



**naica® system Pro software
for 21 CFR Part 11 compliance**

S30021

**User Manual
naica® Data Service v1.0
naica® Reader Pro v4.0 & naica® Analysis Pro v4.1**

TECHNICAL SUPPORT

For help and technical advice, please contact the Technical Support Department

For customers from Europe, China and Africa:

Monday to Friday, 9:30 AM - 6:30 PM, Central European Time (CET).

Closed on French bank holidays.

Phone: (+33) 9 82 27 47 47

Email: support@stilla.fr.

For customers from America, Asia (excluding China) and Oceania:

Monday to Friday, 8:00 AM – 6:00 PM, Eastern Standard Time (EST).

Closed on American bank holidays.

Phone: 1-833-888-0150 ext. 1

Email: support@stilla-inc.com

LEGAL NOTICES

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage or retrieval system, without permission in writing from Stilla® Technologies.

Stilla® Technologies reserves the right to modify its products and services at any time. Information contained in this user manual is subject to change without notice. Stilla® Technologies assumes no liability for errors or any damage resulting from the use of this information.

The naica® system and/or its uses are covered by US and corresponding non-US patents owned by or under license to Stilla Technologies.

The naica® system and/or its use is licensed under U.S. and/or non-U.S. patents, and/or pending U.S. and non-U.S. patent applications owned by or under license to Bio-Rad Laboratories, Inc., including, but not limited to, U.S. Patent Nos. 9,968,933; 9,127,310; RE41,780; and 8,871,444.

Details available at: www.stillatechnologies.com/patents.

Purchase of the naica® system includes a limited, non-transferable right under such intellectual property for use of the products for research and applied applications, including commercial services, but excluding any commercial NIPT services. The exclusion of commercial NIPT services applies only in the United States and the European Union.

No rights are granted for diagnostic uses.

Further information on purchasing licenses may be obtained by contacting Stilla® Technologies, 1 Mail du Professeur Georges Mathé, 94800 Villejuif, France. It is the responsibility of the purchaser/end user to acquire any additional intellectual property rights that may be required from Bio-Rad Laboratories, Inc.

It is the responsibility of the purchaser/end-user to acquire any additional intellectual property rights that may be required.

TRADEMARKS

Crystal Digital PCR®, naica® and Stilla® are trademarks of Stilla® Technologies. All other trademarks are the sole property of their respective owners.

COPYRIGHT & INTENDED USE

Copyright 2018-2022, Stilla® Technologies. All rights reserved.

For Research Use Only. Not for use in diagnostic procedures.

Contents

1. INTRODUCTION	4
1.1. Purpose of the document	4
1.2. naica® system Pro software	4
1.3. Terms and Conditions of Use	6
1.4. Intended use of the naica® system Pro software	8
1.5. Incompatibility with Crystal Reader & Crystal Miner software	8
2. INSTALLATION OPTIONS	9
2.1. Active Directory user authentication & customer hosted PC as server	9
2.2. Active Directory user authentication & naica® system as server	10
2.3. Local Windows user authentication & set up on single naica® system	11
3. INSTALLATION INSTRUCTIONS.....	12
3.1. naica® Data Service installation configuration	12
3.1.1. naica® system Pro software requirements	12
3.1.2. naica® Data Service download and installation	14
3.1.3. naica® Reader Pro & naica® Analysis Pro installation	20
3.1.4. naica® Data Service web interface configuration	21
4. NAICA® DATA SERVICE ROLES / PERMISSION ADMINISTRATION	22
4.1. naica® Data Service Permissions	22
4.2. naica® Data Service Roles	26
4.3. Default User Roles	26
4.3.1. Lab Manager	26
4.3.2. Operator	26
4.4. Administration of customized User Roles	27
4.4.1. Add Role	27
4.4.2. Update an existing Role	28
4.4.3. Delete an existing Role	28
4.5. naica® Data Service User management	30
4.5.1. Create new naica® Data Service user account	31
4.6. naica® Data Service Audit Trail	33
5. NAICA® READER PRO & NAICA® ANALYSIS PRO SOFTWARE	35
5.1. Individual User Authentication	35
5.2. naica® Reader Pro scanning template files	36
5.2.1. Registering default scanning template files in naica® Data Service	36
5.2.2. Creating a new custom naica® Reader Pro scanning template files	37
5.3. naica® Analysis Pro sample validation	38
5.3.1. Electronic signatures	40
5.3.2. Experiment Audit Trail	42
5.3.3. Experiment PDF Report creation	44
6. SERVICE & SUPPORT	48

1. INTRODUCTION

1.1. Purpose of the document

This document provides detailed information for the installation and the operation of the naica® system Pro software applications (naica® Data Service, naica® Reader Pro and naica® Analysis Pro).

This User Manual details only the software features specific and relevant for the 21 CFR Part 11 compliance of the naica® system Pro software.

naica® Reader Pro and naica® Analysis Pro share common features with the standard RUO software Crystal Reader and Crystal Miner, respectively. All general software features common for the 21 CFR Part 11 naica® system Pro software, naica® Reader Pro and naica® Analysis Pro, and their equivalent standard RUO software, Crystal Reader and Crystal Miner respectively, are detailed in the respective User Manuals for Crystal Reader and Crystal Miner software.

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

1.2. naica® system Pro software

naica® system Pro software enables naica® system users (customers) to meet the Food and Drug Administration’s regulations on good laboratory practices (GLP) as well as good manufacturing practices (GMP) in pharmaceutical as well as biotechnology industries. 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.

Stilla® Technologies 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 Stilla® Technologies to ensure compliance with 21 CFR Part 11.

An overview of the supported 21 CFR Part 11 requirements fulfilled by the use of the naica® system Pro software are provided in Table 1

To ensure fulfillment of all 21 CFR Part 11 sections user’s organization responsibilities to establish respective Standard Operation Procedures (SOPs) are indicated in the table with “X”.

Section	Subject	User’s organization	naica® system Pro software	Compliance management
11.10 (a)	Validation	X	X.	System validation as well as experiment result validation is supported by naica® system Pro software. SOPs of the user’s organization for validation is required.

Section	Subject	User's organization	naica® system Pro software	Compliance management
11.10 (b)	Human readable records	n.a.	X	Electronic records in human readable form supported throughout naica® system Pro software
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.
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 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.
11.10 (h)	Device checks	X	X	Experiment configuration and parameters are checked by 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 Manuals and training documentation are provided by Stilla Technologies. Establishing and maintaining the appropriate training level is the responsibility of the user's organization.
11.10 (j)	Written policies	X	n.a.	Establishing and maintaining SOP to comply with the regulation 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

Section	Subject	User's organization	naica® system Pro software	Compliance management
				to the users and version control of the documentation is the responsibility of the user's organization.
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	Certification of equivalence.
11.200 (a/b)	Electronic Signature components and control	n.a.	X	Signature with username and password ensure genuine owner.
11.300 (a)	Controls for identification username and passwords	X	X	Uniqueness of username and password.
11.300 (b)		X	X	Periodical check of issuance.
11.300 (c)		X	X	Loss management.
11.300 (d)		X	X	Safeguards and detection of unauthorized attempts.

1.3. Terms and Conditions of Use

- Stilla® Technologies 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 terms and conditions of use of the naica® 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 is not allowed to
 - 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 other purpose outside the described intended use,
 - sub-license or grant access to the naica® system Pro software to any third parties.
 - copy the naica® system Pro software and its documentation.

- The customer is subject to the same prohibitions and restrictions regarding software, belonging to third parties, used or embedded in the naica® system. The customer must also comply strictly with the terms of use and licensing required by any third-party owner of software used or embedded in the naica® system.

1.4. Intended use of the naica® system Pro software

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 the compliance of all naica® system operations with respect to regulation 21 CFR Part 11.

- naica® Reader Pro

The naica® Reader Pro software application functions as the operating interface to define the experimental settings for the image acquisition of the scanner instrument (Prism3 / Prism6) for the Crystal Digital PCR® workflow. naica® Reader Pro is the 21CFR part 11 software equivalent to the standard RUO Crystal Reader software.

- naica® Analysis Pro

The naica® Analysis Pro software is the data analysis application of the naica® system. naica® Analysis Pro is used to analyze data from the images acquired using the naica® Reader Pro, and to calculate the absolute concentrations of targeted nucleic acids. naica® Analysis Pro is the 21CFR part 11 software equivalent to 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®.

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

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

For Research Use Only. Not for use in diagnostic procedures.

©2015-2024 Stilla® Technologies. All rights reserved.

1.5. Incompatibility with Crystal Reader & Crystal Miner software

Crystal Reader and Crystal Miner software are not 21 CFR Part 11 compliant.

- naica® Reader Pro and naica® Analysis Pro files are not compatible with Crystal Reader and Crystal Miner software.
- Utilization of Crystal Reader and Crystal Miner v4.0 to edit files produced by naica® Reader Pro and naica® Analysis Pro is prohibited.
 - Utilizing Crystal Reader and Crystal Miner v3.1 or below to edit files produced by naica® Reader Pro and naica® Analysis Pro is not prohibited but the experiment files and or templates will be corrupted.

2. INSTALLATION OPTIONS

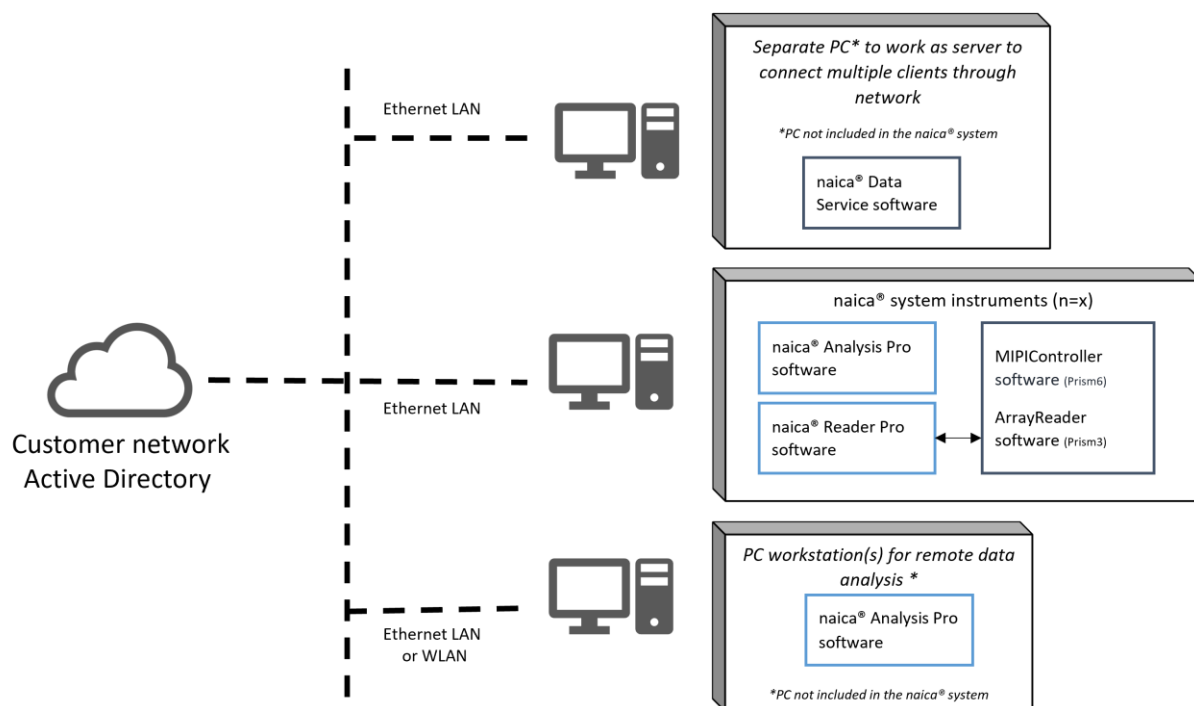
There are three different ways to install the naica® system Pro software at a customer's organization, depending on the individual customer's requirements and infrastructures. All three options require their own specific set of parameters to be put in place. The different options are detailed below.

2.1. Active Directory user authentication & customer hosted PC as server

Recommended installation set up for naica® system Pro software

Utilize the customer's organization's Microsoft Windows Active Directory user authentication. Utilize the customer's local area network (LAN) to host the naica® Data Service on a separate computer to work as a server, to which multiple naica® system instruments and or other workstations, such as office PCs, can be connected.

The naica® Data Service must be connected through a network to all naica® system instruments and all other user workstations running naica® Analysis Pro.



In this installation set-up (separate PC working as a server), multiple simultaneous communication sessions may be initiated with the naica® Data Service.

- The customer must ensure the IT department has established a separate network hosted PC fulfilling all specified requirements to work as a server for the installation of the naica® Data Service.
- The customer must ensure that the IT department will provide all required information about the separate PC working as a server (IP address / port number).
 - In computer networking, a port is a number assigned to uniquely identify a connection endpoint and to direct 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 provide a service for multiple PCs used as a server to communicate or for multiple communication sessions to be held at one network address.
- The customer must 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.
- The customer must ensure that their IT department will provide a naica® system guest account within the Microsoft Windows Active Directory user authentication. They must ensure to record and document the guest account login details (user ID & password).

- The guest account is required by the Stilla Technologies representative. This account will allow for the installation qualification and operation qualification (IQOQ) and service maintenance routines executed on the naica® system under 21 CFR Part 11 conditions.
- If the guest account cannot be provided by the customer's IT department, the IQOQ procedure as well as any future service maintenance routines cannot be tracked and traced within the 21 CFR Part 11 configuration and will be documented separately by the Stilla Technologies representative.

