testo Saveris 21CFR Part 11 · Software

Instruction manual

1   Contents

2 Specifications

2.1. Intended purpose

The Saveris Professional software is used to save, read out and evaluate monitoring projects. The CFR version was especially developed to fulfil the requirements of the FDA regarding the electronic storage of data records in accordance with 21 CFR Part 11 when working in conjunction with the testo Saveris system.

The top priority is the regulation of user access:

For this, the Saveris CFR software uses the security mechanisms of the Windows® operating systems.

A system administrator with special rights must set up the Saveris CFR software during the installation phase with the help of the Windows security settings. These include, above all, the allocation of the users to the local groups. The allocation of the user IDs and passwords and of user rights and the regulation of document flow within the company must comply with the stipulated organizational guidelines.

The factory setting of the Saveris CFR software security settings corresponds to the requirements laid down in 21 CFR Part 11.

It lies largely within the responsibility of the operator to ensure that the appropriate access authorizations are made available to its users on an individual basis. Testo is not responsible for the consequences that occur at the operating system or application program level due to the improper handling of access authorizations.

The readings recorded together with date and time are integrated into a special 21 CFR Part 11 form; unmodified original data and data that have been processed, for example for better comprehension, can be distinguished and are appropriately marked.

21 CFR Part 11 places special requirements on the personal responsibility of the operator of the complete system, consisting of one or more PCs and the respective Saveris components.

In this sense, the solution provided by testo is to be considered a tool that contains all the necessary aids for implementing a validated measuring system within the FDA regulations and for securely managing the electronic data records that are generated by this.

Proper use in this context means, above all, that a set of standard operating procedures (SOPs) is drawn up for the use of the data acquisition system which ensures that the testo Saveris and Saveris CFR software tool is handled properly (also see **Standard operating procedures (SOPs)**, page 22).

These procedures are to be adapted to the particular organization and purpose of use and, together with the testo measuring system, form the validated system required by the FDA in 21 CFA Part 11 for the creation of electronic data records, authenticated where required by electronic signatures.

In particular, the operator is responsible for instruction and training of users; testo can only provide the necessary basic material in the form of the present instruction manual.

It is also the responsibility of the operator to ensure that the measurement data are available during the required storage period.

2.2. 21 CFR Part 11 and terminology used

What is 21 CFR Part 11?

Section 21 of the Code of Federal Regulations (CFR) is a part of the laws and regulations passed by the government of the United States of America in connection with the Food and Drug Administration (FDA).

In particular, Part 11 deals with "Electronic Records" and the use of "Electronic Signatures", i.e. with the handling of electronically stored data records and the security measures required for this.

What is affected by these regulations?

All data that are included in GxP inspections and are permanently stored on electronic data storage media. Thus all files and data records that may be included in an FDA inspection are affected.

Also affected are all electronic signatures that, as computer-generated authorizations, represent the legally binding equivalent of handwritten signatures.

Why are these regulations so important?

In the pharmaceutical industry, paper-based systems and handwritten signatures are increasingly being replaced by electronic systems and procedures. In order for these data records to be recognized by the FDA as binding in the same way as the former paper-based organizations and processes, the requirements of 21 CFR Part 11 must be fulfilled.

These regulations provide that data records in the pharmaceutical industry may also be handled electronically and regulate the use of electronic signatures in the place of traditional handwritten signatures.

All pharmaceutical companies who manage electronic signatures and electronic data records for their production processes together with the associated burden of proof and who wish to sell their

pharmaceutical products on the US market must meet the requirements of 21 CFR Part 11.

During an inspection by the FDA, the fulfilment of these requirements is actively verified and failure to fulfil them leads to corresponding blocking notes.

Who must fulfil these regulations?

All companies or manufacturers that market or intend to market their pharmaceutical products in the USA must fulfil these requirements. The regulations are also approved, present and compulsory as the quality standard in other countries.

What are the possibilities, especially in the area of measuring technology and data recording?

