OPUS

Spectroscopy Software

Version 6

User Manual

VALIDATION

BRUKER

The following publication has been worked out with utmost care. However, Bruker Optik GmbH does not accept any liability for the correctness of the information. Bruker Optik GmbH reserves the right to make changes to the products described in this manual without notice.

This manual is the original documentation for the OPUS spectroscopic software.

Table of Contents

1 Introduction

1.1 General

Spectrometers running OPUS as spectrometer software may be used in companies or institutes which are legally bound to quality regulations. One of these regulations is ***21 CFR Part 11 Electronic Records; Electronic Signatures*** **[1]** issued by the United States Food and Drug Administration, FDA (Federal Register 62, n. 54 (1997)). This document deals with electronic records and electronic signatures as a replacement for printed documents and hand-written signatures.

Bruker develops software that helps users to comply with the *21 CFR Part 11* regulation.

General information about the ***21 CFR Part 11*** regulation and a summary of OPUS features supporting the regulation and/or actions to be taken by the users of the spectrometer system can be found in the Bruker documentation ***Compliance of OPUS with 21 CFR Part 11*** **[2].** This document includes all the paragraphs of the regulation and provides information on how each paragraph has been implemented.

1.2 Scope

This manual focuses solely on the software related aspects of the regulation and will assist you in setting up your system according to the *21 CFR Part 11* regulation. The following paragraphs of the regulation are not, or only partially, discussed in this manual:

11.10 (i)	Education and training
11.10 (j)	Written policies for electronic signatures
11.10 (k)	Systems Documentation
11.10. (k) (1)	Distribution, access and use of documentation
11.10. (k) (2)	Documentation revision and change control
11.30	Controls for open systems
11.100 (b)	Identity of the individual
11.100 (c)	Legal binding of electronic signatures
11.100 (c) (1)	Certification for 11.100 (c)
11.200 (a) (2)	Signing by genuine owners
11.200 (a) (3)	Abuse of signatures
11.200 (b)	Biometric authentication

11.300 (c)	Following loss management
11.300 (e)	Periodic testing of identification devices

Make sure that you read the comments for these paragraphs in **[2]**[1].

1.3 About this Manual

This manual includes the following main topics:

- Software Validation (2)
- System Access Control (3)
- Electronic Records (5)
- Audit Trails (6)
- Electronic Signatures (4)
- Retention of OPUS Data (7)

Each chapter will start with a reference listing those paragraphs of the *21 CFR Part 11* regulation which are discussed in the chapter. As already mentioned, the text of these paragraphs and a comprehensive description of the implementation can be found in **[2]**[2].

At the end of each chapter you will find a comprehensive list of *Key points* which can be used as a check list for actions and measures to be taken.

1. , 2. See references in Chapter 1.1

2 Software Validation

2.1 Reference to 21 CFR Part 11

The following paragraph is discussed in this chapter:

11.10 (a)

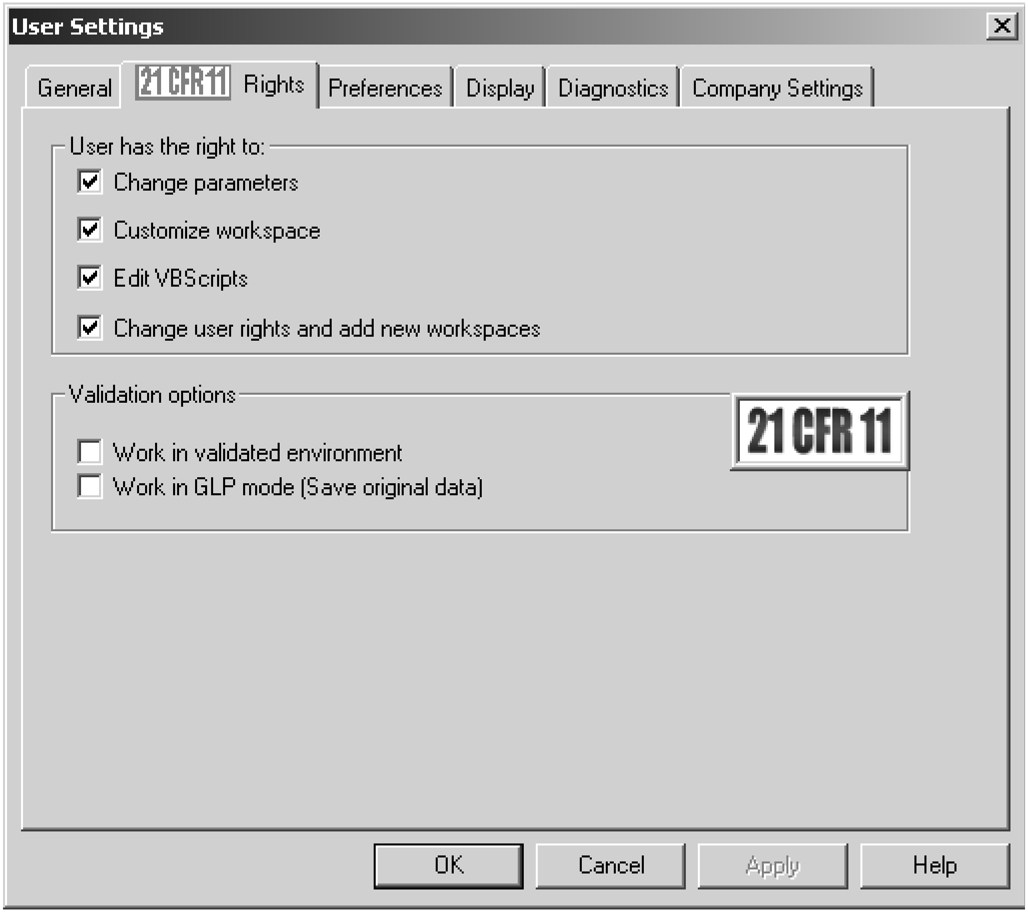
2.2 General

Validation of the entire spectrometer system and the software required to run the spectrometer and manipulate and evaluate data is one of the key points of the *21 CFR Part 11* regulation. OPUS is a multi-purpose application software consisting of several independent software packages. The most commonly used OPUS functions and extended packages have been thoroughly validated. **Appendix A** shows the functions which are available in a *Validated Environment,* and are subject to change without notification. Contact Bruker to get an up-to-date list of all functions available in validation mode. A validation certificate is part of the OPUS/VALIDATION software package.

2.3 Validation Options

To use OPUS in a *Validated environment* it is necessary to allow access to validated functions and software packages only. Activate the *Work in validated environment* check box on the *21CFR11 Rights* tab of the *User settings* command in the *Setup* menu.

The *21CFR11 Rights* tab shows the *21 CFR 11* logo used within OPUS for all features relevant to this regulation. If the logo is displayed in red, the *Work in validated environment* check box has been activated. If the logo is displayed in gray, the check box has been deactivated (see figure 1).



User has the right to:

☑ Change parameters

☑ Customize workspace

☑ Edit VBScripts

☑ Change user rights and add new workspaces

Validation options

□ Work in validated environment

□ Work in GLP mode (Save original data)

Figure 1: User Settings - 21 CFR 11 Rights

Several options are available in two group fields. The options in the *User has the right to* group field are explained in more detail in chapter 3.5.

The *Validation options* group field with the *21 CFR 11* logo provides two different options.

- Work in validated environment
- Work in GLP mode (Save original data)

Note that all options on this tab do not depend on the kind of user logged in but on the workspace specified, i.e. the options are stored in the workspace. **Therefore, it is essential to activate the required options for all workspaces which are used on the system.** For more details on the OPUS workspace philosophy refer to chapter 3.5.

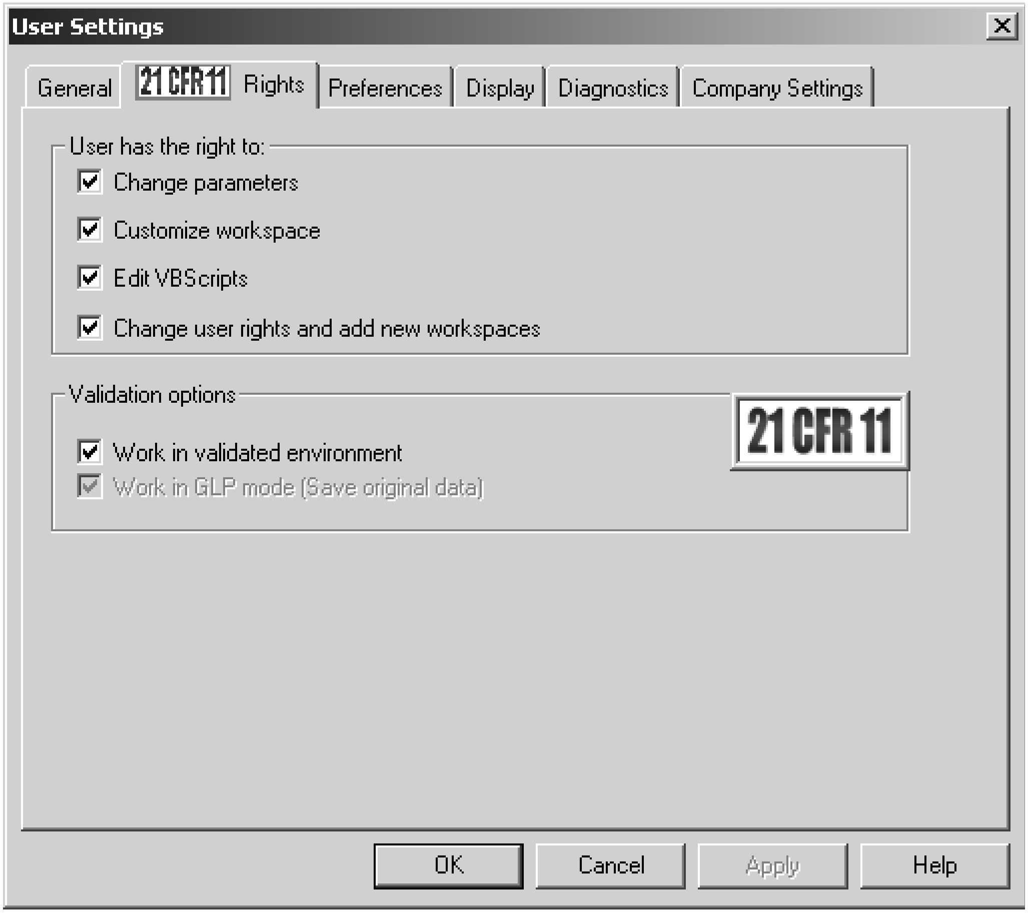
2.3.1 Working in GLP Mode

To work in GLP mode activate the *Work in GLP mode (Save original data)* check box (figure 1). In this case the original measured spectra are securely stored in the spectrum data file. The original data will not be overwritten or deleted in OPUS. If you use different manipulation functions, these functions will only modify a copy of the original data. At any time it is possible to restore either the original data or any step in the sequence of manipulation/evaluation of the data, using the *Replay* command in the *Edit* menu.

2.3.2 Working in Validated Environment

This option is required for all systems which run in a validated environment.

If you activate the *Work in validated environment* check box, the *Work in GLP mode* check box is automatically activated as well and cannot be deactivated. The validation state is clearly indicated by the red *21 CFR 11* logo.



User has the right to:

☑ Change parameters

☑ Customize workspace

☑ Edit VBScripts

☑ Change user rights and add new workspaces

Validation options

☑ Work in validated environment

☑ Work in GLP mode (Save original data)

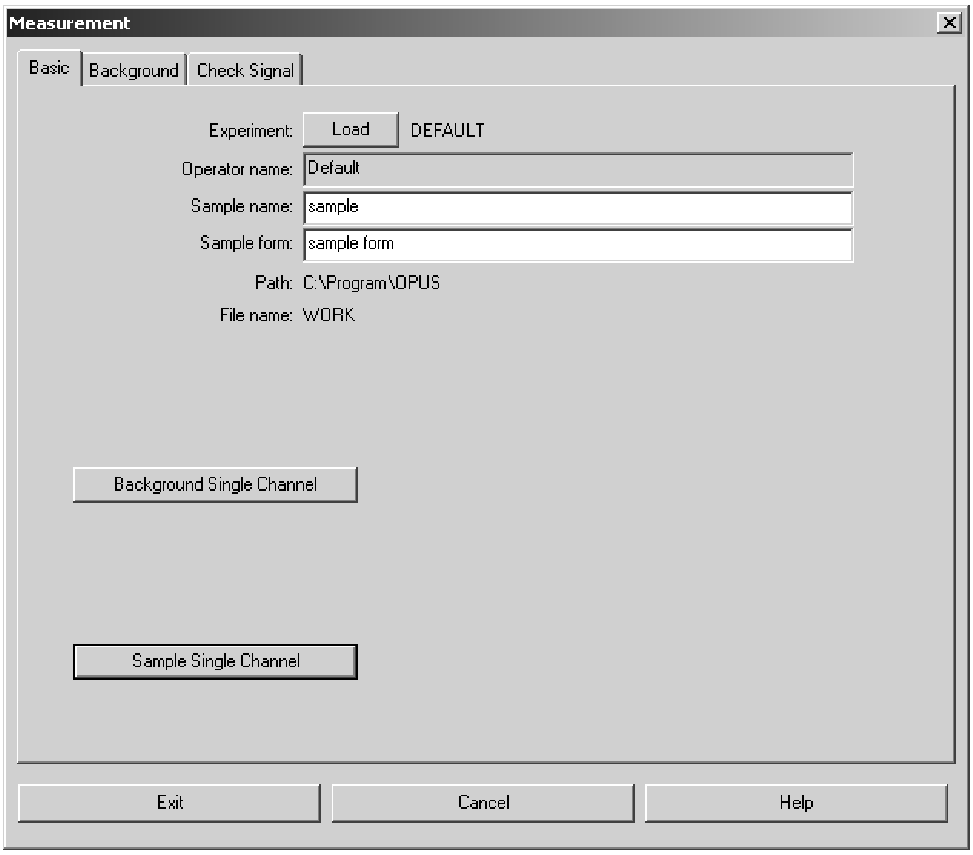
Figure 2: User Settings - Work in validated environment

The *Work in validated environment* option has the following effects:

- The only OPUS functions that are available are those that have been declared as being *Validated Functions* (see chapter 2.2 and appendix A). All other functions will not be accessible, neither directly nor by macros or VB scripts.
- When measuring a spectrum the original data is securely stored (see chapter 2.3.1).

- Measurements can only be performed by using *released* (i.e. electronically signed) measurement experiment methods. For more details on releasing files and methods by electronically signing the files see chapter 4.5.
- Evaluation functions using method files (e.g. QUANT, IDENT) can only run by using *released* (i.e. electronically signed) method files.
- Evaluation methods (e.g. QUANT methods) can only be set up by using *released* (i.e. electronically signed) spectra.
- Library searching can only be done in *released* (i.e. electronically signed) user-generated libraries or (access protected) commercial libraries.
- Only *released* (i.e. electronically signed) spectra can be stored in user-generated libraries.
- Spectra and methods can be modified but cannot be overwritten by other spectra or methods.

If you use the *Advanced Measurement* command from the *Measure* menu when measuring in validation mode, you can only use *released* (i.e. electronically signed) measurements experiments. In this case it is not possible to change the measurement parameters. The *Measurement* dialog includes the following options (see figure 3).


Measurement

Experiment: Load DEFAULT

Operator name: Default

Sample name: sample

Sample form: sample form

Path: C:\Program\OPUS

File name: WORK

Figure 3: Work in validated Environment - Measurement Dialog

The *Setup Measurement Parameters* command in the *Measure* menu allows complete access to all measurement parameters and *released* (i.e. electronically signed) measurement experiments. In this case you can also use changed parameters in combination with the *Advanced Measurement* command without storing the corresponding measurement experiment. The HISTORY data block (see chapter 6), however, precisely indicates which parameters have been changed compared to the *released* measurement experiments.

If you want to make sure that only unmodified and *released* measurement experiments are used in validation mode, you have to assign limited access workspaces to the different users. These workspaces must not allow the user to access the *Setup Measurement Parameters* command in the *Measure* menu.

2.4 OPUS Test Plans

All test plans which have been used to validate OPUS functions, the necessary validation macros, test data and reference data as well as the required documentation are included in the *OPUS Software Validation Manual*.

In contrast to the hardware which has to be validated on a regular basis using OVP (*OPUS Validation Program*) it is normally not necessary to repeat the software validation tests for an installed system. For further details on OVP, refer to the OPUS Reference Manual.

2.5 Validating Methods, Macros, VB Scripts and other Software

2.5.1 Evaluation Methods

Extended OPUS packages like QUANT and IDENT or other evaluation functions like *Integration* and *Peak Picking* have been validated by Bruker. This means that the algorithms used for these methods have been proven to work properly.

If you are going to develop methods based on these functions (e.g. quantification of a certain component in combination with QUANT) you have to validate these specific methods yourself. The QUANT and IDENT software packages provide tools for method validation. For further details, see the OPUS QUANT and IDENT manuals.

OPUS assists you in this respect by restricting the use and setup of methods to signed (with *released* category) methods or spectra.

Note: The release signature has to be the last entry in the History Block of the spectra. If the evaluation method shall be modified later and some of the original spectra in the method have been modified in the meantime, these spectra have to be signed by the *release* category again.

2.5.2 Macros

Macros can be used to comply with paragraph 11.10 (f) of the *21 CFR Part 11* regulation. User-written macros should be validated as well. Note that you can only use validated OPUS functions within the macro, otherwise the macros might not run when activating the *Work in validated environment* check box.

Macros can be easily tested in the macro debugger where you can execute them step by step, observe results and verify whether they perform as expected.

By default, macros are stored as text files with the extension **.MTX*. To prevent unauthorized macro modifications of the macros you have to compile the macros once they have been validated. The compiled macros will have the same name as the original text file, but the extension **.MTB*.

Follow the steps listed below:

- Validate the (text) macro(s).
- Copy the original text macros onto a removable storage medium (e.g. disk) and keep them in a secure location or copy them onto a secure network server which operators have no access to.
- Compile the validated macro(s). Do not forget to compile sub macros used within the main macro(s) as well.

Note: It is recommended to start with the compilation of sub-macros, delete the original macro from the directory and check whether the main macro still runs. If not, it is to be expected that the main macro calls the sub-macros using <macroname.MTX>.

The compiled sub-macros are called <macroname.MTB> and will not be found by the main macro. In such a case, the main macro has to be modified such that all <macroname.MTX> calls are replaced by <macro-name(no file extension)>.

- After copying, delete the text macros from the local drive.

Modifying a compiled macro:

- Whenever it is necessary to modify a macro, copy the original macro text file onto the local drive.
- Modify the text version of the macro, re-validate it and make a new backup copy of the modified macro.
- Compile the modified macro.
- Delete the original text macro from the local drive.

2.5.3 Visual Basic – Scripts

The procedure with Visual Basic Scripts is similar. However, instead of compiling the text, the Visual Basic Script is encoded. Just as is the case with macros the encoded script can no longer be modified. Unfortunately, the encoded script cannot be decoded either. Therefore, you should always store a copy of the original VB Script before encoding it.