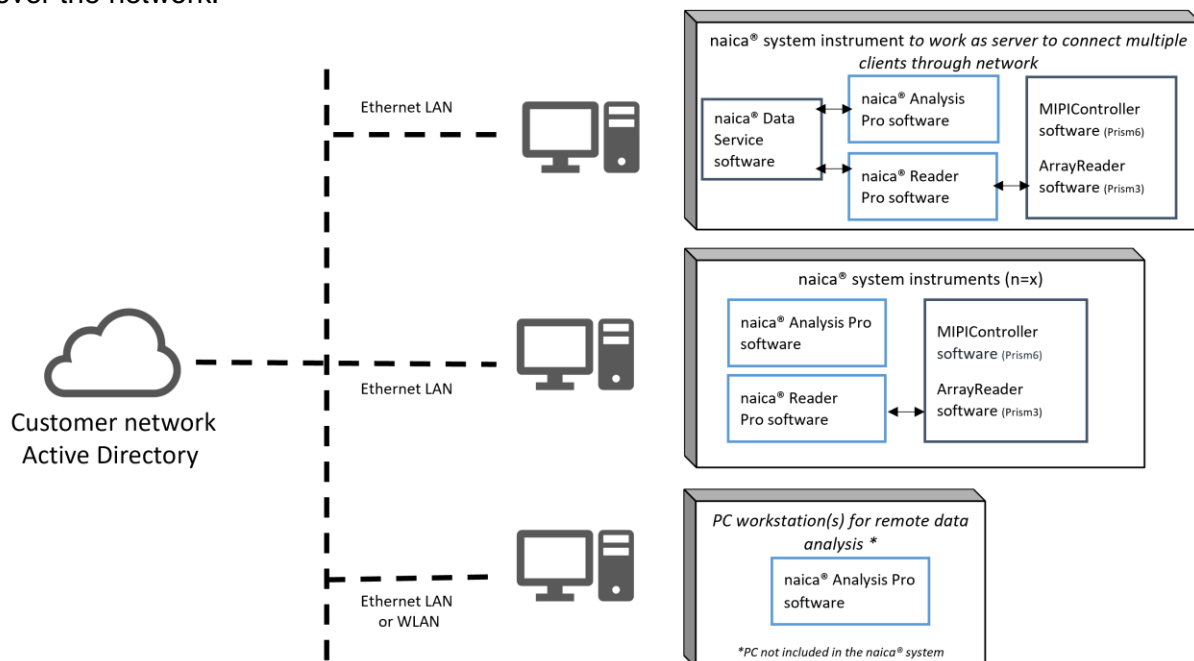
The customer must ensure that their IT department administrator will be available on-site the day of the installation, as administration privileges are required for the 21 CFR Part 11 naica® system Pro software installation.

2.2. Active Directory user authentication & naica® system as server

Limitation of this installation set-up:

The naica® system instrument, where the naica® Data Service is hosted, must always remain powered on. Each time this naica® system instrument is powered off the naica® Data Service will not be available for any naica® Reader Pro and naica® Analysis Pro software applications. Utilize the customer's organization's Microsoft Windows Active Directory user authentication. Utilize the customer's local area network (LAN) to host the naica® Data Service on the naica® system instrument PC. In this configuration, the naica® system instrument will act as a server; multiple naica® system instruments and or other workstations, such as office PCs, can be connected to it through the network.

The naica® Data Service will communicate with naica® Reader Pro and naica® Analysis Pro over the network.



In this installation set-up (naica® system PC working as a server), multiple simultaneous communication sessions may be initiated with the naica® Data Service.,

- The customer must ensure that their IT department will provide all required information about the naica® system PC working as a server (IP address / port number).
- The customer must 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.
- The customer must ensure that their IT department will provide a naica® system guest account within the Microsoft Windows Active Directory user authentication. They must ensure to record and document the guest account login details (user ID & password).

- The guest account is required by the Stilla Technologies representative. This account will allow for the installation qualification and operation qualification (IQOQ) and service maintenance routines executed on the naica® system under 21 CFR Part 11 conditions.
 - If the guest account cannot be provided by the customer's IT department, the IQOQ procedure, as well as any future service maintenance routines, cannot be tracked and traced within the 21 CFR Part 11 configuration, and will be documented separately by the Stilla Technologies representative.
- The customer must ensure that their IT department administrator will be available on-site the day of the installation, as administration privileges are required for the 21 CFR Part 11 naica® system Pro software installation.

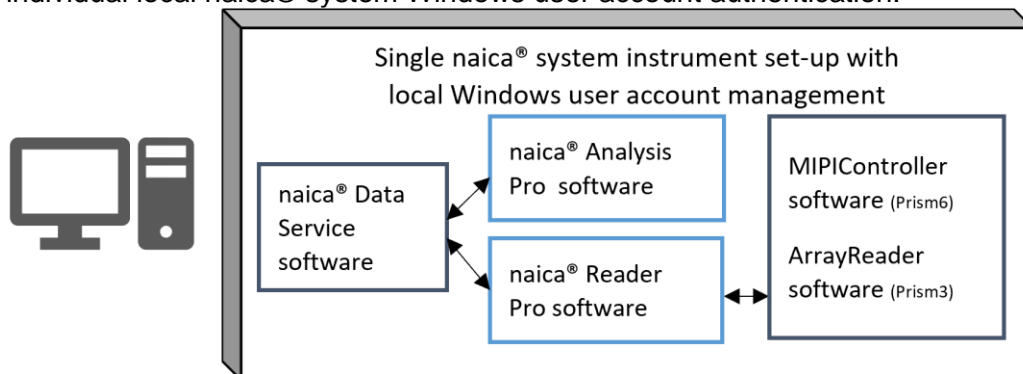
2.3. Local Windows user authentication & set up on single naica® system

Limitation of this installation set-up:

This installation is not recommended for multi-instrument installations, as each instrument is independent and must have its own naica® Data Service installed.

Each user must prepare and analyze Crystal Digital PCR® experiments directly on the 21 CFR Part 11 naica® system instrument. It will not be possible to open experiments on any other workstation or any other naica® system offsite the configured 21 CFR Part 11 naica® system instrument hosting the naica® Data Service.

Utilize local naica® system Windows user account authentication and selected single naica® system instrument to host naica® Data Service without any network integration. With this installation configuration the client will be responsible for managing and administering the individual local naica® system Windows user account authentication.



No possibility to connect multiple clients

No offsite data analysis using naica® Analysis Pro on any other workstation

- Local Windows user account authentication must be created for each 21 CFR Part 11 naica® system instrument individually.
- Custom scanning templates will not be recognized across the different 21 CFR Part 11 naica® systems within the same facility. The scanning templates must be imported individually on each naica® system instrument.
 - Sharing experiments across different 21 CFR Part 11 naica® system instruments is prohibited.

This installation set-up can be managed by the Stilla Technologies representative and does not require support of a customer IT department administrator.

3. INSTALLATION INSTRUCTIONS

3.1. naica® Data Service installation configuration

This procedure documents the installation process of the naica® Data Service including the Microsoft Windows Active Directory user authentication. The customer must ensure an IT department administrator is available to assist the 21 CFR Part 11 naica® system Pro software installation.

The naica® Data Service software is used to administrate naica® system user management, audit trails and electronic document signature capabilities to the software applications naica® Reader Pro and naica® Analysis Pro.

The naica® Data Service software is a network connected application that must be installed, in addition to naica® Reader Pro and naica® Analysis Pro software applications, to ensure 21 CFR Part 11 compliance.

The naica® Data Service application can either be installed on a separate PC to work as a server or directly on the naica® system instrument.

After installation and setup, all user actions are logged and documented in the naica® experiment file audit trails as well as in the naica® Data Service audit trails.

3.1.1. naica® system Pro software requirements

3.1.1.1 Prerequisites for using the naica® Data Service

The naica® Data Service software can run either directly on the naica® system PC or on any other PC which fulfills the following specifications for optimal performance:

- Operating System: Windows 10 Pro (version 21H2) in 64 bits
- RAM: at least 16 GB
- Processors: Intel Core i5 or higher, at least 2 cores of 2 GHz or higher
- Screen resolution: at least 1920 x 1080; aspect ratio 16:9
- Network: any wired or wireless networking environment.

To install the naica® Data Service software, the provided USB device PN S30021 is required.

Note: 2 GB of disk space is required for software installation.

3-color naica® system	6-color naica® system
External naica® PC	Embedded PC
<u>Operating System:</u> Windows 10 in 64 bits 21H2	<u>Operating System:</u> Windows 10 in 64 bits 21H2
<u>Disk storage:</u> 1 disk of size 1 TB 1 SSD disk of size 256 GB	<u>Disk storage:</u> 1 SSD disk of size 1 TB 1 SSD disk of size 512 GB
<u>RAM:</u> 1 RAM of size 32 GB (2x16 GB) DDR4 type	<u>RAM:</u> 1 RAM of size 32 GB
<u>Processors:</u> Intel Core i5, 6 cores with a clock frequency of up to 4.1GHz	<u>Processors:</u> 1 CPU equivalent to CPU i5-8500 in performance
<u>Interfaces:</u> 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.	<u>Interfaces:</u> 2 Ethernet ports

For integration of the naica® system to the customer’s network or installation of customer specific antivirus applications, it is important to ensure that access to the following naica® system directories is not prevented:

- C:\ProgramData\Stilla
- C:\Program Files\Stilla
- %USERPROFILE%\Stilla
- %USERPROFILE%\AppData\Local\Stilla

Additional directories for 3-color naica® system:

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

3.1.1.2 Microsoft Windows Active Directory user authentication service

The naica® Data Service uses the Microsoft Windows Active Directory user authentication feature to authenticate users. It is recommended to follow Microsoft password policy to ensure accounts are secure against password attacks.

If the client’s IT infrastructure allows the integration of the naica® system in Microsoft Windows Active Directory domain for user authentication, the naica® Data Service can be installed:

- on a separate PC to work as a server
- on a naica® system instrument to work as a server

The naica® Reader Pro and naica® Analysis Pro software applications must be configured to communicate with the naica® Data Service over the network.

If Microsoft Windows Active Directory user authentication is not available, it is possible to configure the naica® Data Service to use local Microsoft Windows accounts for user

authentication. In this case, the naica® Reader Pro and naica® Analysis Pro software applications must be installed and used on the same naica® system instrument where the naica® Data Service is installed.

3.1.1.3 naica® Data Service security

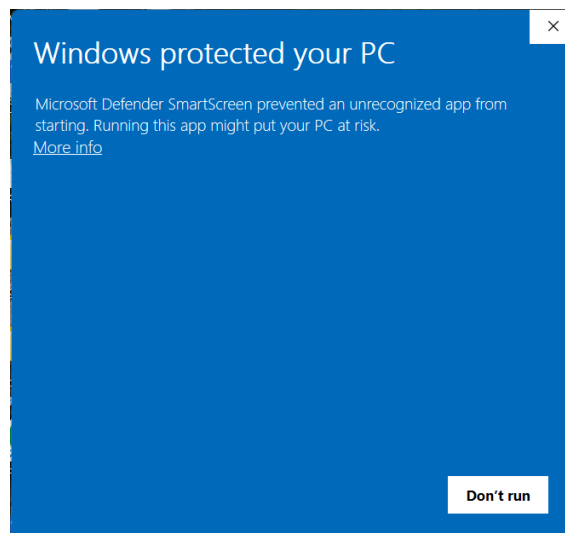
The separate PC to work as a server must be configured such that only the IT administrator has administration privileges to access the installation directory on the naica® Data Service. Other naica® system users shall not have “write” or “execute” rights on the installation directory of the naica® Data Service.

This configuration is mandatory to guarantee the security of the naica® system Pro software. It is the customer’s responsibility to ensure the set-up configuration as described for the naica® Data Service.

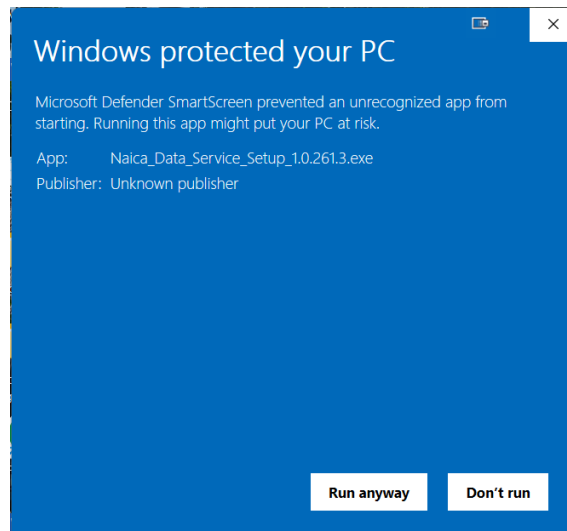
3.1.2. naica® Data Service download and installation

The installation of the naica® Data Service, on separate PC to work as a server, should be executed with IT administration privileges.

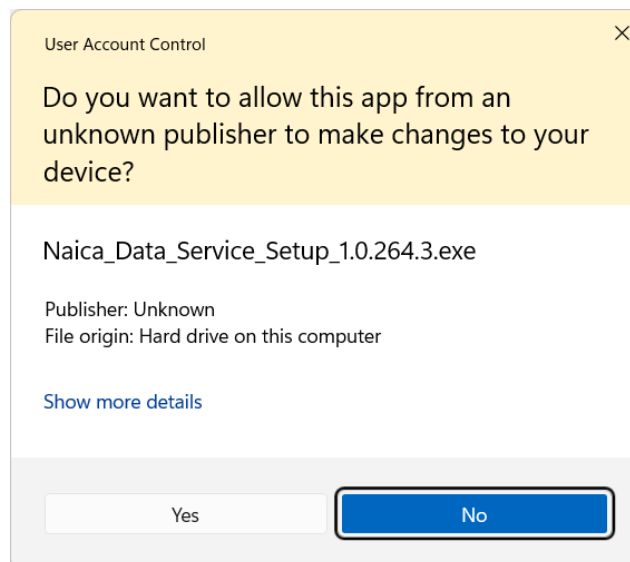
1. Plug the provided USB device and locate the file Naica_Data_Service_Setup_1.0.264.3.exe.
2. Download the file to the PC and double-click to start the installation process.



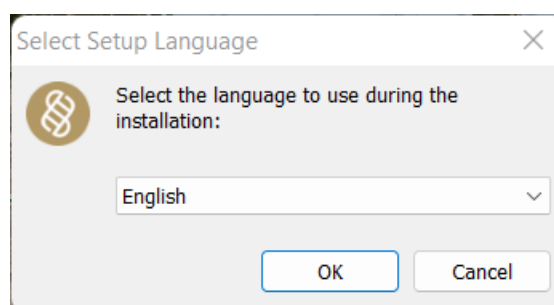
3. Click « More info » in the Microsoft Defender SmartScreen dialog.



