Metrohm
Ion analysis

04.2017

Using the Touch Control family to comply with 21 CFR Part 11

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

The Code of Federal Regulations Title 21 Part 11 of the U.S. Food and Drug Administration, known as 21 CFR Part 11, defines the requirements for using electronic records and electronic signatures (ERES). These regulations, which became effective on August 20, 1997, specify in general how the system components, controls and procedures have to be designed to ensure the reliability and authenticity of electronically saved records. It can be accessed at following link «https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11».

Achieving and maintaining full compliance with these regulations requires standard operating procedures (SOPs) that support and complement the functionality of the electronic systems. This means that no product alone can ensure compliance. However, products with integrated functions supporting 21 CFR Part 11 requirements are mandatory for achieving and maintaining full compliance with the regulations.

This document describes in detail how the Touch Control family devices (900 Touch Control, 915 KF Ti-Touch, 916 Ti-Touch and 917 Coulometer) comply with these requirements. In the following text the 4 devices will be referred to as 'Touch Control devices'.

Each relevant section of 21 CFR Part 11 is listed together with the corresponding feature of the Touch Control devices' software.

General Provisions

> § 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.
>
> (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.

The electronic records of the Touch Control family 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 Touch Control device shipment, Metrohm provides detailed user documentation and certificates of software validation. All documents and source code are available for inspection by FDA at Metrohm International Headquarters.

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

- Declaration of conformity for each Touch Control device. All certificates are included on the delivered USB stick in Portable Document Format (PDF).
- Installation Qualification (IQ) records (the software automatically performs software 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 (OQ) records for the systems and methodologies used (Metrohm can provide validation documentation, which helps to perform the OQ).
- Site-specific standard operating procedures for security and records management.

§ 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.

Touch Control devices allow the export of copies of the electronic records – i.e. the determinations – either as PC/LIMS report in "ISO 8859-1", "UTF-8" format, or as PDF for submission to agency units, in accordance with FDA guidelines. The PC/LIMS report files faithfully preserve the contents of the analysis data. The PDF report files preserve the contents and formatting of the printed reports and can be protected against any modification. The PC/LIMS and/or the PDF reports should be archived together with the determination file. The clear assignment of the PC/LIMS report and the PDF reports to the corresponding determination file is guaranteed by the corresponding file name containing the identification, date and time of the determination. PC/LIMS and PDF reports of signed determinations contain all information about the electronic signatures (full name of the user, date, time and meaning of the signature).

§ 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 Touch Control devices are implemented as a closed system. Users accessing the system include system administrators, who set up and maintain user accounts, and any other users (e.g. laboratory managers, laboratory technicians).

Digital signatures are implemented in the Touch Control devices as described in sections *§ 11.50*, *§ 11.70*, *§ 11.100*, *§ 11.200*, and *§ 11.300*.

With respect to 21 CFR Part 11, the primary electronic records in Touch Control devices are the original records (the determinations), which are encrypted and provided with a checksum. Each record contains all of the information pertaining to the analysis of a sample and the following items:

- Sample information (sample IDs, sample size, sample size unit)
- Method information (method name, method version, method status, method sequence with all method parameters)

- Raw data and results (endpoints and other raw data, measuring point list, titrant data, sensor data, all variables, used devices and calculated results)

The audit trail documents all user entries and actions regarding changes in the security settings, in the user administration, method, data and system modifications, as described under section *§ 11.10* of this document.

Touch Control devices can also generate backup files of all system data for data recovery and/or archiving purposes. Contents of backup files cannot be accessed by other means than the Touch Control devices. The audit trail keeps track of all backup and restore operations.

Electronic Records

> § 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.
>
> (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.

The validation of analytical systems generally includes an IQ and an OQ. Metrohm offers a wide range of validation services ranging from IQ/OQ on-site tests performed by Metrohm service technicians up to automated routines built into the software (see section *§ 11.1*). Method templates for system validation are delivered with the system on a USB stick. 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)*) documents all changes made to the data objects produced with the application.

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

The Touch Control devices provide all the necessary functions for locating and viewing the electronic records on the system. Complete and accurate copies of the electronic records (i.e. the determinations) can be generated as PC/LIMS report in "ISO 8859-1", "UTF-8" format or as PDF report for submission to agency units. The automatic output at the end of a determination can be enforced using specific settings in the method options. Furthermore, determination data can be printed out as a configurable report. All electronic and paper copies can be unambiguously assigned to the corresponding determination file by the corresponding file name/determination name, which contains the sample identification, date and time of the determination (see also section *§ 11.2*)

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

> § 11.10 CONTROLS FOR CLOSED SYSTEMS
>
> (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

The Touch Control devices facilitate long-term record storage by an external archiving system through its built-in export tool. Each determination includes sample information (sample ID, sample size and sample size unit), method information (method name, method version, method status, method sequence with all method parameters), raw data and results. Those data can be exported manually or automatically as original determination file (*.mdtm), as PC/LIMS report (in "ISO 8859-1" or "UTF-8" format) or as PDF. The determination files (*.mdtm) are encoded and provided with a checksum to protect them from unwanted or improper alteration.

§ 11.10 CONTROLS FOR CLOSED SYSTEMS

(d) Limiting system access to authorized individuals.

The system provides a login system with three internal access levels (Administrator, Expert, or Routine User).

The person responsible for the system – the administrator – must ensure that access rights are granted to authorized persons only.

The access rights for the routine users can be defined in the following dialog (please refer to *Fig. 1*). Individual access rights can be assigned to routine users when using identification profiles.

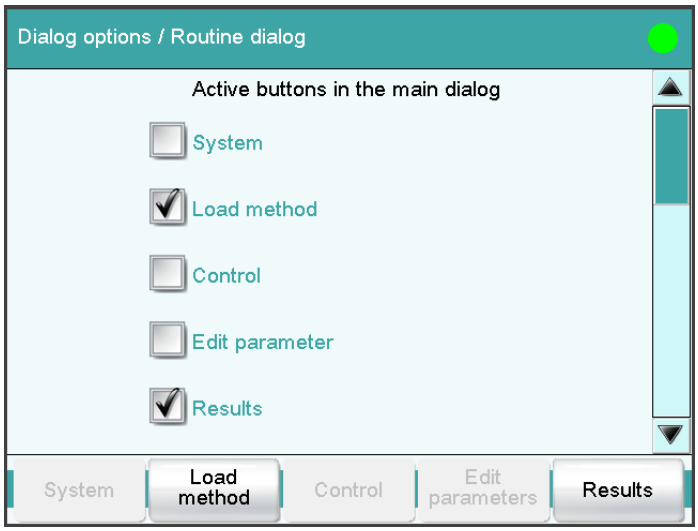


Fig. 1: Definition of active buttons in routine dialog

When the user logs in via identification profile, his specific dialog settings are automatically loaded. The same identification profile can be used on several Touch Control devices, where the user is registered. The administrator can copy the user configuration from one Touch Control device to another one – of the same type – using the backup function.

The security system of the Touch Control device provides the user administration settings most often requested by system administrators.

