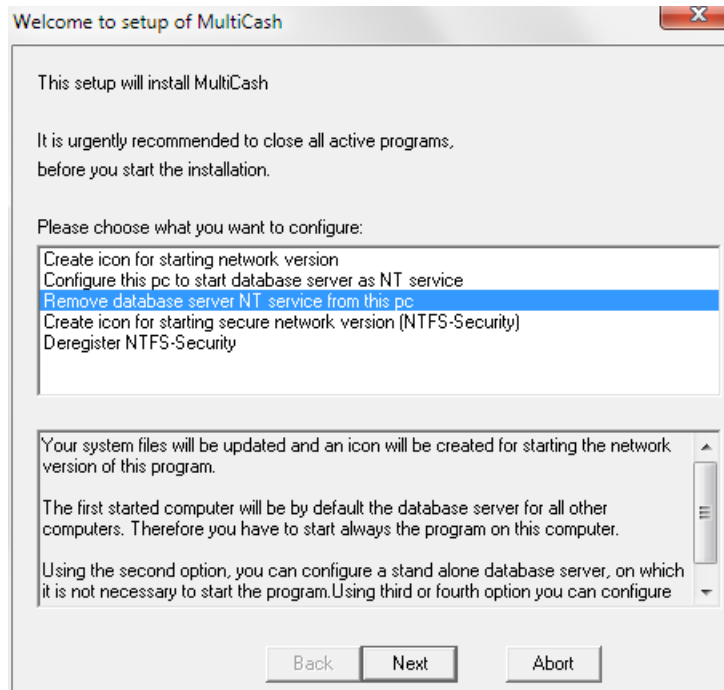
To configure the function of the database server as service, start the program SETUP.EXE in the main directory ('E:\EB') and select the option '**Configure this PC to start database server as NT service**'. Now the database will be added to the NT services and automatically started the next time you boot the PC. On the second page of the wizard dialog, you must enter details of the user under which the service is to be started. Please note that 'Domain' does not refer to the domain for which the user should logon, but the domain in which the user is defined. This is usually the local PC name. The database service automatically logs on in the network under this user ID and accesses the network resource installed for the program.



The dialog box is titled "User data database server as NT service". It contains several input fields: "User for starting NT service", "Log on to domain", "Password of user", "Please repeat password", and "IP port for database access" (which has "4711" entered). Below these fields is a text area with the message: "Additional information for preparing your system to use this NT service is available in a separate documentation." At the bottom are three buttons: "Back", "Next", and "Abort".

3.1.4 Deregister database as service

If you do not want to use the service for the database server any longer, start the program SETUP.EXE in the main directory of the PC (e.g. 'E:\EB') and select the option '**Remove database server NT service from this PC**'. This removes the database from the services. Quit the appropriate message with [OK].



The dialog box is titled "Welcome to setup of MultiCash". It contains the following text: "This setup will install MultiCash", "It is urgently recommended to close all active programs, before you start the installation.", and "Please choose what you want to configure:". Below this is a list box with five options: "Create icon for starting network version", "Configure this pc to start database server as NT service", "Remove database server NT service from this pc" (which is highlighted in blue), "Create icon for starting secure network version (NTFS-Security)", and "Deregister NTFS-Security". Below the list box is a text area with the following text: "Your system files will be updated and an icon will be created for starting the network version of this program.", "The first started computer will be by default the database server for all other computers. Therefore you have to start always the program on this computer.", and "Using the second option, you can configure a stand alone database server, on which it is not necessary to start the program. Using third or fourth option you can configure". At the bottom are three buttons: "Back", "Next", and "Abort".

3.1.5 NTFS-Security: User groups for secure environment

If you want to stop the access of the users to the central databases, you can establish a secured environment using the "NTFS-Security" concept.

The configuration of the NTFS-Security can only be accomplished by the Windows system administrators in your company. For further prerequisites, please see the corresponding documentation from Microsoft. But you also have the possibility for the installation to be made by Omikron or an Omikron Partner.



Please note:

The NTFS-Security cannot be used under Windows Vista. Instead of that, we recommend to activate the encryption of certain file types in the system parameters (see Chapter 3.1).

The NTFS security concept for Omikron systems is based on the separation of the network resource (on which all data and programs are saved) from the external workstations. In order that the users of these workstations can access the functions of the application nevertheless, special services have been developed, which control the access to the network resource. These service programs are installed on each workstation, on which the application should be started under the terms and conditions of the NTFS-Security. You work as described in the following:

Omikron Secure Client

To start the respective application under the NTFS-Security, a special loader program is used ("LOADCLNT.EXE"), which sends a corresponding request to the Secure Loader described below. This loader program is located in the ..\system32 directory of the relevant workstation.

Omikron Secure Loader

The Secure Loader ("LOADSVC.EXE") runs under the system account, whereby it has access to the desktop of the workstation (i.e. can display dialogs on the screen). From the Secure Agent, the Secure Loader gets then access information for the network resource and can then start the relevant application with it.

Omikron Secure Agent

The Secure Agent ("LOADSVCP.EXE") runs under any account which has access to the network resource and is equipped with the right "Logon as a service". The Secure Agent accesses the "SECURITY.PAR" file, which is located on the network resource and in which the access information for this resource is contained.

To be able to make use of the possibilities of this security concept, we recommend you, apart from the standard users who should use the functions of the application, to configure on operating system level an internal user account (e.g. user "MCSEVER") for the logon of the Secure Loader. This user account must be authorized in the security policy of the network for the "Logon as a service". This user account must be equipped with all rights on the network resource. The information concerning this account is stored by the Omikron application also when defining the corresponding system parameter in the "SECURITY.PAR" file. The right for the local logon should be revoked from this user account in order that no user can log on with this identifier.

Note:

In order to ensure the smooth execution of all functions with activated NTFS Security, please make sure that for the NTFS user account the rights for launching COM objects are set correctly. The NTFS user must have the right "DefaultLaunchPermission".

If necessary check the settings under Windows 2000 as follows:

Choose Properties (right mouse button) under Control Panel / Administration / Component Services / Computers / My Computer and switch to the Default Security tab. Under "Default Launch Permissions" you can check after clicking the [Edit default...] button, whether the access type "DefaultLaunchPermission" is allowed for the NTFS user or "Everyone".

Under Windows XP you check the settings as follows:

Choose Properties (right mouse button) under Control Panel / Administration / Component Services / Computers / My Computer and switch to the COM Security tab. Under "Launch and activation permissions" you can check after clicking the [**Edit default...**] button, whether for the user the permissions "Local launch" and "Local activation" are allowed.

Information concerning the configuration of users on operating system level can be found in the documentation regarding your Windows operating system.

The following short instruction summarizes again the steps for configuring the NTFS-Security. It is assumed, that a network version (server / client installation) is already installed and working:

Server Configuration

1. Use the user administration of the Windows operating system to configure an internal user account for the logon of the Secure Loader (e. g. user "**MCSERVER**");

The following user rights has to be assigned in the **Local Computer Policy** to this user account: "**Log on as a service**", "**Log on as a batch job**" and if need be "**Deny logon locally**".

You can find these rights in the Group Policy (GPEDIT.MSC) under: *Local Computer Policy\ Computer Configuration\ Windows Settings\ Security Settings\ Local Policies\ User Rights Assignment*.

In the context of the **sharing/security settings on directory level** the user account requires the following authorizations:

In each case "**Full Control**" to all folders and files of the network installation on the File server (\\<File server>\<main path> and all subordinate folders and files).

You set these authorizations in the "Properties" menu of the file server directory using the *Security settings property page* and the *Sharing property page* (via [**Permissions**] button). Using the [**Add ...**] button you can choose and assign the user account respectively.

2. Logon on the **server** as ADMINISTRATOR (this user must be allowed to access the central resource having also local administrator rights in order that software can be installed on the clients and entries can be made in the registry). Start application. Activate subsequently the NTFS-Security on the *General parameters property page* in the system parameters, enter User-ID with password for "MCSERVER" and save it.



Please note:

The NTFS-Security must be activated after the setup of the user account on the **General parameters property page** in the **system parameters** of your Omikron application. For this, highlight there the "Activate NTFS-Security" check box with a mouse click. Then a text box opens in which you must enter the details (name and password) of the internal user account for the logon, which is authorized for the access to the network resource. The details for this user account are written to the "SECURITY.PAR" file.

When entering, please make absolutely sure that the spelling of the user name and password agree with that one which has been used for the setup of this internal user account on the operating system level of Windows (see point 1).

**Please also note:**

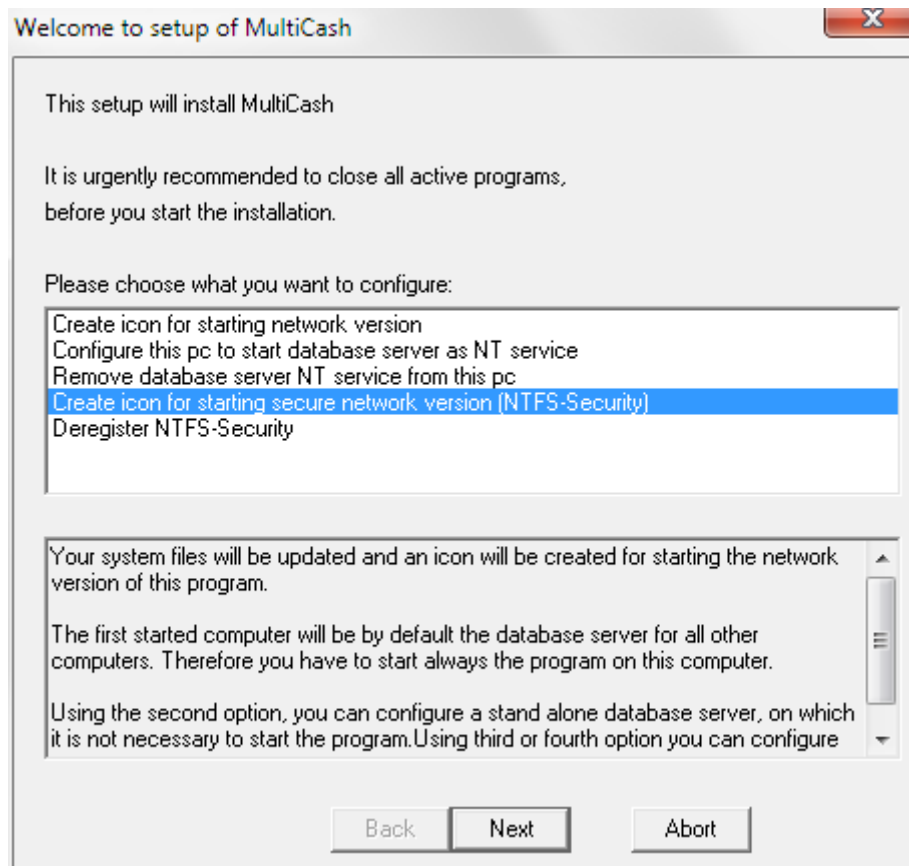
If you connect the program's network resource with a **drive letter**, this drive letter may not be filled under **Windows 2000** for the local user. Under Windows 2003 this restriction does not apply any longer, since here the drive connections for each current user are administered separately.

Client Configuration

3. Logon on the **clients** as **ADMINISTRATOR** (this user must be allowed to access the central resource and must have local administrator rights in order that software can be installed on the Clients and entries can be made in the registry).

The following user rights has to be assigned in the **Local Computer Policy** to the "**MCSERVER**" user account: "**Log on as a service**". You can find this right in the Group Policy (GPEDIT.MSC) under: *Local Computer Policy\ Computer Configuration\ Windows Settings\ Security Settings\ Local Policies\ User Rights Assignment*.

Execute now the "SETUP.EXE" file in the main path of the central resource in order to create a new icon for starting the secured network version (NTFS Security).

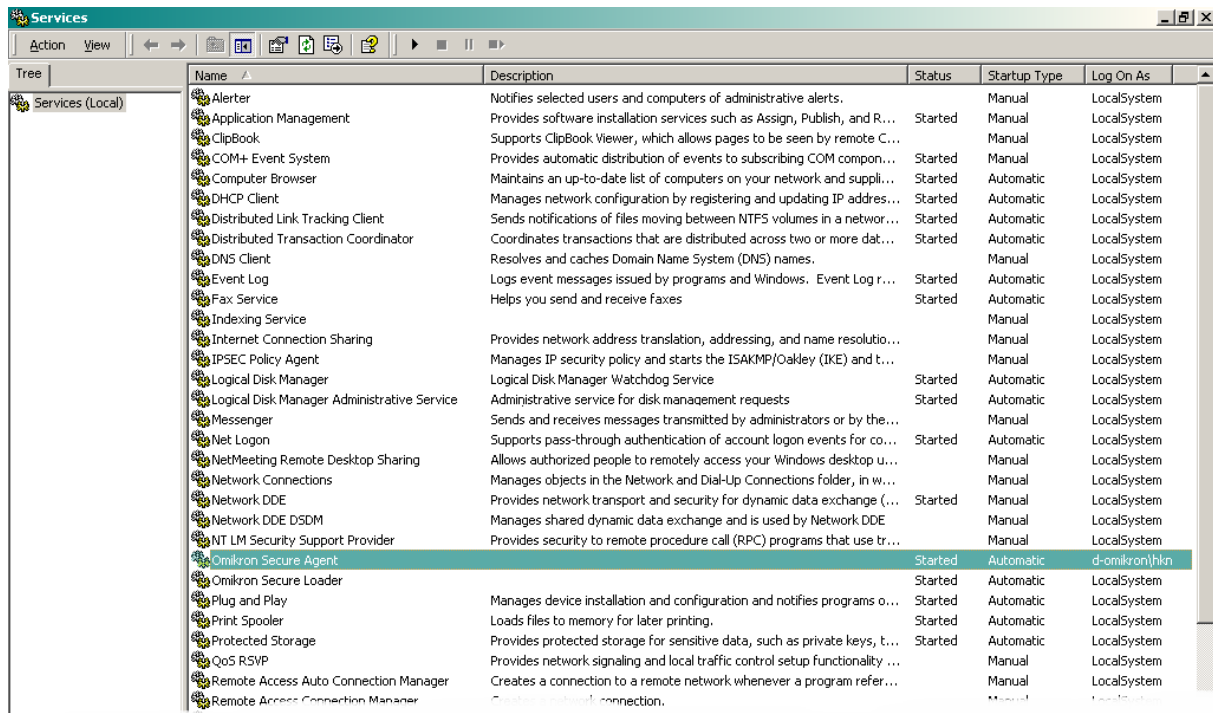


Choose the setup item

"Create icon for starting secure network version (NTFS-Security)"

and enter subsequently the user account name "MCSERVER" with password (must be repeated for security reasons).

4. Program files and service entries for the Omikron Secure Agent and the Omikron Secure Loader are created during the installation (the setup) of the application on the respective workstation:



Name	Description	Status	Startup Type	Log On As
Alert	Notifies selected users and computers of administrative alerts.		Manual	LocalSystem
Application Management	Provides software installation services such as Assign, Publish, and R...	Started	Manual	LocalSystem
ClipBook	Supports ClipBook Viewer, which allows pages to be seen by remote C...		Manual	LocalSystem
COM+ Event System	Provides automatic distribution of events to subscribing COM compon...	Started	Manual	LocalSystem
Computer Browser	Maintains an up-to-date list of computers on your network and suppli...	Started	Automatic	LocalSystem
DHCP Client	Manages network configuration by registering and updating IP address...	Started	Automatic	LocalSystem
Distributed Link Tracking Client	Sends notifications of files moving between NTFS volumes in a networ...	Started	Automatic	LocalSystem
Distributed Transaction Coordinator	Coordinates transactions that are distributed across two or more dat...	Started	Automatic	LocalSystem
DNS Client	Resolves and caches Domain Name System (DNS) names.		Manual	LocalSystem
Event Log	Logs event messages issued by programs and Windows. Event Log r...	Started	Automatic	LocalSystem
Fax Service	Helps you send and receive faxes	Started	Automatic	LocalSystem
Indexing Service			Manual	LocalSystem
Internet Connection Sharing	Provides network address translation, addressing, and name resolutio...		Manual	LocalSystem
IPSEC Policy Agent	Manages IP security policy and starts the ISAKMP/Oakley (IKE) and t...		Manual	LocalSystem
Logical Disk Manager	Logical Disk Manager Watchdog Service	Started	Automatic	LocalSystem
Logical Disk Manager Administrative Service	Administrative service for disk management requests	Started	Automatic	LocalSystem
Messenger	Sends and receives messages transmitted by administrators or by the...		Manual	LocalSystem
Net Logon	Supports pass-through authentication of account logon events for co...	Started	Automatic	LocalSystem
NetMeeting Remote Desktop Sharing	Allows authorized people to remotely access your Windows desktop u...		Manual	LocalSystem
Network Connections	Manages objects in the Network and Dial-Up Connections folder, in w...		Manual	LocalSystem
Network DDE	Provides network transport and security for dynamic data exchange (...)	Started	Manual	LocalSystem
Network DDE DSDM	Manages shared dynamic data exchange and is used by Network DDE		Manual	LocalSystem
NT LM Security Support Provider	Provides security to remote procedure call (RPC) programs that use tr...		Manual	LocalSystem
Omikron Secure Agent		Started	Automatic	d-omikron\hkn
Omikron Secure Loader		Started	Automatic	LocalSystem
Plug and Play	Manages device installation and configuration and notifies programs o...	Started	Automatic	LocalSystem
Print Spooler	Loads files to memory for later printing.	Started	Automatic	LocalSystem
Protected Storage	Provides protected storage for sensitive data, such as private keys, t...	Started	Automatic	LocalSystem
QoS RSVP	Provides network signaling and local traffic control setup functionality ...		Manual	LocalSystem
Remote Access Auto Connection Manager	Creates a connection to a remote network whenever a program refer...		Manual	LocalSystem
Remote Access Connection Manager	Creates a network connection.		Manual	LocalSystem

5. After the next system start (or manually using the service manager), these services are started automatically. Afterwards the application can be started by each user with its menu item.



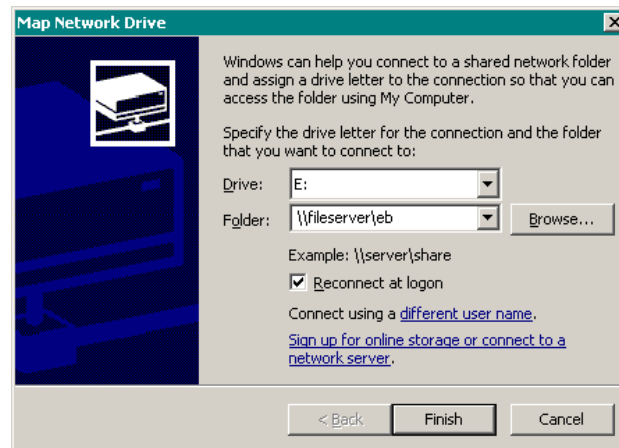
Please note:

For this, no drive DDE connection must exist any longer for the central resource on the respective client PC.