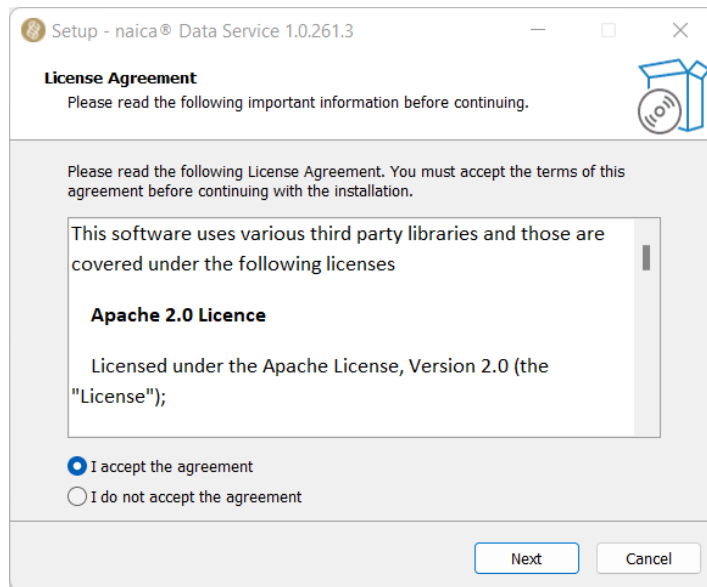
4. Click « Run anyway » in the Microsoft Defender SmartScreen dialog to allow the installer to execute the Naica_Data_Service_Setup_1.0.261.3.exe



5. Click « Yes » in the Windows User Account Control Dialog asking to allow changes to the device



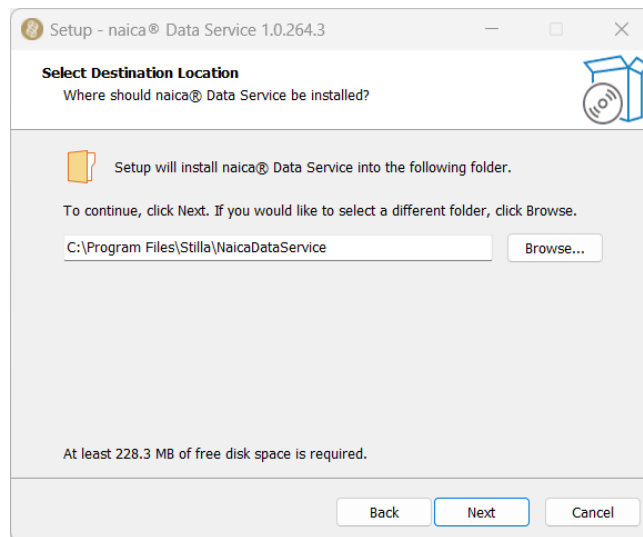
6. Select the language to use during the installation



7. Carefully read the License Agreement

8. Check the « I accept the agreement » in License Agreement dialog

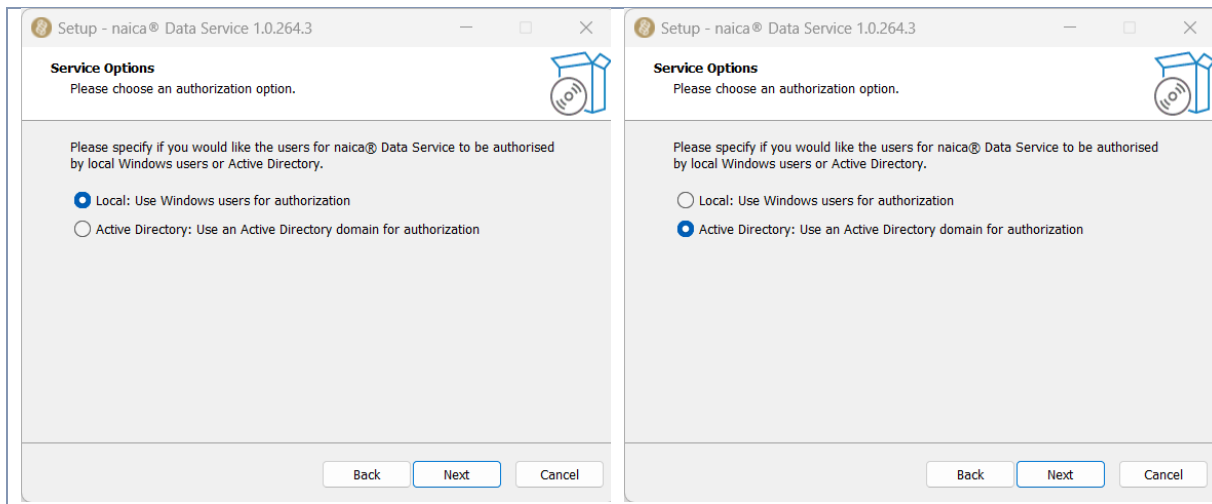
9. Click « Next »



10. Select the preferred installation location for naica® Data Service software.

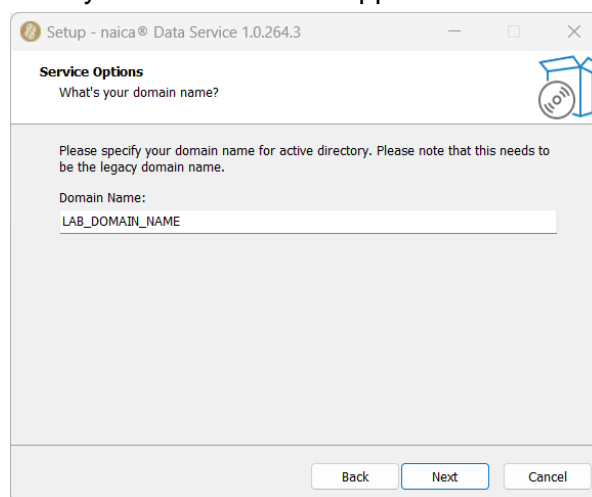
11. Click « Next » to install in the default installation directory

12. Click « Browse » to choose a different Destination Location for the naica® Data Service.



13. Check the preferred installation option for local Windows user authorization (left, section 2.3) or Active Directory domain for authorization (right, sections 2.1 & 2.2).

- For Section 2.3 (Local Windows user authentication)
If local authentication is selected, the naica® Data Service must be installed on an individual naica® system instrument and all 21 CFR Part 11 naica® system Pro software applications can only be used locally. Local Windows user accounts must be administrated by the customer.
- Sections 2.1 and 2.2 (Active Directory user authentication)
Stilla Technologies recommends the installation supported by the Microsoft Windows Active Directory user authentication to benefit from a centralized customer organization user authentication as well as to allow multiple clients access to all 21 CFR Part 11 naica® system Pro software applications.

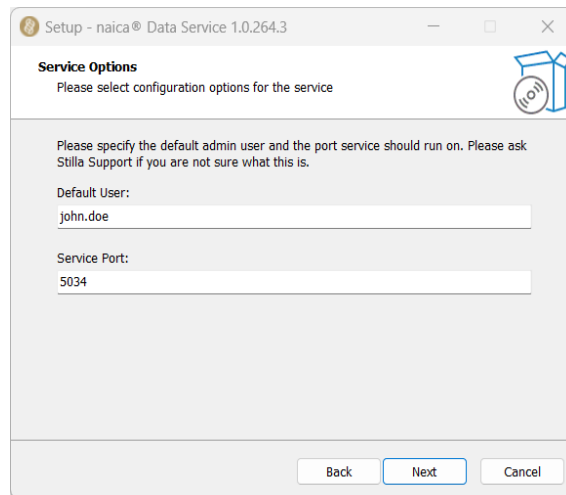


14. Specify the domain name

If the naica® Data Service is to be used with Local Windows accounts (section 2.3), there is no need to provide the domain name.

If the naica® Data Service is to be used with Microsoft Windows Active Directory user authentication (sections 2.1 & 2.2), the customer specific domain name needs to be configured.

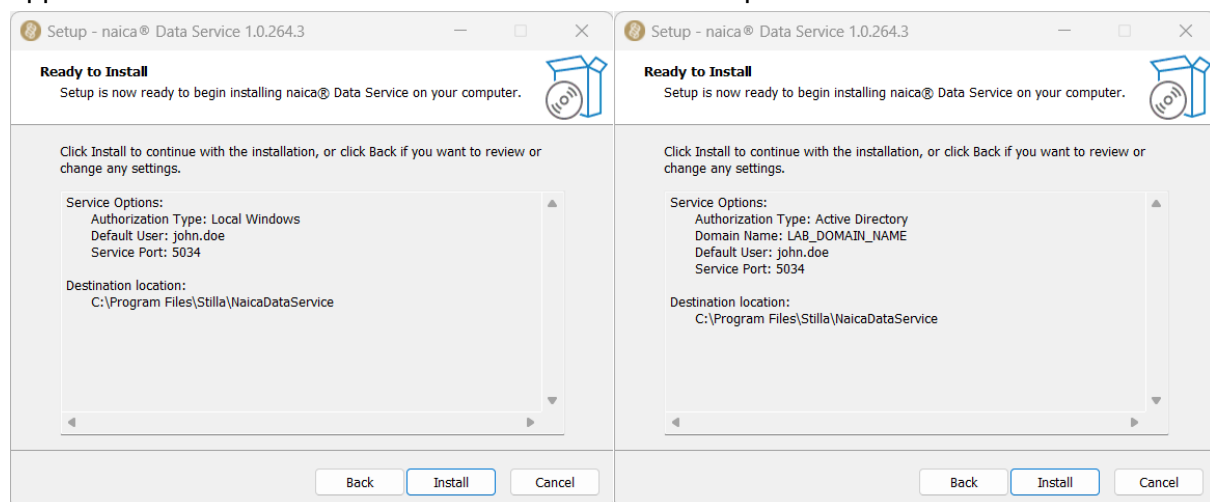
The naica® Data Service installer automatically detects the domain name. Make sure the correct domain name is displayed. Modify if required



15. Specify the default Administrator user and configure the service port number.

The naica® Data Service installer automatically detects the current user's Microsoft Windows Active Directory account ID as the default user. Make sure the correct spelling for the Default User is detected. Correct manually if required. At this stage, it is recommended to use the username of the IT Administrator from the customer's organization as the default user.

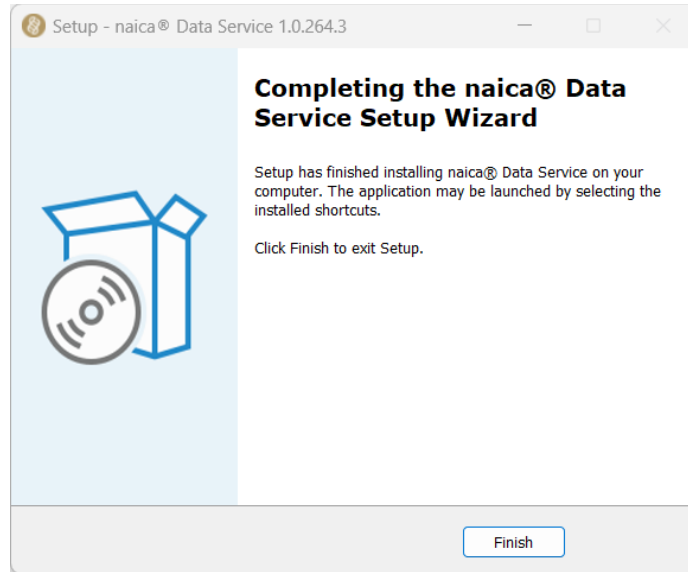
By default, the Service Port is set to « 5034 ». The Service Port can be configured to another value. The PC that is selected to work as a server to host the naica® Data Service application must allow TCP connections on the selected port.



16. Review all specified settings in the « Ready to Install » dialog box

17. Click on « Back » to edit settings.

18. Click on « Install » to complete the naica® Data Service installation with all specified settings.



19. Click on « Finish » to exit the naica® Data Service setup

After successful installation, the naica® Data Service is automatically activated to run on the configured PC.

Note! The PC that is selected to work as a server to host the naica® Data Service application must always be turned on to ensure the 21 CFR Part 11 compliant communication between naica® system instruments, as well as with any separate workstations. The PC hosting the naica® Data Service must not use hibernation to ensure the proper execution of the service software.

3.1.3. naica® Reader Pro & naica® Analysis Pro installation

The naica® Reader Pro and naica® Analysis Pro installers must be executed to install the applications and configure the connection with the naica® Data Service-hosting PC. naica® Reader Pro and naica® Analysis Pro must be installed on every naica® system instrument.

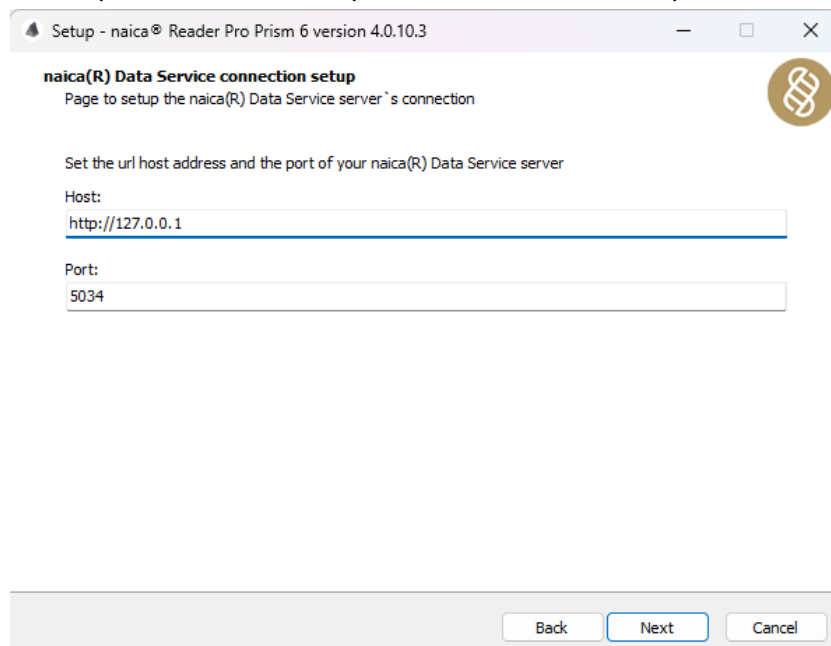
In addition, both applications can be installed on additional workstations meeting the specified minimal technical requirements (Section 3.1.1.1) to allow experiment preparation using naica® Reader Pro and experimental data analysis using naica® Analysis Pro offsite the naica® system instrument.

