naica System Pro Software

User Guide

naica Data Service version 1.0
naica Reader Pro version 4.0
naica Analysis Pro version 4.1

BIO-RAD

naica System Pro Software

User Guide

naica Data Service Version: 1.0

naica Reader Pro Version: 4.0

naica Analysis Pro Version: 4.1

For 21 CFR Part 11 compliance

Technical Support Department

Email: Support-stilla@bio-rad.com

Monday to Friday, 9:30 am – 6:30 pm, Central European Time (CET)

Legal Notices

Revision History

Document	Date	Description of Change
naica System Pro Software User Guide (Doc ID 10000255612)	January 2026	Initial release

Table of Contents

Revision History i

Chapter 1 Overview 4

About the Software 4

Terms and Condition of Use 8

Incompatibility with Crystal Reader and Crystal Miner Software 9

Intended Use 9

Chapter 2 naica Data Service User Roles and Permissions 11

naica Data Service Permissions 11

naica Data Service User Roles 14

Default User Roles 14

naica Data Service Custom User Roles 16

Creating a Custom Role 16

Updating an Existing Role 17

Deleting an Existing Role 17

Managing Users 18

Users Menu 19

Deleting a User Account 20

naica Data Service Audit Trail 20

Users Tab 21

Roles Tab 21

Electronic Records Tab 22

Backing Up the System 23

Chapter 3 Using naica System Pro Software 24

Individual User Authentication 25

naica Reader Pro Scanning Template Files 26

Registering Default Scanning Template Files in naica Data Service 27

Creating New Custom naica Reader Pro Scanning Template Files 28

naica Reader Pro Sample Validation 30

Validating Samples for Pooled Chambers 30
Electronic Signatures Section 31
Experiment Audit Trail 33

Appendix A naica System Pro Software Installation 34
naica System Pro Software Installation Options 36
Installing naica System Pro Software Using Active Directory Authentication and a PC as a Server 37
Installing naica System Pro Software Using Active Directory Authentication and the naica System as a Server 38
Using Local Windows User Account Authentication on a Single naica System Instrument 39
Installing naica Data Service 42
naica Data Service System Requirements 42
naica Data Service System Prerequisites 42
Microsoft Windows Active Directory User Authentication Service 43
naica Data Service Download and Installation 44
Configuring the naica Data Service Web Interface 48

Chapter 1 Overview

This document explains how to install and operate the following naica™ System Pro software applications:

- naica Data Service
- naica Reader Pro
- naica Analysis Pro

This user guide only describes the software features that specifically support 21 CFR Part 11 compliance in the naica System Pro software.

The naica Reader Pro and naica Analysis Pro share common features with the standard RUO software Crystal Reader and Crystal Miner, respectively. General software features shared by the 21 CFR Part 11 naica System Pro software, naica Reader Pro, naica Analysis Pro, and their equivalent RUO software (Crystal Reader and Crystal Miner) are described in the Crystal Reader and Crystal Miner User Manuals.

All user guides are available at bio-rad.com/naica-pro-software.

About the Software

The naica System Pro software enables naica system users to meet the Food and Drug Administration's regulations for good laboratory practices (GLP) as well as good manufacturing practices (GMP) in pharmaceutical and biotechnology environments. When enabled, naica System Pro software provides the necessary features to permit the naica system to operate in compliance with Title 21 of the U.S. Code of Federal Regulations Part 11 (21 CFR Part 11), within a closed system. A closed system is defined as "an environment in which system access is controlled by the persons who are responsible for the content of electronic records that are on the system".

Note: The security controls built into naica System Pro software must be properly configured and administered by the naica system administrator(s) in the customer's organization to be secure and in compliance with 21 CFR Part 11.

Bio-Rad makes no claim that naica system Pro software is 21 CFR Part 11 compliant in and of itself, nor does the company guarantee compliance for the user. The naica system user organization must establish policies and standard operating procedures (SOPs) that work in conjunction with the tools provided by Bio-Rad to ensure compliance with 21 CFR Part 11.

Table 1 provides an overview of the 21 CFR Part 11 requirements supported by the naica System Pro software. To ensure full compliance with all sections of 21 CFR Part 11, responsibilities that a user organization's Standard Operating Procedures (SOPs) must address by the are marked with an “X”.

Table 1. 21 CFR Part 11 requirements and responsibilities

Section	Subject	User’s Organization	naica System Pro software	Compliance Management
11.10 (a)	Validation	X	X	The naica System Pro software supports system and experiment result validation. The user organization's SOPs are required for validation
11.10 (b)	Human readable records	N/A	X	All electronic records are kept within the naica System Pro software environment until the user transfers them to external electronic archives in line with user´s organization policies
11.10 (c)	Protection of records	X	X	All electronic records are kept within the naica System Pro software environment until the user transfers them to external electronic archives in line with user´s organization policies.
11.10 (d)	Limited system access	X	X	Control of access to naica System Pro software through individual user authentication.

Section	Subject	User's Organization	naica System Pro software	Compliance Management
11.10 (e)	Audit trails	X	X	naica System Pro software tracks changes in an audit trail which does not expire. The creation of backups is under the responsibility and control of the user´s organization.
11.10 (f)	Operating system checks	X	X	naica System Pro software provides guidance and checks for setting up an experiment. naica System Pro software provides a default experiment template that can be customized. Customized assays can be released for routine workflows following validation by the user.
11.10 (g)	Authority checks	X	X	Control of access to naica System Pro software by individual authentication and user role assignments. User cannot modify electronic records. Protocol modification require specified permissions and requires validation prior to release for routine workflow.

Section	Subject	User's Organization	naica System Pro software	Compliance Management
11.10 (h)	Device checks	X	X	Experiment configuration and parameters are checked by the naica System Pro software. The sample ID input and template file validation is under the responsibility and control of the user´s organization.
11.10 (i)	Determination of education	X	X	User guides and training documentation are provided by Bio-Rad. Establishing and maintaining the appropriate training level is the responsibility of the user´s organization.
11.10 (k)	System documentation	X	X	naica System Pro software documentation cannot be changed by the user. The distribution of documentation to the users and version control of the documentation is the responsibility of the user´s organization.

Section	Subject	User's Organization	naica System Pro software	Compliance Management
11.100 (a)	Electronic Signature general requirements	X	X	Unique to individual users
11.100 (b)		N/A	X	Verification of identity
11.100 (c)		N/A	X	Signature with username and password ensure genuine owner
11.20 (a/b)	Electronic Signature components and control	N/A	X	Signature with username and password ensures genuine owner
11.300 (a)	Controls for identification username and passwords	X	X	Uniqueness of username and password
11.300 (b)		X	X	Periodic check of issuance
11.300 (c)		X	X	Loss management
11.300 (d)		X	X	Safeguards and detection of unauthorized attempts

Terms and Condition of Use

Bio-Rad grants a personal, non-exclusive, and non-transferable license to use the naica System Pro software, but only to the extent that the software components are described in this document.

Customers must comply with all of the terms and conditions of use of thenaica System Pro software, as well as any third-party software, which are set out in the license included in this document.

Subject to any applicable mandatory law provisions, the customer cannot:

- Modify, adapt, or alter the naica System Pro software

- Decompile, disassemble, or reverse engineer in any manner the naica System Pro software, in whole or in part
- Use the naica System Pro software for any purposes other than its intended use
- Sub-license or grant access to the naica System Pro software to third parties
- Copy the naica System Pro software and its documentation

The customer is also subject to the same prohibitions and restrictions for any third-party software used or embedded in the naica system. The customer must also comply fully with the terms of use and licensing requirements set by third-party owners.

Incompatibility with Crystal Reader and Crystal Miner Software

The Crystal Reader and Crystal Miner software are not 21 CFR Part 11 compliant. The following restrictions apply when using these programs with files from naica Reader Pro or naica Analysis Pro:

- Files from naica Reader Pro and naica Analysis Pro are not compatible with Crystal Reader or Crystal Miner.
- Editing naica Reader Pro or naica Analysis Pro files using Crystal Reader or Crystal Miner version 4.0 is prohibited.
- Editing these files using Crystal Reader or Crystal Miner version 3.1 or earlier is not prohibited, but it will corrupt the experiment files and templates.

Intended Use

The naica System Pro software includes the following products:

- **naica Data Service** – The naica Data Service functions as the naica system user account manager and ensures that all naica system operations comply with 21 CFR Part 11 regulations.
- **naica Reader Pro** – The naica Reader Pro application serves as the operating interface to define the experimental settings for the image acquisition on the Prism3 / Prism scanner in the Crystal Digital PCR workflow. The naica Reader Pro is the 21 CFR part 11 software equivalent of the standard RUO Crystal Reader software.
- **naica Analysis Pro** – The naica Analysis Pro software is the data analysis application of the naica system. The naica Analysis Pro analyzes image data acquired from the naica Analysis Pro, and calculates the absolute concentrations of targeted nucleic acids. The naica Analysis Pro is the 21CFR part 11 software equivalent of the standard RUO Crystal Miner software.

All naica System Pro software products are intended for use by laboratory personnel trained in the techniques of Crystal Digital PCR.

The naica Data Service, naica Reader Pro, and naica Analysis Pro are intended to be used only with naica system.

The naica Data Service, naica Reader Pro, and naica Analysis Pro are compliant with 21 CFR Part 11.

All products are for research use only, and are not to be used for diagnostic procedures.