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

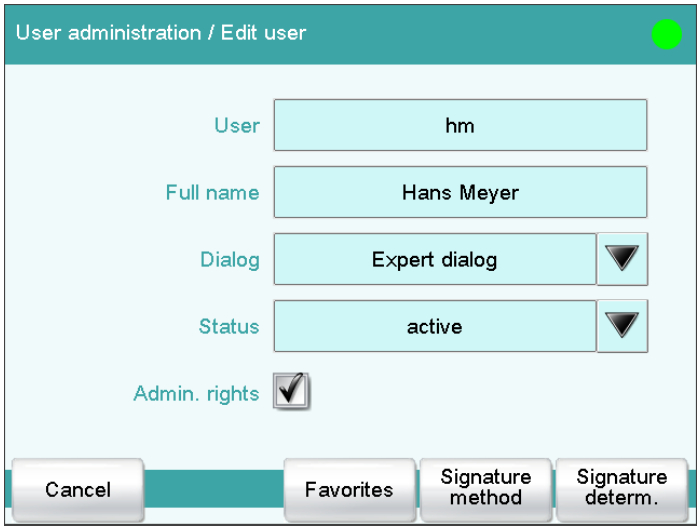


Fig. 2: User administration, user data input

- Automatic logout after a defined period of inactivity can be set. Furthermore, there is the possibility to enforce login only for the same user.

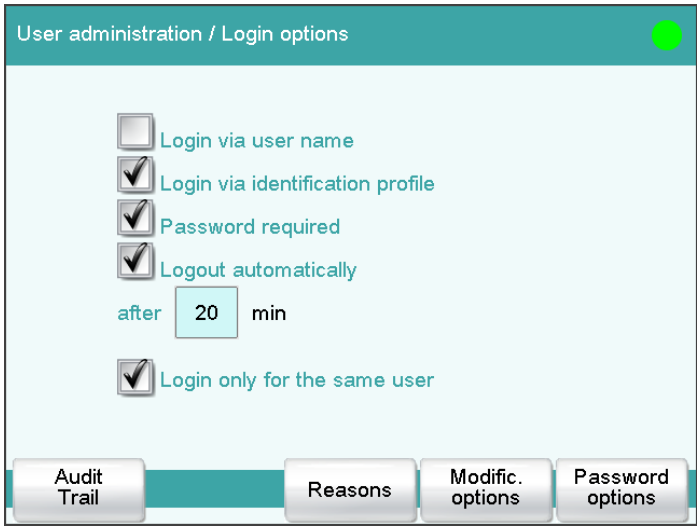


Fig. 3: User administration, settings for the login

- Password controls can be enforced: minimum password length, maximal number of entry attempts, request for special characters in the password and password expiration. The password can be changed by the user at any time. It is never visible as plain text, thus only the user knows her or his password.
- The user account is disabled automatically after a defined number of unsuccessful login attempts. In order to be able to login again, the user (account) must be set back to the status "active" by a system administrator.

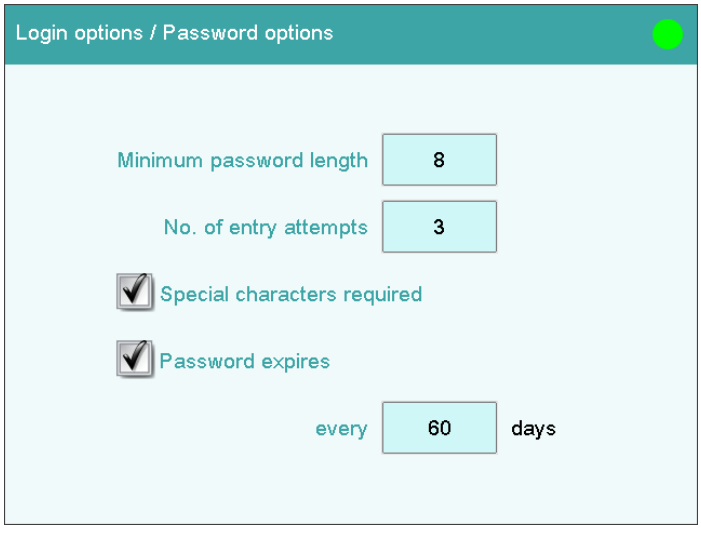


Fig. 4: Settings for the password as part of the login options

- User logins are automatically recorded in the audit trail.

§ 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.

If the audit trail has been enabled by the administrator, all relevant operator entries are recorded in an automatically generated audit trail. Each audit trail entry consists of date/time (according to ISO 8601), user identification, event category (i.e. warning, information), action and details (see *Fig. 5*). The audit trail is stored internally and can be backed up to a USB stick.

According to the settings in the dialog "Login options / Audit Trail", the audit trail can document all user entries and actions regarding changes in the security settings, in the user administration, method and data modifications, and all other data system modifications.

If a change is made to an electronic record, the system overwrites the information in the internal memory. If data is altered and then saved, a new version will be created automatically. However, this process overwrites the previous version.

Organizational safeguards have to be implemented to ensure that, prior to the any modification of the electronic record, the file (containing the original electronic record) is stored and archived with an unambiguous file name.

Changes to electronic records create new entries in the audit trail, i.e. previously recorded entries are not overwritten. Audit trail entries cannot be modified – they can be examined using the Audit Trail Viewer software which is delivered on a USB stick (along with firmware and documents).

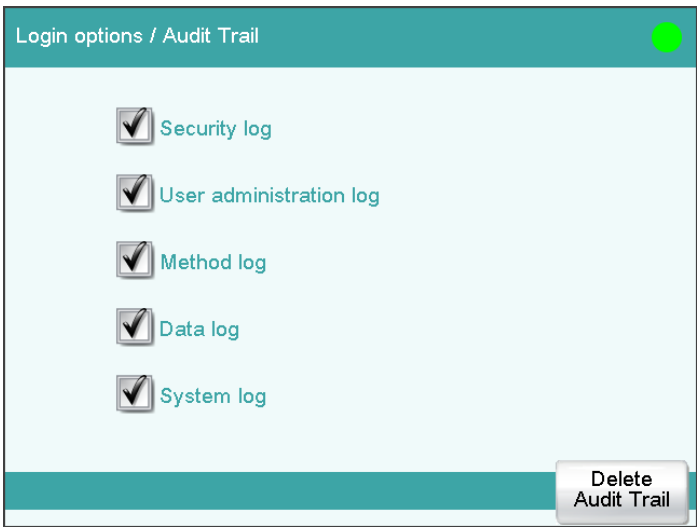


Fig. 5: Audit trail settings as part of the login options

For all changes the old and the new value are recorded.

The user can be forced to enter a reason for changes made to methods and results (recalculation of determinations) in order to ensure that their intentions are clearly documented (see *Fig. 8*).

