NanoPhotometer® CFR21 Software

User Manual

Version 3.0

Software Version NPOS 4.6j.16350

The end user of the NanoPhotometer® product (“End User”) hereby takes full responsibility for safe storage and backup of all files and/or data that may be created, saved on or transferred from the device. End User acknowledges that it is possible that data and/or files may be lost or damaged, and further acknowledges and agrees that it has sole responsibility to maintain all appropriate backup of files and data. By using the NanoPhotometer® device, End User hereby agrees to these terms, and agrees that Implen shall not be held liable for any loss, deletion or damage of any data or files for any reason, including any damages attributable thereto.

Telephone support is available using one of the following phone numbers from your geographic region:

Europe, Asia, South Pacific, Middle East, Africa

Phone: +49 89 72637180
Fax: +49 89 726371854
Email: info@implen.de
Website: www.implen.de

Implen GmbH
Schatzbogen 52
81829 München
Germany

North and South America

Phone: +1 818 748 6400
Fax: +1 818 449-0416
Email: info@implen.com
Website: www.implen.com

Implen, Inc.
Unit 104
31194 La Baya Drive
Westlake Village, CA 91362
USA

Contents

1. OVERVIEW

The CFR21 software complies with FDA 21 CFR part 11 requirements and is an optional software tool ideal for GxP laboratories, which require proper electronic record keeping. It includes user management, access control, electronic signatures, data integrity, security, and audit trail functionality.

Note: This CFR21 Software user manual does not describe the general functionality of the NanoPhotometer®. The CFR21 software user manual is to be used in conjunction with the NanoPhotometer® user manual.

User Management
Individual Role Based Access Control (RBAC) provides password protected access and control of the NanoPhotometer®. Create multiple user accounts with different access rights which are handled in a hierarchic structure. User role options are Administrator, Power User, User, and Viewer. Organize users into working groups to facilitate access of shared data and stored methods within a laboratory. There is also an option for increased transparency with Four Eye Authentication. Various password settings are available within the CFR21 Software – for example secure password and password expiration options. Effectively improve data security and fulfill audit requirements easily with flexible and appropriate RBAC user management solutions. All features can be enabled or disabled on demand to meet your laboratory needs.

Electronic Signature
Measurement data can only be saved when confirmed with user ID and password by the logged in user. All saved files include the user name/author, date and time of saving for proper electronic records. IDS and PDF files cannot be altered and ensure data integrity.

Audit Trail
The audit trail automatically records all actions and preference changes in an audit log. The audit log contains a log ID, time stamp, user ID, and category for each action. Audit trails can be exported by an Administrator or Viewer for documentation purposes. Power User can read the audit trail, but is not allowed to save it.

Important Compliance Information
The NPOS Software, containing the activated CFR21 Software, in conjunction with your company's SOPs can assist you in complying with FDA 21 Part 11 requirements.
Your company must ensure that all aspects of the FDA regulations are maintained. Compliance may include (but is not necessarily limited to):

- Validating your NanoPhotometer®.
- Access control and proper documentation.
- Determining that the system users have the knowledge, training, and experience required to perform their assigned tasks.
- Verifying the identity of each user.
- Restricting user accounts appropriately.
- Requiring a periodic change of account passwords.
- Certifying the use of electronic records and electronic signatures to the FDA.
- Configuring the CFR21 software consistently with your intended use.
- Establishing and following conforming SOPs.

Note: For more information on complying with the FDA 21 CFR Part 11 requirements, refer to the FDA website: http://www.fda.gov.

2. CFR21 Software Activation

The CFR21 software is part of the installed NPOS Software. No further installation is necessary. Activation of the CFR21 Software is only possible with a serial number related license file (NPOS.lic).

Note: The purchased license file for the CFR21 software is stored on the Implen USB flash drive included in the NanoPhotometer delivery.

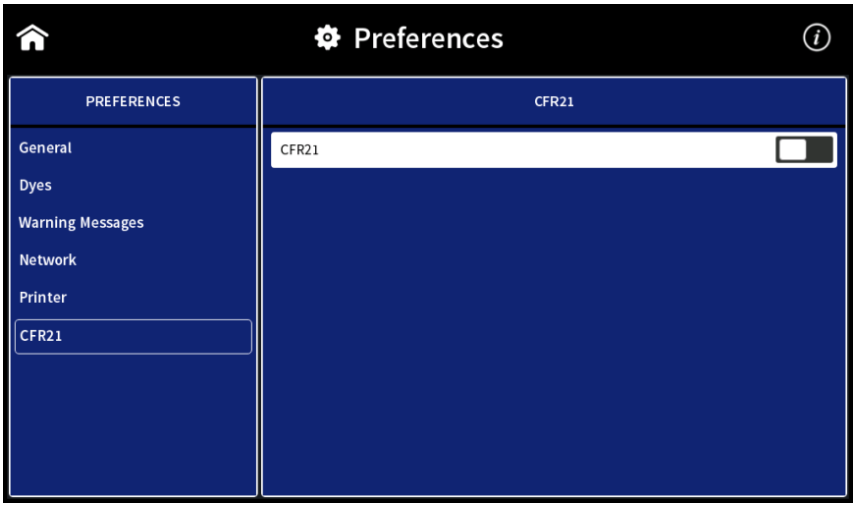
The CFR21 Software is available for NanoPhotometer® N120/NP80/N60/C40.

Note: The CFR21 Software is not available for NanoPhotometer® N50 and control devices like tablets and smartphones.

Enabling CFR21 Software

Activation Steps:

- Save the NPOS.lic (license file) into the root folder of a USB flash drive
- Insert the USB flash drive into the NanoPhotometer®
- Select Preferences / CFR21
- Activate CFR21 toggle
  Note: All existing network folder and server access entries will be deleted by this step.
- Add an Administrator account (see page 9 Add Account)
  Note: It is necessary to add at least one Administrator account otherwise the CFR21 Software is not activated.
  Note: Please keep a copy of your Admin password for your records. For security purposes, Admin passwords cannot be recovered. Should you lose your Admin login details, you will need to contact the Implen Support team (support@implen.de) for assistance with password reset.



