Metrohm
ion analysis

06.2006/jb

Using the Titrando™ system to comply with 21 CFR Part 11

U.S. Department of Health and Human Services
Food and Drug Administration

The Title 21 Code of Federal Regulations Electronic Records; Electronic Signatures of the U.S. Food and Drug Administration, known as 21 CFR Part 11, defines the requirements for using electronic documentation and signatures. This rule, which has been in effect since 20 August, 1997, specifies in general how the system components, controls, and procedures have to be designed to ensure the reliability and authenticity of electronically stored records. It can be accessed at «http://www.fda.gov/ora/compliance_ref/Part11».

Achieving and maintaining full compliance to this rule necessitates Standard Operating Procedures (SOPs) that support and complement the functionality of electronic systems, this means that no product alone can ensure compliance. However, products with integrated functions supporting 21 CFR Part 11 requirements can make the task of achieving and maintaining full compliance with the rule significantly easier.

This document describes in detail how the Titrando system – either controlled by a Touch Control or the PC Control software – makes compliance with the requirements much easier. Each relevant section of 21 CFR part 11 is listed together with the corresponding feature of the Touch Control and the PC Control software.

21 CFR 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.

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

The electronic records of the Titrando system are described in Section 11.3 of this document, which covers their creation, modification, maintenance, archiving, and retrieval. The transmission of electronic records to agencies is discussed in Section 11.2 (b).

With each Titrando shipment, Metrohm provides detailed user documentation and certificates of software validation. Metrohm stores copies of all versions of its software documentation and source code in multiple secure locations, including a fireproof vault. Documentation includes product requirements, product specifications, design specifications, project schedules, test plans, test results, and validation documentation. All of these documents are produced for every release per the Metrohm Design Control Procedure, which has been registered to ISO 9001 and is periodically audited. All Metrohm documents and source code are available for inspection by FDA at Metrohm facilities.

To be prepared for a possible FDA audit, customers need to retain the following documents at their facilities:

Declaration of Conformity

Software Validation

Metrohm
ion analysis
CH-9101 Herisau, Switzerland
Tel. +41 71 353 85 85
Fax +41 71 353 89 01
www.metrohm.com

for the program

PC Control 4.1

Description

PC software for controlling Metrohm titration and automation instruments. Simple and intuitive user guidance. Creation of methods, carrying out titrations, storage and recalculation of results. Methods and data are compatible with Touch Control. Contains numerous tried and tested titration methods. Including hardware Dongle. Dialog in English, German and further freely definable languages.

6.6050.310 PC Control 4.1 Software

The above software was developed in accordance with the requirements of the ISO 9001 quality system regarding the design, testing and servicing of Metrodata software. The relevant procedures are described in the attached document «Project procedure for creating Metrodata software».

The technical specifications are documented in the instruction manual.

The software was validated with respect to functionality, analytical performance and accuracy of results. The software functions are documented in the instruction manual.

Herisau, 26 June, 2006

D. Strohm
Vice President
Head of R&D

Ch. Buchmann
Vice President
Head of Production
Responsible for Quality Assurance

8.840.0923

Fig. 1: Certificate of Software Validation

- Certificate of Software Validation (see *Fig. 1*). All certificates (PDF format) are included on the installation CD for the PC Control software.
- Completed Installation Qualification records (blank forms and procedures for the hardware installation can be obtained from Metrohm; the software automatically performs software IQ tests to verify that program files are correctly installed; after the installation a log-file containing the file structure of the program is stored with date and time of the installation: InstallLog-YYYYMMDD-hhmmss.txt).

- Operational Qualification and Performance Qualification records for the systems and methodologies used (Metrohm provides validation documentation which helps to perform the OQ and PQ).
- Site-specific standard operating procedures for security and records management.

21 CFR 11.2 IMPLEMENTATION

(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; and

(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.

Titrando users can export copies of the electronic records i. e. the determinations either as PC/LIMS Report in "formatted ASCII" format or in Portable Document Format (PDF, PC Control only) for submission to agency units, in accordance with FDA guidelines. The PC/LIMS Report files faithfully preserve the contents of the Touch Control or PC Control data. The PDF report files preserve the contents and formatting of the printed reports and can be protected against any modification. The PC/LIMS Report file and/or the PDF reports should be archived together with the determination file. The clear assignment of the PC/LIMS Report and the PDF report to the corresponding determination file is guaranteed by the corresponding file name containing the sample identification, date and time of the determination. PC/LIMS report and PDF report (PC Control only) of signed determinations contain all information about the electronic signatures (full name of the signer, date and time of signing and the meaning of signing).

21 CFR 11.3 DEFINITIONS

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

(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.

The Titrando system is implemented in a closed-system environment, where the persons responsible for the records also control access to the system. These persons include system administrators, who set up and maintain user accounts, together with any other persons (such as laboratory managers) who have been granted privileges to control access to locations where

Titrando data are stored. The security system of Touch Control/PC Control supplements the security systems of the chosen operating system by providing control over specific titration-related resources and operations, not just files and records.

Digital signatures are implemented in Touch Control and PC Control as described in Sections 11.50, 11.100, and 11.200.

With respect to 21 CFR part 11, the primary electronic records in Touch Control and PC Control are the original result records (determinations), which are encoded and provided with a check sum. Each record has all of the information pertaining to the analysis of a sample and contains the following items:

- Sample information (sample IDs, sample size)
- Method information (method name, method version, method sequence with all method parameters)
- Raw data and results (endpoints and other raw data, Lists of measuring points, titrant data, sensor data, all variables, used devices and calculated results)
- If any data are modified and stored, a new file version is created.
- The audit trail records all user entries and actions regarding system logs, user administration, result modifications, method modifications, sample data modifications and all other data changes, as described under Section 11.10 of this document.

The Titrando system can also generate backup files of all system data, for data recovery and/or archiving purposes. Contents of backup files cannot be accessed outside of Touch Control or PC Control; the contents of a backup must be restored into the system before they can be read. The audit trail keeps track of all backup and restore operations.

21 CFR 11.10 CONTROLS FOR CLOSED SYSTEMS

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

The validation of analytical systems generally includes installation qualification (IQ) and operational qualification (OQ) of instruments and software, as well as ongoing performance qualification (PQ). Metrohm offers a wide range of validation services ranging from IQ and OQ on-site tests performed by Metrohm service technicians up to automated routines built into the software (see Section 11.1). Ready-for-use methods for system validation are stored in the system. The setup of new method sequences and generation of reports for qualification tests is easily performed using Metrohm method templates.

