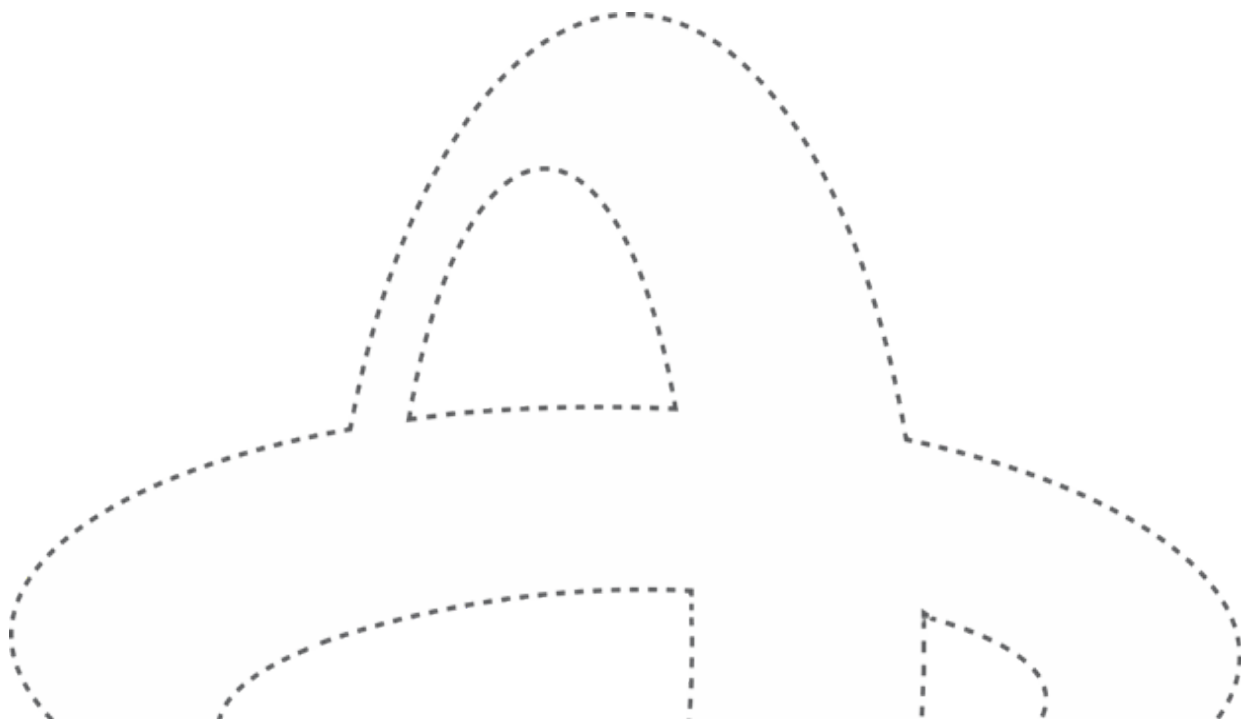




USER MANUAL nCommand

Lite v2.4

Manual Version: V.3



Contents

Chapter 1	Introduction	4
Section 1.1 -	Purpose.....	4
Section 1.2 -	Glossary	4
Section 1.3 -	Description	5
1.3.1.	Intended Use	5
1.3.2.	Indications for Use	5
1.3.3.	Intended Patient Population.....	6
1.3.4.	Environment of Use	6
1.3.5.	Contraindications	6
1.3.6.	Platform Capabilities	6
1.3.7.	Clinical Benefits	6
1.3.8.	Intended Users	7
1.3.9.	Operating Environment.....	7
1.3.10.	Facility Environment	7
1.3.11.	Minimum Requirements.....	8
1.3.12.	Symbols	10
1.3.13.	Service Life	11
1.3.14.	Upgrade / Update	11
Chapter 2	General Warnings and Precautions List	12
Chapter 3	Platform Use in Each Location	14
Section 3.1 -	Access and Use of nCommand Lite.....	14
Section 3.2 -	Accessing the Platform for the First Time	14
3.2.1.	Login via nCommand Lite	14
3.2.2.	Login via External IdP.....	16
Section 3.3 -	Password Management	17
Section 3.4 -	Access with Local Technologist Profile.....	20
Section 3.5 -	Access with Remote Technologist Profile.....	22
3.5.1.	Access Mode	23
3.5.2.	Streaming Bar	25
3.5.3.	Multi-camera	28
3.5.4.	Open Another Device	30

3.5.5.	System Check.....	32
Section 3.6 -	Chat	33
Section 3.7 -	Ending Your Session on the Platform	37
Section 3.8 -	Operational Training	39
Section 3.9 -	Troubleshooting Guidelines	40
Section 3.10 -	Hardware Cleaning Methods	44
Chapter 4	Cybersecurity and Privacy	45
Section 4.1 -	Security and Privacy Risks	45
Section 4.2 -	Personal Data Protection (GDPR / HIPAA Compliance)	45
Section 4.3 -	Access Management and Authentication.....	46
Section 4.4 -	System Check Access Control.....	46
Section 4.5 -	Regional Data Segregation and Log Retention	46
Section 4.6 -	Data Security and Integrity.....	47
Section 4.7 -	Security Incident Response	47
Chapter 5	Service Channels.....	48
Chapter 6	Legal and Regulatory Information.....	49
Chapter 7	Revision History	52
APPENDIX I -	Service Start Checklist	53

**CAUTION**

Federal law restricts this device to sale by or on the order of a physician, as used by a medical technologist licensed in the state where he/she practices.

(for United States of America)

**CAUTION**

In Brazil, this software is authorized by Anvisa for use exclusively with Magnetic Resonance Imaging (MRI) device. Any other use is not permitted.

(for use in Brazil)

**CAUTION**

Before use, make sure you are aware of the specific requirements of your country or region. Failure to comply with regulations may result in health risks.

**CAUTION**

Ensure that the version of this user manual matches the version of the platform in use. Using a mismatched version may result in incorrect operation or misinterpretation of features.

Chapter 1 Introduction

Section 1.1 - Purpose

This manual aims to provide local and remote technologists with a comprehensive understanding of the specific functionalities of the nCommand Lite System. Serving as a User Manual, this document provides concise and practical information, guiding users through system's functionalities and troubleshooting. By following this manual, users will be able to use nCommand Lite efficiently, helping to maximize productivity and reduce dependence on technical support.

Section 1.2 - Glossary

**CAUTION**

This label applies to conditions or actions that have potential hazard. You may cause minor injury or property damage if you ignore these instructions.

**WARNING**

This label identifies conditions or actions which result in a specific hazard. You will cause severe personal injury, or substantial property damage if you ignore these instructions.

Platform Term	Corresponding Term
Imaging Facility	Medical Facility, Unit, Mobile Units, Healthcare Facility, Healthcare Unit
Remote Facility	Remote Workstation, Remote Place, Remote Office, Remote Location, Command Center
Platform	nCommand Lite web application
System	nCommand Lite with all subsystems
Device	Medical Scanner, Scanner, Equipment, Medical Device, Imaging Device, Imaging Equipment
Local Technologist	Local User, Local Technician, Local Healthcare Professional (LHP), On-site User

Section 1.3 - Description

The nCommand Lite System is a SaMD (Software as a Medical Device) that is customer-facing and provides remote access through a web application for viewing/reviewing images as well as the ability to remotely provide real-time guidance to the near-patient licensed technologist (local user) operating the medical imaging devices in the context of training or procedure assessment, for MRI, CT, and PET/CT scanners.

Remote users are licensed technologists, who are able to access an imaging medical device from a computer that meets the minimum required specifications anywhere, using a secure software connection that streams video and provides keyboard and mouse access. This allows remote users to assist local users without distance being a limitation. This access must be granted by the local user using the system, and it can also be revoked at any time by the local user, thus allowing him/her to maintain complete control of the session at all times. Also, each remote session is controlled via a secure credential that is managed by the local user. Connections to a medical device are limited to one remote session at a time to maintain strict control over who is remotely interacting with the system. Images reviewed remotely are not for diagnostic use.

nCommand Lite System consists of an IT hardware and software-based installation solution that supports multi-sessions, allowing remote technologists to access multiple medical imaging devices as needed. Scanners that are compatible with the nCommand Lite System comply with a common protocol, allowing for scanning parameter management and remote scanning.

1.3.1. Intended Use

The nCommand Lite System provides remote access for viewing/reviewing images, as well as the ability to remotely provide real-time guidance to the licensed technologist operating the scanner. This guidance includes training, procedure assessment, and scanning parameter management.

1.3.2. Indications for Use

The nCommand Lite System allows remote access for viewing/reviewing images, as well as the ability to remotely provide real-time guidance to the licensed technologist operating a compatible MRI, CT, or PET/CT scanner. This access must be granted by the local licensed technologist

who is operating the system. Remote access is only available for systems supporting remote connectivity capability. Images reviewed remotely are not for diagnostic use.

1.3.3. Intended Patient Population

For any patient prescribed to undergo imaging via a connected imaging medical device.

1.3.4. Environment of Use

Imaging facilities that carry out Magnetic Resonance Imaging (MRI), Computed Tomography (CT) and Positron Emission Tomography – Computed Tomography (PET/CT) exams and remote Command Centers.

1.3.5. Contraindications

The platform should not be operated by users who are not licensed technologists and who have not received training in using nCommand Lite.

1.3.6. Platform Capabilities

- **Remote Scanning:** exhibits medical imaging device screen in real time, allowing a remote licensed technologist to attend an exam.
- **Chat:** makes communication available between the remote and local licensed technologists through text and voice messages. The local and remote technologists can also make and receive voice and video calls.
- **Multi-camera:** facilitates remote observation of patients and the medical facility during the procedure. The remote technologist can access the view of the cameras through the tabs that are divided between all camera tabs and the individual ones. This mechanism replicates the visual oversight a healthcare professional would have if situated near the patient, thereby introducing an augmented layer of safety.
- **Multisession remote scanning** allows the remote technologist to access multiple medical imaging devices as needed.
- **Access mode:** allows the remote technologist to choose between views or to control the device. In view mode, remote technologists can only see what is streaming. In Control mode he/she has control over the mouse and keyboard.
- **Manage remote technologist access:** allows the local technologist to control the remote technologist access and their access mode (View or Control). To allow the remote technologist connection, access must be granted by the local technologist using the platform, and it can also be revoked at any time by the local technologist, thus allowing him/her to maintain complete control of the session at all times.
- **Streaming size:** the remote technologist can see the original streaming size and the current streaming size in pixels. He/she is also notified when the current streaming size is smaller than the original.
- **Mouse and Keyboard Status:** the remote technologist has feedback if the medical imaging device's mouse and keyboard are working correctly.
- **Session details:** local and remote technologists can access details about the session.

1.3.7. Clinical Benefits

nCommand Lite enhances diagnostic imaging by enabling the remote operation of **MRI, CT, and PET-CT** systems, ensuring consistent imaging quality and adherence to protocols. It allows experienced technologists to oversee and assist with scans in real time, optimizing workflow efficiency and reducing errors that could affect diagnostic accuracy. The system facilitates

collaboration between technologists, improving exam consistency and enabling faster decision-making in complex cases. By enabling remote professionals to support multiple facilities, **nCommand Lite** increases the **availability, variety, and quality** of imaging exams, ensuring that more patients have access to advanced diagnostics while optimizing healthcare resources. Additionally, it helps mitigate staff shortages by reducing dependence on on-site specialists, all while maintaining compliance with strict regulatory and data security standards.

1.3.8. Intended Users

- **Local Technologist**

The local technologist is the on-site user responsible for assisting and guiding patients in-person at the medical facility. He/she must have the necessary knowledge to perform scanning procedures for a given imaging device. Additionally, he/she controls the remote technologist's access mode (View or Control) and the remote access must be granted by the local technologist via the platform and can be revoked at any time.

- **Remote Technologist**

A professional who performs operations remotely, with access to and control of the device computer. Like the local technologist, the remote technologist must also have the necessary knowledge to perform scanning procedures for a given imaging device.

- **Support/IT User**

Professional responsible for setting up the platform (not included in this User Manual).

1.3.9. Operating Environment

The following specifications refer to the environmental requirements of the e-KVM computer.

- **Maximum altitude (without pressurization)**

- Operating: From 0 m (0 ft) to 3048 m (10 000 ft)
- Storage: From 0 m (0 ft) to 12192 m (40 000 ft)

- **Temperature**

- Operating: From 10°C (50°F) to 35°C (95°F)
- Storage: From -10°C (14°F) to 50°C (122°F)

- **Relative humidity**

- Operating: 20%-80% (non-condensing)
- Storage: 10%–90% (non-condensing)

1.3.10. Facility Environment

The nCommand Lite platform has two different environment location types:

- **Imaging Facility:** Facilities that carry out Magnetic Resonance Imaging (MRI), Computed Tomography (CT) or Positron Emission Tomography – Computed Tomography (PET/CT) exams.
- **Remote Facility:** A location where remote technologists can access and remotely manage devices (MRI, CT, or PET/CT scanners). This workstation can be used in various environments such as offices, command centers, remote locations, or even secondary locations within the healthcare facility. The remote workstation can be located in any space

that provides the user with appropriate conditions for concentration and minimum connectivity, and computer configuration requirements.