File Filter Info

No.		Date	User	Category	Action	Details
1	⚠	2017-05-08 19:31:11+02...	hm	Admin	Delete Audit Trail	Hans Meyer
2	⚠	2017-05-08 19:31:17+02...	hm	Admin	Change Audit T. opt.	Security log off --> on
3	⚠	2017-05-08 19:31:17+02...	hm	Admin	Change Audit T. opt.	User administration log off --> on
4	⚠	2017-05-08 19:31:17+02...	hm	Admin	Change Audit T. opt.	Method log off --> on
5	⚠	2017-05-08 19:31:17+02...	hm	Admin	Change Audit T. opt.	Data log off --> on
6	⚠	2017-05-08 19:31:17+02...	hm	Admin	Change Audit T. opt.	System log off --> on
7	🖫	2017-05-08 19:31:26+02...	hm	Security	Logout	Hans Meyer
8	🖫	2017-05-08 19:31:50+02...	Johnson	Security	Log in	Peter Johnson
9	🖫	2017-05-08 19:31:55+02...	Johnson	Method	New	01 Dynamic Titration pH
10	🖫	2017-05-08 19:32:02+02...	Johnson	Method	Edit	New method V0 01 DET pH Dosing device 2
11	🖫	2017-05-08 19:32:02+02...	Johnson	Method	Edit	New method V0 01 DET pH Titrant not defined
12	🖫	2017-05-08 19:32:02+02...	Johnson	Method	Edit	New method V0 01 DET pH Titrant
13	🖫	2017-05-08 19:32:11+02...	Johnson	Method	Edit	New method V0 01 DET pH Stop volume 5 mL
14	⚠	2017-05-08 19:32:20+02...	Johnson	System	Message	020-905 Group name Yes/OK
15	🖫	2017-05-08 19:32:27+02...	Johnson	Method	Edit	New method V0 Options Save determination automatically on
16	🖫	2017-05-08 19:32:27+02...	Johnson	Method	Edit	New method V0 Options Group TIT
17	🖫	2017-05-08 19:32:42+02...	Johnson	Method	Save	Acid V1 Internal memory
18	🖫	2017-05-08 19:32:51+02...	Johnson	Method	Load result template	Acid V1 Content (mmol/L)
19	🖫	2017-05-08 19:33:07+02...	Johnson	Method	Edit	Acid V1 02 CALC Calc. formula EP1*0.1*1000*TITER/C00
20	🖫	2017-05-08 19:33:13+02...	Johnson	Method	Save	Acid V2 Internal memory
21	🖫	2017-05-08 19:33:51+02...	Johnson	Security	Sign	Acid V2 Chang Yang Chang Review (signature level 1) Approval Method ok
22	🖫	2017-05-08 19:34:12+02...	Johnson	Security	Sign	Acid V2 Meyer Hans Meyer Signature Release
23	🖫	2017-05-08 19:34:37+02...	Johnson	Data	Edit sample data	Identification 1 --> Sample 1
24	🖫	2017-05-08 19:34:37+02...	Johnson	Data	Edit sample data	Sample size 1.0 --> 2.550
25	🖫	2017-05-08 19:34:37+02...	Johnson	Data	Edit sample data	Sample size unit g --> mL
26	🖫	2017-05-08 19:34:37+02...	Johnson	Method	Start	Start key pressed
27	🖫	2017-05-08 19:34:38+02...	Johnson	Method	Start	Acid V2 Sample 1 2.550 mL
28	⛔	2017-05-08 19:34:46+02...	Johnson	System	Message	010-119 Check exchange/dosing unit Yes/OK
29	⚠	2017-05-08 19:34:52+02...	Johnson	System	Message	010-122 Prepare dosing device Yes/OK
30	🖫	2017-05-08 19:37:09+02...	Johnson	Method	Stop	Acid V2
31	🖫	2017-05-08 19:37:09+02...	Johnson	Data	Save determination	Sample_1-20170508-193452 V1 External memory 1
32	🖫	2017-05-08 19:37:22+02...	Johnson	Data	Edit sample data	Sample size 2.550 --> 2.500
33	⚠	2017-05-08 19:37:23+02...	Johnson	Data	Recalculate	
34	🖫	2017-05-08 19:37:28+02...	Johnson	Security	Logout	Peter Johnson
35	⛔	2017-05-08 19:37:45+02...	Meyer	Security	Login message	Wrong password
36	⚠	2017-05-08 19:37:47+02...	Johnson	System	Message	002-102 Wrong password Yes/OK
37	🖫	2017-05-08 19:37:51+02...	Meyer	Security	Log in	Hans Meyer
38	🖫	2017-05-08 19:37:57+02...	Meyer	Method	Start	Start key pressed
39	🖫	2017-05-08 19:37:58+02...	Meyer	Method	Start	Acid V2 Sample 1 2.500 mL
40	⚠	2017-05-08 19:38:08+02...	Meyer	Method	Manual stop	Acid V2
41	🖫	2017-05-08 19:38:08+02...	Meyer	Data	Save determination	Sample_1-20170508-193758 V1 External memory 1

Fig. 6: The audit trail documents all relevant changes to the data objects

Fig. 7: Request settings for modification

> **§ 11.10 CONTROLS FOR CLOSED SYSTEMS**
>
> (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

Checks are carried out by the system when instruments are configured and also each time a determination is started. For example, a check is performed whether all necessary devices are present.

Metrohm delivers many ready-to-use templates, e.g. for methods and results. The sequence of an analysis is defined in the method and cannot be altered during the analysis.

Maintaining the sequence is supported by using the sample assignment table (see *Fig. 8*) or the automatic sample data request. Only the functions to be carried out are accessible.

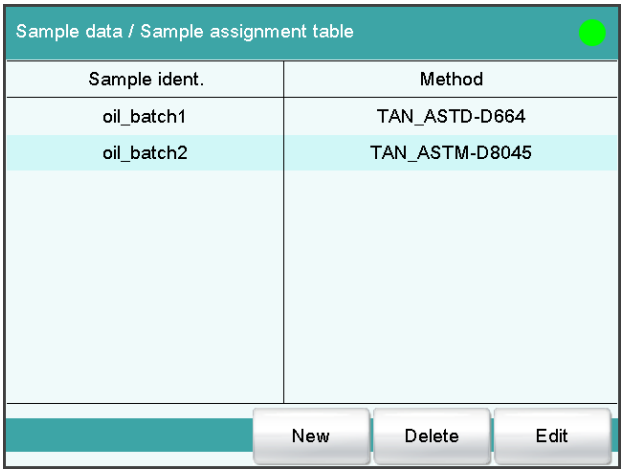


Fig. 8: List of sample identifications and their method

§ 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.

The person responsible for the system (the administrator) must ensure that the SOPs of the operator are followed and that access rights are granted to authorized persons only. The administrator function can be clearly separated from user roles, please refer to ***§ 11.10 (d)***.

Methods and determinations can be signed and released electronically. There are two signature levels. The system enforces that the user reviewing the electronic record (level 1 signature) is not the same as the one releasing it (level 2 signature).

§ 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.

Metrohm devices (control devices and auxiliary equipment) are automatically recognized and configured, their validity is checked and they are included in the list of the devices configured in the system.

Non-Metrohm USB instruments – e.g. printers, barcode scanners and keyboards – are recognized, their validity is checked, but they must be configured. The vendor ID is automatically read off and inserted in the list of devices.

The Touch Control device records specific information about devices included in the device manager (hardware configuration, serial numbers, etc.).

Qualification of the connected instruments is carried out as part of the system validation for which the operator is solely responsible.

§ 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 required by ISO 9001.

The operator is solely responsible for training users and the support staff at his site.

Metrohm offers standard training courses for all application fields, but individual training courses can be arranged separately.

§ 11.10 CONTROLS FOR CLOSED SYSTEMS

(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.

If an electronic signature is used, then the operator must have a policy in place in which the equality of handwritten and electronic signatures is made clear.

§ 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 system has a comprehensive, context-sensitive online help that always provides detailed information about the functions in use.

Metrohm supplies user documentation in electronic form together with the firmware on a USB stick. The documentation is unambiguously assigned to a particular software version, as release notes are, too.

The operator is responsible for the distribution of paper-based documentation. The operator must also maintain records about documentation and system changes – e.g. in a device logbook.

§ 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).

In the user administration, the administrator can grant user-specific rights to apply electronic signatures to methods and determinations (see *Fig. 11*).