Encoding a VB script:

- First, make a backup copy of the VB script (file extension: **.OBS*) you want to encode.
- Make sure that the *Edit VB Scripts* check box on the *21CFR11 Rights* tab of the *User Settings* dialog is activated.
- Open the VB script. Click on the *Open* command in the *File* menu and select *OPUS VB script* from the *File type* drop-down list.
- Switch to *Object View.*
- Open the *Properties* dialog for the form and right click anywhere into the form.
- Select the *Active Engine* item.
- Select *VBScript.Encode* and click on *Apply.*
- Switch to *Script View.*
- Select *Encode* from the *Edit* menu.
- Save the VB script.

2.5.4 Other Software

The Client/Server interface allows external programs to communicate with OPUS. If you are using this option, the same restrictions must apply to these external programs as is the case for macros and Visual Basic Scripts. Always use compiled software versions of software to prevent abuse and keep the source code of these programs in a secure location, i.e. not on the local drive of the system.

2.6 Key Points

- The *Work in validated environment* option (Setup → User Settings → *21CFR 11 Rights* tab) is <u>required</u> for working in a validated environment.
- Set this option in <u>all</u> OPUS workspaces which are used on the system.
- Check the list of validated functions and packages. If you need access to functions which are not available in *Validation mode,* contact Bruker.
- Check existing macro and/or VB scripts for non-validated functions.

- Read the *Electronic Signatures* chapter.
- Validate your evaluation methods.
- Validate and compile macros.
- Validate and encode VB Scripts.
- Validate and use compiled versions of other external programs.

3 System Access Control

3.1 Reference to 21 CFR Part 11

The following paragraphs are discussed in this chapter:

11.10	Procedures and controls for closed systems
11.10 (d)	Limiting system access
11.10 (f)	Sequencing of steps
11.10 (g)	Authority checks
11.10 (h)	Device checks

3.2 General

It is assumed that the spectrometer and thus OPUS runs on a closed system. This means that the access to the spectrometer is only possible from the local data station and not from external systems e.g. via internet or telephone lines. In the latter case the IT personnel within the company must implement measures to ensure that access to the spectrometer system and the data is strictly limited to authorized personnel only. In general, this should be a very rare exception.

3.3 Access Control Features of the Operating System

3.3.1 General

OPUS requires Windows NT 4.0, Windows 2000 or Windows XP as an operating system. These operating systems already offer a quite extensive level of access security and allow the set up of individual user accounts for all operators working with the system.

The setup of security specifications and user accounts highly depends on the operating system and requires a knowledgeable and careful configuration. Thus, this will not be referred to in this manual.

In general, the management and configuration of operating system security is regulated by internal company standard operating procedures (SOPs) and is performed by the IT department.

The items listed below are to be seen as a guideline and should ideally be in accordance with your company SOPs.

3.3.2 Key Points of Access Control Features for the Operating System

- **The head of the laboratory or department should have a separate account with administrator rights** if this is in compliance with your company regulations. This account is useful because access to the OPUS User database and Signature data base is only allowed for users with *Administrator* rights for Windows and OPUS (see chapter 3.4). If the company policy does not allow to have *Administrator* rights for the operating system, you need the assistance of the IT department to modify the OPUS User and Signature database.
- **Standard operators should have *User* or *Power User* rights** but never *Administrator* rights. This is important to prevent operators accessing the OPUS User database (see comments above).
- You can create **individual user accounts for each operator** working on the system, and you can implement a **single group account for all operators** as OPUS itself offers an independent User Management (see chapter 3.4)
- The user account should **limit access to drives/directories/files** used for special purposes like archiving etc. Appendix B includes in the most relevant OPUS files and file extensions all files which can be set to *read only* (for standard operators), and files which require *write access* during standard operation of the system.
- For directories which are used to store measured spectra the **right to delete files** should be disabled. This allows the user to measure new data and process this data, but does not allow the user to delete any files in these directories.
- The user account should **limit the possibility to modify system settings.**
- The screen saver of the **operating system** should be protected by a **password** to lock the operating system after a specified (short!) inactivity time interval. This prevents access of unauthorized personnel to the system if the operator is not close to the system.
- Your company should have SOPs dealing with the importance of **password security** and consequences of **password abuse** and **password sharing.**
- Your company should have an **account policy for passwords** which regulates, for example, password length, password ageing.
- A user account should be locked as a result of **invalid login attempts,** i.e. when using a wrong password.
- Create a *Service* account for Bruker service personnel with *Administrator* rights. Lock this account by default and unlock it only when service of the instrument is required.

3.4 OPUS Access Control

3.4.1 General

OPUS offers an independent user account system which regulates access to both OPUS and OPUS workspaces. Users are managed in a user database which can only be accessed by operators who are logged into Windows with *Administrator* rights. Thus, it is desirable for the responsible person to have a Windows User Account with *Administrator* rights if this is not in conflict with company regulations. As an additional level of security the responsible person also needs to have *Administrator* rights for OPUS.

OPUS access control provides the following features:

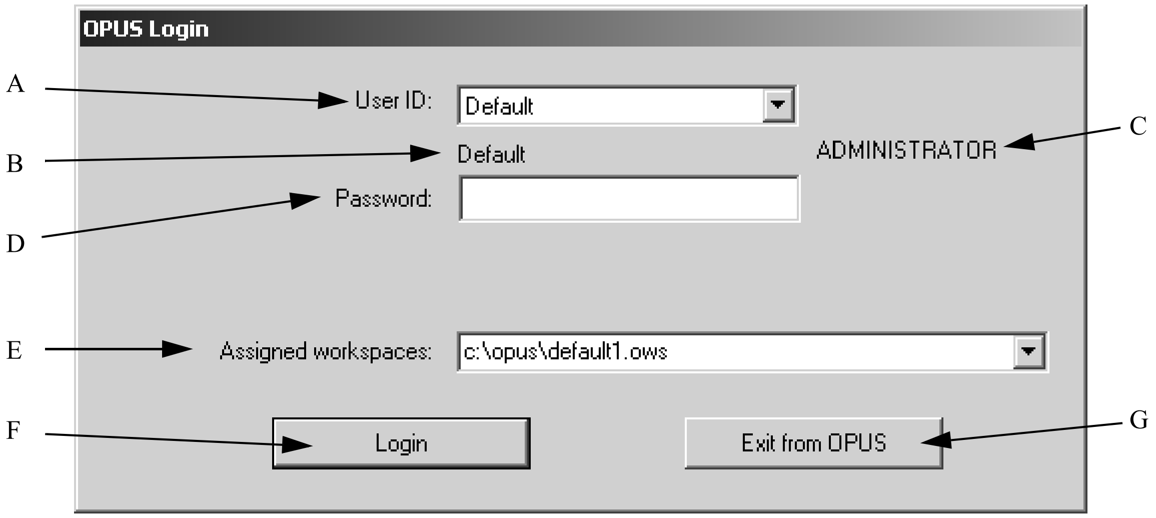
- OPUS user login with user authentication and workspace selection
- Logout function within OPUS to switch users without leaving OPUS, or to temporarily lock OPUS
- User-dependent audit trail
- *User Management* function to add new users or modify user records
- Global settings to adapt the system to company requirements (e.g. password ageing)
- Change *User Password* function
- Workspace configuration to customize the OPUS user interface

Independent access control for OPUS is essential if you want to implement a *shared desktop* system for multiple operators working on a single system. *Shared desktop* means that a group of operators can login into the operating system with a single *User ID/Password* combination which is known to all members of the group, while access to OPUS requires each operator to use a private User ID/Password combination which is only known to the operator. The advantage of such a configuration is obvious as this allows new users to login without re-booting the whole system. In addition, you can change between different users without even leaving OPUS.

3.4.2 First-Time OPUS Login

When installing OPUS a default user database is installed which includes two pre-defined user records, *Default* and *Administrator*. This allows immediate access to OPUS similar to all previous versions.

If you start OPUS, the following login dialog is shown:



User ID: Default

Default

ADMINISTRATOR

Password:

Assigned workspaces: c:\opus\default1.ows

Figure 4: OPUS Login

The User ID of all registered users can be selected from the *User ID* drop-down list (A). This prevents login attempts with unknown or incorrect user IDs. Below the *User ID* drop-down list the operator name (B) is indicated, which can differ from the User ID, together with the user type *Administrator* or *Operator* (C). The password (D) must be typed in and is always shown as a sequence of "*". The OPUS workspace, which will be loaded when OPUS is started, is selected from the *Assigned workspaces* drop-down list (E) (see chapter 3.5 for details about workspaces).

Clicking on the *Login* button (F) will start OPUS, while clicking on the *Exit from OPUS* button (G) will close this dialog.

Important: To prevent unauthorized access to OPUS you must change the password for *Default* and *Administrator* users (see chapter 3.4.8). We do NOT recommend deleting these two user records.

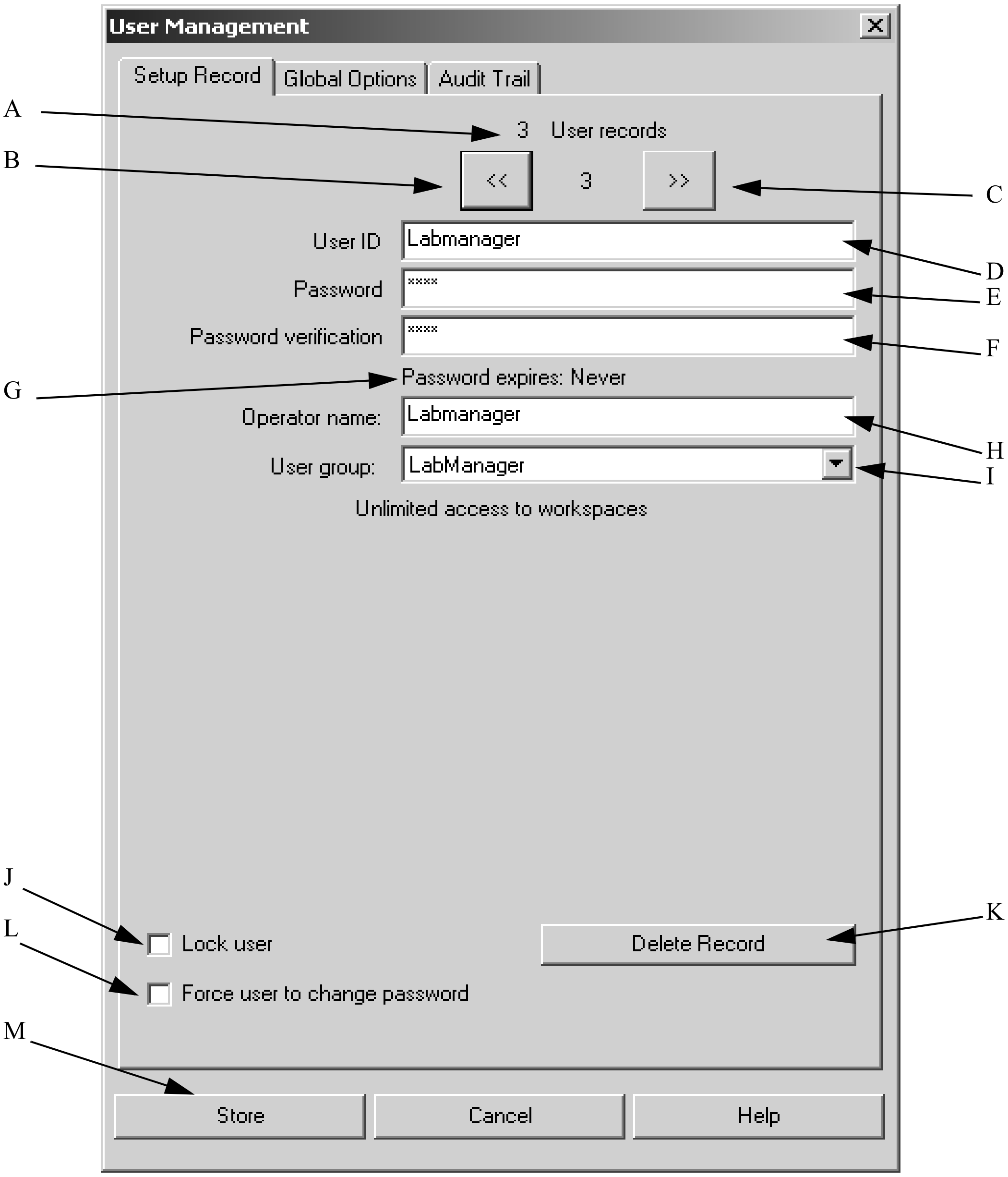
3.4.3 Adding a New User to the User Database

Select the *User Management* function from the OPUS *Setup* menu. This function can be used to modify existing records, or add new user records.

In order to ensure unique User ID/Password combinations the *User Management* function does not allow to create user records with the user ID or operator name being identical to an existing record. Both cases are clearly indicated, and such a record cannot be stored. How to create a new user record will be described in the following.

The user records are stored in the same database as the signature records (USERDATABASE.DAT in the USERDATABASE sub-directory of OPUS). The file is encrypted and thus cannot be modified externally. We recommend protecting this file against deletion, using the security options of Windows and making a backup copy whenever the file is modified.

Due to the necessity to write the audit trail into the database you must not set this file to *read only.*



User Management

Setup Record | Global Options | Audit Trail

3 User records

<< 3 >>

User ID: Labmanager

Password: ****

Password verification: ****

Password expires: Never

Operator name: Labmanager

User group: LabManager

Unlimited access to workspaces

☐ Lock user

☐ Force user to change password

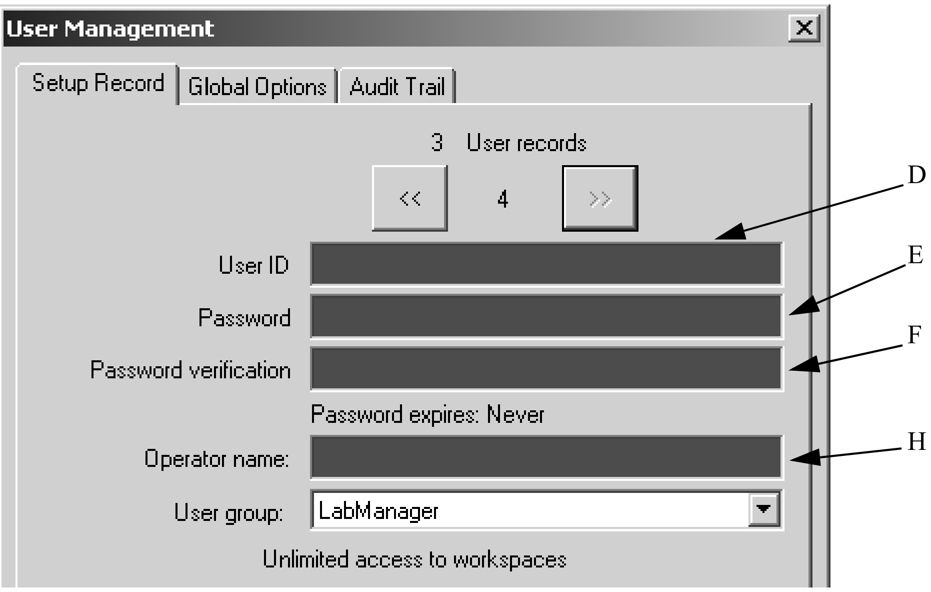
Figure 5: User Management - Setup Record

To add a new user select the *User Management* function in the *Setup* menu.

A) Total number of user records
B) Go to the previous record
C) Go to the next or to a new record
D) Entry field for User ID of user
E) Entry field for user password
F) Entry field for password verification
G) Information about password expiration
H) Entry field for operator name
I) Drop-down list for the user group
J) Check box to (temporarily) lock a user

K) Button to delete the current record
L) Check box to force user to change password
M) Button to store all changes

Click on the “>>” button (C) to go to a new empty page.



3 User records

4

User ID

Password

Password verification

Password expires: Never

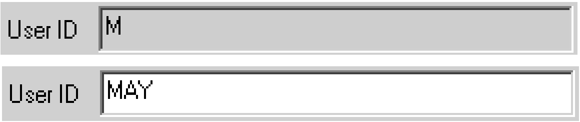
Operator name:

User group: LabManager

Unlimited access to workspaces

Figure 6: User Management - New Record

The entry fields (D), (E), (F) and (H) are now marked in red which means that these fields are required. Once you start entering text in any of the fields the field turns yellow until the entry specification (e.g. minimum length of User ID) is fulfilled. Once the entry specification is met (3 characters in figure 7) the entry field color turns to white.



User ID M

User ID MAY

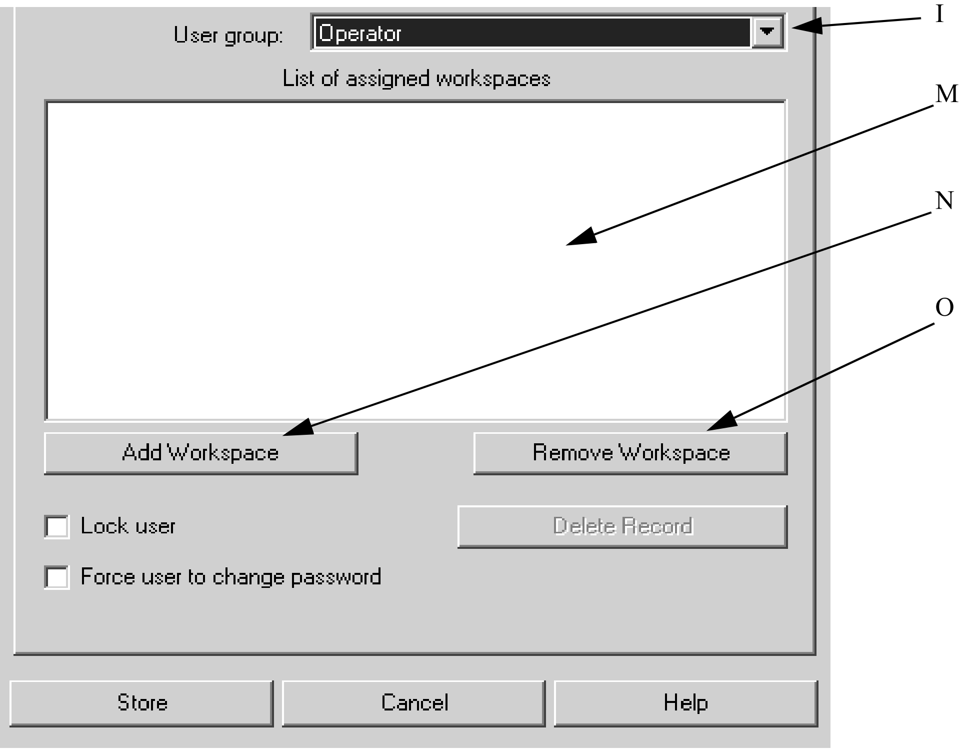
Figure 7: Entering User ID

Enter the following text:

- User ID → ***MAY***
- Password → ***test***
- Password Verification → ***test***
- Operator Name → ***Mayer***

Select *Operator* from the *User group* drop-down list (I in figure 8).

The lower part of the *User Management* dialog now shows a selection field (M) and two additional buttons (N) and (O in figure 8).