Compliance with 21 CFR Part 11

- Such compliance with the requirements means satisfying issues that are organizational above all but are also partly technical.
- Fulfilling organizational requirements means that pharmaceutical companies will set up organizational structures and define, describe and document all processes in order to demonstrate what protective measures are used by the respective company in order to comply with the regulations and how they are enforced.
- The core of such documentation consists of standard operating procedures (SOP), which describe and regulate all processes in detail. These describe in detail how the responsible persons are to carry out and use processes and systems in order to meet the requirements placed on them (also see **Standard operating procedures (SOPs)**, page 22).
- Fulfilling technical requirements: the fulfilment of requirements on the technical level is based on the use of products that are already suitable for this area according to the manufacturer.
- This area includes the Saveris CFR software according to 21 CFR Part 11 as described here together with the testo Saveris system approved for this.

Only when suitable technical systems are combined with SOPs adapted to the respective process is complete fulfilment of the FDA requirements for the manufacturers of pharmaceutical products guaranteed.

However, this also means that the use of technically suitable products, such as the testo Saveris system, does not in itself completely fulfil the FDA requirements; this can only be achieved by integrating measuring technology in an established organization that complies with 21 CFR Part 11, supplemented by company-specific SOPs.

What providing suitable systems means for testo: wherever possible, we seek to meet the requirements placed at the technical level in order to reduce the number of SOPs needed within the respective company to a minimum.

This is the task of our system and also the subject of this instruction manual which should help you to identify critical processes in data recording and archiving and makes recommendations on where you can secure your position with regard to the FDA by means of additional SOPs.

The complete text of the regulation is available on the Internet at:

http://www.fda.gov

The following is only a short summary:

Part 11 – electronic records and electronic signatures, deals with the criteria for regarding electronic data records and signatures as equivalent to handwritten signatures and paper documents. This covers data records that are created, altered, maintained, archived and transmitted.

Such data records can be securely handled in so-called closed systems, i.e. in an environment to which only a controlled group of persons has access. With the Saveris CFR software, user/access control is performed via the tried and tested Windows security system (allocation of user IDs, rights management, user and password management, user authentication). The authorization concept (user rights, release or block the software functions) is determined by the IT administrator for three user levels in the Saveris CFR software.

The system used must be validated within its environment in order to ensure precision, reliability and performance. Invalid or altered data records should be identified in good time, either automatically or via suitable validation techniques, and isolated.

Further measures described in paragraph 11.10 serve to protect established electronic data records against unauthorized access and modifications.

In addition to the actual readings/data records, so-called audit trails are also stored in the database that contain all peripheral information since the commissioning of the system.

Every action relevant for an electronic data record is recorded together with a unique user ID and the date/time.

Paragraph 11.10 draws special attention to the obligation to keep all persons concerned in the creation, processing and archiving of electronic data records up-to-date with regular training in order to ensure that these persons are sufficiently reliable with regard to the required systems and procedures. With regard to the implementation of the technical requirements in the testo Saveris system and the Saveris CFR software, reference will be repeatedly

made throughout this instruction manual to the text of 21 CFR Part 11 in order to show how various detail functions are implemented in the context of 21 CFR Part 11.

3 First steps

3.1. Scope of delivery

- CD with Saveris CFR software
- CD with operating instructions
- CD with supplementary documents for the validation process
- Ethernet cable for connection of the Saveris base to the PC
- USB cable for operation of the service interface in combination with the mini-DIN USB adapter (to be purchased separately) for commissioning Ethernet components, for example.

3.2. System requirements

Operating system

The software will run on the following operating systems:

- Windows® Vista SP2 64-bit/ 32-bit or later
- Windows® 7 SP1 64-bit/ 32-bit or later
- Windows® 8 64-bit/ 32-bit
- Windows® 8.1 64-bit/ 32-bit
- Windows® Server 2008 SP2 64-bit
- Windows® Server 2008 R2 64-bit
- Windows® Server 2012 64-bit
- Windows® Server 2012 R2 64-bit

Computer

The computer must meet the requirements of the corresponding operating system. The following requirements must additionally be fulfilled:

- 4.5 GB unused hard drive capacity with maximum size of the database
- USB 2.0 interface
- Microsoft® Internet Explorer 9.0 or later
- Microsoft® Windows® Installer 4.5 or later
- Microsoft® .NET Framework 4.0 SP1 or later
- MDAC 2.8 SP1 or later
- Microsoft® Outlook® (only for MAPI installation)

i	The computer's processor, hard disk and interfaces must be configured for continuous operation in order to ensure smooth automatic operation. If necessary, check your computer's energy-saving options.

i	If Windows® Installer 4.5, MDAC 2.8 SP1 and .NET Framework 4.0 SP1 are not present on the computer, they will be installed with the Saveris software. Restart after installation.

i	Saveris CFR should be installed in a Windows domain to enable shared working.

i	Date and time settings will be automatically accepted by the PC. The administrator must make sure that the system time is regularly compared with a reliable time source and adjusted if necessary, to ensure authenticity of the measurement data.

Database

- SQL-Server® 2012 R2 Express is delivered.
- The versions Microsoft SQL Server 2008, 2012, 2014 and Terminal Server are supported.

i	In client-server operation, we recommend a network with AD and DNS (Domain Name System) to enable online updating using MSMQ (Microsoft Message Queuing).

3.3. Information for the administrator

One of the main points in the 21 CFR Part 11 regulation deals with controlled system access. The background to this is the fact that so-called closed systems, i.e. clear, small system units with only a few precisely defined external interfaces and a defined group of authorized users, can be easily controlled with a small number of SOPs.

As the responsibility for allocating user accounts and user rights in practice lies in the hands of administrators who have extensive, cross-system rights, the following information is addressed to the administrator or the group of people authorized to integrate the Saveris CFR software into a validated process or a validated total system.

The testo installation program links the Saveris software program with the access control mechanisms of the Windows® operating systems.

The installation program requires administrator rights.

Whilst installing the program,

- local groups are created in order to connect the Saveris CFR software with the NT security system: In the system administration, 3 local groups are added to those which already exist:

  Testo-Comsoft-Admins

  Testo-Comsoft-Power Users

  Testo-Comsoft-Users

  The local groups are only valid on the PC on which they were created and are the key to the database concept.
- the Saveris software is registered as a source of event log entries (audit trail and event logs).

After the installation you must allocate individual users who are to work with the program to one of the above named groups.

The following procedure is valid specifically for the installation or operation of the Saveris software within a company network:

Server/domain

1. Create global user group(s) centrally in the active directory, e.g. "Saveris admin", "Saveris main user" and "Saveris user").
2. Assign group members.

PC

3. Install Saveris software on the PC (local).
4. Include global group(s) as a member in local testo Saveris group(s).

4   First steps

4.1.   Performing installation

Please observe the following notes before installation:

> **i**   Administrator rights are required for installation of the program.
>
> Parallel operation of Saveris CFR and Saveris SBE/ PROF on one PC is not possible.
> Please therefore do not install the Saveris CFR software on a PC on which Saveris SBE or PROF is already running. Use a different PC or a virtual environment for the installation of the Saveris CFR software.
>
> Should you perform a software update, please note the following:
>
> - It is only possible to perform an update from Saveris

Professional to Saveris CFR (not from Small Business Edition to CFR).

- When updating from Saveris Professional to Saveris CFR, the **Audit Trail** feature is not available for running projects. We therefore recommend ending all active projects and creating new projects after an update. This guarantees that all functions of the CFR software are available.

Installation of testo Saveris CFR software

✓ Older versions of Saveris software are uninstalled.

1. Insert CD-ROM in the drive
- After a short wait, the installation program will start automatically.
    > If not: Double click on **Setup.exe** in the corresponding directory on the CD-ROM.

i The preset path for saving is the user's **My Documents**. This is determined by the MFC class library, the Windows® version and the set-up data at operating system level (it is not recommended to attempt to make changes here).

i Only users who are administrators or members of the above named groups can start the Saveris CFR program; it is the responsibility of the system administrator to ensure that each password is only used once, i.e. two users may not work with the same password.

Remember, also, that changes to the security parameters affect the whole system and influence other applications.

After a successful installation

Once installed, the Saveris CFR software must be started by the administrator one time in order to perform any additionally needed settings.