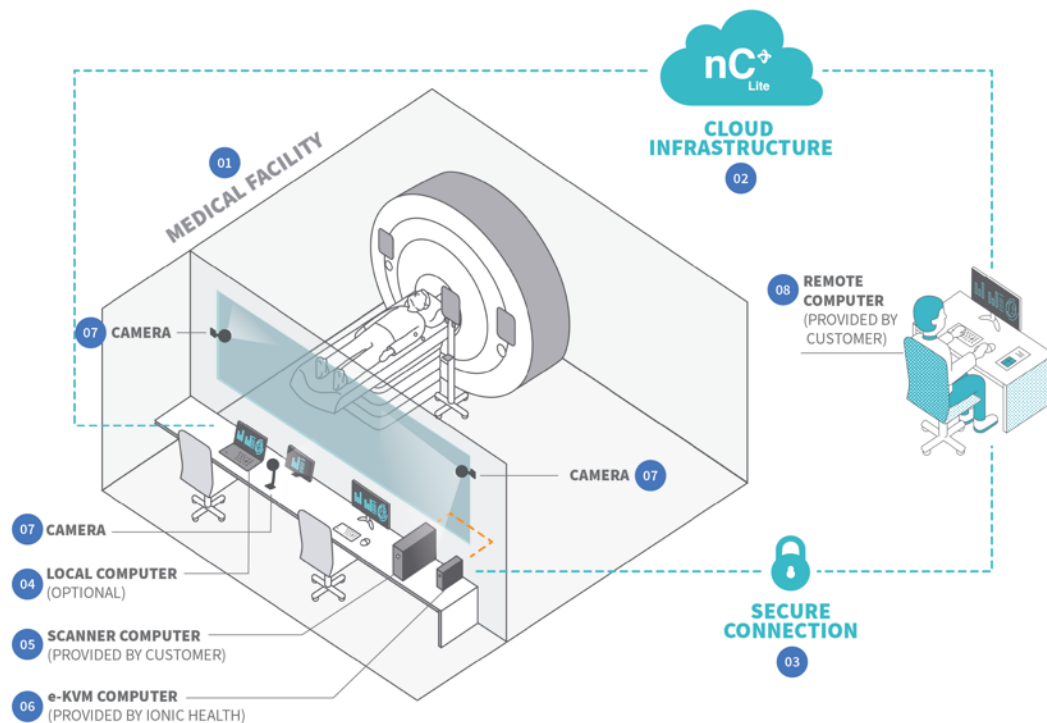


Figure 01: Overview of the product and its connections through a secure connection (e.g. VPN).
 01 – Medical Facility; 02 – Cloud Infrastructure; 03 – Secure Connection; 04 – Local Computer (Optional);
 05 – Scanner Computer (Provided by Customer); 06 – e-KVM (Provided by IONIC Health);
 07 – Camera; 08 – Remote Computer (Provided by Customer)



WARNING!

Remote Scanning Compatibility

IONIC Health (IH) validates remote scanning functionality on the listed compatible devices. IH conducts a full assessment of IH remote scanning requirements and tests the system in the target environment during installation. This ensures compatibility and proper performance at that time for remote scanning. This verification does not imply that all OEM (Original Equipment Manufacturer) device requirements are met in this configuration. Any deviation from OEM requirements is the responsibility of the end user.

Modifications to the system or environment after installation must be reported to IH to verify continued compatibility. IH cannot guarantee performance or assume responsibility for configurations different from those validated during installation.

1.3.11. Minimum Requirements

- **Local Computer**

This computer is used by the **local technologist** to authorize and support the remote access of the device through nCommand Lite®. It also allows direct communication with the **remote technologist** via chat feature on the platform.

The minimum required technical specifications are:

- Processor: AMD® A4-9120C or higher, or similar
- Memory: 4GB or higher
- Storage: 128 GB SSD or higher
- Peripherals: microphone and speaker, or headset and webcam
- Monitor: 14" FHD (1920 x 1080) or higher
- Operating System: Chrome OS, Windows OS, or MAC OS
- Installation site: this computer must be near the Scanner Computer
- IT routine: Create nCommand Lite shortcut in every user's Desktop
- Browser Compatibility: Google Chrome or Microsoft Edge.

- **Remote Workstation**

This station is used by the **remote technologist** to access and control the device via nCommand Lite®. The Remote Workstation must establish a secure connection to the e-KVM Computer (provided by IONIC HEALTH®).

The customer is responsible for providing the Remote Computer and will decide on either of two scenarios: the first is a 24x7 operation, and the second is a business-hours operation.

For each scenario, you will find below the proper specs for choosing the computer models:

Scenario 1 (24x7 Operation) - Must meet the following specs:

- Intel Xeon W-2223 (4 cores, 8 threads, 8.25 MB cache, 3.90 GHz Turbo) or higher.
- RAM: 16GB or higher.
- Graphics: NVIDIA RTX A2000 6GB or higher, or similar.
- Storage: 128 GB SSD or higher.
- Operating System: Windows 11 Pro 64B or higher.
- Monitor minimum requirements: Size 27", Aspect ratio 16:9, Resolution 4k.
- Headset: BLACKWIRE 3200 or similar.
- Browser Compatibility: Google Chrome or Microsoft Edge.

Scenario 2 (Business-hours Operation) - Must meet the following specs:

- Intel® Core™ i7-12700k vPro® or higher.
- RAM: 16GB or higher.
- Graphics: NVIDIA T400 GB or higher, or similar.
- Storage: 128 GB SSD or higher.
- Operating System: Windows 11 Pro 64B or higher.
- Monitor minimum requirements: Size 27", Aspect ratio 16:9, Resolution 4k.
- Headset: BLACKWIRE 3200 or similar.
- Browser Compatibility: Google Chrome or Microsoft Edge.



WARNING!

Not meeting the appropriate setup and minimum requirements may result in degraded or failed communication between users.

- **Network Configurations (Minimum Requirements)**

To establish the session between the Remote User and the e-KVM Computer, network communication between the two devices must be ensured. The nCommand Lite System uses peer-to-peer (P2P) to establish connection between local user, remote user and e-KVM computer. There are three compatible scenarios:

- **Scenario 1** – Corporate network that use one of the following protocols: LAN, LAN-to-LAN, MPLS or VPN;
- **Scenario 2** – Corporate network that uses trusted WAN (external network) and does not use any of the following protocols: LAN, LAN-to-LAN, MPLS or VPN;
- **Scenario 3** – Public Network on the Remote Computer Side (Remote User).

The configurations for each scenario are detailed in the technical documentation.

1.3.12. Symbols

Symbol	Description	Reference
	Manufacturer	ISO 15223-1, ISO 7000-3082
	Date of Manufacture	ISO 15223-1, ISO 7000-2497
	Symbol indicates that this product is a medical device	ISO 15223-1
	Unique Device Identifier	ISO 15223-1
	Model reference	ISO 15223-1, ISO 7000-2493
	Importer	ISO 15223-1, ISO 7000-3725
	Consult User Manual	ISO 15223-1, ISO 7000-1641
	Distributor	ISO 15223-1, ISO 7000-3724
	Caution	ISO 15223-1, ISO 7000-0434A
	Warning	ISO 7010-W001
	Serial number (or software version)	ISO 15223-1, ISO 7000-2498
	Authorized Representative in the European Community	ISO 15223-1
	Swiss authorized representative (CH-REP)	ISO 15223-1

	CE - European Conformity Marking; 2803 – Notified Body designation	EU Regulation 2017/745
---	---	------------------------

1.3.13. Service Life

The expected service life of the product is 5 years, considering the useful life of the components that make up the product. This comprehensive evaluation ensures that each critical component's lifespan aligns with the overall service life, guaranteeing consistent performance and reliability throughout the product's intended duration.

1.3.14. Upgrade / Update

IONIC Health will update the nCommand Lite system as part of planned maintenance or upgrade releases. These updates are designed to ensure continued performance and reliability without disrupting the currently deployed version at customer sites. Depending on the nature of the update, the product may be upgraded remotely or may require an on-site visit by a Field Engineer.

Chapter 2 General Warnings and Precautions List



WARNING!

Please read all the warnings below before using the nCommand Lite System.



CAUTION

The nCommand Lite system cannot undergo repair or maintenance while being used to control a MRI, CT or PET-CT equipment in the presence of a patient.

- Pay close attention to all system alerts, as they are crucial for safe operations.
- Prioritize safety and attention during all operations.
- Federal law restricts this device to sale by or on the order of a physician, as used by medical technologists licensed in the state where he/she practices.
- The nCommand Lite System must only be used by technologists who have received training on the use of the platform.
- Use this system only with compatible web browsers. Supported browsers are Google Chrome and Microsoft Edge.
- In case of contingency, a trained, licensed technologist must remain in the Imaging Facility to perform the MRI, CT, or PET/CT operation without the nCommand Lite.
- Accessing multiple devices simultaneously demands intense focus and communication with local teams.
- Avoid accessing devices with identical layouts or examinations of the same anatomical region at the same time.
- You can view multiple screens, but control is limited to one device at a time.
- Always initiate a chat when connected to a device for clear communication.
- Call alerts appear on the associated device screen; only one call can be active at a time.
- Test the video communication when accessing the application (before the beginning of a work session) to check if there is any failure in the video output connection of the MRI, CT, or PET/CT devices or any device related to video streaming.
- The device should not be plugged into the outlet and/or the uninterruptable and stabilized power supply through extension cords or "plug strips".
- If video failures occur, check the video connection between the device system and the e-KVM computer.
- If the application is slow in its remote access, refresh the page with the commands Ctrl+F5 in the remote technologist computer's browser. If the problem persists, contact technical support.
- Whenever the browser page is refreshed, the connection to the device is interrupted, requiring the approval process to be performed again.
- Do not log in using a different browser when you are already logged in.
- The customer's Imaging Facility must have a redundant internet link with a different supplier from the main one for immediate change in case of loss of system/platform communication.
- In case of communication loss or mouse slowness, conduct a "mouse resync" on the page used in the browser.
- Make sure that the computers used for nCommand Lite System control, both in the Imaging Facility and in the Command Center, meet the minimum requirements; otherwise, there may be a loss in application performance.

- QoS (Quality of Service) should be applied to the main link and the redundant link for transmission of the platform, and the performance of the link should be monitored.
- Before use, check the audio and microphone volume levels, as well as the audio and microphone permission in the web browser.
- Before use, check the functioning of the keyboard and mouse; if they are slow or out of sync, activate the "mouse resync" button. Check if the e-KVM Computer is connected and turned on.
- Ensure that the keyboard layout at the Remote Facility is identical to the keyboard layout at the Imaging Facility.
- If it is necessary to change the place where the platform is used, the client must call technical support to make a new installation. Do not reinstall without contacting technical support.
- Before starting the remote access process of the MRI, CT, or PET/CT device, it is important for the technologists' teams to check all the items required for the proper performance of the platform, so as not to hinder the exam. These items are listed in the document "Service Start Checklist".
- The Imaging Facility's firewall configuration must be checked monthly with the IT Team, verifying that there are no problems with the firewall release that could compromise the use of the nCommand Lite.
- Any anomaly observed in the use of the application must be immediately notified to the support team before starting the access or aborting it if it has already started.
- Only licensed technologists trained in the use of the nCommand Lite should operate the application.
- Remote access via the platform does not replace or compete with any other operating procedure for MRI, CT, or PET/CT operation established by the medical device manufacturer and care facility protocols and procedures.
- Avoid bending or stretching the hardware cables.
- If problems occur with voice or chat communication, use the phone call function to establish communication between the local technologist at the Imaging Facility and the remote technologist at the Command Center. Follow the instructions described in the section "Guidelines in Failure Case" and, if necessary, contact technical support to perform the repair.
- If it is necessary to replace a computer or any other equipment that directly influences the nCommand Lite installation, activate technical support, guaranteeing the preservation of the system's operation.
- Just one person at a time can remotely access the MRI, CT, or PET/CT device.
- Do not touch any physical video cables while the device computer and the nCommand Lite System are powered on.
- When accessing an additional device, a new tab will open. Drag this tab to a second monitor, as the system is designed to be used with a separate screen for each device.
- Any serious incident related to the use of this device should be reported to both the manufacturer and the health authority/competent authority where the device is installed (*See more details in the Service Channels chapter*).

Chapter 3 Platform Use in Each Location

Section 3.1 - Access and Use of nCommand Lite

**WARNING!**

In case of any issues, contact technical support for assistance.

**WARNING!**

Check the keyboard layout and ensure that it is identical in both locations (Medical Facility and Remote Facility). Different keyboard layouts may hinder user experience.

This chapter provides everything you need to know to access and start using the nCommand Lite platform. You'll find simple, step-by-step instructions to log in, navigate the interface, and understand the main features. Whether you're working on-site or remotely, this guide will help you get started quickly and confidently.

Changing the Language - The system is pre-set to English by default, but you can easily change the language according to your preference. On the login screen, click on the top-right corner where "English (en-US)" is displayed. This will open a dropdown list of available languages for you to select from.

After logging in, you can also change the language by clicking on the currently selected language on the right side of the top bar. This will open a dropdown list of available languages for you to choose from.

Please note that if you change the language while you are connected to a device, the current connection will be automatically terminated, and you will need to reconnect.