Chapter 2 naica Data Service User Roles and Permissions

This section explains how the naica Data Service user roles and their permissions.

naica Data Service Permissions

The naica Data Service assigns predefined sets of operational permissions to users based on their roles. These roles control access to features in the naica Reader Pro and naica Analysis Pro.

Permission details include:

- Permissions are managed under the Roles / Permission tab in the naica Data Service interface.
- Granted permissions are shown with a check mark; those not granted are unchecked.
- Users are responsible for assigning roles and limiting Manage Users permission to authorized personnel.

Available permissions include:

- **Create Templates** – This permission allows the user to:
  - Register default scanning template files supplied by Bio-Rad for the naica Data Service so they can be used by users who have the Run Experiment permission on the same naica Data Service
  - Create and customise scanning template files (.ncx format). The creation and customization of scanning template files is registered in the so they can be used by users who have the Run Experiment permission on the same naica Data Service
  - Edit the Experiment Details, Embedded Files and Scanning Parameters of the scanning template.

  Note: For better traceability, Bio-Rad recommends using Bio-Rad scanning templates for the first few optimized assay runs to define the final scanning template parameters. For routine use, Bio-Rad recommends using only specific, customized scanning template parameters.

  For more information on releasing a new or an imported scanning template, see naica Reader Pro Scanning Template Files on page 26.
- **Edit Scanner Settings** – Allows a user to configure the naica Reader Pro Settings page.

- **Export Data** – In addition to analytical data included in the 21 CFR Part 11 Regulatory Report, the Export Data permission allows a user with Export Data permission to export all the data files listed below using the naica Analysis Pro. Preselected data elements (greyed out) are always included in the data export. You can add additional data elements by selecting their checkboxes.

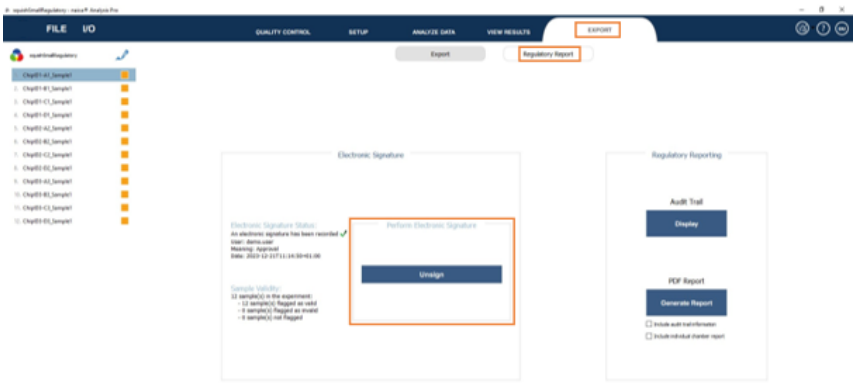
Note: After exporting, you can edit XLSX and CSV files outside the naica System Pro software, but these changes are not recorded in the Experiment Audit Trail. Use only the generated PDF report for sample results reporting to remain compliant with 21 CFR Part 11.

- **Generate PDF Report** — Allows the user to create and export a 21 CFR Part 11-compliant PDF report of electronically signed experiments using naica Analysis Pro. This option allows you to include the experimental audit trail information as part of the PDF report.

  Note: The Validate Experiments permission is required to electronically sign an experiment.

- **Invalidate Experiments** — Allows the user to remove another user's existing electronic signature. After removing the signature, the user can make further data edits or modifications.

  In GMP and GLP environments, organizations often follow a “two-man rule” or “four-eye principle,” requiring a second person to review results as a control to ensure data security. Under this rule, more than one authorized person must have access to data and the ability to modify results. The Invalidate Experiments permission enforces this hierarchy while maintaining full compliance with 21 CFR Part 11. For more information, see Electronic Signatures on page 1.



- **Manage Users** — Allows the user to
  - ☐ Assign a role to a user
  - ☐ Create, edit, or delete user roles and permissions

  Note: Only users with the Manage Users permission can create, modify, or delete user roles and user permissions.
- **Run Experiments** — Allows the user to run experiments with naica Reader Pro. Users with this permission can scan experiments, re-scan experiments, and save experiments.

  Note: Users with the Run Experiments permission who do not have the Create Templates permission must use existing scanning template files previously registered by a user with the Create Templates permission in the naica Data Service software to scan an experiment.
- **Validate Experiments** —A llows the user to analyze the results of each individual sample in an experiment run using the naica Analysis Pro Result Table .

Users with the Validate Experiments permission can also electronically sign the validated result of the entire experiment in the Regulatory Report page of thenaica Analysis Pro Export menu. For more information, see Electronic Signatures on page 1.

naica Data Service User Roles

Users with the Manage Users permission can assign user roles on the naica Data Service Roles / Permission tab.

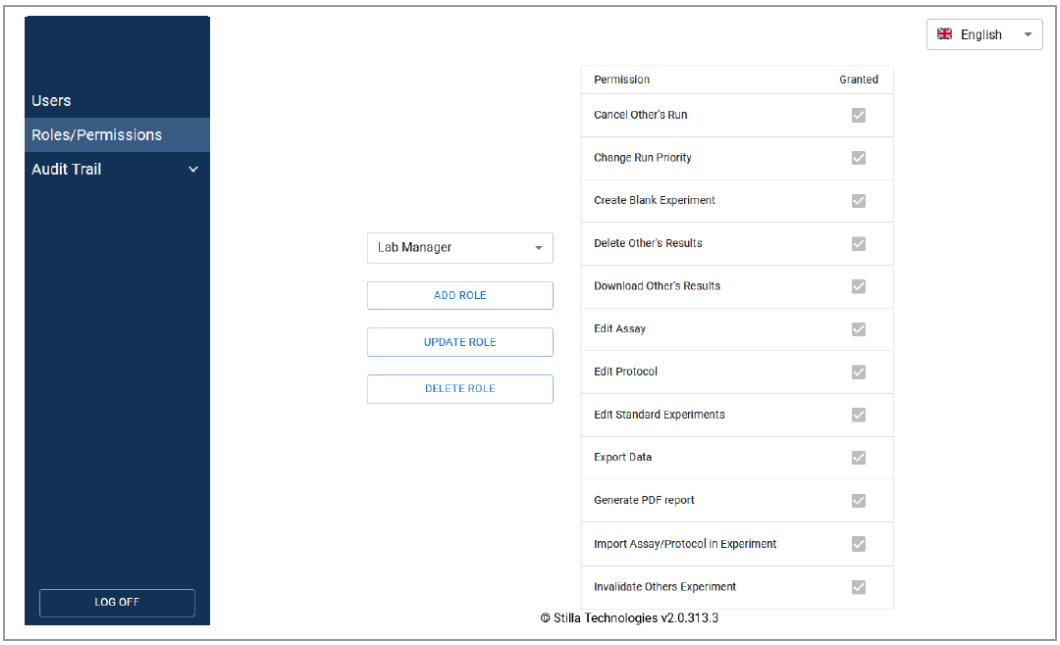
Roles details include:

- All available user roles are listed in a drop-down menu.
- Each user role determines the permissions assigned to users.
- Roles control access to predefined permissions for both naica Reader Pro and naica Analysis Pro applications.

Default User Roles

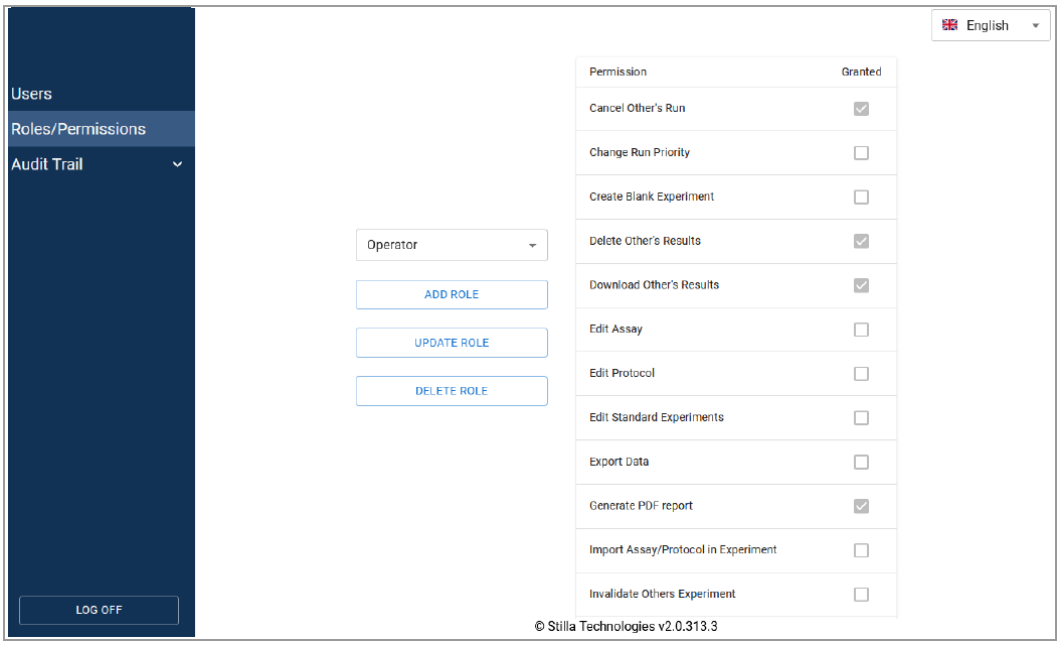
The naica Data Service installation includes two predefined user roles:

- **Lab Manager** — Lab managers have full permissions for naica Reader Pro and naica Analysis Pro.