3.2 Preparations on all workstations

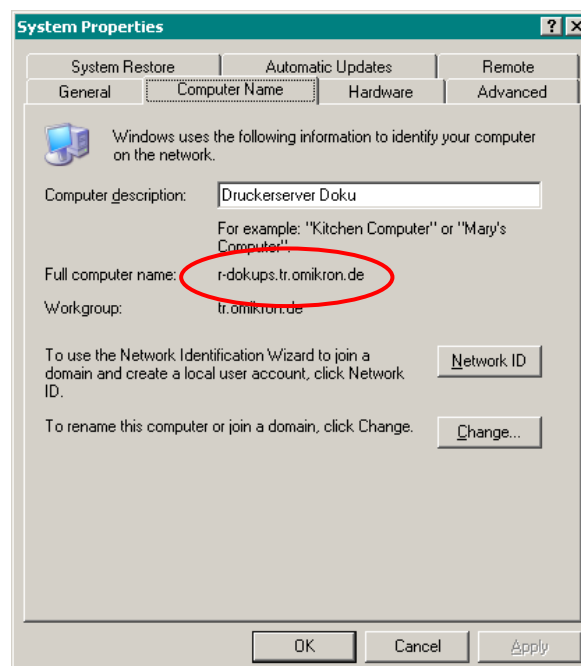
By means of the "Connect network drive" in the Explorer or file manager, a connection to the directory is established. Please make sure that the same letter is assigned to the drive on all PCs. You have to connect the directory as network drive even if installing on the file server. Once the letter is assigned, it is impossible to change it when the installation has been completed.

Example:



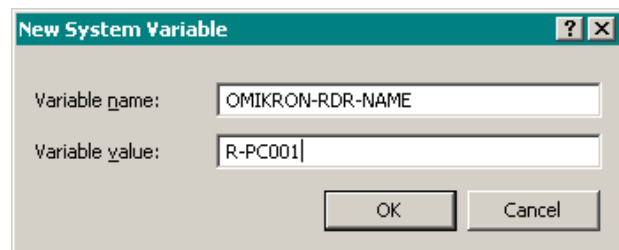
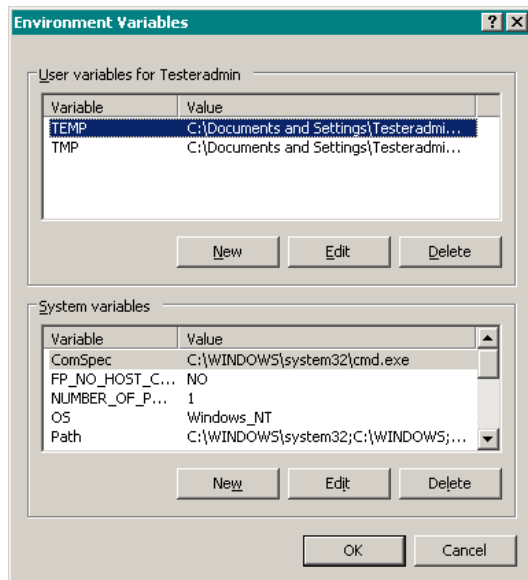
Alternatively you can directly use the so-called UNC names, i.e. the network resource is not assigned to a drive letter, but to the UNC name ('\\fileserver\eb' in our example) by entering it as route path when installing the software. This method has the disadvantage that the name and server cannot be changed at a later point.

For many functions, the program uses the name of the PC in the network. This name is unique within the network. The name of the PC can be seen e.g. in the properties of the desktop on the 'Computer Name' (WindowsXP) or 'Network Identification' (Windows2000) property page.



If you are using a network that does not support the static assignment of computer names, (e.g. NOVELL - Server), then it is possible to set this using an environment variable manually.

You can do this in the properties of the desktop on the "Advanced" property page using the "Environment variables" button. Then the entry would look e.g. as follows (the computer name may be up to 15 digits long):



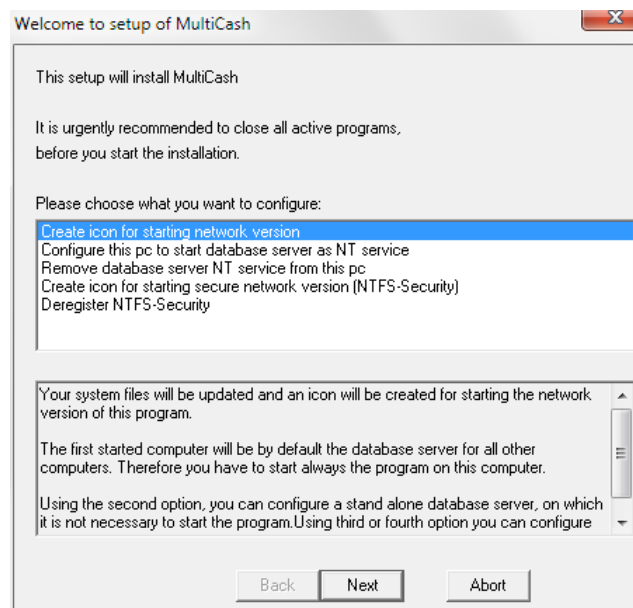
3.3 Installation of the software on other workstations

In the main path for the installation you selected, the installation routine for other workstations can be called. On the required workstation, start the program SETUP.EXE in the main path (e. g. 'E:\EB').

MCCWIN	15.02.2012 09:32
INTPIC.BMP	09.12.2002 11:00
mcc.sub	23.01.2012 11:14
mccDE.ino	10.01.2012 09:41
mccGB.inf	10.01.2012 09:41
MFC.ZIP	07.02.2012 10:52
SETUP.EXE	28.11.2011 16:55
SETUP.INI	27.03.2002 16:39
Setup.LogFile	15.02.2012 09:32
SETUPINF.INI	15.02.2012 09:32

Under operating systems of the generation starting from Windows Vista / Windows 7 , please deactivate only for the configuration of the network clients the user account control, if possible

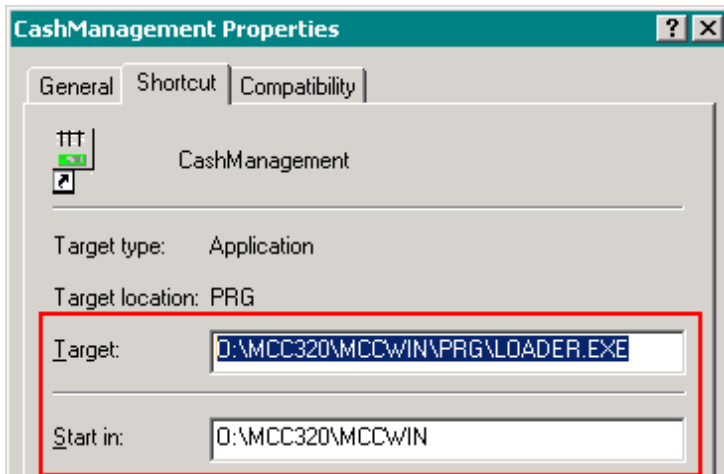
Start SETUP.EXE with administrator profile. After double-clicking setup.exe, the following selection option appears.



Choose there the standard option "**Create icon for starting network version**". Here some system files will be checked and an icon for starting the network version will be created.

**Please note ...**

For installations with drive mapping and activated user account control under operating systems of the generation starting from **Windows Vista / Windows 7**, the UNC path is entered in the program shortcut instead of the connected drive. This is caused by the fact that for the administrator logged on for the installation the drive shortcut is not available. In this case, please change the paths in the properties of the program shortcut accordingly:



Starting from program version 3.22.006, here the path is entered automatically, under which the system has been installed on the server, so that here a correction is no longer required.

**Please note:**

After the update of the network version the central setup can be started once again on the clients from the server resource. By this, the old registry entries of the signature environment will be removed. This step is technically not required, but the only way to remove the registry entries completely. This functionality will not be contained any longer in later versions, since then the setup creates only the program shortcut on the clients.

If you like to accomplish an automatic software installation on the network PCs by using tools like Netinstall or the like, you can do with the setup program as follows:

The setup program on the central server partition can be called with the parameter /AUTO. Then the program shortcuts and the registration of all installed ES modules are made automatically without any user interaction. If the parameter /SILENT is used additionally, no screen output occurs during the installation.

Note: the sequence of the parameter calls must be: SETUP /AUTO /SILENT. Please call always with capital letters!

The central client setup can also be called for the NTFS shortcuts in an unattended mode, so that also for this operating option an automatic installation with appropriate tools is possible, which run under an administrator identification. For NTFS security setup.exe need to be called with "/AUTONTFS /USER:<username> /PASS:<password>". Here user identification and password have to be passed on for the "MCSEVER" user, who has access to program resources (see Chapter 3.1.5).

4 Update over an older version

In principle with a program update we try to transfer all data from the old system fully automatic, so that work can be continued without any further interventions. Nevertheless changed requirements with "large" version changes can cause fundamental changes in the program flow, which make manual examinations and possibly interventions necessary.

First some fundamental prefaces to release politics and compatibility between the components of the program's environment: All components of Omikron systems are provided with unique six digits version numbers, which have the following meaning:

Position 1:	Platform version	This number labels the fundamental technical platform of the development, e.g.: 1 = DOS programs 2 = Windows 16bit programs 3 = Windows 32bit multi-thread programs
Position 2 to 3:	Program version	This version number is increased, if functional extensions or changes (particularly in the data structures) were accomplished.
Position 4 to 6:	Program release	With eliminations of errors and changes in detail, which do not affect the compatibility, only the release number is increased.

Based on these specifications it is simple to realise that, that e.g. modules with the version numbers 3.00.005 and 3.00.138 can be used together, however such with version 3.01.005 and 3.20.005 normally not.

For a simple change of the release, e.g. from 3.20.006 to 3.20.007 only the installation routine has to be called. Therefore the hints described in the following only apply to an update of program versions or platform versions, thus e.g. from version 3.01.XXX to 3.20.XXX.

In principle the conversion routines are carried along over several program versions within the applications, so that in principle the skipping of a program version is possible is (e.g. from version 2.12.XXX to 3.20.XXX). However we cannot guarantee (and we also cannot provide any support for this), that after this everything works smoothly, since we only can accomplish update tests with the last program version in each case. Thus we recommend to avoid skipping of program or platform changes.

4.1 Prior to the update installation

The update installation of a system, which is complex and important for the everyday business, requires thorough preparation and a systematic procedure, also allowing to reset in the case of problems. If you are not sure how to proceed or if you have special questions concerning your system environment, please contact your Omikron partner **before** the installation.

4.1.1 Existing modules

Please check that all modules, which were installed in the old version, are available on the installation CD of the new version. After the installation of the new version old modules possibly are no longer executable.

4.1.2 Pending transmit sessions

Please execute now first all transmit sessions to the bank in order that no open items remain in the file manager.

4.1.3 Audit trail of settings

Before the update you should document the settings important for you (if not already happened with the first setup of the system). It is then easier to check the settings after the update. These are:

1. User administration: Function and data profiles
2. System parameters
3. WVD files
4. Predefined reports

Hint: This information can be printed out starting from version 3.20, in order to facilitate the documentation.

4.1.4 Backup

In any case, please run a backup **BEFORE EXECUTING THE UPDATE**. A useful proceeding is to copy the content of the complete program's basis path into another directory.



Please note:

The backup should comprise also the storing of the ADMIN2 master password file, which is usually present on disk, since it is converted with the first start of the version 3.20. In the case of restoring of an older version the access is only possible using this also stored ADMIN2.MPW belonging to the older version.

When changing an environment with a version of the Electronic Signature before 3.01.008 to version 3.20, you should also save the key files on your signature diskettes, since here also the keys which have been used once in the new version are not identified any longer by the old program version.

4.1.5 Change of installation path

We recommend, not to change the program path. If you would like to install the new version in another directory or another network resource than the old version, please contact your Omikron partner **before** the installation.

4.2 Installation

Install the new version into the original basis path of the old version (normally this path is prompted automatically, if an installation has already been accomplished on your computer). Then all data and settings will be transferred as far as possible to the new version and converted automatically. Thereby the programs of the old version are deleted and cannot be not executed any longer.

4.3 After the update installation

As far as possible, all settings and data from an old version are taken over. Due to program enhancements, usually new functions, settings and access rights were added, which require if necessary manual adjustments. In the following, you'll find several comments on what you should pay attention to / check after an update installation:

4.3.1 Databases

On the first program startup, all necessary data bases are converted automatically.



Please note absolutely:

After having started the version 3.20 for the first time, you may never restore backup files from the old version into the system, because they cannot be converted then and this will cause errors.

4.3.2 Users/Access rights

All users and user groups from an old version are taken over, as well as their respective access rights. New functions and with this new acces rights are deactivated by default.

However if function profiles for functions already **existing** are introduced, these new rights are activated by default, so that all existing functions can be used.

After the installation is completed, please check all user / user group access rights and correct them if required.

4.3.3 Users/Data profiles

The data profiles are taken over as far as possible. However, you should check all users' / user groups data profiles since some fields have been changed in structure and new fields have been added.

Hint: The data profiles can be printed from version 3.20 on.

4.3.4 Parameter settings

Partly, new functionalities have been added, requiring new system parameter settings to be implemented.

Please check the system parameters on all workplaces and in all modules, as well as the Communications parameters in the Core module.

**Please note:**

In Version 3.20, the allocation of parameters to computers, users and the system has been consistently restructured. For this reason, you should check the parameter settings carefully.

4.3.5 WVD files

Because of extensions of the data bases we cannot guarantee in either case that the WVD files can be used further without any change. Partly, the fields have been extended as well, which may affect your export files.

From WVD files important for you you should note the field sequence and the structure of the WVD file within the old version.

**Please note:**

Please check all your import/export files and, if required, adjust them or create new ones. They should be stored in either case, even if no obvious change can be seen.

Hint: WVD files can be printed out starting from version 3.20.

4.3.6 Backup

In principle the stored data always belong to a respective program release. A backup from an older program version should never be restored into the current version.

We recommend to make a backup immediately after finishing the update work and checking the installation.

4.3.7 Output orders/Autoroutine

All output orders will be taken over from the old version. Because of enhancements in databases we cannot guarantee in each case, that you can use your output orders any longer unchanged.

**Please note:**

Please delete all your output orders and create new ones.

5 Getting started

Before you start the program for the first time,

- Windows must be running and
- you must have installed the program modules.

The icon for the Core module is found in the program group that was created during the installation of the program system.

To start the Core module, click on the start menu entry or double-click on the shortcut icon on the desktop.

The program has a **start user name**, which you should only use for user validation the first time you start the program and which you should use in case of blocking all other users.

This start user name is: **ADMIN2**.

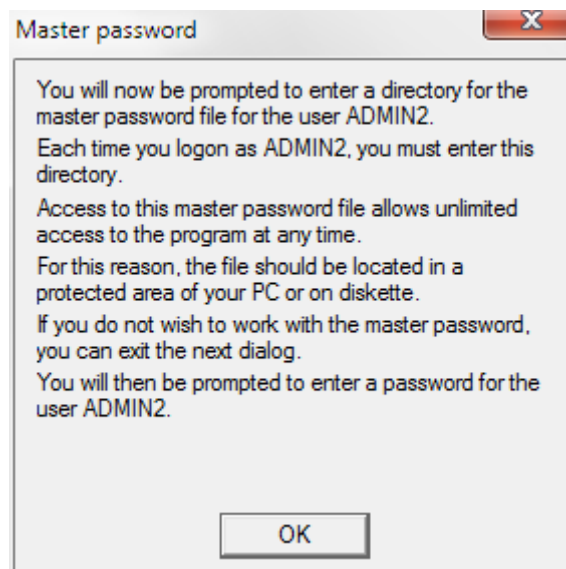


Please note absolutely:

The access with the ADMIN2 ID is the ultimate possibility to start the program if all other users have blocked themselves. This occurs more often than you first think. For this reason, there are two options for the creation of this user:

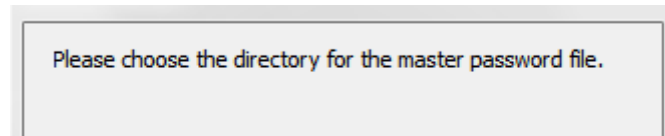
1. Access using a master password file (MPW file). In this case, you require access to this file for the access, but no password.
2. Access using a password. In this case, you require the password, but not the MPW file.

With **alternative 1** you are prompted to select a directory for the master password file which can be stored for the user ADMIN2. At each later logon as ADMIN2 you have to enter this directory again. The access to this master password file provides unrestricted access to the program at any time. Therefore this file should be stored in a protected area on your computer or on a data storage medium.

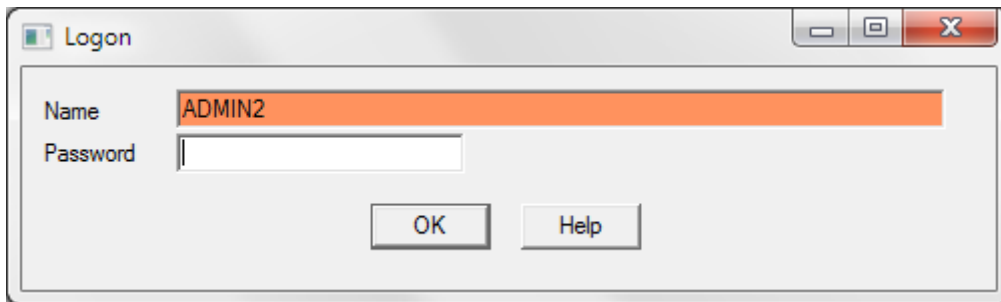


Confirm this message concerning the master password file with [**OK**].

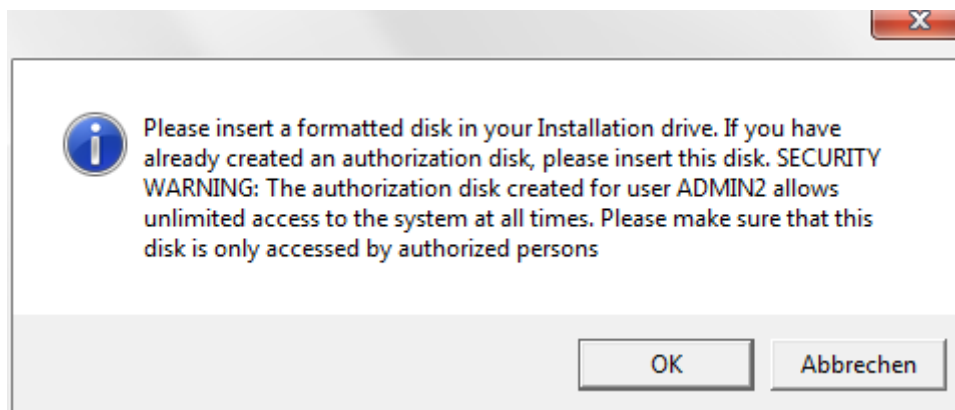
Then a directory overview is shown, where you can select the directory for storing the master password file by mouse-click. If necessary, you can create a new directory using the [**Make new folder**] button. Confirm your entry with [**OK**].



After this you must log on for the first time. Enter the start user name "admin2" in the "**Name**" box in the User Validation dialog box. Press <TAB> to skip the password box and then confirm your entry of the start user name by pressing <Return> or clicking on [OK].



If you have selected a floppy disk drive/a removable data carrier drive as storage location for the master password file before, you are now requested to insert the data medium. Confirm this prompt with [OK].



Do not write-protect the data storage medium because the program must write data to it. Possibly arising error messages can also be confirmed with [OK].

If you start the program at a later date and try to log on as user "admin2", you will be asked to enter the directory or to insert the data storage medium with the master password file.

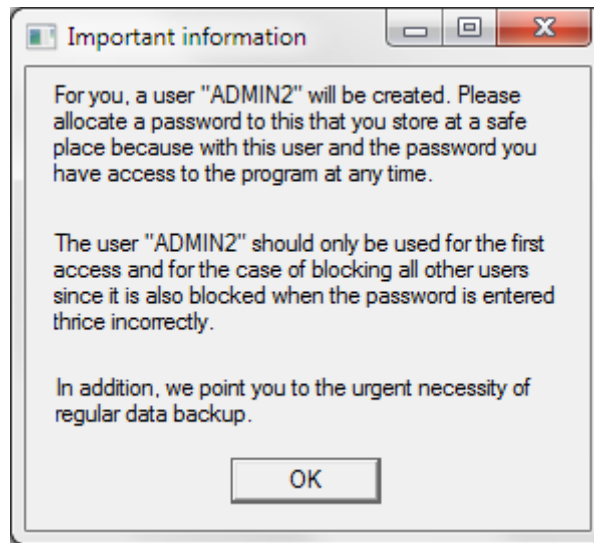
The program will read the information saved on the medium and - as long as the information on the medium matches the data saved by the installation routine on the hard disk - will allow you access to all of the program's functions.



