Be sure. testo

On the safe side:
Fulfilling the requirements of FDA 21 CFR Part 11 with testo Saveris 1

Table of contents

21 CFR Part 11:
Fulfil all requirements with confidence

Pharmaceuticals are manufactured with the highest quality and safety precautions. Regulatory authorities such as the Food & Drug Administration (FDA) in the USA stipulate how these requirements are to be implemented. Seamless and tamper-proof documentation of the entire value-added process plays a key role here.

The FDA has specific requirements for electronic documentation. In 1997, in order to ensure the trustworthiness of electronically stored and signed records, the FDA drew up a binding catalogue: The Electronic Records and Signature Rule 21 CFR Part 11[1]. This regulation sets out the technical framework within which electronic documents can be created, signed and archived with the required maximum level of forgery protection and secure access controls. Additional precautions are also required at process and administrative level, such as standard operating procedures (SOPs) and user training. Only the combination of suitable technical systems with SOPs adapted to the respective process guarantees complete fulfilment of FDA requirements for manufacturers of pharmaceutical products. This white paper primarily describes the technical requirements of the Electronic Records and Signature Rule 21 CFR Part 11 and how these are implemented in environmental monitoring with testo Saveris 1.

Many of our customers who are bound by FDA regulations rely on testo Saveris 1 for their environmental monitoring tasks. With the testo Saveris software, the automated and completely paper-free measurement data monitoring system offers integrated functions that comply with FDA requirements, and is thus validation-capable. This makes it much easier for our customers to fulfil the respective requirements in a sustainable and seamless manner and to switch from paper-based to electronic documentation.

21 CFR Part 11 contains a total of 19 regulations that specify all the system requirements, controls and processes that the FDA requires for the security of electronically transmitted and electronically signed documents. This white paper provides you with the wording of the 21 CFR Part 11 requirement catalogue and the corresponding technical specifications of testo Saveris 1 in a systematic form.

FDA APPROVED
FDA
FDA APPROVED

The text displayed on a light blue background in the document describes the requirements of FDA 21 CFR Part 11.

[1] For more information on FDA 21 CFR Part 11, as well as the original wording, please visit the following websites: http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11Guidance for Industry1 Part 11, Electronic Records; Electronic Signatures - Scope and Application http://www.fda.gov/RegulatoryInformation/Guidances/ucm125067.htm http://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/ucm124787.htm

Scope and criteria of the CFR regulations

11.1 Scope

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with § 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

testo Saveris 1 – designed for 21 CFR Part 11

The testo Saveris software is designed to fulfil the requirements of 21 CFR Part 11 regarding electronic records and electronic signatures throughout its lifetime. In order to achieve and maintain full compliance with the CFR, organizational and technical requirements must be met:

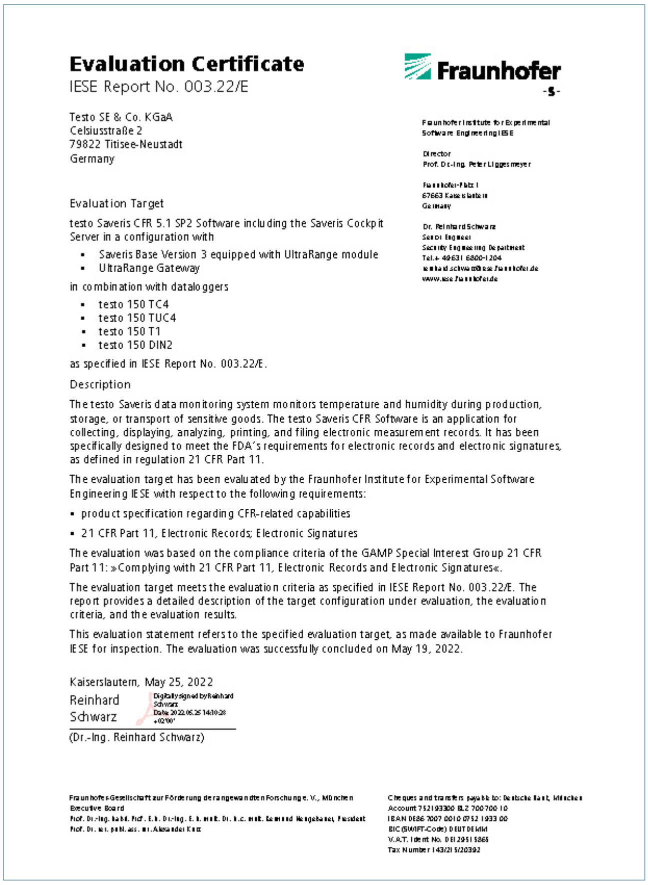
- Fulfilment of the organizational requirements means that pharmaceutical companies establish organizational structures and define, describe and document all processes in order to demonstrate what safeguards the respective company has in place to comply with the regulations and how these are enforced. The core of such documentation consists of SOPs (Standard Operating Procedures), which describe and regulate all processes in detail. These set out how those responsible should carry out processes and use systems to meet the requirements placed on them.

- Fulfilment of the technical requirements means that the requirements are met at the technical level through the use of products which, according to the manufacturer, are already suitable for this area, e.g. testo Saveris 1.

The advantages of the testo Saveris 1 data monitoring system include secure, centralized documentation and a range of different alarm options. In production processes and when storing and transporting pharmaceutical products, the system guarantees the secure recording, storage and archiving of measurement data. This means that testo Saveris 1 fulfils the requirements of 21 CFR Part 11 and enables users to save time and money with fully compliant automated measurement data management.

Prepared for the FDA audit: Software validation certificate

Tested measurement data monitoring system with certificate: The Fraunhofer Institute for Experimental Software Engineering confirms that the testo Saveris 1 measurement data monitoring system meets the requirements of 21 CFR Part 11. Testing took place in accordance with the evaluation guidelines of the GAMP Special Interest Group: complying with 21 CFR Part 11 Electronic Records, Electronic Signatures.



Evaluation Certificate
IESE Report No. 003.22/E

Fraunhofer
-S-

Testo SE & Co. KGaA
Celsiusstraße 2
79822 Titisee-Neustadt
Germany

Fraunhofer Institute for Experimental
Software Engineering IESE

Director
Prof. Dr.-Ing. Peter Liggesmeyer

Fraunhofer-Platz 1
67663 Kaiserslautern
Germany

Dr. Reinhard Schwarz
Senior Engineer
Security Engineering Department
Tel.+ 49 631 6800-1204
reinhard.schwarz@iese.fraunhofer.de
www.iese.fraunhofer.de

Evaluation Target

testo Saveris CFR 5.1 SP2 Software including the Saveris Cockpit Server in a configuration with

- Saveris Base Version 3 equipped with UltraRange module
- UltraRange Gateway

in combination with dataloggers

- testo 150 TC4
- testo 150 TUC4
- testo 150 T1
- testo 150 DIN2

as specified in IESE Report No. 003.22/E.

Description

The testo Saveris data monitoring system monitors temperature and humidity during production, storage, or transport of sensitive goods. The testo Saveris CFR Software is an application for collecting, displaying, analyzing, printing, and filing electronic measurement records. It has been specifically designed to meet the FDA´s requirements for electronic records and electronic signatures, as defined in regulation 21 CFR Part 11.

The evaluation target has been evaluated by the Fraunhofer Institute for Experimental Software Engineering IESE with respect to the following requirements:

- product specification regarding CFR-related capabilities
- 21 CFR Part 11, Electronic Records; Electronic Signatures

The evaluation was based on the compliance criteria of the GAMP Special Interest Group 21 CFR Part 11: »Complying with 21 CFR Part 11, Electronic Records and Electronic Signatures«.

The evaluation target meets the evaluation criteria as specified in IESE Report No. 003.22/E. The report provides a detailed description of the target configuration under evaluation, the evaluation criteria, and the evaluation results.

This evaluation statement refers to the specified evaluation target, as made available to Fraunhofer IESE for inspection. The evaluation was successfully concluded on May 19, 2022.