Following this, the user accounts are assigned to the Saveris user groups (testo-Comsoft-Admin, testo-Comsoft-Power-User and testo-Comsoft-User).

Then you can change the default settings for the rights within the Saveris software application for the 3 user groups, see Individual rights for user groups, page 13.

5 Using the product

5.1. Access control at the system level

5.1.1. Users and user groups

After the installation, you must assign the individual users that are to work with the program to one of the local groups Testo-Comsoft-Admins, Testo-Comsoft-Power Users and Testo-Comsoft-Users.

The following procedure is valid specifically for the installation or operation of the Saveris software within a company network:

Server/domain

1. Create global user group(s) centrally in the active directory, e.g. "Saveris admin", "Saveris main user" and "Saveris user").

2. Assign group members.

PC

3. Install Saveris software on the PC (local).

4. Include global group(s) as a member in local testo Saveris group(s).

For a detailed description, see the user manual for your Windows operating system.

Assignment of the individual rights is performed in detail in the Saveris CFR software. The rights assigned there are valid for all members of the respective user group.

5.1.2. Individual parameters

Here you can define the boundaries of the local security and set the necessary control parameters.

For Windows XP select the **Administrative Tools** area under **Start / Settings / Control Panel** and click on the **Local Security Policy** icon.

Perform the settings as desired for the following functions:

- Password Policy
- Account Lockout Policy
- Account lockout threshold
- Monitoring Policy
- User rights
- Security Options

For a detailed description, see the user manual for your Windows operating system.

|	The control mechanisms of the Windows® security come into operation as defined with regard to the (system) session. A session performed in the audit trail is properly ended with the system lockout. After closing the Saveris application, log out as the user.

5.2. User regulation on Saveris CFR level

5.2.1. Individual rights for user groups

An administrator or member of the Testo-ComSoft-Admins local group can activate or deactivate individual functions or system possibilities for user groups previously set up on operating system level.
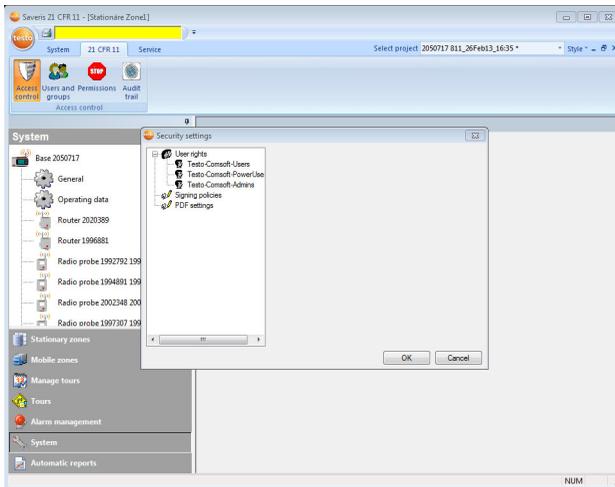
> In the main menu **System**, on the tab **21 CFR 11** click the **Security settings** button.

- The Security Settings window opens.

Under Local Groups, individual rights can be granted for the 3 user groups: Admins, Power User and User.

Under each group there appears a list of individual rights, each of which is marked with a tick when clicked on and thus made accessible for the selected user group.
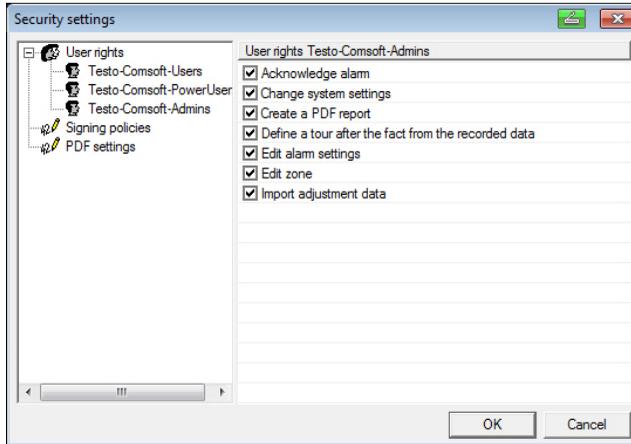
In detail, the following rights can be granted/withdrawn:

• Acknowledging an alarm
• Changing alarm settings
• Change name or content of a zone
• Changing settings in the system range
• Importing adjustment data
• Creating a PDF report
• Define tour retroactively from existing data record

5.3. General information for the Saveris CFR user

The descriptions and chapters of this instruction manual relate specifically to the requirements of 21 CFR Part 11.