User group: Operator

List of assigned workspaces

□ Lock user

□ Force user to change password

Figure 8: Assigned Workspaces for Operators

M) Selection field of assigned workspaces
N) Button to add a workspace to the list
O) Button to remove the selected workspace from the selection field

Users belonging to the *Administrator* user groups have unlimited access to all OPUS workspaces, while users defined as *Operator* can only access those workspaces which have been added to the selection field of assigned workspaces (M).

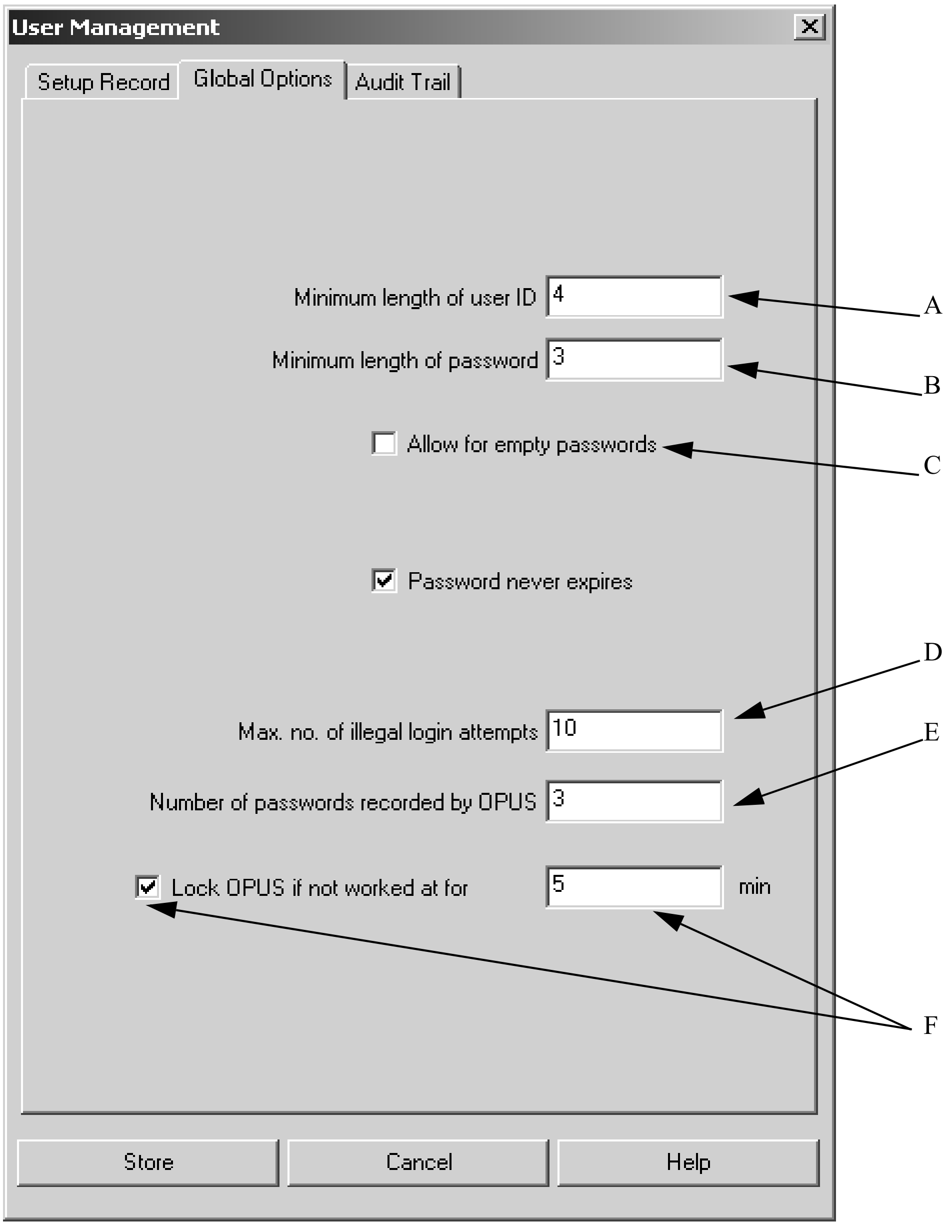
- Click on the *Add Workspace* button, the OPUS load box opens.
- Select the *Simple1.ows* and *Simple2.ows* workspaces and click on the *Load* button. Both workspaces are added to the selection field (M).

To remove a workspace from the selection field (M) select the workspace and click on the *Remove Workspace* button.

Click on the *Store* button to save the changes.

3.4.4 Global Options

The *Global Options* tab of the *User Management* dialog allows any company-specific regulations to be applied.



User Management

Minimum length of user ID: 4

Minimum length of password: 3

□ Allow for empty passwords

☑ Password never expires

Max. no. of illegal login attempts: 10

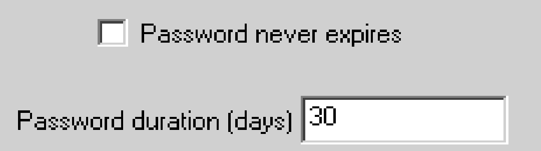
Number of passwords recorded by OPUS: 3

☑ Lock OPUS if not worked at for: 5 min

Figure 9: Signature Setup - Global Options

A) Entry field for the minimum length of user ID
B) Entry field for the minimum length of password
C) Check box to enable empty passwords
D) Entry field for the maximum number of illegal login attempts
E) Entry field for the number of password recorded by OPUS
F) Check box to lock OPUS after a certain period of time has passed

If you deactivate the *Password never expires* check box, an additional entry field will be displayed to specify the password duration in days:



□ Password never expires

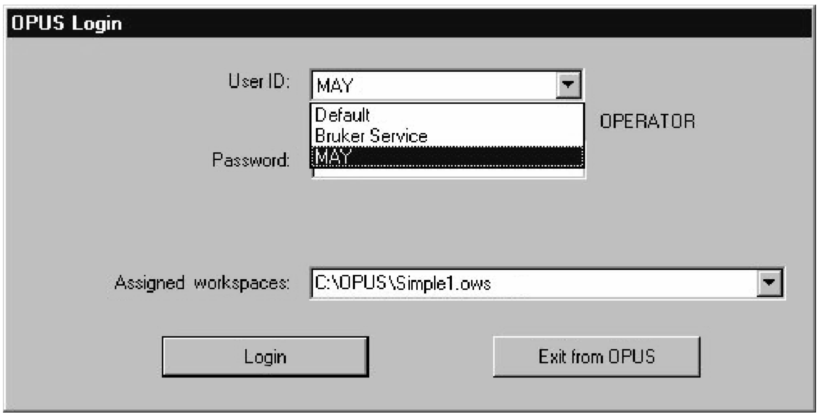
Password duration (days) 30

Figure 10: Password Duration

If the password duration is expired, you have to specify a new password (see chapter 3.4.8).

3.4.5 User Login

If you start OPUS the next time, the new user (MAY) can be selected from the *User ID* drop-down list in the *OPUS Login* dialog.



OPUS Login

User ID: MAY

Default
Bruker Service
MAY

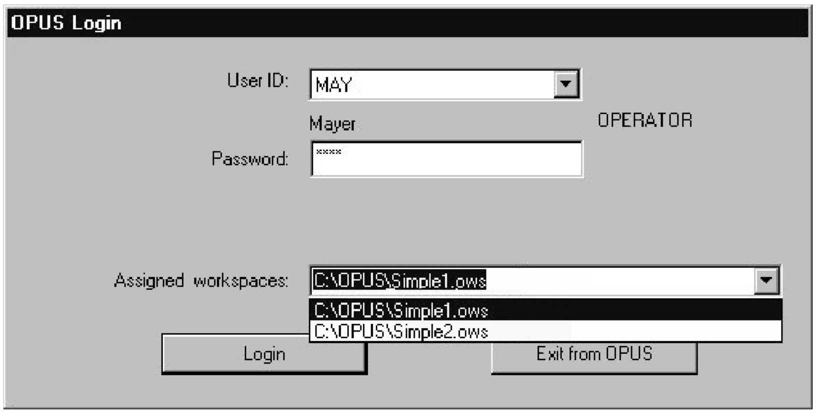
OPERATOR

Password:

Assigned workspaces: C:\OPUS\Simple1.ows

Figure 11: User Login

The workspaces which have been assigned to the user *Mayer* (i.e. *Simple1.ows* and *Simple2.ows*) can be selected from the *Assigned workspaces* drop-down list.



OPUS Login

User ID: MAY

Mayer

OPERATOR

Password: ****

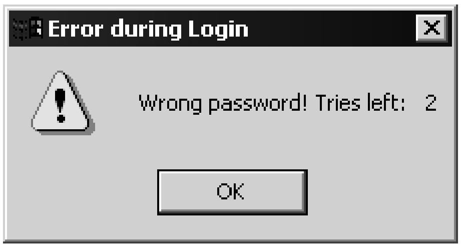
Assigned workspaces: C:\OPUS\Simple1.ows

C:\OPUS\Simple1.ows
C:\OPUS\Simple2.ows

Figure 12: User Login - Select Workspace

If you enter a wrong or mistyped password, a warning message pops up indicating the number of remaining login attempts. The maximum number of login attempts can be specified on the *Global Options* tab in the *User*

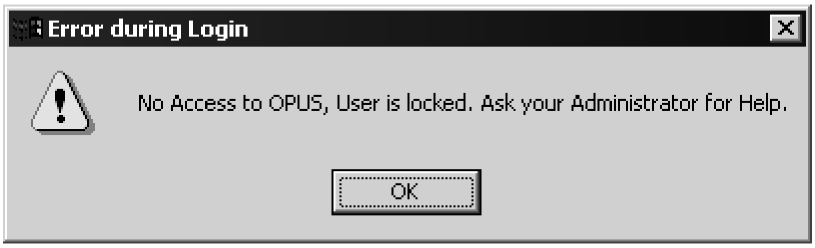
Management dialog. Once a user login has been successful the attempt count is automatically reset.


Error during Login

Wrong password! Tries left: 2

Figure 13: Error During Login - Wrong Password

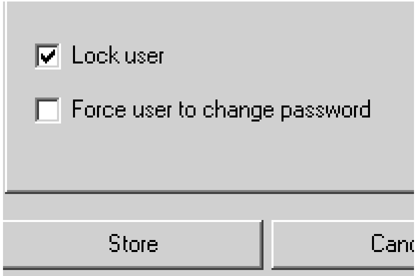
After the allowed number of tries the user will automatically be locked.


Error during Login

No Access to OPUS, User is locked. Ask your Administrator for Help.

Figure 14: User Locked

The lock prohibits any further access to OPUS, until the administrator has deactivated the *Lock user* check box on the *Setup Record* tab in the *User Management* dialog.

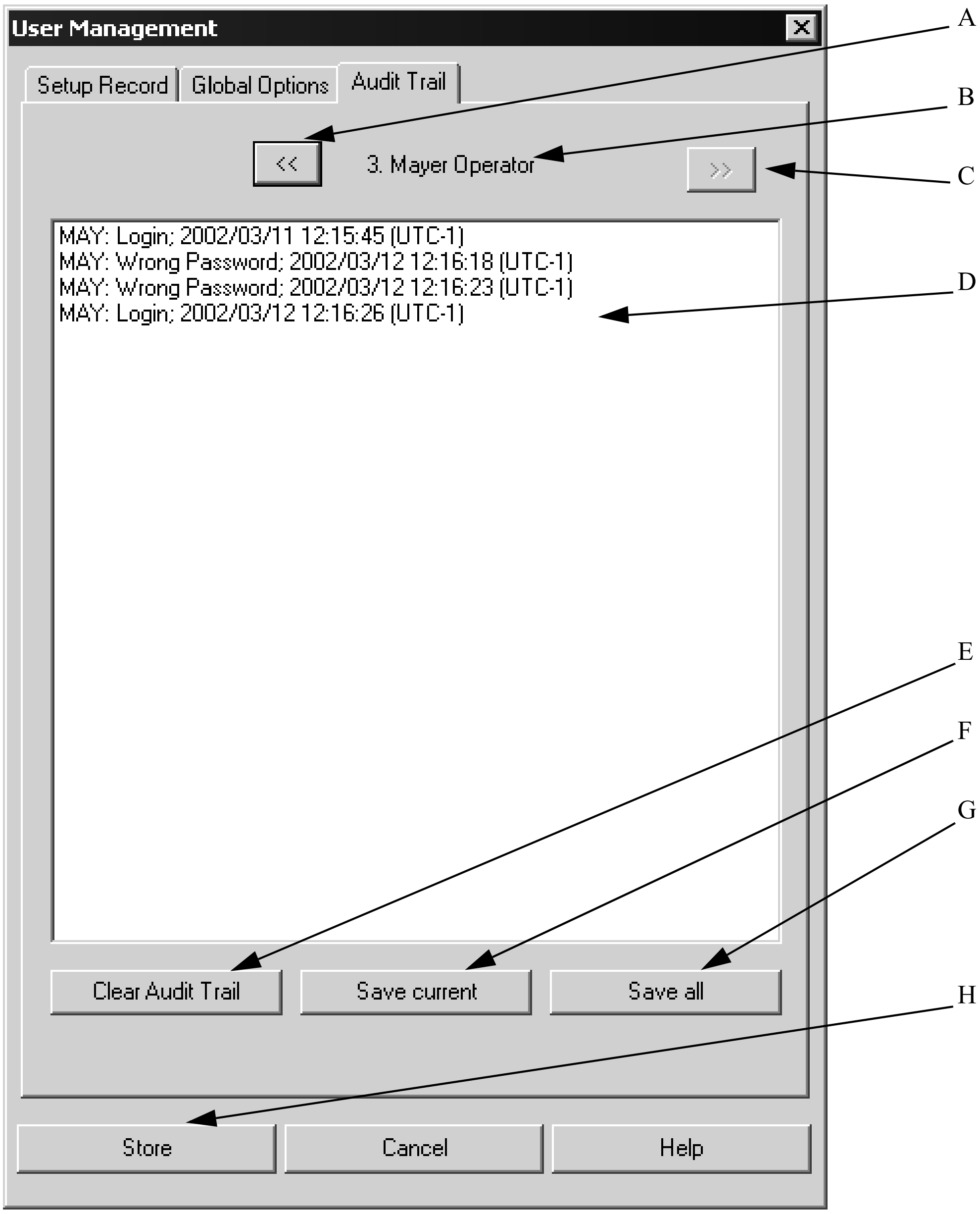

☑ Lock user

□ Force user to change password

Figure 15: Deactivate to Unlock User

3.4.6 User-Dependent Audit Trail

All logins, illegal login attempts and password changes are recorded in a user-specific audit trail. This audit trail can be controlled by the administrator. The *Audit Trail* tab of the *User Management* dialog shows the audit trail of each user.



```
MAY: Login; 2002/03/11 12:15:45 (UTC-1)
MAY: Wrong Password; 2002/03/12 12:16:18 (UTC-1)
MAY: Wrong Password; 2002/03/12 12:16:23 (UTC-1)
MAY: Login; 2002/03/12 12:16:26 (UTC-1)
```

Figure 16: User Management - Audit Trail

A) Use this button to go to the previous user record.
B) User name
C) Use this button to go to the next user record.
D) The selection field shows the audit trail with User ID, actions performed, date and time of the single actions.
E) This button clears the audit trail of the selected user. Note that the audit trail cannot be restored.
F) This button allows the current audit trail to be exported into a text file for archiving.
G) This button allows the audit trails of all users to be exported into a text file for archiving.
H) You must store the record if you have cleared the audit trail.

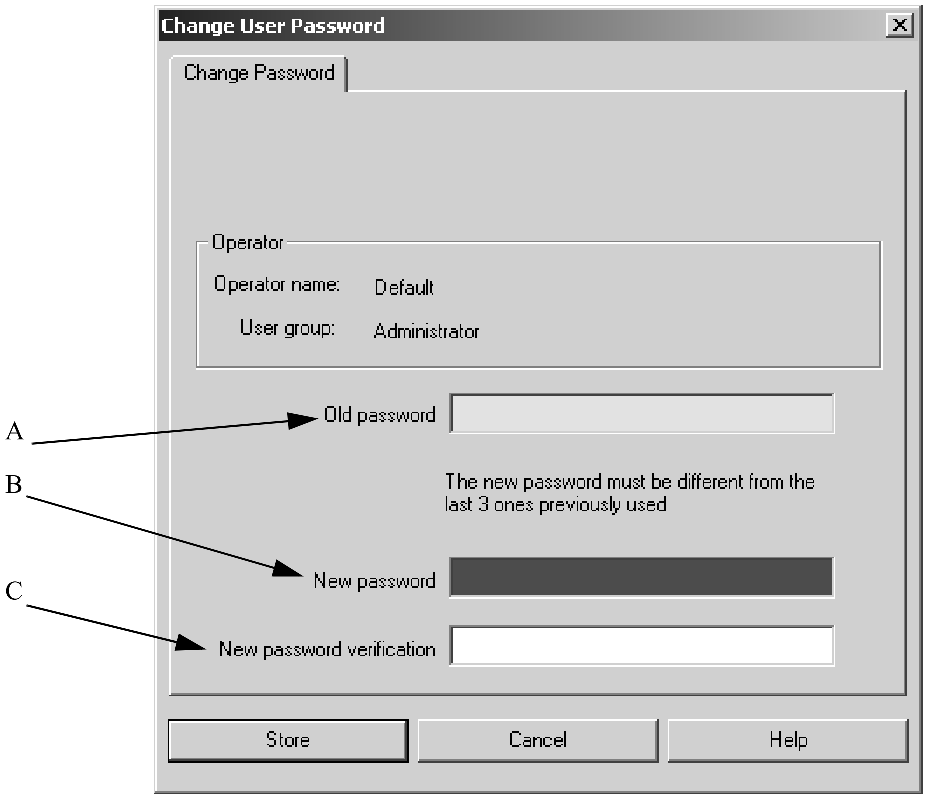
The audit trail cannot be deleted or modified by standard operators as they have no access to the *User Management* command.

3.4.7 Logout

The *Logout* command in the *Setup* menu allows to change between users without closing OPUS. If you click on the *Logout* command, the *OPUS Login* dialog will be displayed (see chapter 3.4.2). You can either login again using the same or a different user ID, or exit OPUS. Thus, selecting the *Logout* command also allows to temporarily lock OPUS.

3.4.8 Change User Password

Whenever required each user can change his password, provided the user is logged into OPUS by the previous password. Select the *Change User Password* command from the *Setup* menu. No separate login is required.



Change User Password

Operator

Operator name: Default

User group: Administrator

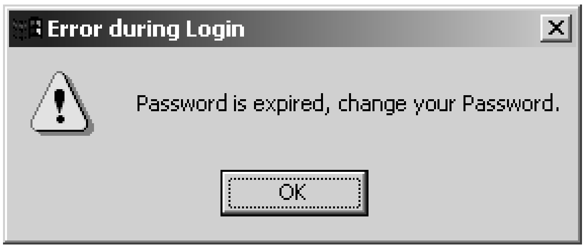
The new password must be different from the last 3 ones previously used

Figure 17: Change User Password

The entry field for the old password (A) is displayed in yellow. As soon as you enter the old password the entry field turns to white. When entering the new password (B), make sure that it is different from the last one previously used. Verify the new password (C).