1. Plug the provided USB device and locate the specific installer files for the naica® system

3-color naica® system	6-color naica® system
Setup_naicaReaderPro_Prism3_v4.0.10.3.exe	Setup_naicaReaderPro_Prism6_v4.0.10.3.exe
Setup-naicaAnalysisPro_v4.0.10.3.exe	

2. Download the files to the PC and double-click to start the installation process.
3. Follow the instructions of the installation wizards.

During the installation process, the URL address of the naica® Data Service's host and the naica® Data Service port number are required information to complete the installation



For local installation options (Section 2.3), the URL host address must be set to « **http://127.0.0.1** ». The port must be configured with the default port number « **5034** ».

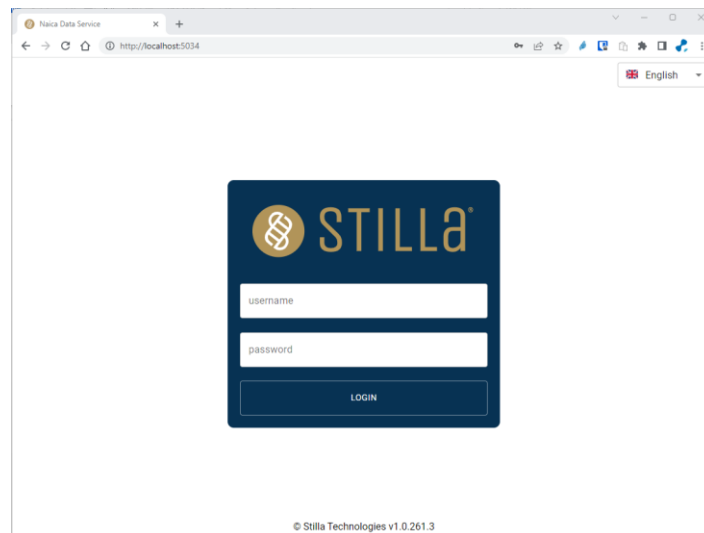
For customer network integrated installation using a separate PC to work as server (Section 2.1), as well as when the naica® system instrument PC is used to work as the server (Section 2.2), the URL host address must be configured with the IP address of the PC hosting the naica® Data Service.

The port must be configured with the port number used by the naica® Data Service.

The configuration parameters will ensure the communication between the customer-configured server and the 21 CFR Part 11 naica® system Pro software applications.

3.1.4. naica® Data Service web interface configuration

1. To configure the naica® Data Service web interface, open a web browser and enter the specific naica® Data Service URL: **http://<server_ip_or_dns>:<port_number>**.
 - a. For network integrated installation options (Sections 2.1 & 2.2) the IT administrator must replace the internet protocol address (IP) or Domain Name Server address (DNS) and the port number, according to the naica® Data Service configuration. It is important to configure the selected server to allow HTTP connexions on the naica® Data Service port. To facilitate naica® Data Service's interface connexions, it is recommended to associate a Domain Name Server (DNS) address to the server.
 - b. For the local installation option (Section 2.3), the default parameters to configure the naica® Data Service web interface are:
 - http://localhost:5034 (DNS)
2. It is recommended to create a bookmark for the naica® Data Service web interface URL in the web browser, to support easy access to the naica® Data Service web interface, without the need to enter the specific complete naica® Data Service URL.



3. The IT administrator must log in to naica® Data Service using their individual Microsoft Windows Active Directory user authentication (username and password) to create the first 21 CFR Part 11 naica® system account.
 - This first 21 CFR Part 11 naica® system account must be a “Lab Manager” account, to allow the creation of additional user accounts, independent of any additional support from the individual IT administrator Microsoft Windows Active Directory user authentication.
 - This first 21 CFR Part 11 naica® system account must be selected among the naica® system users.

For instructions to create and manage 21 CFR Part 11 naica® system user accounts and user roles, refer to Section 4.

4. NAICA® DATA SERVICE ROLES / PERMISSION ADMINISTRATION

4.1. naica® Data Service Permissions

The naica® Data Service software introduces the notion of Permissions. Each User Role grants assigned users access to a set of predefined permissions for the naica® Reader Pro and naica® Analysis Pro software applications.

The permission settings can be administrated through the Roles / Permission tab on the naica® Data Service user interface. All available Permissions are displayed in a list format, where granted permissions are marked with an activated check-box symbol for a defined User Role. Permissions not granted for a User Role display an unchecked box.

The available permissions to select are:

1. Create Templates

The “Create Template” permission allows the user to:

- Register default scanning template files supplied by Stilla Technologies into naica® Data Service. Once registered, the default scanning templates can then be used by users within the same naica® data Service that are assigned to a User Role with the “Run experiment” permission.
- Create and customise scanning template files (.ncx format). The creation and customisation of scanning template files is registered in the naica® Data Service. Once registered, these custom scanning template files can then be used by users within the same naica® data Service that are assigned to a User Role with the “Run experiment” permission.
- Edit scanning template parameters, including the “Experiment Details”, “Embedded Files” and “Scanning Parameters”.

Note: For better traceability, it is recommended that users only use default scanning templates files supplied by Stilla Technologies in the first few optimizations runs of an assay, to define the final scanning template parameters. For routine use, it is recommended to only use specific customized scanning templates parameters.

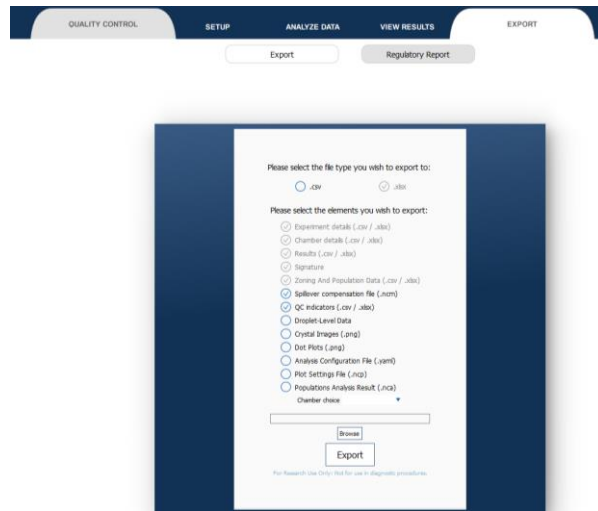
Note: For instructions on how to release a new or an imported scanning template, please see section 5.2.

2. Edit Scanner Settings

The «Edit Scanner Settings» permission allows the configuration of the settings page in the naica® Reader Pro.

3. Export Data

In addition to analytical data included in the 21 CFR Part 11 Regulatory Report, the «Export Data » permission allows the User Role to export all the data files listed below with naica® Analysis Pro. The preselected data elements (greyed out) are always part of the data export. Additional data elements can be selected by activating the checkbox.



Note! Once exported, the data in XLSX and CSV file formats can be edited / modified, outside the naica® system Pro software environment, without Experiment Audit Trail recording. Therefore, only the generated PDF report is to be used for sample results reporting compliant with 21 CFR Part 11.

4. Generate PDF report

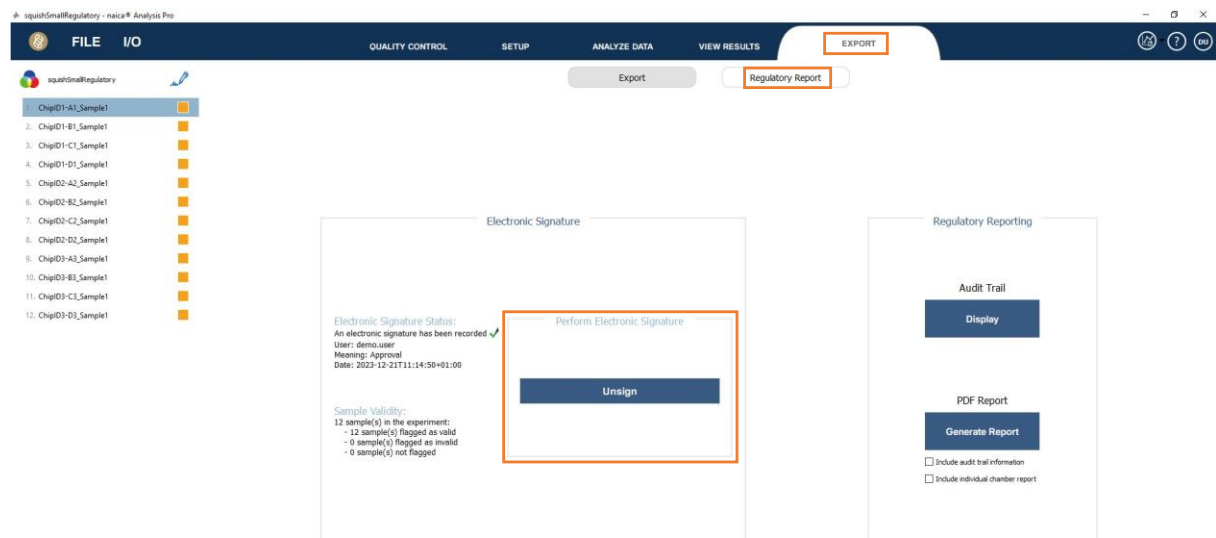
The «Generate PDF report» permission allows the user to create and export a 21 CFR Part 11-compliant PDF report of electronically signed experiments using naica® Analysis Pro. The user has the option to include the experimental audit trail information as part of the PDF report. To electronically sign an experiment, User Role permission «Validate Experiments » is required.

5. Invalidate Experiments

The «Invalidate Experiments» permission allows the user to remove an existing electronic signature executed by a different user. Once the signature is removed, the user can make further data edits or modifications.

In GMP / GLP environments organizations are often operating under « two-man rule / 4-eye principle », where results must be reviewed by a second person as a control mechanism designed to achieve a high level of data security. Under this rule data access, and actions to modify data results, must always be available to more than one authorized person. The «Invalidate Experiments» permission supports the respective 4-eye principle hierarchy within an organization with full compliance for 21 CFR Part 11.

Note: For detailed instructions please see Section 5.3.1 - Electronic Signatures.



6. Manage Users

The «Manage Users» permission allows the user to manage User Roles within the naica® Data Service application.

Only a person with the granted permission «Manage Users» will be able to create new User Roles, or to modify and delete existing User Roles and Permissions.

Only a person with the granted permission «Manage Users» will be able to activate a defined User Role to a new naica® system user or manage / administrate all created Users.

7. Run Experiments

The «Run Experiments » permission allows the user to run experiments with naica® Reader Pro software. The granted «Run Experiment» permission includes the ability to scan experiments, re-scan experiments as well as save experiments.

Note: To be able to scan an experiment, users with the “Run Experiments” permissions, but without the “Create Template” permissions must use existing scanning templates files previously registered by a user with a “Create Template” permission in the naica® Data service software.

8. Validate Experiments

The «Validate Experiments » permission allows the user to conclude the result of the experiment for each individual sample in the experimental run in naica® Analysis Pro software Result Table.



Chamber Name	Chamber Context	Valid Sample	Invalid Sample	Blue Channel				Green Channel				Red Channel			
				Nb Droplets	Dilution	C (cp/vL)	Nb Pos	Dilution	C (cp/vL)	Nb Pos	Dilution	C (cp/vL)	Nb Pos		
1. Chip01-A1_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	100	10	12859	49	10	13238	30	10	10759	43		
2. Chip01-B1_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	200	10	12125	94	10	13048	99	10	12859	98		
3. Chip01-C1_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	300	10	14017	156	10	13484	152	10	12611	145		
4. Chip01-D1_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	400	10	14217	210	10	13333	201	10	12397	191		
5. Chip02-A2_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	500	10	14747	269	10	12934	246	10	13085	248		
6. Chip02-B2_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	600	10	13559	305	10	14017	312	10	13484	304		
7. Chip02-C2_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	700	10	14890	379	10	13021	346	10	13075	347		
8. Chip02-D2_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	800	10	14572	427	10	12720	389	10	13672	409		
9. Chip03-A3_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	900	10	12489	432	10	13069	446	10	13365	453		
10. Chip03-B3_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	1000	10	13702	512	10	12562	482	10	12415	478		
11. Chip03-C3_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	1100	10	13238	550	10	12724	535	10	13659	562		
12. Chip03-D3_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	1200	10	14150	628	10	12427	574	10	12550	578		
13. Chip04-A4_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	1300	10	14048	677	10	12489	624	10	12831	636		
14. Chip04-B4_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	1400	10	13457	708	10	13596	713	10	12436	670		
15. Chip04-C4_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	1500	10	13340	754	10	12710	729	10	13398	764		
16. Chip04-D4_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	1600	10	13333	804	10	13071	793	10	13333	804		
17. Chip05-A5_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	1700	10	14158	890	10	13738	872	10	12281	811		
18. Chip05-B5_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	1800	10	13027	890	10	12839	881	10	13174	897		
19. Chip05-C5_Sample1		<input checked="" type="radio"/>	<input type="radio"/>	1900	10	13603	960	10	12938	935	10	12761	926		

The «Validate Experiments» permission further allows the user to electronically sign the validated result of the entire experiment in the “Regulatory Report” page of the “Export” menu of naica® Analysis Pro software.

Note: For detailed instructions please see Section 5.3.1 - Sample Validation and Electronic Signatures.

4.2. naica® Data Service Roles

The naica® Data Service software introduces the notion of User Role.

The User Roles can be administrated through the Roles / Permission tab on the naica® Data Service user interface.

All available User Roles will be listed in the available drop-down menu in the Roles / Permission tab on the naica® Data Service user interface.