- **Operator**— Operators have limited permissions for naica Reader Pro, including:
  - Generating PDF reports
  - Running experiments
  - Validating experiments

  The Operator role is restricted to validated standard experiment files that comply with the customer's SOP and have been approved by a Lab Manager for routine operation.



naica Data Service Custom User Roles

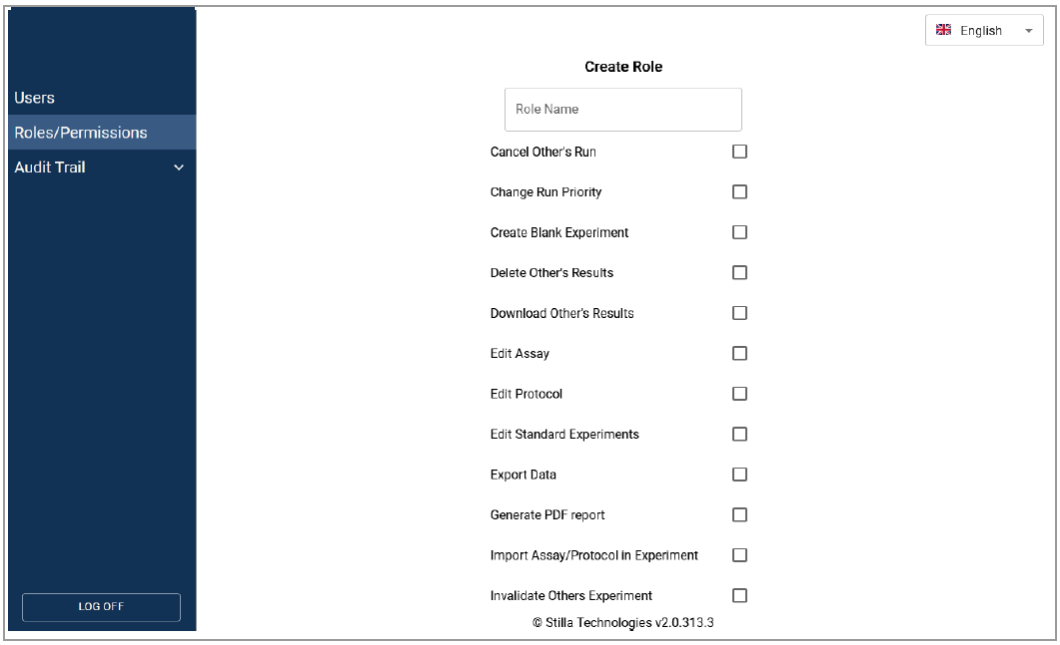
The naica Data Service enables users assigned Manage User permissions to create user roles or change existing user roles.

Creating a Custom Role

To add a user role

1. Open the Roles/Permissions Tab in the naica Data Service user interface.
2. Click Add Role to begin creating a new user role
3. Enter the role name in the designated field.
4. Select the role permissions by checking all permissions to be included in the new role.
5. Click Create Role.

   The new role appears in the User Role drop-down menu in the Roles/Permissions tab.



Updating an Existing Role

To update an existing role

1. Open the Roles/Permissions Tab in the naica Data Service user interface.
2. Click Update Role.
3. (Optional) Edit the Role Name.
4. Modify permissions by activating or deactivating permission settings.
5. Click Update Role. The updated role will appear in the User Role drop-down menu in the Roles/Permissions tab.

Changes take effect when assigned users log in to naica Reader Pro or naica Analysis Pro.

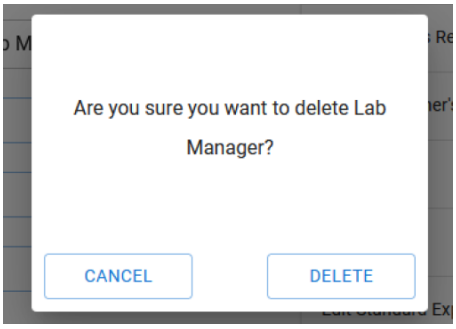
Deleting an Existing Role

To delete an existing role

Important: You cannot delete a role if it's assigned to on or more users.

1. Open the Roles/Permissions Tab in the naica Data Service user interface.
2. Select the role you want to remove.

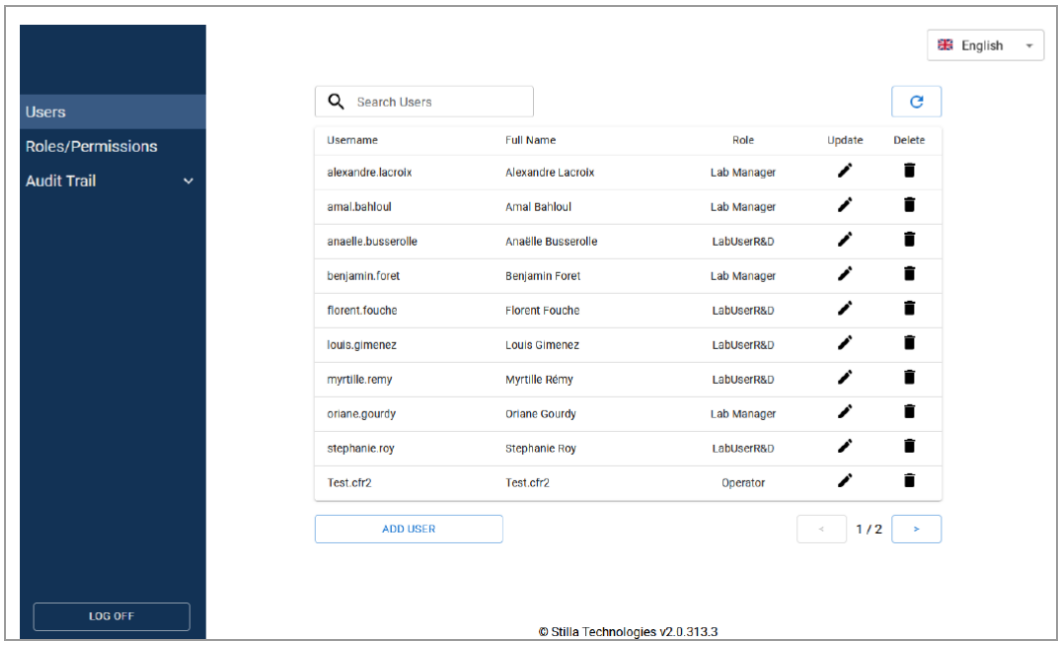
3. Click Delete Role,
4. In the confirmation modal, click Delete.



The deleted role is removed from the User Role drop-down menu in the Roles/Permissions tab.

Managing Users

To comply with 21 CFR Part 11, only authorized individuals can access naica Data Service. Additionally, each user must log in using individual credentials (username and password).



Users Menu

The users menu

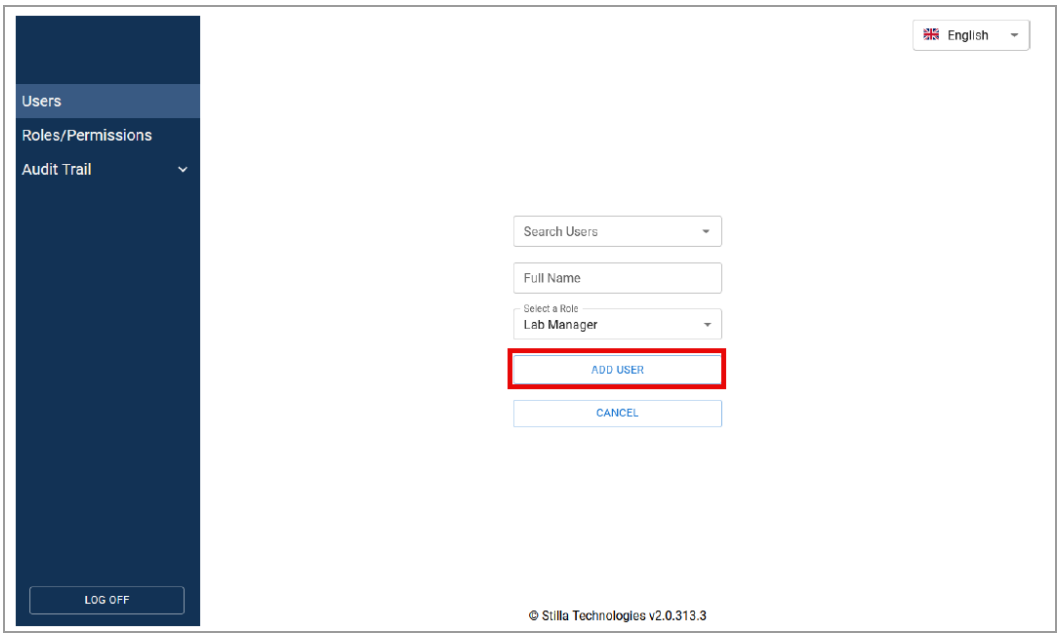
- Displays all naica Data Service user accounts within the organization.
- Lists users that can access all 21 CFR Part 11-compliant naica System software applications.

Only users with the Manage Users permission can add, update, or delete user accounts. To modify a user account, click on the respective icon in the Users menu.

Creating a New User Account

To create a user account

1. Navigate to the Users Menu and click Add User.



2. Enter the Microsoft Windows username in the Search Users field.

   Note: The username source depends on the organization's authentication setup:

   - Active Directory user authentication. For more information see Installing naica System Pro software Using Active Directory Authentication and a PC as a Server on page 1 and Installing naica System Pro software Using Active Directory Authentication and a the naica System as a Server on page 1.