The global settings (see chapter 3.4.3), i.e. minimum length of the password and password duration, apply to the *Change User Password* command as well. If the password ageing option is activated, the expiration time is automatically reset when changing the password. To store the new password click on the *Store* button.

If a user attempts to log in with an expired password a warning message is shown.



Password is expired, change your Password.

Figure 18: Error During Login - Password Expired

If you click on the *OK* button, the *OPUS Login* dialog pops up. Enter the new password (A) and verify it (B).

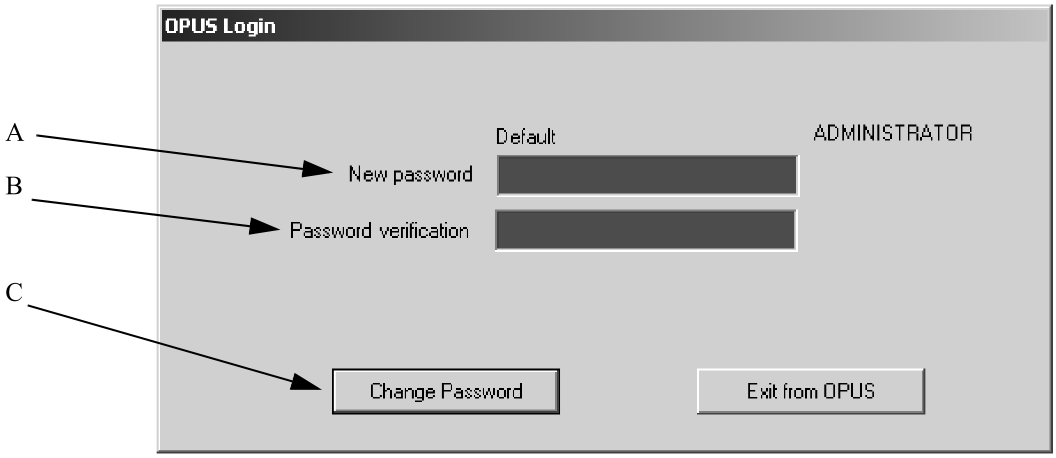


Figure 19: Enter and Verify New Password

Click on the *Change Password* button (C), and the *OPUS Login* dialog is displayed again. Now, login by using the new password.

3.4.9 Bruker Service

Due to security reasons no special Service record has been added to the default OPUS User Database. Therefore, make sure that the Bruker service engineer can get *Administrator* access to OPUS if any service is required.

We recommend writing a special procedure for service visits which clearly defines what has to be done prior to, during and after a service visit.

3.4.10 Key Points of OPUS Access Control

- As soon as you have installed OPUS, immediately change the password for *Default* and *Administrator* users.
- If there is no global company policy, define a password policy to ensure authenticity and confidentiality of user passwords.
- Adapt the *Global Settings* to your (company) password policy.
- Set up a user record for each operator who works with OPUS.
- Keep the OPUS CD at a secure place to prevent (temporary) replacement of your user database.
- Do not write-protect the user database but protect it against deletion.
- Implement procedure controls for service visits and train operators accordingly.

3.5 OPUS Workspace Configuration

3.5.1 General

Due to the configuration of the OPUS user interface the OPUS workspaces provide an additional extended level of security. The basic features which can be specified in a workspace are:

- Toolbar configuration
- Menu configuration
- Basic path settings
- Access restrictions

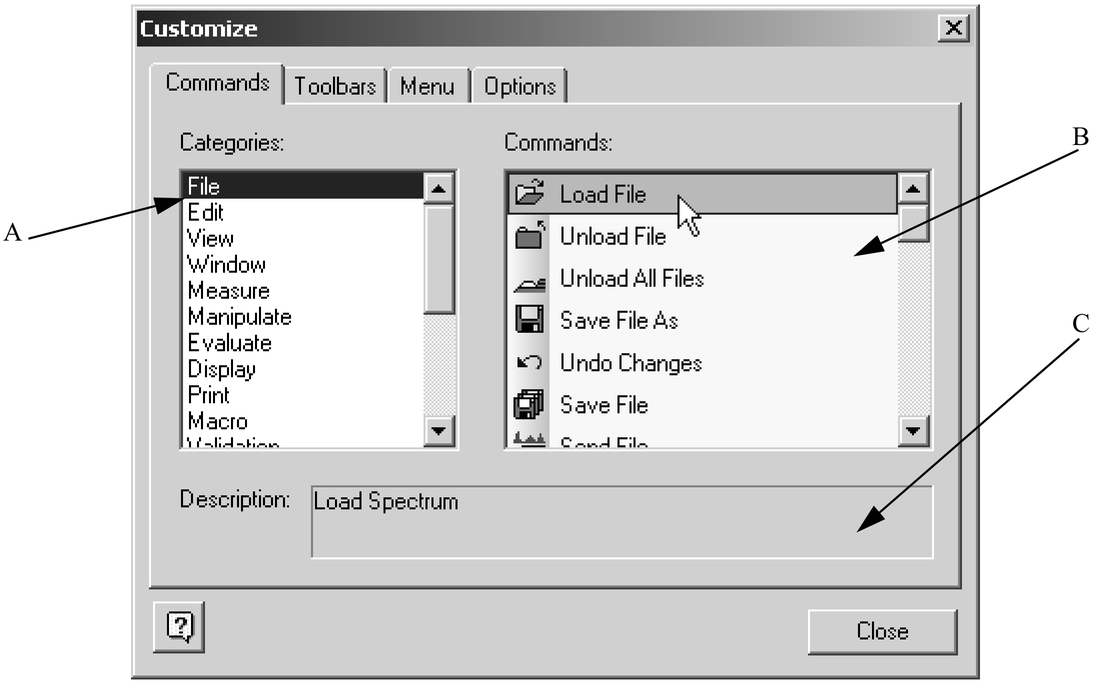
The ability to configure both the toolbar and the menus allows to limit operator access to just a few selected OPUS functions, or even to only specific macros or Visual Basic scripts.

Each registered user can work with more than one workspace provided these workspaces have been properly assigned (see chapter 3.4.3). This enormously extends the flexibility and possibilities when working with OPUS.

The *User Settings* dialog has additional options which are not relevant when working in a validated environment and are therefore not discussed in this manual. For further details on these options, refer to the OPUS Reference Manual.

3.5.2 Customizing Toolbars

To configure OPUS toolbars select the *Customize Toolbars* command from the *Setup* menu.

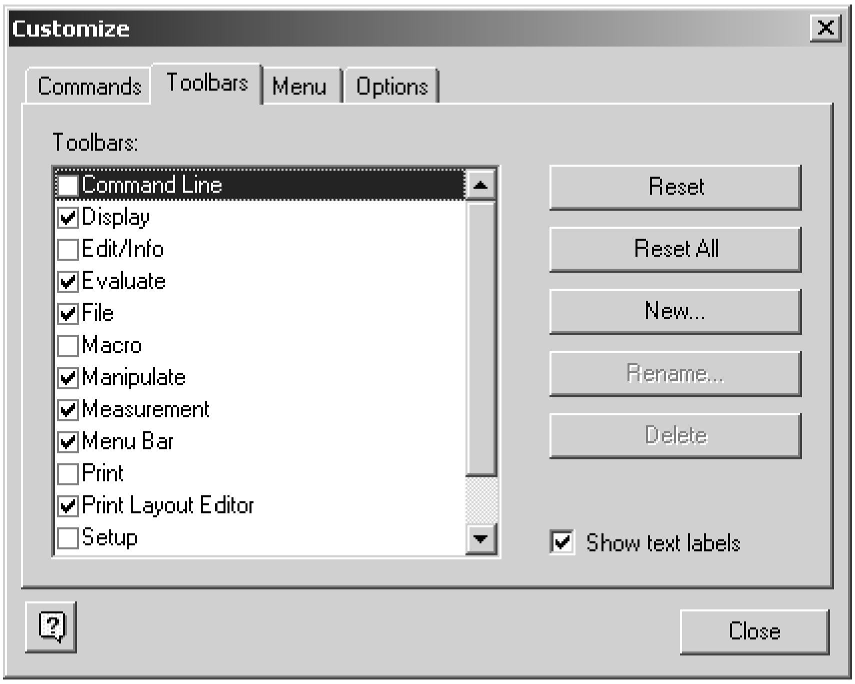


Load Spectrum

Figure 20: Customize - Toolbars

The *Commands* tab contains both the different menu categories and menu commands with the respective icons. If you, e.g., select the *File* category (A in figure 20), all commands available for the *File* menu are displayed in the *Commands* drop-down list (B). If you click on any command in this drop-down list, a short text (C) comes up describing this command. For further information on this dialog refer to the OPUS Reference Manual.

The *Toolbars* tab helps to define which OPUS toolbar is to be displayed.



Customize

Toolbars:

- □ Command Line
- ☑ Display
- □ Edit/Info
- ☑ Evaluate
- ☑ File
- □ Macro
- ☑ Manipulate
- ☑ Measurement
- ☑ Menu Bar
- □ Print
- ☑ Print Layout Editor
- □ Setup

☑ Show text labels

Figure 21: Customize - Toolbars

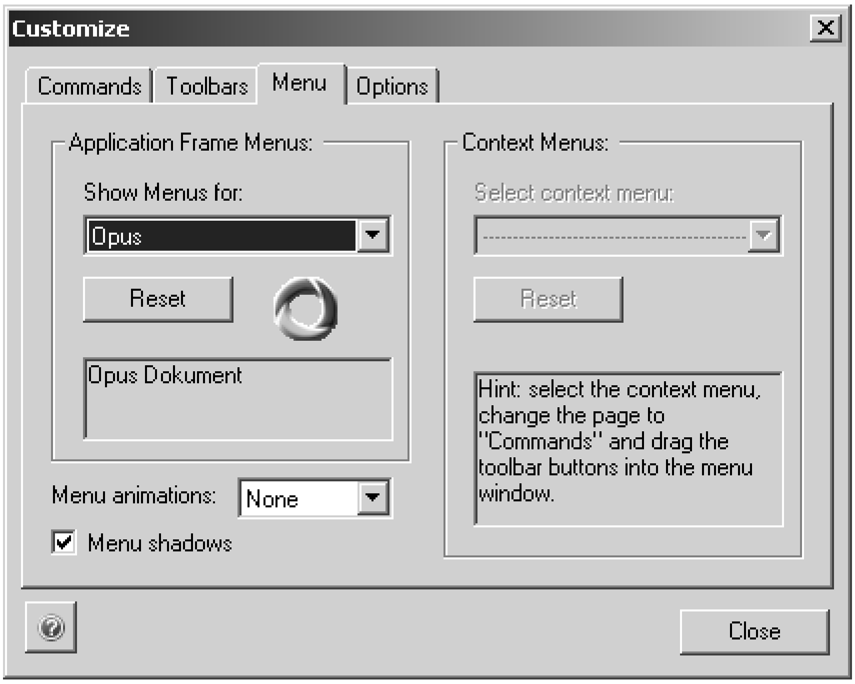
Therefore, set a check mark in front of the toolbar name. If you remove the check mark, the toolbar will not be displayed. To generate additional toolbars proceed click on the *New* button. For further detailed information on this subject refer to the OPUS Reference Manual.

To reset the standard OPUS toolbars, i.e. have them displayed by their default symbols, names and commands, set a check mark in front of the toolbar name and click on the *Reset* button. Similar to this, all toolbars which have a check mark in front can be set to their default contents by clicking on the *Reset All* button.

Further settings can be made on the Options tab. For details refer to the OPUS Reference Manual.

3.5.3 Customizing Menus

To configure OPUS menus select the function *Customize Menus* command from the *Setup* menu.



Show Menus for: Opus

Opus Dokument

Menu animations: None

☑ Menu shadows

Hint: select the context menu, change the page to "Commands" and drag the toolbar buttons into the menu window.

Figure 22: Customize - Menu

Select the workspace for the menu to be customized from the *Show Menus for* drop-down list. You can edit the menus for the following OPUS workspaces:

- OPUS
- PLE (Plot Layout Editor)
- VBScript
- GMacro
- Default Menu

To undo the changes made click on the *Reset* button, and the menus of the workspace in question are displayed again with their standard icons and commands. For further detailed information on how to configure menus refer to the OPUS Reference Manual.

3.5.4 Adding Macros and Visual Basic Scripts to the OPUS User Interface

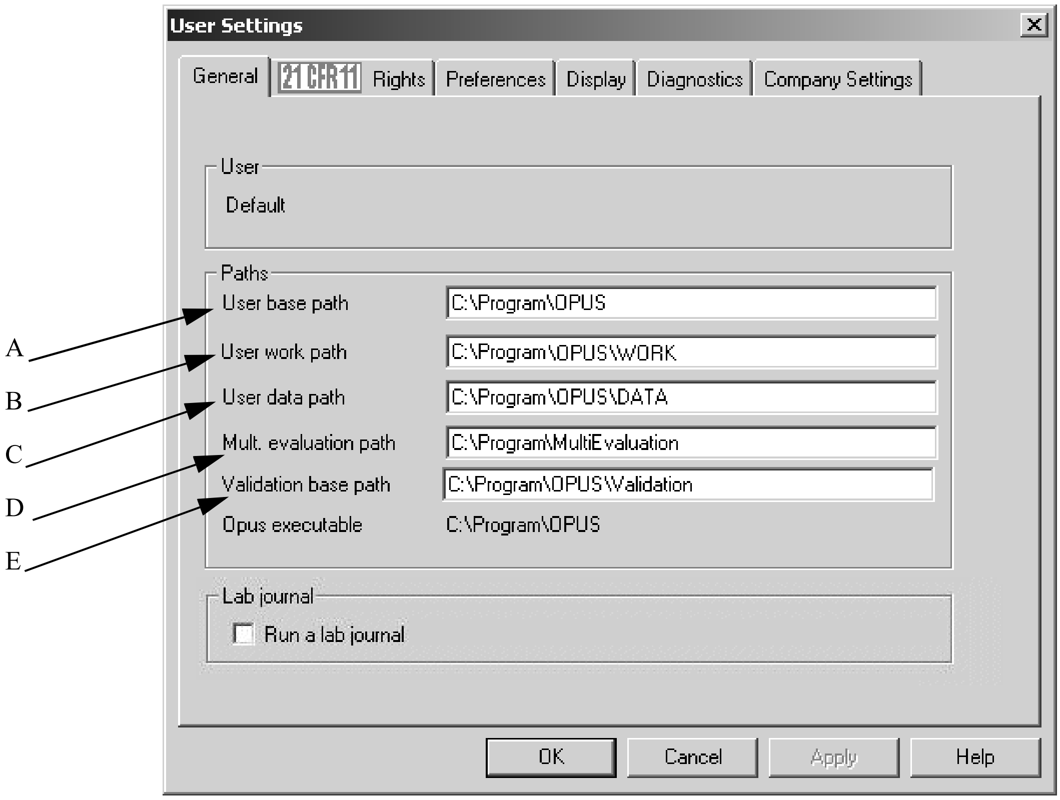
Macros and Visual Basic Scripts are an important tool to fulfill the requirements of Paragraph 11.10 (f) of the *21 CFR Part 11* regulation: "*...to enforce permitted sequencing of steps...*". If a certain method requires a fixed sequence of manipulation and evaluation steps, the only way to ensure that all the steps have been performed and properly executed is to execute a macro or Visual Basic script. In such a case we recommend removing all functions from the menus and toolbars and adding only the macros/VB scripts describing the pre-defined sequence of steps to menus and toolbars.

A global list of all executable macros and VB scripts, which should be made available in OPUS, can be set up by selecting the *Setup User Macro List* command in the *Setup* menu. For further details on this subject refer to the OPUS Reference Manual.

Both the *Customize Toolbars* and *Customize Menus* command allows these macros/VB scripts to be used in exactly the same way as native OPUS functions.

3.5.5 Basic Path Settings

The *User Settings* command, which has partly been described in chapter 2.3, displays the individual path settings of a workspace on the *General* tab.



User
Default

Paths
User base path: C:\Program\OPUS
User work path: C:\Program\OPUS\WORK
User data path: C:\Program\OPUS\DATA
Mult. evaluation path: C:\Program\MultiEvaluation
Validation base path: C:\Program\OPUS\Validation
Opus executable: C:\Program\OPUS

Lab journal
□ Run a lab journal

Figure 23: Basic Path Settings

A) The user base path is the individual workspace home directory, i.e. operators can measure and store spectra in this directory or its sub-directories specified. Other operators should not get access to this path.

B) All temporary files are stored in this path.

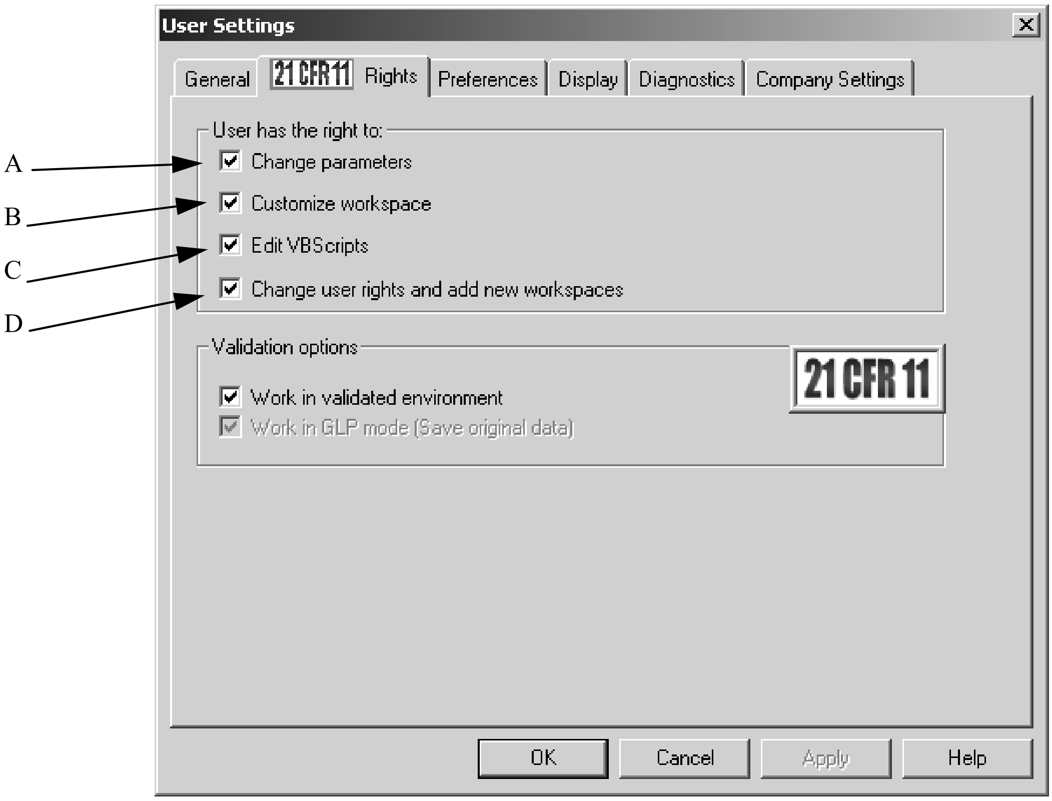
C) All user data are stored in this path.

D) Multi evaluation method files are stored in this path.