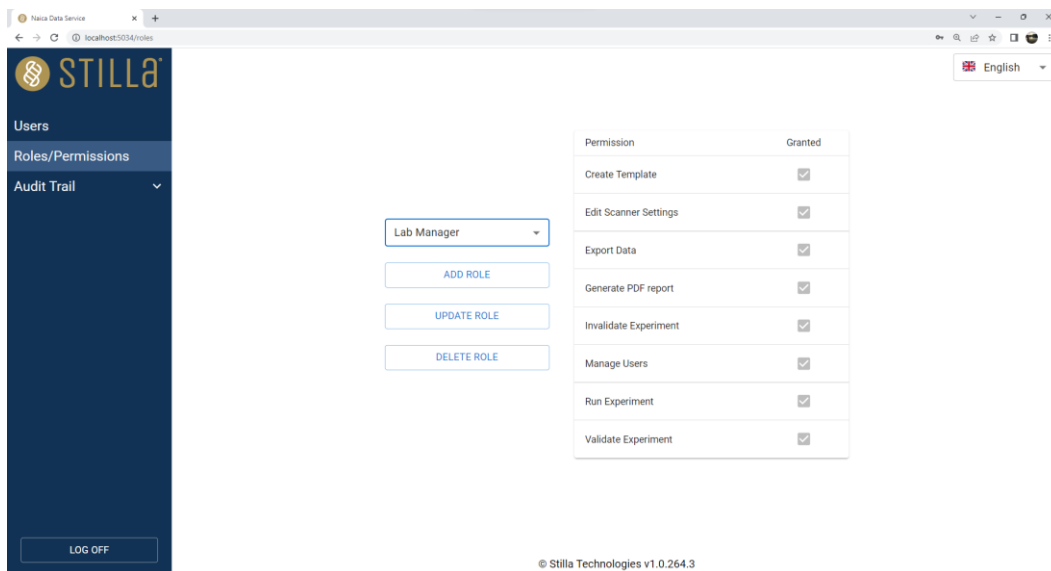
Each User Role defines what naica® Data Service permissions are granted to the assigned users. The User Role manages the access to a set of predefined permissions for the naica® Reader Pro and naica® Analysis Pro software applications.

4.3. Default User Roles

The naica® Data Service installation provides two predefined default User Roles.

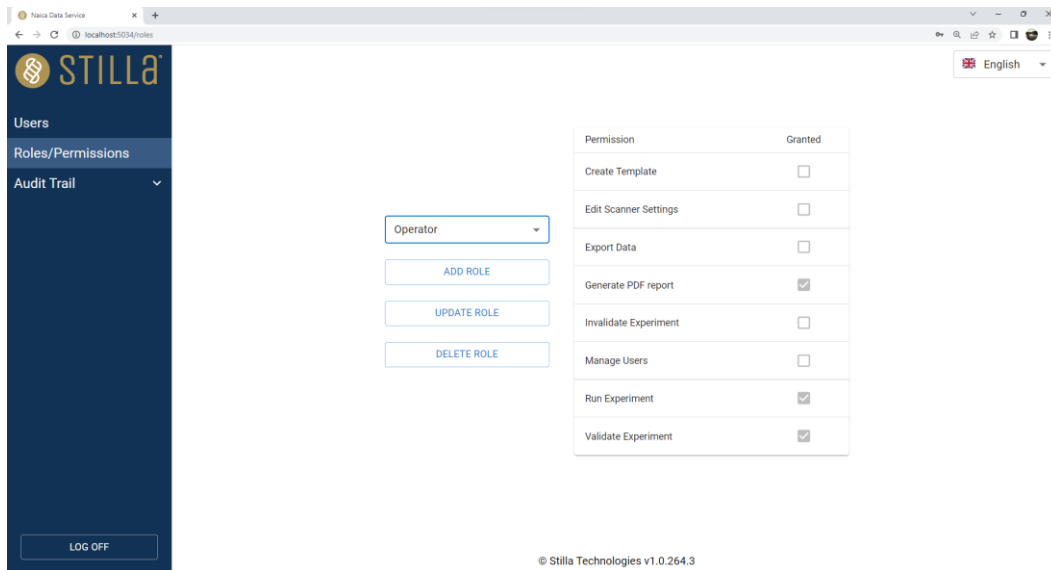
4.3.1. Lab Manager

With the Lab Manager User Role, all available permissions are granted for naica® Reader Pro and naica® Analysis Pro.



4.3.2. Operator

With the Operator User Role, only limited permissions are granted for naica® Reader Pro and naica® Analysis Pro.



An Operator User Role will have permissions to:

- Generate PDF report
- Run experiments
- Validate experiments

The Operator User Role is intended to only have access to validated template files included in the customer's SOP that are released for routine operation after Lab Manager validation.

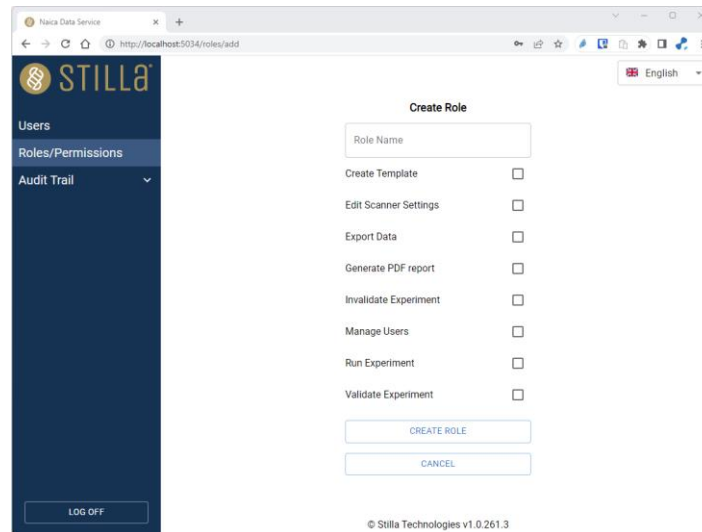
4.4. Administration of customized User Roles

Customized User Roles can be created as described below.

4.4.1. Add Role

To add a new User Role select "Add Role".

Enter the Role Name and select all permissions that are to be included in the customized User Role. Confirm the creation of the new User Role by acknowledging "Create Role". The newly created User Role will then be listed in the User Role drop down menu in the Roles / Permission tab.



4.4.2. Update an existing Role

Click on the **Update Role** button to update any existing User Role.

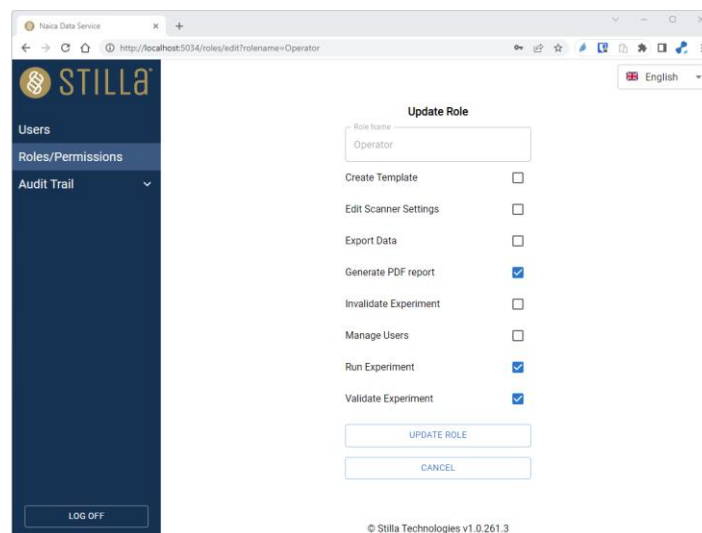
Modify the Role Name

Modify the User Role permission by activating or deactivating permission settings.

Confirm the modifications of the updated User Role by acknowledging “Update Role”.

The updated User Role will then be listed in the User Role dropdown menu in the Roles / Permission tab.

Updated roles / permission settings will be activated for assigned users at the next login to naica® Reader Pro and naica® Analysis Pro.



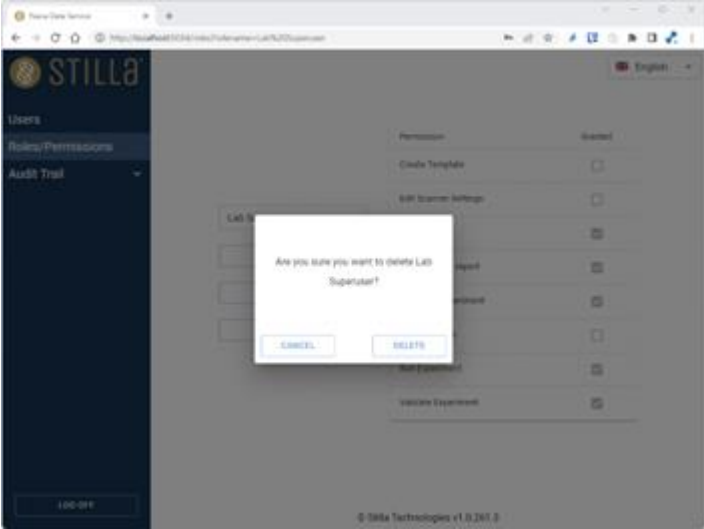
4.4.3. Delete an existing Role

Note: User Roles that are assigned to at least one User cannot be deleted.

Click on the **Delete Role** button to delete any existing User Role.

A warning message will appear. Confirm the deletion of the selected User Role by acknowledging “Delete”.

The deleted User Role will then no longer be listed in the User Role dropdown menu in the Roles / Permission tab.

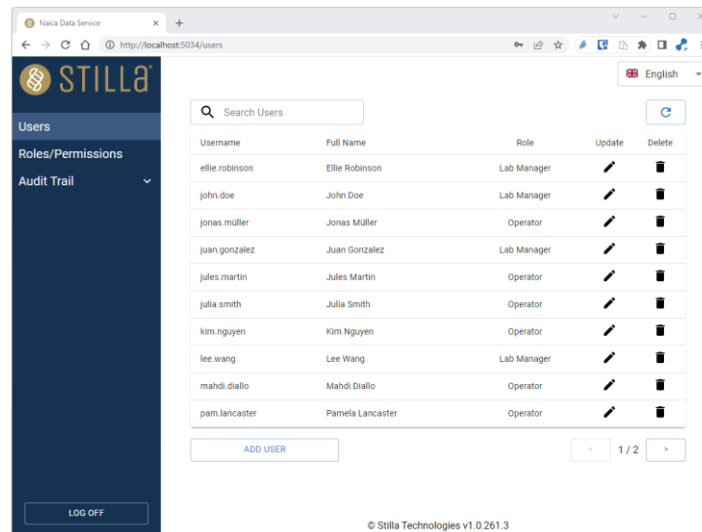


4.5. naica® Data Service User management

For 21 CFR Part 11 compliance it is obligatory to ensure that only authorized individuals have access to naica® Data Service.

Therefore, all users are obliged to log in to the naica® Data Service using individual user authentication credentials (username and password).

The Users menu displays the list of all naica® Data Service user accounts within the customer's organization. All listed naica® Data Service user accounts will be able to log in to all 21 CFR Part 11 naica® system Pro software applications.



Only naica® Data Service User Roles with the permission «Manage Users» can administrate the Users menu to Update, Delete or Add Users.

To modify an existing naica® Data Service user account, click on the respective icon

Update



To update a naica® Data Service user account with a different User Role

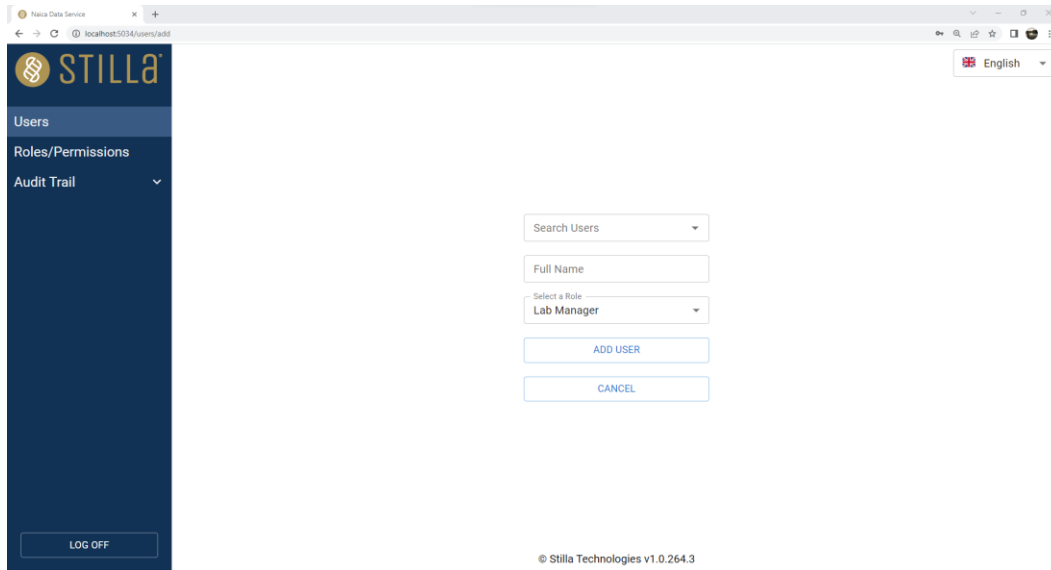
Delete



To delete a naica® Data Service user account.
A warning message will request to confirm the deletion of the selected naica® Data Service user account.

4.5.1. Create new naica® Data Service user account

1. To create a new naica® Data Service user account, click on «Add USER»

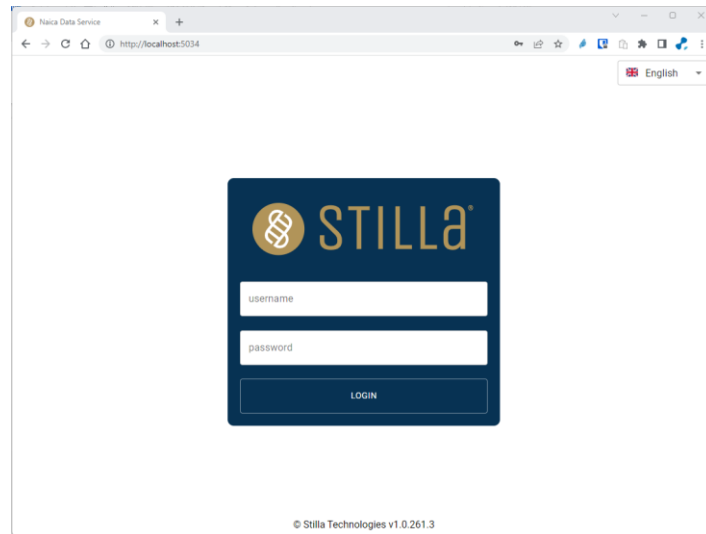


2. Enter the Microsoft Windows username of the new user in the «Search Users» field.
Note! Based on the installation setup in the customer's organization, this Microsoft Windows specific username will either depend on
 - the customer organization's Microsoft Windows Active Directory user authentication (Sections 2.1 & 2.2)
 - local naica® system-specific Microsoft Windows user authentication (Section 2.3)

The naica® Data Service will search all available Microsoft Windows accounts that match the provided username.