Kaiserslautern, May 25, 2022

Reinhard
Schwarz

Digitally signed by Reinhard
Schwarz
Date: 2022.05.25 14:10:28
+02'00'

(Dr.-Ing. Reinhard Schwarz)

Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V., München
Executive Board
Prof. Dr.-Ing. habil. Prof. E.h. Dr.-Ing. E.h. mult. Dr. h.c. mult. Reimund Neugebauer, President
Prof. Dr. rer. publ. ass. iur. Alexander Kurz

Cheques and transfers payable to: Deutsche Bank, München
Account 752193300 BLZ 700 700 10
IBAN DE86 7007 0010 0752 1933 00
BIC (SWIFT-Code) DEUTDEMM
V.A.T. Ident No. DE129515865
Tax Number 143/215/20392

Fig. 1: Independent certificate from the Fraunhofer IESE Institute

Documents to support your validation

These documents support you in the validation of the testo Saveris 1 system based on GAMP5:

1. Customizable templates for risk analysis

2. Customizable templates for
   - Validation Master Plan
   - Validation specifications

How to proceed with electronic submission

11.2 Implementation

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that

(1) The requirements of this part are met;

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S–0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

Access-protected PDF

For the reliable storage of electronic records, testo Saveris 1 offers the option of restricting the creation of PDF reports to a configurable, predefined report folder. If the user attempts to save the electronic PDF record to another location or to overwrite an existing measurement report, the report creation process is aborted.

PDF functions of testo Saveris 1:

- Automatic PDF reports (daily/weekly/monthly)
- Manual creation of PDF reports for user-defined time, secured with master password
- 21 CFR Part 11-compliant printouts
- Identification code for clear allocation of PDF reports

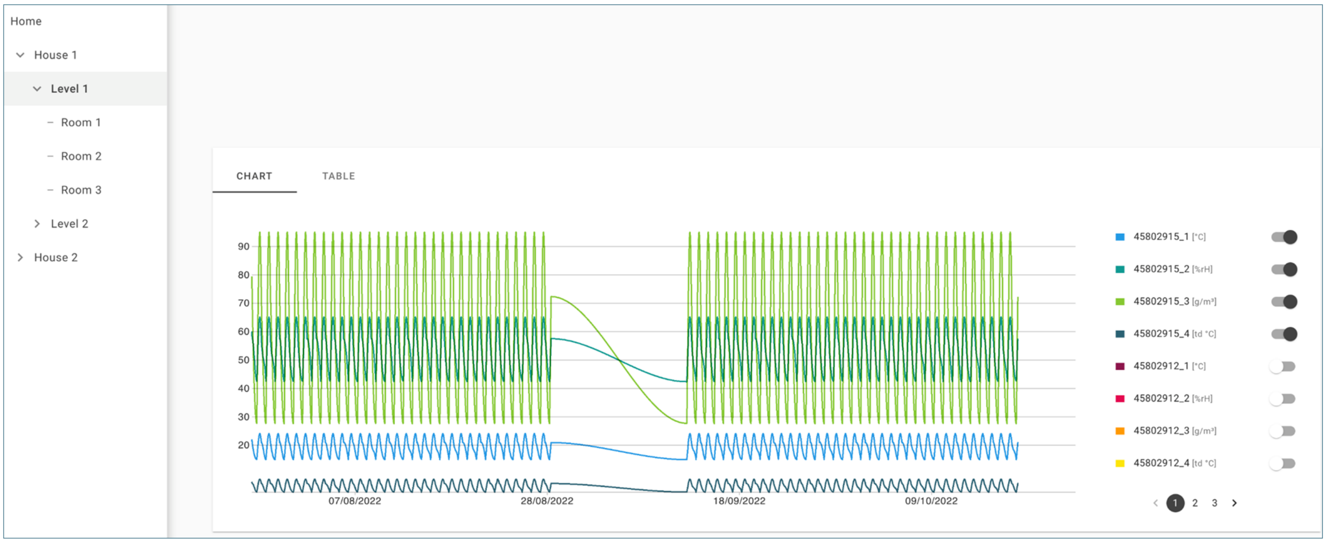
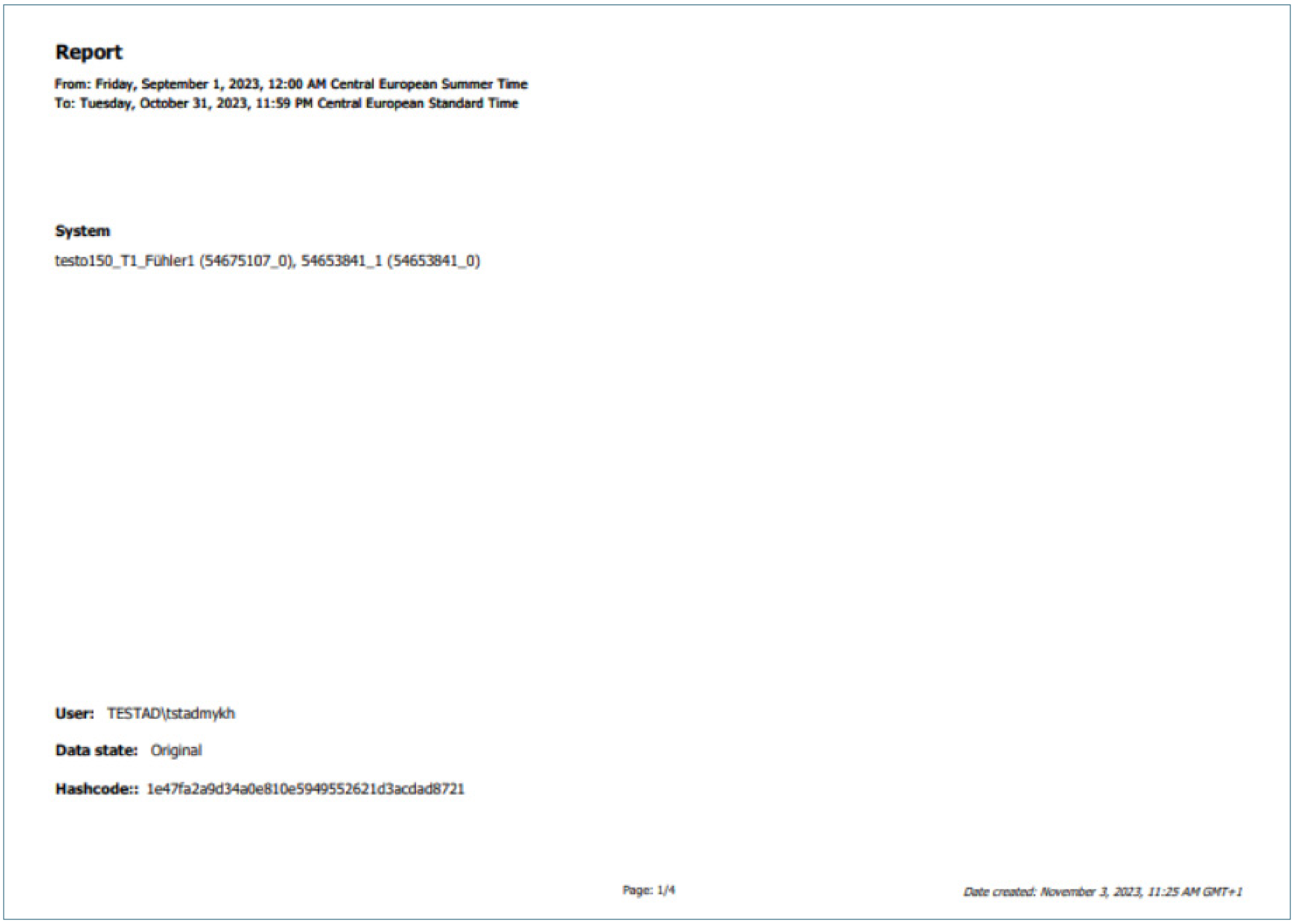


Fig. 2: Tamper-proof PDF report



Report

From: Friday, September 1, 2023, 12:00 AM Central European Summer Time
To: Tuesday, October 31, 2023, 11:59 PM Central European Standard Time

System

testo150_T1_Fühler1 (54675107_0), 54653841_1 (54653841_0)

User: TESTAD\tstadmykh

Data state: Original

Hashcode:: 1e47fa2a9d34a0e810e5949552621d3acdad8721

Page: 1/4

Date created: November 3, 2023, 11:25 AM GMT+1

Fig. 3: Report with electronic signature

User and access controls in closed systems

11.3 Definitions

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those **terms** when used in this part.

