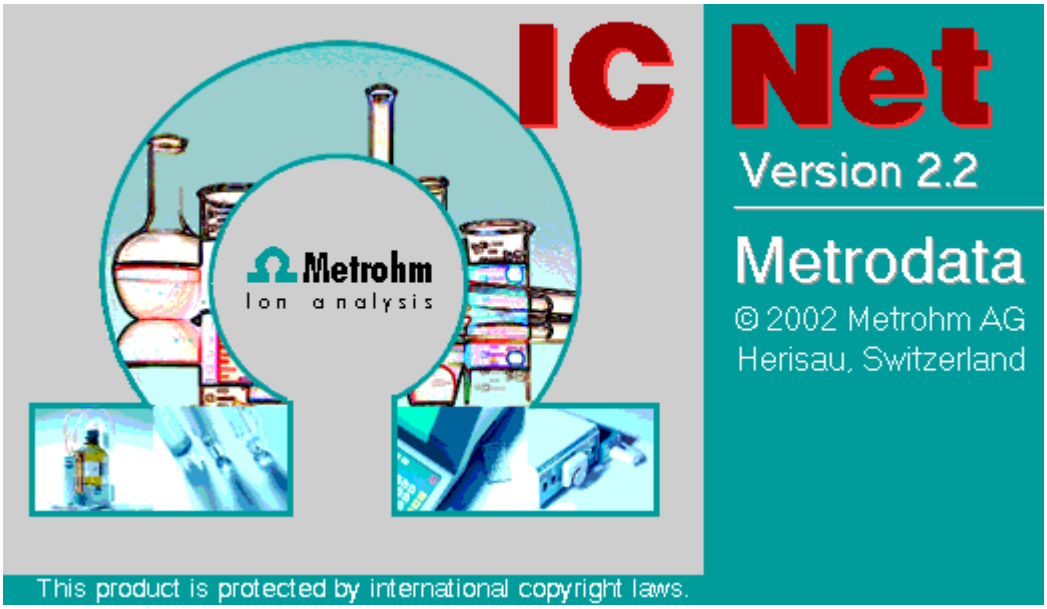
Metrohm
Ion analysis
CH-9101 Herisau/Switzerland
E-Mail info@metrohm.com
Internet www.metrohm.com

Using "IC Net 2.2™" software to comply with FDA 21 CFR Part 11



Compliance white paper 8.110.8273

Metrohm
Ion analysis
CH-9101 Herisau/Switzerland
E-Mail info@metrohm.com
Internet www.metrohm.com

Using "IC Net 2.2™" software to comply with FDA 21 CFR Part 11

Compliance white paper 8.110.8273

Teachware
Metrohm AG
Oberdorfstrasse 68
CH-9101 Herisau
teachware@metrohm.com

1st Edition 2003

Although all the information given in these instructions has been checked with great care, errors cannot be entirely excluded. Should you notice any mistakes please inform the author at the address given above.

Table of contents

1 Introduction

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 (see **Annex 4.2**), 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 (see **Section 11.1 (a)**).

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.

The *section 2* of this document describes in detail how the IC Net 2.2 software makes compliance with the requirements much easier. Each relevant section of 21 CFR part 11 is listed together with the corresponding feature of IC Net 2.2. *Section 3* describes thoroughly how to install, configure and use IC Net 2.2 for sustainable compliance to 21 CFR Part 11.

2 How "IC Net 2.2™" meets the 21 CFR Part 11 requirements

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 IC Net 2.2 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 IC Net 2.2 shipment Metrohm provides detailed user documentation and certificates of software validation.

Metrohm stores copies of all versions of its software documentation and source codes in multiple secure locations, including a fireproof vault. This documentation includes product requirements, product specifications, design specifications, project schedules, test plans, test results and validation documentation. All these documents are produced for every release via the Metrohm Design Control Procedure, which has been registered to ISO 9001 and is periodically audited. All Metrohm documents and source codes 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:

- Certificate of Software Validation (see *Annex 4.1*)
- Completed Installation Qualification records (Metrohm provides validation documentation which helps to perform the IQ; the software automatically performs software IQ tests to verify that program files are correctly installed, and stores the results on the system)
- 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

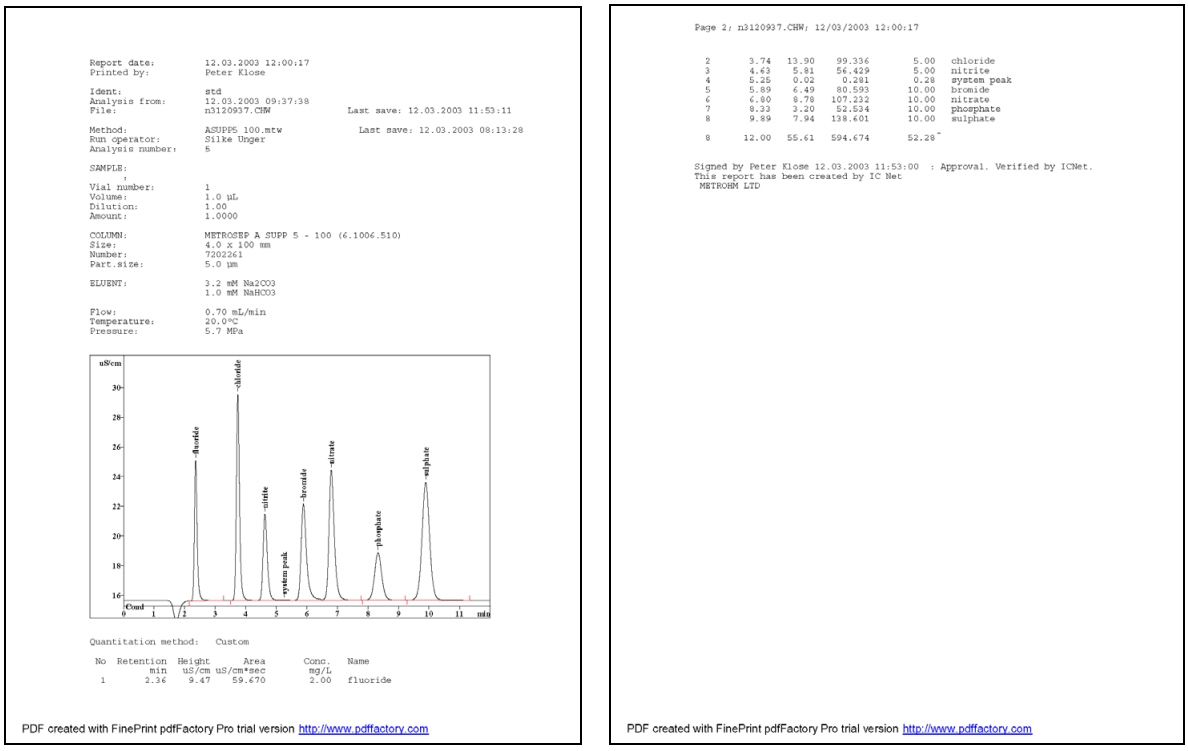
21 CFR 11.2 IMPLEMENTATION

(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.