- Local naica System authentication. For more information, see Using Local Windows User Account Authentication on a Single naica System Instrument on page 1.

3. Select the correct username from the list of matching accounts. The system automatically populates the Full Name field based on the Windows account.
4. Assign a User Role using the Select a Role drop-down menu.
5. Click Add User.

   The system activates the new user account, and the user can log in with their Windows authentication credentials.

   Note: Any inactive user will be automatically logged out to comply with 21 CFR Part 11. The system displays the login prompt after timeout.

Deleting a User Account

To delete a user account

1. Open the Users Menu in the naica Data Service interface.
2. Select the User Account to be deleted.
3. Click Delete.
4. Click Delete on the Delete User confirmation modal.

   The user account will be removed from the system.

naica Data Service Audit Trail

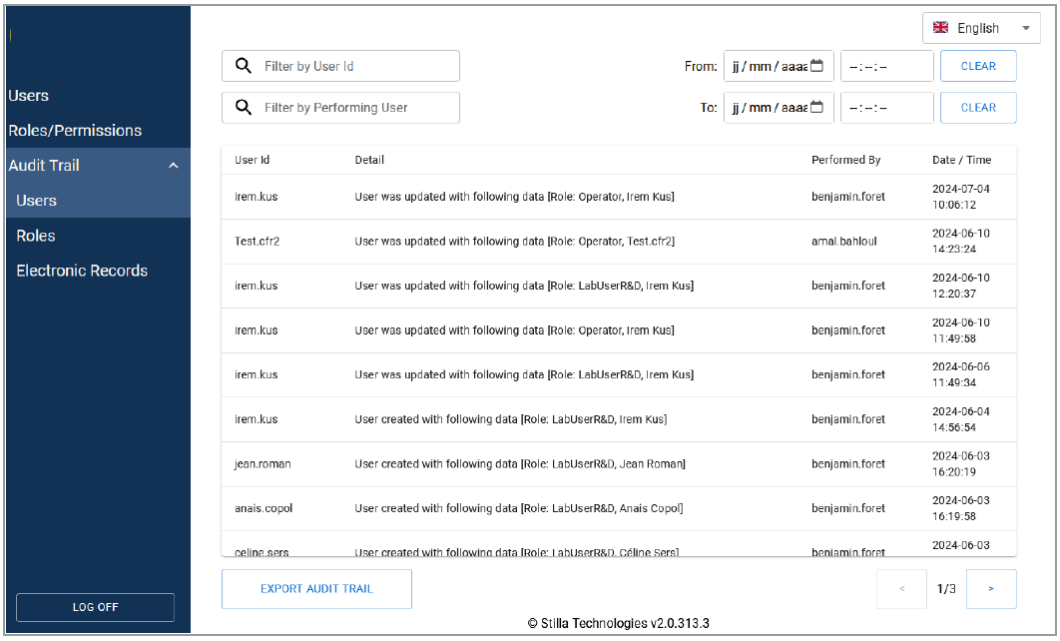
The naica Data Service Audit Trail automatically generates time-stamped electronic records that document the history of events related to the creation or modification of electronic records, based on individual user accounts.

The Audit Trail is divided into three categories, each with filtering options.

Users Tab

The Users tab

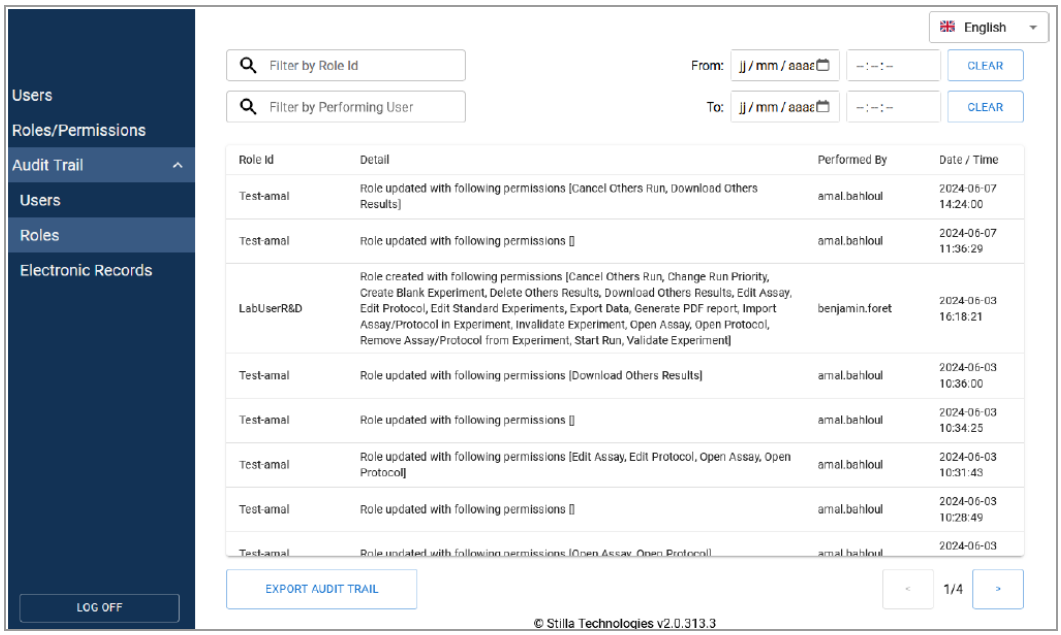
- Tracks changes to User Role management.
- Can be filtered by Role ID (the affected role)



Roles Tab

The Roles tab

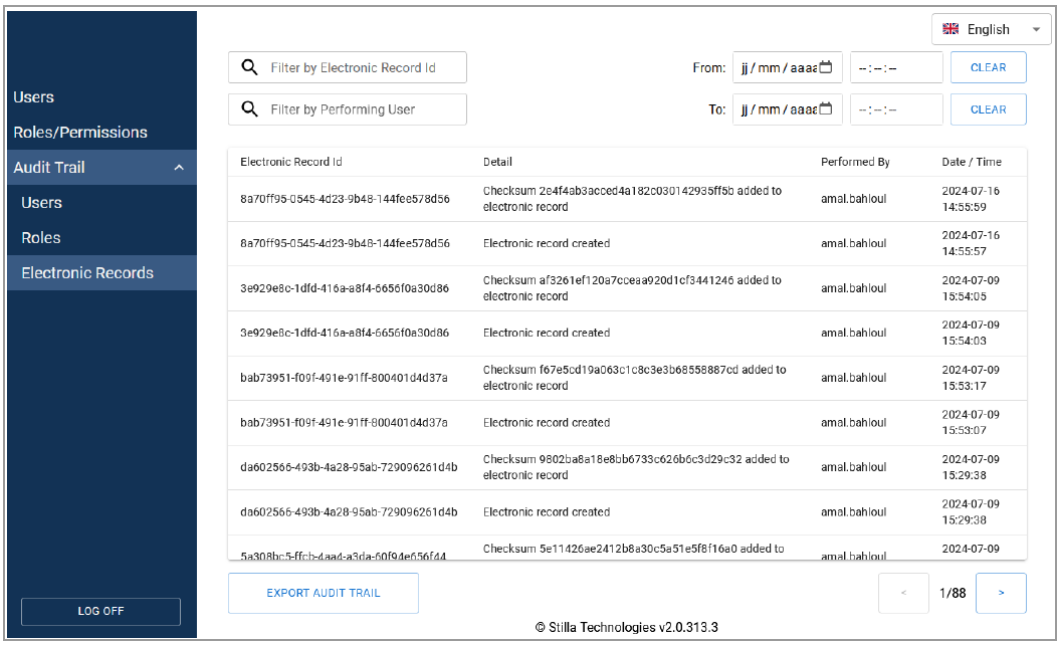
- Tracks changes to User Role management.
- Can be filtered by Role ID (the affected role)



Electronic Records Tab

The Electronic Records tab

- Logs the history of any naica System Pro software file.
- Can be filtered by Electronic Record ID (a unique ID created by naica Data Service for each naica System Pro software file).
- Includes an electronic record checksum (a condensed version of the naica System Pro software file) required by the naica Data Service to verify file integrity.



Backing Up the System

Regular backups of the naica Data Service Audit Trail database are essential. The database file is stored at: C:\Program Files\Bio-Rad\QX700DataService\Naica.db. Users are responsible for establishing and maintaining a backup routine to safeguard audit records.

To ensure consistent Audit Trails, all computers running 21 CFR Part 11 naica System Pro software must be correctly configured with the appropriate date and time settings. This responsibility of the user and the user's organization.

Audit trail categories in naica Data Service can be filtered by date and time to track events chronologically or by the Performing User (the naica Data Service user account executing the recorded event) to identify the user who executed a recorded action.

All naica Data Service audit trail categories can be exported as a PDF document by clicking EXPORT AUDIT TRAIL .

Chapter 3 Using naica System Pro Software

This section describes the naica Reader Pro and naica Analysis Pro 21 CFR Part 11 -compliant features.

All other general software features common to naica Reader Pro, naica Analysis Pro, Crystal Reader, and Crystal Miner software are described in the Crystal Reader and Crystal Miner User manuals, respectively.

All User Manuals are available at https://www.stillatechnologies.com/digital-pcr/naica-system-support/technical-resources/.

Individual User Authentication

To maintain 21 CFR Part 11 compliance, only authorized individuals may access naica Reader Pro and naica Analysis Pro. All users must log in to naica Reader Pro and naica Analysis Pro using their authenticated user ID and password.