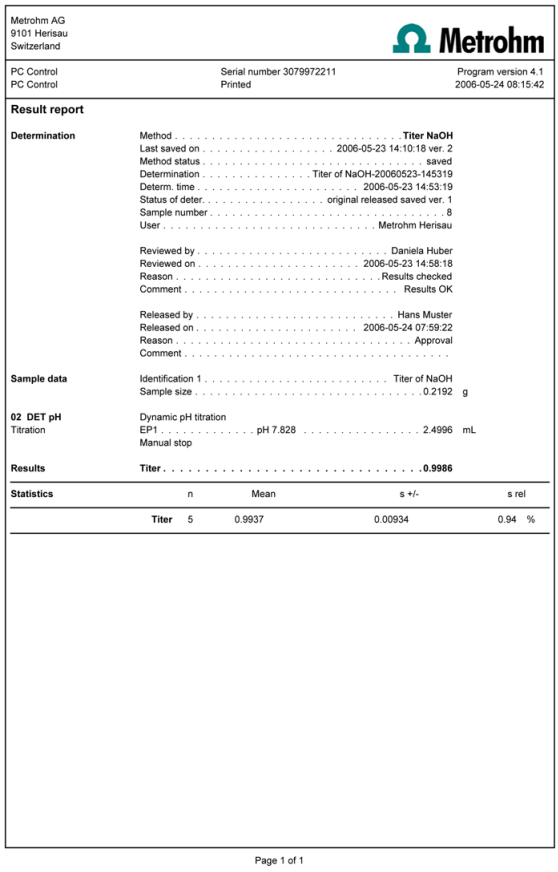
The audit trail (discussed in detail in Section 11.10 (e)), tracks all changes made to all data objects that are made within the application. The audit trail lists the time (incl. difference to UTC), date, user name, category, action, and details about the action and the affected data object for each event.

Modifications of stored data are labeled unambiguously in the reports. Data corruptions due to defects or failure of storage devices or media, or to deliberate attempts to modify records, are detected by the Titrando system (see Section 11.70).

21 CFR 11.10 CONTROLS FOR CLOSED SYSTEMS

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.

The Titrando system provides all the necessary functions for locating and viewing the electronic records on the system. Complete, accurate electronic copies of the electronic records i. e. the determinations can be generated as PC/LIMS Report in "formatted ASCII" or in PDF format (PC Control only) for submission to agency units. The automatic output at the end of a determination can be enforced using specific method settings. Besides, all determination data can be printed out as a configurable report. The clear assignment of all electronic and paper copies to the corresponding determination file is guarantied by the corresponding file name / determination name, containing the sample identification, date and time of the determination (see also section 11.2).



Metrohm AG
9101 Herisau
Switzerland

Metrohm

PC Control
PC Control
Serial number 3079972211
Printed
Program version 4.1
2006-05-24 08:15:42

Result report

Determination
Method . . . . . **Titer NaOH**
Last saved on . . . . . 2006-05-23 14:10:18 ver. 2
Method status . . . . . saved
Determination . . . . . Titer of NaOH-20060523-145319
Determ. time 2006-05-23 14:53:19
Status of deter. . . . . original released saved ver. 1
Sample number 8
User . . . . . Metrohm Herisau

Reviewed by . . . . . Daniela Huber
Reviewed on 2006-05-23 14:58:18
Reason . . . . . Results checked
Comment . . . . . Results OK

Released by . . . . . Hans Muster
Released on 2006-05-24 07:59:22
Reason . . . . . Approval
Comment . . . . .

Sample data
Identification 1 . . . . . Titer of NaOH
Sample size . . . . . 0.2192 g

02 DET pH
Titration
Dynamic pH titration
EP1 . . . . . pH 7.828 . . . . . 2.4996 mL
Manual stop

Results
Titer 0.9986

Statistics	n	Mean	s +/-	s rel
Titer	5	0.9937	0.00934	0.94 %

Page 1 of 1

Fig. 2: First page of a result report generated with the Titrando system

21 CFR 11.10 CONTROLS FOR CLOSED SYSTEMS

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

The Titrando system provides several layers of protection to ensure that accurate records can be readily retrieved.

Using PC Control, the foundation for record protection is a secure operating system that provides positive user tracking and prevents unauthorized access to computers and files. Metrohm recommends the use of Windows® 2000 or Windows® XP, with the NTFS file system.

The Touch Control is based on a secure, validated embedded system where unauthorized access to the data is inherently impossible.

The Titrando system controlled by Touch Control or PC Control provides a comprehensive, titration-oriented security system that controls access to data, described further in Section 11.10 (d). This ensures that only authorized users are able to access records and make changes; any such changes are tracked by system-generated audit trails, as described in Section 11.10 (e).

The Titrando system facilitates long-term record storage by an external archiving system through its built-in export tools. For each determination, all determination data including sample information (sample IDs, sample size), method information (method name, method version, method sequence with all method parameters), raw data and results (endpoints and other raw data, lists of measuring points, titrant data, sensor data, all variables, used devices and calculated results) can be exported manually or automatically as original determination file or PC/LIMS Report ("formatted ASCII" format). The determination files are encoded and provided with a check sum to protect it from unwanted or improper alteration.

21 CFR 11.10 CONTROLS FOR CLOSED SYSTEMS

d) Limiting system access to authorized individuals.

The advanced security system provided by the Titrando system supports an unlimited number of security levels if identification cards are used for login and two security levels in addition to the administrator level if the login screen is used. The security system of the Titrando is designed to fit the titration workflow.

Up to 100 different privileges can be allocated as appropriate to different routine users (see *Fig.* 3). These allow exact definitions of privilege profiles for different users (for example, Lab Managers would typically be granted privileges to create and modify methods, whereas Operators might only have privileges to start methods.)