As described in **Section 11.3**, IC Net 2.2 produces electronically sealed reports. These are protected together with their root data and state the users who electronically signed the records. IC Net 2.2 users can easily export copies of electronic records in Portable Document Format (PDF) for submission to agency units in accordance with FDA guidelines. These PDF report files faithfully preserve the contents and formatting of the IC Net 2.2 reports and are protected against any modification. Adobe Acrobat software (full version) or the pdfFactory Pro software must be used to generate a PDF file (*Figure 1*) of the reports.



Report date: 12.03.2003 12:00:17
Printed by: Peter Klose

Ident: std
Analysis from: 12.03.2003 09:37:38
File: n3120937.CHW Last save: 12.03.2003 11:53:11

Method: ASUPP5 100.mtw Last save: 12.03.2003 08:13:28
Run operator: Silke Unger
Analysis number: 5

SAMPLE:

Vial number: 1
Volume: 1.0 µL
Dilution: 1.00
Amount: 1.0000

COLUMN: METROSEP A SUPP 5 - 100 (6.1006.510)
Size: 4.0 x 100 mm
Number: 7202261
Part.size: 5.0 µm

ELUENT: 3.2 mM Na2CO3
1.0 mM NaHCO3

Flow: 0.70 mL/min
Temperature: 20.0°C
Pressure: 5.7 MPa

Quantitation method: Custom

No	Retention min	Height uS/cm	Area uS/cm*sec	Conc. mg/L	Name
1	2.36	9.47	59.670	2.00	fluoride

PDF created with FinePrint pdfFactory Pro trial version http://www.pdffactory.com

Page 2; n3120937.CHW; 12/03/2003 12:00:17

2	3.74	13.90	99.336	5.00	chloride
3	4.63	5.81	56.429	5.00	nitrite
4	5.25	0.02	0.291	0.28	system peak
5	5.89	6.49	80.595	10.00	bromide
6	6.80	8.78	107.232	10.00	nitrate
7	8.33	3.20	52.534	10.00	phosphate
8	9.89	7.94	138.401	10.00	sulphate
8	12.00	55.61	594.674	52.28	

Signed by Peter Klose 12.03.2003 11:53:00 : Approval. Verified by ICNet.
This report has been created by IC Net
METROHM LTD

PDF created with FinePrint pdfFactory Pro trial version http://www.pdffactory.com

Figure 1: IC Net 2.2 reports can be exported as PDF files for convenient submission of results to regulatory agencies

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.

IC Net 2.2 is normally 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 IC Net 2.2 data storage locations. IC Net 2.2's security system complements the security system of the chosen operating system by providing control over specific ion-chromatography-related resources and operations.

Digital signatures are implemented in IC Net 2.2 as described in **Sections 11.50**, **11.100**, and **11.200**.

With respect to 21 CFR 11, the primary electronic records in IC Net 2.2 are the original chromatogram records. Each record has all of the information pertaining to the analysis of a sample and contains the following items:

- Sample information (method assignment, sample ID, sample size, remark)
- Method information (method name, column, eluent, data processing, report settings)
- System information (system name, device configuration, time program)
- Electronically signed original results
- Chromatogram audit trail (modification history, electronic signature information)

After the end of a determination all the source data and settings required to produce a report are automatically locked and the result record contents, the operator's identification and the current date and time are used to calculate a hash code. A preview of the result report can be displayed. To add an electronic signature (discussed in **Section 11.50**) to the chromatogram records the operator is prompted to enter his or her user name, password and a meaning of the signature. Once chromatogram records are signed they cannot be modified; if anyone needs to alter the source data then the signature(s) must be removed by an appropriate authority first.

To backup data IC Net 2.2 can also export the records mentioned above, both for data recovery and/or for archiving purposes. The contents of this backup files cannot be accessed outside of IC Net 2.2; the contents have to be restored into the system before they can be read. Integrity issues are also discussed in **Section 11.3** of this document.

The other type of electronic record stored by IC Net 2.2 is the Audit Trail for the program history. In this Audit Trail all the actions performed in the IC Net window are logged. This is a tool for tracking the login and user administration history.

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.

At the installation of IC Net 2.2 all the files and the type and status of the installation are checked and a detailed installation log file is created in the installation directory; this can be used for IQ.