(b) The following definitions of terms also apply to this part:

(1) **Act** means the Federal Food, Drug, and Cosmetic Act (secs. 201–903 (21 U.S.C. 321–393))

(2) **Agency** means the Food and Drug Administration

(3) **Biometrics** means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable

(4) **Closed system** means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system

(5) **Digital signature** means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified

(6) **Electronic record** means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system

(7) **Electronic signature** means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature

(8) **Handwritten signature** means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark

(9) **Open system** means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system

User creation and role assignment in the testo Saveris 1 user management system

New users can be created within the user management system by persons authorized to manage users. When creating a user, it is mandatory to enter a user name, email address and full name, while entering a telephone number is optional. It is also possible to assign roles to the user during the creation process. The newly created user then receives an e-mail with a link to a website where they can set their password.

Access rights

Basic access control is based on the operating system's administrative functions for user accounts and user groups. Authorized users of the testo Saveris software require a valid user name and password. They must also belong to one of the testo Saveris software's authorized user groups in order to be able to use the Editor or the Viewer

System validation

The system used must be validated in its environment to ensure accuracy, reliability and performance. Invalid or altered data records should be detected and isolated in good time, either automatically or via appropriate validation techniques. Testo Customer Service provides on-site software validation together with qualification documentation for installing testo Saveris 1.

Functions of the testo Saveris software

- Full integration of the access concept into the tried-and-tested Windows security system (e.g. user and password management)
- Authorization concept with allocation of rights by the Administrator for three user levels
- Testo's own protocol (proprietary) for wireless and Ethernet communication
- CFR-compliant data management with checksum-protected measured values
- Use of checksums to guarantee correct and secure data transmission
- Automatic and manual backup of the database possible

How to link the testo Saveris software to the NT security system

Local groups are created to link the testo Saveris software to the NT security system.
Here, three local groups are added to the existing groups in the system management:

- Testo-Cockpit-Admins
- Testo-Cockpit-Power Users
- Testo-Cockpit-Users

The testo Saveris software is registered as the source of event log entries (audit trail and event logs).
An Administrator or a member of the Testo-ComSoft-Admins group can enable or disable individual functions or options in the system for user groups previously created at OS level.

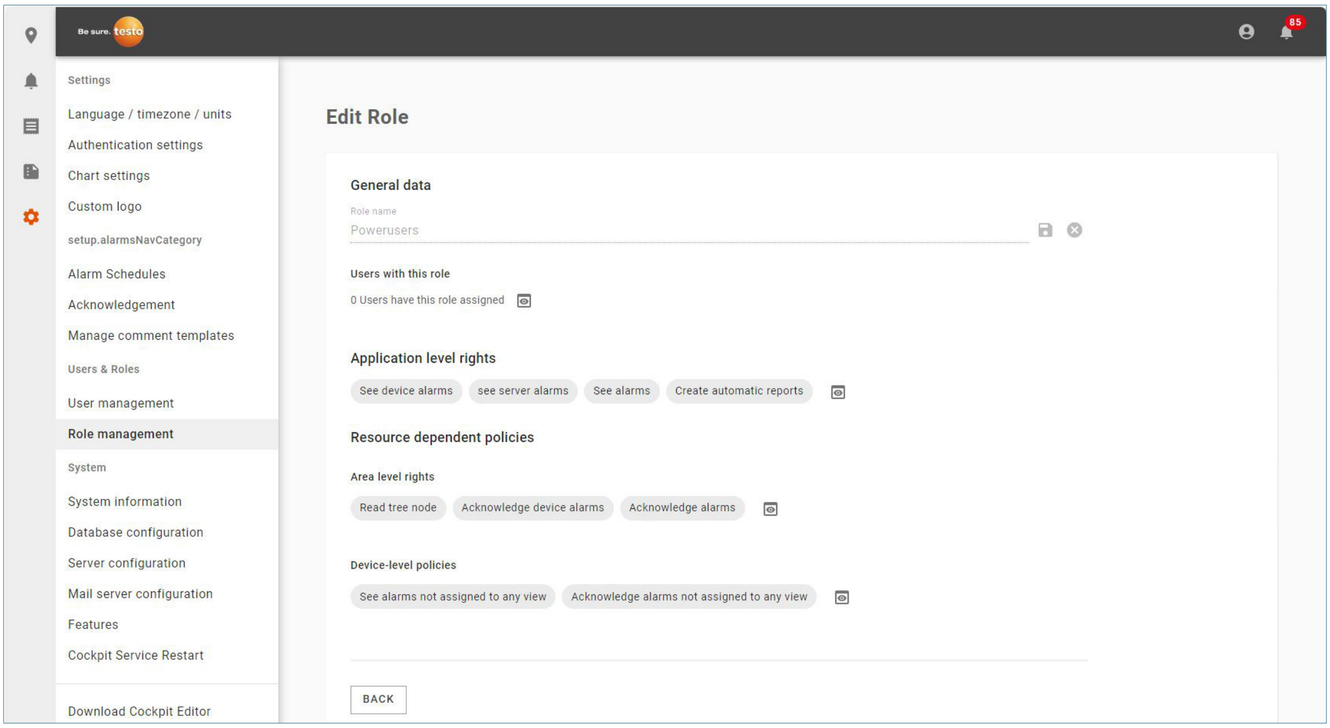
Tamper-proof processes and controls in closed systems

11.10 Controls for closed systems

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records

* Testo Customer Solution Services offer a wide range of country-specific validation services, such as system installation qualification (IQ) and operational qualification (OQ). We also support computer validation.



Edit Role

General data

Role name
Powerusers

Users with this role
0 Users have this role assigned

Application level rights
See device alarms | see server alarms | See alarms | Create automatic reports

Resource dependent policies

Area level rights
Read tree node | Acknowledge device alarms | Acknowledge alarms

Device-level policies
See alarms not assigned to any view | Acknowledge alarms not assigned to any view

Fig. 4: Checking and customizing user rights in the testo Saveris software (a)

(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

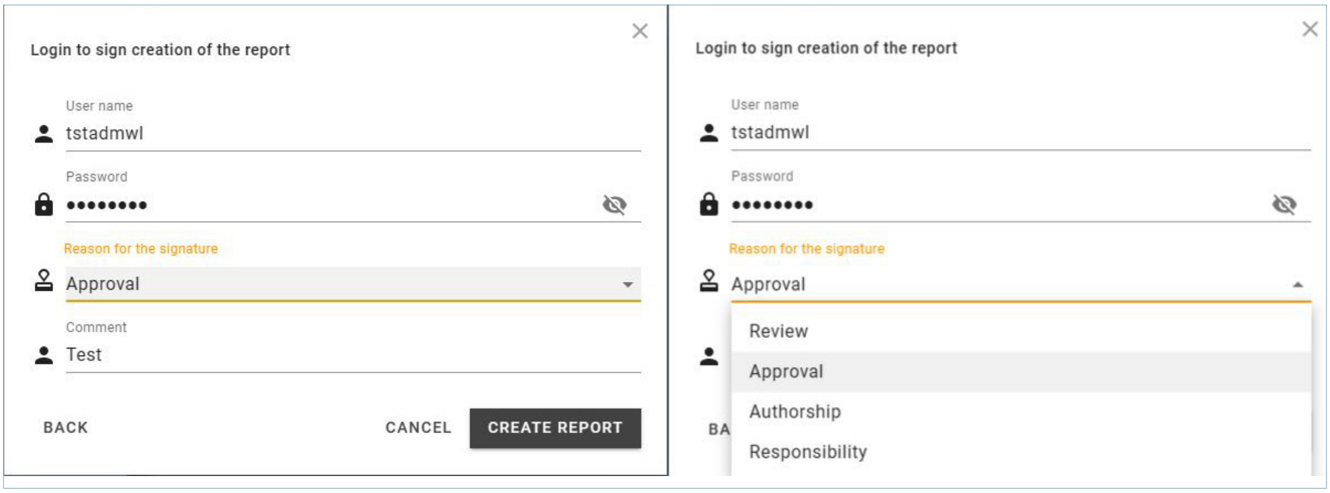
* With testo Saveris 1, reports on temperature ranges can be exported and viewed in PDF format, while the raw data is still securely stored in the database.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period

* The system supports both automatic backup rules and manual backups.