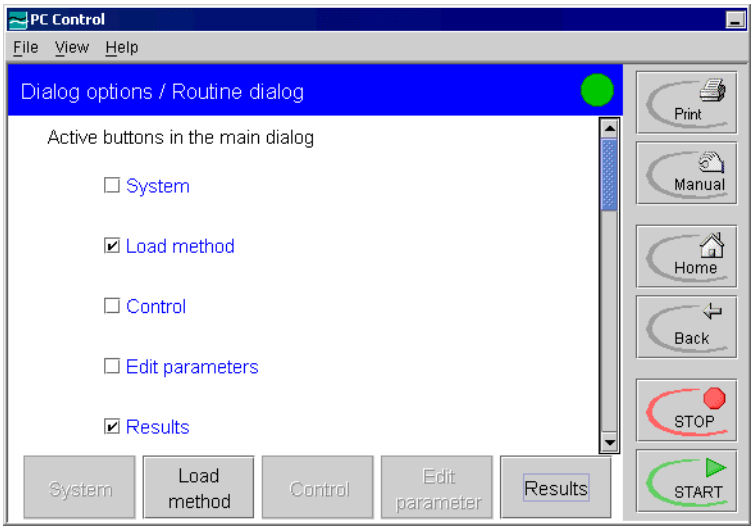


Fig. 3: The comprehensive, titration-specific security system of the Titrando gives the system administrator detailed control over each user's access to all functions

Ideally the routine configuration for each user is stored together with the user identification (user name) and the methods the user is allowed to use on an identification card. When the user logs in, his specific dialog settings are loaded after he has entered his password. The same identification card can be used on several Titrando systems, where the user is registered. The administrator can copy the user configuration from one Titrando system to another using the backup function of the system.

The security system of the Titrando provides the user management capabilities most often requested by system administrators:

- Users are identified by a unique user name and the full name throughout the software.

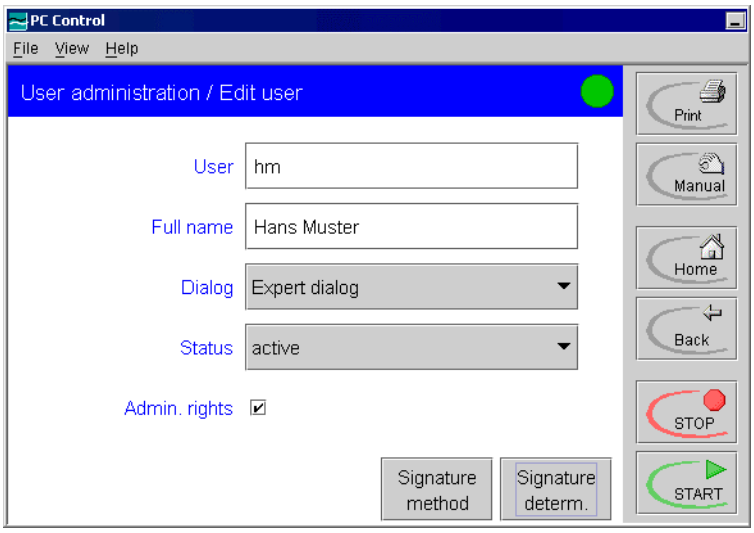


Fig. 4: Users are identified by user name and full name throughout the software

- Sessions can be automatically locked after a specified period of inactivity to make sure that unauthorized people cannot access the system if an authorized user fails to log out before leaving the Titrando system. It can be enforced that as long as the system is not shut down only the last registered user can login again.

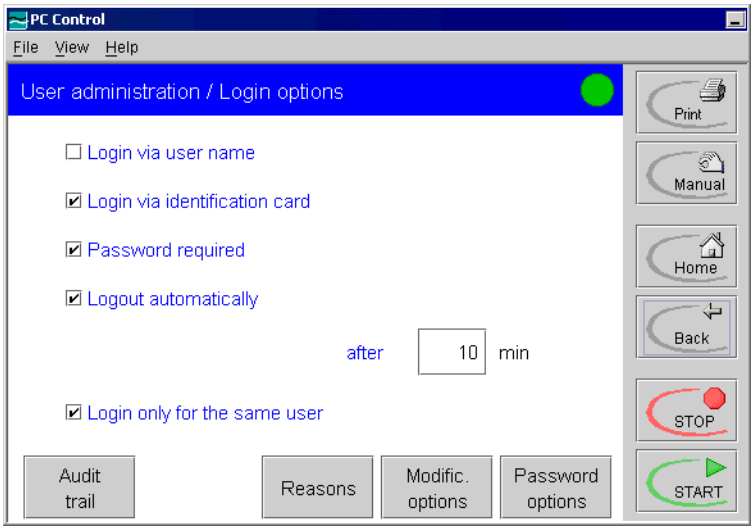


Fig. 5: Security policies for login like e. g. automatic logout after a pre-set time the system was not used can be set

- Password controls – such as minimum password length, special characters requirements, and password age limits – can be enforced. The password can be changed by the user at any time. It is never displayed, thus only the user knows his or her password.
- Users can be automatically locked out after a pre-set number of login failures. The user account is disabled automatically and must be reactivated by the system administrator before it can be used again.

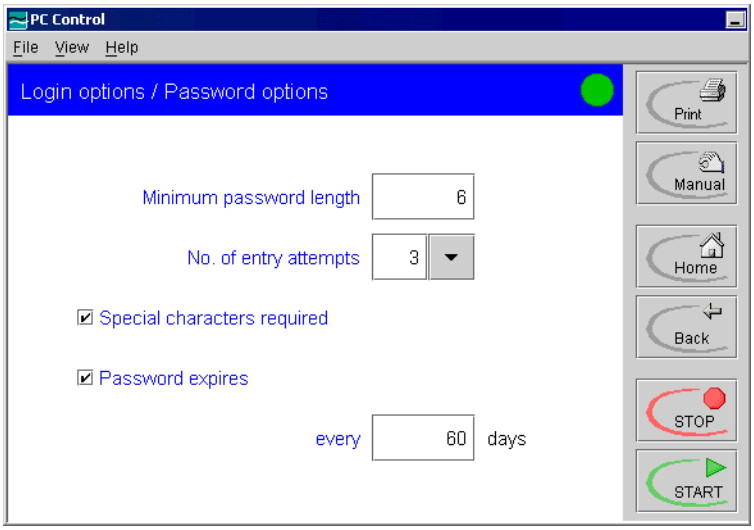


Fig. 6: Security policies for password protection like e. g. automatic deactivation of a user account after a preset number of failed login attempts can be set

- User and password history logs are automatically maintained in the audit trail.

21 CFR 11.10 CONTROLS FOR CLOSED SYSTEMS

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 Titrando system automatically tracks all operator entries and actions that create, modify, or delete electronic records. It does this by maintaining secure, system-generated, time-stamped audit trails. The audit trails record the time (incl. difference to UTC) and date of each event together with the name of the operator involved. Changes to records add new entries to the audit trails, in such a way that previously recorded information is not obscured. The system administrator has fine control over who is allowed to make changes to data. Audit trail entries cannot be modified afterwards.

The audit trail keeps detailed records of all relevant changes made to data objects and electronic records in a Titrando data source. It documents the creation and modification of methods and sample entries. The recording of audit trail can be enabled by the Titrando system administrator (see *Fig. 7*).