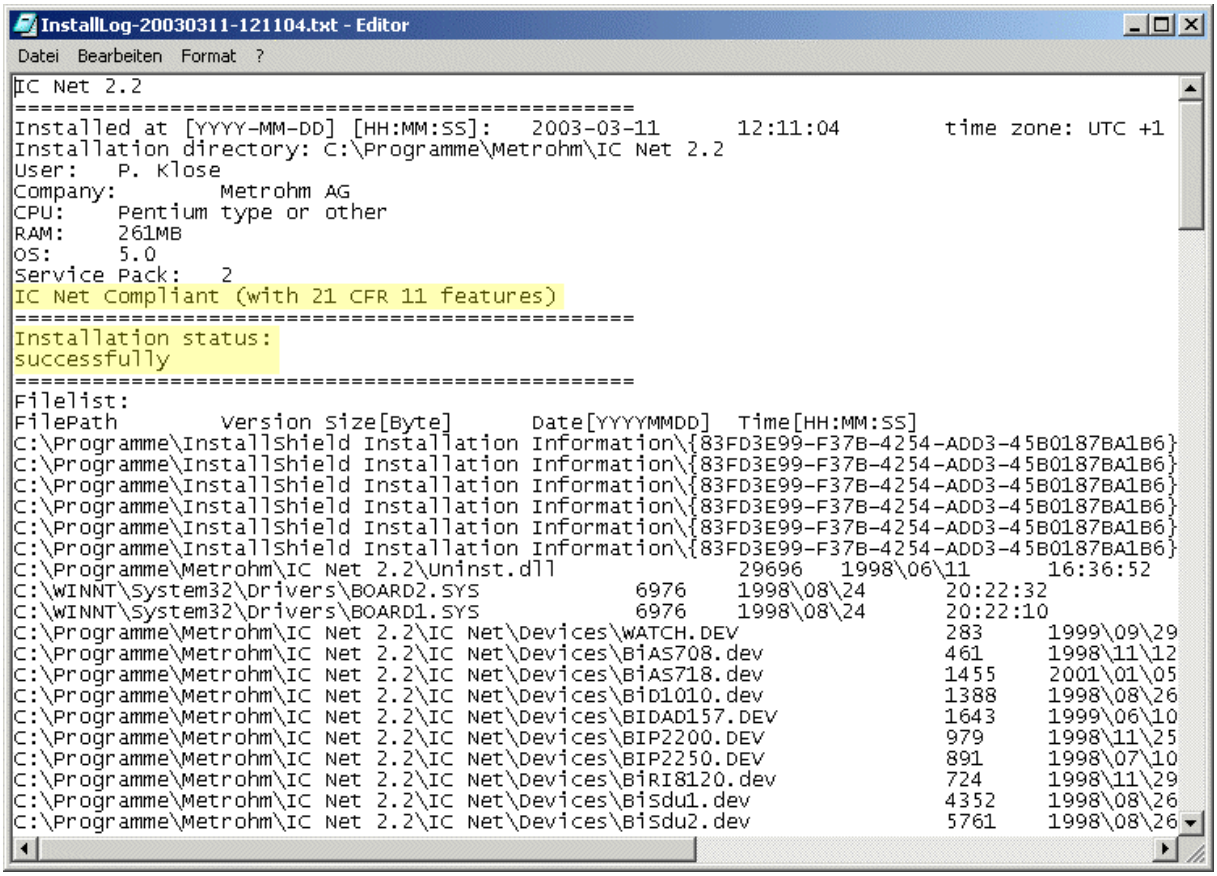


Figure 2: Installation log of IC Net 2.2.

IC Net 2.2's 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, date, affected data object, user name, messages and comments for each event.

Data corruption due to defects or failure of storage devices or media, or to deliberate attempts to modify signed records, are detected by IC Net 2.2 (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.

IC Net 2.2 provides all the necessary functions for locating and viewing the electronic records on the system and for generating complete, accurate paper and electronic copies for agency submissions. Electronic copies can be produced in Portable Document Format (PDF) as per agency guidelines; this is discussed in **Section 11.2**.

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

IC Net 2.2 provides several layers of protection to ensure that accurate records can be readily retrieved.

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 Microsoft® Windows® 2000 or Windows® XP, with the NTFS file system.

The next layer of protection is a secure file system with non-editable chromatogram files. This ensures that even those users who have access to files at the operating system level cannot read or modify records through means outside the secured application.

In addition to the protection provided by the operating system, IC Net 2.2 also provides a comprehensive, chromatography-oriented security system that controls access to data; this is 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 computer-generated audit trails as described in **Section 11.10 (e)**.

Records can be electronically signed, which simultaneously locks them and documents the signing authority, as described in **Section 11.50**.

Replacement of data is tracked by the Audit Trail.

The export tools included in IC Net 2.2 facilitate long-term record storage by an external archiving system. All the relevant data for each determination, including raw data, method, system, chromatogram Audit Trail and the results can be exported manually or automatically.

21 CFR 11.10 CONTROLS FOR CLOSED SYSTEMS
d) Limiting system access to authorized individuals.

IC Net 2.2's advanced security system supports three different security levels which are designed to fit the chromatography workflow.

Every user is assigned to one of three access levels (*Figure 3*).

- **Novice**
  Has restricted access to program functions; is only allowed to start and stop determinations using existing system and method files and has manual control over the devices. Modifications to the system, method and data files are not allowed.

- **Master**
  Has access to all program functions with few exceptions: the user cannot set Global preferences, open the Workplace window, change the hardware settings of interfaces and devices, or change Security options.

- **Administrator**
  Has access to all program functions. This level should be switched on only while installing the system or if the configuration is changed. The administrator user is authorized to change the name, access level and status of all other users.

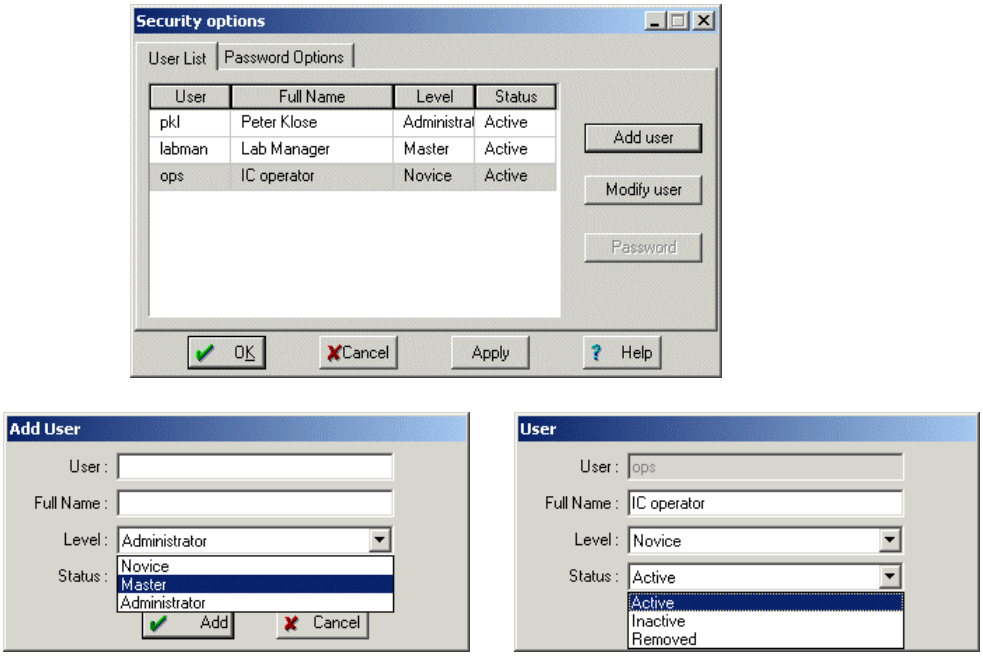


Figure 3: ***IC Net 2.2's comprehensive, chromatography-specific security system gives the System Administrator control over each user's access level and status.***

IC Net 2.2's security system provides the user management capabilities most often requested by system administrators:

- Easy maintenance of user administration (*Figure 4*).
- Users are identified by their User name and Full name throughout the software (*Figure 4*).
- Password controls – such as minimum password length, password uniqueness requirements and password validity limits – can be enforced (*Figure 5*).
- User and password history logs are automatically maintained in the Audit Trail.
- Users can be automatically locked out after a preset number of failed login attempts (*Figure 5*).
- 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 work (*Figure 5*).