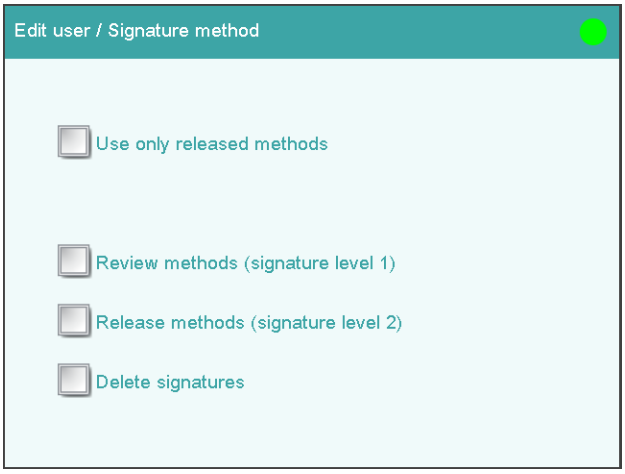


Fig. 9: User settings for electronic records (methods)

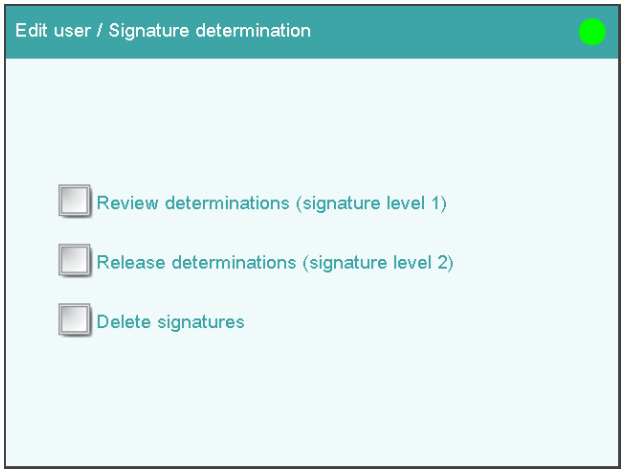


Fig. 10: User settings for electronic records (determinations)

Applying electronic signatures to methods and determinations is a simple and straightforward process. In the "Electronic signature" dialog, the operator selects the signature level (“Review (signature level 1)” or ”Release (signature level 2)”), enters his user identification and password, selects a reason for signing from a predefined list and possibly enters an additional comment (see *Fig. 11*).

By tapping on the "Sign" button, the record is signed and the information associated with the signature is stored. Full signature data are shown on the display (see *Fig. 12*) and on printouts.

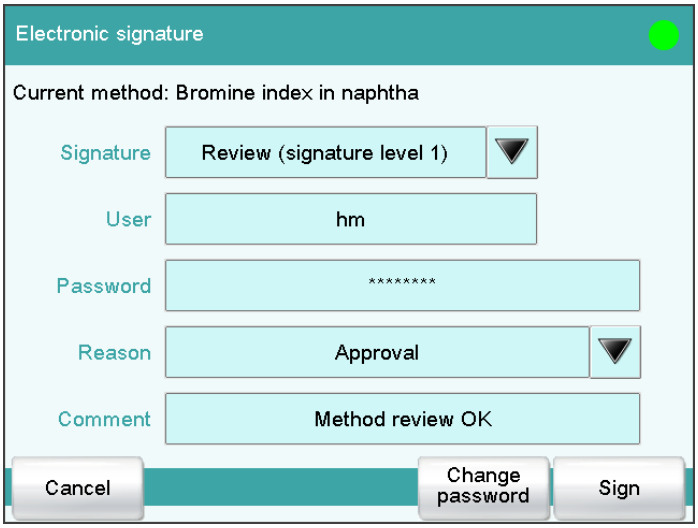


Fig. 11:"Electronic signature" dialog

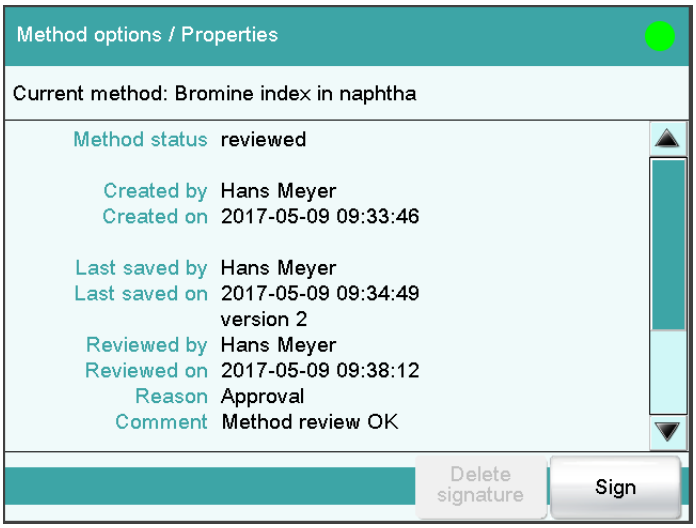


Fig. 12:Method properties

§ 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.

The signature is securely linked to the respective method or determination. Electronic signature data are stored as an integral part of signed-off records in such a way that they cannot be deleted, copied, or otherwise transferred by ordinary means.

User information is completely integrated in the signature. When displaying the signature, this information is always readable as plain text.

§ 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.

Each user gets a unique identification. The operator is solely in charge to ensure that identifications are not shared by many individuals.

§ 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.

Electronic signatures are implemented by using a combination of user's identification and password.

Both components of the electronic signature (user identification and password) are always required at each signing, independently if signings are executed during a continuous or a non-continuous session.

The operator solely is in charge to ensure that identifications are not shared by many individuals.

Nobody has access to the electronic signature data by ordinary means; an attempt to falsify an electronic signature requires the collaboration of at least two individuals.

§ 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.

As discussed in Sections *§ 11.100* and *§ 11.200*, each individual's electronic signature is unique.

The system ensures that each user identification code is used only once within the system and therefore each combination of identification code and password can also exist only once.

The Touch Control devices facilitate the administration of password maintenance through controls.

The use of unambiguous identification codes (e.g. personnel number or initials) is recommended for all systems throughout the whole organization. It is suggested to define SOPs for the whole organization for the creation of user accounts and the use of passwords (length, period of validity).

The system administrator can use these controls to force users to change their passwords at regular intervals to ensure new passwords of a specified minimum length. The administrator can also disable any user account, if necessary, e.g. because the corresponding identification profile was lost.

The operator is solely responsible for checking the identification codes periodically. This can be supported by a system function which allows the administrator to print out a list of all the registered users.

The validity period of the password can be defined by the administrator – values between 30 and 90 days are common. After this period has passed, the user is forced to change his/her password. The system maintains the password history and prevents the user from reusing a password.

If an individual leaves or is transferred elsewhere, her/his user account can be disabled in the user administration by the administrator by setting the status to "inactive". The same procedure applies if an identification code or a password is potentially compromised or lost.

All security-related events (user configuration changes, successful and failed login attempts) can be automatically tracked in the audit trail.

At the last but one allowed login attempt the user gets a warning that she/he has just one last attempt to enter the correct password. If the last login attempt is not successful, a message is displayed and the user account gets blocked – the user can no longer log in. The corresponding message can be sent to the management by email.