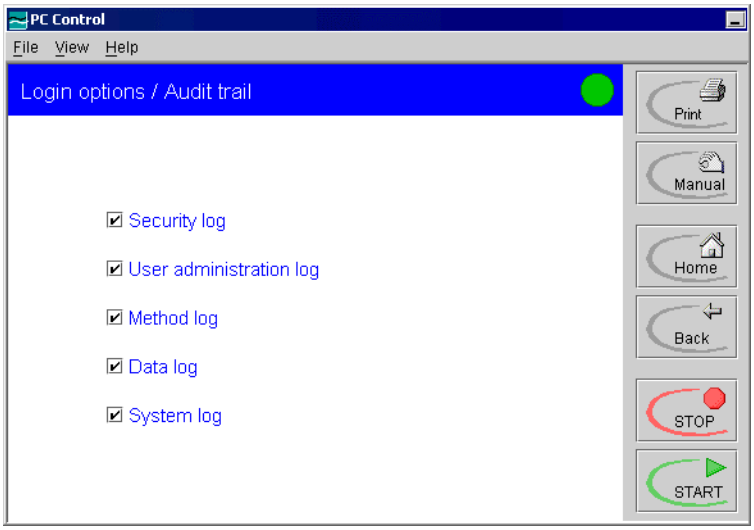


Fig. 7: Audit trail settings accessible to the system administrator

For each event the audit trail display (see *Fig. 8*) lists the type of event, the corresponding time and date, user name, category, action, and details about the action and the affected data object. Time and date are represented in an unambiguous format according to ISO 8601. Together with the time, the difference to UTC (Coordinated universal time) is displayed. For all value changes the old and the new value are registered.

Users can be obliged to enter a reason after changes made to methods and results (recalculation of determinations) in order to ensure that their intentions are clearly documented.

However, in an unsecured operating system, it could be possible for a user to gain access at the operating system level and delete or corrupt one of the files cited above. Missing or altered electronic records are recognized by the system. Nevertheless, Metrohm recommends that regulated laboratories store all data on secured computers running Windows 2000® or Windows XP®, with the NTFS file system.

The PC Control software provides all the necessary functions for sorting, filtering and viewing audit trails in the system and for exporting the audit trails at any time. The exported file can be archived and would be available for agency review and copying.

Audit trail

File Filter

No		Date	User	Category	Action	Details
1	⚠	2006-05-19 11:26:24		Admin	Change audit t. opt.	Security log off --> on
2	⚠	2006-05-19 11:26:24		Admin	Change audit t. opt.	User administration log off --> on
3	⚠	2006-05-19 11:26:24		Admin	Change audit t. opt.	Method log off --> on
4	⚠	2006-05-19 11:26:24		Admin	Change audit t. opt.	Data log off --> on
5	⚠	2006-05-19 11:26:24		Admin	Change audit t. opt.	System log off --> on
6	🖫	2006-05-19 11:26:58		Admin	Edit user	jb Jürg Expert dialog Status active Admin. rights on Use o
7	🖫	2006-05-19 11:27:02		Admin	Edit user	jb Jürg Expert dialog Status active Admin. rights on Use o
8	⚠	2006-05-19 11:27:40		Admin	Change sign options	jb Review methods (signature level 1) off --> on
9	⚠	2006-05-19 11:27:40		Admin	Change sign options	jb Release methods (signature level 2) off --> on
10	⚠	2006-05-19 11:27:40		Admin	Change sign options	jb Delete signatures off --> on
11	🖫	2006-05-19 11:28:18		Admin	Edit user	ak Angelika Routine dialog Status active Admin. rights off
12	⚠	2006-05-19 11:28:30		Admin	Change login options	Login via user name off --> on
13	⚠	2006-05-19 11:28:30		Admin	Change login options	Password required off --> on
14	⚠	2006-05-19 11:28:36		Admin	Change password opt.	Password expires off --> on
15	⚠	2006-05-19 11:28:36		Admin	Change password opt.	Password expires 365 --> 30
16	⚠	2006-05-19 11:28:48		System	Message	002-113 Method not saved Yes/OK
17	🖫	2006-05-19 11:28:48		Security	Logout	
18	⚠	2006-05-19 11:29:06	Admin	Security	Change password	
19	🖫	2006-05-19 11:29:10	Admin	Security	Login	Admin
20	🖫	2006-05-19 11:29:29	Admin	Method	New	Empty method
21	🖫	2006-05-19 11:29:38	Admin	Method	Insert command	New method V0 01 CAL pH
22	🖫	2006-05-19 11:29:44	Admin	Method	Edit	New method V0 01 CAL pH Stirrer off
23	🖫	2006-05-19 11:30:09	Admin	Method	Start	New method V0 1.0 g
24	🖫	2006-05-19 11:30:09	Admin	Method	Start	Start key pressed
25	🖫	2006-05-19 11:30:36	Admin	Method	Stop	New method V0
26	⚠	2006-05-19 11:31:14	Admin	System	Message	002-113 Method not saved Yes/OK
27	🖫	2006-05-19 11:31:14	Admin	Security	Logout	Admin
28	⛔	2006-05-19 11:31:28	jb	Security	Login message	Password expired
29	⚠	2006-05-19 11:31:40	Admin	System	Message	002-110 Password expired Yes/OK
30	⚠	2006-05-19 11:31:44	jb	Security	Change password	
31	🖫	2006-05-19 11:31:46	jb	Security	Login	Jürg
32	🖫	2006-05-19 11:32:11	jb	Method	New	Empty method
33	🖫	2006-05-19 11:32:36	jb	Method	Insert command	New method V0 01 DET pH
34	⛔	2006-05-19 11:33:08	jb	System	Message	010-003-1-X Other devices at MSB Yes/OK

Fig. 8: The audit trail tracks all relevant changes to the data objects

21 CFR 11.10 CONTROLS FOR CLOSED SYSTEMS

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

The Touch Control and PC Control software has a context-sensitive structure that hides or disables functions that are not relevant, not appropriate, or not permitted within the current context. This structure helps to ensure that steps and events occur in a proper sequence. The Titrando system provides many ready-for-use templates e. g. for methods and calculations that help users to avoid errors. The sequence of an analysis is defined in the method and must be strictly observed. It cannot be altered during the analysis. Specific methods can be assigned to sample identifications to enforce the use of the correct method. The Titrando system performs numerous error checks when instruments are configured and when methods are defined and readied for execution. Any conflicts must be resolved before the user is allowed to proceed.

21 CFR 11.10 CONTROLS FOR CLOSED SYSTEMS

(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.