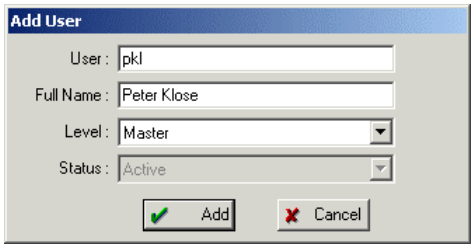


Figure 4: ***Users are identified by their User Name and Full name throughout the software.***

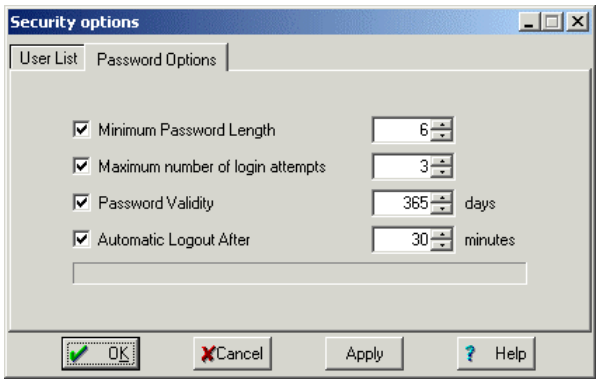


Figure 5: ***Security options for Login and Password protection can be set.***

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.

IC Net 2.2 automatically tracks all operator entries and actions that create, modify, or delete electronic records. It does this by maintaining secure, computer-generated, time-stamped audit trails. The audit trails record the time 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.

The Audit Trail keeps detailed records of all changes made to data objects and electronic records in a IC Net 2.2 data source. It documents the creation and modification of methods and sample entries. The recording of Audit Trail is enabled with the installation of IC Net 2.2.

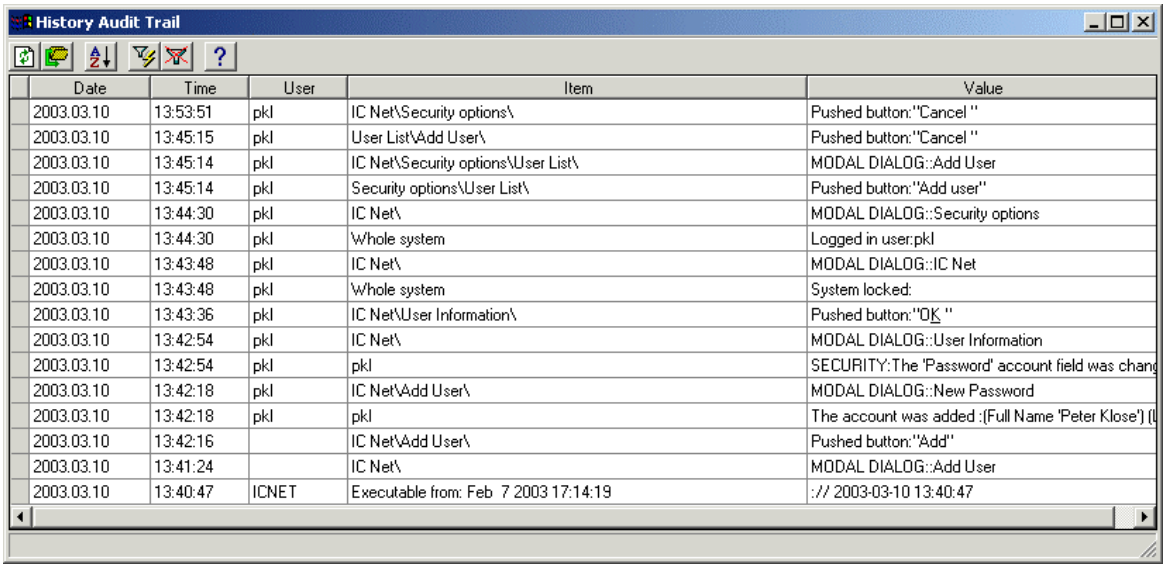
For each event the Audit Trail display (*Figure 6*) lists the type of event, the corresponding time and date, event source, operator name, message and comments.

Users are obliged to enter comments after changes made to methods 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. Metrohm therefore recommends that regulated laboratories store all data on

secured computers running Windows 2000 or Windows XP with the NTFS file system.

IC Net 2.2 provides all the necessary functions for sorting, filtering and viewing all the audit trails in the system and for exporting the audit trails at any time.



Date	Time	User	Item	Value
2003.03.10	13:53:51	pkl	IC Net\Security options\	Pushed button:"Cancel "
2003.03.10	13:45:15	pkl	User List\Add User\	Pushed button:"Cancel "
2003.03.10	13:45:14	pkl	IC Net\Security options\User List\	MODAL DIALOG::Add User
2003.03.10	13:45:14	pkl	Security options\User List\	Pushed button:"Add user"
2003.03.10	13:44:30	pkl	IC Net\	MODAL DIALOG::Security options
2003.03.10	13:44:30	pkl	Whole system	Logged in user:pkl
2003.03.10	13:43:48	pkl	IC Net\	MODAL DIALOG::IC Net
2003.03.10	13:43:48	pkl	Whole system	System locked:
2003.03.10	13:43:36	pkl	IC Net\User Information\	Pushed button:"OK "
2003.03.10	13:42:54	pkl	IC Net\	MODAL DIALOG::User Information
2003.03.10	13:42:54	pkl	pkl	SECURITY:The 'Password' account field was chang
2003.03.10	13:42:18	pkl	IC Net\Add User\	MODAL DIALOG::New Password
2003.03.10	13:42:18	pkl	pkl	The account was added :(Full Name 'Peter Klose') (U
2003.03.10	13:42:16		IC Net\Add User\	Pushed button:"Add"
2003.03.10	13:41:24		IC Net\	MODAL DIALOG::Add User
2003.03.10	13:40:47	ICNET	Executable from: Feb 7 2003 17:14:19	:// 2003-03-10 13:40:47

Figure 6: IC Net 2.2's Audit Trail tracks all changes to all 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.

IC Net 2.2 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)**, IC Net 2.2 provides a comprehensive, ion-chromatography-specific security system that controls access to instruments and data and also defines the types of operations that each class of user can perform. As described under **Section 11.50**, IC Net 2.2 also controls who is authorized to electronically sign chromatogram records.

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, IC Net 2.2 automatically performs a Software Installation Qualification to verify that all software components are correctly installed. A report is stored on the hard disk and can be printed out (see *Figure 3*). Password-controlled logins, both at the operating system level and at the IC Net 2.2 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 an IC Net 2.2 course.

Off-site classes are regularly conducted in Metrohm field offices. Customized 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.

Metrohm supplies user documentation in printed form together with the software. User documentation in electronic format is available from Metrohm on request. 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).