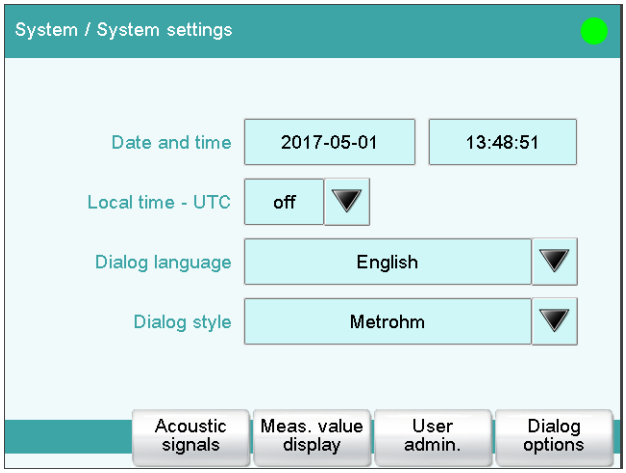
The procedure to inform the security manager has to be implemented by the operator.

How to configure the Touch Control devices to be compliant with 21 CFR Part 11

Setting the date, time and time zone

Date and time should be set as follows:

1. Open the dialog **System / System settings**.



2. Enter date and time as described in the manual.

Time stamps should allow clear understanding of which **time zone** reference is used. Therefore, the time can be documented together with the difference of the local time to UTC.

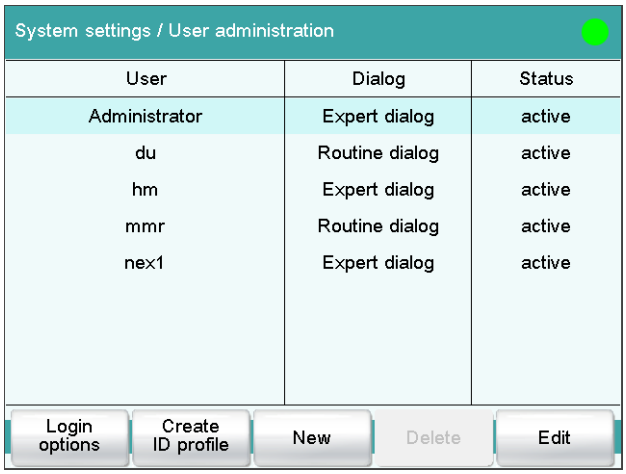
3. In the **Local time - UTC** input field, the time difference to UTC (Coordinated Universal) should be selected.

Date/time is always indicated with the time zone.

User administration

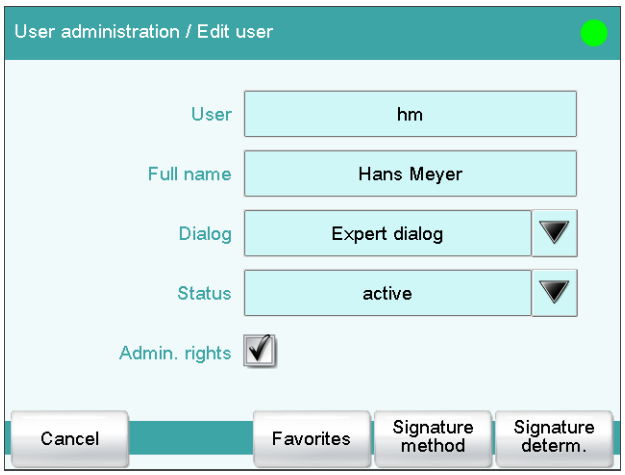
A system-specific **list of users** who can operate the titration system can be drawn up.

4. Open the dialog **System settings / User administration**. (When login is switched on, this dialog is accessible to users with administrator rights only; please refer to *steps 10* and *14*).

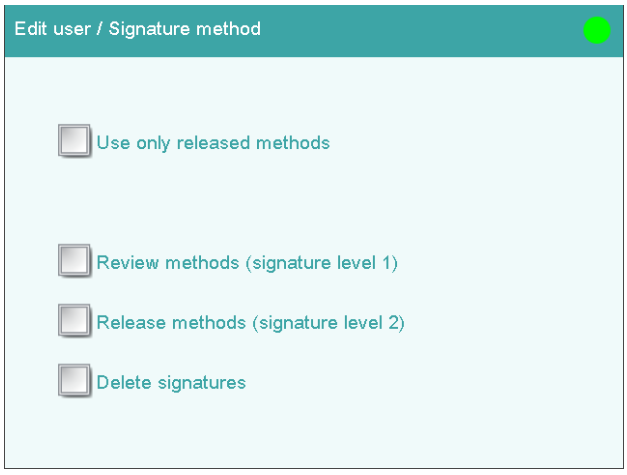


In the user administration the user list is initially empty.

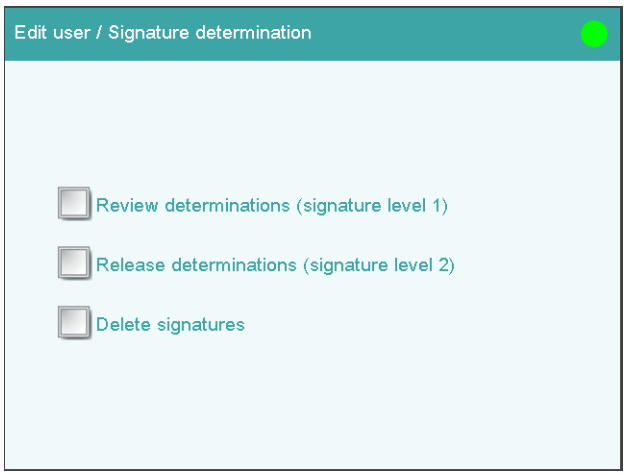
5. With **[New]** it is possible to define the users who are allowed to operate the system. The dialog **User administration / Edit user** in which the user data can be entered is opened automatically.



6. Enter an unambiguous identification in the field **User**, for example the in-house abbreviated form of the name or the personnel number. Each user identification can only appear once in the user list. Guidelines on how to name user accounts should be prepared before implementation.
7. In the field **Full name** the proper name of the user should be entered, i.e. first and family name.
8. Select the **Dialog** type 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 (please refer to *step 34 ff.*). If each user must have dedicated routine dialog settings, then an identification profile can be created for each user in which these settings are stored (please refer to the manual). During the login procedure the dialog settings – stored on the identification profile – will be loaded automatically.
9. The default **Status** of a user is defined as **active**. The status of a user should be set **inactive** when, for example, she/he is absent for a longer period of time, or is no longer authorized to use the system. A user with status **inactive** can no longer log in to the system until her/his status is set back to **active** by an administrator.
10. 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.
11. By pressing the button **Signature method** the dialog **Edit user / Signature method** is opened. In this dialog the settings for signing methods and deleting methods' signatures can be defined.



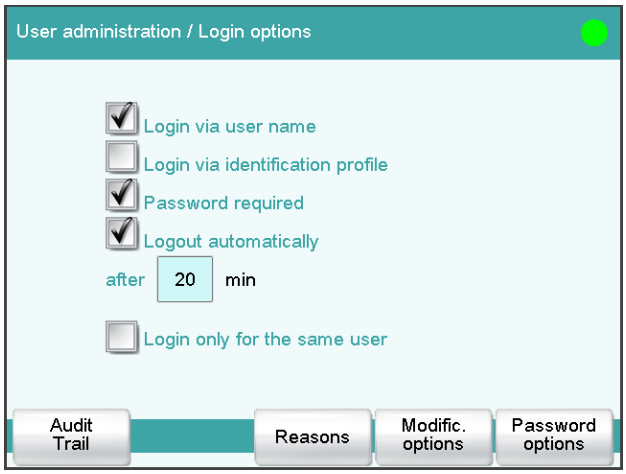
12. From the dialog **User administration / Edit user** the dialog **Edit user / Signature determination** can be reached by tapping the button **Signature determ.** In this dialog you can assign the rights for signing determinations, and deleting determinations' signatures.