As described under Section 11.10 (d), the Titrando system provides a comprehensive, titration-specific security system that controls access to instruments and data and also defines the types of operations that each user can perform. As described under Section 11.50, the Touch Control and PC Control software also control who is authorized to electronically sign methods and results.

21 CFR 11.10 CONTROLS FOR CLOSED SYSTEMS

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

Upon installation, PC Control automatically performs a Software Installation Qualification to verify that all software components are correctly installed. A report (InstallLog-YYYYMMDD-hhmmss.txt) is stored to disk and can be printed out. All connected Metrohm devices are recognized automatically, checked for validity and entered into the device list. The Titrando system records specific information about actual devices used (hardware configuration, serial numbers, etc.). Password-controlled logins, both at the operating system level and at the PC Control and Touch Control level, are used to prevent unauthorized access and to identify users, regardless of where they log in.

21 CFR 11.10 CONTROLS FOR CLOSED SYSTEMS

(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.

Metrohm regularly provides appropriate training for its product developers, service engineers, and support personnel. Records of training are maintained in accordance with training policies that are registered to ISO 9001.

Metrohm provides on-site introductory training for users at the time of installation. Additional training is recommended for laboratory managers and for support personnel. System administrators should also attend a Titrando course.

Off-site classes are regularly conducted in Metrohm field offices. Custom on-site training courses are also available.

21 CFR 11.10 CONTROLS FOR CLOSED SYSTEMS

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

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

The Titrando system possesses an extensive, context sensitive online help system that always provides detailed information about the functions the operator just uses. Metrohm supplies user

documentation in printed and electronic form together with the software. Release notes providing a history of changes from release to release are provided with the software.

21 CFR 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).

The comprehensive implementation of electronic signatures in the Titrando system provides all the functionality required by Section 11.50, while satisfying laboratory workflow needs.

In the security and user management system of Touch Control/PC Control, the system administrator can grant specific users the privilege of applying electronic signatures (see *Fig. 9*) for methods and results.

The individual signature password (identical to the login password) is defined for each individual user. Functions such as minimum password length, password uniqueness requirements, password age control, and password history are supported for passwords (see *Fig. 6*).

Applying electronic signatures for method and result records (determinations) is a simple, straightforward process. In the Sign dialog for methods and determinations, the operator selects the signing level (review or release), enters his user identification and individual password, selects a reason for signing from a previously defined list and eventually enters an additional comment (see *Fig. 9*). With the sign button, the record is signed and the information associated with the signing (full name of the signer, date and time of signing and meaning) is stored.

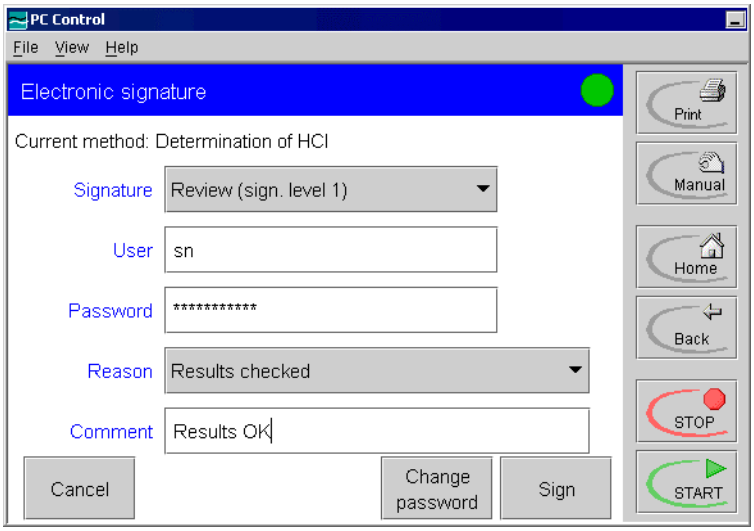


Fig. 9: The user applies the electronic signature to the method or determination by entering his/her user identification and individual password

21 CFR 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 so as to falsify an electronic record by ordinary means.

In the Titrando system, electronic signature data is stored as an integral part of signed-off records, in such a way that the signature data cannot be deleted, copied, or otherwise transferred by ordinary means.

21 CFR 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.

In the Titrando system electronic signatures are implemented using a combination of a user's unique login name and a password. Because the software requires a unique login name for each individual, each person's signature combination is unique.

The software maintains a history of passwords, and prohibits the re-use of a password. The system administrator can require users to change passwords when they next log in, and can set an expiration interval for passwords (see *Fig. 6*).

21 CFR 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.

In the Titrando system electronic signatures are implemented by using a combination of the user's unique login name and a password. The user must enter a user name and password every time to electronically sign a record. Continuity of sessions can be easily enforced through an option that automatically logs a user out if no system activity is detected for a period whose length is specified in advance by the system administrator. Signings always require all electronic signature components. Signings using only one electronic signature component are not possible.

Because the user name is unique for each individual, each person's signature combination is unique, and can only be used by its genuine owner. Of course, system users must not reveal their passwords to anyone else; attempted use of the signature by anyone other than the genuine owner would require collaboration of two or more individuals.

21 CFR 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 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.

As discussed under Sections 11.100 and 11.200, each person's signature combination is unique. The Titrando system facilitates the administration of password maintenance through controls such as minimum password length, password validity limit, and password re-use prevention (see *Fig. 6*). The system administrator can use these controls to force users to change their passwords at regular intervals to ensure new expressions of a specified minimum length. The system administrator can also disable any user account if necessary, e. g. because the corresponding identification card was lost.

Attempts to breach the security system can be thwarted through automatic account deactivation, which can be set to disable any account after a specified number of failed login attempts (see *Fig. 6*). Via e-mail a message can be sent to the system administrator automatically when a login attempt fails.

All security-related events (user configuration changes, successful and failed logins) are automatically tracked in the audit trail. The convenient audit trail viewer makes it easy for system administrators to see particular events of interest. Available viewing filters include time and date, user involved, event categories and actions.

How to configure the Titrando system to be compliant with 21 CFR Part 11

Setting the date, time and time difference to UTC

With **PC Control** the date and time will be taken directly from the operating system of your computer. If the computer clock is synchronized automatically to that of a designated network computer clock, this time will be taken. The change from Summer to Winter time and vice versa is made automatically. In order for the **Summer /Winter time** to be taken into account in the **Windows** time display you must activate the checkbox **Automatically adjust clock for daylight saving changes** under System settings in the menu Date/Time Properties under Time zone.

With **Touch Control** you should set the date and time as follows:

1. Open the dialog **System/System settings**.
2. Enter date and time as described in the Instructions for Use.

Time stamps should allow clear understanding of what **time zone** reference is used. Therefore the time can be documented together with the difference of the local time to UTC (Coordinated universal time).