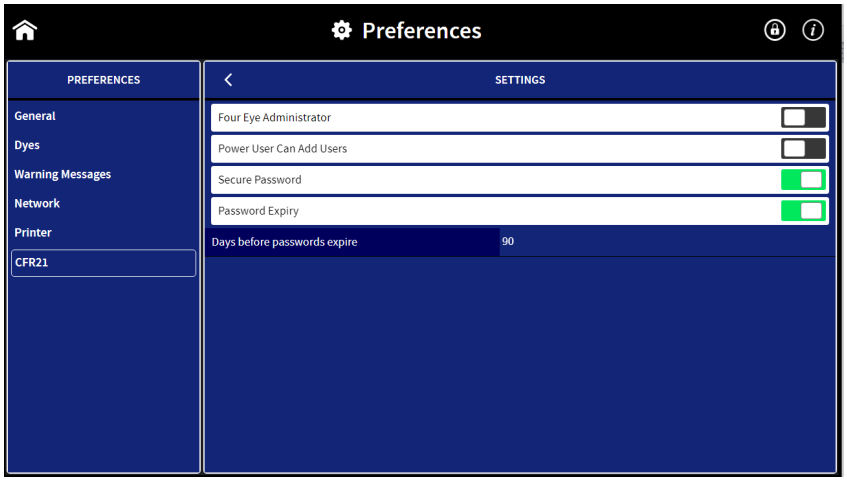
DEACTIVATION CFR21 SOFTWARE

For deactivation of the CFR21 Software deactivate the CFR21 toggle switch in Preferences/CFR21. This step will perform a factory reset of the NanoPhotometer®. Save all data before deactivation of the CFR21 Software and perform a factory reset.

Note: Deactivating the CFR21 Software requires a factory reset of the NanoPhotometer®. All data, user accounts, permissions and settings will be lost. Save all necessary data in advance.

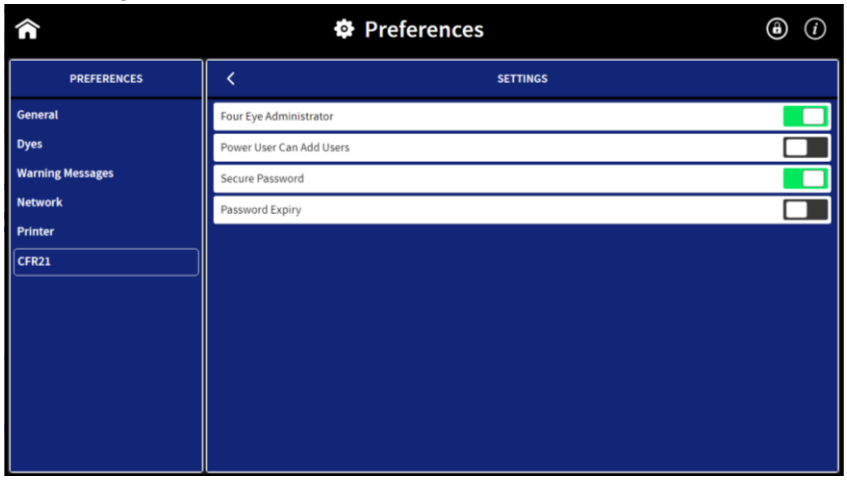
3. SETTINGS

The CFR21 settings menu includes: Four Eye Administrator, Power User Can Add Users, Secure Password and Password Expiry.



FOUR EYE AUTHENTICATION

Four Eye Authentication requires confirmation from a second Administrator account when implementing critical software changes. To enable the Four Eye Administrator setting, activate the Four Eye Administrator toggle switch. It is necessary to create at least two Administrator accounts for this setting.



The following features, settings and actions require confirmation from a second Administrator account if four eye authentication is active:
Factory reset, change of date and time, deactivation of CFR21 software, deactivation of Four Eye Administrator, secure password, password expiry, rename, delete, move folder, and delete result file.

POWER USER CAN ADD USERS

Administrator accounts have the option to enable/disable the ability for Power Users to create other Users via the toggle switch. If this function is disabled, only Administrator accounts have permission to create new Users.

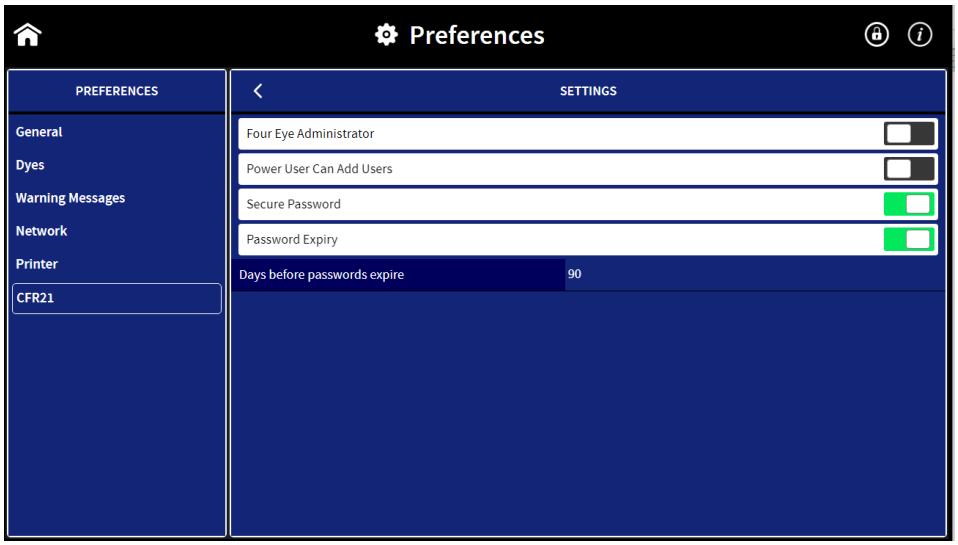
Secure Password

Secure password is set by default and can be switched off.

- Secure password ON: At least 8 characters with a minimum of 1 special character, 1 capital letter, 1 lowercase letter and 1 number.
- Secure password OFF: At least 4 characters/numbers and no further restrictions.

Password Expiry

Password expiry offers the possibility to have each user prompted to change the account password on a regular basis. When password expiry is active it is possible to enter a timeframe between 1 and 365 days. Default setting is 90 days.