(d) Limiting system access to authorized individuals

* testo Saveris 1 offers flexible user management. It has user levels with different user rights and ensures that only authorized persons have system access.



Login to sign creation of the report

User name: tstadmwl

Password: ••••••••

Reason for the signature: Approval

Comment: Test

Login to sign creation of the report

User name: tstadmwl

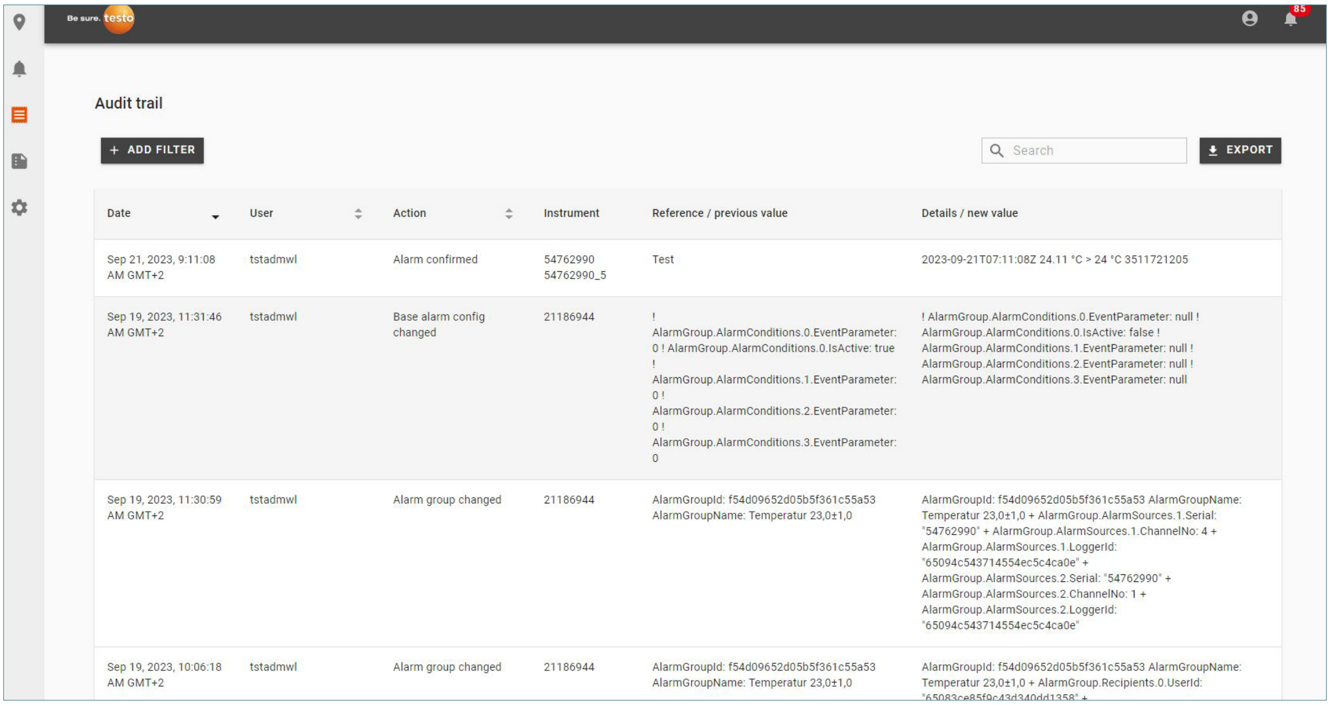
Password: ••••••••

Reason for the signature: Approval

Fig. 5: Generating an electronic report with signature (b)

(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying

* The testo Saveris software automatically tracks all user activities in the system. An audit trail documents the testo Saveris components, the time and user name of each event and the activity carried out.



Audit trail

Date	User	Action	Instrument	Reference / previous value	Details / new value
Sep 21, 2023, 9:11:08 AM GMT+2	tstadmwl	Alarm confirmed	54762990 54762990_5	Test	2023-09-21T07:11:08Z 24.11 °C > 24 °C 3511721205
Sep 19, 2023, 11:31:46 AM GMT+2	tstadmwl	Base alarm config changed	21186944	! AlarmGroup.AlarmConditions.0.EventParameter: 0 ! AlarmGroup.AlarmConditions.0.IsActive: true ! AlarmGroup.AlarmConditions.1.EventParameter: 0 ! AlarmGroup.AlarmConditions.2.EventParameter: 0 ! AlarmGroup.AlarmConditions.3.EventParameter: 0	! AlarmGroup.AlarmConditions.0.EventParameter: null ! AlarmGroup.AlarmConditions.0.IsActive: false ! AlarmGroup.AlarmConditions.1.EventParameter: null ! AlarmGroup.AlarmConditions.2.EventParameter: null ! AlarmGroup.AlarmConditions.3.EventParameter: null
Sep 19, 2023, 11:30:59 AM GMT+2	tstadmwl	Alarm group changed	21186944	AlarmGroupId: f54d09652d05b5f361c55a53 AlarmGroupName: Temperatur 23,0±1,0	AlarmGroupId: f54d09652d05b5f361c55a53 AlarmGroupName: Temperatur 23,0±1,0 + AlarmGroup.AlarmSources.1.Serial: "54762990" + AlarmGroup.AlarmSources.1.ChannelNo: 4 + AlarmGroup.AlarmSources.1.LoggerId: "65094c543714554ec5c4ca0e" + AlarmGroup.AlarmSources.2.Serial: "54762990" + AlarmGroup.AlarmSources.2.ChannelNo: 1 + AlarmGroup.AlarmSources.2.LoggerId: "65094c543714554ec5c4ca0e"
Sep 19, 2023, 10:06:18 AM GMT+2	tstadmwl	Alarm group changed	21186944	AlarmGroupId: f54d09652d05b5f361c55a53 AlarmGroupName: Temperatur 23,0±1,0	AlarmGroupId: f54d09652d05b5f361c55a53 AlarmGroupName: Temperatur 23,0±1,0 + AlarmGroup.Recipients.0.UserId: "65083ce85f9c43d340dd1358" +

Fig. 6: Audit trail for tracing user activities in the system (e)

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate

* Each audit trail records the sequence of processes and activities carried out after the software has ensured a correct sequence by specifying the necessary steps. In this way, testo Saveris 1 ensures that it is possible to perform a system check of events based on the sequence.

(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand

* In the case of actions that require a specific authorization, user and role management ensures that they can only be carried out by an appropriately authorized person. The verification of critical work steps (e.g. electronic signatures) is ensured by querying login data.

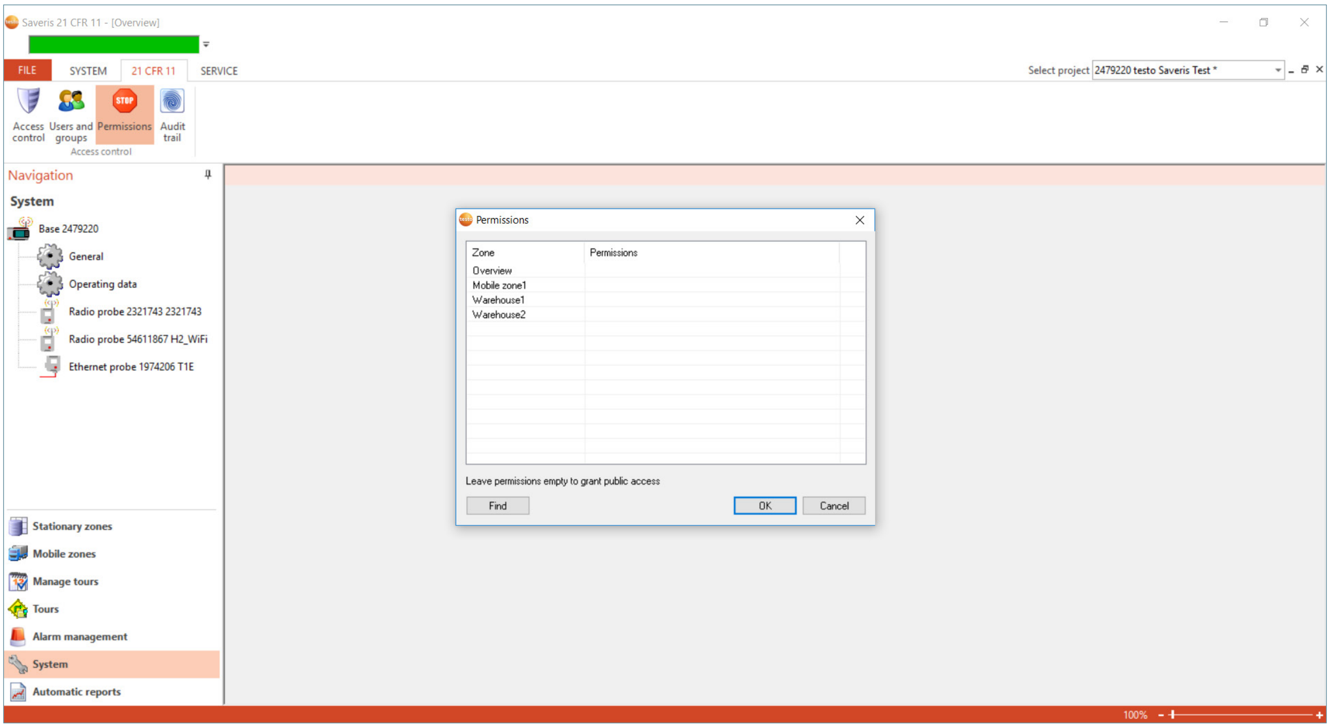
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction

* If required, the testo Saveris Cockpit V6.0 uses certificates to ensure the authenticity of the server in the browser and to protect the connection from data manipulation by means of encryption. All data connections between the devices are encrypted and use Testo certificates for authentication. This ensures the authenticity and integrity of the measurement data at all times.

(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification

* In addition to the technical precautions provided by testo Saveris 1 to comply with CFR regulations, additional precautions and controls are always required by the user. These include written policies and SOPs to ensure that individuals are accountable for the signatures they provide.



Zone	Permissions
Overview	
Mobile zone1	
Warehouse1	
Warehouse2	

Leave permissions empty to grant public access

Fig. 7: Individual zone assignment (j)

(k) Use of appropriate controls over systems documentation including:

*(1) All system documentation is available in electronic form. Each electronic document is given a unique identification code and publication date by Testo to facilitate distribution and version control.

*(2) Further developments and changes to the system are documented in the audit trail. This traceability ensures effective control.

* Testo Solutions GmbH Declaration of Regulatory Conformity

Secure application in open systems

11.30 Controls for open systems

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

testo Saveris 1 - a closed system even in open environments

testo Saveris 1 hosts the data centrally in a closed system that offers two different options:
On-premise (managed by the customer's IT department) and private cloud.

If you opt for a private cloud, the data is stored on a server that is managed by a third party. For this type of hosting, an assessment must be carried out to ensure that the supplier's security policies comply with the GxP guidelines and the requirements of FDA 21 CFR Part 11.[2] Our engineers will be happy to advise you on how to best configure your system.

Unlike data hosting, this feature uses buckets only as a means of transferring data from multiple locations to the central database. A bucket is temporarily filled with data and as soon as this data is synchronized with the central database, it is removed from the bucket.

[2] Information about AWS and GxP: https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_GxP_Systems.pdf
Information about Microsoft Azure and GxP: https://gallery.technet.microsoft.com/Azure-GxP-Guidelines-ab1b98d9

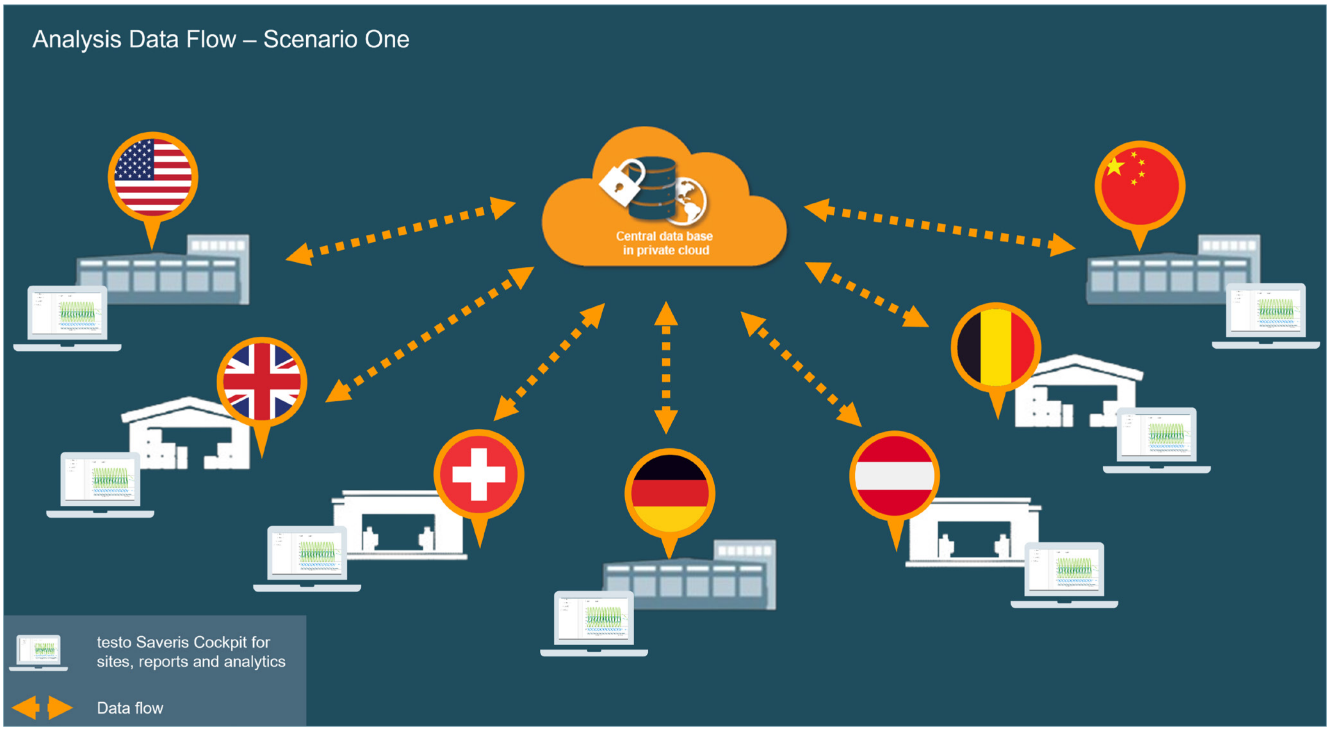

Analysis Data Flow – Scenario One
Central data base in private cloud
testo Saveris Cockpit for sites, reports and analytics
Data flow