The standard functions and general use of the software are still described in the instruction manual for the Saveris Professional (on CD).

If you cannot select individual functions that are described in the instruction manual for the Saveris Professional, it is possible that you do not have the corresponding rights. In this case, contact the administrator.

Note the following exceptions in the CFR operation:

• The base is connected to the PC via an Ethernet cable. Connection via USB is not possible.
• Alarms cannot be acknowledged via the base, but rather only with the corresponding rights directly in the CFR software.
• Alarms cannot be acknowledged via SMS or e-mail (SMTP).

5.4. CFR-specific functions

5.4.1. Electronic signature

For certain user actions, an electronic signature is required by the system. This signature is also shown in the audit trail with the specification of the reason for the signature.

Configure electronic signatures:

1. In the main menu **System**, on the tab **21 CFR 11** click on **Security settings**.

- The **Security Settings** window opens.

2. Under **Electronic Signatures** select the user actions for which an electronic signature should be required.
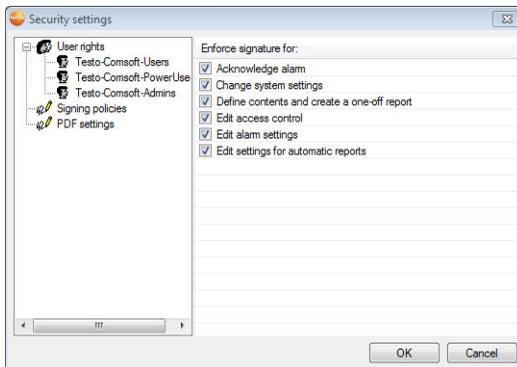
An electronic signature can be made necessary for the following user actions:

• Acknowledging alarms
• Changing alarm settings
• Edit settings for automatic reports
• Define report contents and create a one-off report
• Changing settings in the system range
• Edit security settings

The signature for a specific user action includes:

• The type of user definition (e.g. Alarm confirmed)
• Serial numbers of the corresponding Saveris components with the corresponding channel.
• Date and time
• Reason for the signature

> **i** The signature of a file consists of the user ID, date, time and reason for the signature.

5.4.2. Manual creation of PDF reports

Use the function **One-off report** to generate 21 CFR 11-compliant printouts of any period of time.

1. Select main menu **Stationary zones**.
2. Mark required time period on the calendar.
3. On the Start tab, under Create reports click on **One-off report**.
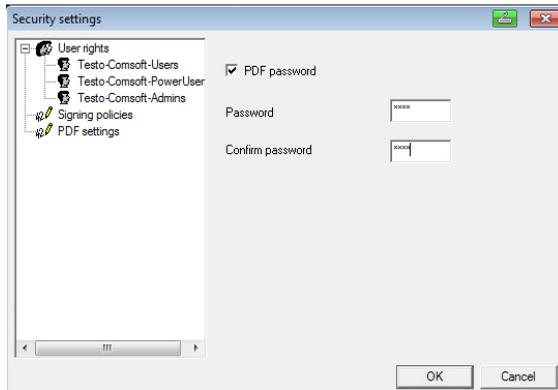
The PDF report contains:

• CFR-compliant cover sheet with hash code of the PDF report
• Graphic, measurement data table and alarms of the selected zone
• Audit trail of the time span specified in the calendar

The PDF report can be stored as a PDF with a master password.

> **i** The master password is only requested when the report is opened with Adobe Acrobat. When opening with Adobe Reader, no request is made.

✓ User is authorized for this.

1. In the main menu **System**, on the tab **CFR** click the **Security settings** button.
2. Select PDF settings.

5.4.3. Automatic creation of PDF reports

> **i** The automatic PDF report creation is not signature-capable.