When accessing the platform, you can choose your preferred language on the sign-in screen. However, some messages shown during the login process may appear in the language set in your web browser, regardless of the language selected on the platform. For a consistent experience, we recommend aligning your browser language settings with your preferred platform language.

Section 3.2 - Accessing the Platform for the First Time

The login process on the platform can be done in two ways: via nCommand Lite or via an External Identity Provider (External IdP). The user can log in using one of the pre-configured methods. If the configured method is the External Identity Provider (External IdP), the nCommand Lite method will not work, and vice versa. To log in via External IdP, go directly to **sub-item 3.2.2**.

3.2.1. Login via nCommand Lite

Note: This section does not apply to users who log in through an External Identity Provider (External IdP).

Turn on the computer and double-click the nCommand Lite shortcut icon, which is usually on the desktop. You can also access the URL directly in the browser.

Your first access is a crucial step to start using the platform safely and efficiently. Here's what you need to know:

1 - Welcome Email: You'll receive an email with your login details, including your associated personal email, a temporary password, and a direct link to the client platform. This email is crucial to begin your journey on nCommand Lite.

2 - Password Creation: Upon accessing the link, you will need to input your associated email and the password received in the Welcome Email. By clicking on "Sign in" you will be directed to a page to create a new password. You need to input the old one, the new password and the confirmation of the new password. It must be strong and secure, including at least 3 items of the following: a lowercase letter, an uppercase letter, a number and a symbol, and be at least 8 characters long. By clicking on "Continue" you will be redirected to a page to confirm your email again. By clicking on "Continue" you will now be redirected to the home screen, which is customized according to your specific user profile.

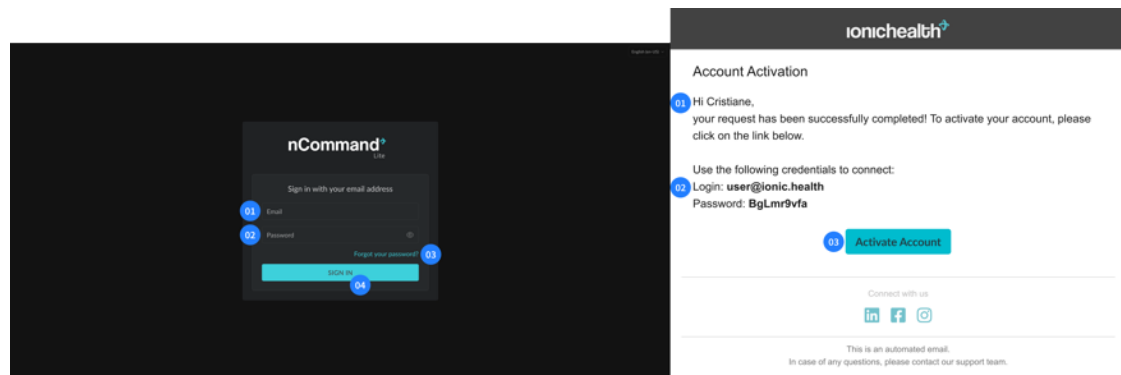


Figure 02: First Access

Left - Login Page: 01 – Email Address; 02 – Password; 03 – “Forgot your password?”; 04 – Sign In button
Right - Welcome Email: 01 – Account activation email text; 02 – Login credentials; 03 – Active Account button

This initial procedure is designed to ensure maximum security for your account from the start. From your second access onwards, the process will be streamlined yet equally secure, with a two-factor authentication code sent to your associated email at each login to ensure the ongoing security of your account.

After logging into nCommand Lite, the system will automatically direct you to the home screen, which is customized according to your specific user profile. Whether you are a local technologist or a remote technologist, the interface is designed to meet the needs and access relevant to your role. This intuitive design ensures you have all the tools and information necessary for an effective and efficient user experience from the moment you log in.

Note: When the login method is configured as nCommand Lite, the login must always be done through this option. Even if an External IdP button appears on the login screen, it will not work for these users. Each user account is registered on the platform with a specific authentication method — either nCommand Lite credentials or an External IdP service. If a user attempts to log in using a different method than the one assigned to their account, the system will display an error message indicating that the account is not authorized for that authentication type.

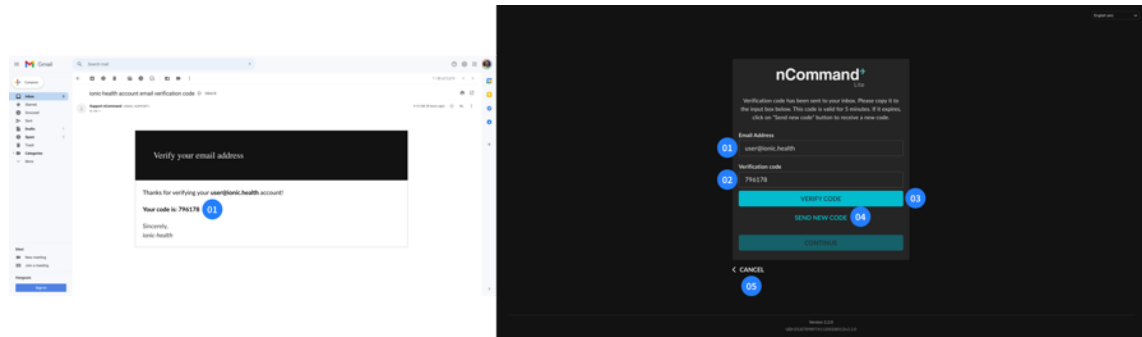


Figure 03: Two-Factor Authentication (2-FA)

Left – Email: 01 – 2-FA Code

Right - Two-Factor Authentication Page: 01 – E-mail Address; 02 – Verification Code; 03 – Verification Code button confirm; 04 – Send New Code; 05 – Cancel

3.2.2. Login via External IdP

In some cases, users may log in to the platform through an External Identity Provider (IdP), which allows them to use their organization's existing authentication service, a mechanism also known as Single Sign On (SSO). By this method, the pre-registered user will not receive a welcome email. The local IT service must check compatibility, configure the method, and inform the user which email (External IdP) should be used.

When this option is available, the user must always log in using the External IdP (e.g., Amazon Cognito, Microsoft Entra ID, Microsoft AD B2C). The login method via nCommand Lite will not be available for External IdP users.

To log in using the External IdP, click the button with the IdP name and follow the instructions provided by the external authenticator. If your institution has more than one External IdP integrated, make sure to confirm which provider you are registered with. Other providers will not work. If you have any questions or encounter difficulties, contact your local IT service.

In scenarios where users share the same machine and use Single Sign-On (SSO), it is recommended that each user selects the “do not stay signed in” option during External IdP login (if available) or signs out of the external provider after logging out of nCommand Lite.

For this login option, the complete login and logout process—including password creation and expiration policies, multi-factor authentication (MFA), and account lockouts—is managed entirely by the client's IT team that configured the External IdP.

When logging in via External IdP, the “Forgot Password” and “Change Password” functions must be performed according to the External IdP's process.

Note: The “Forgot Password” option will still appear on the login screen, but it will not be functional for these users. It may direct to the next steps of the process but will not complete it. If you need to recover your password, follow the instructions from your External IdP.

Important: Even when using an External IdP, the user must be pre-registered in the nCommand Lite platform to gain access.

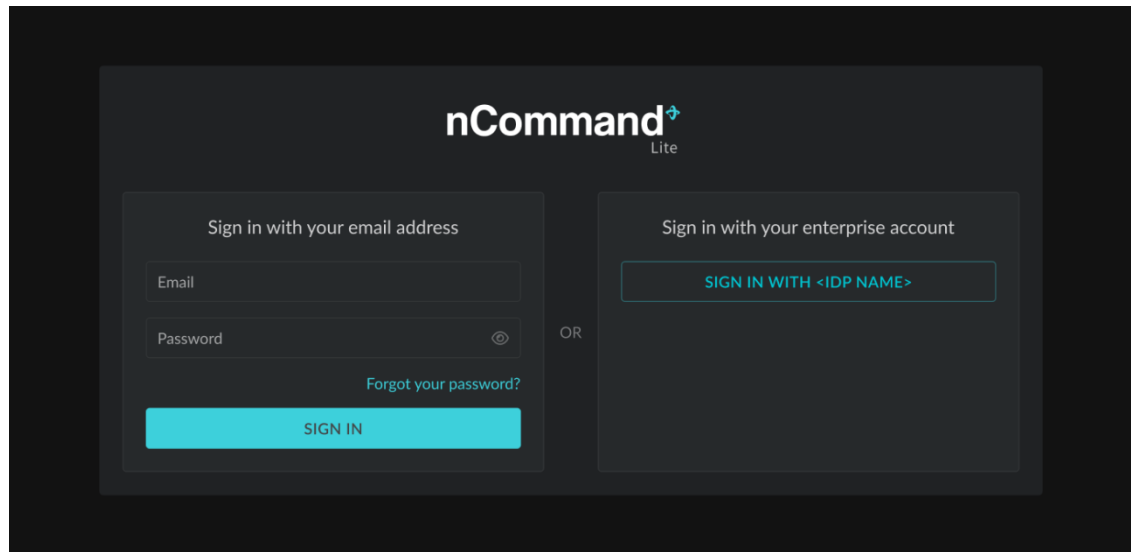


Figure 04: Login screen via External IdP (Example)

Section 3.3 - Password Management

After accessing the platform for the first time, users can change his/her password or, if it was forgotten, set a new password.

Note: When logging in via External IdP, the **Forgot Password** and **Change Password** functions must be performed according to the External IdP's process.

- Recover Password:** Enables users to recover account access in the event of forgetting his/her password. Simply click the "Forgot your password?" link on the login page, enter the associated email address, and submit the information. The system will then send an email containing a verification code. When filling in the code and clicking on "Verify code", users will be asked to confirm the associated email. By clicking on "Continue", users are directed to a page where they can input a new password and confirmation of the new password. If the new password meets system requirements, users can successfully register it and subsequently log in with the updated credentials.

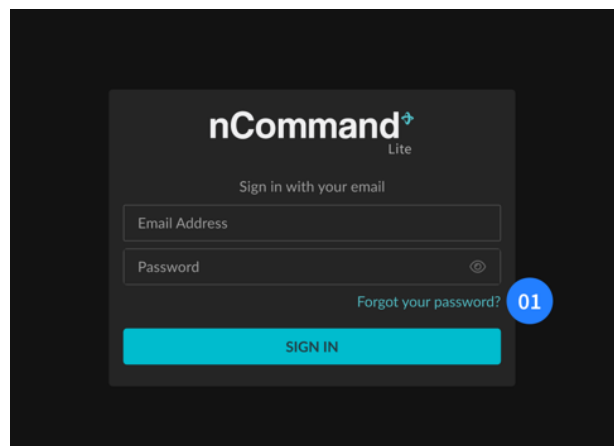
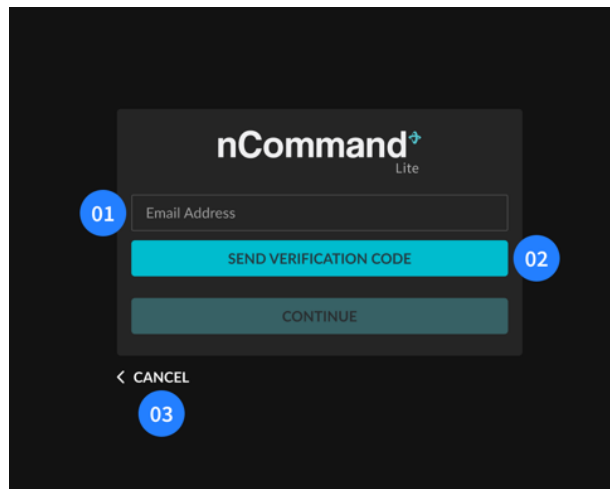
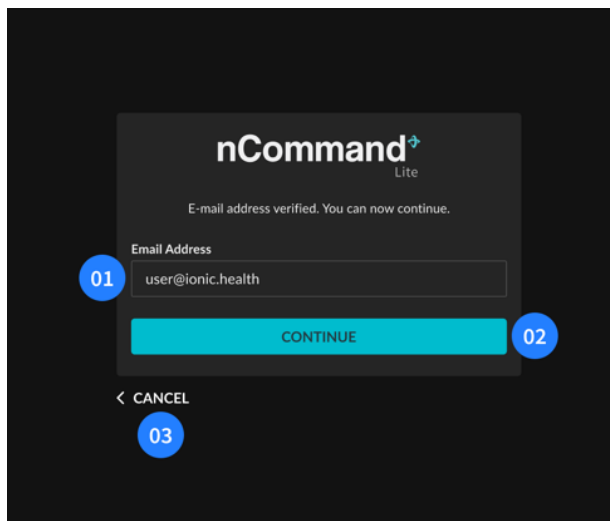


Figure 05: Link to Password Reset Page
01 – Forgot your password?



The image shows the nCommand Lite Password Reset Page. It features a dark background with a white nCommand Lite logo at the top. Below the logo is a form with a text input field labeled 'Email Address' (01). To the right of the input field is a blue button labeled 'SEND VERIFICATION CODE' (02). Below the input field is a grey button labeled 'CONTINUE'. At the bottom left of the form is a '< CANCEL' link (03).