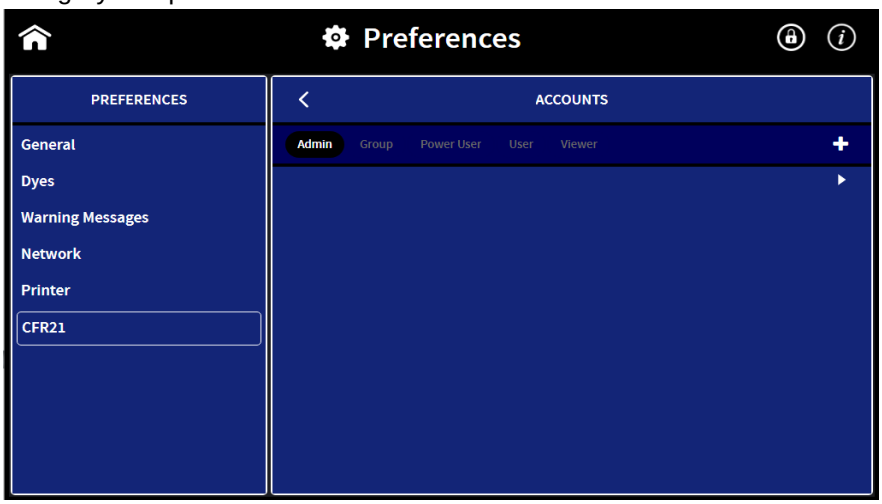


Note: If the amount of days before passwords expire is reduced, it is possible that all passwords expire immediately and must be changed with the next login.

4. Setting up User Accounts

There are four types of user accounts: Administrator, Power User, User, and Viewer.
An Administrator has full access rights and can create Groups, Administrator, Power User, User, and Viewer accounts. Power Users and Users need to be assigned to a group. A Power User can create User accounts in their defined group (this feature can also be disabled by the Administrator).

To add an Administrator, Group, Power User, User or Viewer, select the desired account/group category and press the + icon.



Note: If account/group category or + icon is not available, the logged in user does not have access rights to create the account or group.

Add Account

It is possible to add several Admin, Power User, User and Viewer accounts. Power User and User accounts need to be assigned to a group.

Note: Please keep a copy of your Admin password for your records. For security purposes, Admin passwords cannot be recovered. Should you lose your Admin login details, you will need to contact the Implen Support team (support@implen.de) for assistance with password reset. Power User and User passwords can be recovered by an administrator.

1. Select category: Admin, Power User, User, or Viewer

   Note: In order to add a Power User or User create at least one Group.

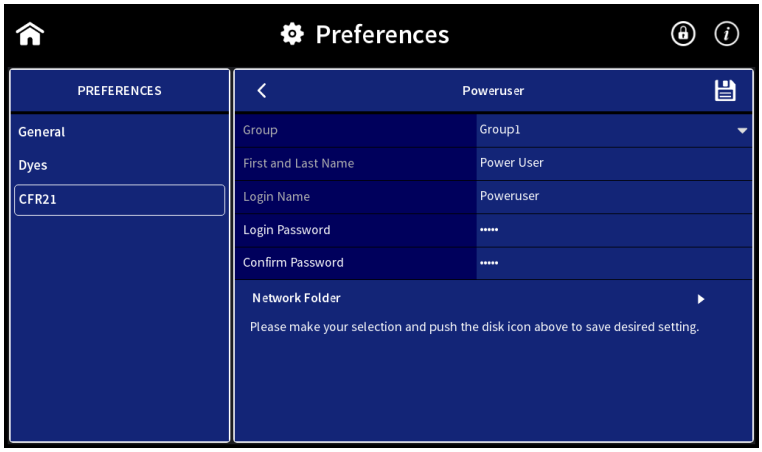
2. For Power User / User account select a Group

3. Enter user's first and last name
   Note: Allowed characters are: letters

4. Enter Login Name
   Note: Allowed characters are: letters, digits, underscores and dashes. Login name needs to start with a letter. Do not use blank character.
   Note: Login names must be unique. It is not possible to use identical login names and/or group names.

5. Set Login Password and confirm the password. This password is a temporary password which the user will be prompted to change after the first login.

   Note: Secure passwords need to have at least 4 characters/numbers, but if secure password is enabled at least 8 characters are required with a minimum of 1 special character, 1 capital letter, 1 lowercase letter and 1 number.

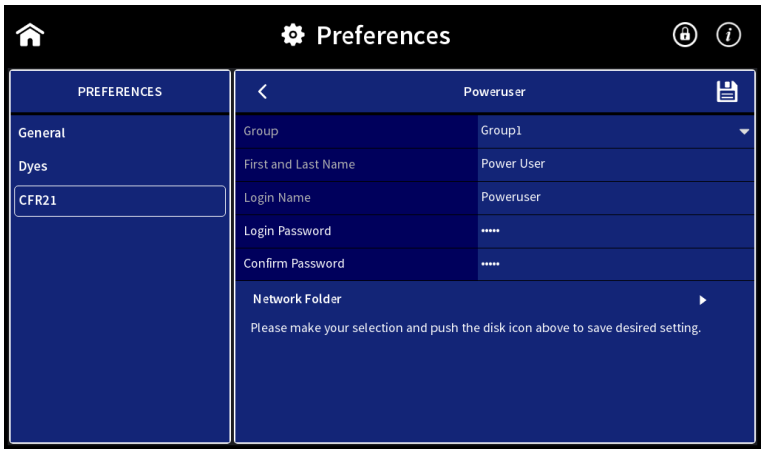


6. Save User account by pressing the icon

Note: It is not possible to delete or change user accounts.