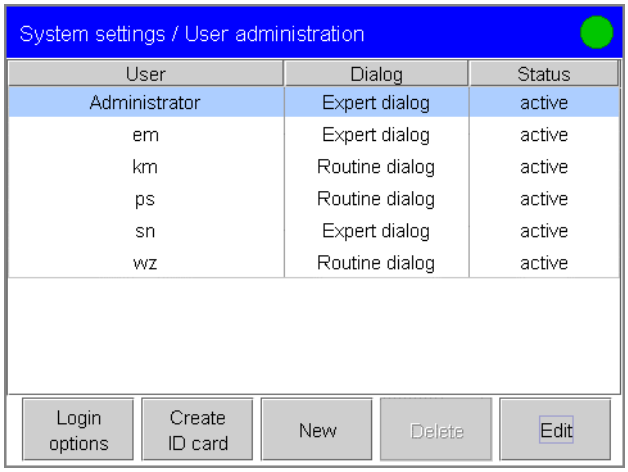
3. Open the dialog **System/System settings**.
4. In the **Local time - UTC** input field you should select the time difference to UTC (corresponds to the previously used GMT = Greenwich Mean Time). The PC Control software takes this time difference directly from the operating system of your computer. When the change to summer time or winter time takes place under Windows (see above) the difference to UTC will be adopted automatically.

The time zone is printed out in the report header together with the date and time.

User administration

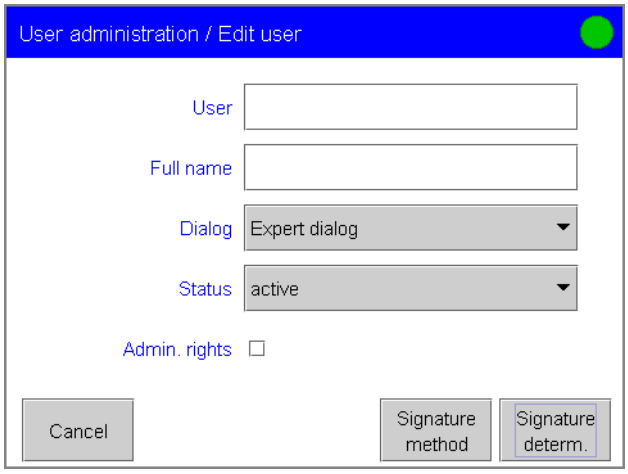
You can draw up a system-specific **list of users** who can operate the titration system.

5. Open the dialog **System settings/User administration**. When Login is switched on (see step 15), this dialog is only accessible to users with administrator rights.



The user list is initially empty.

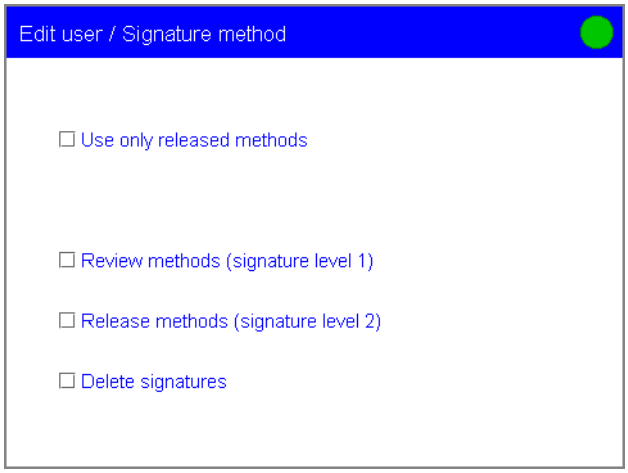
6. Use **[New]** to define all the users who are allowed to operate the system. The dialog in which the **user data** can be entered is opened automatically.



7. Enter an unambiguous identification under **User**, for example the in-house abbreviated form of the name or the personnel number. Each user name can only appear once in the list of users. Guidelines on how to name user accounts should be prepared before implementation.
8. Under **Full name**, enter the proper name of the user, i. e. given name and family name.
9. Select the **Dialog** in which the user is to operate the system. In **Expert dialog** all functions are accessible. For **Routine dialog** the system-specific routine dialog configuration is normally used (see step 34 ff). If each user is to have separately defined routine dialog settings then you can create an identification card for each user on which these settings are stored (see Instructions for Use). During login the dialog settings stored on the card will be loaded automatically.
10. The **user status** normally remains **active**. A user should be deactivated when, for example, he or she is absent for a long time or is no longer authorized to use the system.

This user can then no longer log into the system until the **active** status is reactivated by the administrator.

11. You should activate the **Administrator rights** checkbox for each user who is to have access to the user administration. You must ensure that at least two users have administrator rights so that one of them is always available. Keep the rights of access for a user with administrator rights in a safe place so that it is accessible in an emergency. A general policy for such emergencies should be elaborated.
12. Open the dialog **Signature method** and issue the rights for using and signing methods.

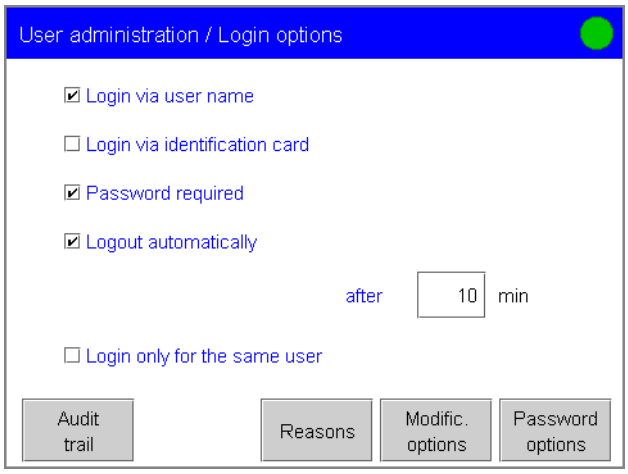


13. Open the dialog **Signature determination** and issue the rights for signing results (determinations).

Login options and Security policies

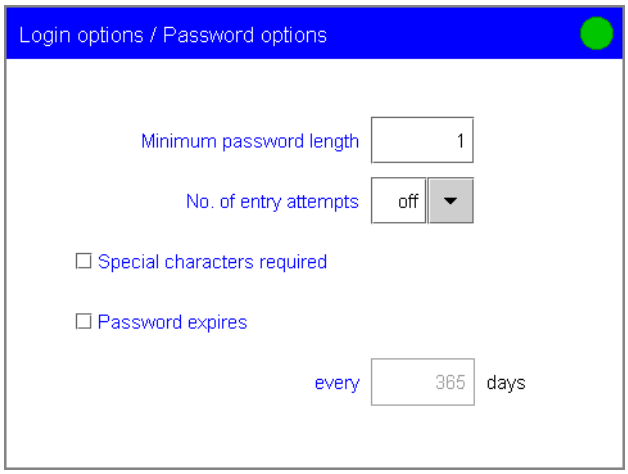
There are various ways of logging into the system: either the user name is requested or identification is carried out by using an identification card (see Instructions for Use). It is also possible to combine both versions.