Figure 06: Password Reset Page
01 – E-mail Address; 02 – Send Verification Code; 03 – Cancel



The image shows the nCommand Lite Email Confirmation Page. It features a dark background with a white nCommand Lite logo at the top. Below the logo is the text 'E-mail address verified. You can now continue.' Below this text is a form with a text input field labeled 'Email Address' (01) containing the text 'user@ionic.health'. To the right of the input field is a blue button labeled 'CONTINUE' (02). At the bottom left of the form is a '< CANCEL' link (03).

Figure 07: Email Confirmation
01 – E-mail Address; 02 – Continue button; 03 – Cancel

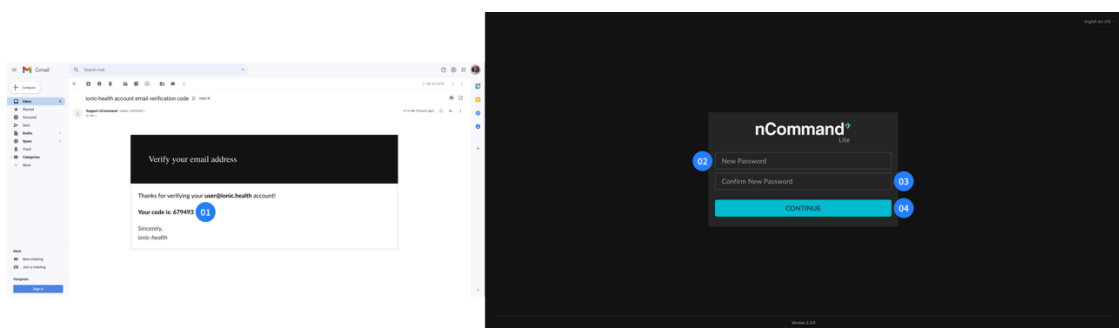


Figure 08: Email with code to Register New Password (left) - 01 – 2-FA Code Change Password page (right) - 02 – New Password; 03 – Confirm New Password; 04 – Continue Button

- Change Password:** Enables users to update their password by adhering to specific criteria, including at least 3 items of the following: a lowercase letter, an uppercase letter, a number and a symbol, and be at least 8 characters long. The system checks whether the new password meets these criteria and prompts the user with a message if it does not. Additionally, users need to confirm the new password to prevent input errors. To change the password, the user, after the login process, needs to click on the upper right corner icon and choose the "Change Password" menu. He/she will be disconnected from the platform and directed to a page to confirm the associated email. The system will then send an email containing a verification code. When filling in the code and clicking on "Verify code", users are redirected to a screen where they can input a new password.

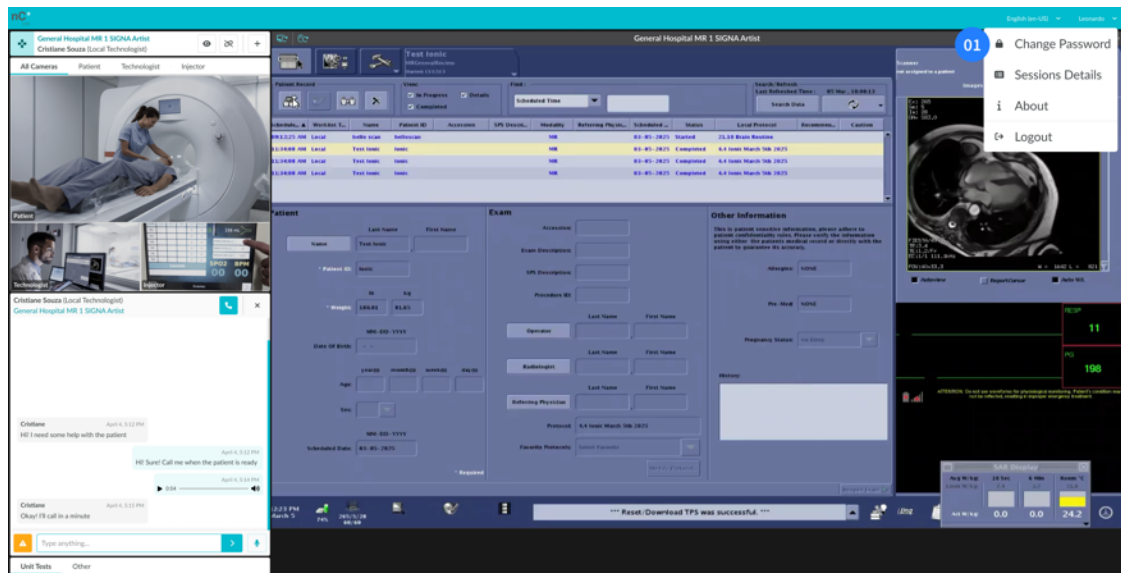


Figure 09: Change Password Dropdown Menu Item
01 – Change Password

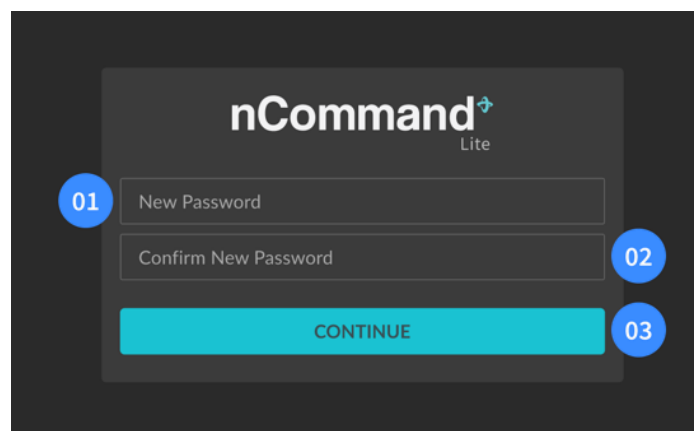


Figure 10: Change Password Page
01 – New Password; 02 – Confirm New Password; 03 – Continue button

Section 3.4 - Access with Local Technologist Profile



WARNING!

Before using the platform, contact the remote technologist by phone.



WARNING!

To avoid overheating, please do not place any objects in front of the air cooler of the e-KVM Computer, and to prevent any damage, do not place any objects on top of it.



WARNING!

During remote sessions, the local technologist is responsible for managing and enforcing local safety rules for each type of exam and its specific requirements. Always remain present in the control room and/or examination room to ensure the safety of both the patient and the professionals involved.



WARNING!

Table movements during the session must only be performed by the local technologist when requested by the system. Before leaving the operation room, the local technologist should always revoke the remote technologist's access.



WARNING!

Only the local technologist is allowed to move the table to position the patient inside the device and to release the patient safely. Before leaving the operation room, the local technologist should always revoke the remote user's access.

After logging into the platform, proceed to select the desired device in the Device Selection box. You will be responsible for this device, so you can review the remote technologist's request to access the device. When a remote technologist wants to access the device, a pop-up window will appear, allowing you to review all the information presented before granting or denying access. Stay alert for an incoming request from a remote technologist. It is of utmost importance to carefully check each detail. In cases where the information provided is not recognized, do not grant access.

The remote technologist can access the device using one of two access modes: **Control** or **View**:

- **Control Mode** - allows the remote technologist to control the mouse and keyboard, as well as view the device's streaming. However, the local technologist does not lose control of the local mouse and keyboard and can take control at any time.
- **View Mode** - allows the remote technologist to only view the device's screen and use the chat for communication

After selecting the device, the user has access to the chat function, enabling communication through text, audio messages, voice and video call with the other users.

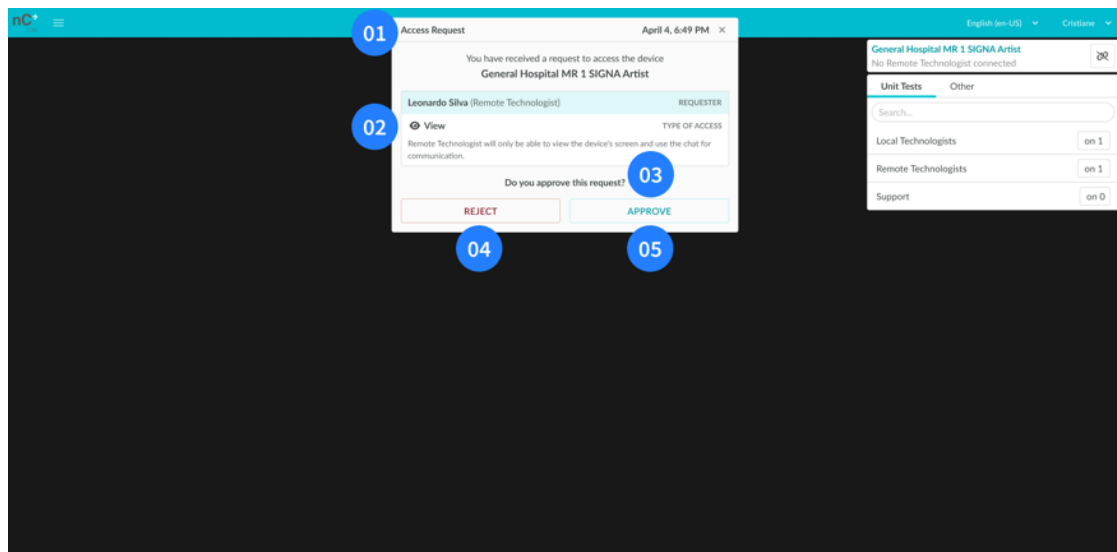


Figure 11: Local Technologist main screen with Access Request Notification
 01 – Title (Access Request); 02 - Requester Name, Role and Access Type Description;
 03 – Prompt: "Do you approve this request?"; 04 – Reject button; 05 – Approve button

After approval, the local technologist can revoke the remote technologist's access at any time by simply clicking on the REVOKE button.

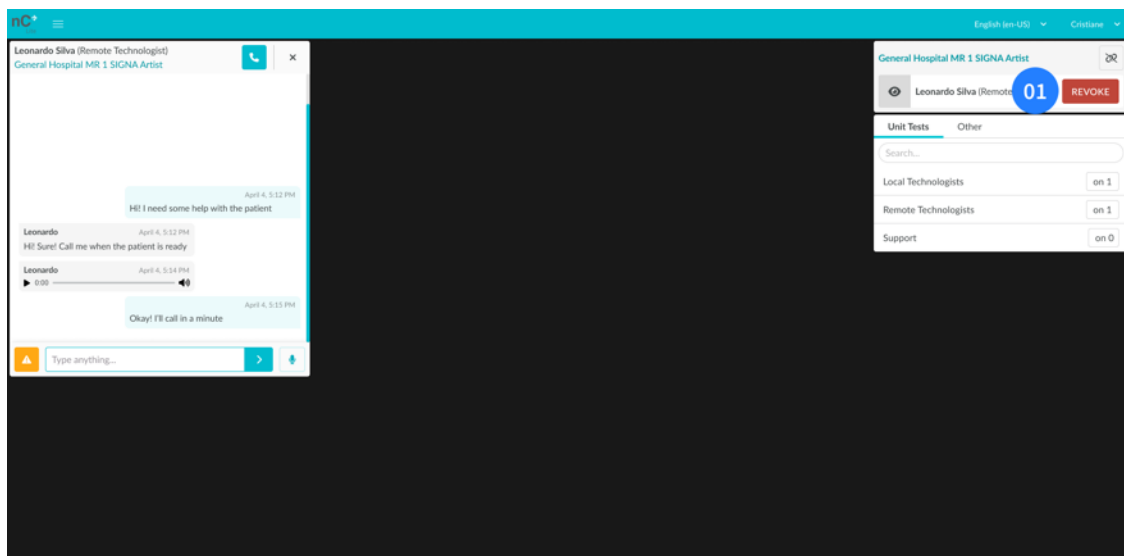


Figure 12: Local Technologist main screen when connected to a device
 01 – Revoke button

During the remote session, the remote technologist can request a change of access mode. A request pop-up will appear on the screen. You can approve or reject it. Be aware of the prerogatives that each access mode allows the remote technologist.

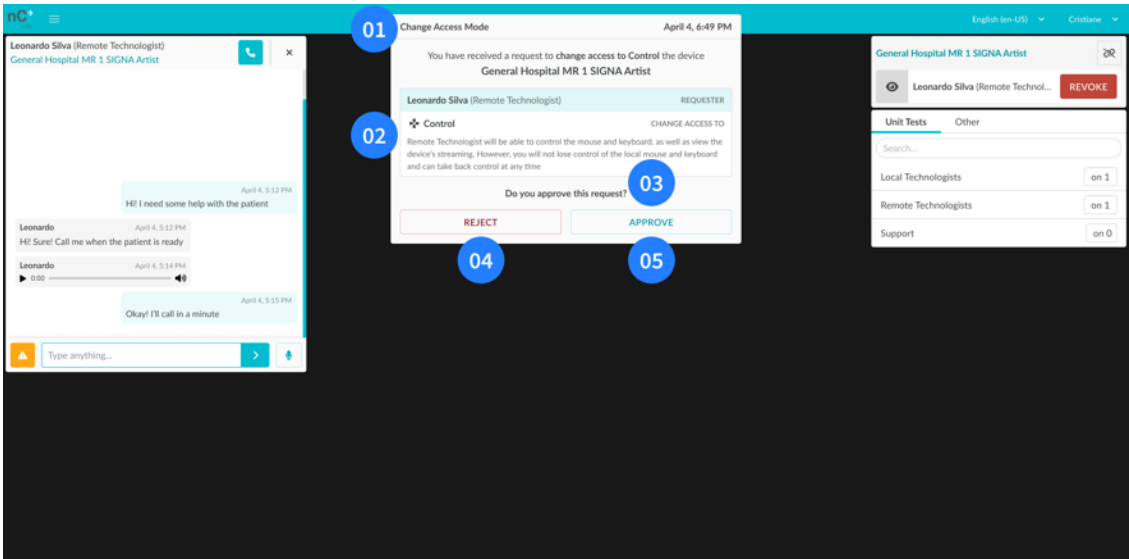


Figure 13: Local Technologist main screen with Request to Change Access Mode
01 – Title (Change Access Mode); 02 - Requester Name, Role and Access Type Description;
03 – Prompt: "Do you approve this request?"; 04 – Reject button; 05 – Approve button



WARNING!