E) All OVP data, i.e. reports, files, databases etc. are stored in this path.

3.5.6 Access Restrictions

The *21CFR11 Rights* tab provides several access restrictions, also see chapter 2.3.



User has the right to:

☑ Change parameters

☑ Customize workspace

☑ Edit VBScripts

☑ Change user rights and add new workspaces

Validation options

☑ Work in validated environment

☑ Work in GLP mode (Save original data)

Figure 24: User Rights

A) If you deactivate the *Change parameters* check box, function dialogs will not show any parameter tabs and disable the setting of parameters on the first main tab. You can only execute functions by using the pre-defined parameters.

Furthermore, if you deactivate this check box, make sure that the parameters for all accessible functions are properly set. If you want to allow the selection of certain parameters for certain functions only, you have to write an appropriate macro or Visual Basic script.

B) The *Customize workspace* check box enables or disables the customizing of toolbars and menus. It is recommended to deactivate this option.

C) The *Edit VBScripts* check box enables or disables the editing of Visual Basic scripts. This option should only be activated in case of operators who are in charge of creating VB script.

D) The *Change user rights and add new workspaces* check box should generally be deactivated for all operator workspaces. Administrators or operators only who are in charge of setting up workspaces should be allowed to change user rights and add new workspaces.

Note that none of the workspace settings can be changed if a workspace is stored with this check box being activated. Therefore, we highly recommend keeping additional copies of all workspaces where this option is enabled to allow you to modify a workspace without the need to configure it completely from the very beginning. Keep these copies at a safe place and delete local copies of these workspaces from the local drive.

3.5.7 Key Points of Workspace Configuration

- Use the *Customize Toolbars* command to add icons and OPUS functions to or remove them from the toolbars.
- Use the *Customize Menus* command to add OPUS functions to or remove them from the menus.
- Supply macros and/or Visual Basic Scripts for a pre-defined sequence of steps and add these macros/VB scripts to toolbars and menus.
- Create a separate home directory for each operator and for all workspaces which are assigned to this operator.
- Deactivate the *Change parameters* check box if you do not want an operator to change any of the function parameters.
- Deactivate the *Customize workspaces* check box in all workspaces defined for the operator.
- Deactivate the *Edit VB Scripts* check box in all workspaces defined for the operator.
- Deactivate the *Change user rights and add new workspaces* in all workspaces defined for the operator.
- Keep copies of all workspaces defined for the operator with the *Change user rights...* check box being activated on a secure location. Remove all these workspace copies from the local drive.
- Remove all workspaces with the *Change user rights...* check box being activated from the local drive.

4 Electronic Signatures

An essential part of the *21 CFR Part 11* regulation is the possibility to **electronically sign** an **electronic record**.

4.1 Reference to 21 CFR Part 11

The following paragraphs are discussed in this chapter:

11.50 (a)	Associated Information in Electronic Signatures
11.50 (a)(1)-(3)	Components of an Electronic Signature
11.50 (b)	Control of Electronic Signatures
11.70	Record - Signature linking
11.100 (a)	Uniqueness of Electronic Signatures
11.200 (a) (1)-(1ii)	Execution of Electronic Signatures
11.300 (a)	Uniqueness of User ID/Password combinations
11.300 (b)	Periodic check of Passwords
11.300 (d)	Reporting illegal access attempts

4.2 Definitions

- **Electronic Records**

  OPUS spectra files and method files are electronic records in the sense of the *21 CFR Part 11* regulation.
- **Electronic Signature**

  An electronic signature is stored in a separate data block of the spectra file as soon as this file is signed. This data block contains all the information required by the *21 CFR Part 11* regulation.
- **Signature Record**

  The data of a person who is authorized to sign files is stored as a signature record in a data base. A separate signature record is created for each person.
- **Signature Database**

  The database where the signature records are stored. The same data base is used for user records.
- **Signature User ID**

  User ID of a signer. This user ID is required to access the signature function within OPUS.

- **Signature Password**

  Password to access the signature function within OPUS. The combination of the signature user ID and signature password must be unique on one single system.

4.3 Setting up Signature Records

Before you can sign any files in OPUS you must specify at least one signature record.

Note: *User Records* and *Signature Records* can only be created, modified or deleted by operators who have *Administrator* rights for the operating system as well as for OPUS. Otherwise this function is not accessible in OPUS.

4.3.1 Signature Setup

Select the *Signature Setup* command from the *Setup* menu. The following dialog opens:

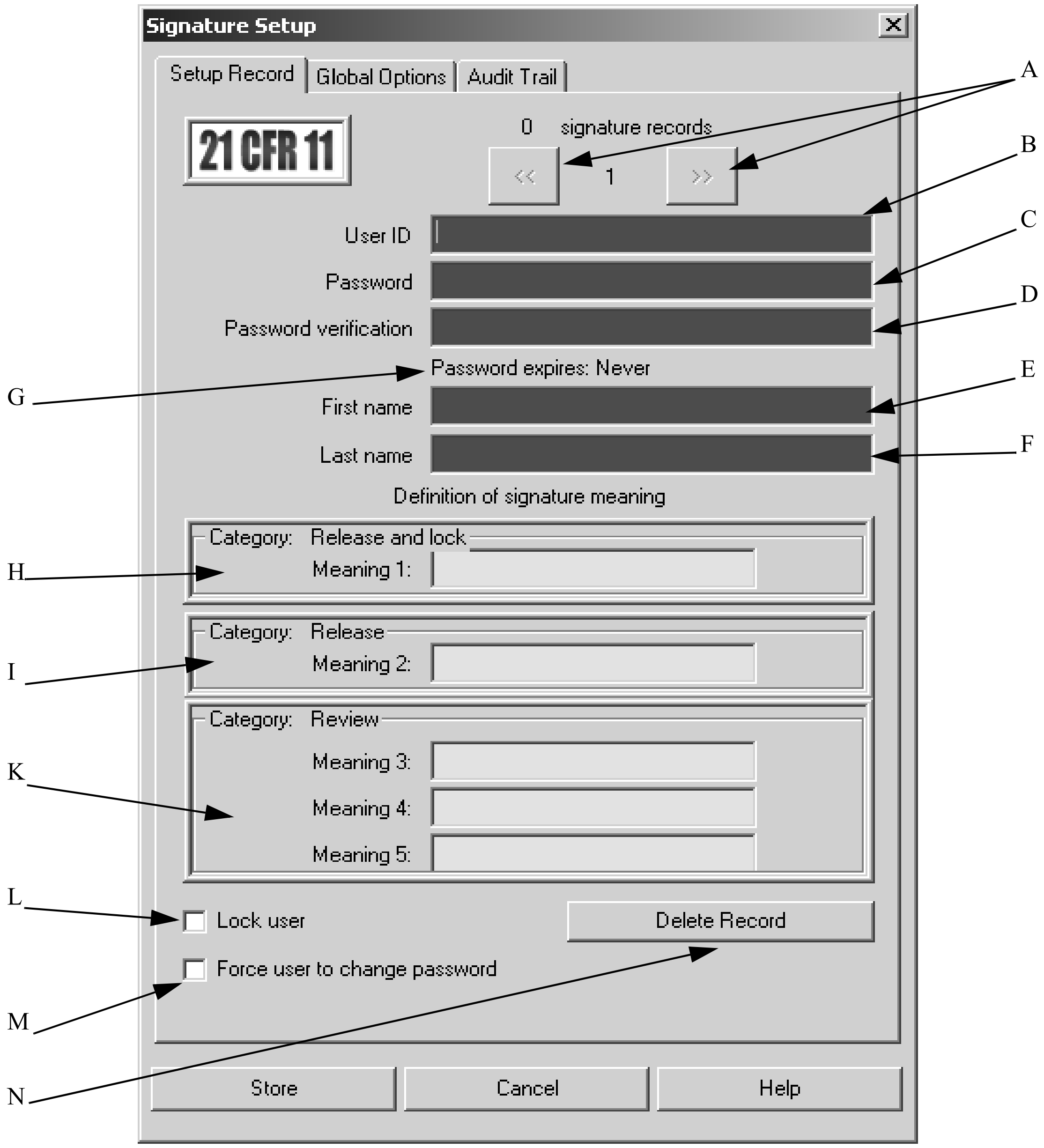


Figure 25: Signature Setup - Setup Record

A) Buttons to go to the previous or next signature records.

B) Enter the signature *User ID* for the signer. The user ID must have a minimum length to be specified on the *Global Options* tab. The entry field changes its color from red to yellow when you start typing, and switches to white if the length of the user ID is sufficient. The user ID is required to log into the signature function itself.

C) Enter the initial signature *Password* for the signer. The password must have a minimum length to be specified on the *Global Options* tab. The entry field changes its color from red to yellow when you start typing, and switches to white if the length of the password is sufficient. The password is always case sensitive and is required to log into the signature function. The entry in the password field is shown as a sequence of “*”.

D) Re-enter the password for verification. This prevents problems with typing errors. The entry field changes its color from red to yellow when you start typing, and switches to white if the entry matches the password. Otherwise, the entry field changes to red. In such a case either re-enter the password or the password verification. The entry in the password verification field is also shown as a sequence of “*”.

E) First name of the signer. This name is written into the signature block to identify the signer.

F) Last name of the signer. This name is written into the signature block to identify the signer. OPUS does not allow two identical combinations of the first and last name on one single system.

G) This line shows the current password duration (if any). The password duration option can be specified on the *Global Options* tab.

H) Entry field for signature meaning 1. The category of this meaning is *Release and Lock* which means that a file signed by this meaning can no longer be modified in OPUS. This category is mainly used for archiving purposes of spectra or to prevent accidental overwriting of method files (see chapter 4.5 for more details).

Note: If you use this category for spectrum files which have been signed, the files can only be displayed in OPUS but not modified anymore. Even evaluation functions cannot be used anymore as they write results into the file.

I) Entry field for signature meaning 2. The category of this meaning is *Release*. The *Release* signature is required to use measurement experiments and all other types of method files in validation mode. Spectrum files must have a *Release* signature if they are to be used for creating methods. In contrast to the *Release and Lock* category the signed files can still be modified in OPUS after they have been signed. Note that a modification after signing invalidates the *Release* signature.

K) Three entry fields for signature meaning 3, 4 and 5. The category of this meaning is *Review*. This type of signature has no special effect in OPUS and thus can be used without limitation.

L) Option to lock a signer. The lock is automatically set if the number of illegal login attempts (i.e. a signer tries to log in with a wrong password) for the signer exceeds the maximum number specified on the *Global Options* tab. This option can also be used to temporarily disable signature access, e.g. if a signer is temporarily absent from the company.

M) If you activate the *Force user to change password* check box, the user has to change the signature password when performing a signature next time.

N) Use the *Delete Record* button to permanently delete the current record from the signature database. Once a signer has been removed from the signature database, login attempts by using his user ID are registered as unknown user.

Store all new records and modifications in the data base by clicking on the *Store* button.

The total number of signature records is shown on top of the *Signature Setup* dialog between the two arrow buttons.

All entry fields which must be filled in are initially marked red. If you start filling in any of the red entry fields, the color of the entry field changes to yellow after the first character has been typed in. The color of the entry field remains yellow as long as the number of characters typed in is lower than the number specified for the current field. If the minimum number of characters is reached, the entry field color changes to white indicating a valid input.

The default settings for the different fields are:

• User ID:	3 characters
• Password:	4 characters

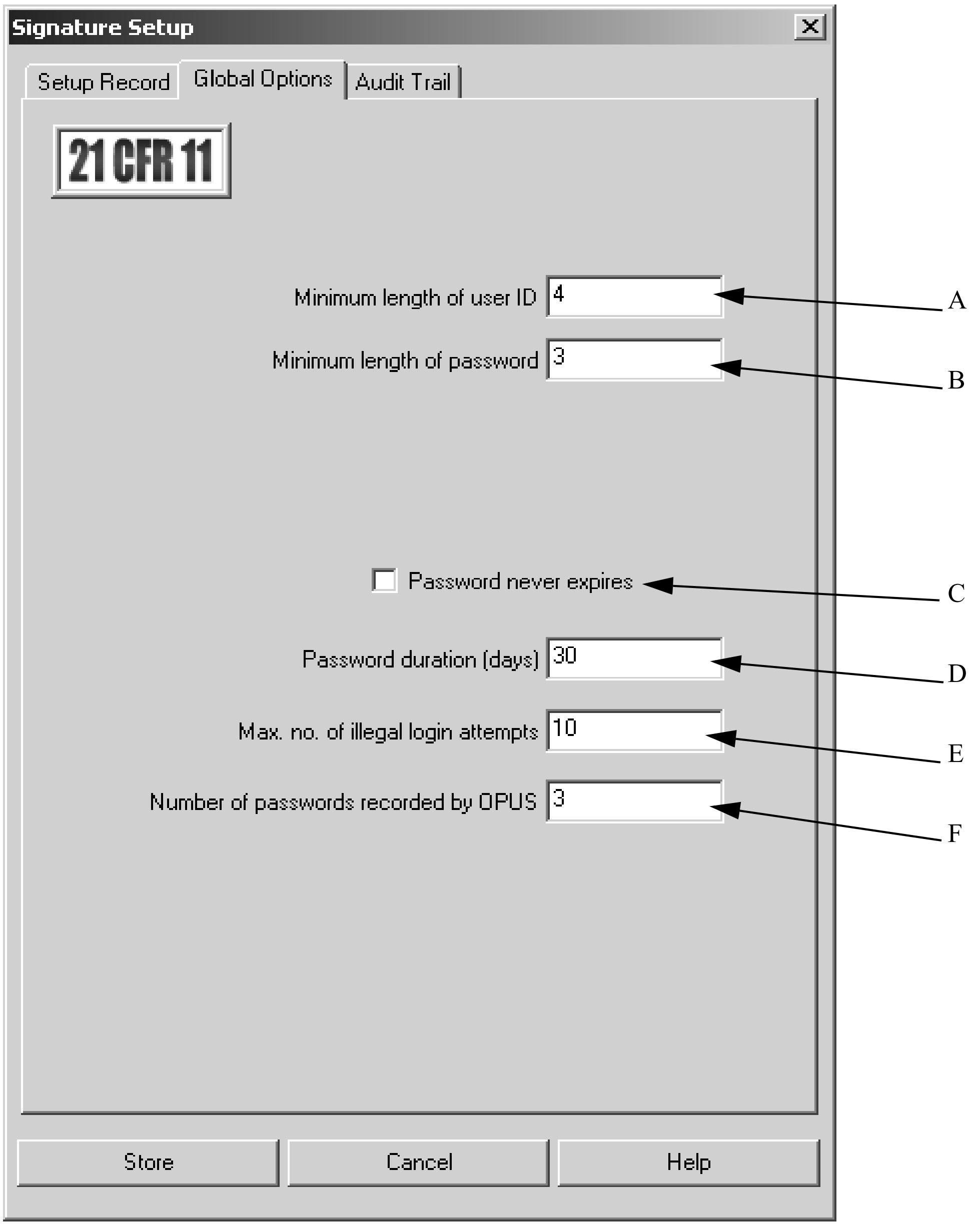
The default settings can be changed on the *Global Options* tab and will immediately influence all signature records.

The color of the password verification field will only change to white if the text entered is identical with the text entered into the password field. Duplicate user IDs or duplicate combinations of first and last names are not allowed and will be indicated by red entry fields. It is not possible to store the signature records, unless all entry fields and at least one signature meaning field show valid entries, i.e. their color turns to white.

The signature records are stored in the same database as the OPUS users (USERDATABASE.DAT in the USERDATABASE subdirectory of OPUS). The file is encrypted and therefore cannot not be modified externally. We highly recommend protecting this file against deletion using the security options of Windows, and to make a backup copy whenever you modify this file. **Due to the necessity to write the audit trail into the database you must not set this file to read only**!

4.3.2 Global Options

The *Global Options* tab is identical to the *Global Options* tab described in chapter 3.4.4. **The settings apply to both user records as well as signature records.** Empty passwords are not allowed for signature records. Thus, this option is not available in the signature setup.



Minimum length of user ID 4

Minimum length of password 3

□ Password never expires

Password duration (days) 30

Max. no. of illegal login attempts 10

Number of passwords recorded by OPUS 3

Figure 26: Signature Setup - Global Options

A) Minimum length of user ID
B) Minimum length of password
C) Password duration option
D) Password duration in days
E) Maximum number of illegal login attempts
F) Number of passwords previously used for the respective signature. OPUS records these passwords which cannot be used anymore when changing the password.

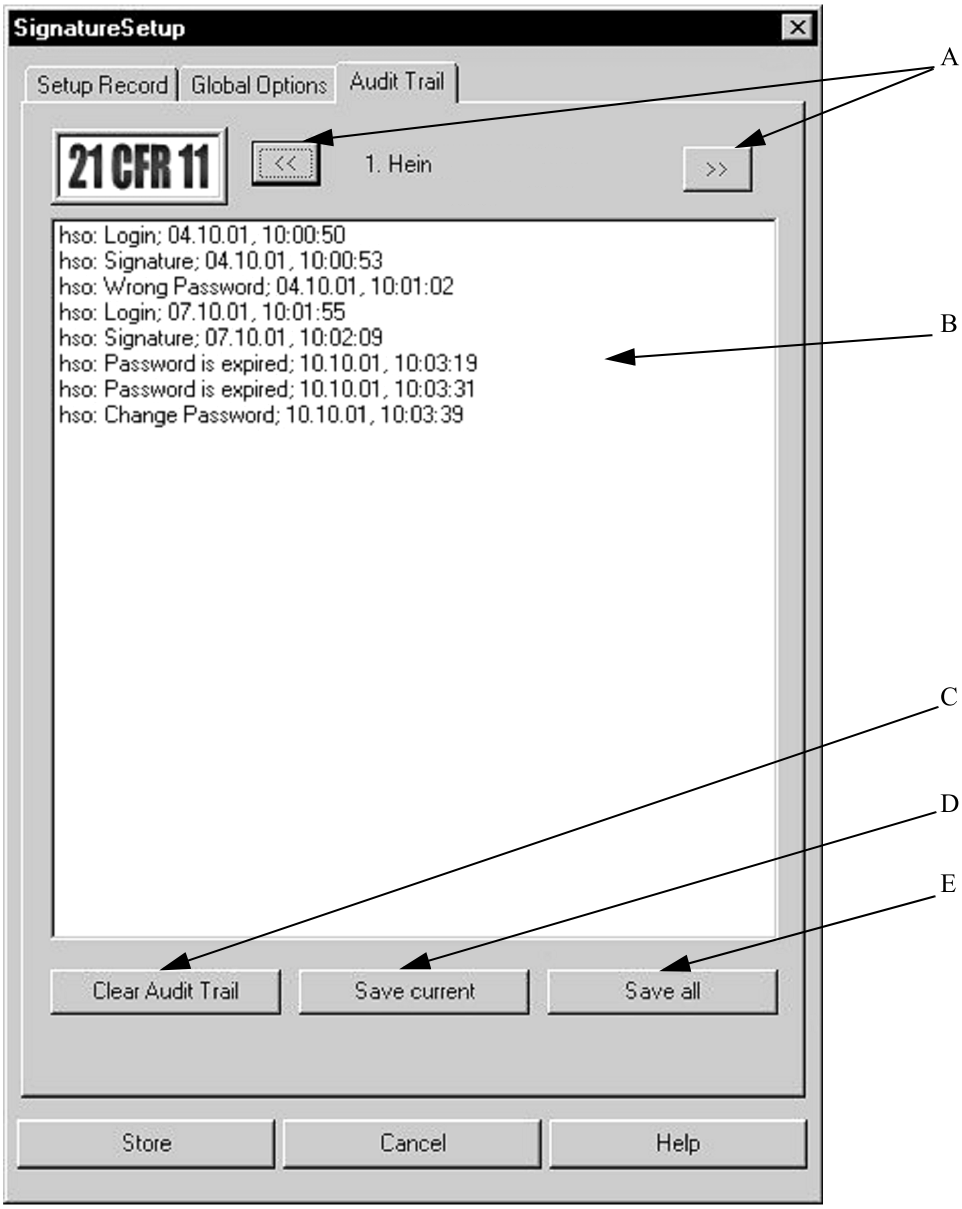
The settings apply immediately to all signature records in the data base. Therefore, you have to check all signature records if you have modified any of the options. Illegal entries will be marked in red.