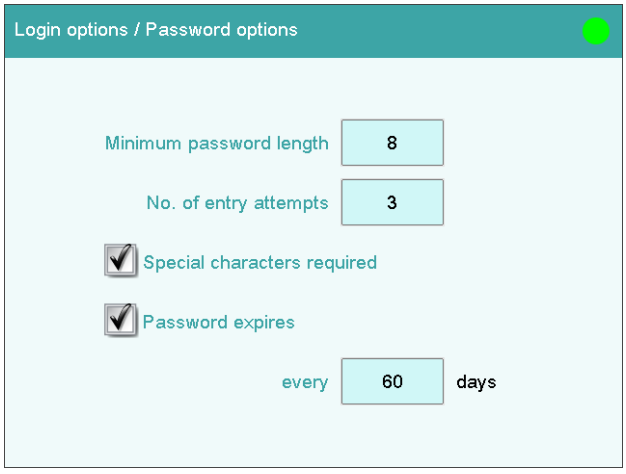
Login options and security policies

There are various ways of logging into the system: either the user name is requested or identification is carried out by using an identification profile (please refer to the manual). It is also possible to combine both versions.

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



14. Activate the checkbox(es) for the login option(s) to be used. If selecting **Login via identification profile,** an identification profile for each user must be created (please refer to the manual).
15. **Password required** checkbox: If this option is activated, then it is no longer possible to delete users from the user list in order to avoid the reuse of user names. Users can only be set inactive (by an administrator).
16. Activate the **Logout automatically** checkbox and enter the period of time after which the user has to be automatically logged out. The time should be determined based on corporate policies.
17. **Login only for the same user** checkbox: If this option is activated, then only the same user can log in again after she/he has logged out. However, users with administrator rights can log in at any time.
18. Open the dialog **Login options / Password options**.



19. Enter the **Minimum password length**. Short passwords are a security risk – a minimum password length of 6 characters is common practice. Very long passwords are not recommended because they are more difficult to remember and may force the user to write it down. It is recommended to prepare a policy that describes good password practices.
20. To limit the number of 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

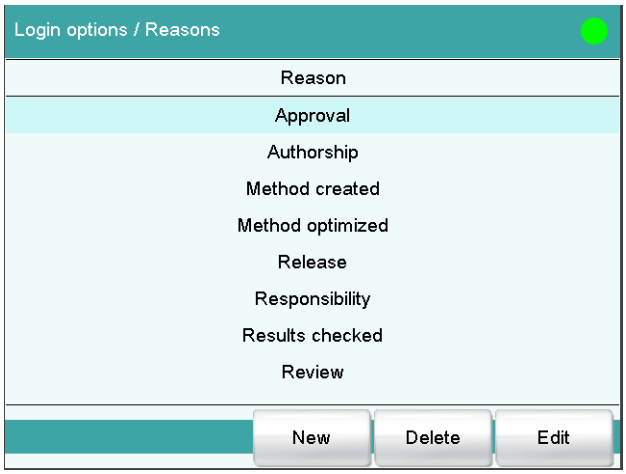
of login attempts is exceeded, the user account is disabled. Unless an administrator sets the account to the **active** status again, the user has no access to the system.

21. Activate the **Special characters required** checkbox. The use of special characters in a password increases its strength.
22. Activate the **Password expires** checkbox and enter the number of days after which the password expires. A period of 30 to 90 days is common practice. Note that a very short password duration requires the user to frequently change and remember a new password.

Definition of default reasons for data modifications

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 their modification. This feature allows the use of company-specific expressions, minimizing typing errors.

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

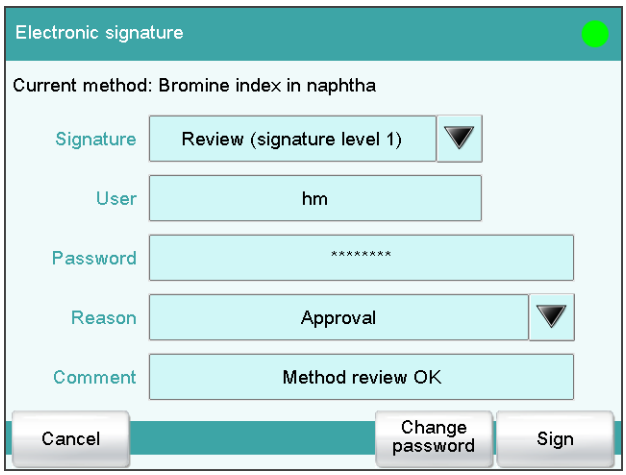


24. With **[New]**, **[Delete]** and **[Edit]** a custom list of default reasons can be defined.

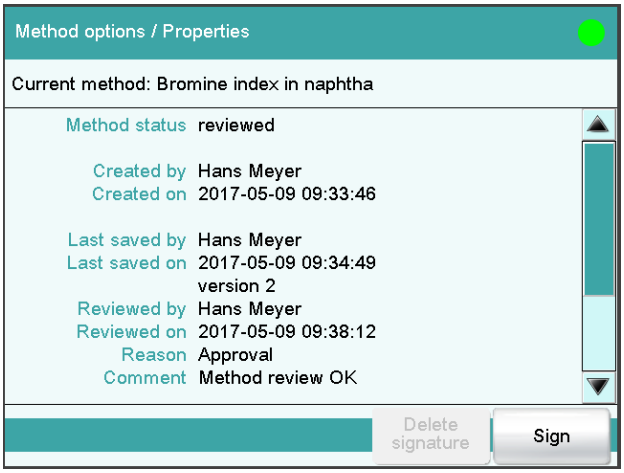
Signing methods and determinations

A user can **sign methods and determinations** only if he or she has been granted the rights to do it (please refer to steps 11 and 12). Methods must be saved before the **[Sign]** button becomes active (in the dialog **Method options / Properties**). The information associated with the signing (full name of the signer, last saved, date and time of signing, reason for signing and comment) is saved in the electronic record.

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



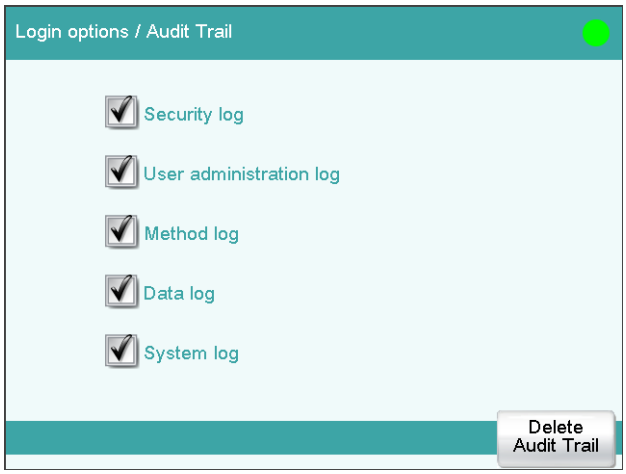
26. In the field **Signature** select the level of the signature to be applied. If this is the first signature, only level 1 can be selected. If a signature for level 2 already exists, then only a signature level 2 can be selected. Up to three signatures from different users are possible for each level.
27. Enter the **User** identification and **Password** and select the **Reason** for signing (the list of default reasons is described in steps 22 and 23). In addition to the reason a **comment** can be entered, which will be recorded together with the electronic signature.
28. By pressing the **[Sign]** button all information about the electronic signature is recorded along with the method or determination.