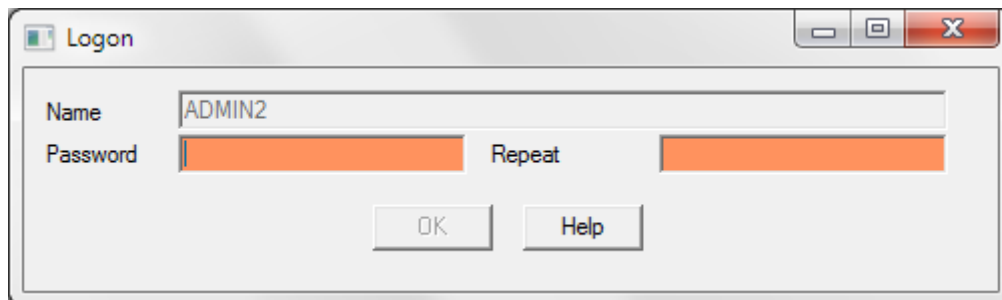
Please note absolutely:

Keep, if you store the master password on a removable data storage medium, this medium at a safe place. If it is necessary to completely re-install the user administration data, it will allow you to log on to the system at any time as system administrator with unrestricted access using the start user name.

If the dialog is cancelled, that means you wish to work **without master password**, the user ADMIN2 is registered and a password must be assigned. Close this message with [OK].



Subsequently, enter the password, repeat it and confirm with [OK].

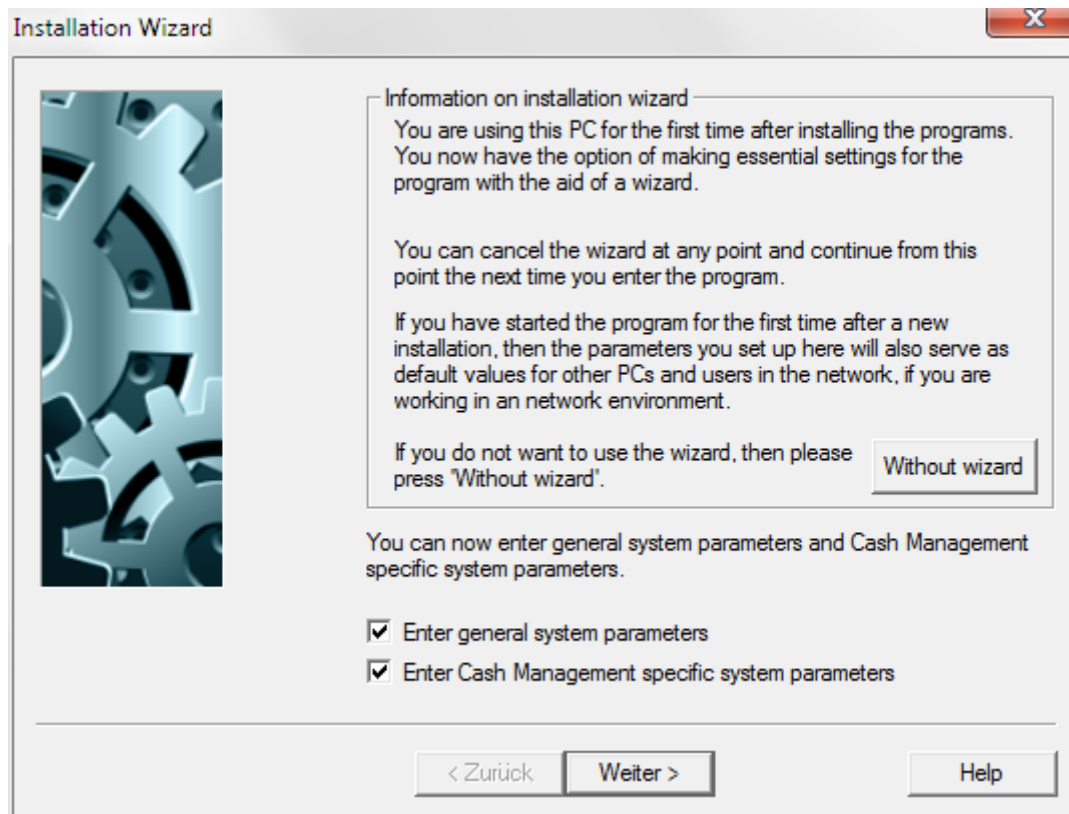


5.1 What to do next ... / Configuration Wizard

The Configuration Wizard will guide you through the first steps that are normally needed after you have installed the program (parameter settings for the system, printing, comms. etc.). You can close the wizard at any time and return to the same point, the next time you start the program.

When you start the program for the first time after a new installation, the parameters, which you set here, will also serve as the default values for other systems in the network, if you are working in a network environment.

If you want to define the settings and parameters without using the wizard, simply click on [**Without Wizard**].



If you accept the assistance of the wizard, it will guide you through the steps necessary to configure the software for operation on a new system:

1 Initial configuration of the software

First, please set the **general system parameters** for the program and the **system parameters specific for Cash Management**. To do so, click on the appropriate check boxes, then click on [**Next >**] and make the desired parameter settings.



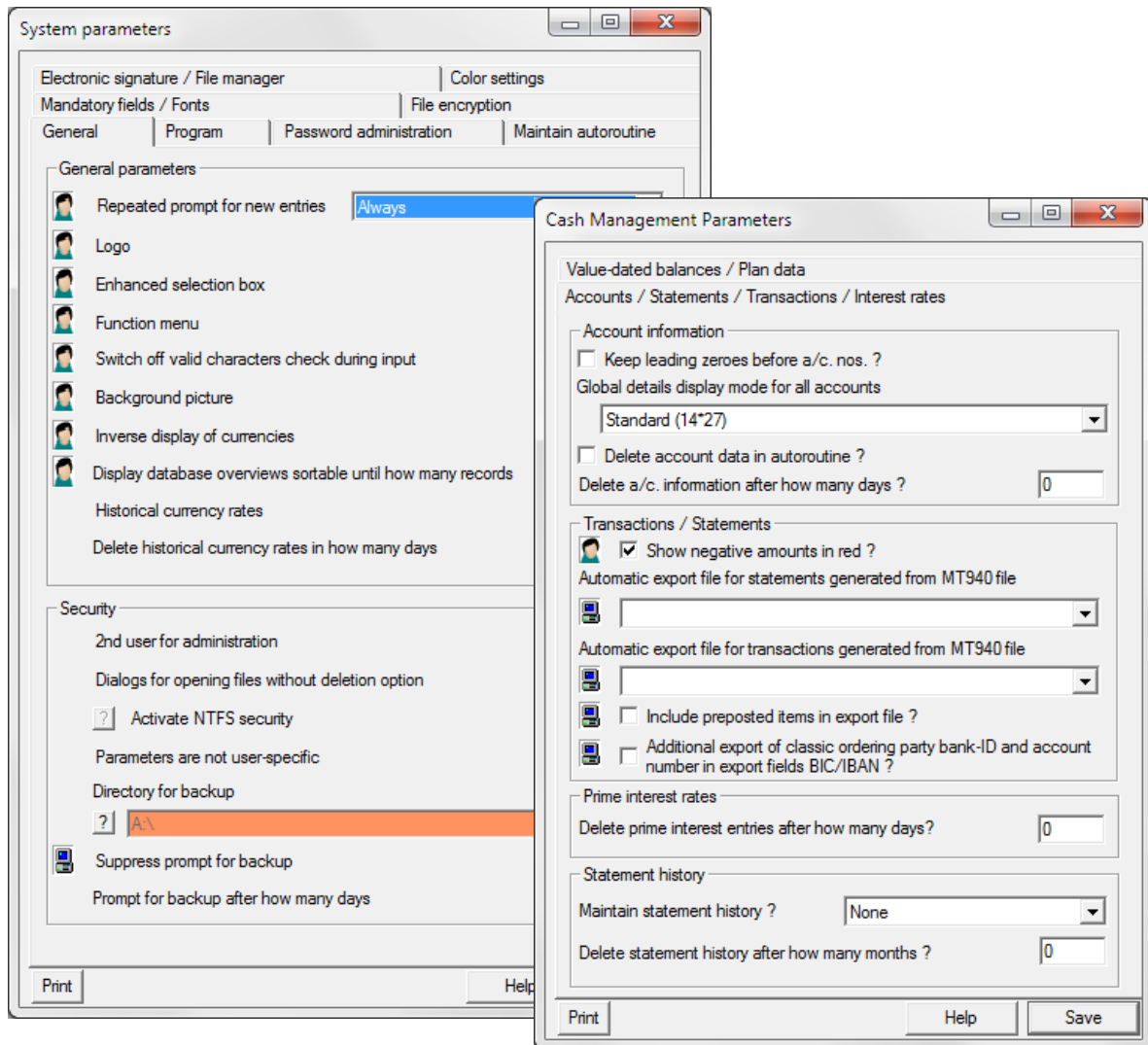
Please note ...

You should activate especially the local **data encryption** in the system parameters on the appropriate property page. Then, files like payment files, collected account information will be protected against unauthorized viewing by automatic encryption as soon as they are opened by the application. Which groups of files are to be encrypted, can be defined here individually.

Once encrypted, the files remain encrypted. Only the application can read these files. If you have not chosen any individual encryption password, these files can be processed with each installation of the program system.

Information regarding the individual parameters can be found in Chapter 6.1: *System parameters* and 6.2: *Cash Management system parameters*.

Finally store your parameter entries in each case using the [Save] button.

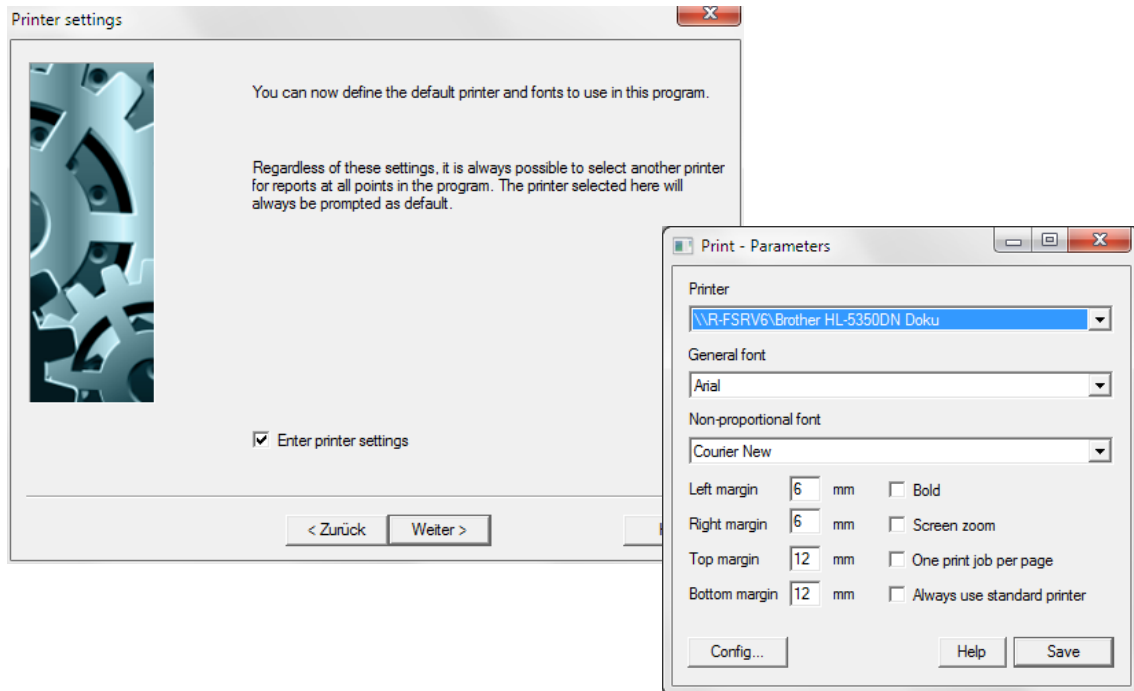


Please note ...

In the system parameters, the specification of the supported signature solution is important. If applicable, this must be repeated later on the individual computers in the network (hardware and floppy drive settings can also be made by the user).

2 Printer parameters

Here, you can set the printer that should normally be used by the program and the default fonts. Regardless of the setting made here, it is always possible to select different printer before printing from the program. The printer selected here will always be suggested as the default printer. To configure the printer parameters, click on the check box "**Configure printer parameters**" and then click on [**Next >**]. Then configure the printer parameters.



Additional information on how to do this is contained in Chapter 4.5: *Print parameters*. Finally store your printer parameter settings by clicking the [**Save**] button.

3 Create user SYSADMIN

You can now create a user SYSADMIN, which is authorised to perform all program functions. You only need to assign a password for this user.

The user SYSADMIN is intended for handling system administration tasks. In contrast to the ADMIN2 user he will be displayed in the user administration, that means that his access rights can be restricted.

If the user SYSADMIN already exists, the corresponding fields here are blocked.

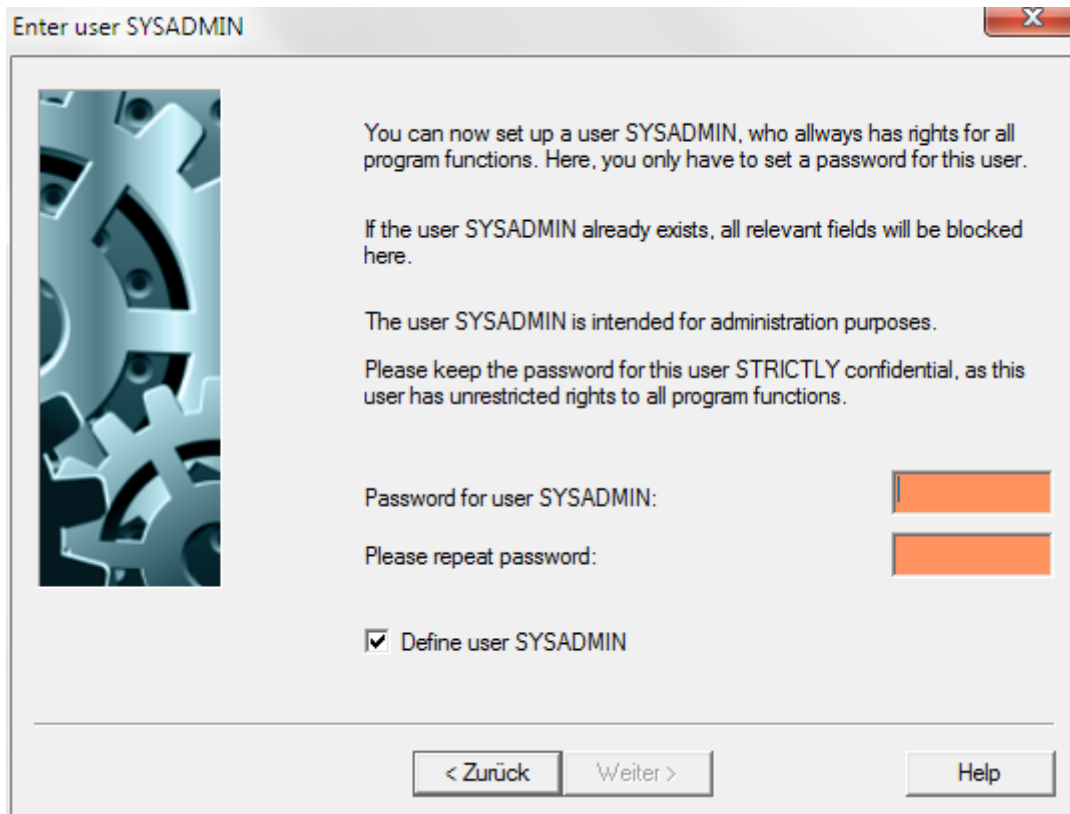


Please note:

Please make certain that this password is kept absolutely secret, since this user has unrestricted access to every program function.

As the **password for the SYSADMIN user** is entered in hidden mode, i.e. each key stroke is represented by an * sign (asterisk), you must enter the password a second time in the appropriate field to ensure that it was entered correctly.

Afterwards, click on the check box "**Define user SYSADMIN**" and then click on [**Next >**].



Enter user SYSADMIN

You can now set up a user SYSADMIN, who allways has rights for all program functions. Here, you only have to set a password for this user.

If the user SYSADMIN already exists, all relevant fields will be blocked here.

The user SYSADMIN is intended for administration purposes.

Please keep the password for this user STRICTLY confidential, as this user has unrestricted rights to all program functions.

Password for user SYSADMIN:

Please repeat password:

☒ Define user SYSADMIN

< Zurück Weiter > Help

4 Creating user groups

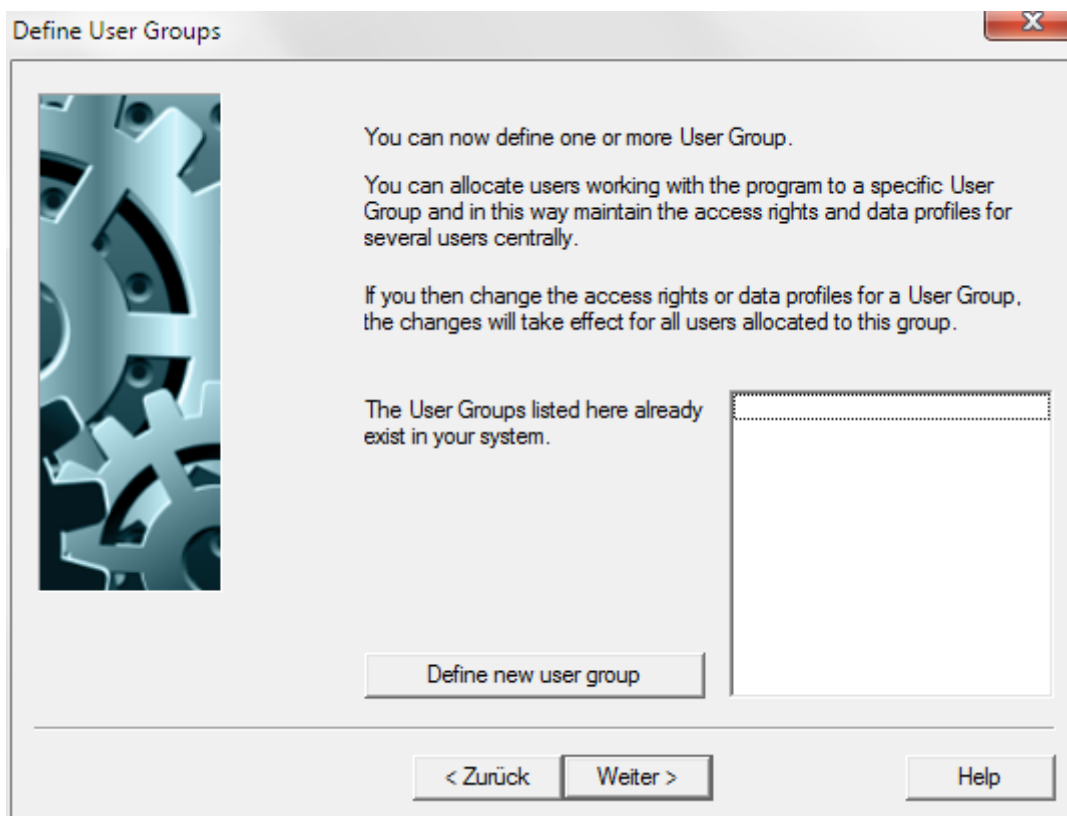
At this point, you can create one or more user groups. You can organise the program users into groups and thus centrally administer the functional profile and the data profile for several users. If you change the functional profile or the data profile for a user group, this change will apply for all the users in the group.