In case of a lost connection at the local computer, the remote technologist still has access to the *device*. **Immediately** contact the remote technologist and ask him/her to **disconnect** OR log in to another computer and **revoke the access** of the remote technologist OR **press the power button** to shut down the e-KVM computer.



WARNING!

In Case of Scanner Maintenance:

Before the Field Engineer begins any procedures (either on the device or in the control room), inform the remote technologist and revoke access by clicking on "REVOKE ACCESS" button. Then, log off from the nCommand Lite platform.

If no remote technologist is connected, log off from the nCommand Lite platform before starting maintenance.

Section 3.5 - Access with Remote Technologist Profile



WARNING!

Device computer user and root password: both must be held by the on-site host who will receive the installation team.



WARNING!

Table movements during the session must only be performed by the local technologist when requested by the system. Before leaving the operation room, the local technologist should always revoke the remote technologist's access.



WARNING!

Only the local technologist is allowed to move the table to position the patient inside the device and to release the patient safely. Before leaving the operation room, the local technologist should always revoke the remote user's access.

**WARNING!**

Always be aware of the room through the video camera and ensure communication with the local technologist before performing any activities.

**WARNING!**

In case of a lost connection at the local computer, contact the local technologist immediately and disconnect.

**WARNING!****In Case of Scanner Maintenance:**

After being notified of the start of device maintenance, ensure that access has been revoked by the local technologist and log off from the nCommand Lite platform.

If access has not been revoked, log off from the nCommand Lite platform and immediately contact the local technologist to notify them.

**WARNING!**

To control the mouse and keyboard remotely, the selected access mode must be Control; in View mode, the remote technologist is only allowed to view streaming and local cameras.

**WARNING!**

If the response to your request takes longer than expected, contact the local technologist via chat or phone.

The remote technologist's workplace includes equipment such as a computer, monitors (usually three), a mouse, a keyboard and a headset.

In the clinical workflow, *local technologists* have direct contact with the patient. They are responsible for patient interaction, positioning, and ensuring safety and protocol compliance during MRI, CT, or PET/CT procedures, according to institutional and regulatory standards.

3.5.1. Access Mode

After logging into the platform, select the device you want to connect to in the Device Selection Box. A popup window will open to choose the access mode between **Control** and **View**:

- **Control Mode** – In this mode, mouse and keyboard control is enabled in addition to screen viewing. Local professionals retain full access to the local mouse and keyboard and can take back control at any time.
- **View Mode** – It is only possible to view the device's screen and use the chat for communication.

By selecting the access mode, a box of "Waiting for approval" will be displayed, indicating that the approval from the local technologist connected is required to proceed. This local technologist has full authority to approve or reject access and revoke access at any time if deemed necessary. This measure is essential to ensure strict control and maintain safety when using the device.

After selecting the device, the user has access to the chat function, enabling communication through text, audio messages, voice and video call with the other users. The user does not need to be approved to access the chat.

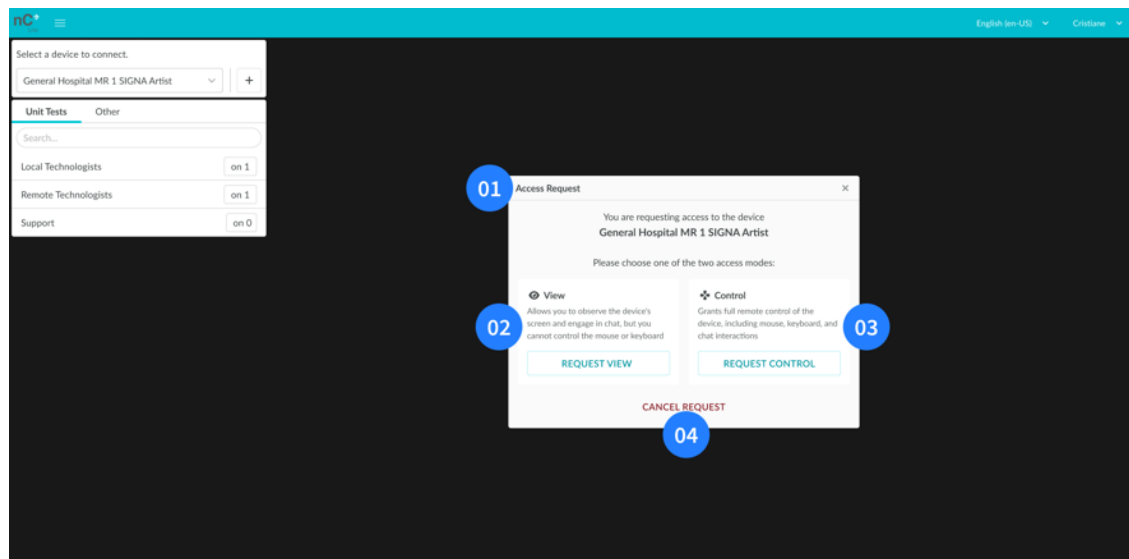


Figure 14: Access Request Dialog for Remote Technologist

01 – Title (Access Request); **02** - View Mode Description and Request View button; **03** – Control Mode Description and Request Control button; **04** – Cancel Request

Once the device access has been authorized by the local technologist, the remote technologist's interface will be updated to display the live feed of the device and its associated cameras. If the chosen access mode is Control, the capability for remote operation of the device will be enabled.

This process ensures effective and secure interaction, allowing for the safe remote use of the device without compromising its integrity or patient safety.

To request a change in access mode during a remote session, click on the corresponding icon. The local technologist can accept or reject the request:

- **Accept** – the streaming will reload, but chat content will not be lost. If you are on a Voice & Video call, it will end and will need to be restarted by one of the users.
- **Decline** - a popup will appear notifying you of the local technologist's rejection and the current access will remain active

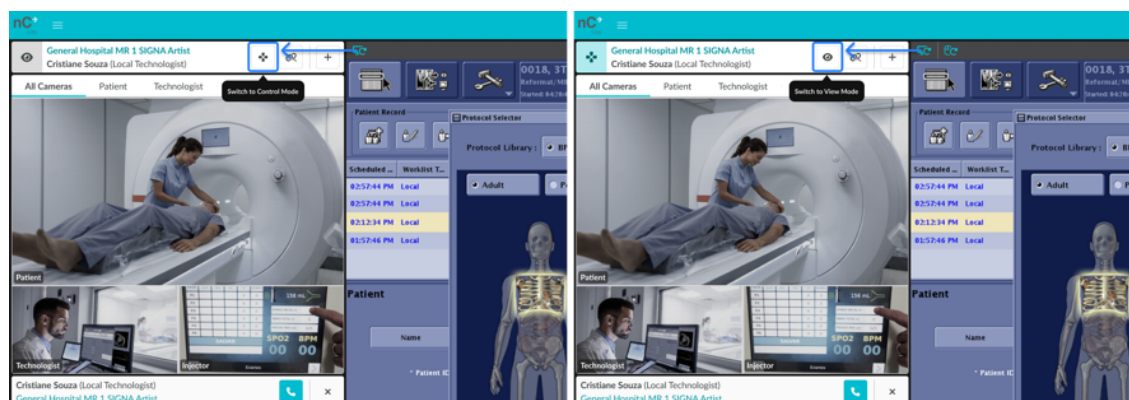


Figure 15: Change Access Mode

Left - Switch to Control Mode Icon and Tooltip / **Right** - Switch to View Mode Icon and Tooltip

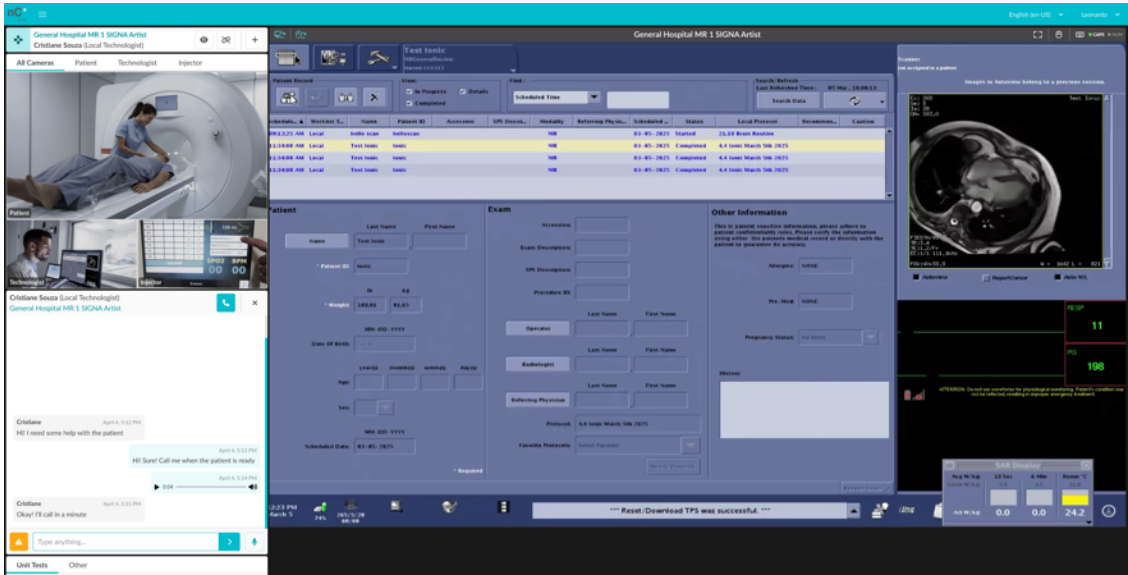


Figure 16: Remote Technologist main screen when connected to a device

When the remote technologist requests access and there is no local technologist connected to the device, the platform displays a popup warning. As soon as the local technologist connects, the platform informs the remote technologist that they can request access again.

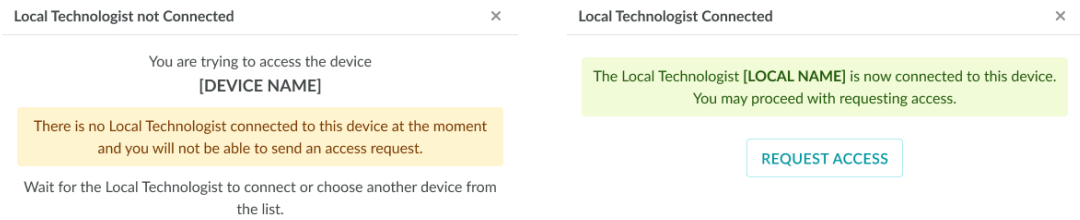


Figure 17: Remote Technologist warnings about the Local Technologist's connection status
Left - Notification indicating that an attempt to access the device was made, but no Local Technologist is currently connected.
Right - Notification confirming that the Local Technologist has connected to the device after previously not being connected.

3.5.2. Streaming Bar

The Streaming Bar displays key information and controls related to the device streaming session. It includes the "Reload Streaming" and "Mouse Resync" buttons, the device name, screen resolution, and the current status of the remote computer's mouse and keyboard.

1 - Reload Streaming

This feature enables remote technologists to recover access to devices in the event of a connection failure or performance slowness. If you experience any type of disconnection or screen lag on the device computer, you can click the "Reload Streaming" icon located in the Streaming Bar. This will prompt the platform to reconnect to the device computer and reload the system cameras as well.