Audit Trail settings

In the dialog **Login options / Audit trail,** the type of entries in the **Audit Trail** can be defined.

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

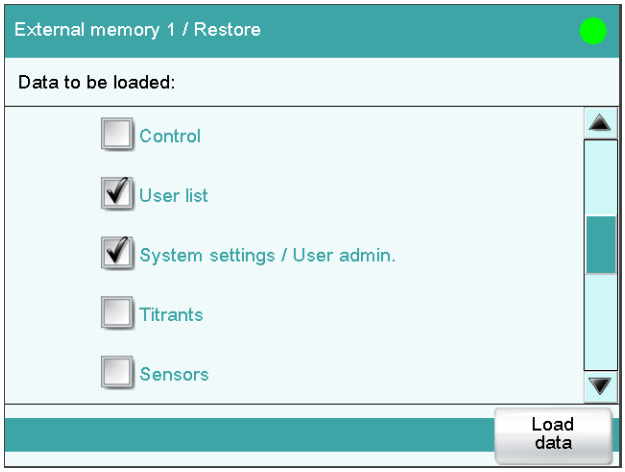


30. By activating all checkboxes, all defined user actions are recorded in the audit trail.

Configuration of several Touch Controls

If several Touch Controls devices of the same type and with identical user administration are to be installed, the user list, login and password options, and audit trail settings can be copied from one system to the other using the **Backup** and **Restore** functions.

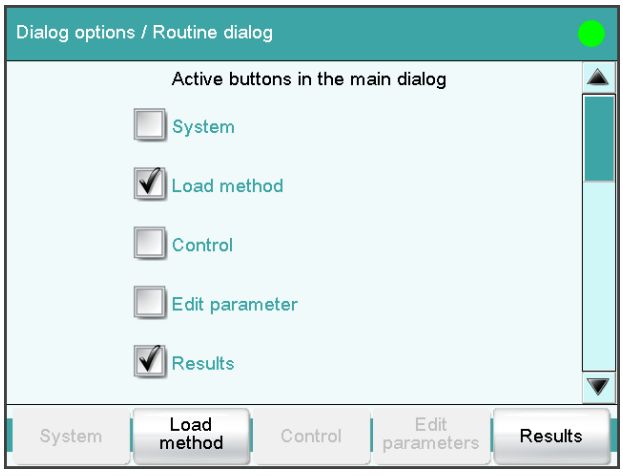
31. Set up the user administration for the first system as described in steps 4 to 23 and 28 to 29.
32. Make a backup of all data and settings of this system. For a detailed description of the backup function please refer to the manual.
33. Recover the **User list** and **System settings / User administration**: 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 and password options, and audit trail).



Routine dialog configuration

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 Touch Control devices supports two access levels in addition to the administrator level if **Login via user name** is used (please refer to step 14). If identification profiles are used for login (please refer to the manual), then the routine dialog settings can be stored user-specifically in the profile.

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



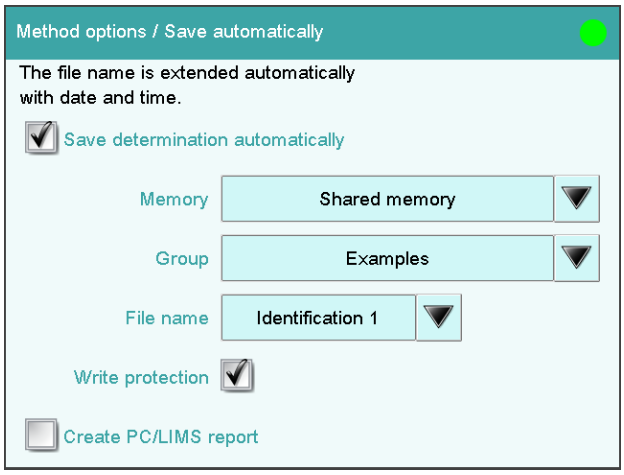
35. Deactivate the checkboxes for the functions to be disabled in the routine dialog (please refer to the manual).
    As for the user administration, the routine dialog settings can be copied from one system to another using the **Backup** and **Restore** functions.

Automatically saving the determination, creating a PC/LIMS report, PDF report and/or a printed report

In order to generate **accurate and complete copies** of records in both human readable and electronic form (please refer to *§ 11.10 (b)*), the original determination can be saved automatically at the end of each determination. At the same time, an electronic copy in form of a PC/LIMS report ("ISO 8859-1" or "UTF-8" format) can be created, and the determination can be printed automatically (both as printout and PDF).

In order to **save the original determination** file **automatically**, set the corresponding method options as follows (for details please refer to the manual):

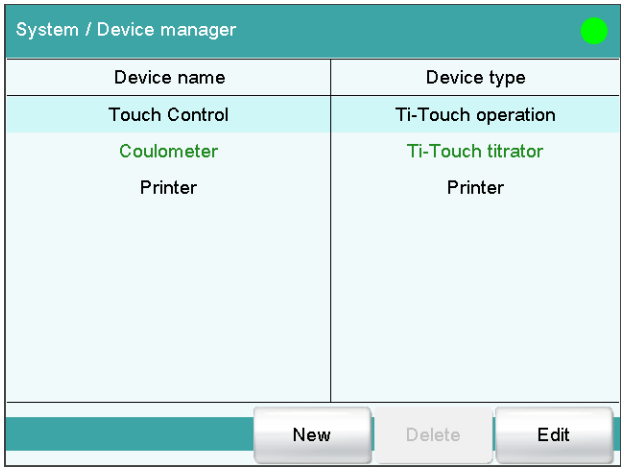
36. Open the dialog **Method options / Save automatically** and activate the **Save determination automatically** checkbox.



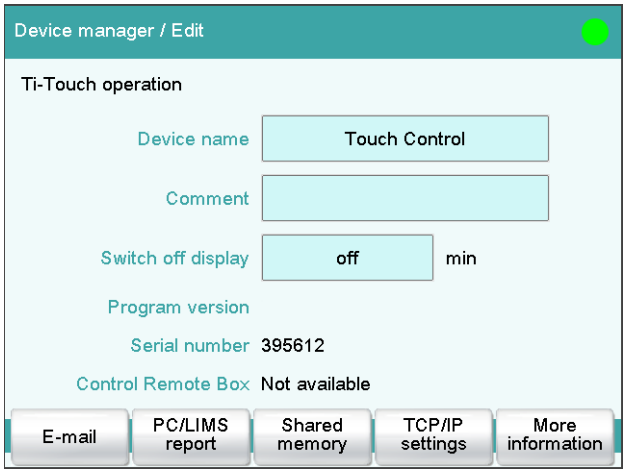
37. In the field **Memory**, the location where the determinations are to be stored can be selected. Determinations can be stored on different memory locations (please refer to the drop-down list). Enter the **Group** in which the determinations are to be stored. Choose **Identification 1** as **File 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). Date and time will be appended so that the file name is always unambiguous): Identification 1-YYYYMMDD-hhmmss.