If user groups have already been set up on your system, they will be listed here.

To create a new user group, click on the check box [**Define new user group**] button and then click on [**Next >**]. Afterwards, create a new user group. Information about this is contained in Chapter 5.3:

User group administration.

Store your entries for the individual user group in each case by pressing the [**Save**] button afterwards. The program returns then in each case to the initial dialog. If you do not wish to create a further user group, click on the [**Next**] button.



5 Creating users

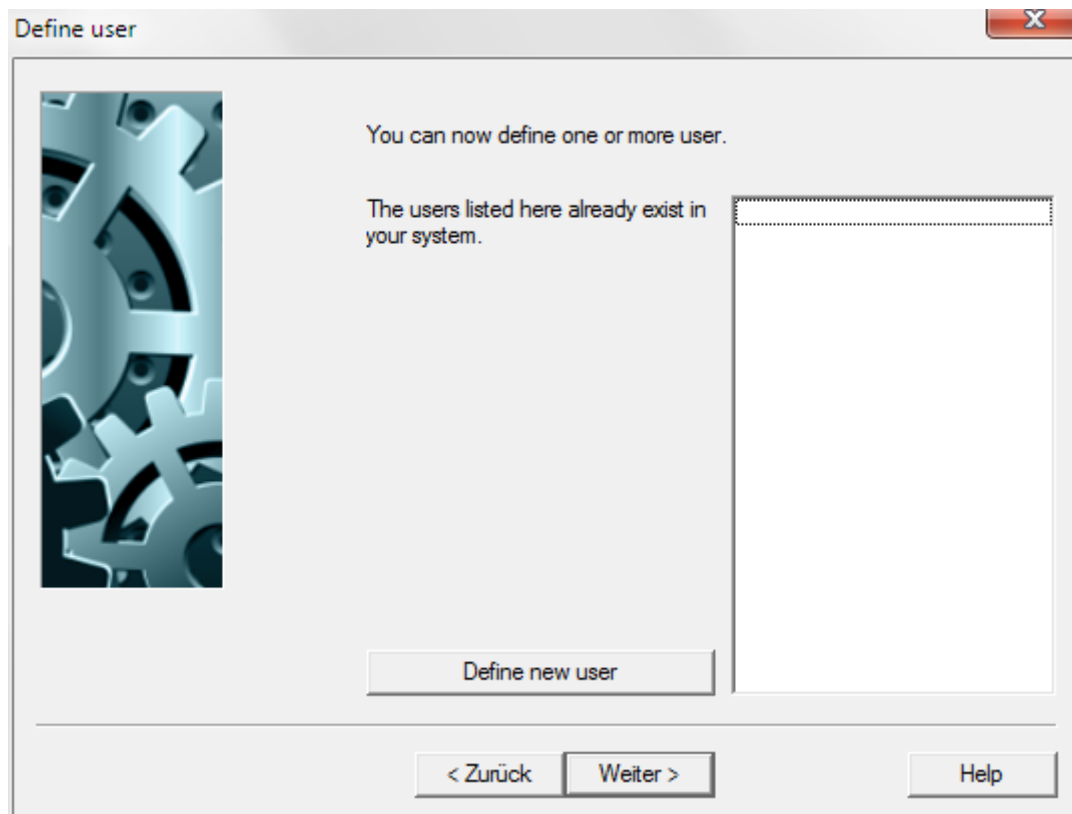
Now, you can create one or more users.

If users have already been set up on your system, they will be listed here.

To create a new user, click on the **[Define new user]** button and then click on **[Next >]**.

Afterwards, create one or more new users. Information about this is contained in Chapter 5.4: *User administration*.

Store your entries for the individual user in each case by pressing the **[Save]** button afterwards. The program returns then in each case to the initial dialog. If you do not wish to create a further user, click on the **[Next]** button.



6 Comms. parameters

Here, you can configure the communications parameters for this system. You must specify which communication paths are supported and, by assigning priorities, specify how these communication paths to the bank should be used. To do so, click on the check box **"Define Comms Parameters"**, then click on **[Next >]** and make the desired parameter settings.



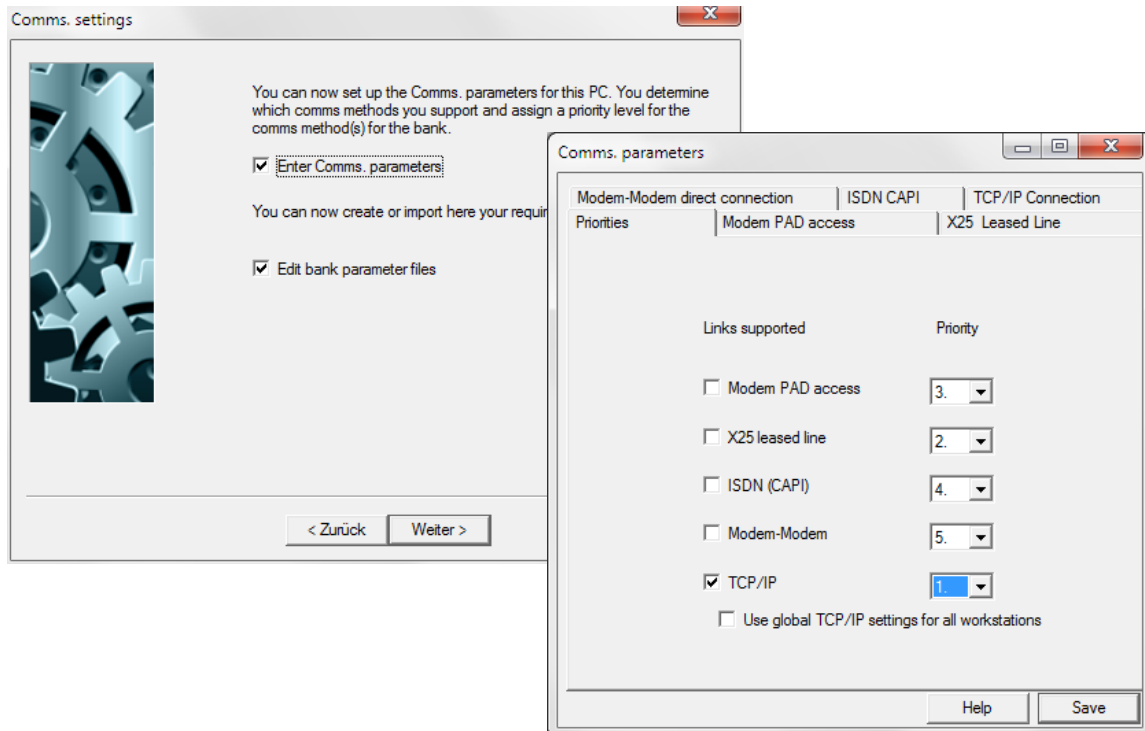
Please note ...

These settings are maintained separately for each computer in the network, since in each case different communication adapters could have been installed (e.g. ISDN adapter). Set these parameters only on computers which really should execute Comms.

Exception: TCP/IP parameters can be set for all computers globally.

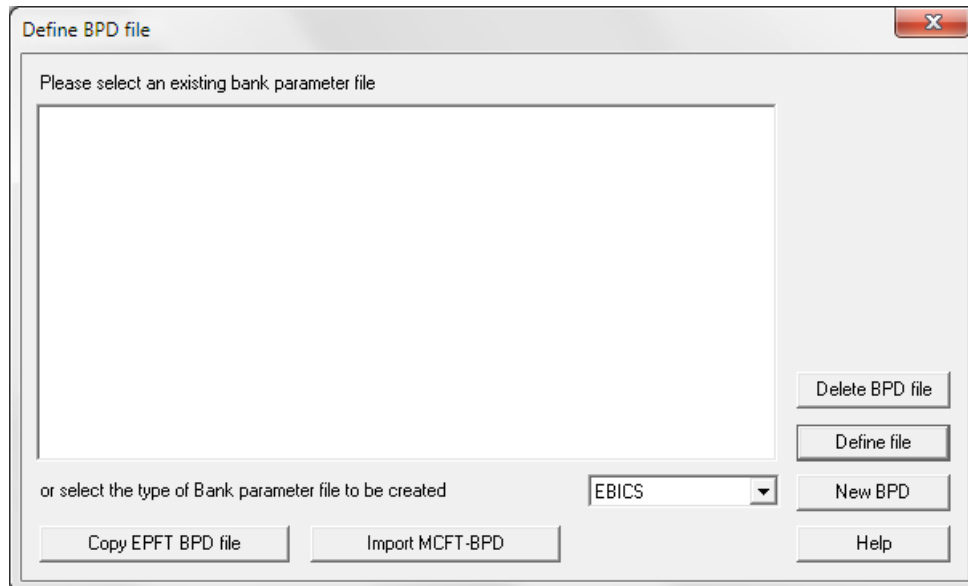
For this, first keep the already highlighted check box **"Enter Comms. parameters"** activated. Then press the **[Next >]** button and enter the **Comms. parameters** subsequently.

Information regarding these settings can be found in Chapters 2.1 - 2.7 of the Comms. module. Finally store your Comms. parameter settings by clicking the **[Save]** button.



7 Edit bank parameter files

If you let the default of the already marked check box "**Edit bank parameter files**" unchanged, the dialog for importing or editing bank parameter files will be opened afterwards.



If you received bank parameter files from the bank, then you import them into the system depending on the procedures using the [**Copy EPFT BPD file**] or the [**Import MCFT BPD**] button. With other procedures e.g. like FTAM or FTP you have to select the procedure using a list box and then to create a new bank parameter file by clicking on the [**New BPD**] button. There you enter then the data provided by the bank.

Information regarding the settings you can find in chapter 3.1 of the documentation for communication: *Create BPD*. [**Save**] all of your entries also in this case.

Example: Editing of an EBICS bank parameter file

After choosing "EBICS" (appropriate Comms. module need to be installed) and selecting the [**New BPD**] button the input mask for the EBICS bank parameters opens:

Choose a bank access from the list of known EBICS bank systems in a second mask and confirm with [**Save**].

Select EBICS bank access

You can select here from the list the suitable one of the EBICS bank systems known by the program, in this process many parameters will be added.
If your bank is not recorded here, you can cancel and add the data manually from the letter of your bank !

Predefined parameters of the EBICS bank access activated below:

URL of bank:

Host name:

Protocol version:

Alphabetical list of known bank accesses for EBICS:

- APO-Bank, Deutsche Apotheker- und Ärztebank
- Bank Austria H002
- Bank Austria H003
- Bank für Sozialwirtschaft AG
- Bankhaus Max Flessa KG
- Bankhaus Neelmeyer
- Bankhaus Plump
- BNP Paribas Fortis
- BTV, Bank für Tirol und Vorarlberg AG
- Commerzbank ..

Help Save

The associated data like bank URL, host name, hash values then fill the appropriate fields in the EBICS bank parameter mask.

Here you have to fill the appropriate field with the customer ID from the bank letter and to allocate the individual user IDs (external names) to the configured users (internal names) using the [**New user**] button.

We recommend on the one hand to store the **Comms. password** of the individual users in the file.

Beyond that we recommend to define one user as **default user**. Thereby the creation of Comms. orders by users not authorized to sign as well as the automated call of information for the distributed signature are made possible. Please contact your bank whether special requirements must be met for this.

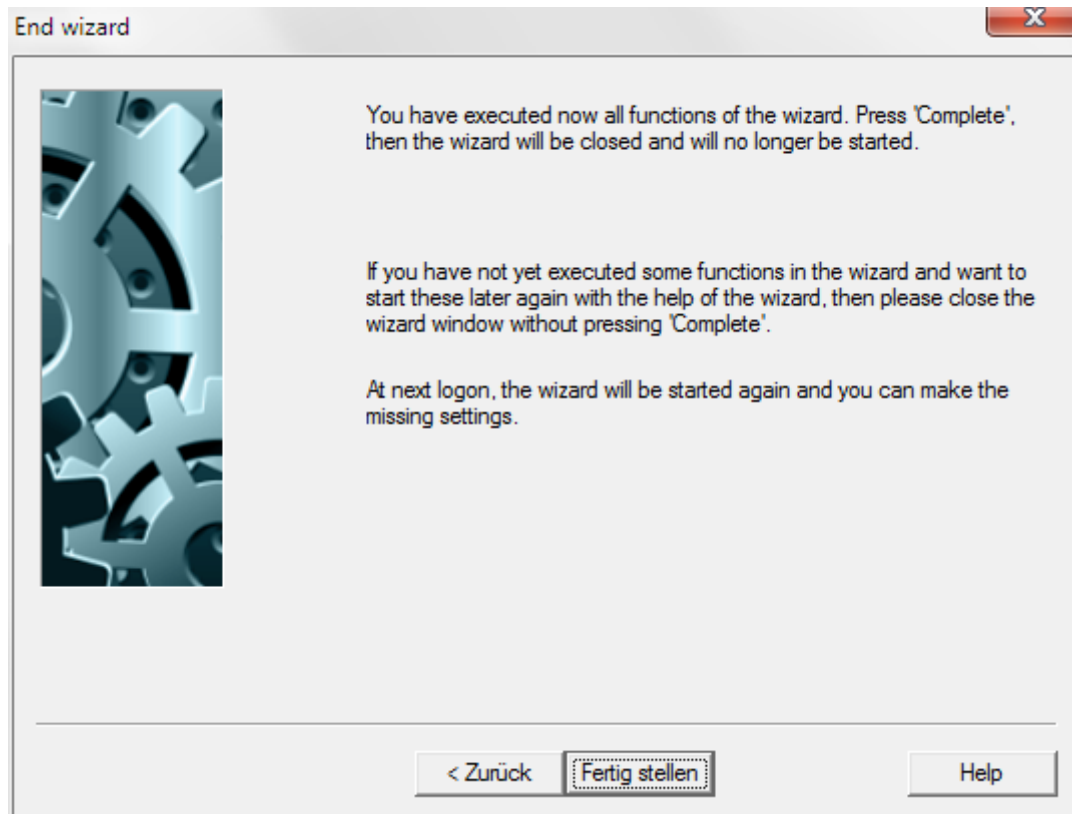
Finally, [**Save**] your entries.

If you do not like to maintain another bank parameter file, deactivate the "**Edit bank parameter files**" button and click on the [**Next >**] button then.

8 Completing the Configuration Wizard

You have now completed all of the necessary steps in the configuration wizard. When you click on [**Finish**], the wizard will be closed and will not be started again.

If there are still some functions that you have not configured using the wizard and you wish to have the assistance of the wizard to complete these later, please close this window via close button **without** clicking on [**Finish**]. In this case, the wizard will be started again the next time you start the program and you can configure the sections that have not yet been completed.



By clicking on [**< Back**] you can step back through the individual steps to make any changes that are needed.

Once you have completed the steps detailed above, the configuration of your computer has been in largest part completed. If you have installed supplementary modules, start them one after the other using the toolbar in the Core module. Each module has its own system parameters, export routines, etc., to allow you to adapt the applications as needed. The relevant information can be found in the Help systems and User Manuals for the individual applications.

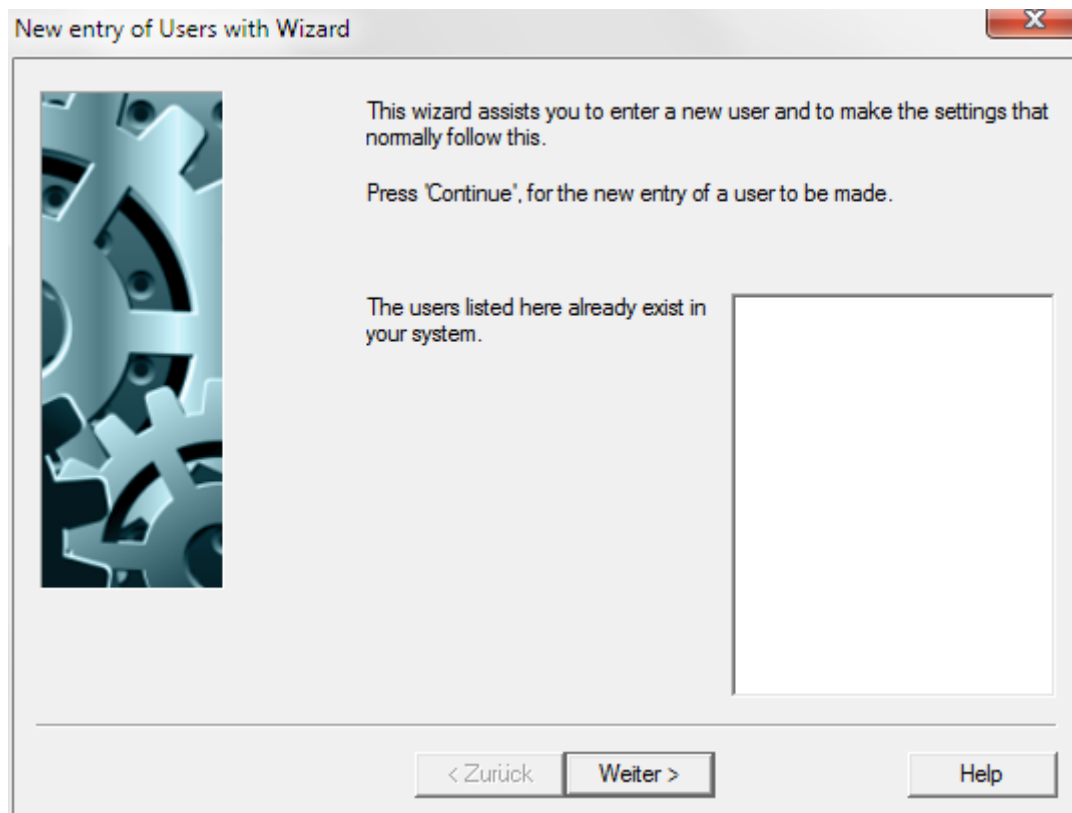
5.2 New entry of a user with the wizard

To enter a new user, you can take advantage of the assistance of a wizard by selecting the menu item **-New user with wizard-** in the **-User-** menu.

The wizard will guide you through the steps that are required in order to enter a new user, assign the new user the appropriate access rights and data profile and to enter the user in the corresponding bank parameter files:

1 New entry of user with wizard

First, an overview window will display a list of all the users that have been entered into the system.



After you click on [**Next >**], you can enter a new user as described in Chapter 5.4: *User administration*.

If users have already been entered, their function profiles and data profiles can be transferred and adapted.

Using the **function profile** you control the access of the user to individual functions (e.g. menu items). A green hook stands for a function which is accessible for the user.