IC Net 2.2's comprehensive implementation of electronic signatures provides all the functionality required by **Section 11.50**, while satisfying laboratory workflow needs.

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 *Figure 5*).

Applying electronic signatures to chromatogram records in IC Net 2.2 is a simple and straightforward process. The operator chooses the relevant record and selects the "Electronic signature" menu command. After having entered user name, individual password and a meaning for the signature, the chromatogram can be signed-off (see *Figure 7*).

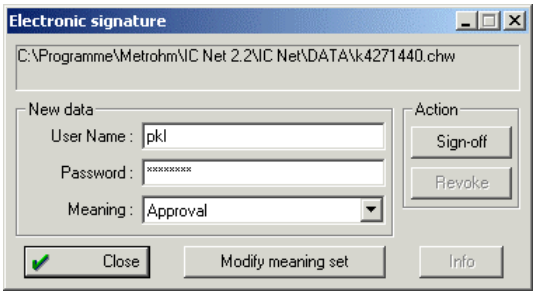


Figure 7: ***The user applies the electronic signature to the chromatogram by entering his/her user name, individual password and a meaning of the signature.***

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 IC Net 2.2, electronic signature data is stored as an integral part of signed-off chromatogram records, in such a way that the signature data cannot be deleted, copied, or otherwise transferred by ordinary means.

When chromatogram records are electronically signed, the chromatogram contents, user information and signature time/date stamp are used to calculate a unique hash code; this hash code is then stored together with the record contents in an encrypted file that is locked to any modification within IC Net 2.2. If any change is made to the file externally, the electronic signature is rendered invalid. When opening a file IC Net 2.2 uses the chromatogram data and signoff information to recalculate the unique hash code of the file and checks the integrity of the data.

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.

IC Net 2.2's electronic signatures are implemented by using a combination of the 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.

IC Net 2.2 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 a validity period for passwords (*Figure 5*).

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.

IC Net 2.2's 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. These features satisfy the requirements of subsections (i) and (ii).

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 the 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. IC Net 2.2 facilitates the administration of password maintenance through controls such as minimum password length, password validity limit and password re-use prevention (see *Figure 5*). The System Administrator can use these controls to force users to change their passwords at regular intervals to ensure new, unique expressions of a specified minimum length. The System Administrator can also disable or remove any user if necessary (see Figure 3).

Automatic account deactivation protects the software against systematic attempts to breach the security system; this can be set to disable any account after a specified number of failed login attempts.

All security-related events (user and group configuration changes, successful logins, failed logins, and electronic signatures) are automatically tracked in the Audit trail of the program history (see Figure 6) of IC Net 2.2's Audit Trail. The convenient sorting and filter options of the Audit Trail makes it easy for Administrators to track and view particular events of interest.

3 How to install and use the program to be compliant with 21 CFR Part 11

3.1 Configuration of Windows 2000/XP

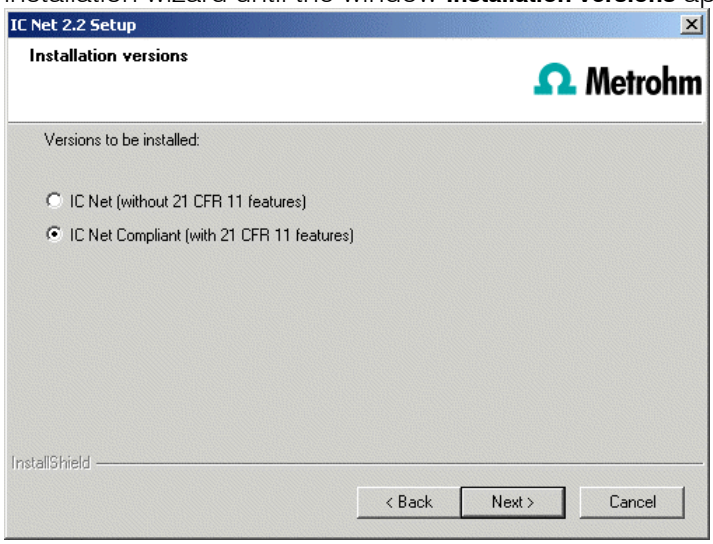
Since the operating system provides the basis for the ion chromatography software, it is important to configure it properly for a 21 CFR Part 11 compliant system.

1. Make sure the operating system **Windows 2000** or **Windows XP** is working with the NTFS file system on the drive where IC Net should be installed. For detailed information see the manual of your operating system.
2. IC Net creates a Windows user with **'power user'** rights that control the access to the IC Net directories. To provide a secure system, the system administrator has to make sure that only Windows users with user rights inferior to a Windows 'power user' are working on the system.

3.2 Software installation

3.2.1 Installation of IC Net 2.2

1. Install IC Net 2.2 from the installation CD and proceed according to the installation wizard until the window **Installation versions** appears.

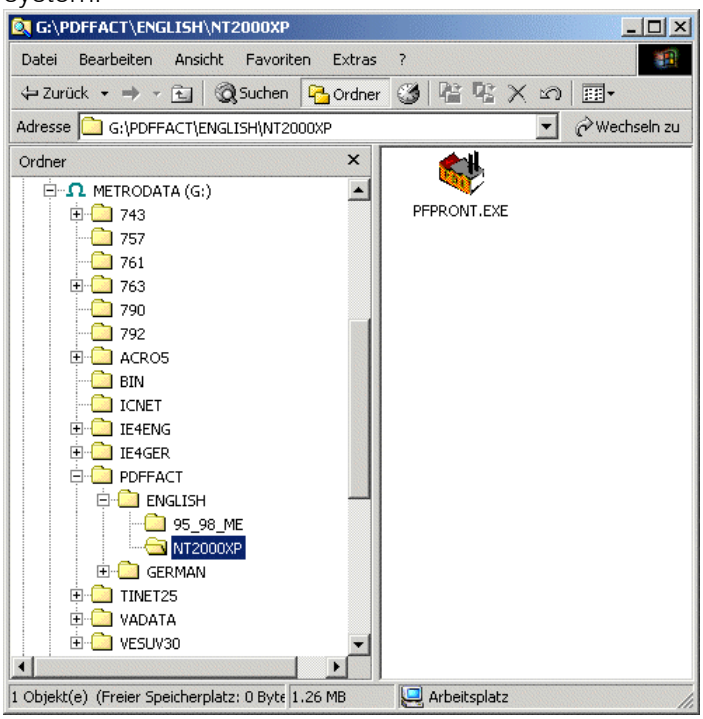


2. Select the option **IC Net Compliant (with 21 CFR 11 features)** and click on **<Next>**.
3. Select the installation directory and click on **<Next>**. The "IC Net 2.2" program will be installed. After the installation you have to restart the computer.
4. Check the installation log file (see *Figure 3*) **InstallLog-date-…txt** in the installation directory of IC Net to verify that IC Net 2.2 has been successfully installed.