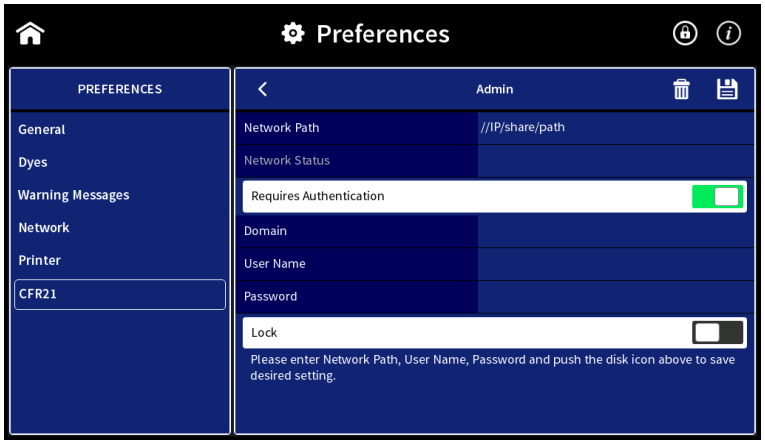
ADD NETWORK FOLDER

Network folders can only be created by the logged in user for their own user account. To create a network folder select Network Folder in the user account preferences.



Enter the Network Path of the network folder using either //IP/share/path or //server/share/path. If the local network requires authentication enter the user name and password for Windows or MacOS logon and the domain if necessary. Save the settings by pressing the icon. The network state changes to “connected” if the network folder is created successfully.

Note: The NanoPhotometer® needs to be connected via LAN or WLAN to the local network.



Network folders can be deleted by pressing the icon.
The folder nickname is created automatically (Network_login name) and is shown in all directories.

5. User Rights

The following table describes the different user rights of Administrator, Power User, User, and Viewer accounts.

Note: If "Yes/4 Eye" is displayed in the administrator rights column, a confirmation by a second administrator is required when Four Eye authentication is active (see page 7).

Action	Administrator	Power User	User	Viewer
Report Problem	Yes	No	No	Yes
Reset	Yes/4 Eye	No	No	No
Update	Yes	No	No	No
Date and Time – Manual setting	Yes/4 Eye	No	No	No
Date and Time – Automatic setting	Yes	No	No	No
Language	Yes	No	No	No
Enable NanoVolume (C40)	Yes	No	No	No
Add Dyes	Yes	Yes	No	No
Dyes show toggle switch	Yes	No	No	No
Delete Dyes/Change Dyes	No	No	No	No
Change Warning Messages	Yes	No	No	No
Change Network (Settings, WLAN)	Yes	No	No	No
Change Printer (Network printer, Report Configuration)	Yes	No	No	No
CFR21 Off	Yes/4 Eye	No	No	No
Add Admin/Power User Account	Yes	No	No	No
Add Group	Yes	No	No	No
Add User Account	Yes	Optional	No	No
Set temporary password for lost password or misentry of password	Yes	No	No	No
Change own password	Yes	Yes	Yes	No
4 Eye Administrator	Yes/4 Eye	No	No	No
Secure Password	Yes/4 Eye	No	No	No
Password Expiry	Yes/4 Eye	No	No	No
Audit Trail	Yes	Yes read only	No	Yes
Audit Trail Search	Yes	Yes read only	No	Yes
Saving of Audit Trail	Yes	No	No	Yes
Save parameter as Stored Method	Yes	Yes	No	No
Change parameters in opened Stored Method	Yes	Yes	No	No
Delete Stored Methods	Yes/4 Eye	No	No	No
Rename Folder	Yes/4 Eye	No	No	No
Delete Folder	No	No	No	No
Move Folder	No	No	No	No
Delete Result File	Yes/4 Eye	No	No	No
Rename Result File	Yes	Yes	No	No
Move Result File	No	No	No	No
Delete Results	Yes	No	No	No

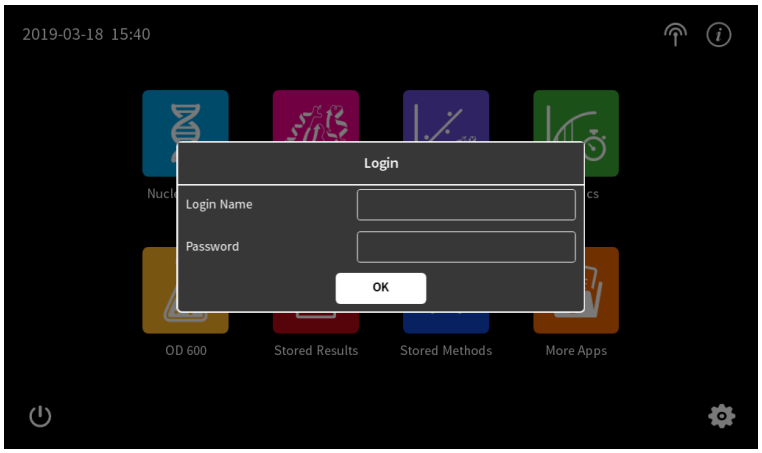
Note: User rights cannot be changed (with the exception of the Power User's ability to add new User accounts, which can be enabled/disabled).

Note: Only functions with restriction are listed. NPOS functions not listed in the table above are available for all user roles (administrator, power user and user).

Note: The Viewer account is designed for Audit purposes. This account has the ability to view all functions (as read only); view all methods and results (and save to a USB); and has full access to the Audit Trail, which they can also save to a defined location.

6. LOGIN TO THE NPOS SOFTWARE

If the CFR21 software is enabled a login is necessary for any action.



To login enter the Login Name and password and confirm with OK.

Note: If another user is logged in e.g. with a control device (computer) it is not possible to login to the NanoPhotometer® directly unless the logged in user logs off or a forced log off is requested with an Administrator account.

AUTOMATIC LOG OFF

There is an automatic screen lock if the NanoPhotometer® is inactive for 10 minutes. The screen can only be unlocked by the logged in user or with a forced log off by an administrator.

SCREEN LOCK

The screen can be locked in all method by pressing the icon in the navigation bar.

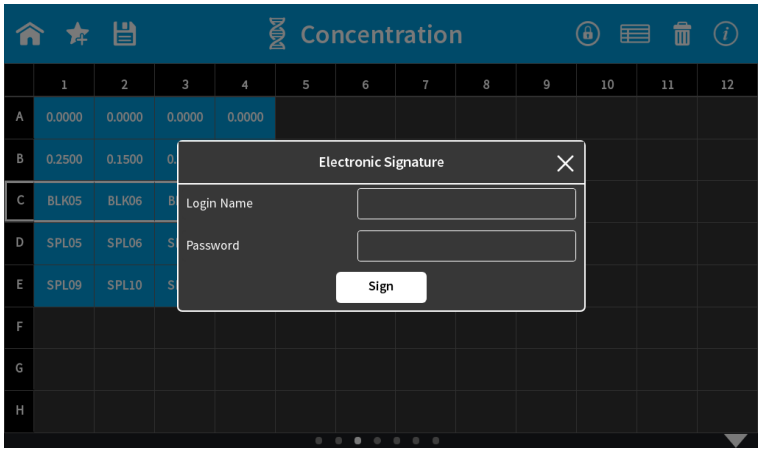
Note: A locked screen can only be unlocked by the logged in user or with a forced log off by an Administrator.