38. Activate the checkbox **Write protection**.. If this parameter is activated, then the file cannot be saved, deleted, or renamed. In order to **Create a PC/LIMS report** automatically, set up the system configuration and the corresponding method parameters as follows (for details please refer to the manual):

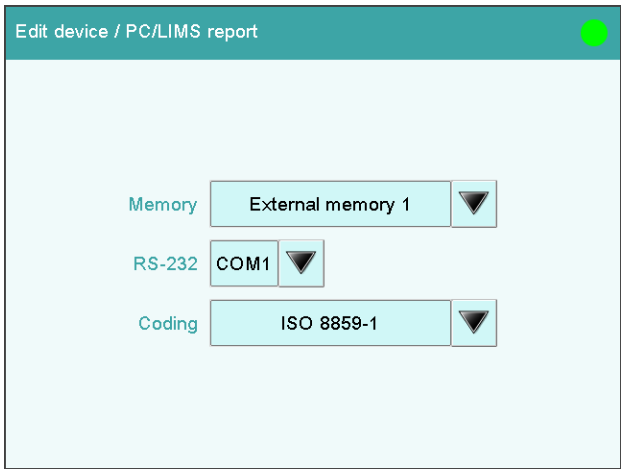
39. Open the dialog **System / Device manager**.



40. Select the device type **900 Touch Control** or **Ti-Touch operation** (according to the used device) and press **[Edit]**.

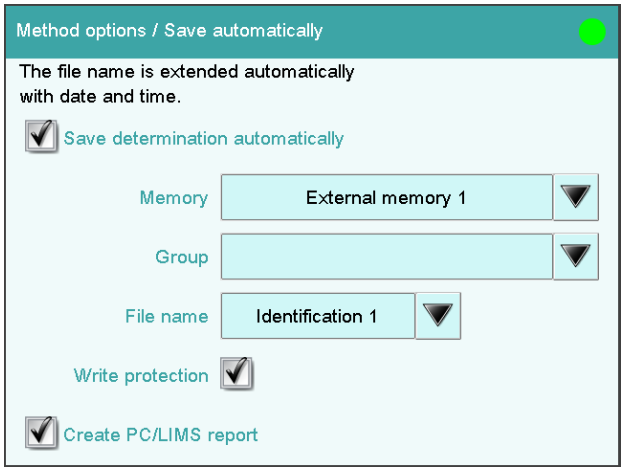


41. Press **[PC/LIMS report]** and set the PC/LIMS report parameters as follows:



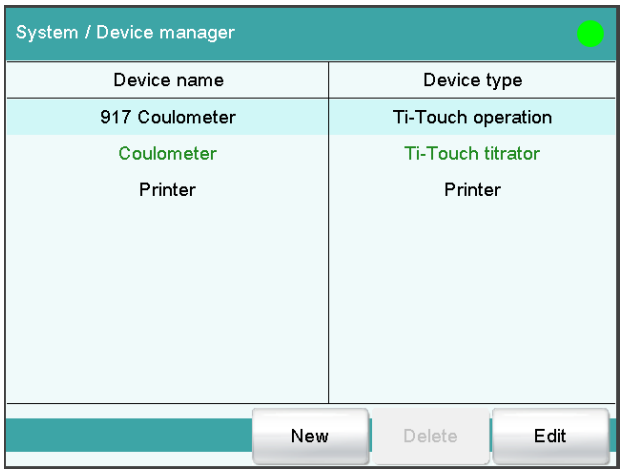
42. Select the **Memory** in which the files are to be stored or the **RS-232** interface via which the PC/LIMS report has to be sent and the **Coding** for the format in which the PC/LIMS report has to be coded and stored.

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

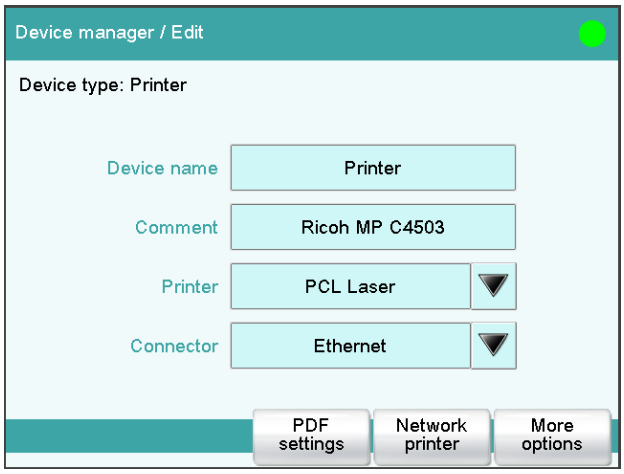


In order to save a report containing the determination data **in PDF format** and **print out a result report** automatically, set the corresponding method parameters as follows (for details please refer to the manual):

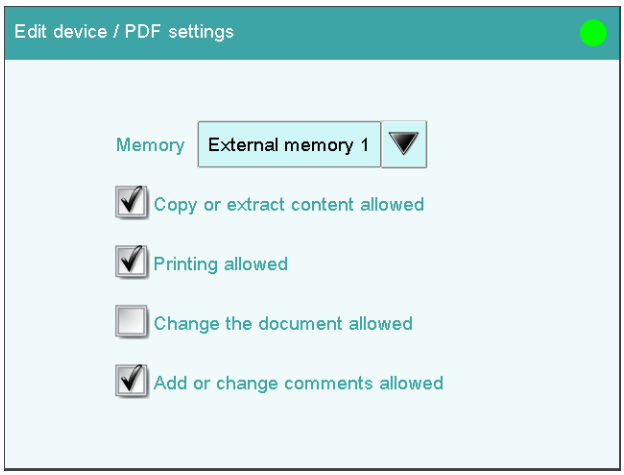
44. Open the dialog **System / Device manager**.



45. Select the device **Printer** and press **[Edit]**.

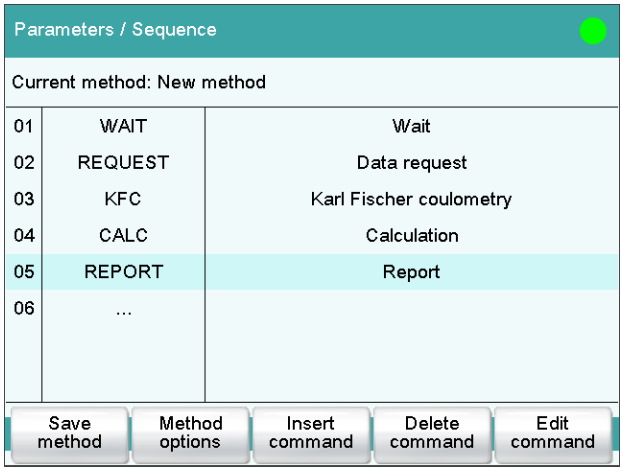


46. Press **[PDF Settings]** and set the PDF parameters as follows:



47. Select the **Memory** in which the files are to be stored (for details please refer to the manual).
48. If the report should be printed on the printer selected above at the same time, in the dialog "Device Manager / Edit" in the Printer field the printer type has to be chosen.

49. Open method sequence (dialog **Parameters / Sequence**) and insert a **REPORT** command at the end of the list.



50. A typical report sequence should contain the following reports:
Result report (all options switched on), **Measuring point list**, **Calculations**, **Used devices** and **Parameters full** (dialog **Insert report / Method reports**).