4.3.3 Signature Audit Trail

The *Audit Trail* tab shows the audit trail of all actions for each signer. The following events are recorded:

- Successful login
- Signature execution
- Password change
- Login attempt of a locked user
- Login with expired password

A global audit trail (user index 0) shows all login attempts of unknown users.



```
hso: Login; 04.10.01, 10:00:50
hso: Signature; 04.10.01, 10:00:53
hso: Wrong Password; 04.10.01, 10:01:02
hso: Login; 07.10.01, 10:01:55
hso: Signature; 07.10.01, 10:02:09
hso: Password is expired; 10.10.01, 10:03:19
hso: Password is expired; 10.10.01, 10:03:31
hso: Change Password; 10.10.01, 10:03:39
```

Figure 27: Signature Setup - Audit Trail

A) Use these buttons to go to the previous or next user records and global records.

B) This selection field shows the audit trail

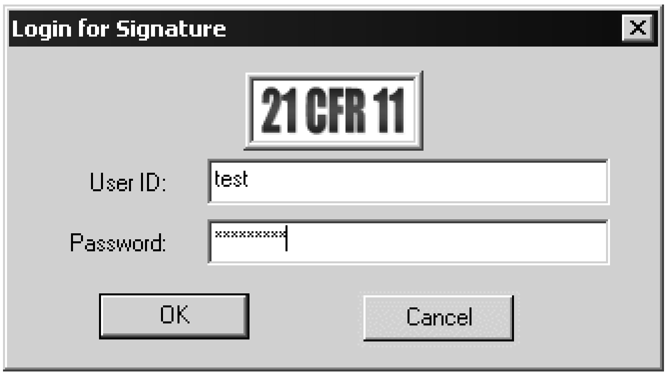
C) Use the *Clear Audit Trail* button to delete the currently shown and stored audit trail. Note that the audit trail will then be lost. If you need to keep it, write it to a text file. If the audit trail has not been stored, the *Clear Audit Trail* button will be disabled.

D) If you click on the *Save current* button, the audit trail of the current signer will be written into a text file for archiving.

E) Use the *Save all* button to write the audit trails of all signers into a text file for archiving.

4.4 Signing a File

To sign a file select the *Add Signatures* command from the *Validation* menu. The *Login for Signature* dialog opens and you have to enter the user ID and password.



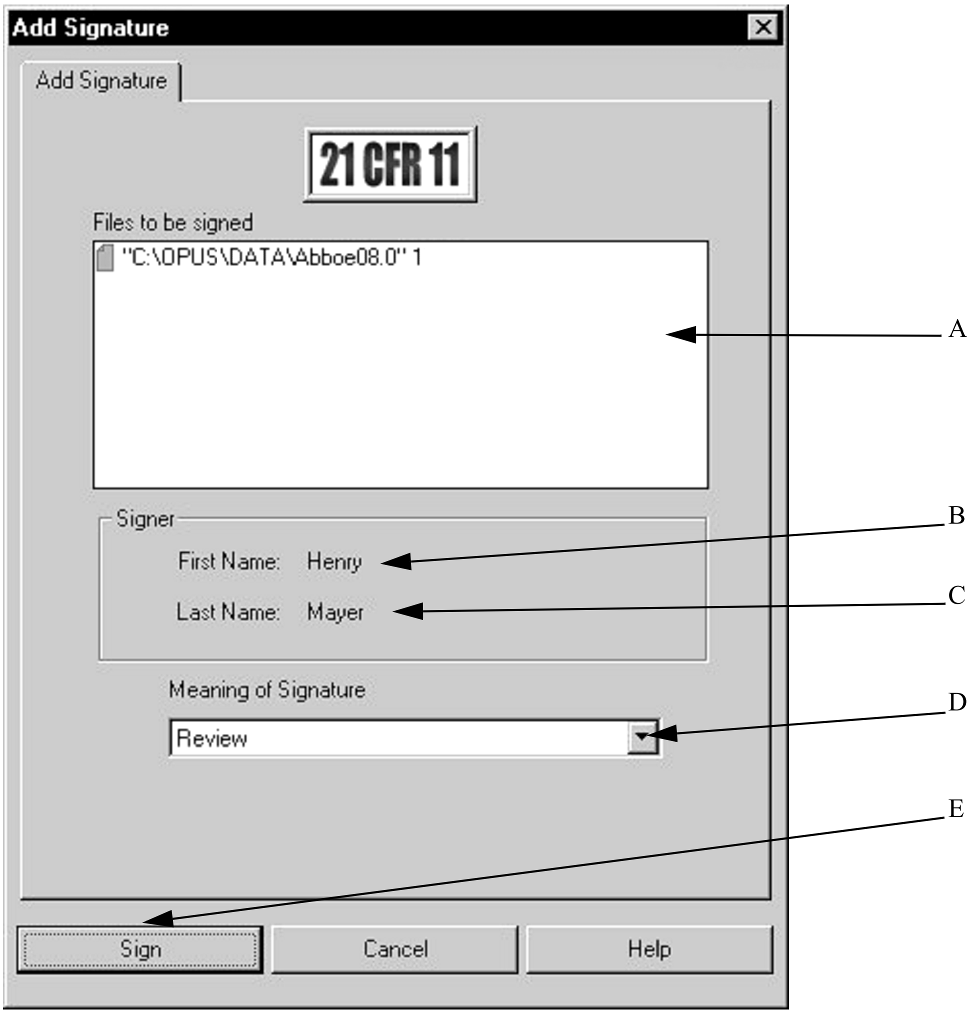
Login for Signature

User ID: test

Password: *********

Figure 28: Login for Signature

Click on the *OK* button and the *Add Signature* dialog opens:



Add Signature

Files to be signed: "C:\OPUS\DATA\Abboe08.0" 1

Signer

First Name: Henry

Last Name: Mayer

Meaning of Signature: Review

Figure 29: Add Signature

A) Drag & drop the file(s) to be signed into this selection fields. Several files can be selected and signed.
B) First name of the logged-in signer is displayed.
C) Last name of the logged-in signer is displayed.
D) Drop-down list to select the signature meaning.
E) Clicking on the *Sign* button will sign the selected file(s).

After signing a file a SIGNAT (signature) data block is added to the file.

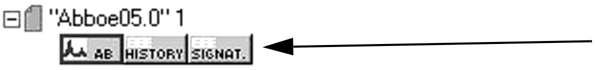
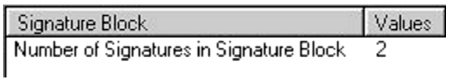


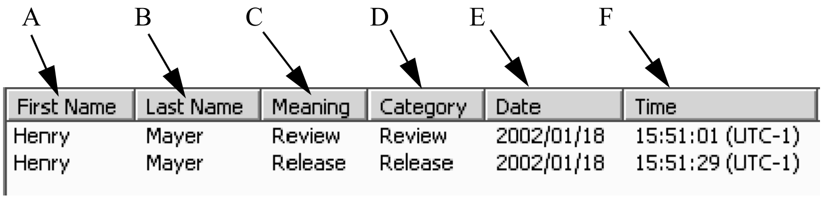
Figure 30: Signature Data Block

The SIGNAT data block is a report block and can be opened like any other report by clicking twice on it. The report header shows the number of signatures in the signature block.



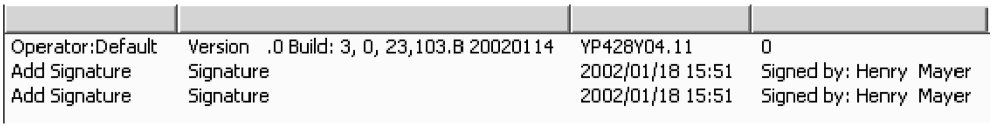
Signature Block	Values
Number of Signatures in Signature Block	2

The signature data in the report itself show the first and last name of the signer (A + B), the meaning (C), category of signature (D) and the date and time when the signature has been executed (E + F)



First Name	Last Name	Meaning	Category	Date	Time
Henry	Mayer	Review	Review	2002/01/18	15:51:01 (UTC-1)
Henry	Mayer	Release	Release	2002/01/18	15:51:29 (UTC-1)

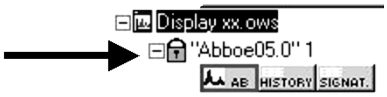
Signature reports can be printed like any other type of report. SIGNAT data blocks can neither be deleted nor copied or transferred to other data files. Additionally, the signature is also recorded in the HISTORY data block.



Operator:Default	Version .0 Build: 3, 0, 23,103.B 20020114	YP428Y04.11	0
Add Signature	Signature	2002/01/18 15:51	Signed by: Henry Mayer
Add Signature	Signature	2002/01/18 15:51	Signed by: Henry Mayer

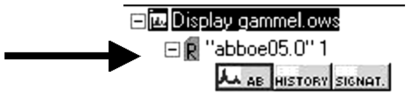
4.5 Signature Categories

Three different signature categories are available which have certain pre-defined effects within OPUS. If a file is signed by the meaning of *Release and Lock* category*,* this file cannot be modified in OPUS anymore. A locked file is marked by a blue lock symbol in the browser window.

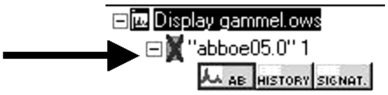


If a locked file is illegally modified (only possible when using an external program), this modification is immediately indicated by a red lock symbol if such a file is loaded in OPUS.

If a file is signed by the meaning of *Release* category, this file is marked by a green *R* symbol in the browser window. This symbol is only displayed if the signature is the last function applied to the data file. As soon as the file is modified by any other OPUS function, the file is no longer *released*.



If such a released file is illegally modified (only possible when using an external program), this modification is immediately indicated by a red cross.

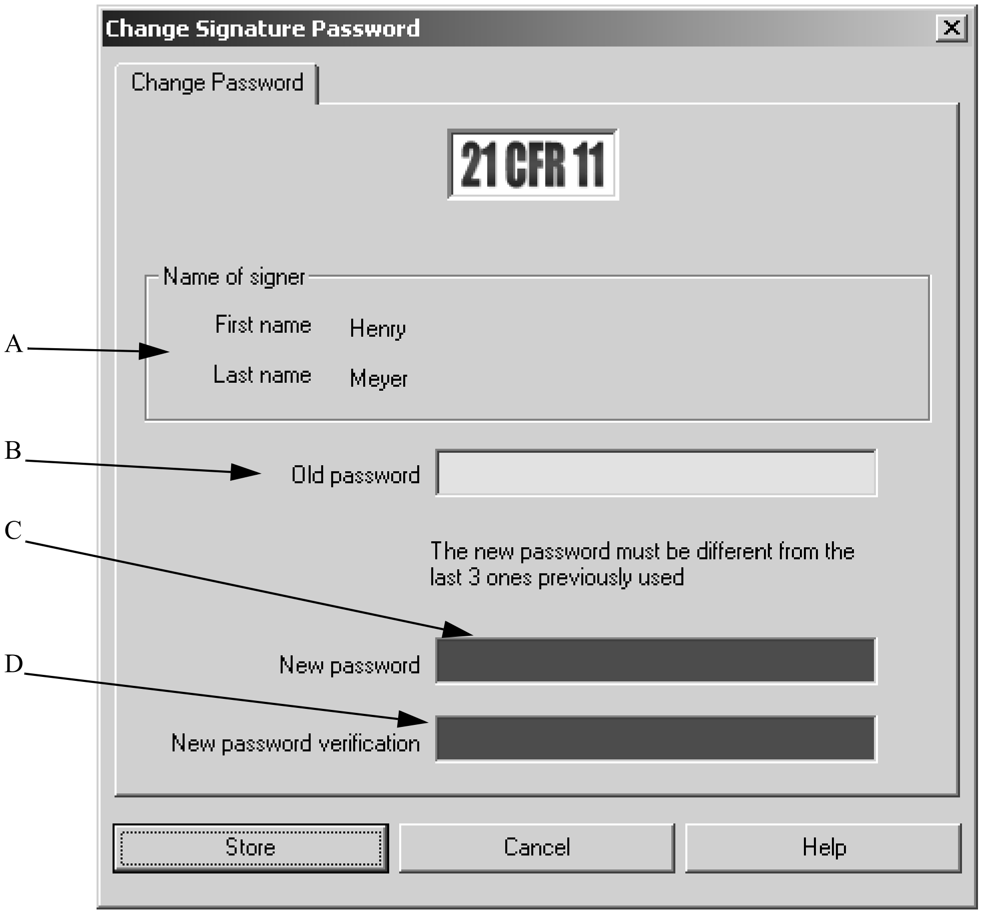


4.6 Changing Signature Password

Each user is allowed to change his signature password. There are several different reasons to change the signature password:

- A new signature record has been entered. In this case the administrator enters the initial password and the user has to change it.
- The *Password Expiration* option is deactivated and the password expires after the specified period of time. In this case the user can no longer login for the signature function.
- The user fears that someone else knows his password.

To change the signature password you have to select the *Change Signature Password* command in the *Setup* menu. The *Login for Signature* dialog opens. Enter the user ID and password. If the login has been successful, the *Change Signature Password* dialog opens.



Name of signer

First name Henry

Last name Meyer

Old password

The new password must be different from the last 3 ones previously used

New password

New password verification

Figure 31: Change Signature Password

A) The first and last name of the signer is displayed.
B) Entry field for the old password.
C) Entry field for the new password. Make sure that the new password is different from the last 3 ones previously used.
D) Entry field for the new password verification.

Clicking on the *Store* button stores the new password into the signature record.

4.7 Key Points of Electronic Signatures

4.7.4 Setup and Database

- Make sure that the signature database is **protected against deletion.**
- Always keep a **copy of the database** in a secure location.
- Only grant signature rights to persons who **must** sign files.
- **Lock Signature Records** as soon as the signers are out of the office for a long period of time.
- **Delete Signature Records** as soon as signers leave the company.
- Check the **Signature Audit Trail** on a regular basis.

4.7.5 Signing Files

- Sign all measurement experiment methods, evaluation methods and search libraries by a *Release* signature when they are to be used by operators.
- Sign all spectrum files which are to be used to create methods or store them in search libraries by a *Release* signature.
- Make sure that you no longer need to modify files if you decide to sign them by a *Release and Lock* signature.

5 Electronic Records

5.1 Reference to 21 CFR Part 11

The following paragraphs are discussed in this chapter.

11.10 (b)	Accurate and complete copies of records
11.10 (c)	Protection of records

5.2 Definitions

In general, an electronic record is any piece of data generated by an analytical instrument as soon as these data records *”hit a durable storage device”*, e.g. a hard disk. This is the FDA definition and therefore all the data recorded by modern analytical instruments are automatically handled as electronic records in the sense of the 21 CFR Part 11 regulation.

It can be distinguished between three major classes of electronic records:

- **Raw Data**
  Measured data generated by the instrument and stored, e.g. on the hard disk of a PC.
- **Result Data**
  Results derived from raw data by manipulation or evaluation functions
- **Meta Data**
  Processing parameters required to derive result data from raw data

If these definitions are applied to the field of Fourier Transform Infrared Spectrometers, we will have the following types of electronic records:

- **Raw Data**
  Infrared data which are recorded by the instrument and stored on the hard disk of the PC. What type of data you store depends on your internal regulations. In most cases only the resulting infrared spectrum is stored, but in some cases the interferograms and/or single-channel spectra might also be requested.
- **Result Data Type 1**
  The results of manipulation functions applied to the spectra, e.g. baseline correction, normalization. Manipulation functions modify the spectral data in some way.

- **Result Data Type 2**

  The results of evaluation functions applied to spectra, e.g. peak picking, quantitative analysis. Evaluation functions derive results from the spectra without modifying the spectra.
- **Meta Data Type 1**

  Processing parameters used for manipulation functions, e.g. baseline correction type.
- **Meta Data Type 2**

  Processing parameters used for evaluation functions, e.g. the calibration data for quantitative analysis.

5.3 OPUS Data Format

The 21 CFR Part 11 regulation requires electronic records to be accurate and complete. These requirements are guaranteed by the unique OPUS data format as well as by validated OPUS functions.

5.3.1 Description

All OPUS files which can be identified as electronic records in the sense of the *21 CFR Part 11* regulation are stored in a proprietary binary format. Data which logically belong together (e.g. spectrum, reports, audit trail, signatures etc.) are always stored in a single physical file. Thus, it is ensured that not any piece of data can be accidentally lost during copying or archiving.

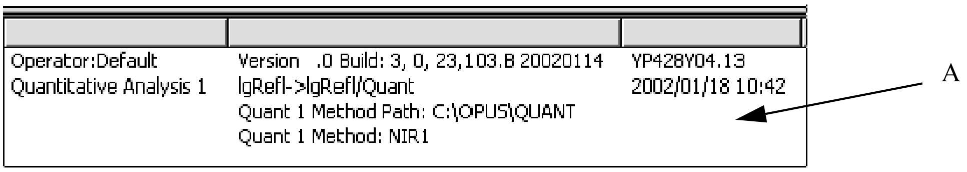
The data files are internally stored in several different data blocks which are preceded by a file header containing information about the type, size and physical location of a data block within the data file.

5.3.2 Spectrum Files

The original measured data (**Raw Data**), results of manipulation functions (**Result Data Type 1**) and evaluation functions (**Result Data Type 2**) as well as the audit trail, which shows all manipulation parameters (**Meta Data Type 1**) and signatures**,** are always stored in a **single** data file. Therefore, no additional content management system is required to manage and track the data.

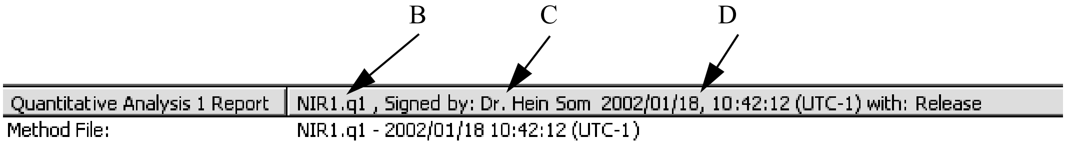
5.3.3 Evaluation Methods

The only type of records which are not part of a spectrum file are the evaluation methods required for QUANT, IDENT, SEARCH and integration (**Meta Data Type 2**). These methods are stored in separate files and a clear, unambiguous reference to these files is stored in the resulting report, as well as the audit trail for a quantitative analysis, see below.