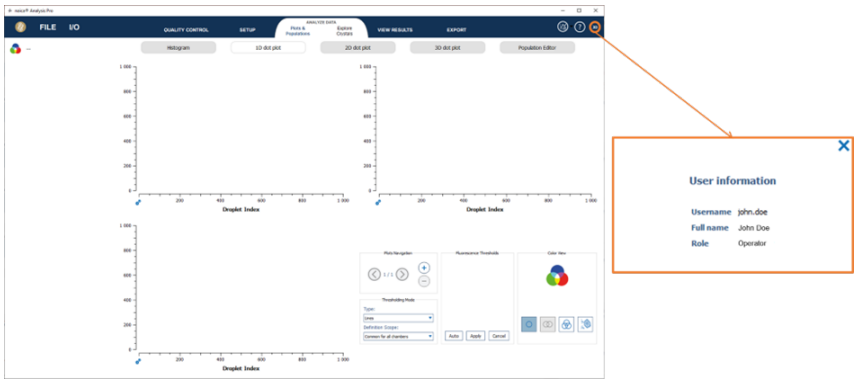
Note: The naica Data Service will lock out a user after too many failed login attempts. To reset credentials and reactivate the Windows account, contact your IT administrator. Connectivity issues with the naica Data Service can also prevent login. Contact your IT department to ensure proper connection.

If a user's session expires, naica Reader Pro and naica Analysis Pro will prompt for re-authentication. Attempting to bypass authentication will automatically close the software, potentially causing unsaved changes.

Automatic log-out is controlled by your organization's Microsoft Windows user account settings. However, always close all naica System Pro software applications when not in use.

Note: Login attempts can fail if Windows authentication is denied or if the software loses connection to the naica Data Service.

In naica Analysis Pro, the user can click the login icon to view individual User Information.



naica Reader Pro Scanning Template Files

To start a run, users must be assigned to a User Role with the Run Experiment permission and must use a scanning template registered with the naica Data Service. Scanning template files have the same file extension as naica experiment files (.ncx) but only contain the information required for scanning and data analysis. Scanning template files include:

- The following parameters and files required for scanning and image analysis, as defined in the naica Reader Pro:
  - An image analysis configuration file (.yaml) used for droplet recognition and concentration calculation depending on the combination of chip type and mix used. Image analysis configuration files are created and validated by Bio-Rad
  - Experiment details, which include the scanned channel information as well as the fluorophores and targets associated to each scanned channel
  - Scanning parameters, which include the exposure times for each channel scanned
- The following parameters and files required for data analysis, as defined in the naica Analysis Pro:
  - A spillover compensation matrix file (.ncm), which includes the compensation matrix parameters applied to the data during analysis
  - A plots configuration file (.ncp), which includes plot display and data visualization parameters in naica Analysis Pro
  - An analyzing configuration file (.nca), which includes the population and thresholding parameters for data analysis

  Important: Only users assigned to a user role with the Create Template permission can create and modify scanning template files.

.

Registering Default Scanning Template Files in naica Data Service

Bio-Rad can provide default scanning template files validated for different combinations of microfluidic chips and PCR mixes. Each default scanning template file includes:

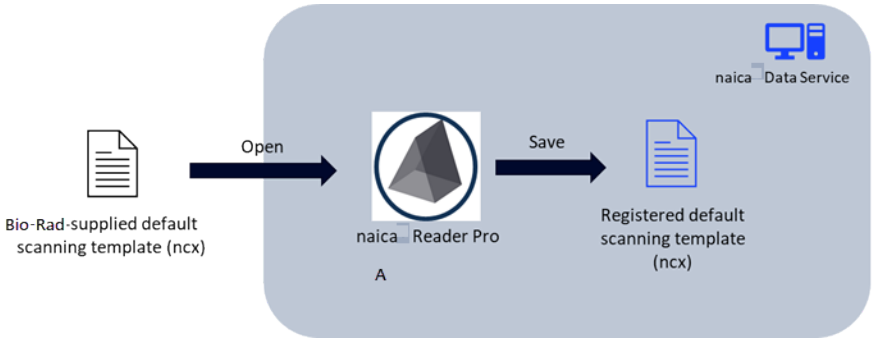
- A pre-defined image analysis configuration file
- Pre-defined, default scanning parameters

All other parameters and files of a default scanning template file are left blank.

Default scanning templates files provided by Bio-Rad are developed outside of the naica Data Service. Users must register with the naica Data Service before first use. Only users assigned a User Role with the Create Template permission can register default scanning template files.

To register a default scanning template file in naica Data Service:

1. In naica Reader Pro click New Experiment.
2. Select the default scanning template supplied by Bio-Rad.
3. Click on Save As to save the scanning template file in a dedicated folder. For more information, see Creating New Custom naica Reader Pro Scanning Template Files on page 28.

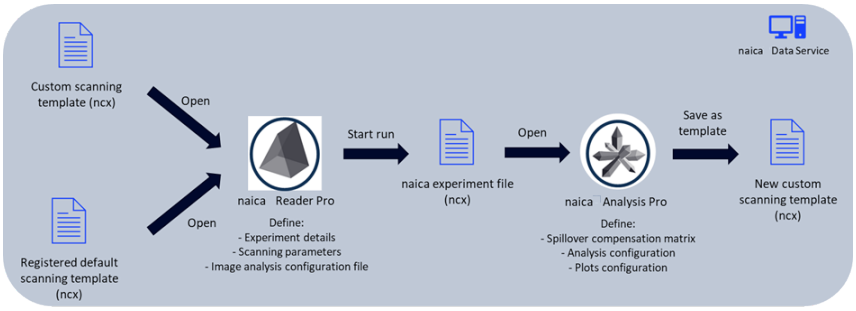


Creating New Custom naica Reader Pro Scanning Template Files

This section explains how to create a new custom naica System Pro software scanning template file.

To create a custom scanning template file

1. Open the naica Reader Pro and select New Experiment.
2. Select either a default scanning template file or another existing custom scanning template file.
3. Define the experiment details, scanning parameters, and image analysis file.
4. Start a run with relevant samples and assay. After the run completes, open the experiment file (.ncx) in naica Analysis Pro.
5. In naica Analysis Pro, define the spillover compensation matrix, analysis configuration (thresholding method and populations, and plots configuration.
6. In naica Analysis Pro, create the template by selecting Save as Template (.ncx) from the I/O menu, and choose a dedicated folder for storage.



Notes:

- Perform a series of assay-specific validation experiments to determine all final scanning template file parameters according to your organization's SOPs.
- As a good practice to ensure data integrity and traceability, all validated naica System Pro software default scanning template and analysis configuration files should use an identical naming structure, and no two scanning templates should have the same name. Bio-Rad recommends naming the scanning template as follows:

  ScanningTemplate_InstrumentName_ChipType_PCR-MixName_AssayIndicator_version.ncx

  - File Type: ScanningTemplate

- InstrumentName: Specify the validated naica® system scanner to use with this template, e.g., Prism3 or Prism6.
- ChipType: Specify the validated chip consumable for the template, e.g., SapphireChip or RubyChip.
- PCR-MixName_AssayIndicator:
- Specify either the validated reagent consumables used with the template, or
- Provide an application-specific indicator for the validated assay.
- Version: Use a version number to track template revisions. Increment the version after each modification.

- To comply with 21 CFR Part 11, Bio-Rad recommends storing scanning templates in a dedicated shared directory with Read-Only access.
- Users are responsible for ensuring full compliance with 21 CFR Part 11 for all customized scanning template files, including adherence to retention periods.
- For routine use, clearly specify the custom scanning template file to use in the Standard Operating Procedure (SOP) for each validated assay.

naica Reader Pro Sample Validation

To be able to sign and export the experiment results, naica Analysis Pro, you must review and flag each sample as valid or invalid.

- Sample acceptance criteria may vary by assay or application. Each organization must define and apply its own conformity criteria for experiments performed using the naica System.
- naica Analysis Pro flags each sample as valid or invalid in the Result Table section of the View Result tab.
- The experiment result table displays two columns: Valid Sample and Invalid Sample.
- By default, all samples have an undefined status. To apply the same status to multiple samples, select them while holding the Shift or Alt key, then click the desired validity status.

Validating Samples for Pooled Chambers

When using the Pooled Chamber feature, the validity status of individual sample chambers must match the pooled chamber result.

- If all individual sample chambers in a pooled chamber have the same validity status, the pooled chamber status is automatically set to that value.
- If the validity status of the individual sample chambers differs, the pooled chamber status remains undefined.

- You can also assign a validity status directly to the pooled chamber sample; doing so will overwrite the validity status of all individual sample chambers to match the pooled chamber status.

Electronic Signatures Section

The Electronic Signatures section consists of three areas: the Electronic Signature Status, the Sample Validity, and Perform Electronic Signature.

Electronic Signature Status

The Electronic Signature Status provides a summary of the electronic signature information for the experiment file. It also records the following:

- Whether the file has already been signed
- The user ID of the signer
- The meaning of the signature
- The date and time of the signature

Note: To sign an experiment electronically, you must first flag all samples in the experiment as valid or invalid on the Result Table page within the View Results menu. If any sample remains unflagged, a warning appears in the Perform Electronic Signature section, and the electronic signature cannot be completed.

Sample Validity

The Sample Validity section displays a summary of the experiment's sample results, and records the following:

- The number of samples flagged as valid
- The number of samples flagged as invalid
- The number of samples not flagged

Perform Electronic Signature

To execute the electronic signature for an experiment file, you may optionally define the Meaning of the Electronic Signature.