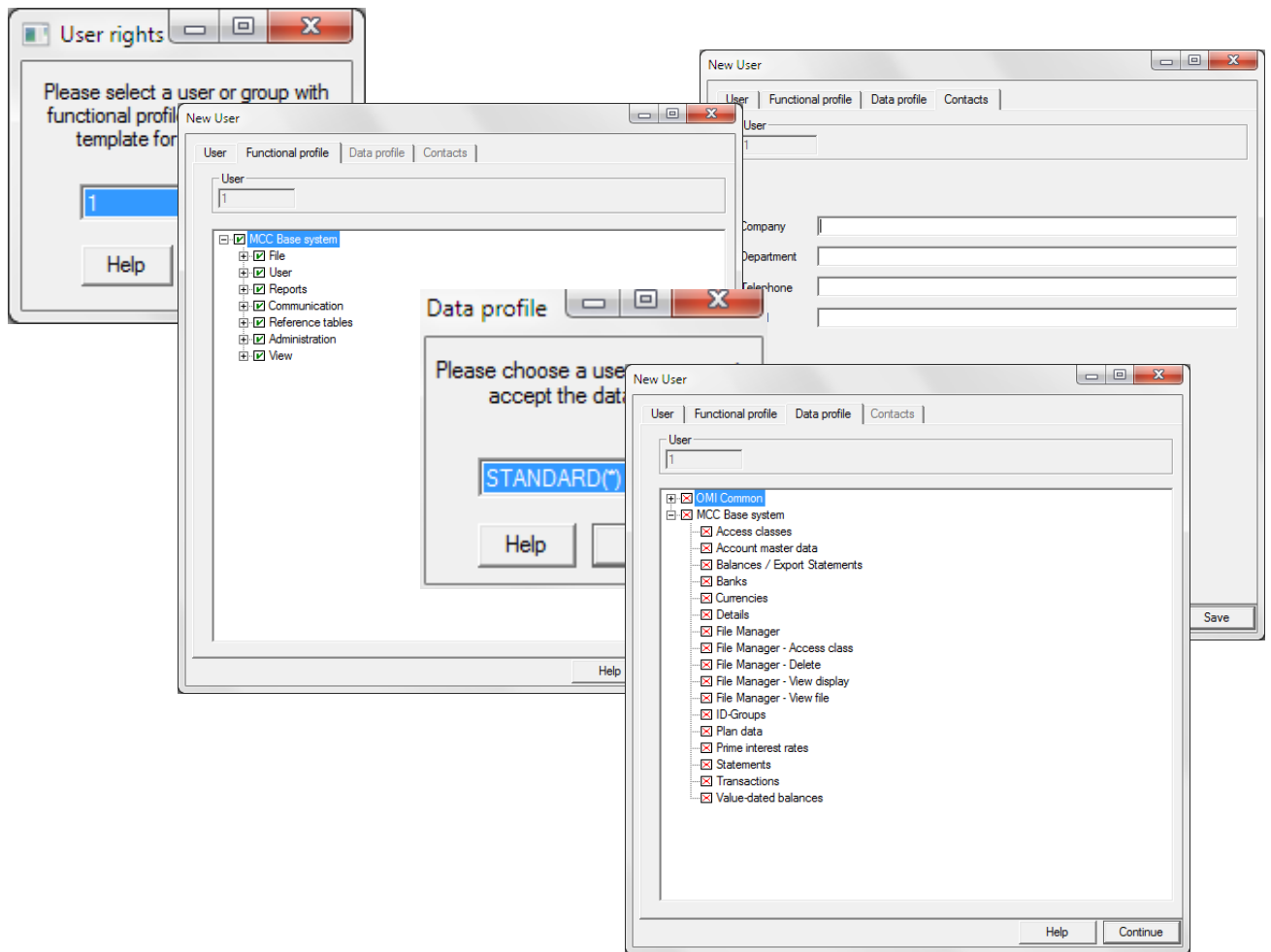
Using the **data profile** you limit the view of the user to certain data within a function. As soon as the access to data within a certain function is limited in any way, this data profile can be identified by a green check mark.

The access rights are represented in a transparent tree-view in each case. The rights can be set by mouse-click (activate/deactivate).

After double-clicking a data profile entry another dialog box opens, where you define the exact criteria (see page S. 28).

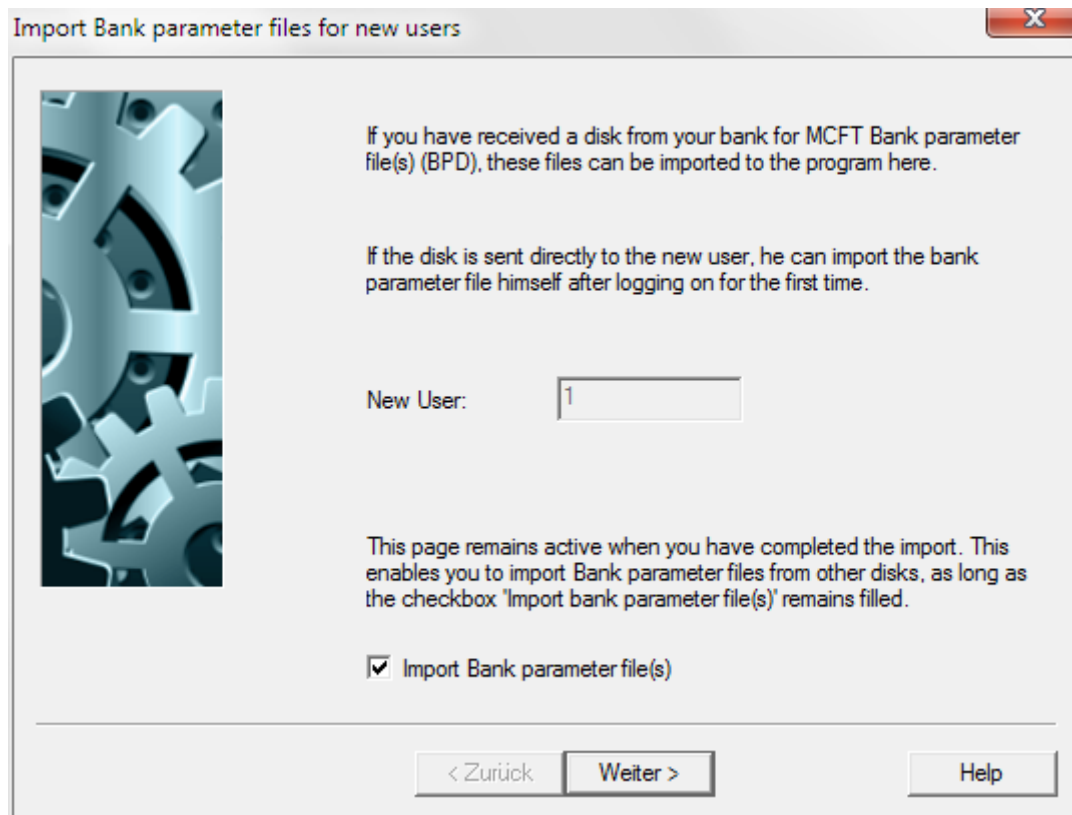
In order to ensure the consistent maintenance of the data profiles for all modules used, a **global data profile** for the fields access class, account group and/or organizational unit (if appropriate module is installed) can be defined, that takes effect to all functions and modules, which contain these fields.

In addition, you can use pre-defined data profiles (see chapter 3.3: User groups and access class for confidential payments). By allocation of the users to certain user groups the users assume standardized data profiles (e.g. access to salary data only for employees of the payroll accounting).



2 Import bank parameter files for a new user

If you received a diskette from your bank with bank parameter files (for the EPFT or MCFT procedure) for the new user, you can import these at this point.



Import Bank parameter files for new users

If you have received a disk from your bank for MCFT Bank parameter file(s) (BPD), these files can be imported to the program here.

If the disk is sent directly to the new user, he can import the bank parameter file himself after logging on for the first time.

New User:

This page remains active when you have completed the import. This enables you to import Bank parameter files from other disks, as long as the checkbox 'Import bank parameter file(s)' remains filled.

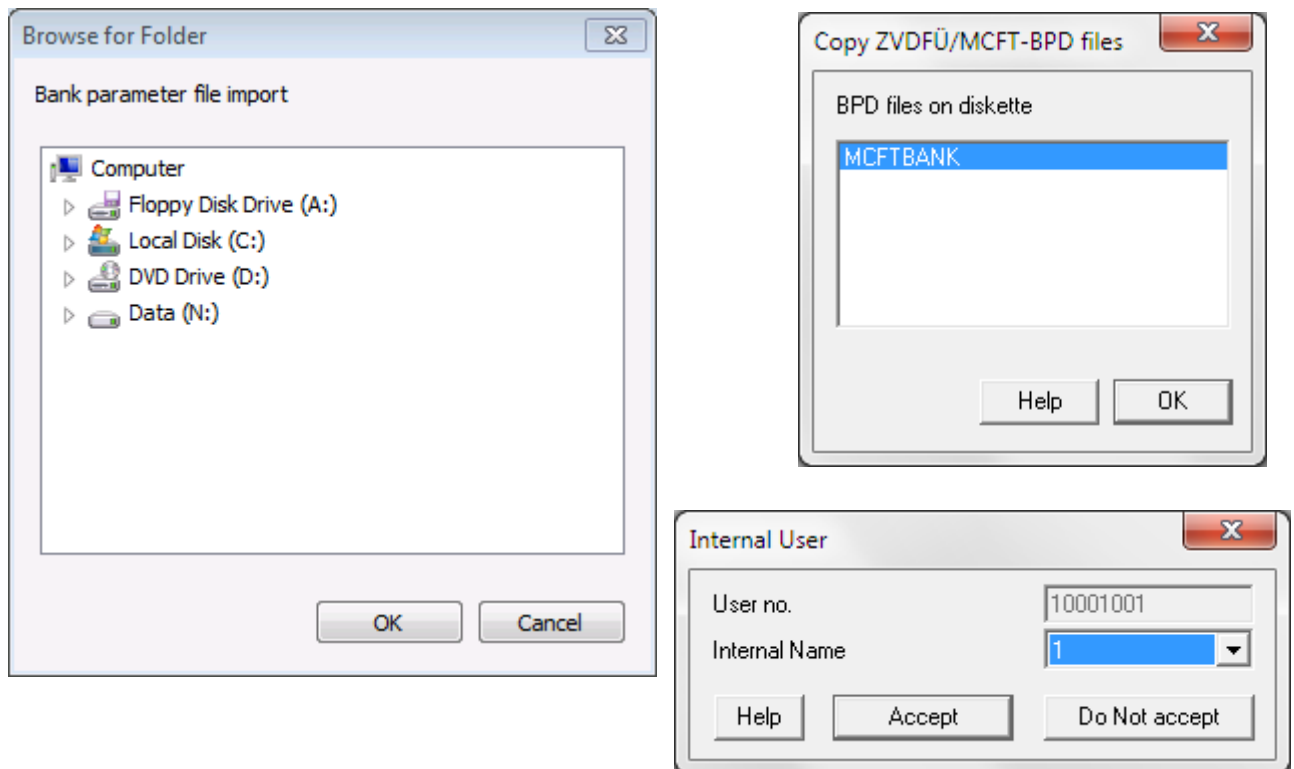
☒ Import Bank parameter file(s)

< Zurück Weiter > Help

If you wish to import a bank parameter file, click on the [**Next**] button now.

After inserting the diskette or selecting a directory, in which the bank parameter files are kept, a selection list with the existing bank parameter files is shown. Select the required file(s) and confirm with [**OK**].

The bank parameter files are imported into the system and in the case of MCFT the users are allocated to specific internal users via [**Accept**] button.



If the diskette(s) were sent directly to the new user, he or she can import the bank parameter files during their initial logon (see Chapter 5.7: *Configuring a new user with the wizard*).

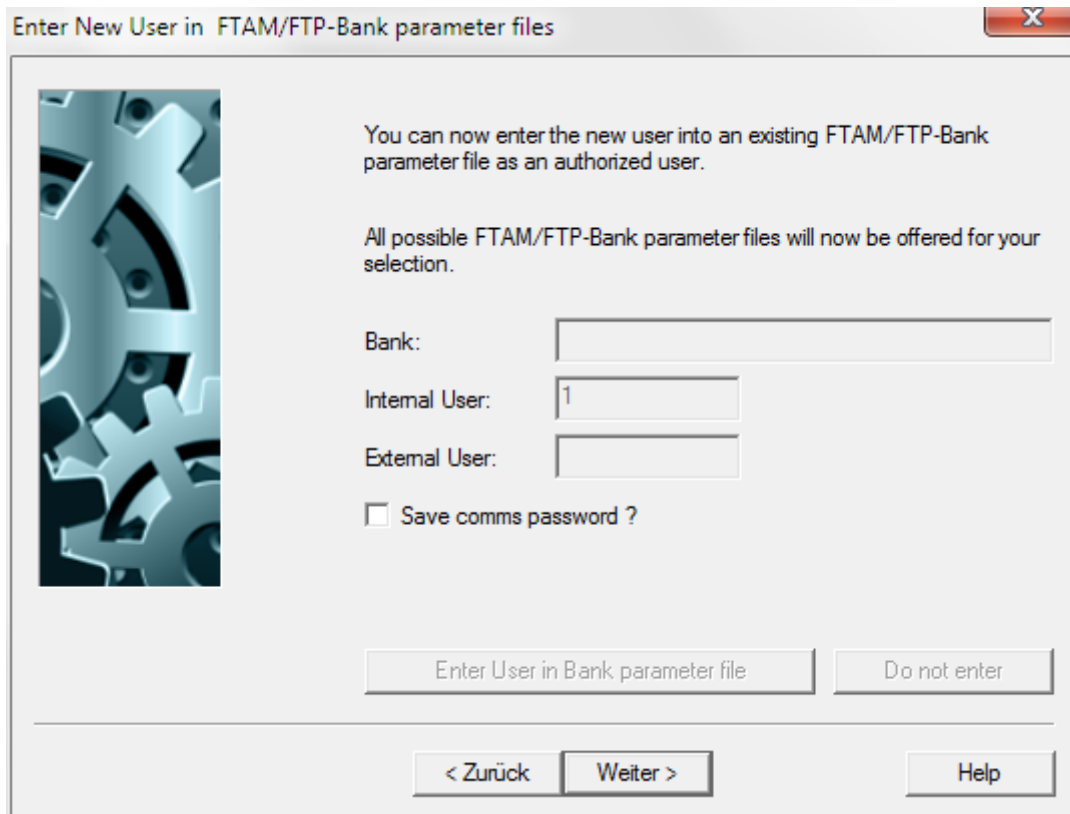
This page remain active as long as the "**Import bank parameter file(s)**" check box remains marked. If you do not wish to import any more bank parameter files, unmark the check box and click on [**Next >**].

3 Registering new users in FTAM/FTP/EBICS bank parameter files

In this step, if you use the FTAM, FTP or EBICS procedure, you can register the new user as an authorized user in the bank parameter files. For this purpose, all of the existing FTAM, FTP or EBICS bank parameter files will be listed.

The "**Bank**" line already contains the name of the respective BPD. Furthermore, the field "**Internal User**" contains the name of the new user, as it was saved in the program. In the field "**External User**", enter the user number provided by the bank. The user number is the name that will be used by the host for the user when communicating with the bank via FTAM, FTP or EBICS.

If the new user should be registered in the offered bank parameter file, click on the [**Enter user in bank parameter file**] button. Otherwise, click on [**Do not enter**].



Enter New User in FTAM/FTP-Bank parameter files

You can now enter the new user into an existing FTAM/FTP-Bank parameter file as an authorized user.

All possible FTAM/FTP-Bank parameter files will now be offered for your selection.

Bank:

Internal User:

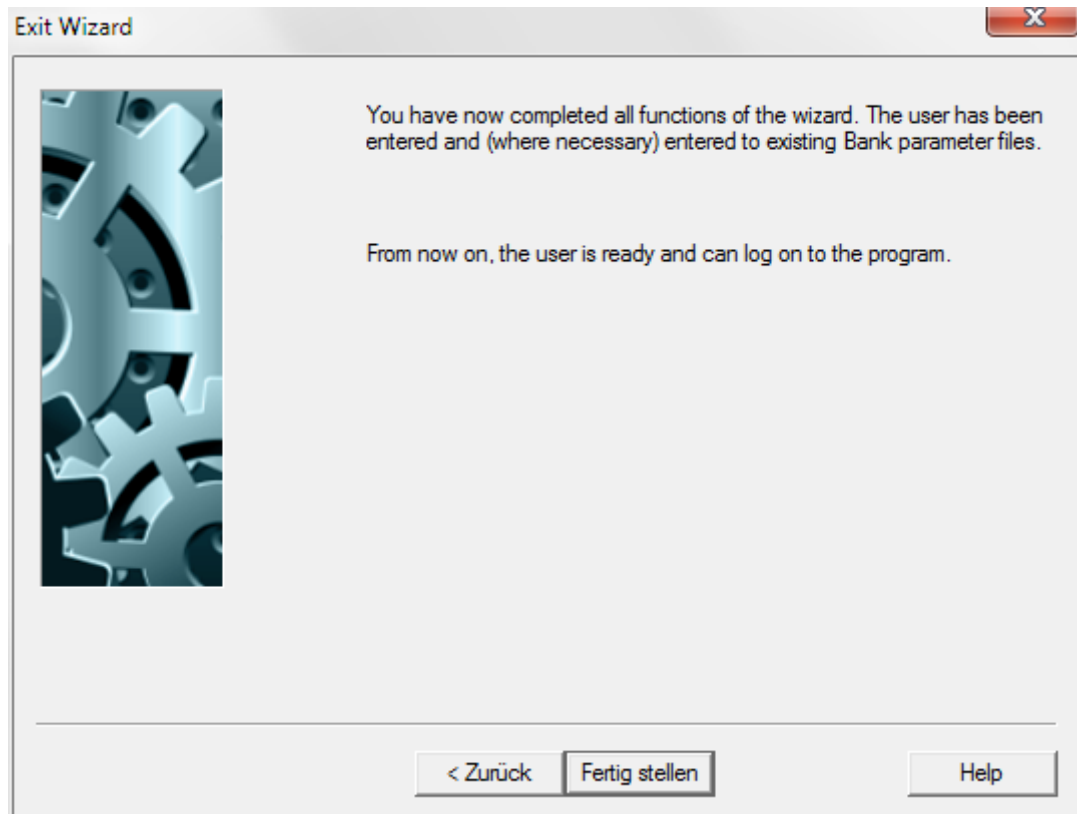
External User:

☐ Save comms password ?

Click on [**Next >**] to continue to the next step.

4 Completing the wizard

All the steps required to register a new user have been completed. When you click on [**Finish**] the new user will be prepared and can be logged on to the system with the defined initial password.



By clicking on [**< Back**], you can step back through the individual steps to make any changes that are needed.

5.3 User groups and access class for confidential payments

The program is increasingly used as central solution in the company network and is used by all departments. With it, payment orders from different origins and jurisdictions of the enterprise are administered in the **databases** of the application which show, as a rule, different confidentiality requirements (e.g. credit transfers to suppliers, wages and salaries, customer direct debits).

On the basis of the requirements derived from that, a protection concept has been implemented, allowing the access to confidential payments throughout the complete system only to authorized persons.

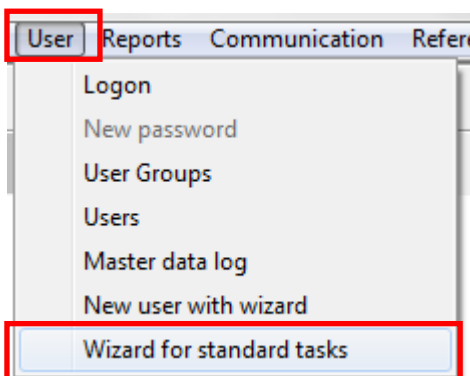
The **access protection** on particular payment contents is realised as follows.

1. The access is similarly effective within all Payments modules both on the basis of single transactions and in the file manager.
2. The access protection is effective in all Payments modules usable in the program system.
3. The rules are centrally defined in the User administration of the Core Module.
4. In the Core Module, there is a new **Access classes** reference table available (see Chapter 7.8 of the Core Module documentation).