LOG OFF

Log off is only possible on the home screen by pressing the icon.

7. ELECTRONIC SIGNATURE

The electronic signature is set by default and cannot be disabled. Saving measurement data needs to be confirmed by the logged in user (Electronic Signature: Login Name and Password).



All saved file reports include the author, User ID, User Name, and date and time of the electronic signature. IDS and PDF files cannot be altered.

A second signature is shown as Read/Save/Print if an IDS file is opened and data are printed or exported as an Excel/PDF file. The second signature is the electronic signature of the logged-in user at the time of printing or data export.

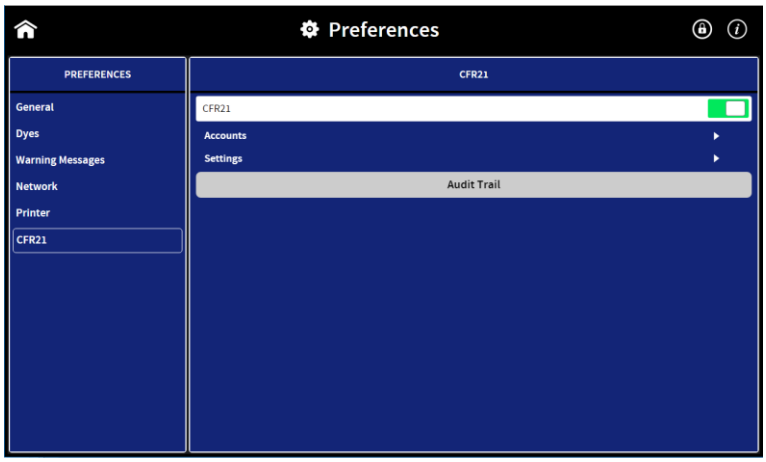
Implen NanoPhotometer®

Instrument Type	NP80	
Version	NPOS 4.2 build 14756	
Serial Number	M80945	
Selftest passed	2019-08-23; 13:17	
Autosave	No	
File Name	Gruppe_A/bjones/Header.ids	
Reason	Author	Read/Save/Print
User ID	bjones	msmith
User Name	Becky Jones	Mark Smith
eSign Date	2019-08-23	2019-08-23
eSign Time	13:25:16	13:27:35

8. Audit Trail

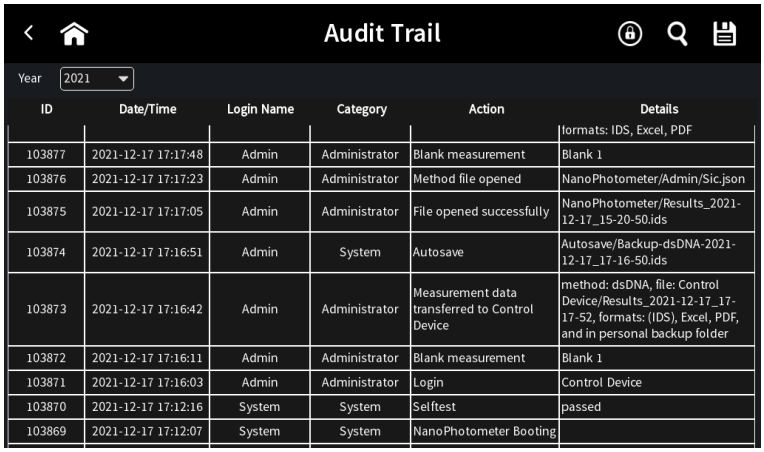
The audit trail function is automatically activated with CFR21 software activation. The audit trail records all actions and preference changes in an audit log. There is no delete or reset option for the audit trail available.

Analyzing and viewing the audit trail is possible as a logged-in Administrator, Power User or Viewer by opening the CFR21 preferences:



The audit trail opens a table including the following information for each recorded action and preference change: ID, Date/Time, User ID, Category, Action and Details. The entries are sorted by year. The year can be changed with the dropdown above the table.

Note: Power User has only reading permissions and cannot save the audit trail.



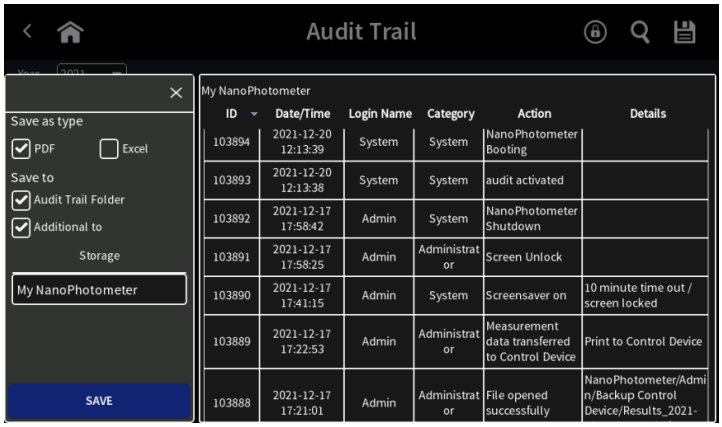
ID	Date/Time	Login Name	Category	Action	Details
					formats: IDS, Excel, PDF
103877	2021-12-17 17:17:48	Admin	Administrator	Blank measurement	Blank 1
103876	2021-12-17 17:17:23	Admin	Administrator	Method file opened	NanoPhotometer/Admin/Sic.json
103875	2021-12-17 17:17:05	Admin	Administrator	File opened successfully	NanoPhotometer/Results_2021-12-17_15-20-50.ids
103874	2021-12-17 17:16:51	Admin	System	Autosave	Autosave/Backup-dsDNA-2021-12-17_17-16-50.ids
103873	2021-12-17 17:16:42	Admin	Administrator	Measurement data transferred to Control Device	method: dsDNA, file: Control Device/Results_2021-12-17_17-17-52, formats: (IDS), Excel, PDF, and in personal backup folder
103872	2021-12-17 17:16:11	Admin	Administrator	Blank measurement	Blank 1
103871	2021-12-17 17:16:03	Admin	Administrator	Login	Control Device
103870	2021-12-17 17:12:16	System	System	Selftest	passed
103869	2021-12-17 17:12:07	System	System	NanoPhotometer Booting	

Saving of Audit Trail

The audit trail can be saved as a PDF or Excel file (Administrator and Viewer only). The selected year is saved. It is not possible to save the complete audit trail.