Fig. 8: Setting up a private cloud database

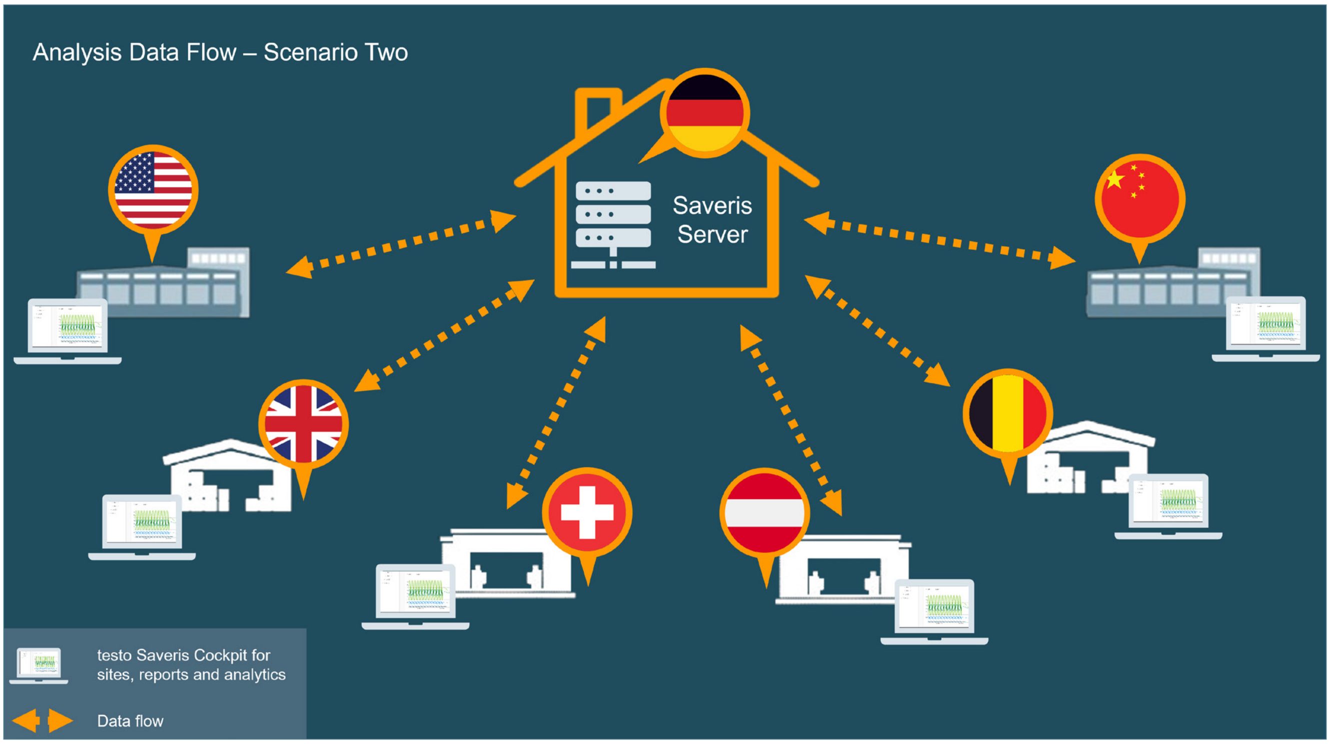

Analysis Data Flow – Scenario Two
Saveris Server
testo Saveris Cockpit for sites, reports and analytics
Data flow

Fig. 9: Setting up on the premises

Signature and signing

11.50 Signature manifestations

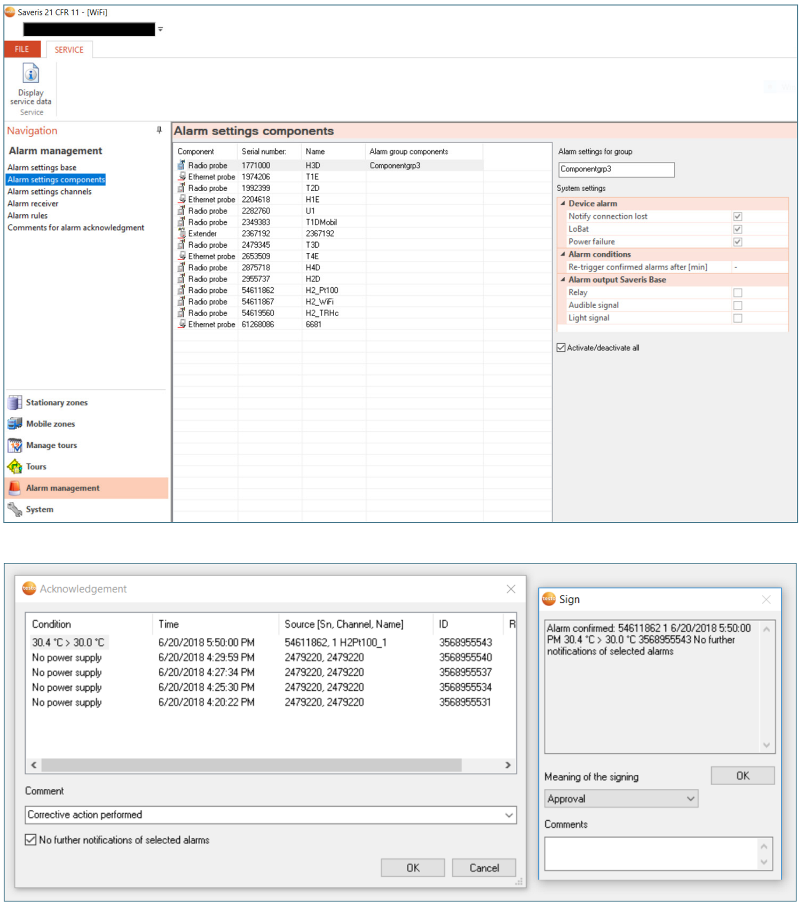
(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).



Saveris 21 CFR 11 - [WiFi]

[redacted]

Alarm settings components

Component	Serial number:	Name	Alarm group components
Radio probe	1771000	H3D	Componentgrp3
Ethernet probe	1974206	T1E	
Radio probe	1992399	T2D	
Ethernet probe	2204618	H1E	
Radio probe	2282760	U1	
Radio probe	2349383	T1DMobil	
Extender	2367192	2367192	
Radio probe	2479345	T3D	
Ethernet probe	2653509	T4E	
Radio probe	2875718	H4D	
Radio probe	2955737	H2D	
Radio probe	54611862	H2_Pt100	
Radio probe	54611867	H2_WiFi	
Radio probe	54619560	H2_TRHc	
Ethernet probe	61268086	6681	

Alarm settings for group: Componentgrp3

System settings

Device alarm	
Notify connection lost	☑
LoBat	☑
Power failure	☑
Alarm conditions	
Re-trigger confirmed alarms after [min]	-
Alarm output Saveris Base	
Relay	☐
Audible signal	☐
Light signal	☐

☑ Activate/deactivate all

Acknowledgement

Condition	Time	Source [Sn, Channel, Name]	ID	R
30.4 °C > 30.0 °C	6/20/2018 5:50:00 PM	54611862, 1 H2Pt100_1	3568955543	
No power supply	6/20/2018 4:29:59 PM	2479220, 2479220	3568955540	
No power supply	6/20/2018 4:27:34 PM	2479220, 2479220	3568955537	
No power supply	6/20/2018 4:25:30 PM	2479220, 2479220	3568955534	
No power supply	6/20/2018 4:20:22 PM	2479220, 2479220	3568955531	

Comment: Corrective action performed

☑ No further notifications of selected alarms

Sign

Alarm confirmed: 54611862 1 6/20/2018 5:50:00 PM 30.4 °C > 30.0 °C 3568955543 No further notifications of selected alarms

Meaning of the signing: Approval

Comments:

Fig. 10/11: Acknowledging an alarm and changing an alarm setting

testo Saveris 1 provides all the functions needed

The system requires an electronic signature for certain user actions. This signature is also displayed in the audit trail, stating the reason for the signature, e.g. to change a configuration. An electronic signature can be made mandatory for defined user actions, such as:

- Acknowledging alarms
- Changing alarm settings
- Editing settings for automatic reports
- Defining report contents and creating a one-off report
- Changing system settings
- Editing security settings