14. Open the dialog **User administration/Login options**.



15. Activate the checkbox(es) for the **login option**(s) that you wish to use. If you select **Login via identification card** then you must create an identification card for each user (see Instructions for Use).

16. Activate the **Password required** checkbox. If this function is switched on then it is no longer possible to delete users from the list of users to avoid the reuse of user names; they can only be deactivated.
17. Activate the **Logout automatically** checkbox and enter the interval after which the log-out is to take place automatically. The delay time should be determined based on corporate requirements.
18. Open the dialog **Login options/Password options**.

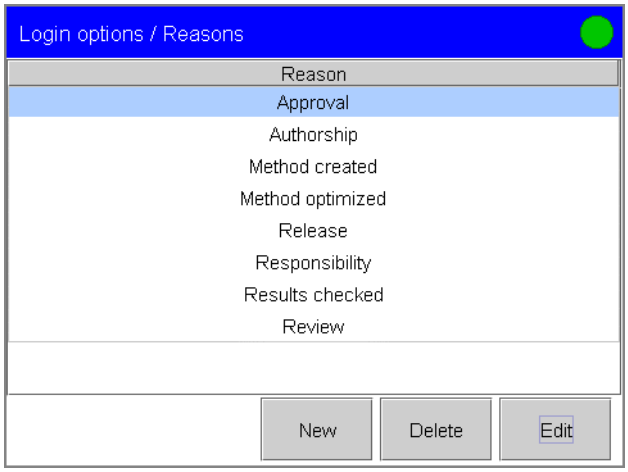


19. Enter the **Minimum password length**. Short passwords are a security risk and a minimum length of 6 characters is common practice. Very long passwords are not recommended because they are more difficult to remember and may be written down by users. It is recommended that a policy be prepared that discusses good password practices.
20. To prevent excessive attempts to access a user account, the maximum **No. of entry attempts** allowed for a login must be set. A maximum of 3 attempts is common practice. If the number of login attempts is exceeded, the user account is disabled. Until a system administrator reactivates the account, the user has no access to the system.
21. Activate the **Special characters required** checkbox. By the use of special characters in a password security is increased.
22. Activate the **Password expires** checkbox and enter a time after which the password expires. A period of 30 to 90 days is common practice. Note that a very short password expiry requires the user to frequently specify and remember a new password.

Definition of default strings for meanings (reasons)

Default strings for reasons allow the administrator to predefine various comments that can be selected from a drop-down list when **signing** methods or determinations or as reason for a modification. This feature allows the use of company specific expressions, minimizes typing and reduces typing errors.

23. Open the dialog **Login options/Reasons**.

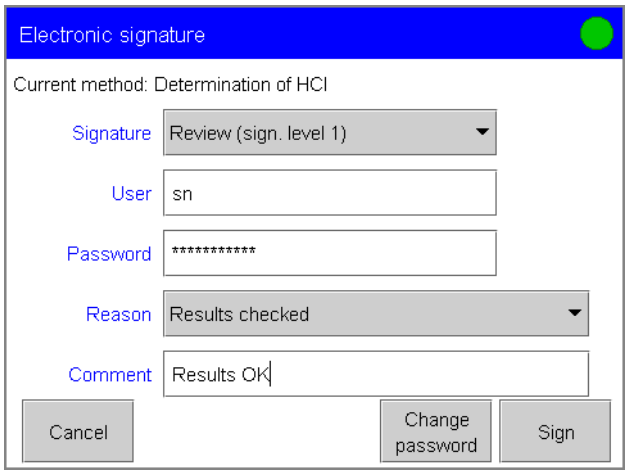


24. With **[New]**, **[Edit]** and **[Delete]** you can define your own list of default strings for reasons.

Sign methods and results (determinations)

A user can **sign methods and determinations** only if he has the relevant privileges (see step 12 and 13). Methods must be saved before the **[Sign]** button becomes active. The information associated with the signing (full name of the signer, date and time of signing and reason for signing) is stored in the electronic record.

25. For signing a method open the **Electronic signature** dialog from the dialog **Method options/Properties** with the **[Sign]** button. For signing a determination open the **Electronic signature** dialog from the dialog **More determination data/Properties** with the **[Sign]** button.

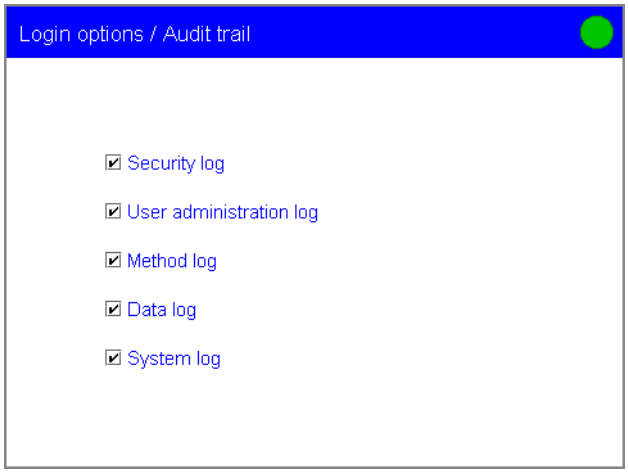


26. Under **Signature** select the level to which the signature is to be applied. If this is the first signature then only level 1 can be selected. If a signature for level 2 exists then only level 2 can be selected. Up to three signatures from different users are possible for each level.
27. Enter the **user** identification and **password** and select the **reason** for signing. A list of default strings for reasons can be defined as described in step 23 and 24. In addition to the reason you can also enter your own **comment**, which will be stored together with the signature.
28. With the **[Sign]** button all information for the electronic signature is stored with the method or determination.

Audit trail settings

The **audit trail** records, for each event, the type of the event, corresponding time and date, user name, category, action, and details about the action and the affected data object.