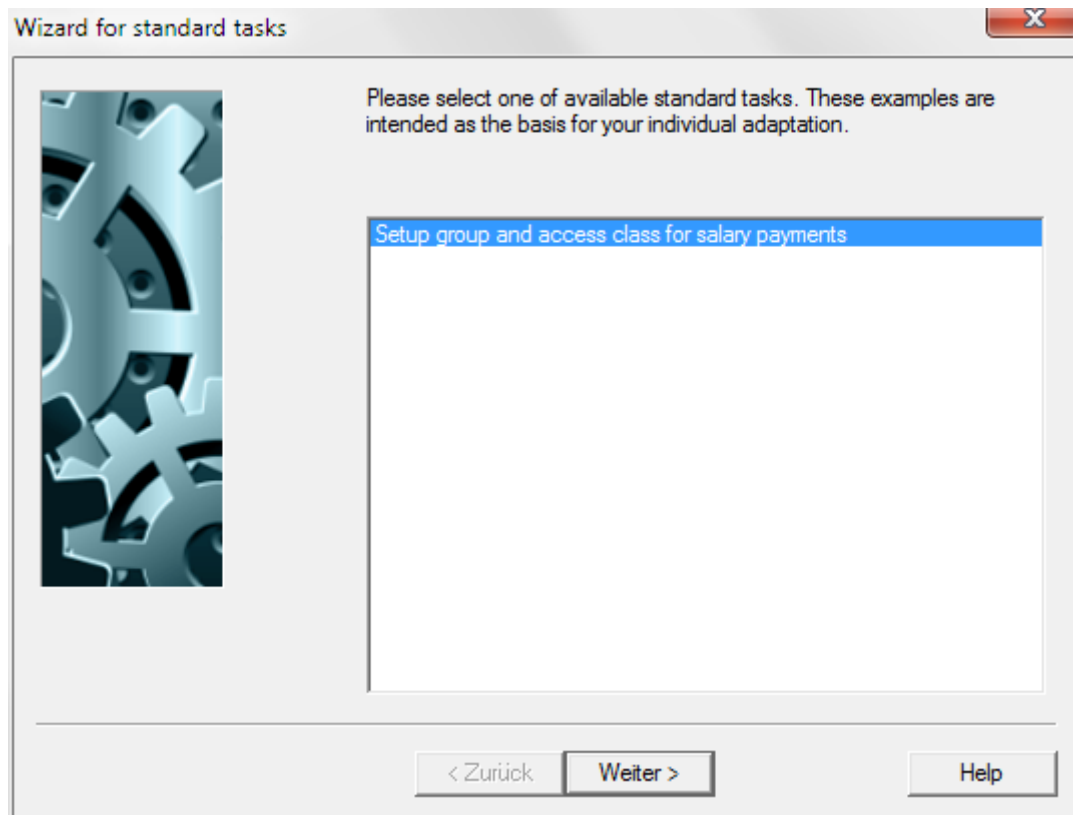
5.3.1 Set up user groups and access class for wages/salary

To setup the User groups and an access class for wage and salary payments, there is a wizard available, leading you through all necessary steps.

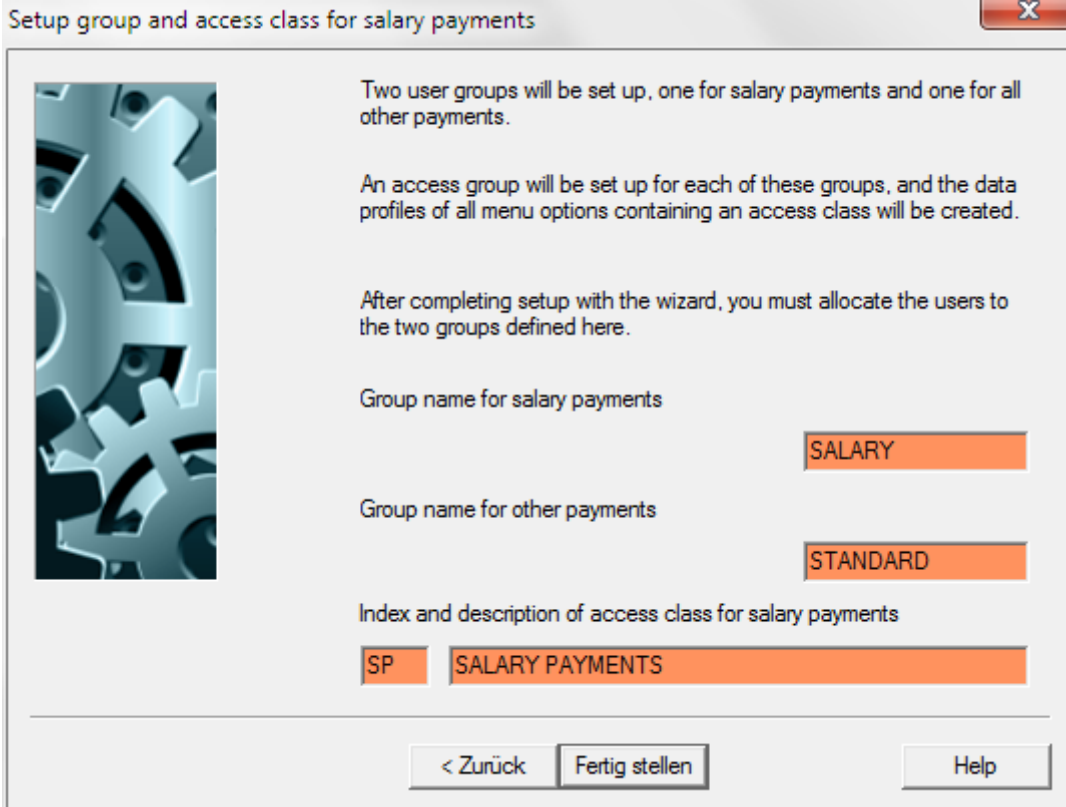
Start this wizard in the -User- menu using menu item **-Wizard for standard tasks-**.



The following dialog appears:



Therein choose "**Set up group and access class for salary payments**" and confirm your selection using the [**Next**] button.



Setup group and access class for salary payments

Two user groups will be set up, one for salary payments and one for all other payments.

An access group will be set up for each of these groups, and the data profiles of all menu options containing an access class will be created.

After completing setup with the wizard, you must allocate the users to the two groups defined here.

Group name for salary payments

SALARY

Group name for other payments

STANDARD

Index and description of access class for salary payments

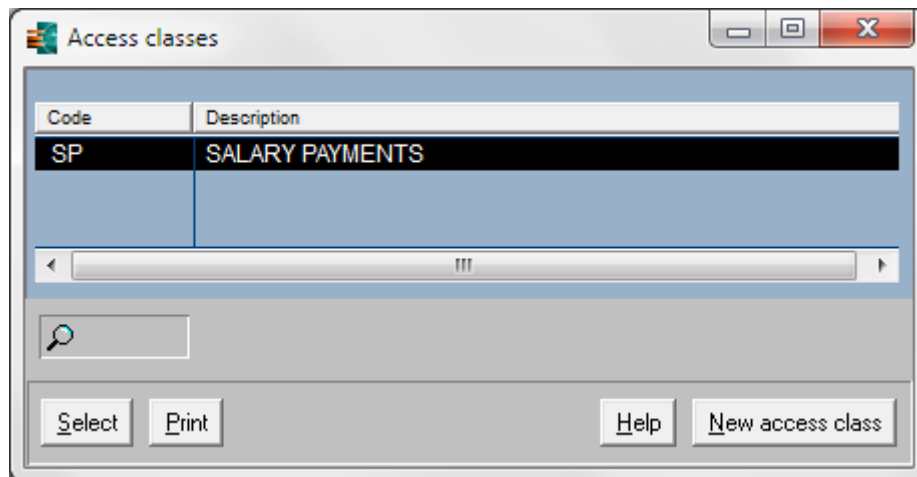
SP SALARY PAYMENTS

< Zurück Fertig stellen Help

In the next dialog, the program prompts names for the user groups to be created as well as for the access class, i.e. *SALARY* as name for the group for wage and salary payments as well as *STANDARD* as name for the group with normal access. By default, the access class is created with the abbreviation *SP* for *SALARY PAYMENTS*.

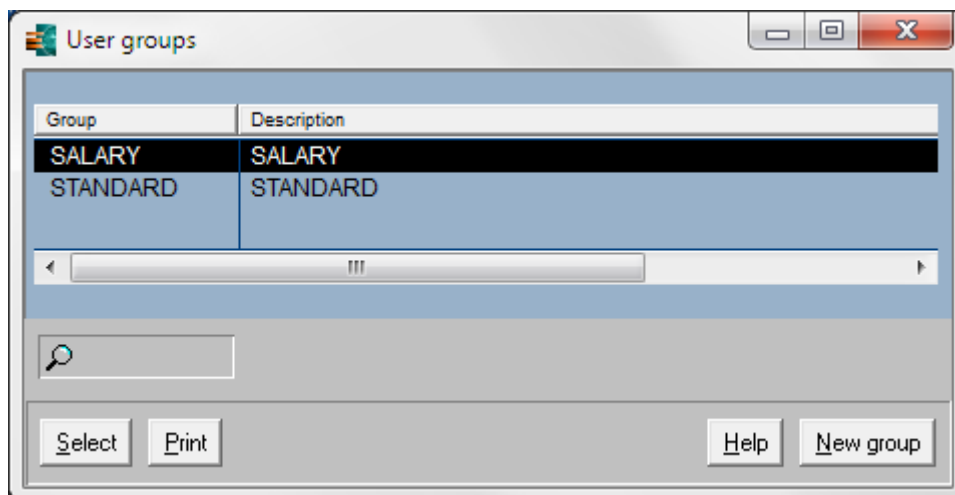
You can accept the name of the group for wage/salary payments, the name of the group for normal access as well as the index and the description of the access class for salary payments according to the prompts given or change them according to your requests. Finally press the [**Finish**] button.

Subsequently the program creates the two user groups and one access class.



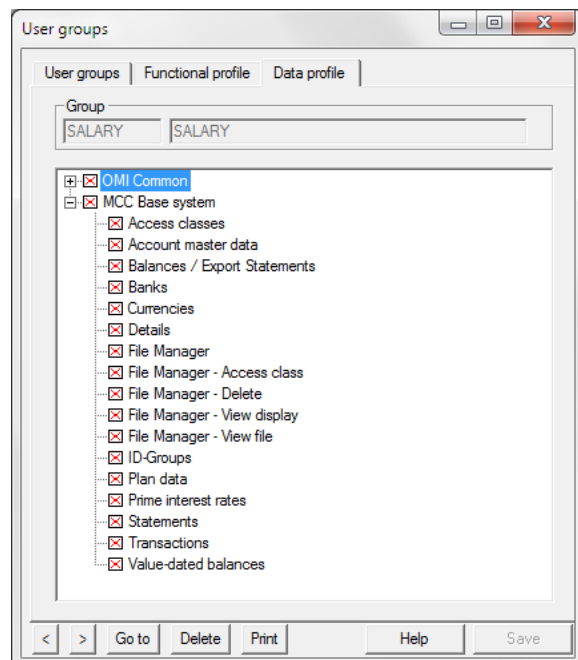
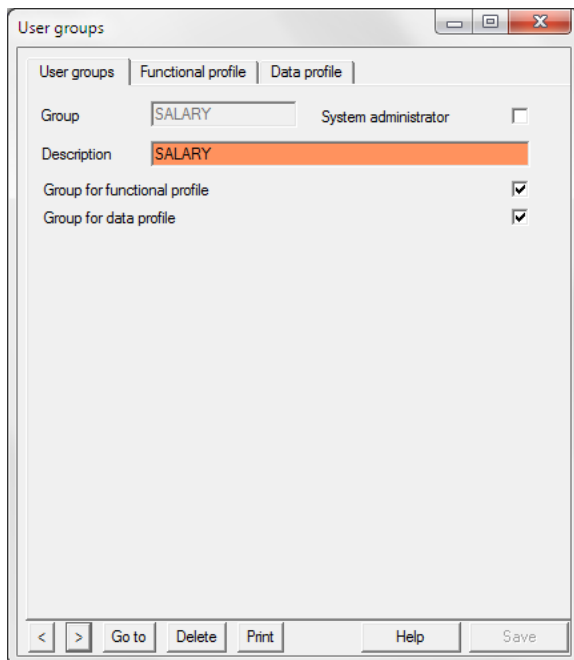
After pressing the [**Complete**] button, the database overviews for the User groups and Users are automatically opened in order to be able to change the predefined profiles of the groups and to allocate the users to the defined groups, if necessary.

First you can define further groups in the database overview of the **User groups** and/or change access rights (functional profile, data profile).



Double-click the group name to switch in each case to the detailed view, where you can make changes in case of need.

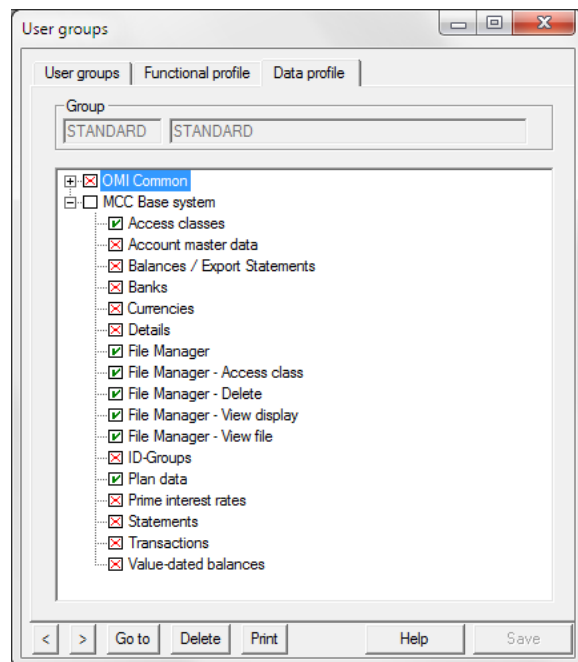
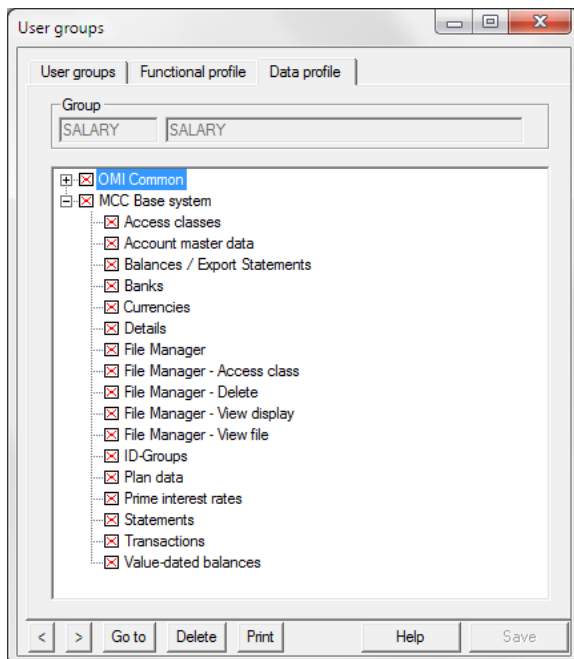
In the following sequence, the property pages of the *SALARY* group for wage and salary payments are shown:



By default, in the group for wage/salary payments, each user may view all data,
i.e. no restrictions of the view to data are defined.

All restrictions must be set manually!

In the following sequence, the property pages of the *STANDARD* group are shown:



Use the data profile to stop the access to menu items which contain an access class for users of the *STANDARD* group (see excursus on the next page).

Therein the following condition is predefined in each case (access class not equal to SP):

Data profile

Group(*)/User: STANDARD Application: MCC Base system Menu item: File Manager

☐ Show selection before
☐ No write-access to database

Only the records matching the following criteria are considered in the display and in the printouts:

Field	Operator	Value
Access class	Not equal to	SP

Buttons: Delete criteria Help Save data profile

All further restrictions/additional authorizations must be set manually!

Examples for certain menu items, where a filtering of access and view is required:

File manager (screenshots are shown further below)

Plan data:

Plan data

A/c. ? A/c. number

Bank name

A/c. name

Currency A/c. group 0

Value date 14.02.2012 Amount 0,00

Entry date 14.02.12 Original amount ? 0,00

Reference ID-Group ?

Details ?

Internal Details

Access class ? SP SALARY PAYMENTS

Delete after 1 Days

Execution frequency None Reliability Non-definite

For the last time or 14.02.2012 Plan type Plan item

Help Save

Value-dated balances:

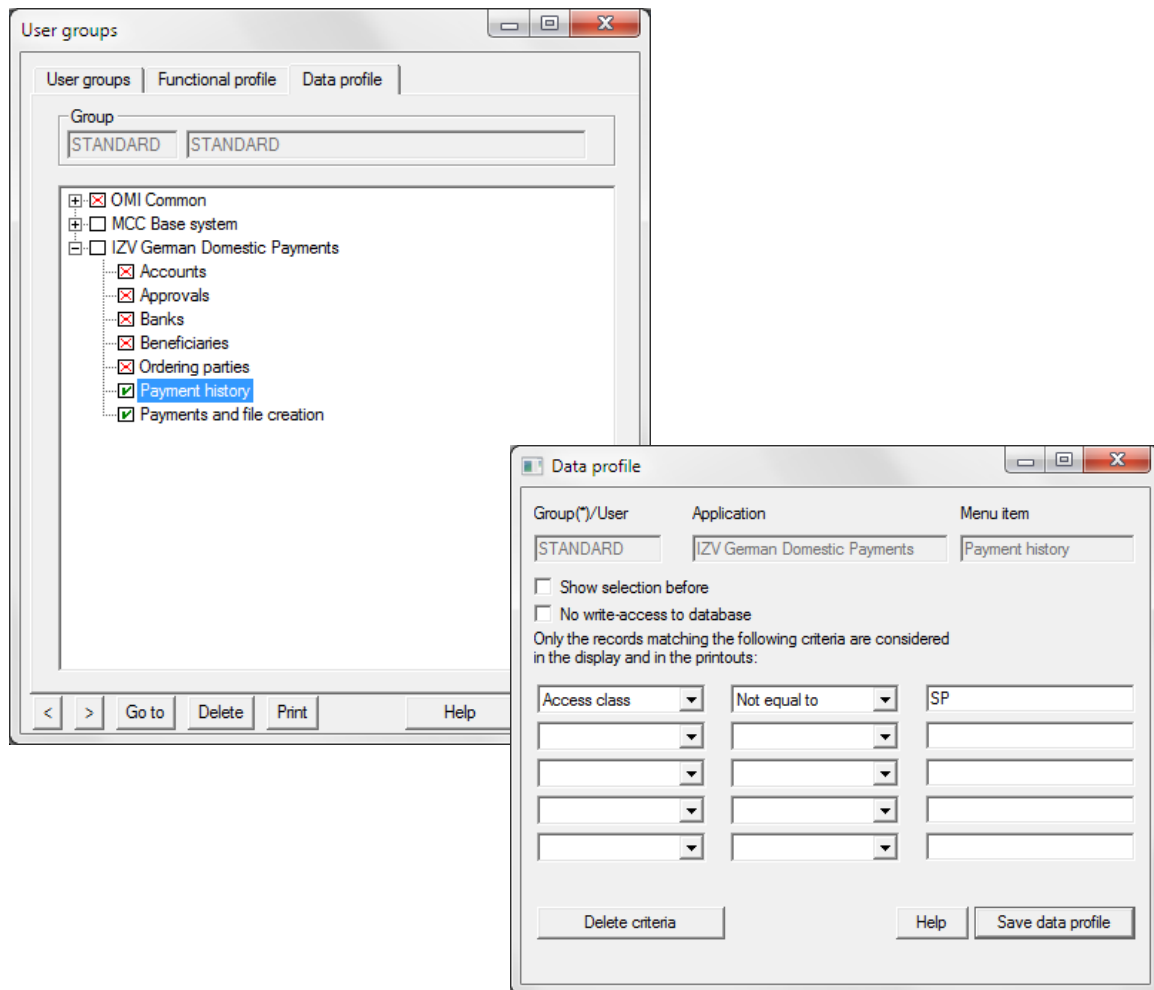
Date	Number	Total preposted items	Number	Total plan data	Number
06.04.04 #	XXXXXXXXXXXXXXXXXXXX				
Σ 06.04.04	0	0,00	1	8.000,00	0

In the detailed list, plan data (#), which does not correspond to the profile of the current user (e. g. not matching access class), is denoted with details made irrecognizable (X).