Note: To save audit trails for a defined time period, use the Audit Trail Search function.
Note: A maximum of 50,000 entries can be saved in one file.

Saved audit trail files are always saved in the Audit Trail folder. It is possible to select an additional folder location by selecting Additional to.

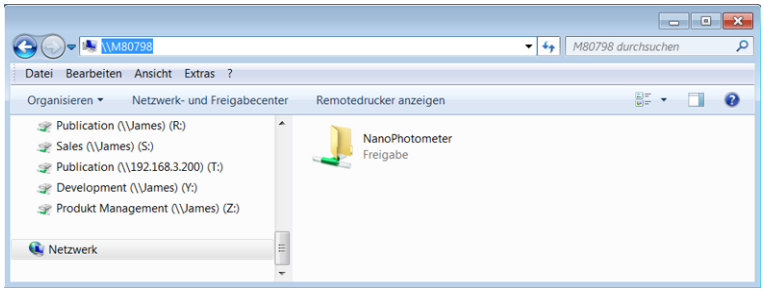


The audit trail folder can only be accessed by Administrators and Viewers via file server access. The folder NanoPhotometer_Admin contains all relevant files including the audit trail. Connection options are LAN/WLAN, USB cable or WiFi Hotspot.

- **File Server Access via LAN/WLAN**

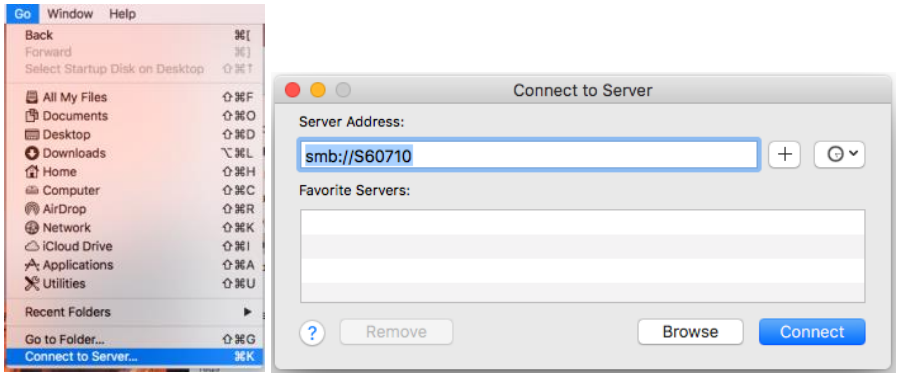
For the file server access via LAN/WLAN it is necessary that both the computer and the NanoPhotometer® are connected to the same LAN/WLAN network.

For **Windows computer** open the Windows explorer and enter the serial number or the NanoPhotometer® IP in the address bar of the Windows Explorer (e.g. \\M80798\ or \\Assigned IP Address\).



Note: Serial number and IP address of the NanoPhotometer® can be found in the NanoPhotometer® software under Preferences/General/About.

For a **MAC computer** open the "Connect to Server" dialog in the "Go" menu of the Mac OS X Finder and enter the NanoPhotometer® serial number or the active NanoPhotometer® IP address in the server address field to connect.



Note: Serial number and IP address of the NanoPhotometer® can be found in the NanoPhotometer® software under Preferences/General/About.

- **File Server Access via USB cable**

For file server access via USB cable connection, connect the NanoPhotometer® with a USB A/B cable to the computer and open the Windows Explorer or Connect to Server option for Mac (see file server access via LAN/WLAN) and enter \\192.168.7.1\ for connection.

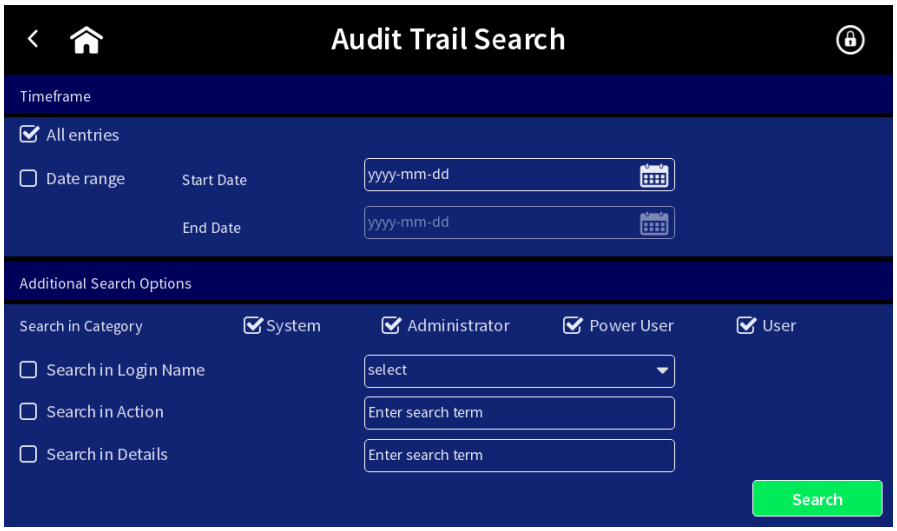
- **File Server Access via WiFi Hotspot**

For file server access via WiFi Hotpot the WiFi Hotspot needs to be active on the NanoPhotometer®. The computer needs to be connected to the NanoPhotometer® WiFi Hotspot (SSID: NanoPhotometer® serial number; password: Implenuser).
Open the Windows Explorer or Connect to Server option for Mac (see file server access via LAN/WLAN) and enter \\192.168.8.1\ for connection.