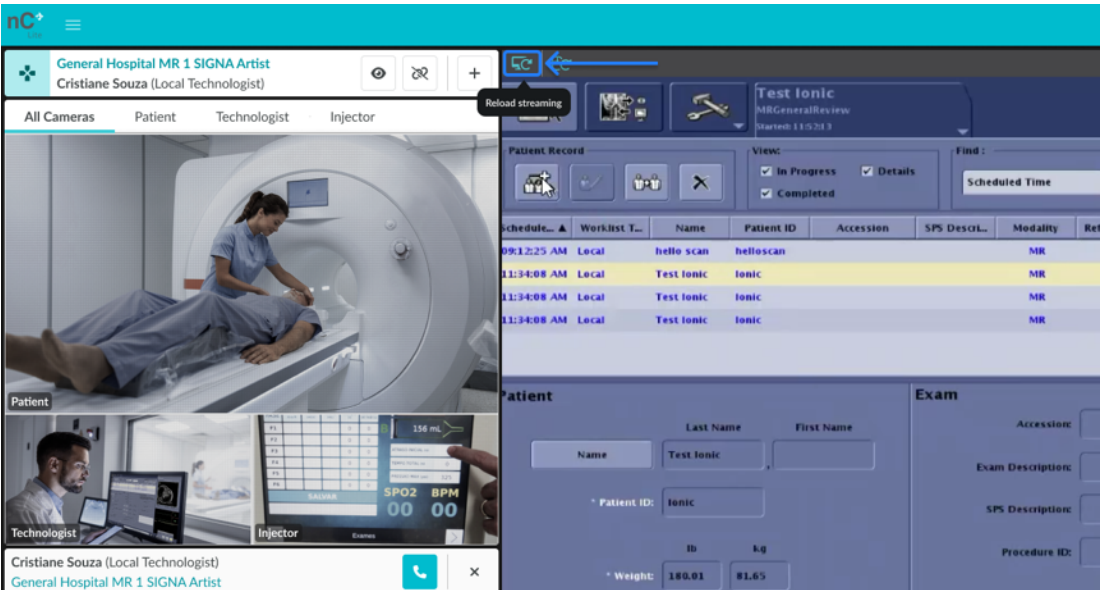


Figure 18: Reload Streaming Button

2 - Mouse Resync

In case of mouse slowness or misalignment, please click the 'Mouse Resync' button located on the bar above the streaming window to resync the device mouse with the e-KVM computer.

An alternative is to move the mouse pointer outside the streaming area and then bring it back in, the system will automatically resynchronize the mouse without any further action needed. You can also click and release the mouse scroll wheel button (when available) to trigger the resync automatically. However, this method may not work on devices with two or more screens if the local and remote mouse pointers are on different screens.

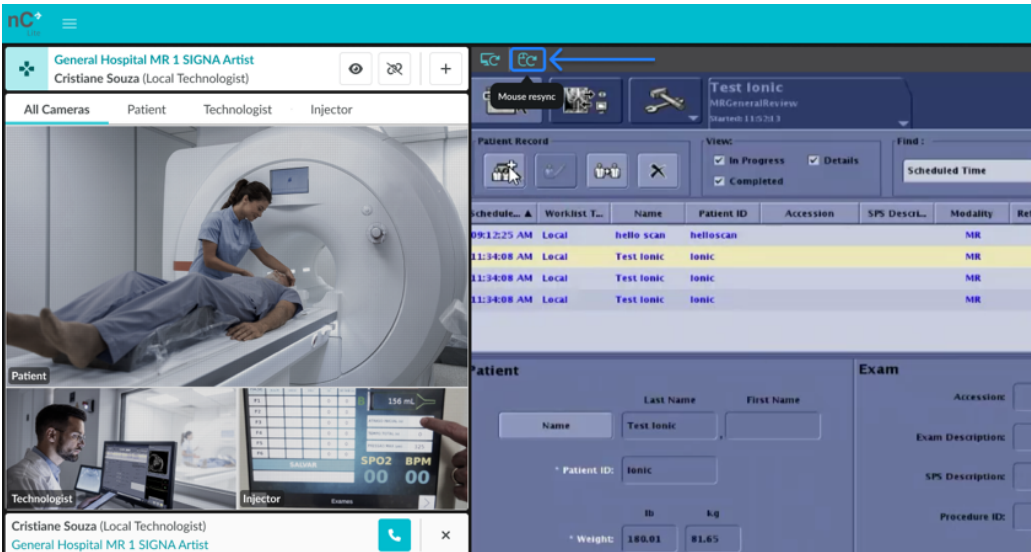


Figure 19: Mouse Resync Button

3 - Streaming Display

This feature provides the remote technologist with information about the original streaming resolution (from the device) and the current resolution in pixels being displayed on the remote workstation.

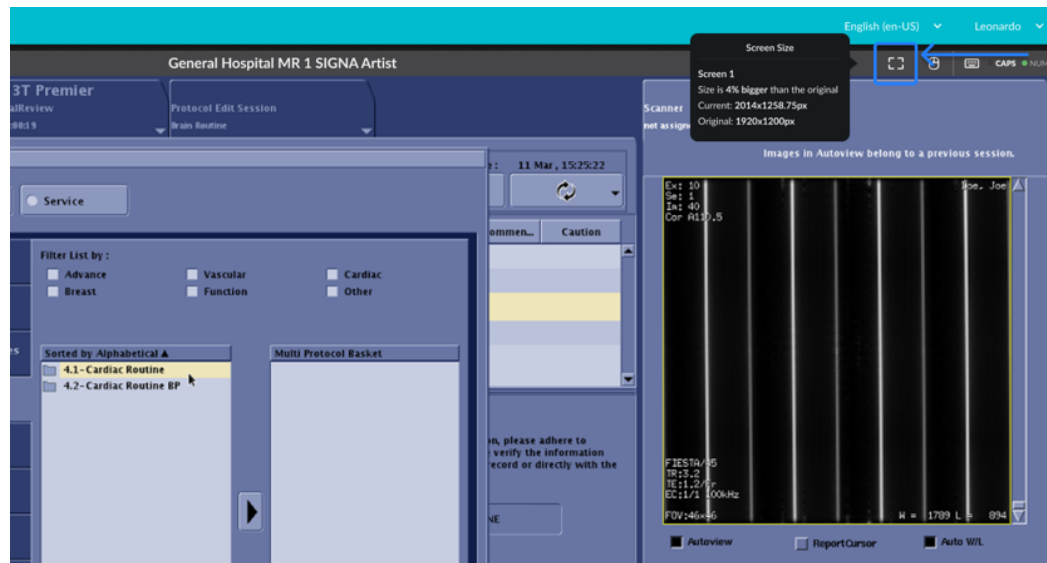


Figure 20: Streaming Information Tooltip

4 - Mouse and Keyboard Status

This feature informs the remote technologist about whether the mouse and keyboard are working correctly. Together with the keyboard status, the user can see if the **Caps lock** and **Num lock** keyboard keys on the device computer are on or off. However, this functionality depends on the device computer providing this information; in scenarios where this information is not made available by the device system, the status of the **Caps Lock** and **Num Lock** keys will not be displayed. Both the Mouse and Keyboard statuses are shown only when the user has Control type of access.

When connecting to a device, a mismatch between the **Caps Lock** and **Num Lock** indicators on the remote computer and the device may lead to inconsistent typing behavior. If the indicators appear enabled on the device but are not actually active on the remote computer, the user may type in uppercase on the device while text appears in lowercase in the chat, or vice versa. Similarly, if **Caps Lock** is enabled on the remote computer but disabled on the device, the same issue will occur in reverse.

To prevent this issue, ensure that **Caps Lock** and **Num Lock** are either both enabled, or both disabled before logging into the device. If a mismatch occurs, the user should disconnect from the device, adjust the key status on the remote computer, and then reconnect.

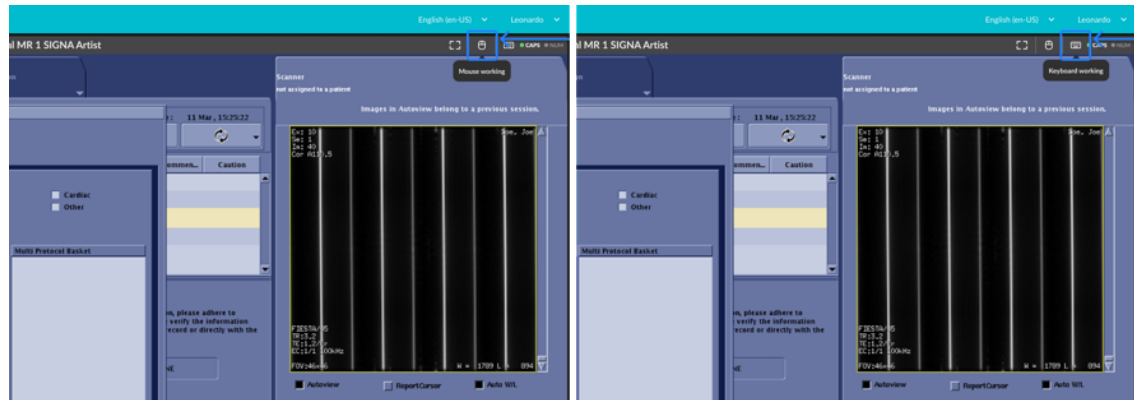


Figure 21: Streaming Bar
Left - Mouse Status Tooltip Information
Right - Keyboard Status Tooltip Information

3.5.3. Multi-camera

This feature allows the remote technologist to view multiple cameras at the same time. If more than one camera is available, it is possible to view only one and switch between them by clicking on the menu with the designated name for each camera. By selecting "ALL CAMERAS," all available cameras will be displayed in the frame, with one of them highlighted. To switch the highlighted camera, simply hover the mouse over one of the cameras in the smaller frame and click on "SWITCH CAMERA."

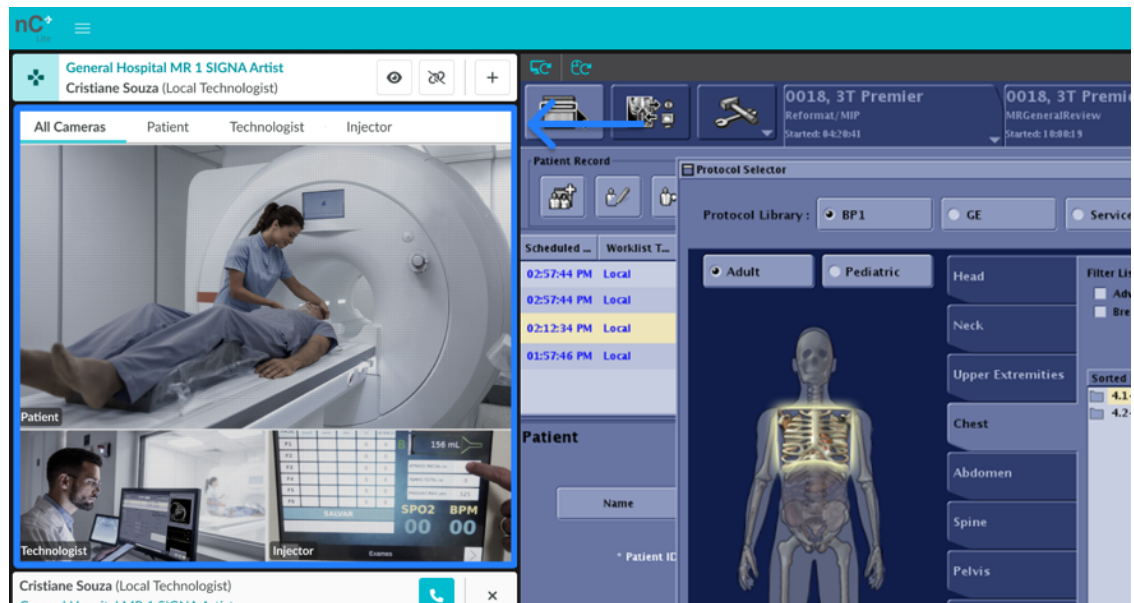


Figure 22: Multi-Camera Frame View

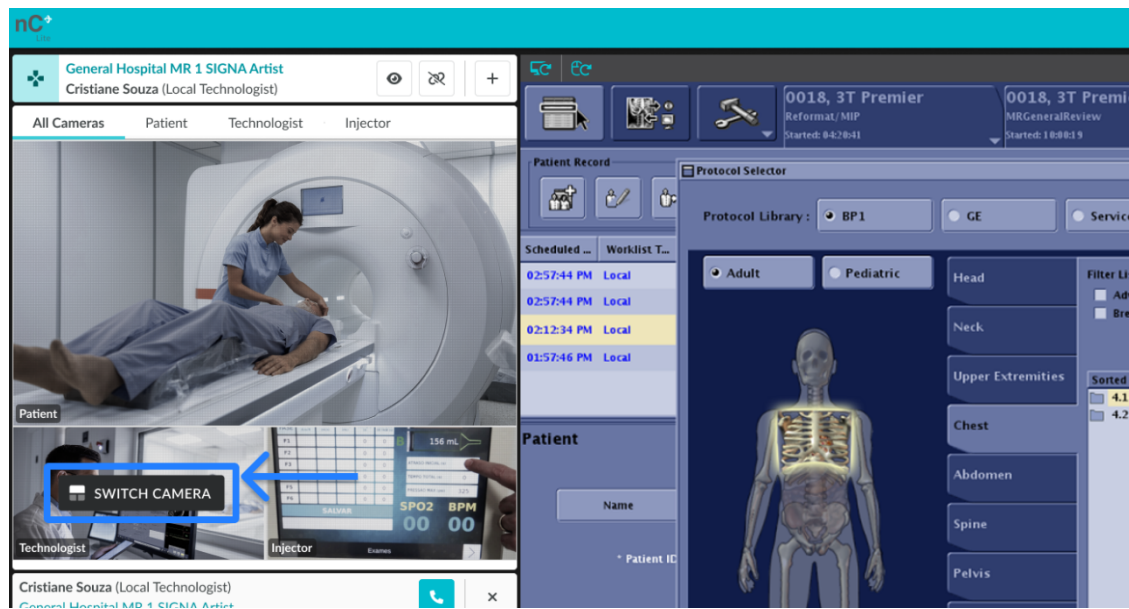


Figure 23: Multi-Camera "SWITCH CAMERA" Hover Button

During an active remote session, if the remote technologist is accessing as **View**, there is an option to turn off one or more cameras by hovering the mouse over the chosen camera and clicking "TURN OFF CAMERA." To view the camera again, simply repeat the process and click "TURN ON CAMERA."