29. Open the dialog **Login options/Audit trail**.

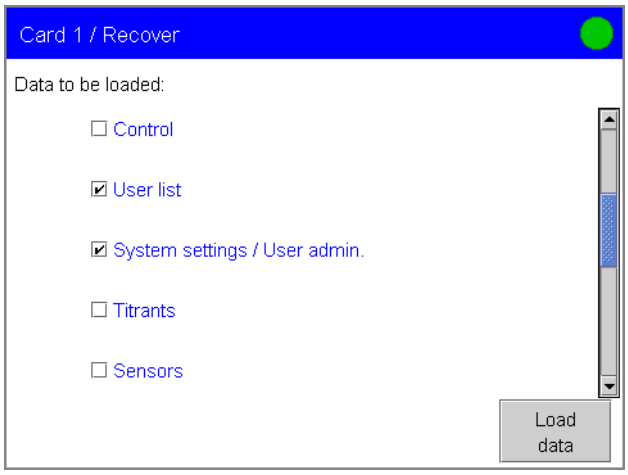


30. Activate all checkboxes. Thus all user actions are recorded in the audit rail.

Configuration of several Titrando systems

If several Titrando systems with identical user access configuration are to be installed, the user list, login options, password options and audit trail settings can be copied from one system to the others using the **Backup** and **Recover** functions.

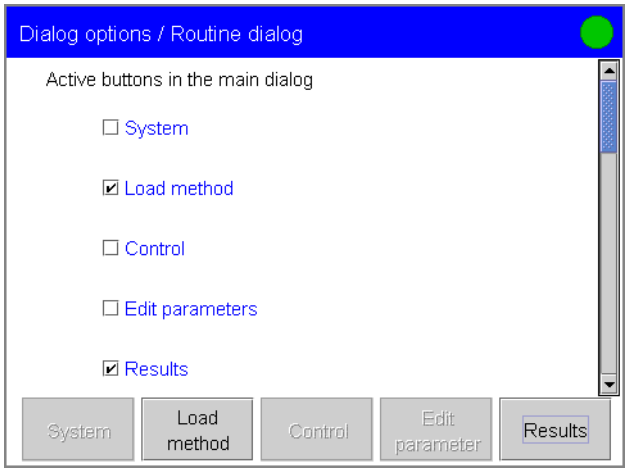
31. Set up the user administration for the first system as described in steps 5 to 24 and 29 to 30.
32. Make a backup from all data and settings on this system. For a detailed description of the backup function see the Instructions for Use. For PC Control use a removable storage medium or a network drive that can be accessed from all systems.
33. Recover the **User list** and **System settings/User administration** (all system settings including device-specific dialog configuration and dialog options for the list of commands and fixed keys, device-specific settings for the user administration (login options, password options and audit trail)).



Routine dialog configuration

Although not required for compliance with FDA 21 CFR Part 11, limiting the access to certain functions for routine users can help to simplify the work with the system and to monitor compliance. The advanced security system provided by the Titrando system supports two access levels in addition to the administrator level if **Login via user name** (see step 15) is used. If identification cards are used for login (see Instructions for Use) then the routine dialog settings can be stored user-specifically on the card.

34. To configure the dialog settings for routine users, open **Dialog options/Routine dialog**.



35. Deactivate the checkboxes for the functions that are to be disabled in routine dialog (see also Instructions for Use).

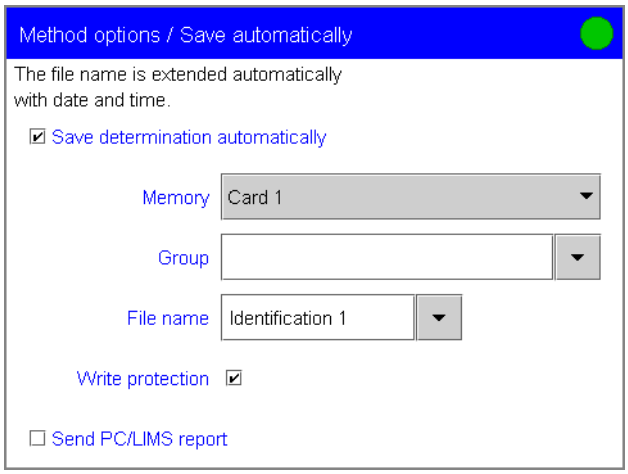
Like the user access configuration, the routine dialog settings can be copied from one system to another using the **Backup** and **Recover** functions.

Automatically saving the determination, sending a PC/LIMS report and a printed report

In order to generate **accurate and complete copies** of records in both human readable and electronic form (11.10 (b)), the original determination can be saved automatically at the end of a determination. At the same time, an electronic copy in form of a PC/LIMS report (formatted ASCII) can be sent and a paper report can be printed automatically.

In order to **save the original determination file** automatically, set the corresponding method parameters as follows (for details see Instructions for Use):

36. Open the dialog **Method options/Save automatically** and activate the **Save determination automatically** checkbox.



37. Under **Memory**, select the memory location in which the determinations are to be stored. Determinations can only be stored on **Card 1** or **Card 2** or a shared file system. Enter the **Group** in which the determinations are to be stored. Choose **Identification 1** as **File name**. The file name will be made up of the first 16 characters which you have entered for **Identification 1** and the **determination time** (date and time): Identification 1-YYYYMMDD-hhmmss. The date and time will be appended so that the file name is always unambiguous.
38. Activate the checkbox **Write protection**.

In order to **save a PC/LIMS report** automatically, set up the system configuration and the corresponding method parameters as follows (for details see Instructions for Use):

39. Open the dialog **System/Device manager**.
40. a. 847 USB Lab Link connected: Select the device and press **[Edit]**.

    b. No Lab Link connected: A virtual Lab Link must be configured. For that, add the device "825 Lab Link" to the device manager and open its configuration dialog with **[Edit]**.
41. Press **[PC/LIMS Report]** and activate the **Save PC/LIMS Report** checkbox (corresponds to default setting).
42. Select the **memory** in which the files are to be stored and the **group**.

Set the corresponding **method parameters** as follows:

43. Open the dialog **Method options/Save automatically** and activate the **Send PC/LIMS report** checkbox.

In order to **print out a result report** containing the determination data and/or **save the report in PDF format** (PC Control only) automatically, set the corresponding method parameters as follows (for details see Instructions for Use):

44. **PC Control**: Open the menu **File/Printer**. Select the **printer** for report prints. Activate the **Generate PDF report** checkbox if a PDF file should be generated. Activate the **Print report additionally** checkbox if the report should be printed on the printer selected above at the same time.
45. Open the list of method commands and insert a **REPORT** command at the end of the list. The report sequence should contain of the following reports: Result report (all options switched on), list of measuring points, Calculations, Used devices ad Parameters full.