A simple and secure option for archiving your data is the automatic creation of reports.

Every report contains a summary of the data from one zone. The contents of the PDF report can be configured individually for every zone (table, graphic, alarms).

The reports are created by the software and stored on a daily, weekly or monthly basis at a specified location on the computer or a server or sent directly to a recipient by e-mail.

The reports are saved as PDF files so that they can easily be read or sent per e-mail.

In the report settings, you can determine how the automatic reporting should take place.

> In the navigation area, click on **Automatic reports**.

- In the data window, the sub-menu **Settings for automatic reports** is displayed.

- The report settings are shown in the display range.
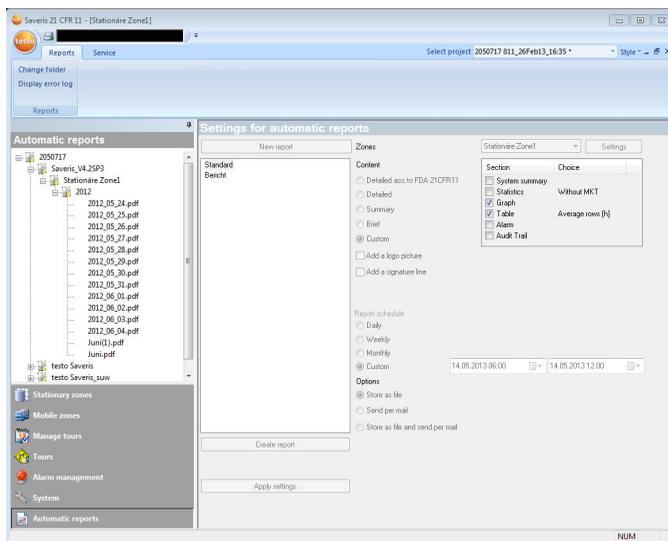
Designation	Explanation
[New report]	Adds a new reporting task to the list.
List of the reporting tasks	List of the created reporting tasks.
Zones	Selection list of the group for which the report should be created.

Designation	Explanation
Report schedule	Specify whether the report is to be generated **daily**, **weekly, monthly** or at a **custom** time.
	i **Daily**: The report is created daily at 1 a.m. **Weekly**: The report is created every Sunday at 1 a.m. **Monthly**: The report is created on the last day of the month at 1 a.m. **Custom**: A future time period can be set (start date/time, end date/time), upon which a report is to be created one time only. The report is created after the time period has elapsed.
Group box **Content**	When option is enabled, the corresponding data sheet is attached to the report • **Detailed** • **Compact** • **Brief** • **Custom** • **Insert logo** • **Insert signature line**
Options	Specify whether the report is to be sent via e-mail (**Send per mail)**, saved (**Store as file**) or both (**Store as file and send per mail**).
Recipient input field	Input field for the e-mail address of the employee to whom the report is to be sent.
[Address book]	Opens the dialogue for the selection of the recipient from the Outlook contact list.
Subject	Input field for the subject line.
Cover sheet address field	Input field for the address that should be shown on the pages of the report.

i   The storage location for the reports was determined during the installation of the Saveris CFR software. With the operating system Windows XP, this is generally

C:\Documents and Settings\All Users\Documents\Testo
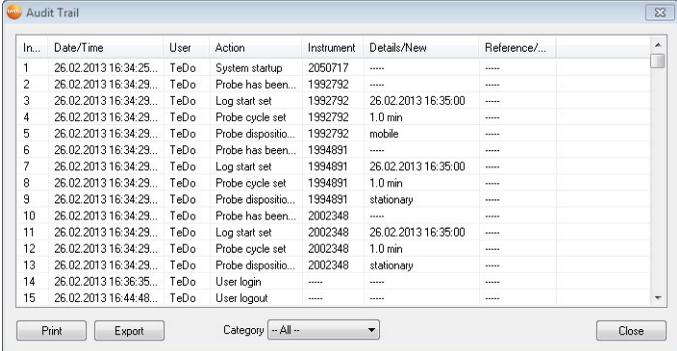Saveris Professional Server CFR \reports.