NOTE: The option to turn off cameras is only available in View Mode; in Control Mode, it is not possible to turn off the cameras.

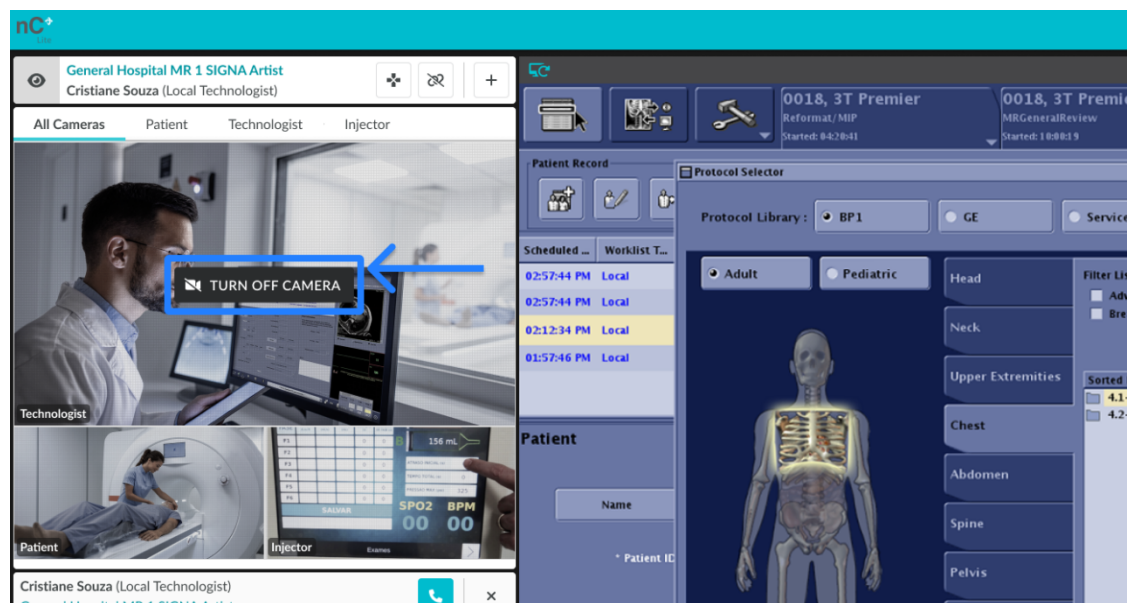


Figure 24: Multi-Camera "TURN OFF CAMERA" Hover Button in View Mode

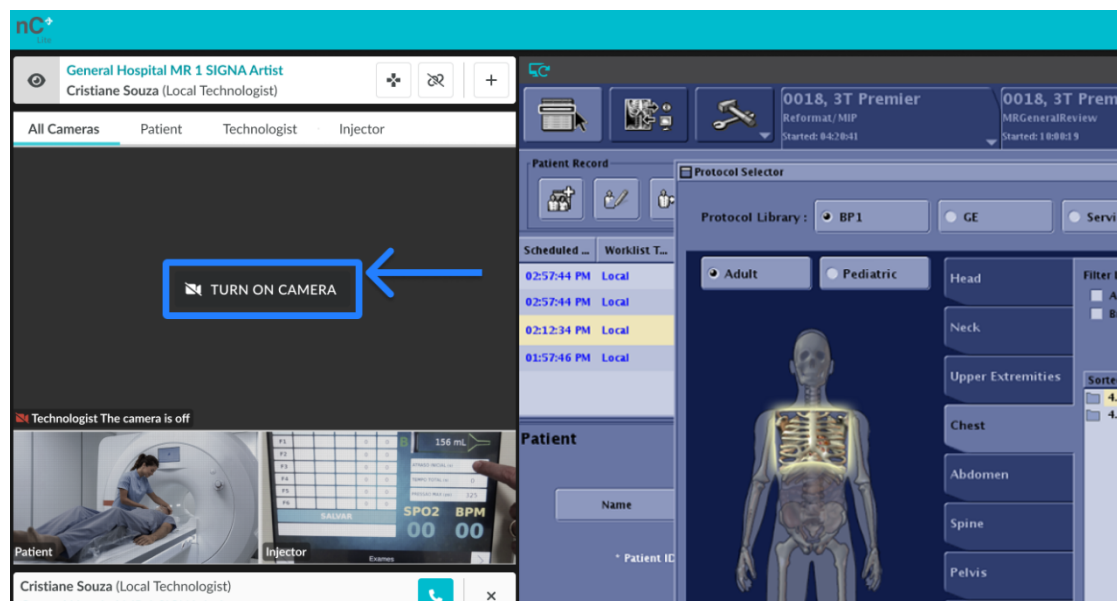


Figure 25: Multi-Camera "TURN ON CAMERA" Hover Button in View Mode

3.5.4. Open Another Device

Allows the remote technologist to open a new browser tab of the nCommand Lite, thus enabling the user to select a new device to perform more than one remote scanning simultaneously. To open a new device to access, just click on the "Open Another Device" button, and a warning is provided so you can safely do this simultaneous operation. You should read the warning before accessing this new window.

NOTE: For better viewing during simultaneous access, it is recommended that, after clicking "OPEN ANOTHER DEVICE" and clicking "OK" on the warnings, drag the new tab to another available monitor.



WARNING!

Safety Warning for Multiple Scanner Access

- **Demand of intense focus:** Simultaneous access requires intense focus and communication with local teams.
- **Choose different layouts:** Avoid accessing devices with identical layouts or examinations of the same anatomical region at the same time.
- **Drag tab to another monitor:** When accessing an additional device, a new tab will open. Drag this tab to a second monitor, as the system is designed to be used with a separate screen for each device.
- **Pay attention to alerts:** Pay close attention to all system alerts, as they are crucial for safe operations.
- **Control one at a time:** You can view multiple screens, but control is limited to one device at a time.
- **Open chat:** Always initiate chat when connected to a device for clear communication.
- **One call at a time:** Voice call alerts appear on the associated device screen; only one call can be active at a time.

- **Safety and alert:** Prioritize safety and stay alert during all operations.



Figure 26: Open Another Device Button (+)



Figure 27: Multiple Device Access Warnings

- 01 – Title (Open Another Device); 02 – Operational Safety Warnings; 03 – Cancel button;
04 – Open Another Device button

3.5.5. System Check

The System Check feature helps to verify that the current device, network and internet connectivity meet the requirements for using nCommand Lite properly. It performs a quick automatic test that checks essential items such as internet quality, access to required servers, and connection stability. This tool can be used before starting a session, during installation, or when any connection issue is suspected. It helps ensure that the platform will work as expected and assists the technical team if troubleshooting is needed.

Note: The System Check should preferably be used with the support or upon request of an IT professional. Running this tool without technical guidance may lead to misinterpretation of the results.

To access System Check, local and remote technologists must open the Session Details option from the drop-down menu available under their username, located in the upper-right corner of the main screen. Then, click **Open** next to the *System Check* tool. Once the tool page is displayed, click **Run Test** to start the verification process.

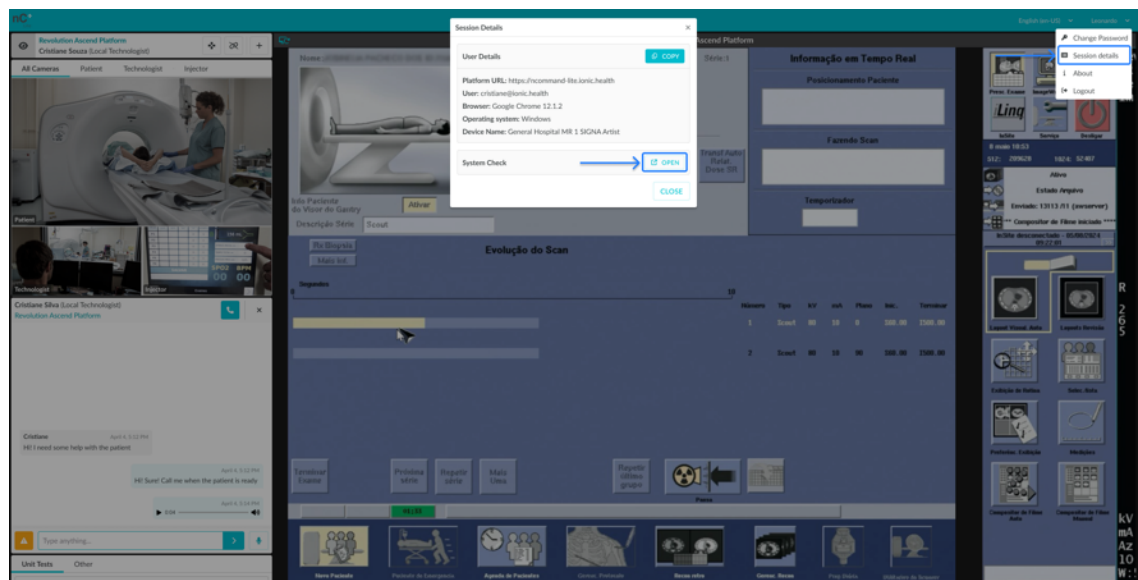


Figure 28: Accessing System Check

When using the remote technologist, it is possible to select a device on the tool's main screen so that it is included in the test results.



WARNING!

Before starting the test, make sure the selected device is not currently in use.

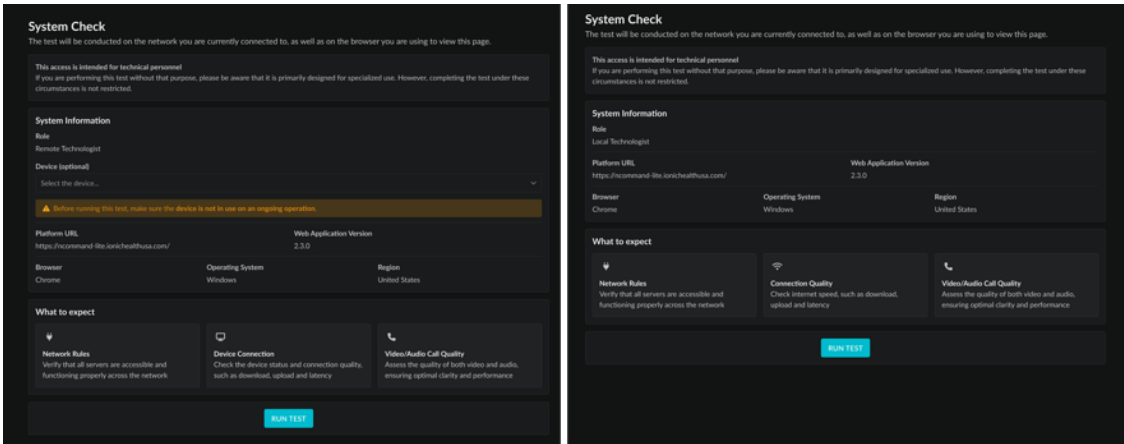


Figure 29: System Check main screen
Left - Remote Technologist / Right - Local Technologist

After the test is complete, a summary of the results is displayed on the screen. IT professionals can review this information to identify possible issues affecting the system's performance.

Section 3.6 - Chat

The platform provides a real-time Chat and Call with voice and video features, which is used for effective communication between licensed technologists. Through these features, the licensed technologists can interact regarding all matters related to the workflow of the session.



WARNING!

In case of failure, call the local technologist by phone.

Upon connecting to a device, you will have immediate access to the chat user list, organized into two tabs. For multi-site customers, each branch can be configured as a separate contract. When enabled, users are grouped by contract, with users from other contracts appearing under the "Others" tab.

To start a conversation, double-click a user's name to open the chat interface, which supports both text messaging and voice calls. Ensure the session selected corresponds to the correct device. The platform notifies users if the network connection becomes slow or unstable.



WARNING!

Before initiating contact, verify the device name shown below the user's name, as some remote technologists may be connected to multiple devices.

Here are the tools available for communication within the platform:

1. **Voice and Video Calls:** Click the icon to initiate a voice and video call of up to 60 minutes between a Remote and a local technologist. Connections between users with the same profile (Local–Local or Remote–Remote) are not supported.

When a local technologist initiates a call, the remote technologist can choose to accept or decline. Conversely, when a remote technologist initiates the call, it is automatically

connected and the local technologist is notified—these functions as a safety mechanism to ensure that the remote technologist can always communicate with whoever is physically present at the site, as if they were there in person.

By default, the microphone is active at the start of the call, while the camera remains off. Each technologist can manually turn their microphone and camera on or off at any time.

To successfully establish a call, both users must have a functioning microphone and audio output, with browser permissions properly enabled. If any of these components are missing, the system will notify both users and the call will not be completed. A camera is optional—if it is unavailable or not detected, the system will update the icon to reflect that video is not supported.

Only one active call is allowed per user. If a technologist tries to start a new call while already in one, the system will block the attempt and display a notification. Similarly, if a user is already on a call and receives another incoming call, the caller will be informed that the recipient is currently unavailable, and the user on the ongoing call will receive an alert indicating that someone attempted to contact them.