3. From the provided list select the correct username.
4. The naica® Data Service will automatically complete the field «Full Name» with information from the Microsoft Windows account.
5. From the available drop-down menu «Select a Role », assign a User Role for the naica® Data Service user account.
6. Confirm the creation of the naica® Data Service user account with «Add User», after validating that all user specific information is correct.

7. The confirmed user account is thereby activated and the user can log into the naica® Data Service application using their individual Microsoft Windows authentication credentials (username and password) in the web interface.

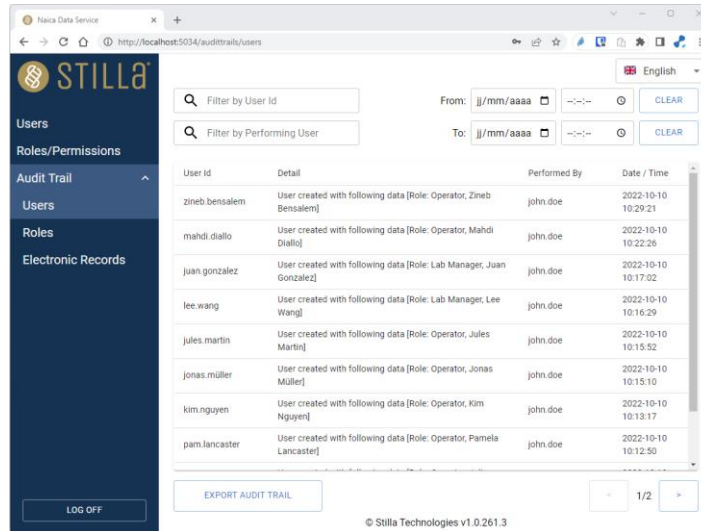


Once logged in to naica® Data Service, any user not executing active events, will automatically be logged-out by the application, to ensure compliance with 21 CFR Part 11. To log in again the naica® Data Service web interface login screen will be presented.

4.6. naica® Data Service Audit Trail

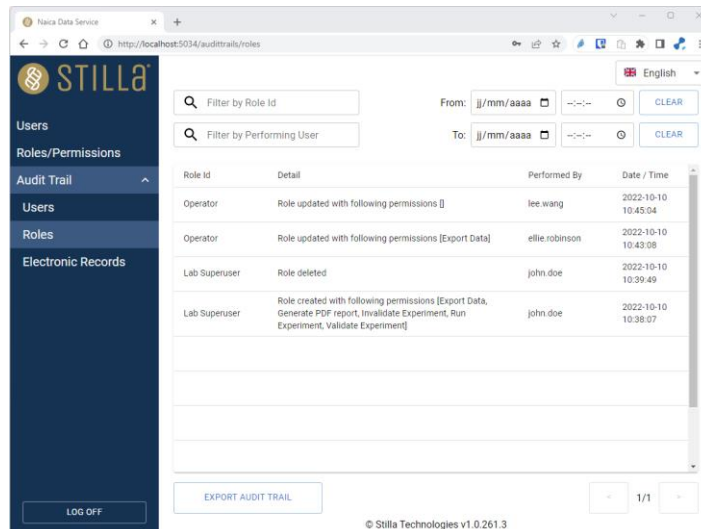
The naica® Data Service Audit Trail provides an automatically generated, time-stamped electronic record that allows to document the history of events related to the creation or modification of electronic records, based on individual naica® Data Service user accounts. Three naica® Data Service Audit Trail categories are available:

1. Users



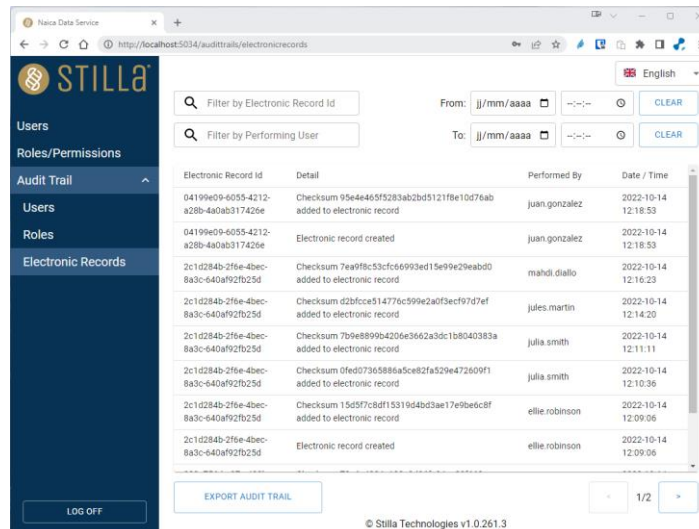
The naica® Data Service Audit Trail «Users» tab documents the event history of naica® Data Service user account management. The naica® Data Service Audit Trail «Users» can be filtered by «User Id», the naica® Data Service user account affected by the recorded event.

2. Roles



The naica® Data Service Audit Trail «Roles» documents the event history of naica® Data Service User Role management. The «Roles» space can be filtered by «Role Id», the naica® Data Service User Role affected by the recorded event.

3. Electronic Records



The naica® Data Service Audit Trail «Electronic Records» documents the event history of any naica® system file. The naica® Data Service Audit Trail «Electronic Records» can be filtered by «Electronic Record Id». The electronic record Id is a unique ID created by the naica® Data Service to identify the event history of any naica® system file. The electronic record checksum is a condensed version of the naica® system file that is required by naica® Data Service to verify the file integrity.

It is important to perform regular back-ups of the naica® Data Service Audit Trail database. The database file is stored in “C:\Program Files\Stilla\NaicaDataService\Naica.db”. It is the responsibility of the customers organization to establish and maintain a backup routine for the naica® Data Service Audit Trail database.

All naica® Data Service Audit Trail categories can be filtered by « Date & Time ». To produce consistent Audit Trails, all computers running 21 CFR Part 11 naica® system Pro software applications must be configured with the correct date and time. It is the customers organizations responsibility to ensure the correct date and time settings are configured. All naica® Data Service Audit Trail categories can be filtered by «Performing User», the naica® Data Service user account executing the recorded naica® Data Service event. All naica® Data Service Audit Trail categories can be exported as a PDF document by clicking «EXPORT AUDIT TRAIL»

5. NAICA® READER PRO & NAICA® ANALYSIS PRO SOFTWARE

This section details the 21 CFR Part 11 specific software features of the naica® Reader Pro & naica® Analysis Pro software.

All general software features common to naica® Reader Pro & naica® Analysis Pro software and Crystal Reader & Crystal Miner software are detailed 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/>

5.1. Individual User Authentication

For 21 CFR Part 11 compliance it is obligatory to ensure that only authorized individuals have access to naica® Reader Pro and naica® Analysis Pro software.

Therefore, all users are obliged to log in to naica® Reader Pro and naica® Analysis Pro using individual user authentication credentials (username and password).

A failed login attempt can come from using incorrect login credentials.

Note! Following several incorrect entries for user login credentials the naica® Data Service account can be locked. Only an IT administrator can reset the user's Windows account to be activated again.

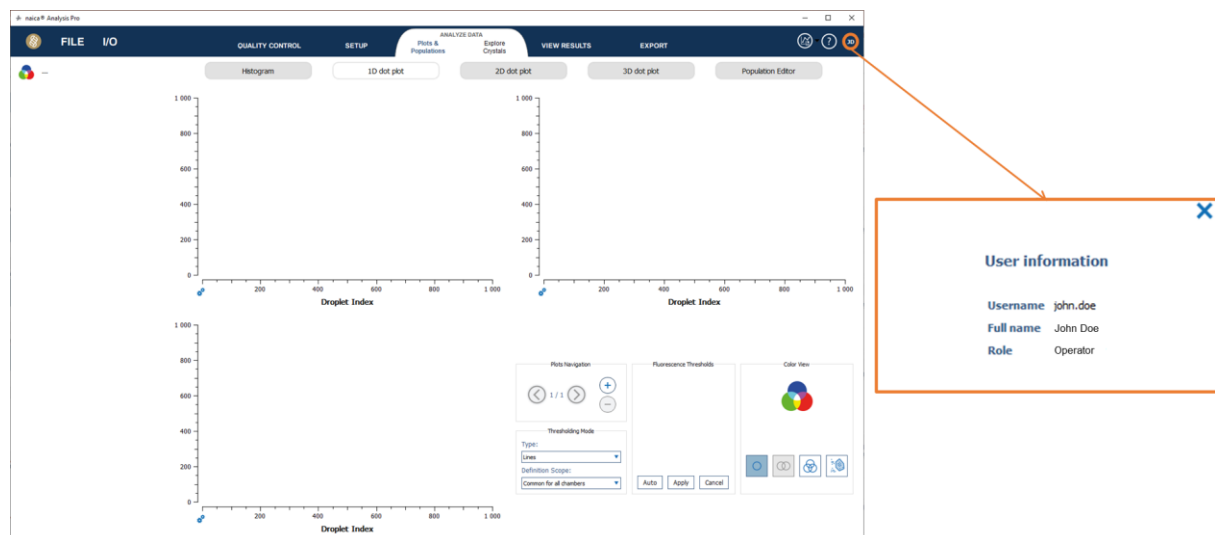
Failed log-in attempts can also be due to a connectivity issue to the naica® Data Service. Please contact the respective IT department to ensure that naica® Data Service connection is provided.

If the user's session expires, the naica® Reader Pro and naica® Analysis Pro will request a new authentication. Any attempt to avoid the user authentication will automatically exit the software, which may lead to unsaved changes.

Automatic log-out is managed through the individual organization's setup for the Microsoft Windows user account settings. However, it is recommended to always proactively close all naica® system Pro software applications if the application is not in use.

Note: The login attempt can fail if the underlying Windows authentication is denied or if the software loses the connection to the naica® Data Service.

In naica® Analysis Pro, the user can click on the login icon to review the individual "User information".



The screenshot shows the naica® Analysis Pro software interface. The main window contains several plots (Histogram, 1D dot plot, 2D dot plot, 3D dot plot, Population Editor) and control panels for 'Plate navigation', 'Fluorescence Thresholds', and 'Color View'. A 'User information' dialog box is open, displaying the following details:

User information	
Username	john.doe
Full name	John Doe
Role	Operator

5.2. naica® Reader Pro scanning template files

To start a run, users must be assigned to a User Role with the permission “Run Experiment” and must use a scanning template registered within the naica® Data Service.

Scanning template files have the same file extension as naica experiment files (.ncx) but do not contain any data and only contain all the information needed for scanning and data analysis. Scanning template files include:

- Parameters and files necessary for scanning and image analysis. These are defined in 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 Stilla Technologies.
 - Experiment details; this includes the information about the scanned channels, and the fluorophores and targets associated to each scanned channel.
 - Scanning parameters; this includes the exposure times for each channel scanned.
- Parameters and files necessary for data analysis. These are defined in 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.

Only users assigned to a User Role including the “Create Template” permission can create and modify scanning template files.

5.2.1. Registering default scanning template files in naica® Data Service

Stilla® Technologies supplies default scanning template files that were validated for different combinations of microfluidic chips and PCR mixes. Each default scanning template file includes pre-defined:

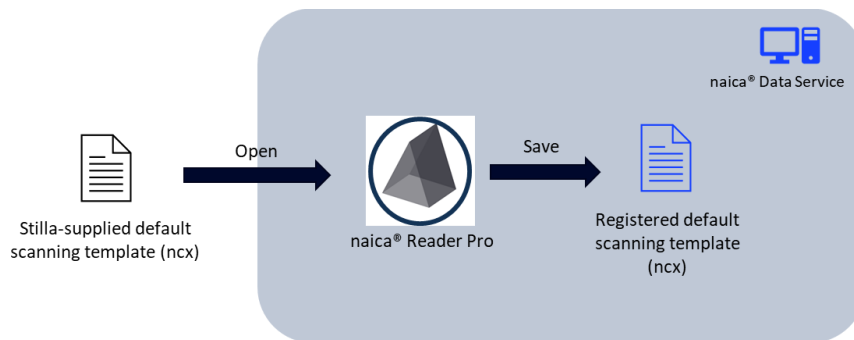
- Image analysis configuration file
- Default scanning parameters

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

Default scanning templates files supplied by Stilla® Technologies are created outside of the user’s naica® Data Service. Before their first use, they must therefore be registered within the user’s naica® Data Service. **Only users assigned to a User Role including the “Create Template” permission can register default scanning template files into naica® Data Service.**

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

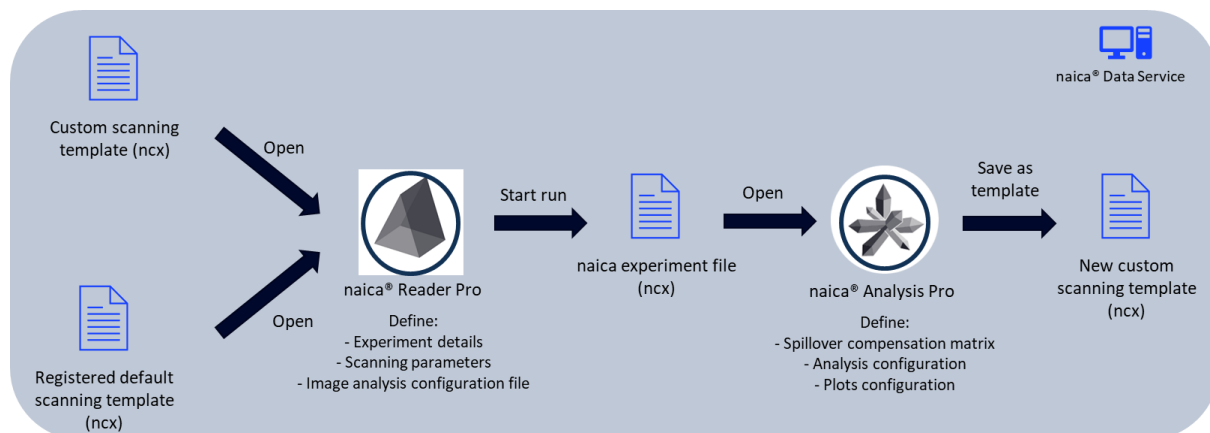
1. In naica® Reader Pro select “New Experiment” and select the default scanning template supplied by Stilla® Technologies.
2. Click on “Save As” to save the scanning template file in a dedicated folder (see next section for recommended naming structure).