Even in the Payments modules, the access to data which are marked with the access class SP for wage/salary payments (for the → **Marking of confidential payments**, see beneath) is stopped using the data profile for defined menu items (here: approvals, payment and file creation, payment history) (see excursion on the next page).

The marked payments are not visible in the described menu items for users of the user group *STANDARD*.

Example from the Domestic Payments:



Examples for certain menu items of the payment modules, where a filtering of access and view is required:

Payment entry (screenshot is shown further below)

Approval:

Approval Single orders

Payments | Partner | Details | Internal fields | LDGR data | Times

Order number 1 Single order Credit transfer

Access class SP SALARY PAYMENTS

Partner Beneficiary name
PARTNER NAME

Bank code A/c. number Currency Amount
37050299 10203040 EUR 2.000,00

Bank name
KREISSPARKASSE KOELN

Details

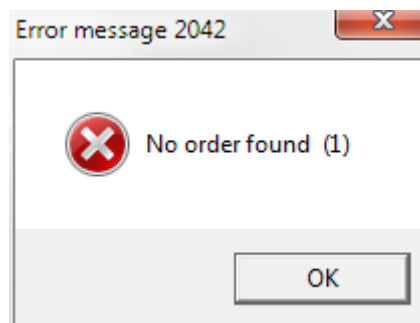
Account code Bank code A/c. number A/c. currency Text key
1 37050198 33633322 EUR 51

Ordering party Ordering party name
1 MYNAME

Approvals 0 of 1 Due date 14.02.2012 Earliest transmission 14.02.12

< > Go to Print Help Approval

File creation:



A file creation on diskette is not possible in case of confidential payments.

Payment history:

Payment order from file 12021401.IZV

Payments | Partner | Details | Internal fields | LDGR data | File

Order number: 1 Creation: 14.02.12 Single order Credit transfer

Internal fields

ID-Group / Supplementary ID-Groups

--	--	--

Internal number

--

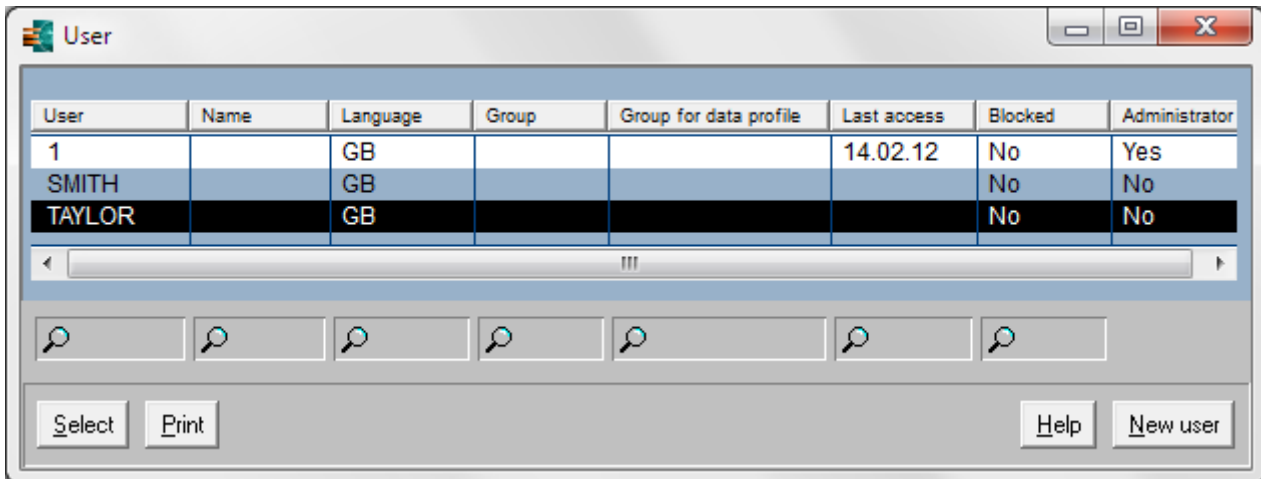
Access class: SP SALARY PAYMENTS

Ordering party

MYNAME

< > Generate single payment Print Help

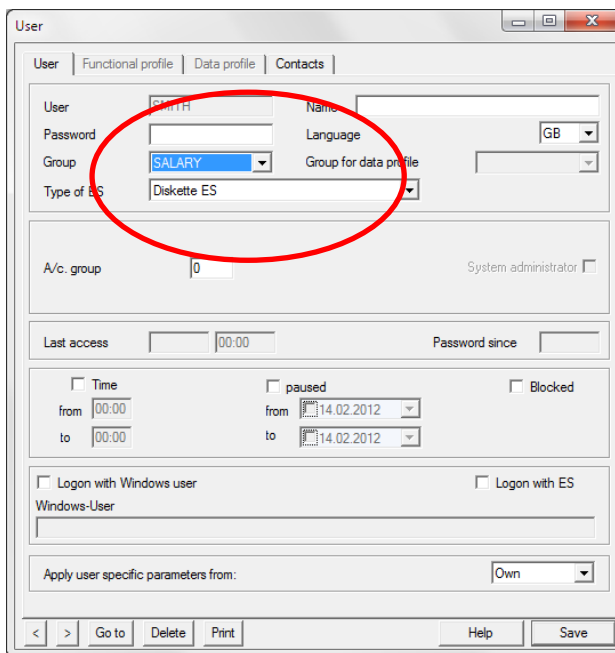
After the user groups have been defined and provided with the required rights, you only have to allocate the users to the defined groups (the database overview of the **Users** has already been opened automatically).



User	Name	Language	Group	Group for data profile	Last access	Blocked	Administrator
1		GB			14.02.12	No	Yes
SMITH		GB				No	No
TAYLOR		GB				No	No

Below the table are search filters and buttons: Select, Print, Help, New user.

Double-click the user name to switch in each case to the detailed view, where you can make the allocation to a group.



User: SMITH

Group: SALARY

Language: GB

Type of ES: Diskette ES

A/c. group: 0

System administrator: ☐

Last access: 00:00

Password since: 00:00

Time: ☐ from 00:00 to 00:00

paused: ☐ from 14.02.2012 to 14.02.2012

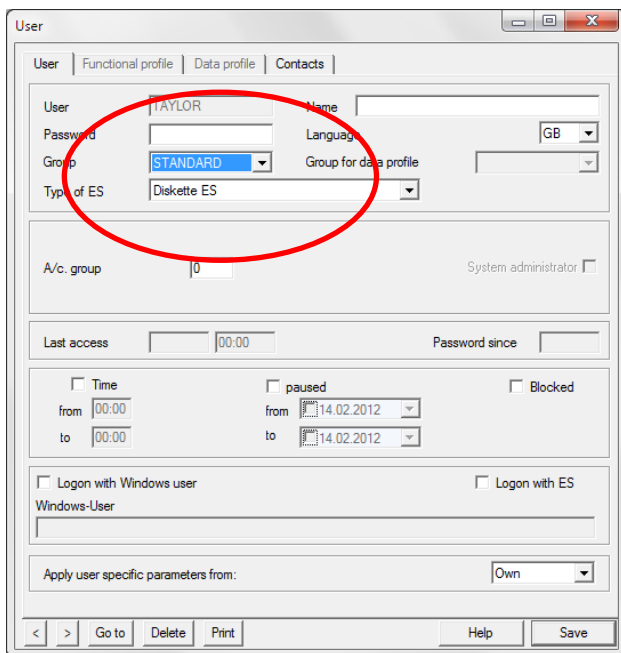
Blocked: ☐

Logon with Windows user: ☐ Logon with ES: ☐

Windows-User:

Apply user specific parameters from: Own

Buttons: < > Go to Delete Print Help Save



User: TAYLOR

Group: STANDARD

Language: GB

Type of ES: Diskette ES

A/c. group: 0

System administrator: ☐

Last access: 00:00

Password since: 00:00

Time: ☐ from 00:00 to 00:00

paused: ☐ from 14.02.2012 to 14.02.2012

Blocked: ☐

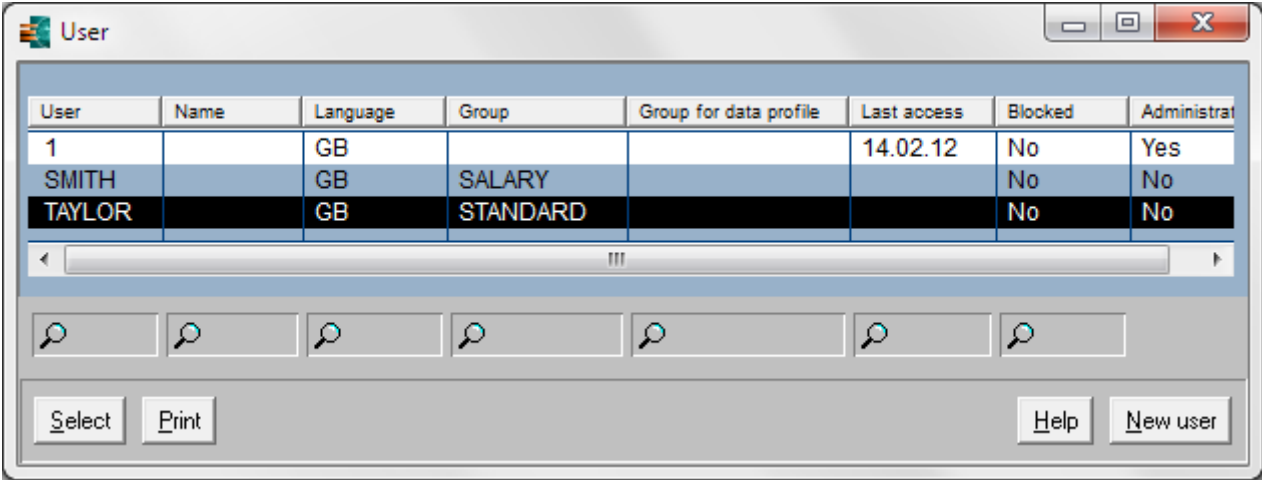
Logon with Windows user: ☐ Logon with ES: ☐

Windows-User:

Apply user specific parameters from: Own

Buttons: < > Go to Delete Print Help Save

Database overview of the users after the allocation:



User	Name	Language	Group	Group for data profile	Last access	Blocked	Administrator
1	SMITH	GB	SALARY		14.02.12	No	Yes
	TAYLOR	GB	STANDARD			No	No
		GB				No	No

After closing the database overview, all steps of the wizard to set up two user groups and one access class for wage and salary payments are completed.

5.3.2 Marking of confidential payments

In the program, the user of the group for wage/salary payments has the option to mark confidential payments during payment entry, during file import and during inclusion of an externally created file into the file manager with an access class defined suitably (Default: SP).

Marking during payment entry e.g. in the Domestic Payments:

The screenshot shows the 'Single orders' window with the following fields and values:

- Order number: 1
- Single order: [dropdown]
- Credit transfer: [dropdown]
- Access class: [?] SP SALARY PAYMENTS (circled in red)
- Partner: [?]
- Beneficiary name: PARTNER NAME
- Bank code: 37050299
- A/c. number: 10203040
- Currency: EUR
- Amount: 2.000,00
- Gross/Net: [dropdown]
- Bank name: KREISSPARKASSE KOELN
- Details: [text area]
- Account code: [?]
- Bank code: 37050198
- A/c. number: 33633322
- A/c. currency: EUR
- Text key: 51
- Ordering party: [?]
- Ordering party name: MYNAME
- Approvals: 0 of 1
- Due date: 14.02.2012
- Earliest transmission: 14.02.12
- Buttons: < > Go to Delete Print Help Save

Marking during file import:

The screenshot shows the 'Import of payment file(s)' window with the following fields and values:

- Order form: Single order
- Delete order file(s) after import: [checkbox]
- Access class: [?] SP SALARY PAYMENTS (circled in red)
- ID-Group: [?]
- Buttons: Help OK

Marking during inclusion of an externally created file into the file manager:

The screenshot shows the 'File manager' window with the following details:

- Tab:** Password and execution data
- Bank:** MCFTBANK
- Session:** IZV
- File Type:** Original file with signature
- User:** 10001001
- File:** E:\multlang\IZVWIN\11080102.IZV
- Make Electronic Signature:**
 - User: 1
 - ES password: (empty)
- Other:**
 - ID-Group: ?
 - Access class:** ? **SP** **SALARY PAYMENTS** (circled in red)
 - ☐ For this file, plan data shall be generated additionally in a new way
- Execution:**
 - Repetition: Once
 - Pause in minutes before repetition?: 0
 - Execute on workstation: Own
 - 1. Comms: 14.02.2011
 - Last Date: 14.02.2011
- Buttons:** Help, Save

Thereby, also these files can be viewed and signed only by authorized persons.

In the file manager, the payment file is also visible in detail for a user of the group for wage/ salary payments using the [**View file**] button.

File manager

Signatures Time

Display transmit sessions: Stock: Current

☐ Do not show successfully sent files
☐ Only show files pending ES
☐ Do not show files signed by yourselves

General information about the file E:\multilang\IZVWIN\11080102.IZV

File creation date	Number of logical files	Total number of payments	Sum payments	Currency
01.08.2011	1	1	2.000,00	EUR

Summary information on all payments

Type	Value date / Ordering party	Number	Amount	Currency
Transfer	01.08.2011 37050198 MEIN NAME	1 0033633322	2.000,00	EUR

Se...	ONo	Status	Original file name	Bank name	Curre...	Amount	A...	ES ...	ES ...	ID-Group	Comms...	Comm...	Hash
I...	A010	Pending ES	E:\multilang\IZVWIN\11080102.IZV	Omikron ...	EUR	2.000,00	O						2C74
I...	A000	Pending Co...	E:\multilang\IZVWIN\12021401.IZV	Omikron ...	EUR	2.000,00	D			IZV18424			F84A
I...	A000	Own	E:\multilang\IZVWIN\12021401.IZV	Omikron ...	EUR	2.000,00	D			IZV18424			F84A

Execute order Execute all due orders New entry from favourite Delete signature Sign

Select Print Collect data from several banks **View file** Help New order

DAT\IZVA010.DSP

General information about the file E:\multilang\IZVWIN\11080102.IZV

File creation date	Number of logical files	Total number of payments	Sum payments	Currency
01.08.2011	1	1	2.000,00	EUR

Payment singles overview

Type	Value date	Ord.Party/Receiver
Transfer (G)	01.08.2011	37050198 / 0033633322 MEIN NAME

Partner Bank/Account/Name	Ordering party Bank/Account/Name/ Details	Amount	Currency
37050299 / 0010203040 PARTNER NAME	37050198 / 0033633322 MEIN NAME	2.000,00	EUR

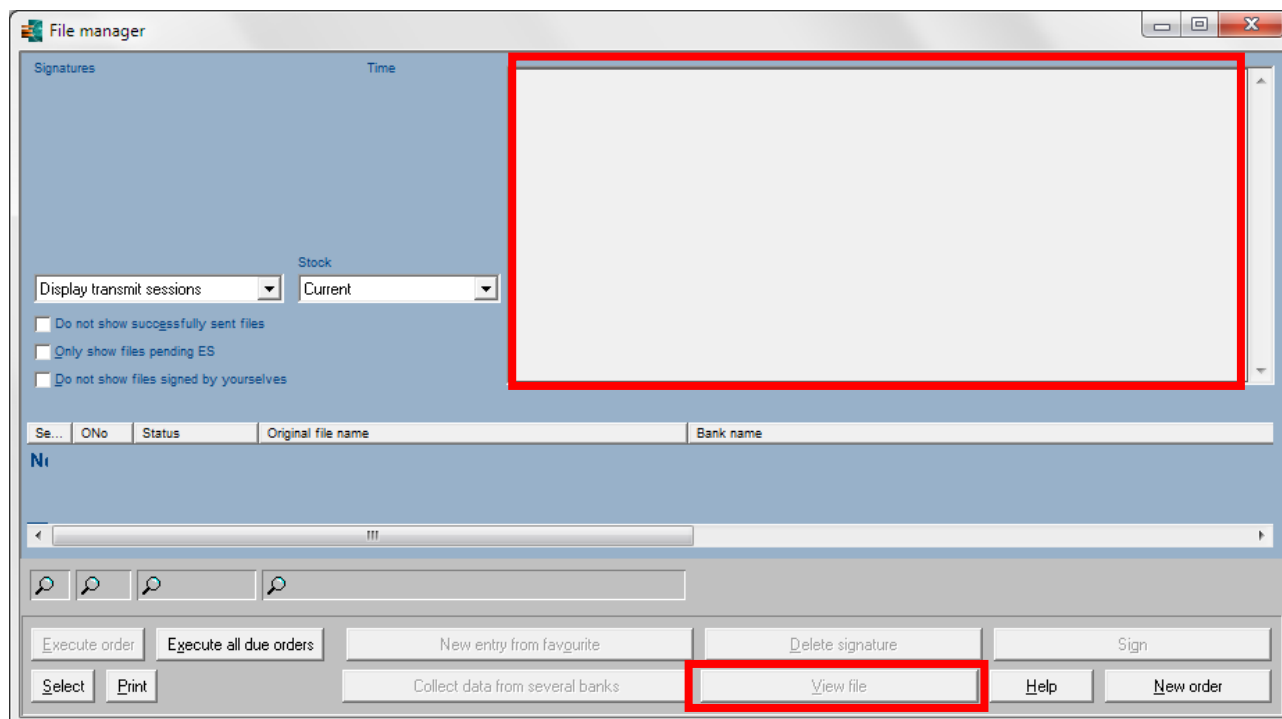
Totals information of logical file

Type	Value date	Ordering party	Total number of payments	Sum payments	Currency
Transfer	01.08.2011	37050198 / 0033633322 MEIN NAME	1	2.000,00	EUR

End of logical file

End of file

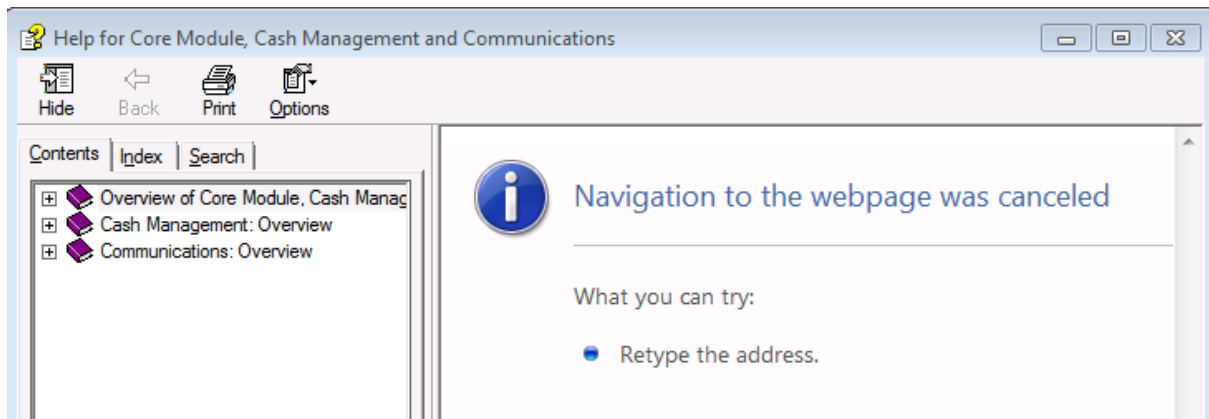
Example for someone who may not see anything and who may only execute the orders, matching with the predefined access rights of the *STANDARD* group (see above):



6 How to make CHM files accessible via network

Problem:

.CHM (HTML Help) files cannot be accessed from a network drive. E.g. the following message appears:



Cause:

This problem is caused by security updates of Microsoft, which prevent the display of HTML content that is outside the Local Machine zone. These changes were introduced to reduce security vulnerabilities in HTML Help (which allow code execution). These security patches should prevent the opening of infected CHM files from the internet in the first place, but have the side-effect that opening from the intranet is also no longer possible.