9. AUDIT TRAIL SEARCH

The audit trail search function provides the option to search in the audit trail by time period, category (administrator, power user, user, viewer), login name action or details.
To open the audit trail search function press the magnifier icon on the top right in the audit trail.
It is possible to search for a time period (timeframe) and additional search options.

Once all search parameter are selected, press the search button to start the search. The search result will be displayed as table.



TIMEFRAME

Either all entries or date range needs to be selected.
Selection of:

All entries: search is done in all audit trail entries. If no further search option is selected the complete audit trail is shown.

Date Range: option to enter a start and end date to limit the search period. Date can be entered by keyboard or time picker. Date needs to be entered in the following format: yyyy-mm-dd (year-month-day).

ADDITIONAL SEARCH OPTIONS

There are four additional search options available: Category, login name, action and details.

Category: At least one category needs to be selected.

Login name: Dropdown shows all available login names depending on category selection

Action: Free text field to search in the action table column of the audit trail.

Details: Free text field to search in the details table column of the audit trail.

AUDIT TRAIL SEARCH RESULT

The audit trail search result is shown in table format:

ID	Date/Time	Login Name	Category	Action	Details
103886	2021-12-17 17:20:34	Admin	Administrator	File opened successfully	NanoPhotometer/Admin/Backup Control Device/Results_2021-12-17_17-17-52.ids
103885	2021-12-17 17:19:35	Admin	Administrator	Method file opened	NanoPhotometer/Admin/Sic.json
103884	2021-12-17 17:19:15	Admin	System	Autosave	Autosave/Backup-CreateStandardCurve-2021-12-17_17-19-14.ids
103883	2021-12-17 17:19:15	Admin	Administrator	Method closed without saving data	Autosave/Backup-CreateStandardCurve-2021-12-17_17-19-14.ids
103882	2021-12-17 17:18:59	Admin	Administrator	Blank measurement	Blank 1
103881	2021-12-17 17:18:57	Admin	Administrator	Measurement continued	Previous results deleted, original IDS file still available
103880	2021-12-17 17:18:36	Admin	Administrator	File opened successfully	NanoPhotometer/Admin/Sic.ids
103879	2021-12-17 17:18:26	Admin	System	Autosave	Autosave/Backup-CreateStandardCurve-2021-12-

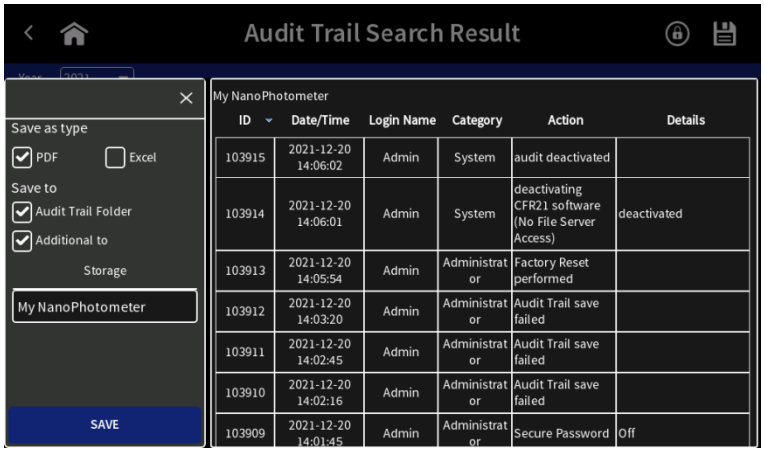
Year dropdown is only shown if the search result contains more than 1000 entries.

SAVING AUDIT TRAIL SEARCH RESULTS

The audit trail search result can be saved as a PDF or Excel file (Administrator and Viewer only). The complete search result is saved independent of the year dropdown selection. A maximum of 50,000 entries can be saved in one file.

Note: Change search parameter / time period of search if search result has more than 50,000 entries.

Audit trail files are always saved in the Audit Trail folder. It is possible to select an additional folder location by selecting Additional to.



The audit trail folder can only be accessed by Administrators and Viewers via file server access.

Note: Power user has only reading permissions and cannot save the audit trail.

10. Password Loss/Misentry

If a Power User/User/Viewer has lost the login password or entered it three times wrong, an Administrator can change the password of the Power User/User/Viewer in the account settings (Preferences) to a temporary password. The Power User/User/Viewer/secondary Admin accounts will be prompted to change the temporary password after the first login.

Administrator passwords cannot be recovered, if an administrator has lost the password please contact the Implen support team (support@implen.de).

11. VERSION HISTORY

Version	Date	Changes
1.0	August 2019	Initial Release
1.1	May 2020	Change of firmware version number in CFR21 Software Statement
1.2	March 2021	- Change of firmware version number in CFR21 Software Statement - Power User can read audit trails - Note / warning message added that administrator passwords cannot be recovered. Implen support is necessary.
2.0	January 2022	- Saving of Audit Trail (Excel and folder selection) - Audit Trail Search - User rights updated (Audit Trail Search)
3.0	March 2024	- Change of firmware version number in CFR21 Software Statement - New CFR21 role: Viewer - New preference – Administrator can enable/disable permission for Power Users to add new Users.

12. APPENDIX

CFR21 SOFTWARE STATEMENT

Paragraph	Summary	Features
11.10 Controls for closed systems		
11.10 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	Controls for closed systems	The NanoPhotometer® Software NPOS 4.2.14756 and higher contains the optional CFR21 feature. Once this CFR21 feature is activated all these requirements are fulfilled.
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	System validation	The complete NanoPhotometer® Software NPOS 4.6j.16350 and higher is validated by Implen to ensure accurate, reliable and intended performance of all the components of the NanoPhotometer® system. IQ/OQ procedures for proper function of the NanoPhotometer® instrument can be put in place. The proprietary file format IDS is protected by hash codes and encryption to allow identification of altered files.
(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.	Record generation and copying	In addition to the protected IDS files, all relevant measurement parameters and results can be exported to PDF using the PDF/A standard as well as Excel file format.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Record protection	Every export is accompanied with an IDS file, which is protected by hash codes and encryption to allow detection of tampering. At