5.2.2. Creating a new custom naica® Reader Pro scanning template files

To create a custom scanning template file:

1. In naica® Reader Pro select “New Experiment” and select either a default scanning template file or another existing custom scanning template file.
2. Define the experiment details, scanning parameters and image analysis file as needed for your experiment.
3. Start a run with relevant samples and assay and once the run is over, open the experiment file (.ncx) in naica® Analysis Pro.
4. In naica® Analysis Pro, define the spillover compensation matrix, analysis configuration (thresholding method and populations) and plots configuration.
5. In naica® Analysis Pro, to create the template, select “Save as a template (.ncx)” in the I/O menu and choose a dedicated folder.



Notes:

- Perform a series of assay-specific validation experiments to determine all final scanning template file parameters according to the organization’s SOPs.
- As a good practice to ensure data integrity and traceability, all validated naica® system default scanning template and analysis configuration files should use an identical naming structure, and no two scanning templates should have the same name. It is recommended to name the scanning template explicitly as follows:

ScanningTemplate_InstrumentName_ChipType_PCR-MixName_AssayIndicator_version.ncx

a. File Type: ScanningTemplate

b. InstrumentName: specify the validated naica® system scanner to be used with the respective scanning template file, e.g. Prism3 or Prism6.

- c. *ChipType*: specify the validated chip consumable to be used with the template file, e.g. *SapphireChip* or *RubyChip*.
 - d. *PCR-MIX-Name_AssayIndicator*:
 - i. Either specify the validated reagent consumables to be used with the template file,
 - ii. Or specify an application specific indicator for the validated assay.
 - e. *Version*: it is recommended to manage any change to a template by using a version number to identify specific template file revisions. Increment the version number after each modification of the template file.
- To comply with 21 CFR Part 11, it is recommended to store scanning templates in a dedicated shared directory with “Read-Only” access.
 - It is the user’s responsibility to ensure full compliance with 21 CFR Part 11 for all customized scanning template files with respect to retention period.
 - For routine use, always clearly state the custom scanning template file to use in the a Standard Operation Procedure (SOP) for a given validated assay.

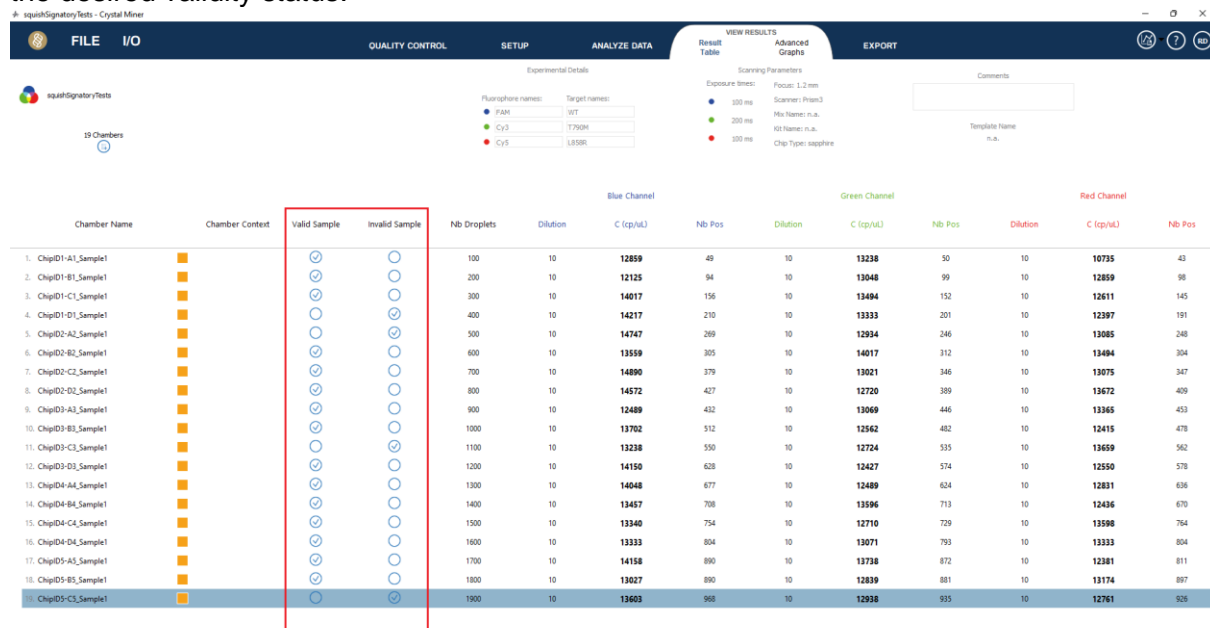
5.3. naica® Analysis Pro sample validation

To be able to sign and export the experiment results, naica® Analysis Pro software requires each individual sample to be reviewed and flagged as “valid” or “invalid”.

Sample acceptance criteria may vary depending on the specific SOP for an application or assay. As such, sample conformity criteria must be defined by the organization using the naica® system within their application area.

The flagging of each individual sample as “valid” or “invalid” is performed in naica® Analysis Pro “View Result” → “Result Table”.

The experiment result table displays two columns: “Valid Sample” and “Invalid Sample”. By default, the status of all samples is undefined. It is possible to apply the same status to a selection of samples; select the samples while pressing the “Shift” or “Alt” key and click on the desired validity status.



The screenshot shows the 'Result Table' in the naica® Analysis Pro software. The table has columns for Chamber Name, Chamber Context, Valid Sample, Invalid Sample, and various assay parameters. A red box highlights the 'Valid Sample' and 'Invalid Sample' columns for the first 18 rows, which are currently empty (undefined).

Chamber Name	Chamber Context	Valid Sample	Invalid Sample	Nb Droplets	Dilution	C (cp/µL)	Nb Pos	Dilution	C (cp/µL)	Nb Pos	Dilution	C (cp/µL)	Nb Pos
1. ChipD1-A1_Sample1	■	○	○	100	10	12859	49	10	13238	50	10	10735	43
2. ChipD1-B1_Sample1	■	○	○	200	10	12125	94	10	13048	99	10	12859	98
3. ChipD1-C1_Sample1	■	○	○	300	10	14017	156	10	13494	152	10	12611	145
4. ChipD1-D1_Sample1	■	○	○	400	10	14217	210	10	13333	201	10	12397	191
5. ChipD2-A2_Sample1	■	○	○	500	10	14747	269	10	12934	246	10	13085	248
6. ChipD2-B2_Sample1	■	○	○	600	10	13559	305	10	14017	312	10	13494	304
7. ChipD2-C2_Sample1	■	○	○	700	10	14890	379	10	13021	346	10	13075	347
8. ChipD2-D2_Sample1	■	○	○	800	10	14572	427	10	12720	389	10	13672	409
9. ChipD3-A3_Sample1	■	○	○	900	10	12489	432	10	13069	446	10	13365	453
10. ChipD3-B3_Sample1	■	○	○	1000	10	13702	512	10	12562	482	10	12415	478
11. ChipD3-C3_Sample1	■	○	○	1100	10	13238	550	10	12724	535	10	13659	562
12. ChipD3-D3_Sample1	■	○	○	1200	10	14150	628	10	12427	574	10	12550	578
13. ChipD4-A4_Sample1	■	○	○	1300	10	14048	677	10	12489	624	10	12831	636
14. ChipD4-B4_Sample1	■	○	○	1400	10	13457	708	10	13596	713	10	12436	670
15. ChipD4-C4_Sample1	■	○	○	1500	10	13340	754	10	12710	729	10	13598	764
16. ChipD4-D4_Sample1	■	○	○	1600	10	13333	804	10	13071	793	10	13333	804
17. ChipD5-A5_Sample1	■	○	○	1700	10	14158	890	10	13738	872	10	12381	811
18. ChipD5-B5_Sample1	■	○	○	1800	10	13027	890	10	12839	881	10	13174	897
ChipD5-C5_Sample1	■	○	○	1900	10	13603	968	10	12938	935	10	12761	926

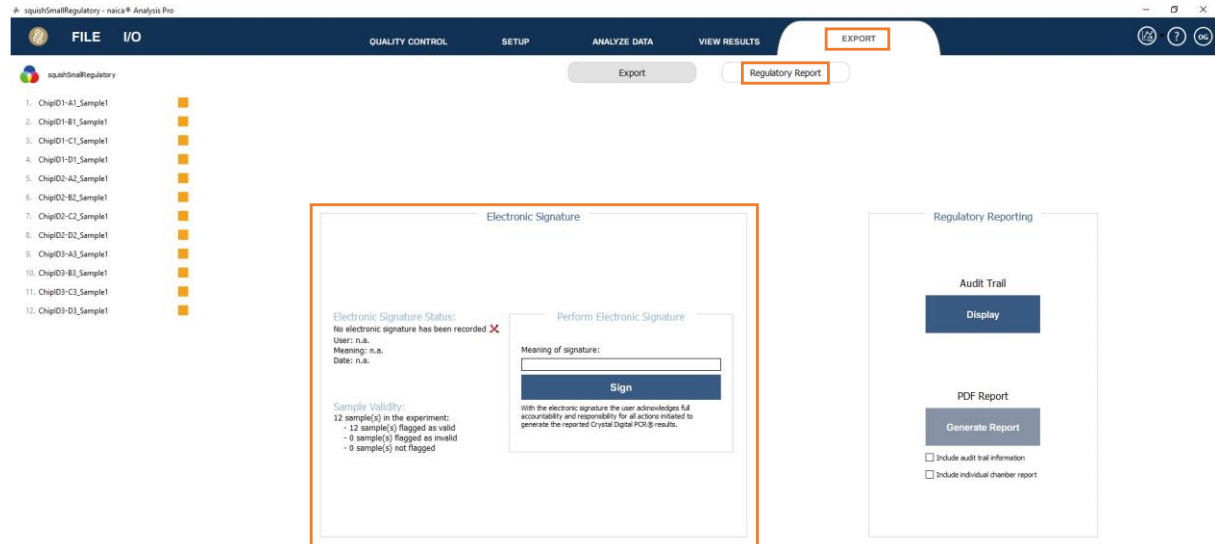
Sample validation for pooled chambers:

When using the “Pooled Chamber” feature, the experiment validity status of the individual sample chambers cannot differ from the pooled chamber sample result.

- If the validity status of all individual sample chambers that compose a pooled chamber sample result are consistent, the validity status of the pooled chamber sample is implicitly set to the same value.
- If the validity status of the individual sample chambers selected for pooling differ, the validity status of the pooled chamber sample remains undefined.
- It is also possible to assign a validity status for the pooled chamber sample directly. By doing this, the validity status of the individual sample chambers will be overwritten to match the pooled chamber sample validation status.

5.3.1. Electronic signatures

naica® Analysis Pro software enables the electronic signature of all validated experiment results, provided that the respective User Role has signature permissions. “Electronic Signature” is available in the “Regulatory Report” page of the “EXPORT” menu.



The Electronic Signature section is structured as follows:

1. Electronic Signature Status displays a summary of the electronic signature status for the individual experiment file:
 - Record of the file has already been signed or not
 - Record of signature user identification
 - Record of signature meaning
 - Record of signature date and time
2. Sample Validity displays a summary of the concluded sample results for the experiments:
 - Record of number of samples in the experiment file flagged as valid
 - Record of number of samples in the experiment file flagged as invalid
 - Record of number of samples in the experiment file not flagged

Note! To electronically sign an experiment, it is mandatory to first flag the result of all samples in the experiment file as “valid” or “invalid” in the “Result Table” page of the “VIEW RESULTS” menu. If the samples have not all been flagged, a warning message is displayed in the “Perform Electronic Signature” section, and it will not be possible to proceed with electronic signature.

3. Perform Electronic Signature

To execute the electronic signature for the experiment file it is optional to define a meaning of the electronic signature.

- Meaning of the electronic signature

The default value for the meaning of electronic signature is set to display “n.a.”

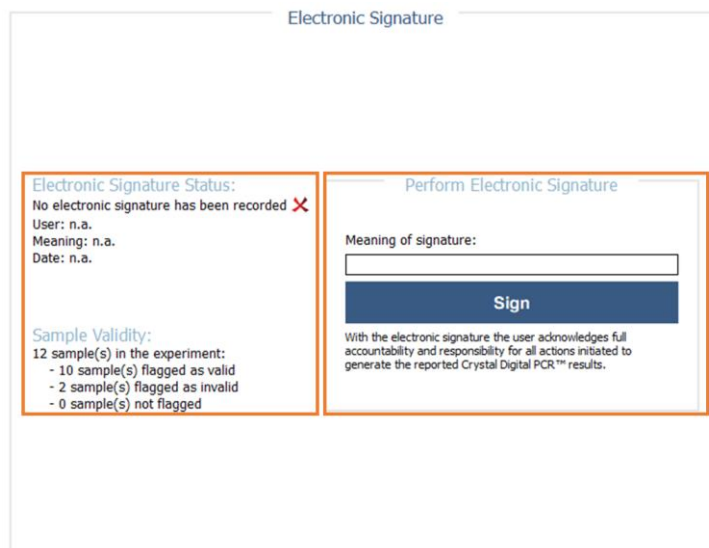
In GMP / GLP environments, organizations are often operating under « two-man rule / 4-eye principle », where results must be reviewed by a second person as a control mechanism designed to achieve a high level of data security. The «Meaning of

electronic signature» field allows to establish an organization-tailored result-release hierarchy with full compliance for 21 CFR Part 11.

The individual meanings of electronic signatures within an organization must be defined within the specific organization process.

- Sign

To execute the electronic signature for the experiment file, it is mandatory to confirm the electronic signature, by again performing a new authentication with login (username and password). With the electronic signature the user acknowledges full accountability and responsibility for all actions initiated to generate the reported Crystal Digital PCR® results.