Solution:

To re-enable the opening of remote content from CHM files within the corporate network, you have to modify the following entries in the registry database using the registry editor (REGEDIT.EXE).



Please note...

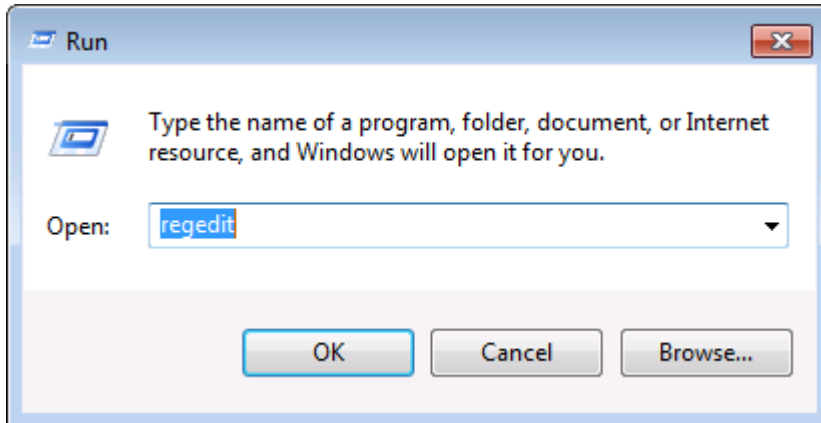
This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs.

6.1 Zone modification

Alternative 1 (configure the access to CHM files in that way, that all sites in a particular zone [here local intranet zone] are enabled to display HTML Help content)

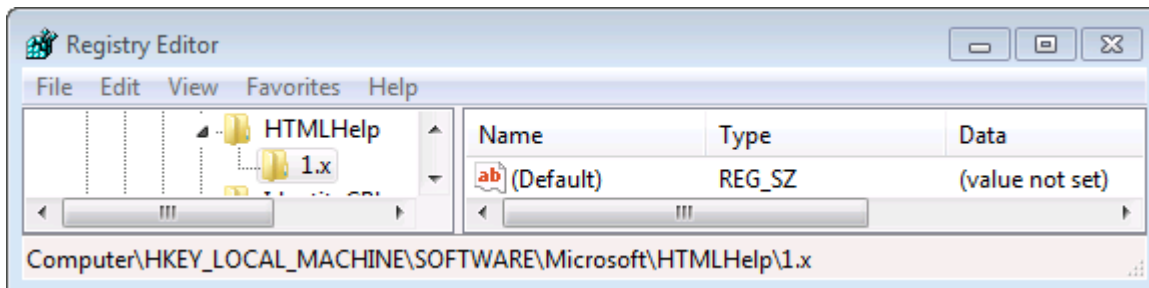
Please proceed as follows:

You start the registry editor by opening **Start / Run**, typing the **regedit** command and confirming with [**OK**]:



Navigate to the following registry key in the registry editor

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x:



If the following registry sub-keys do not exist, you need to create the keys accordingly:

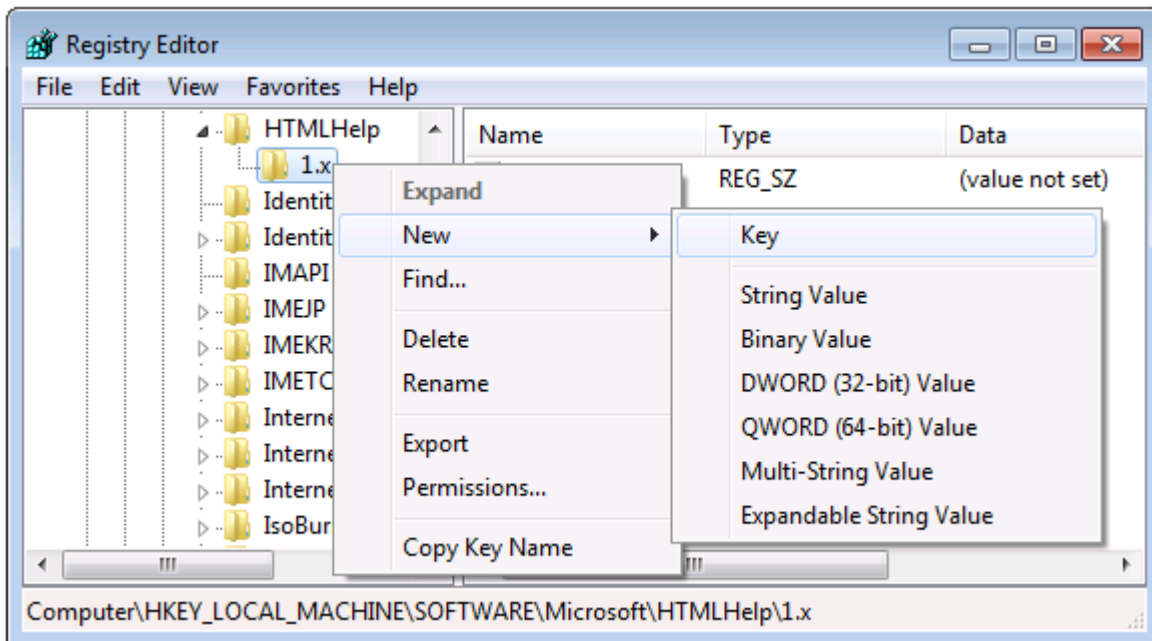
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\HHRestrictions

(for HTML Help files) **and**

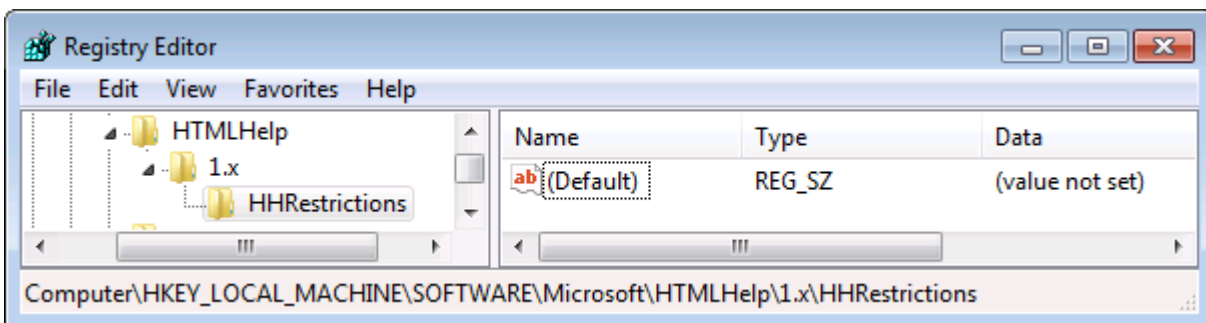
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\ItssRestrictions

(for all Microsoft "InfoTech" storage files; the InfoTech protocol is mainly used by HTML Help; the functionality of this protocol is provided by the „itss.dll“ file)

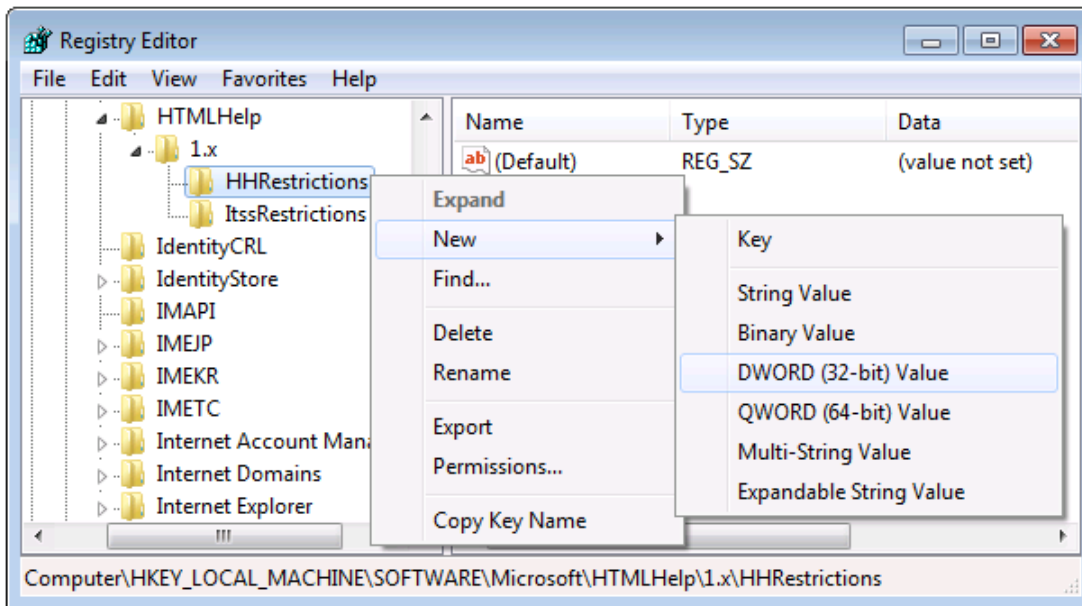
Right-click with the mouse on the indicated registry key and then select **New** and **Key**:



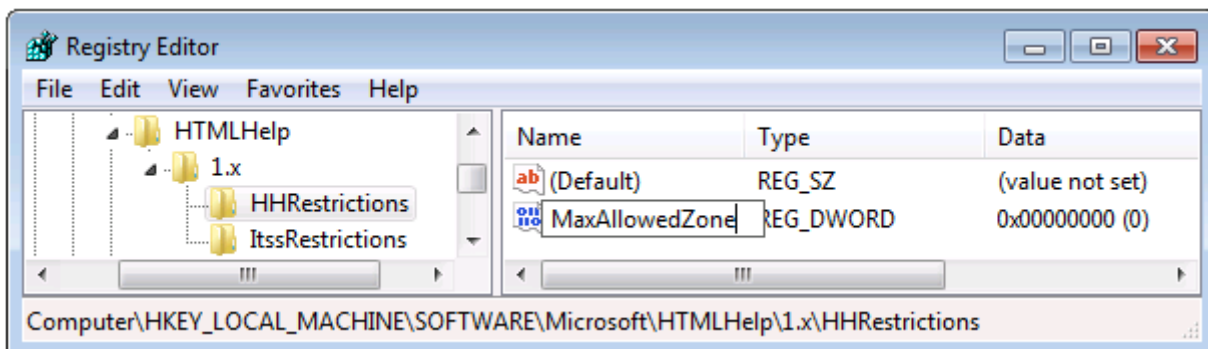
Enter the correct names for each sub-key (**HHRestrictions** and **ItssRestrictions**) and confirm with Enter:



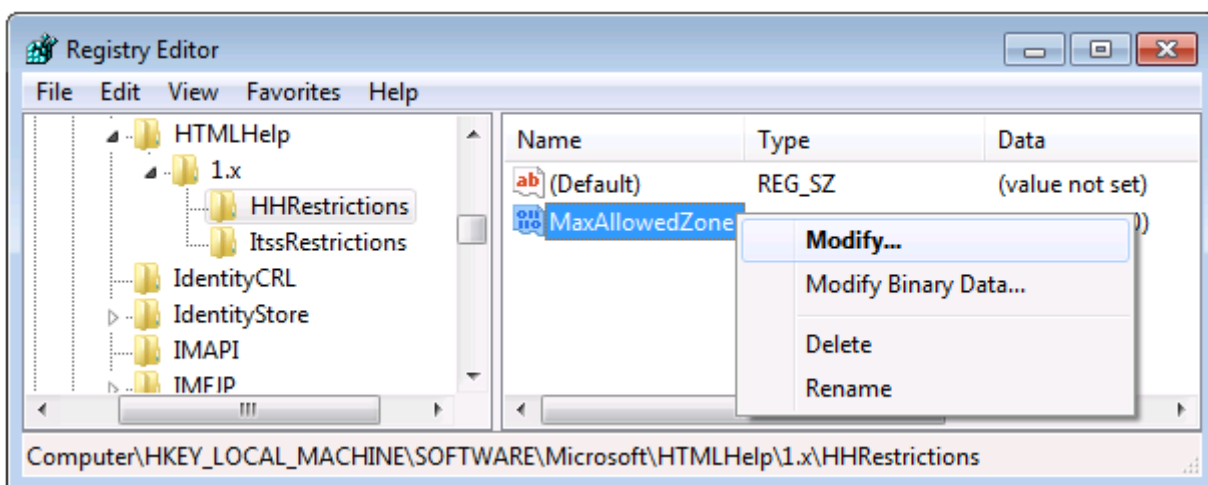
Switch to each entered sub-key and add a new **DWORD Value**:



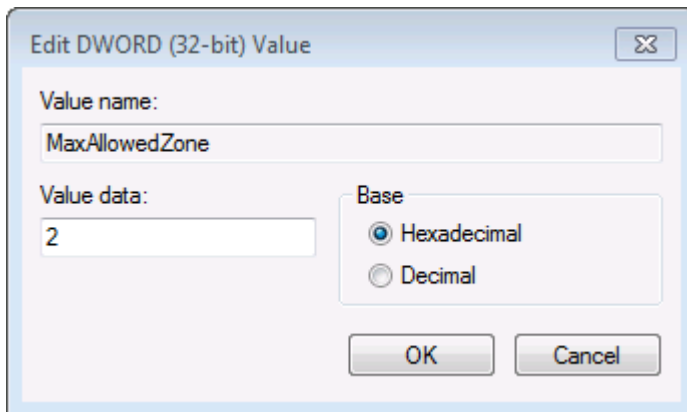
Enter **MaxAllowedZone** in each case and press Enter to confirm:



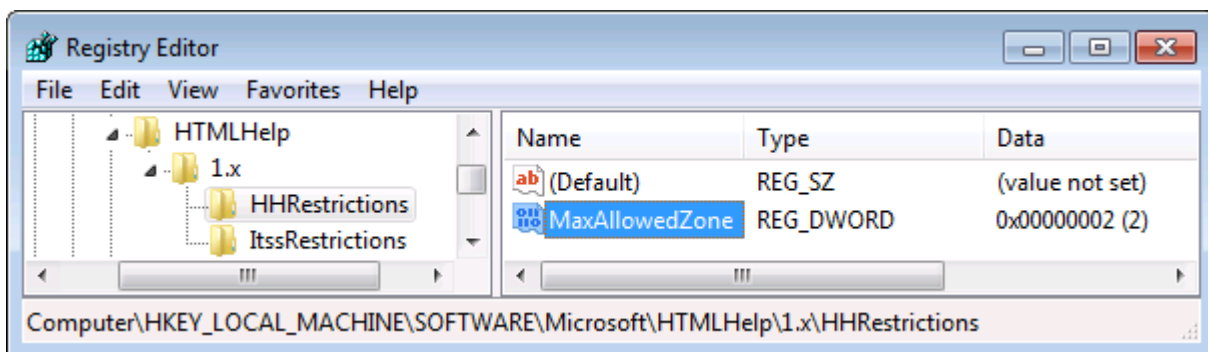
Right-click with the mouse on each MaxAllowedZone value and select **Modify**:



Change the value (default=0) to **2** and confirm with [OK].

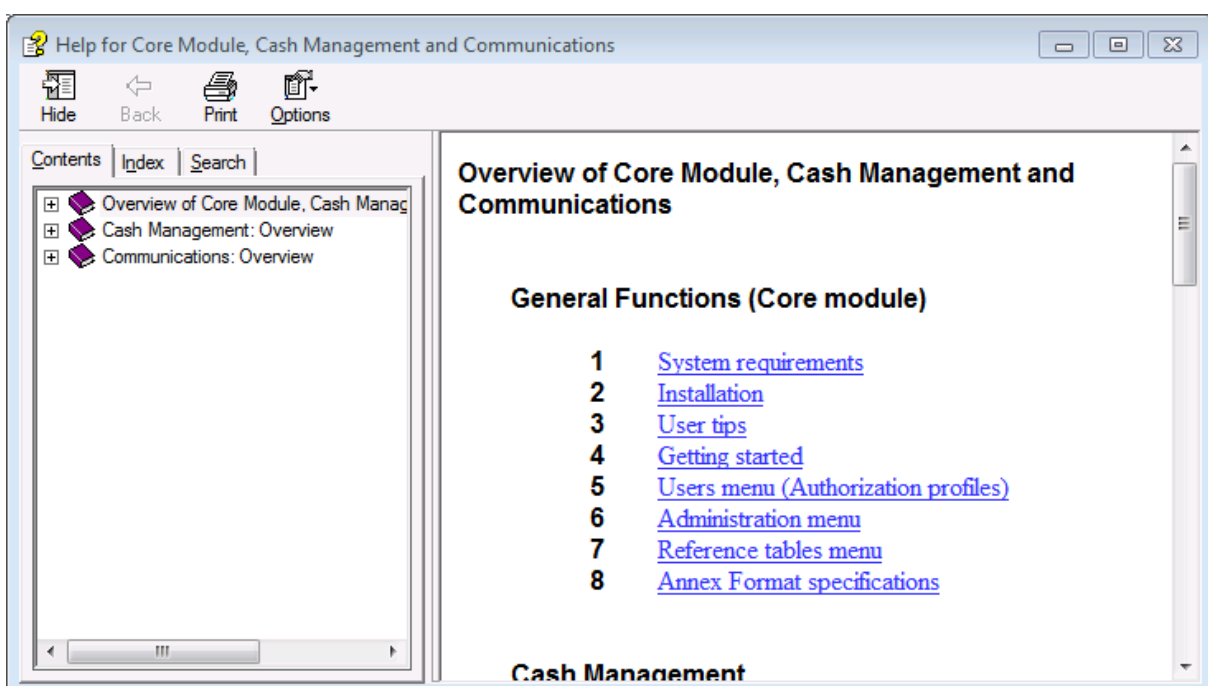


The completed registry sub-keys are as follows:



Exit the registry editor then.

Subsequently, the HTML Help can be displayed from network drives in the same way as it is known from the local call:



6.2 Allow URL

Alternative 2 (enabling of specific network drives for the display of CHM files):

Start the registry editor.

Create under

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\HHRestrictions

(for HTML Help files) **and**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\ItssRestrictions

(for all “InfoTech” files)

a new value named “**URLAllowList**” with data type REG_SZ (string value). Here, the network path is entered as follows:

\\server name\share name\file: //\\server name\share name

Please note the additional entry with the „file: //“ prefix. Always two entries need to be added to activate one UNC path to a shared network folder.

You will find more information on the following Microsoft web pages:

<http://support.microsoft.com/kb/892675/en-us>

<http://support.microsoft.com/kb/896054/en-us>

<http://support.microsoft.com/kb/896358/en-us>