5.4.4. Audit trail

In addition to the restriction of permitted users, the possibility of
granting various rights and the securing of stored records by
access restrictions to the archive area, audit trails are an additional
major support for the demonstrably secure storage of PDF records.

The Saveris audit trail gathers specifically those entries that can be
directly assigned to an electronic record.

These include the creation or saving of electronic records and the
tracking of any changes made to these data during the archiving
period.

The Saveris audit trail data are coupled directly with the data file
and inseparably bound to it. This ensures that, even when
transferring data files from one system to another, the audit trail
data are not lost and always remain fully available.

The following events are recorded in the Saveris audit trail:
• Alarm confirmed
• Alarm confirm failed
• Alarm group has been created
• Alarm group has been updated
• Alarm group has been removed
• Alarm group has been removed automatically
• Alarm recipient changed
• Alarm recipient deleted
• Alarm recipient created
• Alarm route changed
• Alarm route created

- Alarm route deleted
- Alarm settings changed
- Automatic report definition created
- Automatic report definition updated
- Automatic report definition deleted
- Certificate has been imported
- Channel upper/lower warning limit set
- Channel upper/lower limit set
- Channel name set
- Cockpit unit settings changed
- Failed to pass an updated alarm configuration to the base
- Firmwareupdate
- Log start set
- Note has been added
- Note has been updated
- Note has been deleted
- pdf Password changed
- Probe cycle set
- Probe disposition is
- Probe has been added
- Probe has been removed
- Probe replacement
- Probe settings changed
- Report creation has been cancelled
- Report has been created
- Right granted
- Right removed
- Router configuration
- Signed
- Sign report
- Signature enforced
- Signature not enforced
- System startup
- System has been stopped
- Time synced
- Tour created manually
- Tour description created
- Tour description updated
- Tour description deleted
- Tour planning created

- Tour planning updated
- Tour planning deleted
- Tour deleted
- Tour updated
- Unit has been changed
- User login
- User logout
- Zone has been deleted
- Zone has been created
- Zone has been updated
- Zone renamed
- Zone settings have been updated

The following information is stored in the Saveris audit trail for the specified events:

- Index (consecutive audit trail number)
- Date/time (When was a change made in the system?)
- User (How made the change?)
- Action (What was done/changed?)
- Instrument (Specification of the serial number and the channel of the affected Saveris components)
- Details (What additional details are there for the change/event)
- Reference

The Saveris audit trail can be filtered by categories and can be exported and printed as an HTML file. A precondition for export and printing is a browser that supports HTML.

5.4.5. Automatic backup of the Saveris data

With the **Backup settings** function, the readings present in the database can automatically be backed up daily across projects. The backup files can be imported into a new project using the **Restore database** function.

i	For support with database backup, contact softwarehotline@testo.de.
i	The target directory for storage of the backup files must be activated for network services. Otherwise, backup of the data is **not** possible!
i	For safety reasons, the backup files should be stored/archived on a different PC than the Saveris database.

1. In the main menu **System**, on the tab **System** click the **Backup settings** button.
- The **Backup settings** window opens.
2. Activate the **Create daily backup** checkbox.
3. Select the target directory via **Determine folder**.
4. Click on **OK**.

5.4.6. Manual backup of the Saveris data

With the **Database backup** function, the readings located in the database can be stored across projects at any time. The backup files can be imported into a new project using the **Restore database** function.

ⓘ For support with database backup, contact softwarehotline@testo.de.

ⓘ The target directory for storage of the backup files must be activated for network services. Otherwise, backup of the data is **not** possible!

ⓘ For safety reasons, the backup files should be stored/archived on a different PC than the Saveris database.

1. In the main menu System, on the tab **System** click the **Database backup** button.
- The **Save as** window opens.
2. Select target directory.
3. Name the file.
4. Click on **Save**.

6 Tips and assistance

6.1. Standard operating procedures (SOPs)

This chapter contains recommendations for instructions on the operation of Saveris in CFR-relevant environments.