- **Meaning of the Electronic Signature** – This field allows organizations to define a result-release hierarchy tailored to their processes while remaining fully compliant with 21 CFR Part 11.

  The default value is N/A In GMP/GLP environments, organizations often follow the "two-man rule / 4-eye principle", where results must be reviewed by a second person to ensure a high level of data security.

Individual meanings of electronic signatures must be defined within the organization's internal processes.

- **Sign** – To execute the electronic signature, you must confirm your identity by logging in again with your username and password. Signing acknowledges full accountability and responsibility for all actions that generated the reported Crystal Digital PCR results.

  Once signed, a signature icon ( ) appears next to the experiment name in the top-left corner of the experiment file. This icon remains visible in all naica Analysis Pro menus and visually indicates that the experiment has been electronically signed. All features that allow modifications to the experiment file are disabled, effectively locking the file.

- **Unsign** – The author of an electronic signature is always allowed to remove their own signature. To remove the electronic signature from an experiment, click the Unsign button and confirm your identity by logging in with your username and password.

  To edit an experiment file that was previously signed by a different author, you must have the Invalidate Experiment permission assigned to your User Role. If you do not hold this permission, the software will display a "Permission denied" message and prevent modifications.

Experiment Audit Trail

The Experiment Audit Trail records all edition events in naica Reader Pro and naica Analysis Pro applications for an experiment file. Events included in the Audit Trail record are:

- Scanning Template parameters Chip IDs Scanning parameters modifications
- Droplet recognition edition
- Sample edition
- Spill-over compensation edition
- Threshold or polygon position edition
- Electronic signature record of the experiment file including user identification and date and time stamp

The Experiment Audit Trail does not track events related to the Export page in the EXPORT menu. Export events are not in the scope of the Regulatory Report page. To produce a consistent Experiment Audit Trail, all computers running naica System Pro software applications must be configured with the correct date and time.

You can review the Experiment Audit Trail in the naica Analysis Pro software.

To open the Experiment Audit Trail viewer

1. Click on the EXPORT menu.
2. Click the Regulatory Report tab.
3. In the Regulatory Reporting section, click on Display under Audit Trail.

Appendix A naica System Pro Software Installation

This section explains the how to install the following:

- naica Data Service
- naica Reader Pro
- naica Analysis Pro

naica System Pro Software Installation Options

This section explains the naica System Pro software installation options. There are three ways to install the naica System Pro Software, depending on the customer's requirements and infrastructure. Each installation option requires a specific set of parameters:

- Using Active Directory authentication and a PC as a server
- Using Active Directory authentication and a the naica system as a server
- Using Local Windows user account authentication on a single naica system instrument

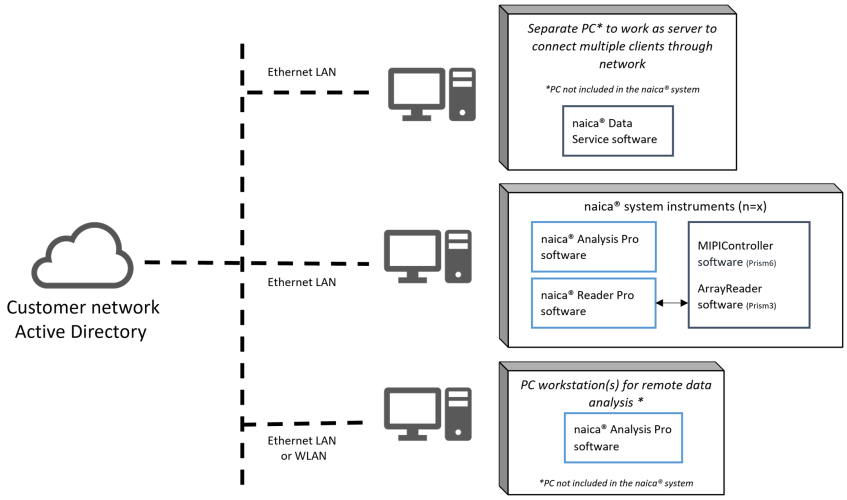
Installing naica System Pro Software Using Active Directory Authentication and a PC as a Server

This configuration allows the naica Data Service to initiate multiple communication sessions simultaneously using Active Directory and a PC as a server.

Note: Bio-Rad recommends this installation method when configuring the naica System Pro software.

To use this option:

- Configure all naica system instruments and workstations running naica System Pro software to use your Microsoft Windows Active Directory.
- Host the naica Data Service on a separate PC within your local area network (LAN). This PC acts as a server, connecting multiple naica systeminstruments and office workstations.
- The naica Data Service must connect through a network to alnaica system instruments and all workstations running naica Analysis Pro.



To enable this configuration, you must:

- Ensure your IT department has established a separate network-hosted PC that meets all requirements to function as a server for the naica Data Service installation.
- Ensure that your IT department provides all required information about the server PC, including IP address / port number.

Note: In networking a port is a number assigned that uniquely identifies a connection endpoint directs data to a specific service. A port number is always associated with an IP address of a host and the type of transport protocol used for communication. Ports enable multiple PCs to communicate or maintain multiple communication sessions at single network address.

- Ensure that Microsoft Windows Active Directory user authentication can be configured on all naica system instruments and customer workstations running naica Analysis Pro.
- Ensure that your IT department provides a naica system guest account with Microsoft Windows Active Directory and documents the guest account login details (user ID and password).

  Important: The guest account is required for installation. This account allows for the installation qualification and operation qualification (IQOQ) and service maintenance for the naica system under 21 CFR Part 11.

  Note: If your IT department cannot provide a guest account, Bio-Rad cannot track or trace the Installation Qualification and Operational Qualification (IQ/OQ), and future naica system service maintenance under 21 CFR Part 11 must be documented separately by a Bio-Rad representative.
- Ensure an IT administrator with administrative privileges is available onsite during installation. Administrator privileges are required for installing 21 CFR Part 11 naica System Pro software.

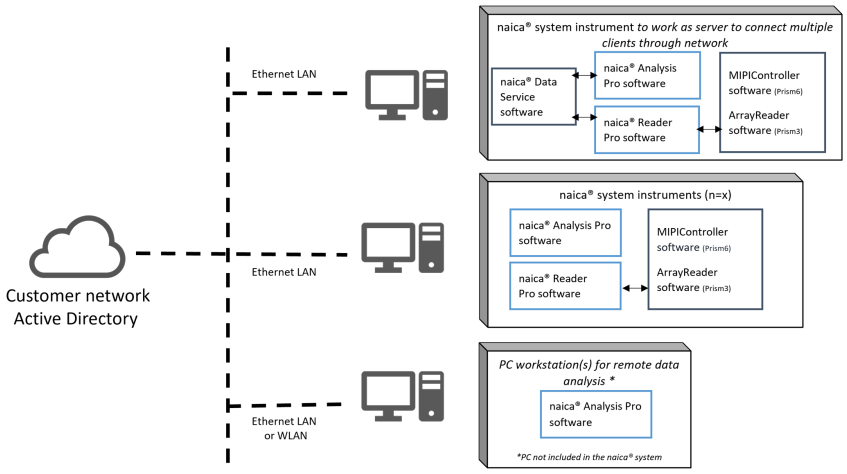
Installing naica System Pro Software Using Active Directory Authentication and the naica System as a Server

In this configuration, the naica system instrument PC functions as a server and enables multiple naica system instruments and other workstations, such as office PCs, to connect through the network. This setup allows the naica Data Service to initiate multiple communication sessions simultaneously using a naica system PC as a server while communicating while communicating with naica Reader Pro and naica Analysis Pro over the network.

Important: The naica system instrument hosting naica Data Service must always remain powered on. If the naica system instrument is powered off the naica Data Service will not be available for naica Reader Pro and naica Analysis Pro software applications.

To enable this configuration:

- Use your organization’s Microsoft Windows Active Directory for user authentication.
- Use your local area network (LAN) to host the naica Data Service on the naica system instrument PC.



To enable this configuration, you must:

- Ensure that your IT department provides all required information about the naica system PC, including IP address / port number.
- Ensure that Microsoft Windows Active Directory user authentication can be configured on all naica system instruments and all other user workstations running naica Analysis Pro.
- Ensure that your IT department provides a naica system guest account with Microsoft Windows Active Directory and documents the guest account login details (user ID and password).

  Important: The guest account is required for installation. This account allows for the installation qualification and operation qualification (IQOQ) and service maintenance for the naica system under 21 CFR Part 11.

  Note: If your IT department cannot provide a guest account, Bio-Rad cannot track or trace the Installation Qualification and Operational Qualification (IQ/OQ), and future naica system service maintenance under 21 CFR Part 11 must be documented separately by a Bio-Rad representative.
- Ensure an IT administrator with administrative privileges is available onsite during installation. Admistrator privileges are required for installing 21 CFR Part 11 naica System Pro software.

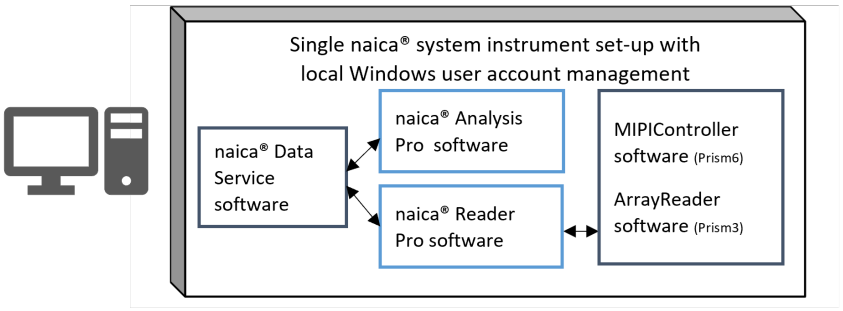
Using Local Windows User Account Authentication on a Single naica System Instrument

This configuration uses a local naica system Windows user account and a single naica system instrument to host the naica Data Service without network integration.