Operator:Default Quantitative Analysis 1	Version .0 Build: 3, 0, 23,103.B 20020114 lgRefl->lgRefl/Quant Quant 1 Method Path: C:\OPUS\QUANT Quant 1 Method: NIR1	YP428Y04.13 2002/01/18 10:42

The audit trail of the spectrum shows path and filename of the used method file (A).



Quantitative Analysis 1 Report	NIR1.q1 , Signed by: Dr. Hein Som 2002/01/18, 10:42:12 (UTC-1) with: Release
Method File:	NIR1.q1 - 2002/01/18 10:42:12 (UTC-1)

The QUANT report shows the filename (B), the name of the user who signed the method (C) and date and time when the signature has been performed (D).

The unambiguousness of the method reference is guaranteed by the unique combination of B, C and D.

If a method has to be changed, you have two options:

- **Option 1:** store the changed method by using a new file name
- **Option 2:** store the changed method by using the same file name

Option 1 is the preferred option for **daily routine work.** The advantage is that you can repeat a previous analysis at any time, if required. Archive the old method as soon as you have stored a new modified method. To prevent an old method from being accidentally overwritten, sign it by the *Release And Lock* category (see chapter 4.5).

Disadvantage: Macros calling up a dedicated method name will not execute any more.

Option 2 should only be used during the **development and test phase** of a method. The audit trail which is stored in the method clearly shows all initial settings and changes made during development.

5.3.4 Copying and Archiving OPUS Data Files

To copy or archive an OPUS data file, i.e. spectrum files and meta data it is sufficient to copy the physical file onto a different storage medium. The internal structure, as described in chapter 5.3.1, ensures that the copies are *accurate and complete* as stated in **11.10 (b)** of the *21 CFR Part 11* regulation.

We do NOT recommend to use the OPUS export functions (JCAMP.DX, Galactic Grams, X-Y stages) for copying or archiving purposes. The binary OPUS format only ensures that copies are *complete and accurate*.

5.3.5 Viewing and Printing OPUS Data

An OPUS *Viewer* provided by Bruker allows to view all kinds of OPUS spectral data including all reports, audit trails and signature data without requiring access to a full OPUS license.

All the different data blocks included in an OPUS data file can be printed, if required. The OPUS *Viewer* allows to print all data blocks quickly and efficiently using the *Quick Print* command from the *Print* menu. Open the data block to be printed and select the *Quick Print* command. To get customized printouts you need to have a full OPUS version. For more details on printing refer to the OPUS Reference Manual.

Make sure that you print all the data blocks listed in the OPUS browser window if you require a *complete* copy.

Note: You need a full OPUS version with the appropriate extended software packages to be able to view and print special types of meta data, for example QUANT or IDENT methods.

5.4 Key Points of Electronic Records

- Create *accurate and complete* copies by simply copying the OPUS data files onto a different storage medium
- Do not use export formats to create *accurate and complete* copies.
- Use the OPUS *Viewer* to view and print OPUS data.
- When developing and testing methods store them by using the same file name.
- If you use measurement experiment methods or evaluation methods in daily work, store changed methods by using a new file name.

6 Audit Trails

6.1 Reference to 21 CFR Part 11

The following paragraphs are discussed in this chapter:

11.10 (e) Audit Trails

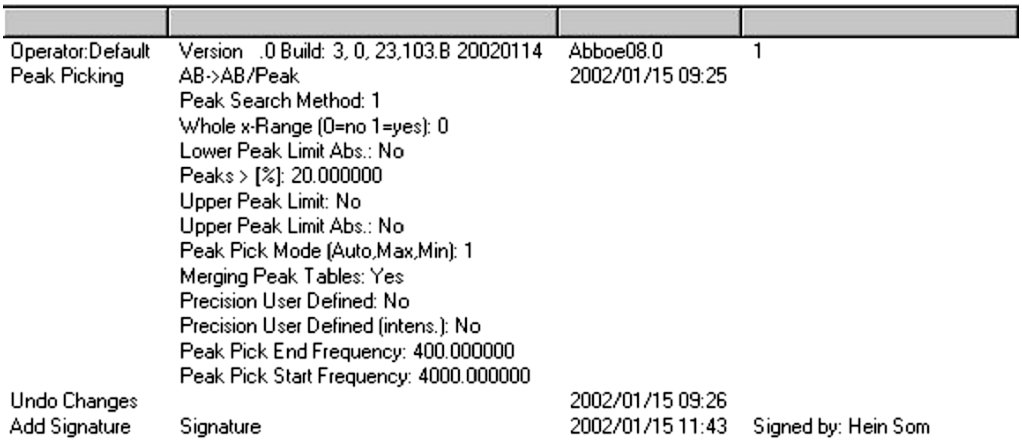
6.2 General

According to the *21 CFR Part 11* regulation audit trails should recorded automatically within OPUS. All functions applied to any kind of data are recorded in the audit trail.

The audit trail is not only recorded for spectra (Raw Data, Result Data Type 1 and 2 and Meta Data Type 1, see chapter 5.2), but also for all measurement experiments, evaluation methods and spectral libraries (Meta Data Type 2). The audit trail is stored in a separate data block (HISTORY) within each OPUS file and cannot be deleted, modified or copied into any other data file.

6.3 Spectrum Audit Trails

Spectrum audit trails include all functions applied to a certain spectrum. Even operations which are repeated several times, or whose results are not stored. If, for example, a peak picking has to be performed several times using different peak sensitivities until a satisfactory result can be stored, all previous attempts are recorded in the audit trail.



Operator:Default	Version .0 Build: 3, 0, 23,103.B 20020114	Abboe08.0	1
Peak Picking	AB->AB/Peak Peak Search Method: 1 Whole x-Range (0=no 1=yes): 0 Lower Peak Limit Abs.: No Peaks > [%]: 20.000000 Upper Peak Limit: No Upper Peak Limit Abs.: No Peak Pick Mode (Auto,Max,Min): 1 Merging Peak Tables: Yes Precision User Defined: No Precision User Defined (intens.): No Peak Pick End Frequency: 400.000000 Peak Pick Start Frequency: 4000.000000	2002/01/15 09:25	
Undo Changes		2002/01/15 09:26	
Add Signature	Signature	2002/01/15 11:43	Signed by: Hein Som

Figure 32: Spectrum Audit Trail

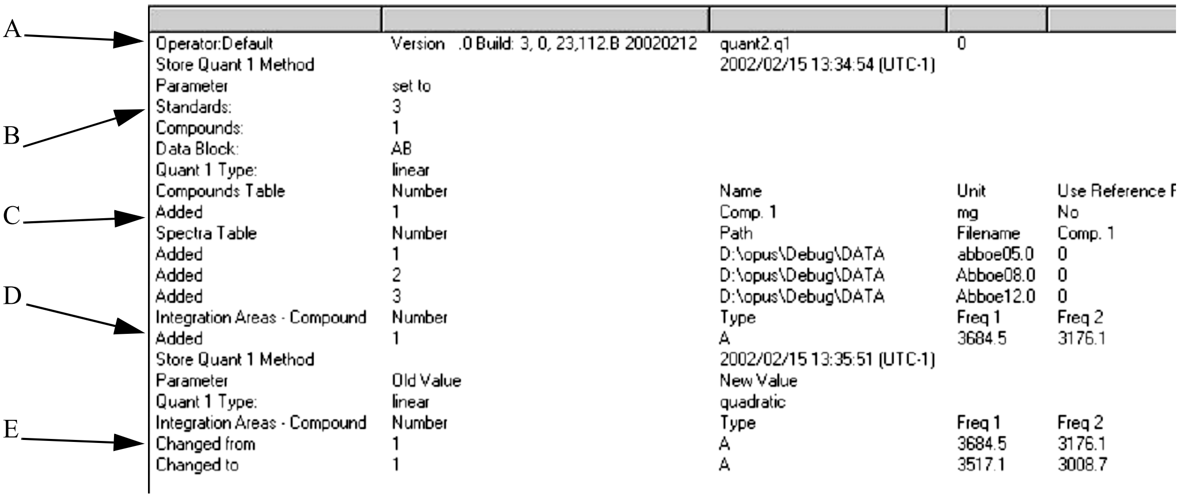
Each audit trail includes a header line indicating the operator name, OPUS version, original file name and a flag which shows whether the validation mode has been activated (1) or not (0). Any time you change one of these items, e.g. the operator, a new header line is appended to the audit trail.

The first column shows all OPUS commands applied to the spectrum with all relevant parameters listed in the second column. Date and time are recorded in the third column while the last column may include additional information about the function. The column with the complete OPUS command line allows all functions to be replayed and to repeat all processing steps if required.

The separate *Add Comment* function in the *File* menu allows to add comment lines to the audit trail.

6.4 Method Audit Trails

Method audit trails record the creation of a method and all subsequent modifications of the method itself, or method parameters.

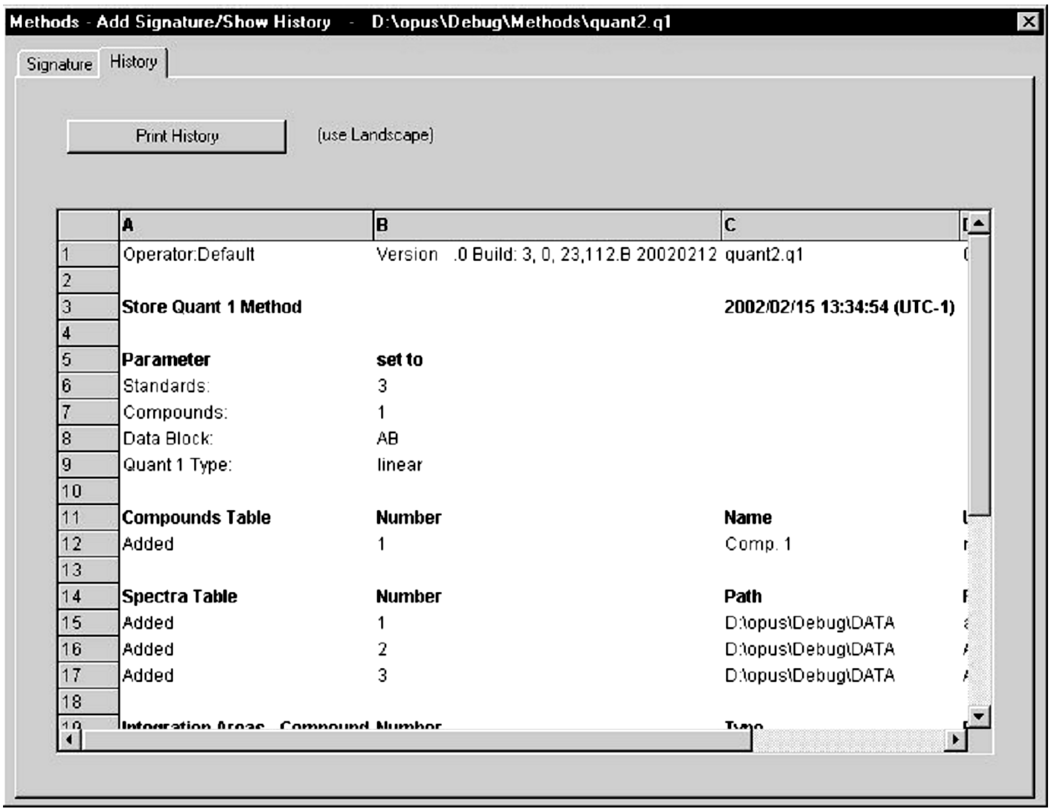


Operator:Default	Version .0 Build: 3, 0, 23,112.B 20020212	quant2.q1	0	
Store Quant 1 Method		2002/02/15 13:34:54 (UTC-1)		
Parameter	set to			
Standards:	3			
Compounds:	1			
Data Block:	AB			
Quant 1 Type:	linear			
Compounds Table	Number	Name	Unit	Use Reference F
Added	1	Comp. 1	mg	No
Spectra Table	Number	Path	Filename	Comp. 1
Added	1	D:\opus\Debug\DATA	abboe05.0	0
Added	2	D:\opus\Debug\DATA	Abboe08.0	0
Added	3	D:\opus\Debug\DATA	Abboe12.0	0
Integration Areas - Compound	Number	Type	Freq 1	Freq 2
Added	1	A	3684.5	3176.1
Store Quant 1 Method		2002/02/15 13:35:51 (UTC-1)		
Parameter	Old Value	New Value		
Quant 1 Type:	linear	quadratic		
Integration Areas - Compound	Number	Type	Freq 1	Freq 2
Changed from	1	A	3684.5	3176.1
Changed to	1	A	3517.1	3008.7

Figure 33: Method Audit Trail

If loaded like a spectrum, the method audit trail can be displayed like a spectrum audit trail. The header line (A) is the same as for spectra but the remaining part of the history is distinguished in different chapters (B) to (D). The changes of parameters are listed in a similar format (E).

If you open a method by the *Methods - Add Signature/Show History* command in the *Validate* menu, the history gives a structured view of the different chapters and can be printed in this format as well.



Methods - Add Signature/Show History - D:\opus\Debug\Methods\quant2.q1
Signature
History
Print History
(use Landscape)

	A	B	C
1	Operator:Default	Version .0 Build: 3, 0, 23,112.B 20020212	quant2.q1
2			
3	**Store Quant 1 Method**		**2002/02/15 13:34:54 (UTC-1)**
4			
5	**Parameter**	**set to**	
6	Standards:	3	
7	Compounds:	1	
8	Data Block:	AB	
9	Quant 1 Type:	linear	
10			
11	**Compounds Table**	**Number**	**Name**
12	Added	1	Comp. 1
13			
14	**Spectra Table**	**Number**	**Path**
15	Added	1	D:\opus\Debug\DATA
16	Added	2	D:\opus\Debug\DATA
17	Added	3	D:\opus\Debug\DATA
18			
19	**Integration Areas Compound**	**Number**	**Type**

Figure 34: Methods - Show History

6.5 Key Points of Audit Trails

- Audit Trails are automatically generated.
- Use the *Add Comment* command from the *File* menu to add additional explanations to the audit trail.

7 OPUS Data Retention

7.1 Reference to 21 CFR Part 11

The following paragraphs are discussed in this chapter:

11.10 (b)	Review of Electronic Records
11.50 (b)	Readability of Electronic Records

7.2 General

Several standard software tools are available to make backup copies of data. Thus, OPUS does not provide a separate tool for this purpose, but supports the generation of complete backups by its data format.

7.3 Spectrum Retention

Whenever a spectrum data file is backed up all relevant information, results, signature and audit trails are also automatically stored as they are an integral part of the spectrum file.

The organization of the directories to store newly measured spectra depends on the amount of data produced and can be operator, week or day-specific.

We always recommend performing a daily back-up, regardless of the number of spectra measured.

7.4 Method Retention

Measurement experiments, evaluation methods, e.g. QUANT and IDENT methods as well as search libraries, are the only type of data which are not stored together with spectral data. Therefore, these methods have to be backed up separately on a regular basis.

For QUANT and IDENT methods you always require reference spectra which have to be backed up as well.

In general, a backup of both methods and newly added reference spectra is required whenever a method is created or changed. Although all method changes are documented in the audit trail we recommend storing changed methods using different names (if possible) in order to facilitate tracing of evaluation results.

7.5 Retention in a Human Readable Form

The FDA requires that data is stored in a *"Human Readable Form"*. Currently, OPUS data files are only visible in OPUS. However, there are some standard formats, e.g. JCAMP-DX or Galactic *Grams* data format, which are supported by several other spectroscopy software packages.

It is possible to store OPUS files in these formats which, however, are **not 21 CFR Part 11 compliant** and just show the spectrum and a few other parameters. Evaluation results, signatures and audit trails are not stored with these formats. For example, the standardized JCAMP-DX format, which is a pure text format, can in no way be verified and protected against falsification.

Therefore, Bruker provides a separate OPUS file viewer which can be used to display OPUS data files including all its data blocks.

7.6 Key Points of Data Retention

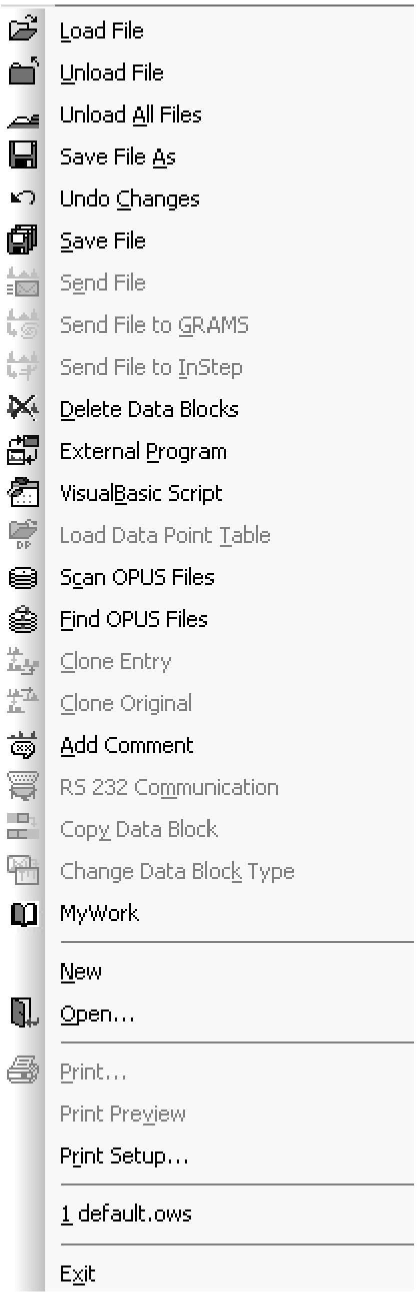
- Use **automated tools** to create backups of all your data.
- Make **regular backups** of **all** measured and processed spectra.
- Make **backups** of all measurement experiments, evaluation methods, reference spectra required for methods and search libraries when **creating** and **modifying** methods.
- Store data in **OPUS format** only to ensure a secure and complete data preservation.
- Note that **JCAMP** and **GRAMS** formats are not *21 CFR Part 11* compliant. Therefore, **do not use** these formats to back up data.

Appendix A

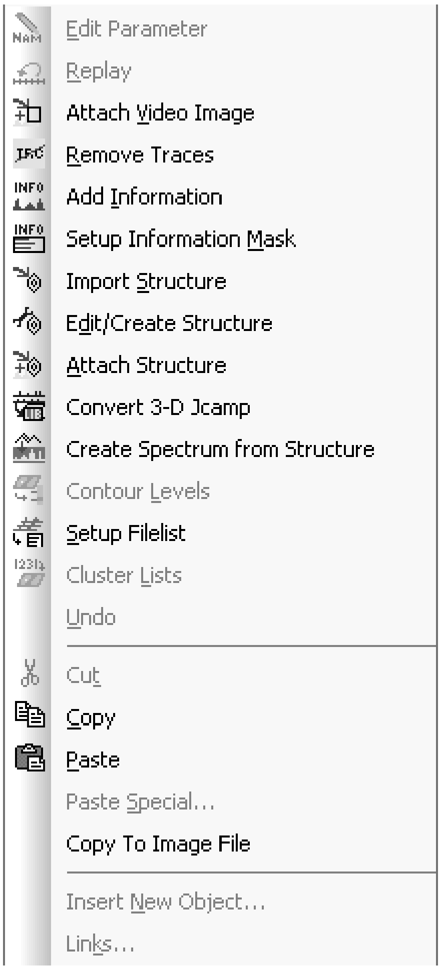
Validation Mode Functions

OPUS menus in validation mode are shown in the following. The grayed functions are either not conform to the *21 CFR Part 11* regulation or have not yet been validated. These grayed functions cannot be used, neither directly nor by means of macros or VB scripts.