11.70 Signature/record linking

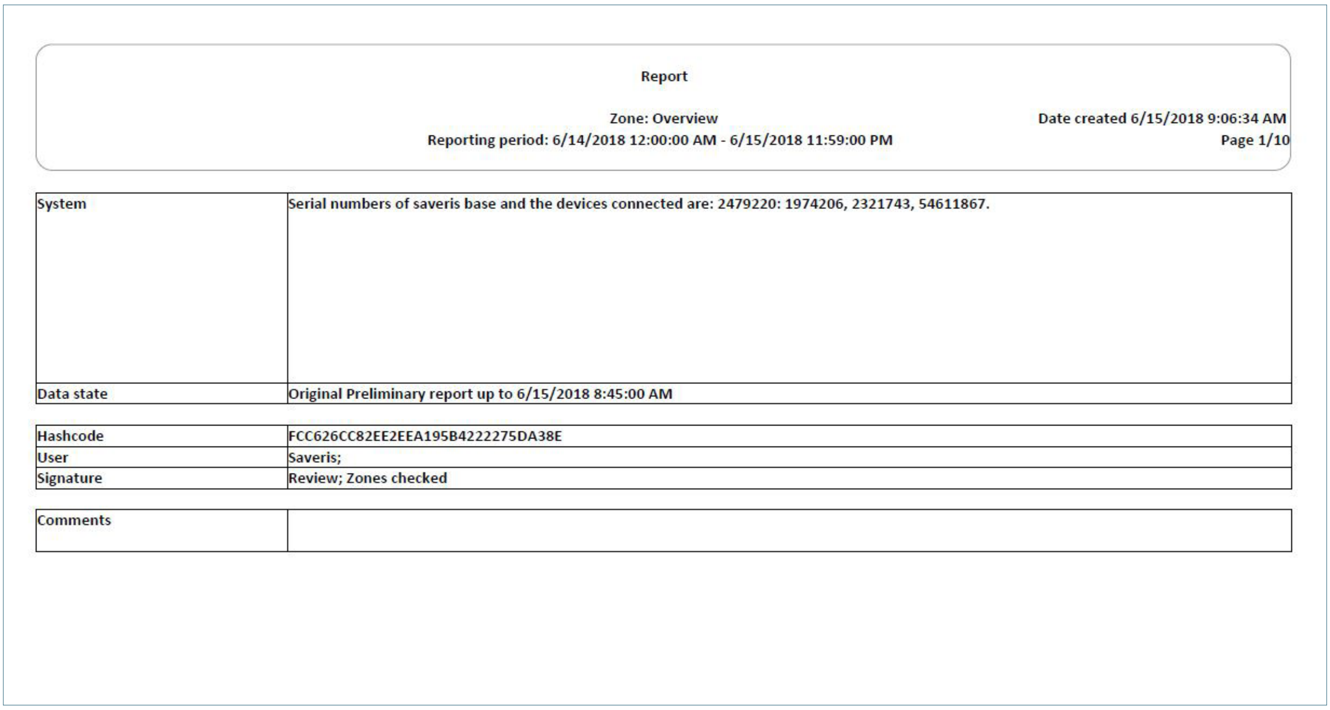
Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

Electronic signature data as an integral part of the record

With testo Saveris 1, once electronic signatures have been created, they can no longer be deleted, copied or altered using conventional methods. Electronic signatures can be enforced and set up for the following parameters/actions:

- Editing and acknowledging alarms
- Defining the content of a report
- Changing system settings
- Editing zones
- Editing settings for automatic reports
- Editing access controls

You can make a comment mandatory for all actions.



Report

Zone: Overview
Reporting period: 6/14/2018 12:00:00 AM - 6/15/2018 11:59:00 PM

Date created 6/15/2018 9:06:34 AM
Page 1/10

System	Serial numbers of saveris base and the devices connected are: 2479220: 1974206, 2321743, 54611867.
Data state	Original Preliminary report up to 6/15/2018 8:45:00 AM

Hashcode	FCC626CC82EE2EEA195B4222275DA38E
User	Saveris;
Signature	Review; Zones checked

Comments	

Fig. 12: How a signature in a system/zone report is linked to an individual

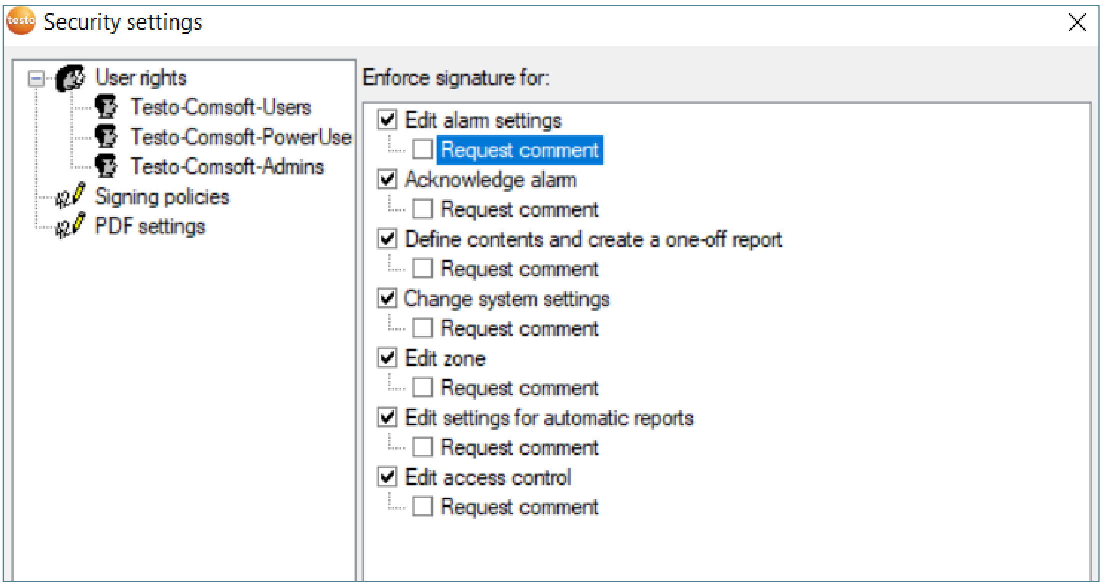
Electronic signatures and controls

11.100 General requirements

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual’s electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.
(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

testo Saveris 1 provides unique electronic signatures

With testo Saveris 1, each person’s electronic signature combination is unique. Electronic signatures are applied using a combination of a unique login name and a signature password. An electronic signature can be made mandatory for defined user actions.



Enforce signature for:

☑ Edit alarm settings
□ Request comment
☑ Acknowledge alarm
□ Request comment
☑ Define contents and create a one-off report
□ Request comment
☑ Change system settings
□ Request comment
☑ Edit zone
□ Request comment
☑ Edit settings for automatic reports
□ Request comment
☑ Edit access control
□ Request comment

Fig. 13: Electronic signatures with information about the reason for the signature, e.g. to change system settings

Non-biometric electronic signatures

11.200 Electronic signature components and controls

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

Maximum security with Windows user management

The testo Saveris software electronic signatures are based on the user management functions of the operating system (user name and password).

To start a session and obtain the right to sign an electronic record, the user must log in to the operating system with a user name and password and have appropriate user and group permissions plus a suitable testo Saveris software user profile. The user must enter their account password for re-authentication each time they sign.

They can also protect testo Saveris software sessions by automatically logging out or using a password-protected screen saver. These mechanisms are provided by the operating system.

With an appropriate configuration, it is possible to force passwords to be changed at the first login. Passwords should therefore be unknown even to the system administrator. They cannot be disclosed in the conventional way.

Security regulations concerning password management

11.300 Controls for identification codes/passwords

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging)

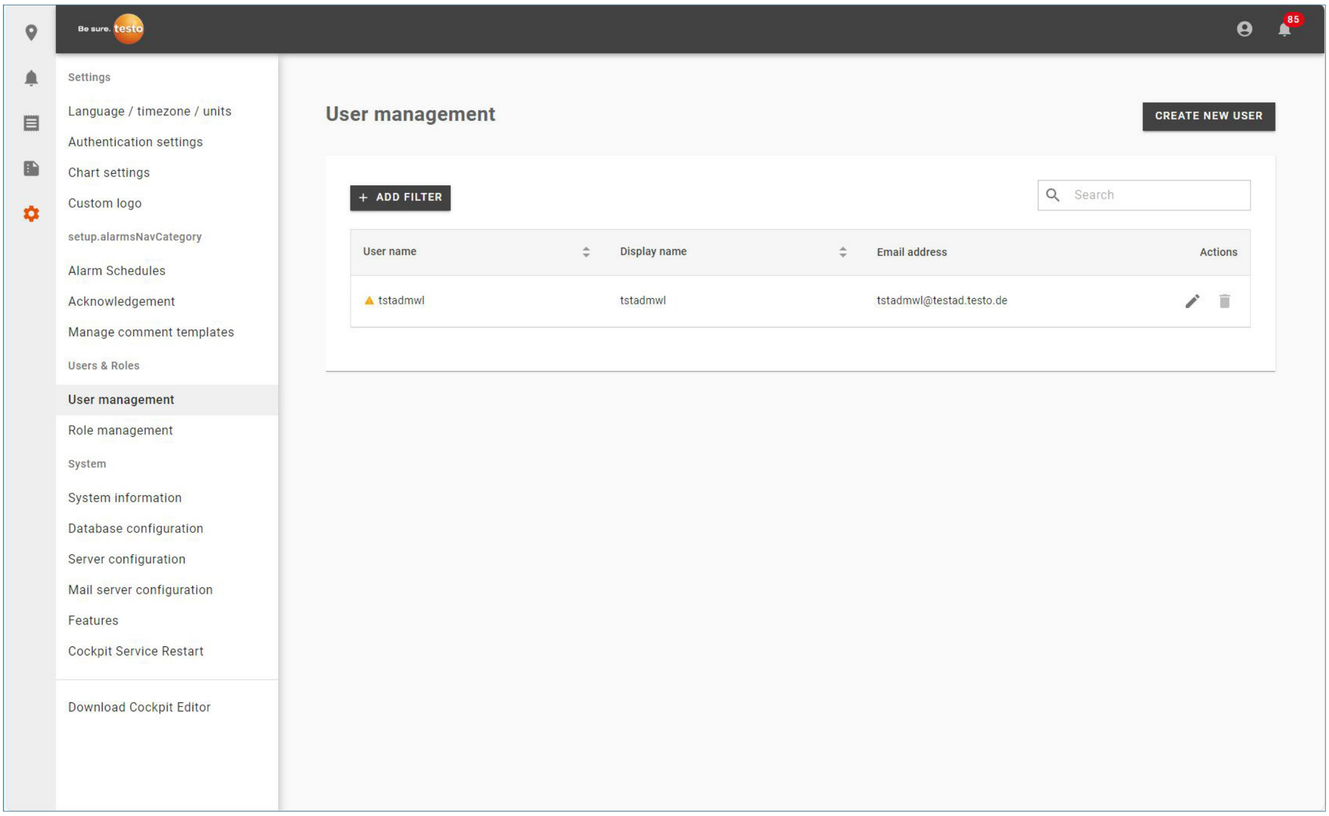
(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner

Convenient and secure password management

The testo Saveris software supports the system administrator in creating and managing passwords through integrated controls such as password length and queries about expiration dates as part of the Windows password policy. Password management must ensure unique user names and passwords for different individuals and the locking of accounts after failed attempts, as well as preventing passwords from expiring.



User name	Display name	Email address	Actions
⚠ tstadmwl	tstadmwl	tstadmwl@testad.testo.de	✎ 🗑

Fig. 14: Managing policies and passwords at Windows level

On the safe side:
CFR compliance with testo Saveris 1

testo Saveris 1 fulfils the requirements of 21 CFR Part 11

21 CFR Part 11 regulates the creation, archiving and management of electronic documents and sets stringent requirements for electronic signatures. With the completely paper-free testo Saveris 1 system, Testo offers the ideal solution to fulfil all CFR requirements at a technical level.

CFR-relevant features at a glance:

- Tested measurement data monitoring system with certificate from Fraunhofer IESE
- Maximum data integrity provided by strict security protocols
- Full integration of the user access concept into the tried-and-tested Windows security system
- Structured authorization management
- Convenient and secure password/signature management
- Testo’s own protocol (proprietary) for wireless and Ethernet communication
- CFR-compliant data storage with checksum-protected database
- Use of checksums to ensure correct and secure data transmission
- Automatic daily backup and manual backup of database files possible
- Ready for a possible FDA audit at any time

You benefit from high technological security standards provided by CFR compliance as well as high-precision and reliable measurement data monitoring in your pharmaceutical and medical processes.

Services related to testo Saveris 1

Pre-installation service

- Project management and personalized consulting
- Thermal mapping for optimum probe localization

Calibration and qualification/validation services

- Adjustment software that allows the customer to carry out their own calibration and adjustment (password protection, historical traceability of the adjustment data in the testo Saveris software)
- For systems with digital probes, the calibration data and expiry date are stored on the probe
- Calibration service in laboratories and on site in numerous countries

Qualification/validation

For all testo Saveris 1 solutions, Testo offers complete documentation and services related to hardware and software installation, commissioning, qualification and validation:

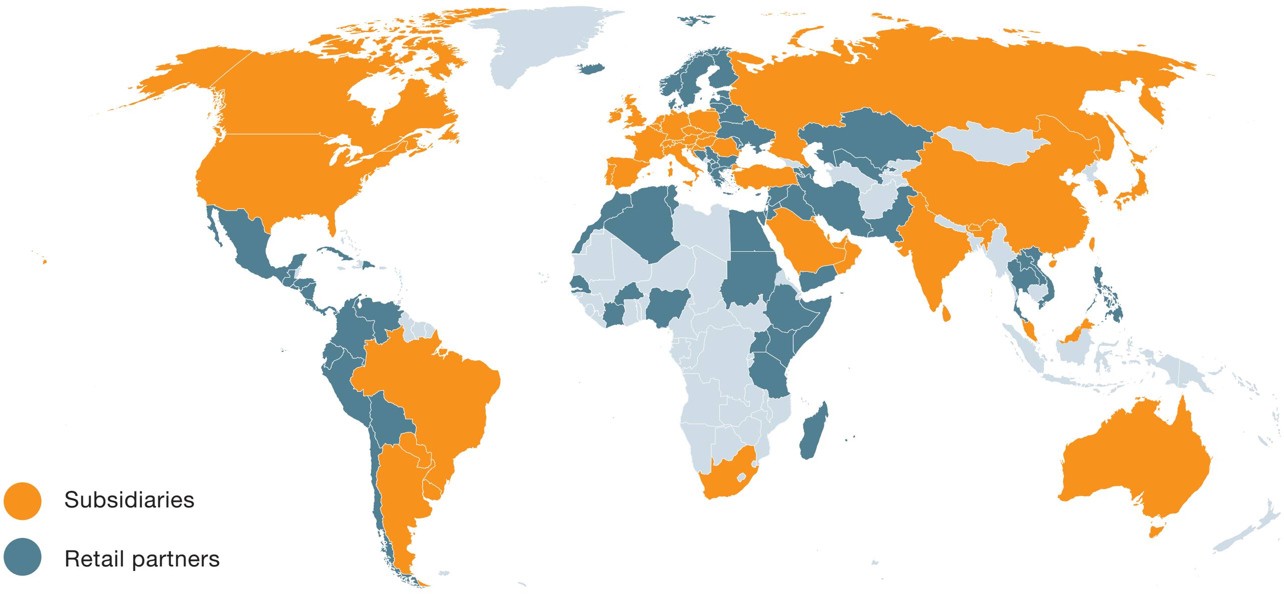
- DQ (Design Qualification), IQ (Installation Qualification), OQ (Operational Qualification), PQ (Performance Qualification)
- Customer-specific risk analyses taking into account GAMP5

Individual customer support with the Helpdesk packages for testo Saveris 1

	Basic	Advanced	Premium
Help with technical issues, usage advice and knowledge sharing beyond the warranty period	X	X	X
If you quote your customer and order number, you will receive advice from an expert, enabling most problems to be directly resolved upon initial contact.	X	X	X
Availability of our support team during our service hours	X	X	X
Guaranteed support team response time	Answer within **3 working days**	Answer within **24 hours**	Call back to clarify details within **3 hours**
Video platform: • Unlimited access to the Saveris video platform during the contract period • Numerous videos on the system operation and configuration		X	X
An annual Remote System Review: • List of the installed software, firmware and hardware inventories • Recommendations regarding the product life cycle of the installed testo Saveris components • Recommendations for improving system stability			X

Find out more at www.testo.com/solutions

High-tech solutions from southern Germany.



For over 60 years, Testo has been known for creating innovative measuring solutions made in Germany. As a world market leader in portable and stationary measuring technology, we help our customers to save time and resources, protect the environment and people's health and improve the quality of goods and services.

In 35 subsidiaries around the globe, more than 3,000 employees work in research, development, production and marketing for the high-tech company. Testo provides more than 1 million customers around the globe with high-precision measuring instruments and innovative solutions for the measurement data management systems of the future. An average annual growth rate of over 10% since the company's foundation in 1957 and a current turnover of just short of 300 million Euros impressively demonstrate that southern Germany and high-tech systems go hand in hand. The above-average investments in the future of the company are also a part of Testo's recipe for success. Testo invests about a tenth of its annual global turnover in research and development.

Find out more at www.testo.com/solutions

Subject to change, including technical modifications.

xxx1 xxx4/dk/12.2023

www.testo.com/solutions