1 The customer must ensure that an emergency power supply exists for the PC on which the Saveris CFR software is operating.
2. The customer must ensure that the password protection is activated and the password is only known to authorized people.
3. The customer must define a sufficient backup cycle and ensure that suitable backup processes, storage media and storage

environments are available for data, software and the required hardware.

4. Before editing zones, the customer must back up the database. This is the only way that reports identical to previously generated reports in the same period can continue to be generated after zone is changed. Ideally, zones are only edited in the startup phase. The right to change zone should then be withdrawn.

5. The customer is responsible for creating suitable operating system accounts and user groups and assigning the user accounts to suitable users.

6. The customer is responsible for only using the Saveris wizard for the commissioning of the system or of a project or for the maintenance (e.g. probe calibration).

7. The customer is responsible for checking and storing the audit trail data.

8. The customer must ensure that the password protection is activated and the password for the PDF documentation is only known to authorized people.

9. The customer is responsible for creating user profiles and assigning these users to the existing user groups (Testo-ComSoft-Admin, Testo-Power User, Testo-User).

10. The customer is responsible for ensuring that only one Saveris software server is connected to the Saveris base.

11. The customer is responsible for protecting the USB interfaces of the Saveris components.

12. The customer must ensure the operating conditions of a closed system.

13. The customer is responsible for defining appropriate processes and checks in order to ensure the proper synchronization of the system clock.

14. The customer is responsible for activating the password function for PDF reports and defining a master password in the Saveris CFR software.

15. The customer is responsible for only forwarding the master password for PDF reports to authorized personnel.

16. The customer is responsible for clearly and non-repetitively assigning accounts and passwords to individual people.

17. The customer is responsible for issuing suitable/appropriate access authorizations.

18. The customer is responsible for checking the database capacity at regular intervals (once every three months) in the startup wizard, under the **Projects** tab and for taking any follow-up measures that may be required if the database is full.

19. It is the responsibility of the customer to configure the project protection functions correctly (for example, a suitable storage site for PDF reports must be defined and equipped with suitable security settings) and to ensure that staff members immediately log out when they leave the system.
20. The customer is responsible for ensuring that the password discipline is maintained.
21. The customer is responsible for defining suitable account processes and regulations and ensuring that they are complied with. The customer retains control over Saveris CFR duplicates.
22. The customer is responsible for performing the user account administration properly.
23. The customer is responsible for operating the system as a closed system and carefully checking the Windows access options and the system event log in good time.
24. The customer is responsible for defining suitable regulations and processes for dealing with improper use of the system.

Testo Industrial Services offers system qualification services in order to support the validation in the customer-specific application. Training for persons responsible for IT is also offered.

6.2. Version history

The document versions are successively numbered with a two-digit number (01, 02, ...). The version is unambiguously identified on the last page of these operating instructions. Within the specified printing standard (bottom right), the **version number** is the fourth character/number block (example: 0970 0466 de **01** V01.00-0).

The following documents critical changes of later versions.

Version	Chapter	Description of change
03	System requirements	Adapted
03	User regulations	New allowable rights
03	Electronic signature	New user action requiring a signature
03	Automatic PDF report generation	No password protection for automatically generated PDF reports
03	Automatic back-up of Saveris data, Manual back-up of Saveris data	Reference to support
03	Audit Trail	New Audit Trail products added

Version	Chapter	Description of change
03	Standard operating procedures (SOPs)	SOP 4 added
04	SOPs	SOP 18 added
04	User regulation at Saveris CFR level	Screenshots replaced
04	CFR-specific functions	Screenshots replaced
05	System requirements	Changed
05	User regulations	Function call at a different position
05	Electronic signature	Function call at a different position Changed user action requiring a signature
05	Manual PDF report generation	Function call at a different position
05	Automatic PDF report generation	Function call at a different position Restriction "No password protection for automatically generated PDF reports" dropped Changed report settings
05	Audit trail	New Audit Trail products added
05	Automatic backup	Function call at a different position
05	Manual backup	Function call at a different position
06a	System requirements	Adapted
06a	Perform installation	Formulation adapted server instead of PC.
06a	Automatic PDF report generation	Time reporting of 24 to 1 clock clock changed.