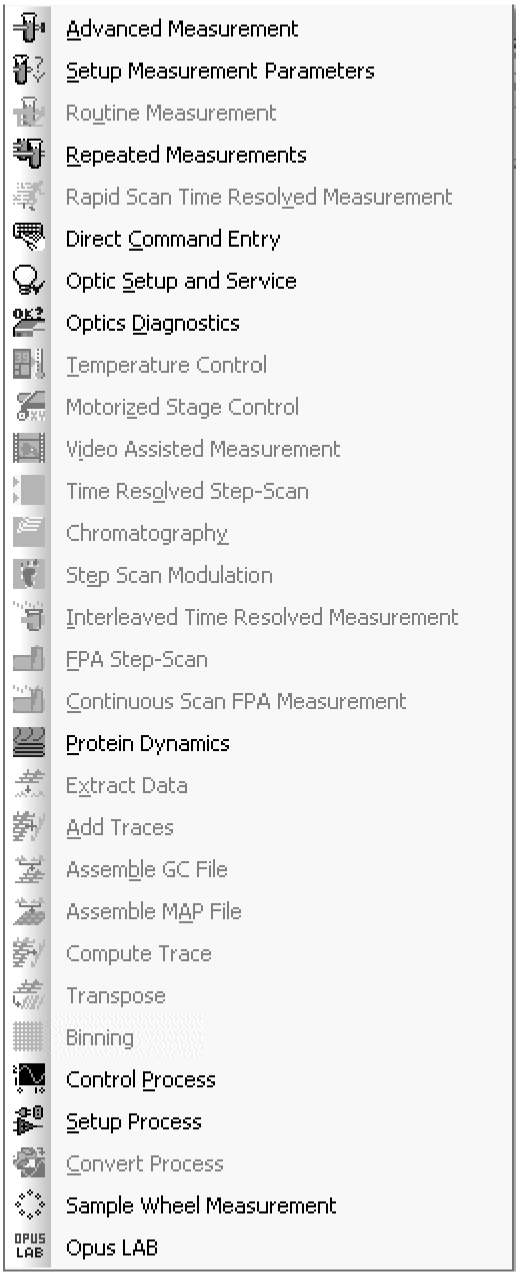
File Menu



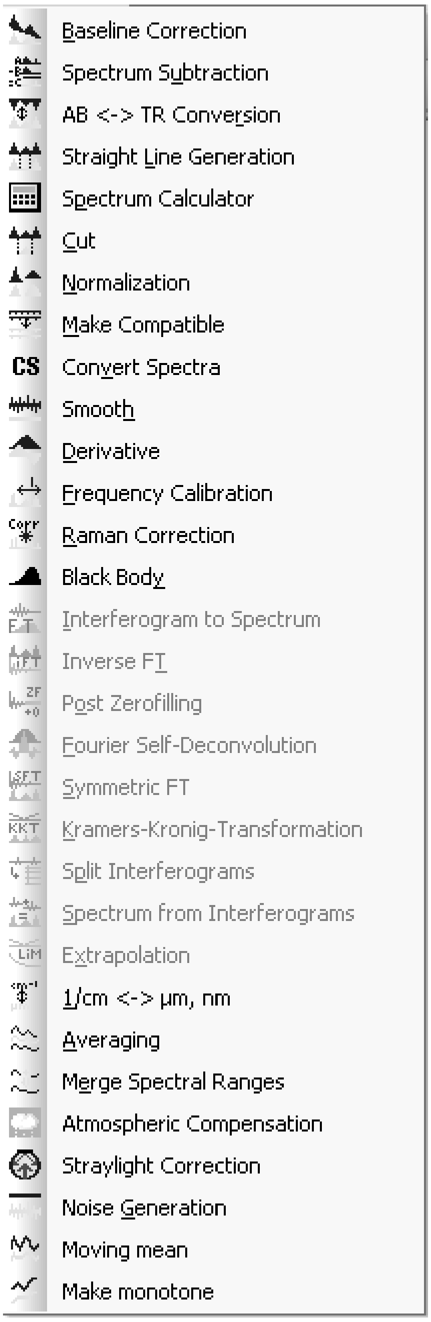
Edit Menu



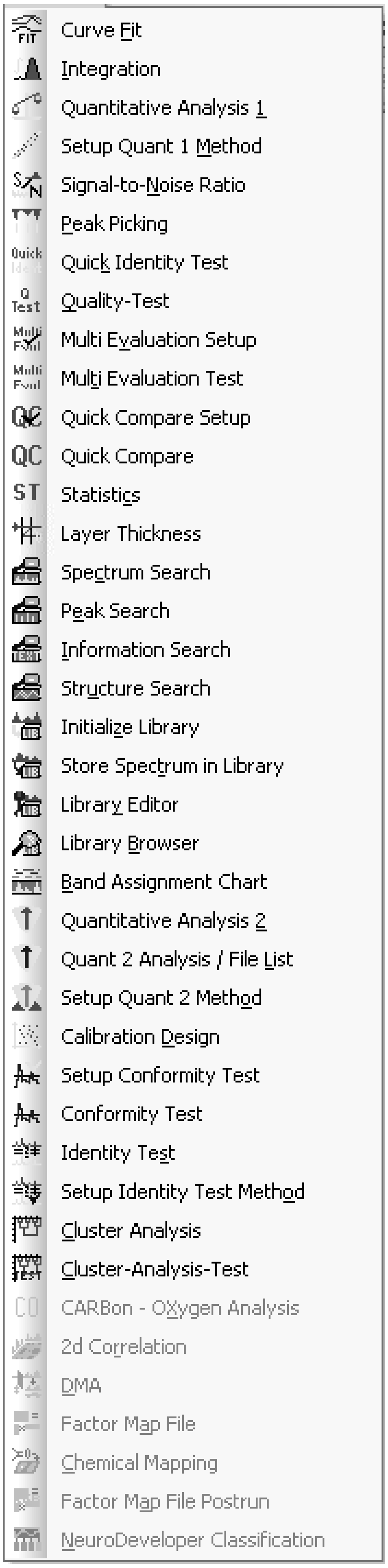
Measure Menu



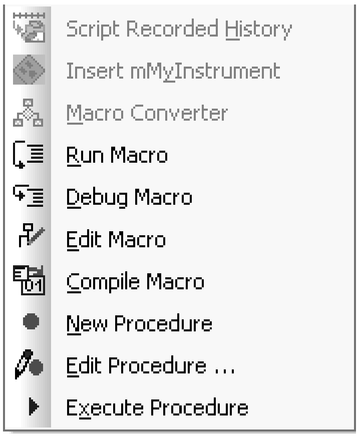
Manipulate Menu



Evaluate Menu



Macro Menu



Appendix B

Directories and File Extensions

The following tables give an overview about files used within OPUS. The first table shows the OPUS directories which are generated during installation, and the most important file extensions of files which are installed in these directories. Files generated during OPUS operation are shown in the other tables.

Definitions:

- **Directory**: the paths created during installation. All paths are subdirectories of the OPUS installation path.
- **Meaning**: explains the meaning and use of the directory.
- **Files**: lists the file extensions (***n*** represents a number) and file names (if only one file of this type exists).
- **Read Only**: Indicates whether a file can be set to read-only (Yes), must be write-allowed (No) or needs to be write-allowed only if the file is manually modified (Mod). Refer to footnotes if available.
- **Purpose**: shows the purpose of the specific file or file type.

Table 1: List of OPUS Directories and File Extensions

Directory	**Meaning**	**Comments**	**Files**	**Read Only**	**Purpose of the files**
OPUS (root)	Files needed to run OPUS.	This is the root directory for OPUS. No files may be removed from this directory	PCI*.01***n***	**Yes**	Optic firmware
			*.BAT	**Yes**	Batch files
			OPUS.BG	No	Last background spectrum
			*.BIN	**Yes**	Binary system files
			BRUKER.DBD	No	System file for SEARCH
			*.DLL	**Yes**	Dynamic Link Libraries for OPUS
			*.EXE	**Yes**	Executable programs
			*.FCS	**Yes**	Firmware system files
			OPUS.FNC	**Yes**	List of DLLs to be loaded on OPUS start
			*.INI	No	Some settings for OPUS

Table 1: List of OPUS Directories and File Extensions

			USERMAC.LST	Mod	List of user defined macros/scripts
			*.NTA	No	Settings for current instrument
			*.NTI	**Yes**	Instrument settings for different spectrometer types
			*.OBS	Mod	VB – Scripts
			*.OWS	No	OPUS workspaces
			ORIGINAL.P	**Yes**	Backup of OPUS parameters
			*.PAR	No	OPUS parameter files
			*.PLE	Mod	Plot layouts for Quick Print
			BRUKERIR.REG	**Yes**	Registry file for optics driver
			*.T8n	**Yes**	Software for Acquisition Processor
AAR-Dir + subdirectories	All files needed for the "Automatic Accessory Recognition" (AAR)		*.DAT	No	AAR settings
			*.BMP	No	Bitmap files
			.	**Yes**	All other files
			*.OBS	**Yes**	
COMPH2OCO2	All files for H_2O and CO_2 compensation.			No	
DATA	Example spectra	This directory is intended for storing manipulated spectra	*.***nnn***	No	OPUS Spectrum files
DATA\LIBRARY	Example libraries OPUS and Sadtler format		*. D01 ...... *.D14 *.K01, *.K02,*.K03 *.S01, *.S02 *.TXD	Mod[a]	All extensions for a library in OPUS format
			*.CSS, *.CWS, *.DAT, *.IDX, *.INF, *.IPK, *.ISM, *.NAM, *.SCR	**Yes**	All extensions for a library in Sadtler format
DATA\SEARCH	Example spectra for SEARCH		*.0	No	

Table 1: List of OPUS Directories and File Extensions

DBFILTERS	(Dynamic Link Libraries (DLLs) needed for accessing spectrum libraries in Sadtler format	Do not remove these files even if you do not use spectrum libraries at all	*.DLL	**Yes**	Dynamic Link Libraries (DLLs)
			*.BIN	**Yes**	Binary system file
DOCUMENTATION + subdirectories ENGLISH GERMAN FRENCH	OPUS Documentation in PDF format.	Depending on the installed language the documentation is in the subdirectories ENGLISH, GERMAN or FRENCH. The documentation can thus be installed in more than one language	*.PDF	**Yes**	Documents for the Acrobat reader
H18	All files needed for the H18 method (determination of Oil in water)			No	
HELP + subdirectories ENGLISH GERMAN FRENCH	OPUS online help files	The online help is always installed for all languages (in the subdirectories ENGLISH, GERMAN and FRENCH). The language is determined by the language in which OPUS is started.	*.CHM *.RED	**Yes**	Windows help files
MACRO	Example macros and VB scripts	This directory is intended for storing your own macros as well.	*.MTX	Mod	OPUS macros (text format)
			*.MTB		OPUS macros (binary format)
			*.OBS		VB - scripts
MCIT + subdirectories	All instrument tests which have been specified at installation	For each specific instrument configuration a subdirectory with a separate instrument test exists	*.MTB	No	IT macros (binary)
			*.BMP	**Yes**	Bitmap for OPUS toolbar
			*.INT	**Yes**	Integration method
			*.PLE	**Yes**	Plot script
			*.XPM	**Yes**	Measurement experiment
			*.TXT	No	Settings
METHODS	Method files for information, spectrum library creation and JCAMP export/import	This directory is intended for storing your own methods as well.	*.TXD	Mod	Info text definition file
			*.MTD	Mod	Library method
			*.PCT	Mod	JCAMP conversion table

Table 1: List of OPUS Directories and File Extensions

PROCESS	Empty	This directory is used for the OPUS/PROCESS package. Please refer to the PROCESS manual for details			
QCLIBRARY + subdirectories BACKUP TESTLIB	Empty library for the QC-macros. A copy is stored in the BACKUP directory. An example library is in the TESTLIB directory	For more details refer to the QC – macro documentation	See OPUS libraries	Mod	
			*.LST	Mod	Sample name list
			*.THR	Mod	Threshold list
QCMACROS	QC - macros and documentation	For more details refer to the QC – macro documentation in this directory	*.MTX	No	OPUS macros (text format)
			*.BMP	**Yes**	Bitmaps for OPUS toolbars
			*.PLE	**Yes**	Plot script
QUANT	Empty	This directory is used to store all methods related to QUANT-1 (part of OPUS/IR) and OPUS/QUANT. For more details refer to the QUANT documentation	*.Q1	Mod	QUANT-1 method
			*.Q2	Mod	QUANT-2 method
			*.Q2V	Mod	Result of validation (binary)
ROUTINE	Files for the ROUTINE interface and for setting up the ROUTINE interface		*.DLL	**Yes**	Dynamic Link Libraries
			*.EXE	**Yes**	Executable program
			*.OBS	**Yes**	VB – Scripts
			*.OCX	**Yes**	ActiveX Control
			*.PAR	No	Parameter files
ROUTINE\MACRO	Macros for use with ROUTINE	All macros called from within ROUTINE must be stored here.	*.MTX	Mod	OPUS macros (text format)
ROUTINE\MEAS	Default path for measured files		***.nnn***	No	OPUS spectra
ROUTINE\METHODS	Method files for evaluation	All methods used for evaluation within ROUTINE must be stored here.	Depends on the evaluation	Mod	
ROUTINE\XPM	Measurement experiments for ROUTINE	All experiments used for evaluation within ROUTINE must be stored here	*.XPM	Mod	Measurement experiments

Table 1: List of OPUS Directories and File Extensions

SCRIPTS + subdirectories A4 LETTER	Predefined plot scripts. Copies for DIN A4 and US Letter format are stored in the subdirectories A4 and LETTER	Depending on the installation language the main SCRIPT directory contains plot scripts either in A4 or in Letter format	*.PLE	Mod	Plot layouts
SEARCH	Default methods for information- and peak-search	This directory is used for all temporary files generated by SEARCH and is intended for user generated methods as well	*.INL	Mod[b]	Query for info search
			*.PKL	Mod[b]	Query for peak search
			REPORTnnn.0	No	Search reports from peak- and info search
USERDATABASE	USERDATA-BASE.DAT This file is not overwritten by repeated OPUS installations	This is the database file for OPUS User Management and Signature records. This file must not be deleted.	USERDATA-BASE.DAT	No	
VBSAMPLE	Examples for VB scripts and external programs		*.OBS *.FRM, *.VBP, *.VBW	Mod Mod	Visual Basic Script Files for Visual Basic programs
			*.C	Mod	Source file for the C language
WORK	Empty	This directory is used for all temporary spectrum files generated by OPUS. A different path can be specified in the OPUS User Settings	***nnnnnnnn***.0	No	Temporary work files (automatically deleted)
			*.***n***		Result files from different OPUS functions
XPM	Empty	This directory is used for storing measurement experiments of all kinds.	*.XPM	Mod	Measurement experiments

[a] Commercial libraries can be set to read-only without limitation, user-generated libraries have to be write-allowed whenever an entry is added or modified.

[b] The DEFAULT.INL and DEFAULT.PKL files have to be write-allowed because these files are overwritten each time an information or peak search is performed. Other user-created queries can be set to read only, unless they need to be modified.

Common File Extensions of Files Created by OPUS

The following tables show all files which can be generated by OPUS. The different tables are sorted by functionality.

Definitions:

- **File Extension**: extensions of files generated by OPUS.
- **Purpose of Files**: describes the purpose and use of the files within OPUS.
- **OPUS Functions/Packages**: OPUS functions and/or OPUS packages which generate the files.

Table 2: OPUS System files

File Extension	Purpose of the files	OPUS Functions/Packages
*.OWS	OPUS Workspace	OPUS User interface and access rights
*.OBS	Visual Basic Scripts	Used for automation and specific user interfaces
*.MTX, *.MTB	OPUS Macros (*.MTX Text format, *.MTB binary format)	Used for automation and specific user interfaces
*.PLE	Plot layouts	Print/Plot

Table 3: OPUS Spectra Files

File Extension	Purpose of the files	OPUS Functions/Packages
*.nnn (numeric extension, one to 3 digits)	OPUS spectra files	All
*.DX, *.DXn	Data files in JCAMP-DX format	Save As, OPUS loads these files directly
*.DAT	Exported data files in "Pirouette" file format	Send File to InStep
*.SPC	Data files in GRAMS format	Save As, Send to Grams, OPUS loads these files directly
*.MOL	Chemical structures in MOLFILE format	Structure handling

Table 4: OPUS Method Files

File Extension	Purpose of the files	OPUS Functions/Packages
Edit Menu		
*.TXD	Information text definition file	Information input, Create libraries, Information search
*.MOL	Chemical Structure in MOLFILE format	Import Structure
Measure Menu		
*.XPM	Measurement experiments	Measurement
*.TRS	Method for Time Resolved Measurement	Rapid Scan Time Resolved Measurement

Table 4: OPUS Method Files

*.XY	X-Y Mapping positions	Motorized Stage Control
Evaluate Menu		
*.INT	Integration method	Integration
*.CON	Conformity Test Method	Conformity Test
*.QT	Quality Test Method	Quality Test
*.SNT	NeuroDeveloper Netfiles	NeuroDeveloper Classification
Evaluate Menu – QUANT 1 and QUANT 2		
*.Q1	Quant-1 Method	Quantitative Analysis 1, Setup Quant-1 Method
*.Q2	Quant-2 Method	Quantitative Analysis 2, Setup Quant-2 Method
*.Q2V	Quant Validation Result	Setup Quant-2 Method
Evaluate Menu – SEARCH		
*.D01 - *.D14, *.K01 - *.K03, *.S01, *.S02, *.TXD	Spectrum Libraries (OPUS Format)	All Search functions, Library creation, Library Editor, Library Browser
*.CSS, *.CWS, *.DAT, *.IDX, *.INF, *.IPK, *.ISM, *.NAM, *.SCR	Spectrum Libraries (Sadtler Format)	All Search functions, Library Browser
*.LLS	Library List	All Search functions
*.RNG	Frequency Range List	Spectrum Search
*.PKL	Peak Search Query	Peak Search
*.INL	Info Search Query	Information Search
*.MTD	Method file for user library	Initialize Library
*.TXD	Info Text Definition for user library	Initialize Library
Evaluate Menu – IDENT		
*.FAA	IDENT Method	Identity Test, Setup Identity Test Method
*.VAL	Validation Report	Setup Identity Test Method
Evaluate Menu – Cluster Analysis		
*.CLA	Cluster Analysis Method	Cluster Analysis, Cluster Analysis Test
Print Menu		
*.PLE	Plot Layout	Print Spectra, Quick Print, Plot Layout Editor

Index

Encoding 9