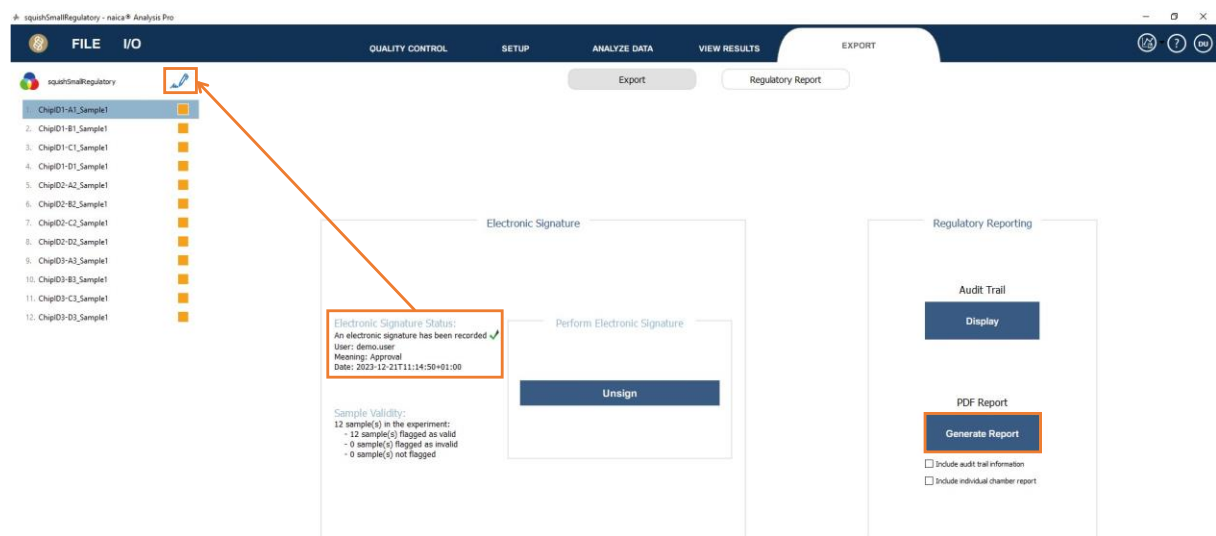


Once the experiment is signed, a signature icon appears to the right of the experiment name in the top left corner of the experiment file that remains displayed in all naica® Analysis Pro software menus (see below).



The signature icon provides the visual indication that the experiment has been electronically signed and is therefore locked to prevent any further modifications.

Subsequently, all naica® Analysis Pro features allowing modifications to the experiment file are disabled throughout the software menu.



- Unsign

The author of an electronic signature is always allowed to remove their electronic signature. To remove the electronic signature of an experiment, click on the “Unsign” button and confirm the user identity with login authentication (username and password) to finally remove the electronic signature.

To be able to edit the experiment file, previously electronically signed by a different Author, the user who attempts to modify the experiment file must have the User Role permission “Invalidate experiment”. If this “Invalidate experiment” permission is not held by the current user, a “Permission denied” message will be displayed.

5.3.2. Experiment Audit Trail

The Experiment Audit Trail records all edition events in naica® Reader Pro and naica® Analysis Pro software applications for an experiment file.

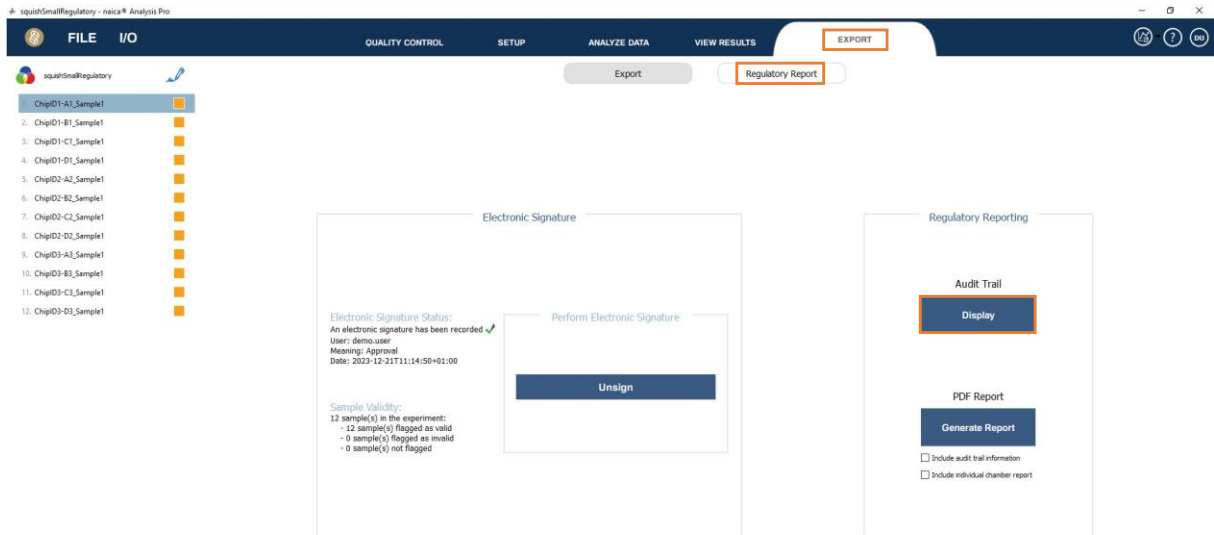
Events included in the Audit Trail record are:

- 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 timestamp.

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.

The Experiment Audit Trail can be reviewed within naica® Analysis Pro software. To open the Experiment Audit Trail viewer:

- Click on the “EXPORT” menu
- Open the “Regulatory Report” tab
- In the “Regulatory Reporting” section click on “Display” underneath “Audit Trail”



The screenshot displays the naica® Analysis Pro software interface. The top navigation bar includes 'FILE I/O', 'QUALITY CONTROL', 'SETUP', 'ANALYZE DATA', 'VIEW RESULTS', and 'EXPORT'. The 'EXPORT' menu is open, showing 'Export' and 'Regulatory Report' options. On the left, a list of 12 samples is shown, each with a corresponding status icon. The main content area is divided into two panels: 'Electronic Signature' and 'Regulatory Reporting'.

Electronic Signature Panel:

- Electronic Signature Status:** An electronic signature has been recorded ✓
User: demo-user
Meaning: Approval
Date: 2023-12-21T11:14:50+01:00
- Sample Validity:**
12 sample(s) in the experiment:
- 12 sample(s) flagged as valid
- 0 sample(s) flagged as invalid
- 0 sample(s) not flagged
- Perform Electronic Signature:** A box containing an 'Unsign' button.

Regulatory Reporting Panel:

- Audit Trail:** A 'Display' button.
- PDF Report:** A 'Generate Report' button.
- Options: Include audit trail information, Include individual chamber report

5.3.3. Experiment PDF Report creation

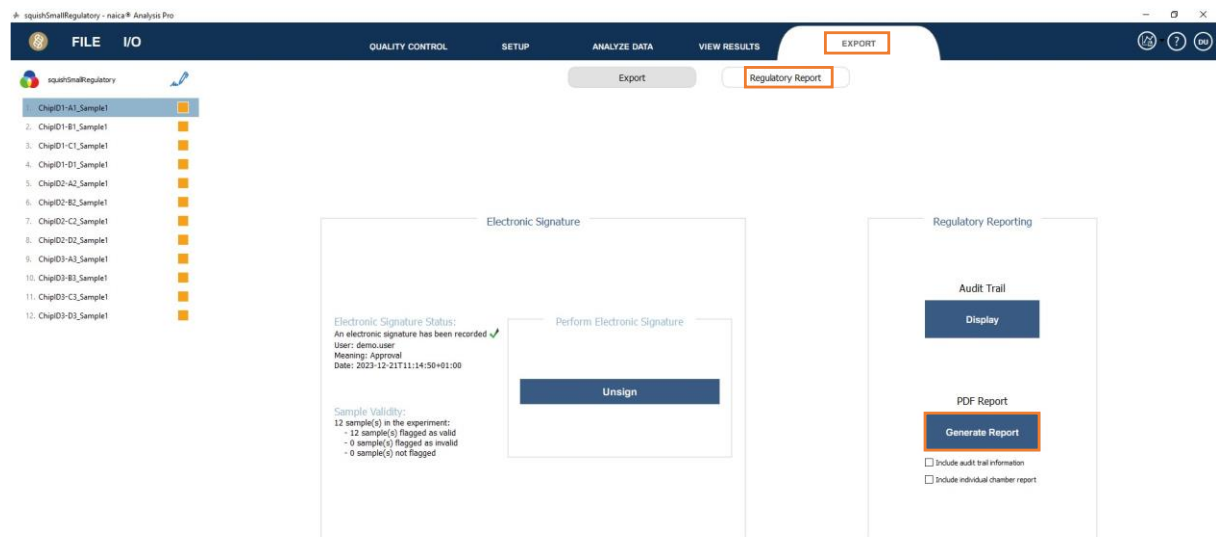
Note: The Experiment PDF report can only be created if the experiment file was signed electronically. All date and time stamps are displayed with the ISO 8601 format.

To export the Experiment PDF Report :

- Open the “Regulatory Report” tab
- In the “Regulatory Reporting” section, click on “Generate Report” underneath “PDF Report”.

Optionally it is possible to include individual chamber report or the audit trail in the Experiment PDF Report:

- To include the Experiment Audit Trail in the PDF Report check the “Include audit trail information” box underneath “Generate Report”.
- To include the individual chamber report in the PDF Report check the “Include individual chamber report” box underneath “Generate Report”.
- Choose the file directory and confirm by clicking ok.
- Upon PDF Report export completion, the PDF file is automatically opened with the default PDF viewer.



The PDF report can be printed in US Letter or A4 format.

The Experiment PDF Report includes:

- The experiment name
- A “User and software traceability information” section, including:
 - Electronic signature operator, date, and time
 - Electronic signature meaning
 - Scan operator, date, and time
 - Report generation operator, date, and time
 - Software name and version used to create the PDF Report
 - Software name and version used to scan the chambers
- An “Experiment and analysis setup information” section, including:

- Instrument type identification
- Instrument Serial Number
- Instrument focus parameters
- Chip type
- Scanning template name
 - Note: To ensure data integrity and traceability, it is important that no two scanning templates have the same name. Best practice is to use an identical naming structure for scanning templates– see section 5.2.*
- Number of analyzed chambers
- Number of analyzed samples (considering pooled chambers)
- Spill-over compensation matrix
- Thresholding scope (common to all chambers or individually per chamber)
- Thresholding type (Lines or Polygons)
- A description of the scanned channels, including:
 - Channel name
 - Fluorophore name
 - Target name
 - The time exposure
- A “Chip Layout” section, including for each chip holder:
 - Chip ID
 - Chamber ID
 - Sample name
 - Pooling ID – if chambers are pooled, the pooling ID is written between brackets next to the Chamber ID.
- A “QC Indicator” section, included for each individual chamber:
 - Chamber ID
 - Sample name
 - Chamber context
 - Image Sharpness quality for chamber
 - Number of analyzable droplets for chamber
 - Number of saturated objects for chamber
 - General quality flag for chamber
 - For the quality flags, High is equivalent to a “Green” flag and Low is equivalent to a “Yellow” flag.
- A “Result Table” section, included for each individual chamber and pooled chamber:
 - Chip ID
 - Chamber ID
 - Chamber context
 - Sample name
 - Sample validity status
 - Population name
 - Dilution factor
 - Concentration

- Number of positive droplets per population
- Number of negative droplets per population
- Separability score
- Minimum concentration
- Maximum concentration
- Relative uncertainty
- Footer section including:
 - Report generation operator, date and time
 - Experiment name
 - Current page and total number of pages

The Experiment PDF Report can also include the following two optional sections, if selected by the user:

- Individual and pooled chamber level information.
This includes, for each individual chamber and each pooled chamber:
 - The pooling/chamber name
 - A “Pooling/Chamber details” section, including:
 - Chamber ID
 - Sample name
 - Chamber/Pooling context
 - Pooling ID
 - General quality flag for pooling
 - Image sharpness quality for chamber
 - Number of analyzable droplets for chamber
 - Number of saturated objects for chamber
 - Per channel: The sample type
 - U = unknown
 - P = positive
 - N = negative
 - S = standard
 - Dilution factor
 - A “Chamber/Pooling result” section, including:
 - Sample validity status
 - Total number of droplets per chamber / pooling
 - Per channel:
 - Dilution factor
 - Concentration
 - Number of positive droplets
 - Number of negative droplets
 - Minimum concentration
 - Maximum concentration
 - Relative uncertainty
 - Separability score

- The PDF Report displays the experiment 2D plots, as configured in the “ANALYZE DATA” menu, “Plots & Population” tab, “2D dot plot” section.
- The experiment audit trail.

Note:

- *The chambers in the ‘QC indicators’ table and the ‘Results’ table will appear in the same order as they appear in the Analysis Pro software when the Experiment PDF Report is generated.*
- *The “Populations” that appear in the “Results” table correspond to the same populations that are visible in Analysis Pro software.*

6. SERVICE & SUPPORT

For technical questions or any issue regarding instrument or software malfunction contact:

For customers from Europe, China and Africa:
Monday to Friday, 9:30 AM - 6:30 PM, Central European Time (CET).
Closed on French bank holidays.
Phone: (+33) 9 82 27 47 47
Email: support@stilla.fr.

For customers from America, Asia (excluding China) and Oceania:
Monday to Friday, 8:00 AM – 6:00 PM, Eastern Standard Time (EST).
Closed on American bank holidays.
Phone: 1-833-888-0150 ext. 1
Email: support@stilla-inc.com

Online Technical Support is also available at: www.stillatechnologies.com/technical-support/

We will try our best to answer as promptly as possible.

Please ensure to provide the following information when contacting the respective service & support team:

- The naica® system software version number
 - For the naica® Reader Pro and naica® Analysis Pro application this is available in the “About” section on the Home page.
 - For the naica® Data Service it is available at the bottom of the web interface, once logged in.
- The log files of the experiments which have been generated in the directories:
“%USERPROFILE%\Stilla\NaicaReaderPro”
“%USERPROFILE%\Stilla\NaicaAnalysisPro”
- The log files of the naica® Data Service which have been generated on the computer hosting the service in the file:
“C:\Program Files\Stilla\NaicaDataService\Logs”

naica® system Pro software 21 CFR Part 11

Headquarters
Stilla Technologies
Villejuif Biopark
1, Mail du Professeur Georges Mathé
94800 Villejuif, FRANCE
Phone: (+33) 09 82 29 50 50

North American Office
Stilla Technologies Inc.
20 Blanchard Road, Suite 9,
Burlington, MA 01803, USA
Tel : 1-833-888-0150

www.stillatechnologies.com

Pat.: www.stillatechnologies.com/patents



MKT-00150 Rev. C