Important: Because each instrument operates independently and must have its own naica Data Service installation, you must prepare and analyze all Crystal Digital PCR experiments directly on the instrument running the 21 CFR Part 11 naica System Pro software . You cannot open any experiments on other workstations or on any offsite naica system except the instrument configured to host the 21 CFR Part 11 naica Data Service.

Note: Bio-Rad does not recommend this installation method for multi-instrument setups.

To configure this setup, you must administer each local naica system Windows user account individually and manage user account authentication.

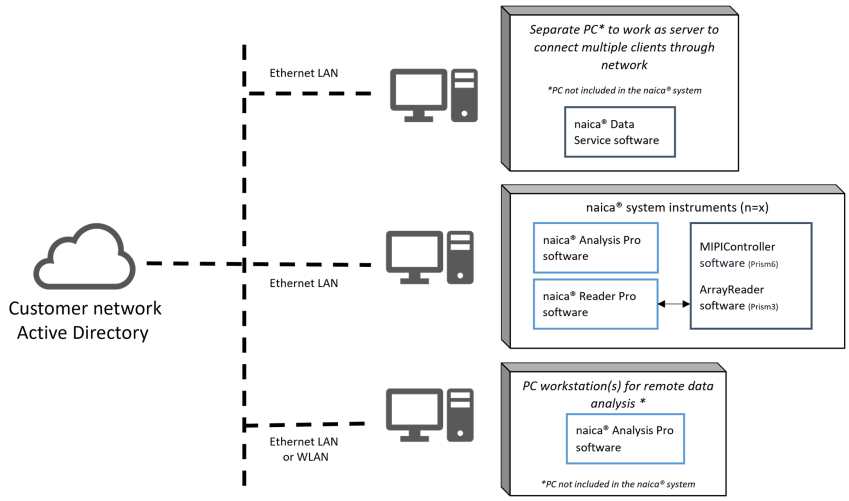


No possibility to connect multiple clients
No offsite data analysis using naica® Analysis Pro on any other workstation

To use this option:

- Create a local Windows user account for each 21 CFR Part 11 naica system instrument individually.
- Import custom scanning templates individually on each naica system instrument, as templates are not recognized across different instruments within the same facility.
- Do not share experiments across different 21 CFR Part 11 naica system instruments

Because Bio-Rad configures this option, your IT department does not to provide an administrator.



To enable this configuration, you must:

- Ensure your IT department has established a separate network-hosted PC that meets all requirements to function as a server for the naica Data Service installation.
- Ensure that your IT department provides all required information about the server PC, including IP address / port number.

  Note: In networking a port is a number assigned that uniquely identifies a connection endpoint directs data to a specific service. A port number is always associated with an IP address of a host and the type of transport protocol used for communication. Ports enable multiple PCs to communicate or maintain multiple communication sessions at single network address.
- Ensure that Microsoft Windows Active Directory user authentication can be configured on all naica system instruments and customer workstations running naica Analysis Pro.
- Ensure that your IT department provides a naica system guest account with Microsoft Windows Active Directory and documents the guest account login details (user ID and password).

  Important: The guest account is required for installation. This account allows for the installation qualification and operation qualification (IQOQ) and service maintenance for the naica system under 21 CFR Part 11.

  Note: If your IT department cannot provide a guest account, Bio-Rad cannot track or trace the Installation Qualification and Operational Qualification (IQ/OQ), and future naica system service maintenance under 21 CFR Part 11 must be documented separately by a Bio-Rad representative.
- Ensure an IT administrator with administrative privileges is available onsite during installation. Administrator privileges are required for installing 21 CFR Part 11 naica System Pro software.

Installing naica Data Service

This procedure explains how to the install the naica Data Service and the Microsoft Windows Active Directory user authentication. The user must ensure that an IT department administrator is available to assist with the installation of the 21 CFR Part 11 naica System Pro software installation.

The naica Data Service software provides centralized management for user authentication, audit trails, and electronic signatures required for 21 CFR Part 11 compliance. It works in conjunction with the naica Reader Pro and naica Analysis Proapplications.

After installed and configured, the naica Data Service records and stores all user actions in the naica experiment file and naica Data Service audit trails.

naica Data Service System Requirements

This section explains the requirements for installing naica Data Service.

naica Data Service System Prerequisites

The naica Data Service can be installed directly on the naica System PC or on a separate PC that meets the minimum specifications in the table below.

Table 2. naica Data Service specifications

Item	External 3-Color naica system PC Specification	Embedded 6-Color naica system Specification
Operating system	Windows 10 in 64 bits 21H2	Windows 10 in 64 bits 21H2
Disk space	1 disk of size 1 TB 1 SSD disk of size 256 GB	1 disk of size 1 TB 1 SSD disk of size 512 GB
RAM	1 RAM of size 32 GB (2x16 GB) DDR4 type	1 RAM of size 32 GB
Processors	Intel Core i5, 6 cores with a clock frequency of up to 4.1GHz	1 CPU equivalent to CPU i5-8500 in performance)
Interfaces	Motherboard interface (USB, sound I/O, ethernet, video I/O port, serial port), Graphic card interface (HDMI, Display Port), USB Ports from a dedicated controller.	2 Ethernet ports

The following naica Data Service installers are required:

- Naica_Data_Service_Setup_1.0.264.3.exe
- Setup_naicaAnalysisPro_v4.1.34.3-36652.exe
- Setup_naicaAnalysisPro_v4.1.34.3-36652.exe.

The software installation requires 2 GB of disk space.

Note: For installations that involve integration with customer networks or antivirus software, make sure that access to the following directories is not blocked:

- C:\ProgramData\Bio-Rad
- C:\Program Files\Bio-Rad
- %USERPROFILE%\Bio-Rad
- %USERPROFILE%\AppData\Local\Bio-Rad

Additional directories for 3-color naica system include:

- C:\Users\Public\Documents\Sensovation
- C:\ProgramData\Sensovation
- C:\Program Files (x86)\Sensovation
- %USERPROFILE%\AppData\Local\Temp\Naica

These folders are essential for operating and configu the naica System Pro software suite.

Microsoft Windows Active Directory User Authentication Service

The naica Data Service uses the Microsoft Windows Active Directory to authenticate users Bio-Rad recommends following Microsoft password policy to protect accounts against password attacks.

If your IT allows the naica system to integrate into the Microsoft Windows Active Directory domain for user authentication, you can install the naica Data Service in one of the following ways:

- On a separate PC as a server
- On a naica system instrument as a server

Important: You must configure the naica Reader Pro and naica Analysis Pro so they can communicate with the naica Data Service over the network.

If Microsoft Windows Active Directory user authentication is not available, you can configure the naica Data Service to use local Microsoft Windows accounts for user authentication. In this case, you must

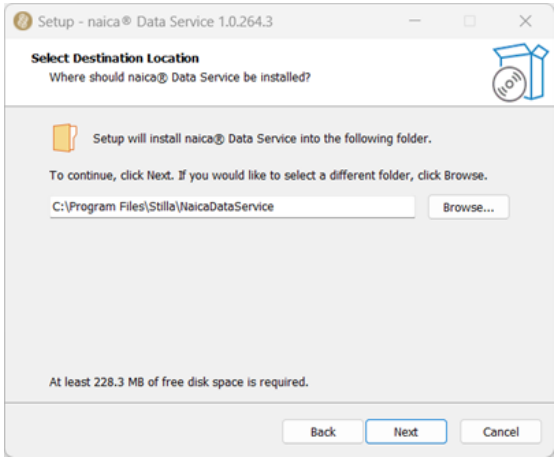
install and use the naica Reader Pro and naica Analysis Pro software applications on the same naica system instrument where the naica Data Service is installed.

naica Data Service Download and Installation

An IT administrator must install the naica Data Service on a separate PC for it to function as a server.

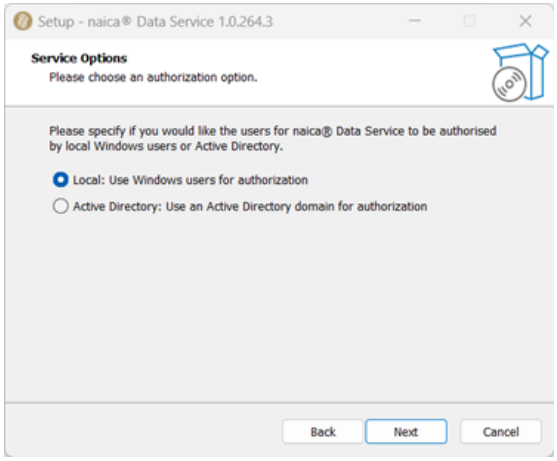
To download and install naica Data Service

1. Download Naica_Data_Service_Setup_1.0.264.3.exe.using the link provided to the PC.
2. Double-click the file to begin the installation process.
3. In the Microsoft Defender SmartScreen dialog, click More info to execute the Naica_Data_Service_ Setup_1.0.264.3.exe.
4. Click Run anyway to proceed with the installation with the Naica_Data_Service_Setup_1.0.264.3.exe installer.
5. When prompted by Windows User Account Control, click Yes to allow changes to the device.
6. Select the preferred language for the installation and click Next.
7. Read and accept the license agreement.
8. In the Select Destination Location window, choose the installation location options:
   - Click Next to use the default location.
   - Click Browse... to select a different location.