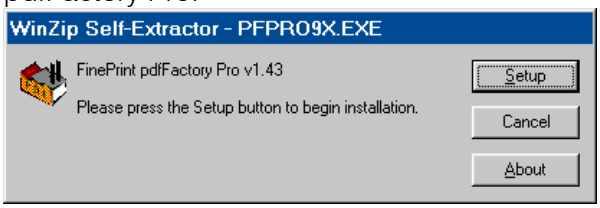
3.2.2 Installation of a PDF printer

For agency submission of electronic records the Portable Document Format (PDF) is recommended. To create PDF files from the electronic records of IC Net a PDF printer is required. On the Metrodata Software CD a trial version of the FinePrint pdfFactory Pro (pdf printer) and the Acrobat reader (pdf viewer) are included.

1. Open the directory for the FinePrint pdfFactory Pro (**...\PDFFACT**)on the Metrodata CD, select the directory for your language and for your operating system.



2. Double-click on the file **PFPRONT.EXE** to start the installation of FinePrint pdfFactory Pro.



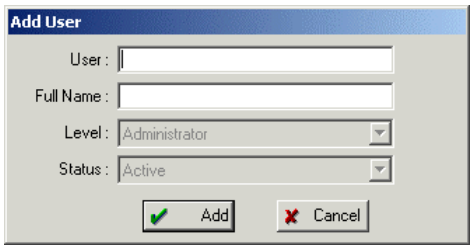
3. Click on **<Setup>** and confirm the installation procedure with **<Yes>**.
4. Restart the computer after the PDF printer driver installation.
5. If the Adobe Acrobat Reader program is not already installed on the computer, open the directory for Adobe Acrobat Reader installation (**ACRO5**.) and open the ***.exe** file.

The version of FinePrint pdfFactory Pro included on the Metrodata Software CD is a **trial** version. If you intend to use FinePrint pdfFactory Pro as the PDF printer for IC Net 2.2 please purchase the full version of FinePrint pdfFactory Pro .

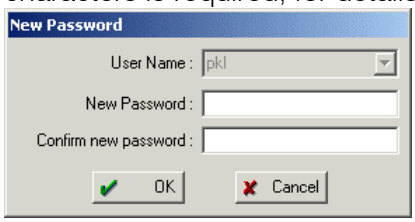
3.3 Work with IC Net 2.2

3.3.1 First login

1. Open the IC Net 2.2 program. When the system starts for the first time after the software installation, the **Add User** window opens and a user with Administrator access level is created.



2. Enter **User** name and **Full name** of the first user. Click on **<Add>**.
3. Enter a **password** for IC Net 2.2 and click on **<OK>**. A password with at least 6 characters is required, for details see section **security**.

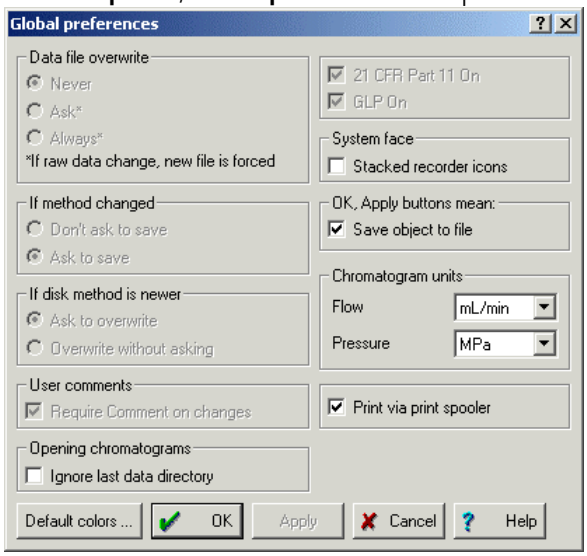


4. At the first login after the installation of IC Net 2.2 not all security features of the software are implemented. Close IC Net 2.2 and start it again to work compliant.

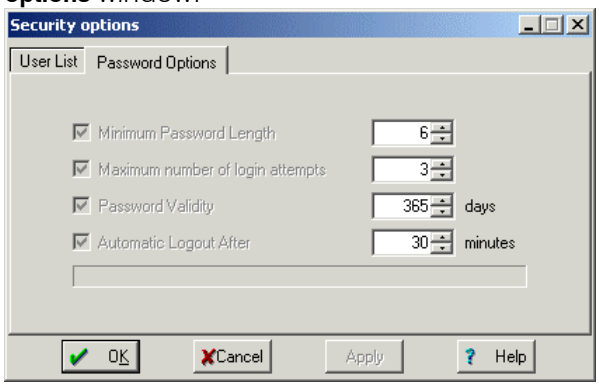
3.3.2 Security

If IC Net 2.2 is installed with the option **IC Net Compliant (with 21 CFR 11 features)**, all settings in the software to comply with 21 CFR Part 11 are made automatically and cannot be altered.

1. Select **Options/Global preferences** to open the **Global preferences** window.

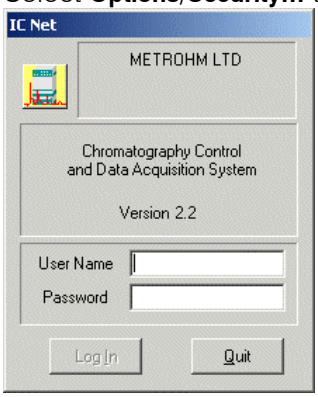


2. Select **Options/Security…/Security options/Password options** to open the **Password options** window.

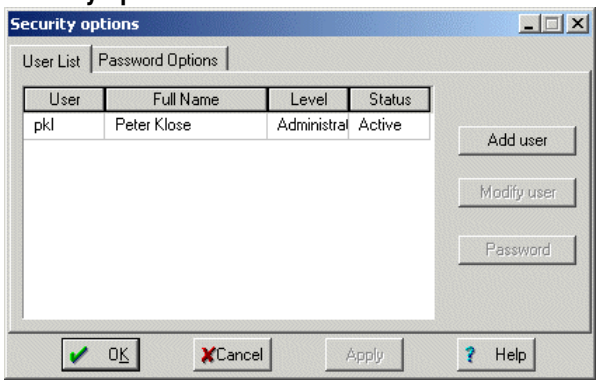


3.3.3 User administration

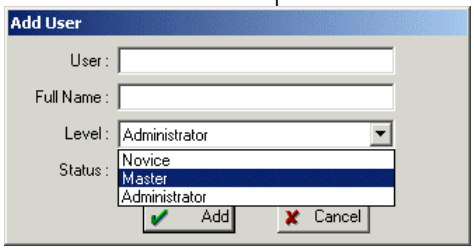
1. Select **Options/Security…** to open the **Security options** window.