		any time, PDF and Excel reports can be regenerated from these IDS files. Security measures for storage of these reports lie within the responsibility of the operating company.
(d) Limiting system access to authorized individuals.	Access limitation	Before any use of the system, every user is required to login for system access. Each user has a defined role, including access privileges.
(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.	Audit trails	Time-stamped audit trails are recorded for actions performed on the instrument by the user such as file storage, transfer activities and preference changes. The audit trails can be exported in PDF format. The creation and signature of the report files also creates an audit trail report entry. Reports cannot be overwritten.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Operational system checks	Not applicable.
(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.	Authority checks	It is ensured that users have the proper authority to carry out particular functions based on their roles and access privileges. It is the responsibility of the operating company to ensure that each user name can be traced to a real individual and to ensure correct assignment of roles.
(h) Use of device (e.g. terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Device/ terminal checks	Checks are applied to allow only valid information input in respective files. All CSV and JSON input files are checked to ensure valid content.
(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.	Training and user accountability	Implen Software Development team is fully and continuously trained. Implen provides NanoPhotometer® Software user trainings. The operating company is responsible for training on their SOPs in regard to electronic records and electronic signatures. Implen supports the installation of these SOPs in relation to NanoPhotometer® Software.
(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.	Policies	Responsibility of the operating company.
(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.	System Document Control	A release-specific software manual is distributed together with the NanoPhotometer® Software. NanoPhotometer® Software development is governed by a design and change control process that ensures the creation and tracking of relevant documents.

11.30 Controls for open systems.		
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.		Not applicable. The NanoPhotometer® operates as a closed system.
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.	Signature manifestations	The user management ensures that all user IDs are unique. (1) The system verifies the user credentials before creating any report (the user is required to re-enter his/her user ID and password). The protected IDS file as well as PDF and Excel files contain the user ID and the full name of the user. (2) The date & time when the signature was executed is associated with the signature. (3) The signature for creating the initial reports including the protected IDS file is indicated as “Author” as reason for signature. The signature for (re-)creating reports in PDF and Excel format are indicated as “Read/Save/Print” as reason for 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).	Signature in electronic records and in human readable form	User’s full name, date and time are included within the IDS file, which is protected by hash codes and encryption. When generating the human readable PDF and Excel files, the electronic signature is displayed with user ID, user’s full name, date & time, and reason.
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.	Signature/ record linking	The signature is integrated in the IDS file and can therefore not be excised, transferred or copied.
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.	Uniqueness of electronic signatures	The user management system ensures that all user IDs are unique. Therefore, all electronic signatures are unique.
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	Verification of identity	It is the responsibility of the operating company to ensure the identity of the individual at the time of creating the individual’s user account.

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	Certification	Responsibility of the operating company.
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.	Controls for electronic signatures	Users are requested to enter user ID and password for every signature action. In order to have access to a signature action, the user must have a user ID in the user management system and must be logged in with user ID and password.
(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.		
(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.		
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.		Not applicable.
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	Uniqueness of ID/	The user management system ensures unique

combined identification code and password, such that no two individuals have the same combination of identification code and password.	password	user IDs.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Password aging	The user management system provides password expiration and account locking after several authentication failures. Criteria can be set individually by the operating company.
(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.	Lost ID/ password management	The user management system allows an administrator to assign a new temporary password in case of lost, stolen or missing passwords. Proper loss management procedures are the responsibility of the operating company.
(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.	Controls to prevent unauthorized credential use	NPOS with activated CFR21 feature will lock the screen after an inactive period of time to prevent unauthorized attempted use. Other transaction safeguards such as supervision of blocked accounts etc. lies within the responsibility of the operating company.
(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.	Periodic testing of ID/ password generation	Responsibility of the operating company.

Important Notice: In accordance with FDA regulation, a vendor cannot claim that its software products are certified 21 CFR Part 11 compliant. A vendor, instead, can provide all Technical Controls for 21 CFR Part 11 compliance built into their product. As such Implen does not, at any time, imply that the use of any Implen CFR21 product will automatically give the customer protection to and therefore compliance with 21 CFR Part 11. It is the responsibility of the user to implement the Procedural and Administrative Controls (both correctly and consistently) along with using products with the correct Technical Controls for overall Part 11 compliance. All CFR21 systems must therefore be independently audited.

DISCLAIMER

THE WARRANTIES SET FORTH IN THE NANOPHOTOMETER MANUAL, ABOVE, ARE IN LIEU OF, AND THIS AGREEMENT EXPRESSLY EXCLUDES, ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, ORAL OR WRITTEN, INCLUDING, WITHOUT LIMITATION, (a) ANY WARRANTY THAT THE SOFTWARE IS ERROR FREE, WILL OPERATE WITHOUT INTERRUPTION, OR IS COMPATIBLE WITH ALL EQUIPMENT AND SOFTWARE CONFIGURATIONS; (b) ANY AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY; AND (c) ANY AND ALL WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE.

LIMITATION OF LIABILITY

IN NO EVENT SHALL LICENSOR OR ITS OWN LICENSORS AND SUPPLIERS BE LIABLE FOR ANY INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS, ARISING OUT OF OR IN ANY WAY CONNECTED WITH YOUR USE OF THE SOFTWARE OR ANY INFORMATION OR MATERIALS AVAILABLE THROUGH THE SOFTWARE, WHETHER BASED IN CONTRACT, TORT, STRICT LIABILITY, OR OTHERWISE, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. IN ADDITION, LICENSOR ASSUMES NO RESPONSIBILITY OR LIABILITY FOR ANY CLAIMS THAT MAY RESULT DIRECTLY OR INDIRECTLY FROM THE RESULTS YOU ACHIEVE USING THE SOFTWARE OR WHICH RELATE TO THE STORAGE OF ANY DATA OR FOR THE DELIVERY, SECURITY, OR AVAILABILITY OF ANY DATA. WITHOUT LIMITATION OF THE FOREGOING, TOTAL LIABILITY OF LICENSOR FOR ANY REASON WHATSOEVER RELATED TO THE SOFTWARE, THE USE OR INABILITY TO USE THE SOFTWARE, OR FOR ANY CLAIMS RELATING TO THIS EULA SHALL NOT EXCEED IN THE AGGREGATE US$5,000.

13. ALPHABETICAL INDEX