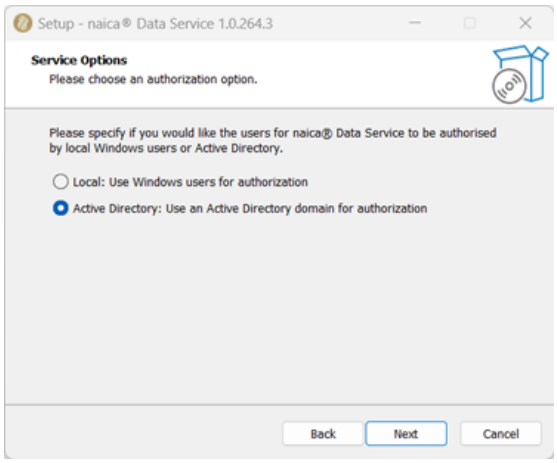


9. In the Authorization Method window, select one of the following authentication methods:

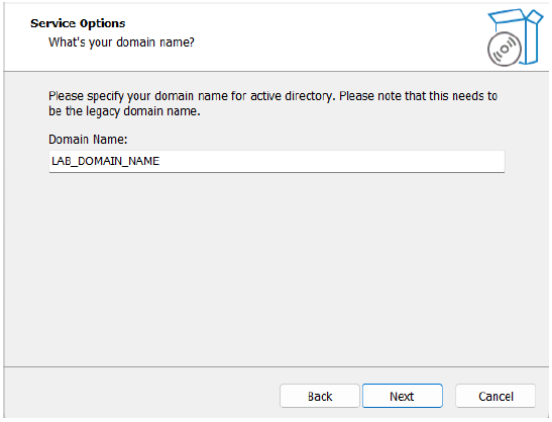
- Local Windows user authentication (see Installing naica System Pro Software Using Active Directory Authentication and the naica System as a Server on page 38
  - ☐ Use this option for standalone installations on a single naica System instrument.
  - ☐ Only local access is available, and user accounts must be administered locally.
  - ☐ The naica Data Service must be installed locally on the same instrument.



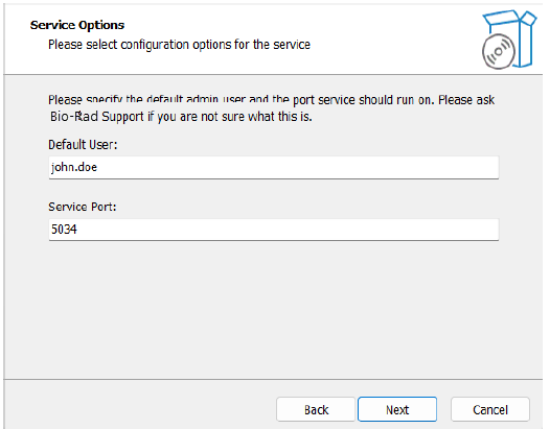
- Microsoft Windows Active Directory authentication (see Installing naica System Pro Software Using Active Directory Authentication and a PC as a Server on page 37):
  - ☐ Is recommended for centralized user authentication
  - ☐ Enables networked access for multiple instruments and workstations
  - ☐ Allows multiple users to access 21 CFR Part 11 naica Data Service software applications



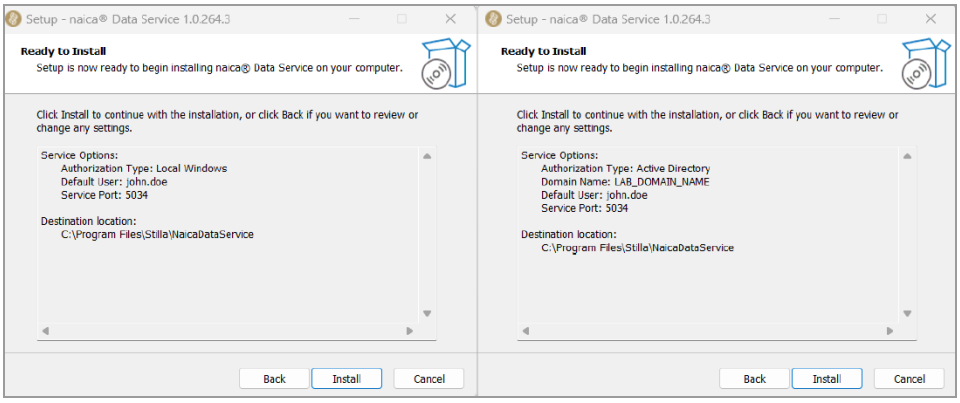
10. If you are authenticating with Active Directory, verify the detected domain name and modify it if necessary.



- If the naica Data Service is to be used with Local Windows accounts (see Local Windows User Authentication and Configuration on Single naica System on page 1), there is no need to provide a domain name.
- If the naica Data Service is to be used with Microsoft Windows Active Directory user authentication (see Active Directory User Authentication with a Customer-Hosted PC as the Server on page 1 and Active Directory User Authentication with a naica System as the Server on page 1), the customer-specific domain name must be configured.
- The naica Data Service installer will automatically detect the domain name. Verify that the detected domain is correct, and modify it if necessary.



11. Specify the default Administrator user:
    - The installer auto-detects the current Active Directory account as the default user.
    - Verify the username and edit if needed. Bio-Rad recommends using the IT administrator's credentials.
12. Specify the Service Port number:
    - Default: 5034
    - You can change this value if needed.
    - Ensure the selected PC allows TCP connections on the configured port.



13. Review all settings on the Ready to Install screen:
    - Click Back to modify settings, if necessary.
    - Click Install to proceed.

14. After installation, click Finish to exit the setup wizard. The naica Data Service starts automatically on the configured PC.

Note: The PC hosting the naica Data Service must remain powered on at all times to ensure proper 21 CFR Part 11–compliant communication between naica Systems and connected workstations.

Configuring the naica Data Service Web Interface

This section explains how to configure the naica Data Service web interface.

To configure the naica Data Service web interface

1. Open a web browser and enter the naica Data Service URL http://<server_ip_or_dns>:<port_number> in the address bar.
   - For network-integrated installations (for more information, see Installing naica System Pro software Using Active Directory Authentication and a PC as a Server on page 1 and Installing naica System Pro software Using Active Directory Authentication and the naica System as a Server on page 1):
     - ☐ An IT administrator must update the Internet Protocol (IP) or Domain Name Server (DNS) address and the port number according to the naica Data Service configuration.
     - ☐ You must configure the selected server to allow HTTP connections on the naica Data Service port. To facilitate naica Data Service interface connections, Bio-Rad recommends associating a DNS address with the server.
   - For local installations, use the default local URL to access the naica Data Service web interface http://localhost:5034.
2. An IT administrator must log into the naica Data Service using their Microsoft Windows Active Directory credentials (username and password).
3. After logging in, the IT administrator must create the first 21 CFR Part 11-compliant naica System account, which must meet the following conditions:
   - The account must be assigned the Lab Manager role to enable creation of additional user accounts without further IT administrator involvement.
   - The account must be created for a naica Systemend user and not for the IT administrator.

For instructions to create and manage 21 CFR Part 11 naica system user accounts and user roles, see naica System Pro Software User Roles and Permissions on page 1.

Stilla Technologies
F-94800 Villejuif, France

Bio-Rad Laboratories, Inc.
1000 Alfred Nobel Drive
Hercules, CA, 94547, USA

BIO-RAD **Bio-Rad Laboratories, Inc.**

Life Science Group

Website *bio-rad.com* ***USA*** *1 800 424 6723* ***Australia*** *61 2 9914 2800* ***Austria*** *00 800 00 24 67 23* ***Belgium*** *00 800 00 24 67 23* ***Brazil*** *4003 0399*
Canada *1 800 361 1808* ***China*** *86 21 6169 8500* ***Czech Republic*** *00 800 00 24 67 23* ***Denmark*** *00 800 00 24 67 23* ***Finland*** *00 800 00 24 67 23*
France *00 800 00 24 67 23* ***Germany*** *00 800 00 24 67 23* ***Hong Kong*** *852 2789 3300* ***Hungary*** *00 800 00 24 67 23* ***India*** *91 124 4029300* ***Israel*** *0 3 9636050*
Italy *00 800 00 24 67 23* ***Japan*** *81 3 6361 7000* ***Korea*** *82 080 007 7373* ***Luxembourg*** *00 800 00 24 67 23* ***Mexico*** *52 555 488 7670*
The Netherlands *00 800 00 24 67 23* ***New Zealand*** *64 9 415 2280* ***Norway*** *00 800 00 24 67 23* ***Poland*** *00 800 00 24 67 23* ***Portugal*** *00 800 00 24 67 23*
Russian Federation *00 800 00 24 67 23* ***Singapore*** *65 6415 3188* ***South Africa*** *00 800 00 24 67 23* ***Spain*** *00 800 00 24 67 23* ***Sweden*** *00 800 00 24 67 23*
Switzerland *00 800 00 24 67 23* ***Taiwan*** *886 2 2578 7189* ***Thailand*** *66 2 651 8311* ***United Arab Emirates*** *36 1 459 6150* ***United Kingdom*** *00 800 00 24 67 23*