2. **User name** and **Password** of an administrator are required to log into the **Security options** window.

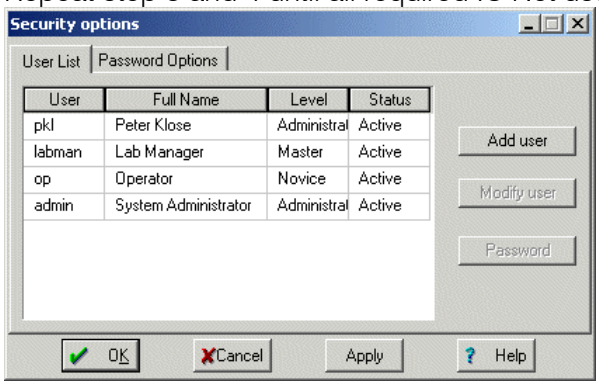


3. Click **<Add user>** to open the Add user window.



4. To create a new IC Net user enter **User** name, **Full name** and access **Level** of the new IC Net user and click **<Add>**.
Create at least one more **Administrator** user as a backup and store the login data for this user in a safe place.

5. Repeat step 3 and 4 until all required IC Net users are created.

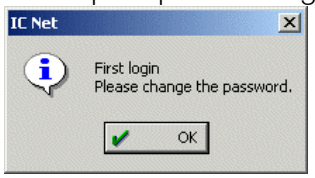


6. Click on **<OK>** to close the **Security options** window.

3.3.4 First login of new users

7. A new user that has been created in IC Net has to enter his user name at the **User Name and** the **Password** entry field at the first login. Click on **<Log In>** to close the **Login** window.

8. IC Net prompts to change the password, click **<OK>**.



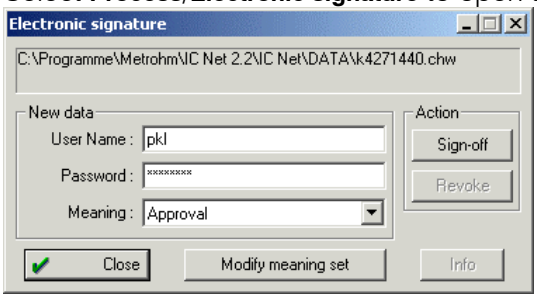
9. Enter a **password** for IC Net 2.2 and click on **<OK>**. A password with at least 6 characters is required, for details see section **security**.

3.3.5 Save Chromatogram

1. Make sure that all chromatograms are saved in the **.../DATA** folder (or in one of it's subfolders) of IC Net to maintain secure and accurate data handling. Check especially the chromatogram paths in the methods.
2. If the chromatogram data is stored outside the data folder of IC Net, the system administrator/user has to take appropriate measures to ensure the data security of these files, the integrity of this files is not longer supervised by IC Net.

3.3.6 Sign chromatogram

1. Select **File/Open/Chromatogram** , select the chromatogram that is to be signed and click **<OK>** to open the chromatogram
2. Select **Process/Electronic signature** to open the **Electronic signature** window.



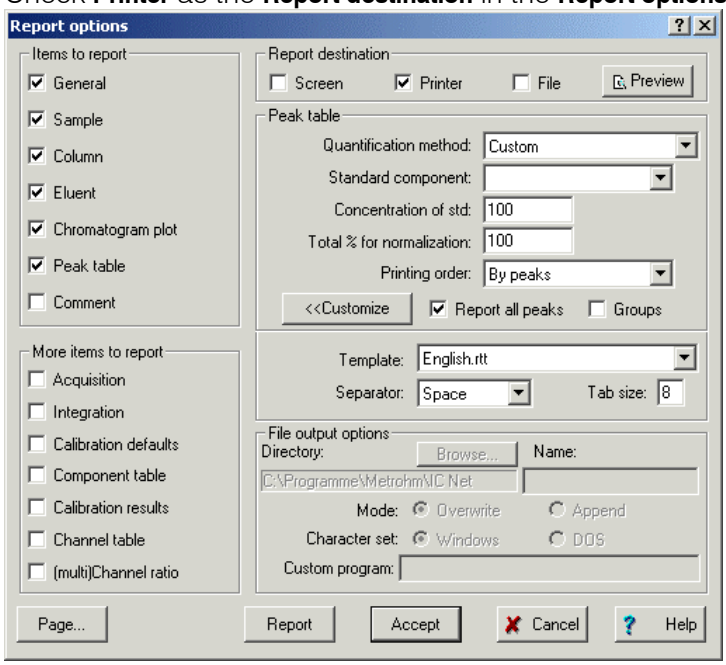
3. Enter **User Name**, **Password** and choose a meaning for the signature. Click **<Sign-off>**. Once a chromatogram is signed, it cannot be altered.
4. Click **<Info>** to see the signatures applied to a chromatogram.

3.3.7 Audit Trails

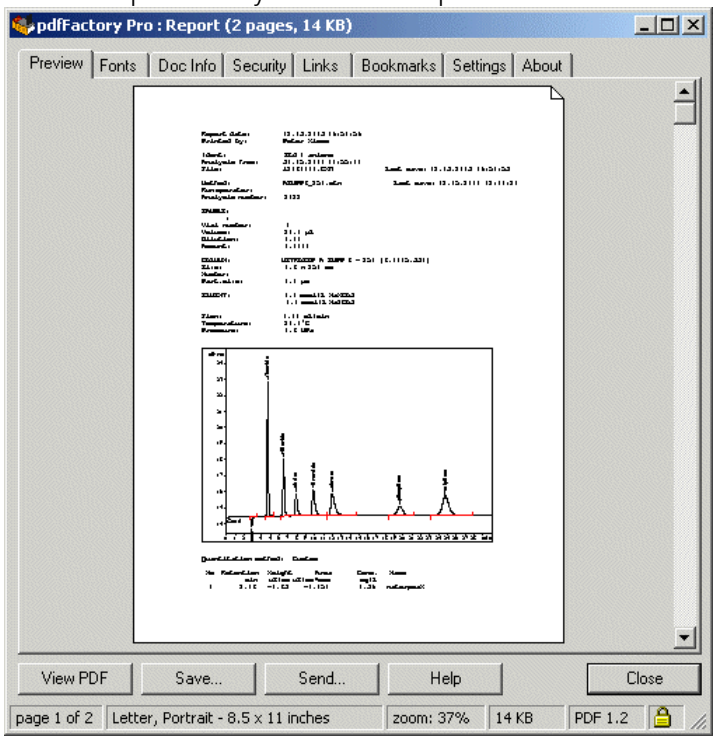
1. Select **Options/Audit Trail/Chromatogram** or **Options/Audit Trail/History** to open the Audit Trails of a chromatogram or the IC Net history, see *Figure 6*.
2. To display the information of interest, use the convenient filter and sort options of the **Audit Trail** window, for detailed information see the software manual or the on-line help of IC Net.

3.3.8 Create secure PDF reports

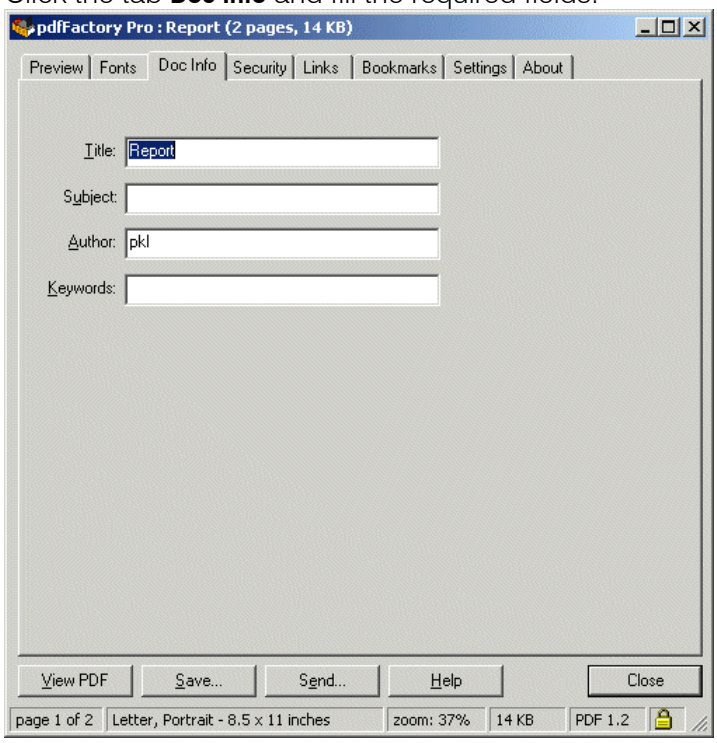
1. Configure Fine Print pdfFactory Pro as standard printer of Windows.
2. Open the **Report options** window with **Process/Make report...**, if you would like to create a report of a existing chromatogram, or **Method/Report options...**, to set the report options of a method.
3. Check **Printer** as the **Report destination** in the **Report options** window.



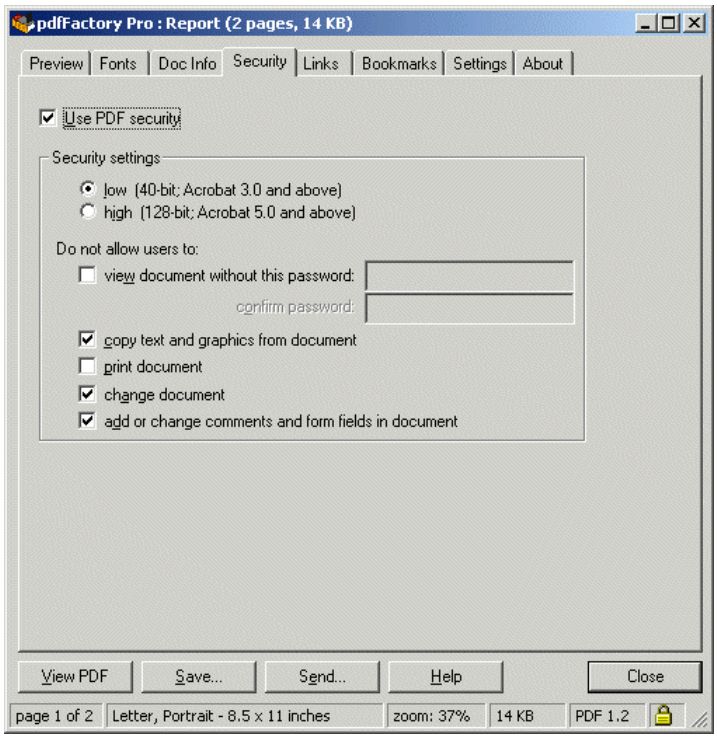
4. Click on **<Preview>** to display a preview of the report.
5. Click on **<Accept>** to accept the setting and close the window without printing.
6. Click on **<Report>** to print the PDF file of the report.
7. Fine Print pdfFactory Pro shows a preview of the PDF file.



8. Click the tab **Doc Info** and fill the required fields.



9. Click the tab **Security** and check the options shown to create a secure PDF document that cannot be altered.



10. Click **<Save>** and enter directory and file name for the PDF report.

4 Annex

4.1 Declaration of conformity

Declaration of Conformity
Software Validation

for the PC program
Metrodata IC Net 2.2

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

Description

IC Net 2.2 is a data acquisition and control software for PC-controlled ion chromatographic systems consisting of Metrohm and Bischoff instruments. IC Net 2.2 can be used in an environment that is compatible with FDA 21 CFR Part 11 (with Windows™ 2000 or XP).

IC Net 2.2 can be used for recording and evaluating chromatograms. Time programs can also be created in which a large number of instrument functions can be triggered for each program step. It is also possible to use programmable signals to control external instruments.

The operating software meets all the requirements demanded from a modern integration software: single or multi-point calibration, internal or external standard, selectable algorithms for non-linear calibration, various integration modes with integration parameters and integration events, different methods for peak recognition, peak editor, free scaling, superimposing of chromatograms, statistics functions, use of sample tables and batch reprocessing plus a powerful, GLP-compliant report generator with output interfaces for monitor, printer and external databases.

The independent Autodatabase PC program included can be used to save in a database and handle results and chromatograms produced by the IC Metrodata programs. With Autodatabase, data can be sorted, filtered and searched applying different criteria. In addition, data and curves can be printed out according to user-defined report templates.

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 Software Manual.

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

Herisau, 24 February 2003

Dr. J. Frank
Development Manager

Ch. Buchmann
Production and
Quality Assurance Manager

IC Net 2.2 – Declaration of Conformity – 2003-03-12 1/11

4.2 Reference

- *Title 21 Code of Federal Regulations Part 11 (21 CFR Part 11) Electronic Records; Electronic Signatures; Final Rule*;
  Department of Health and Human Services, Food and Drug Administration;
  March 20, 1997
  http://www.fda.gov/ora/compliance_ref/part11/FRs/background/pt11finr.pdf