2. **Closing Chats:** When one of the users closes the chat by clicking the close button, an automatic message is sent to the other user, and the chat tab is closed. This ensures that both parties are informed that the conversation has ended. When the chat window is closed, all messages disappear. If you reopen it during the session, the conversation restarts without previous messages.
3. **Text Messages:** Send text messages in the designated field. When a message is sent, an icon with a gray check mark appears, and when the message is received by the recipient, another icon with two blue check marks is displayed. This allows safe, clear, and concise written communication between the two parties.
4. **Call for attention:** Attract the other user's attention by clicking the button with an exclamation mark. This action applies a visual vibration effect to the other user's window for a few seconds and a message is sent automatically, signaling urgency or importance.
5. **Audio Messages:** Send audio messages by clicking the microphone button. This is used when you want to convey a message more personally or when typing is not convenient.

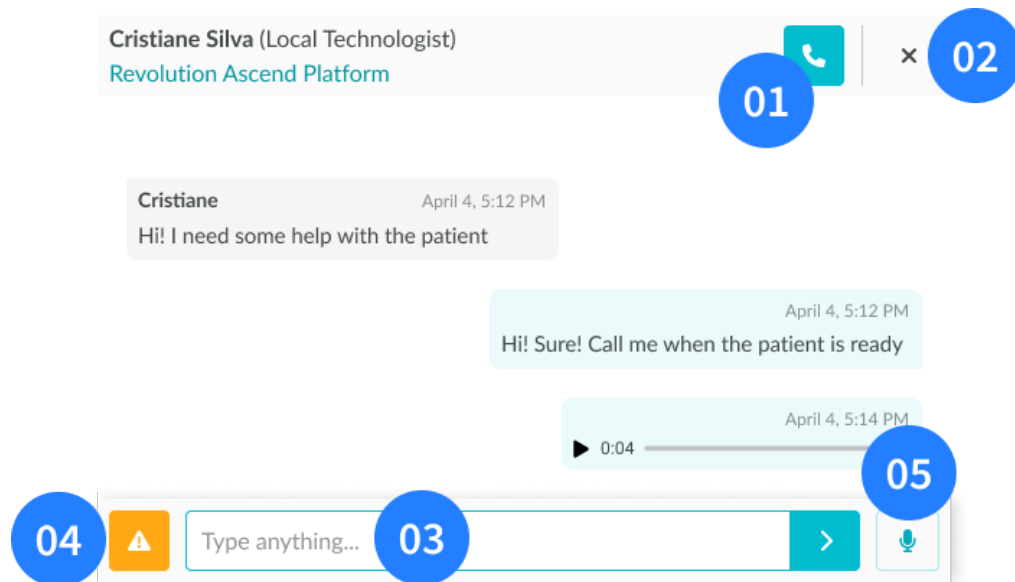


Figure 30: Chat Window View

01 – Voice and Video Call button; 02 – Close Chat button; 03 – Message Text Box;
04 – Call for attention button; 05 – Record Audio Message button

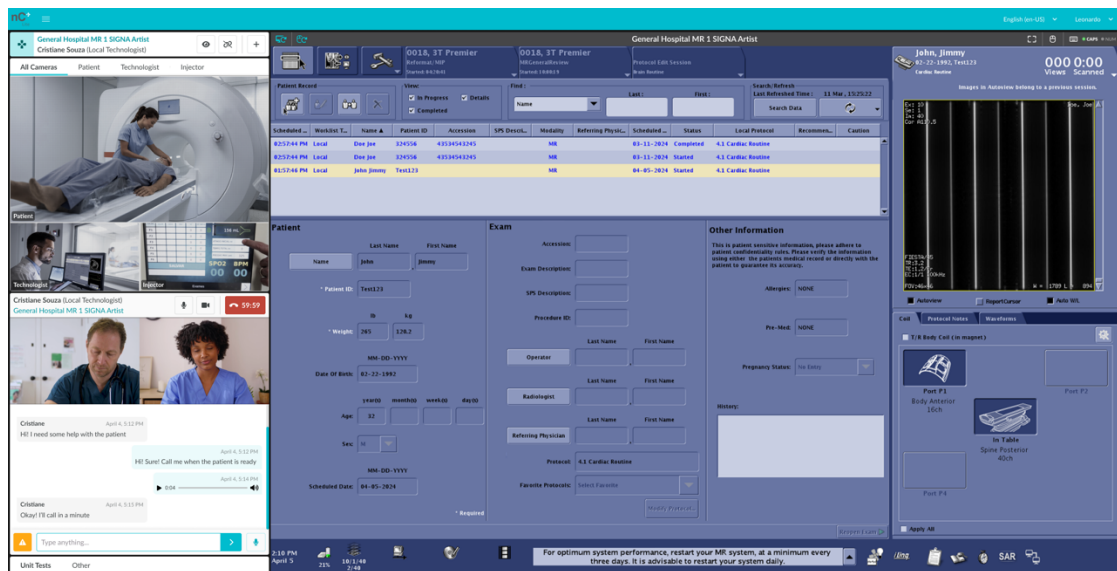


Figure 31: Remote Technologist main screen - Chat window (bottom left corner)

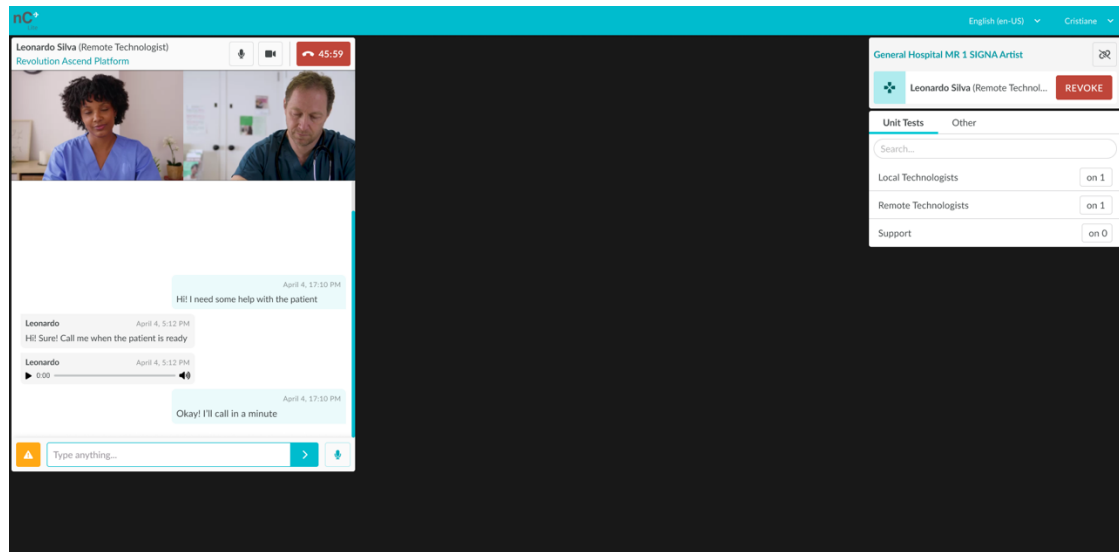


Figure 32: Local Technologist main screen - chat window

Internet Connection Issues - When one of the technologist's experiences network connection issues, the system will display a message and attempt to reconnect. If the connection is restored, the system will show an **ONLINE** message, and the remote session will continue as usual. However, after several reconnection attempts, if the connection is not reestablished, the system will terminate the active session and notify the technologist that they have been disconnected due to internet issues. At the same time, it will also notify the other technologist that their counterpart has been disconnected due to internet issues.

Section 3.7 - Ending Your Session on the Platform

At the end of his/her duty, the licensed technologist must disconnect from the device and log out from the platform.



WARNING!

The licensed technologists must not forget to log out of the platform before their duty ends.

To disconnect from the device, you need to click on the disconnect icon located in the Device Box. Note: If you are working as a local technologist, make sure you have revoked any remote technologist access before disconnecting from the device.

To ensure safety, you will receive a notification to confirm that you wish to disconnect from the device. After confirming, you will be redirected to the home screen, without any device selected.

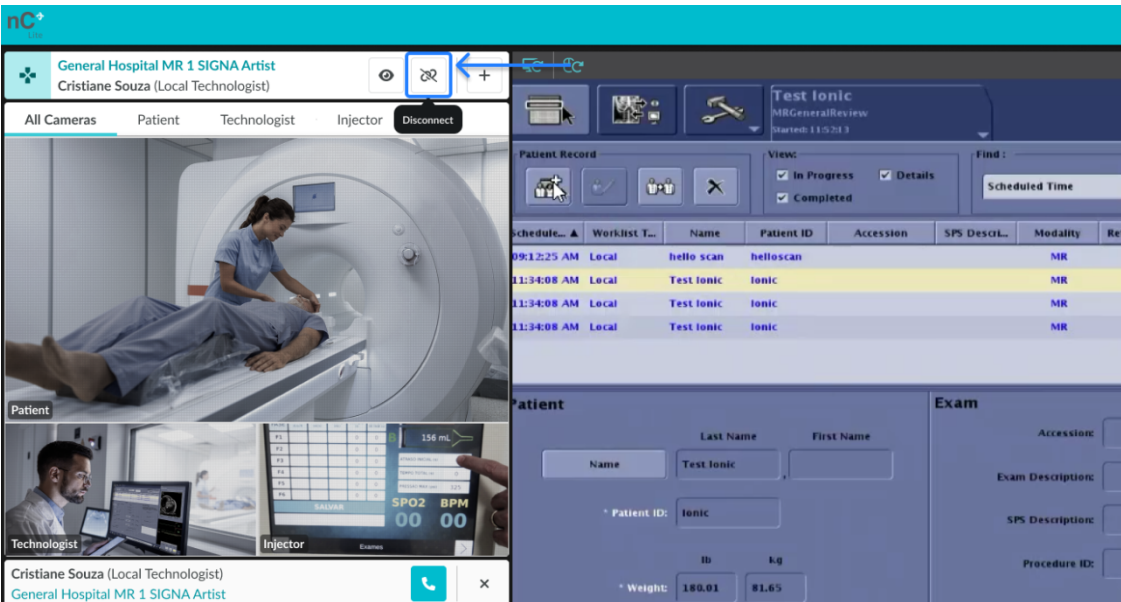


Figure 33: Disconnect Button - Remote Technologist main screen

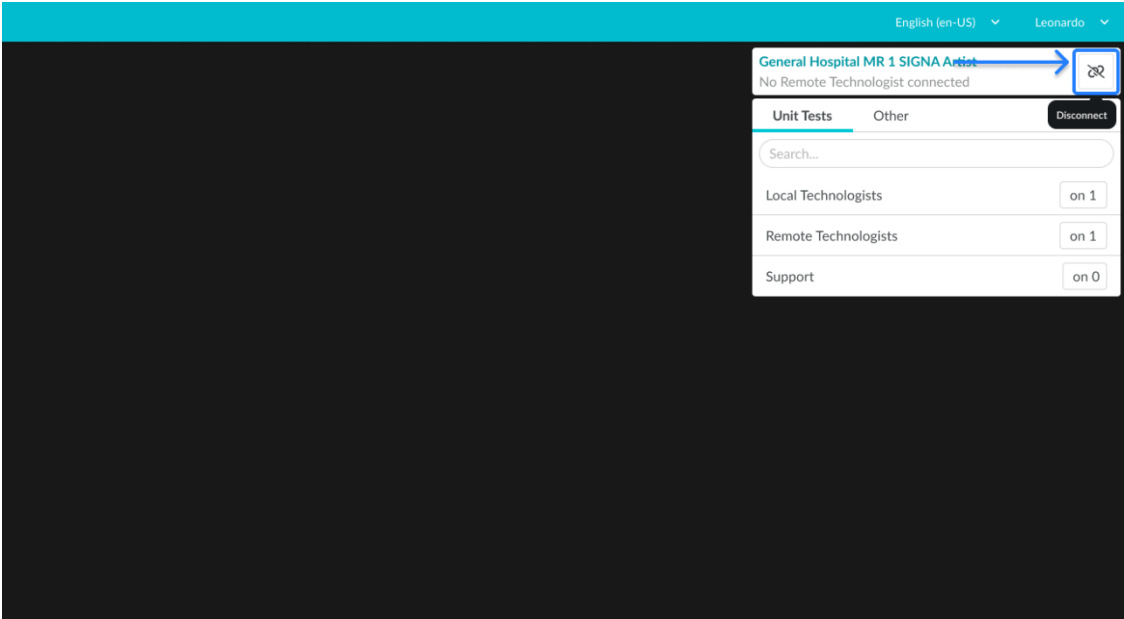


Figure 34: Disconnect Button - Local Technologist main screen



WARNING!

Before logging out, make sure that all additional tabs that were opened are closed.

To end your session on the platform, click on your username located in the upper right corner of the screen and select the “Logout” option. You will receive a notification to confirm that you wish to leave the medical center where you were working. After confirming, you will be redirected to the application's login page, thus safely concluding your work journey.

nCommand Lite does not control the user’s session on the external IdP and therefore cannot perform a logout at the IdP level. In scenarios where users share the same machine and use Single Sign-On (SSO), it is recommended that each user selects the “do not stay signed in” option during External IdP login (if available) or signs out of the IdP after signing out of nCommand Lite. This ensures that no subsequent user on the same device can unintentionally reuse an active session.

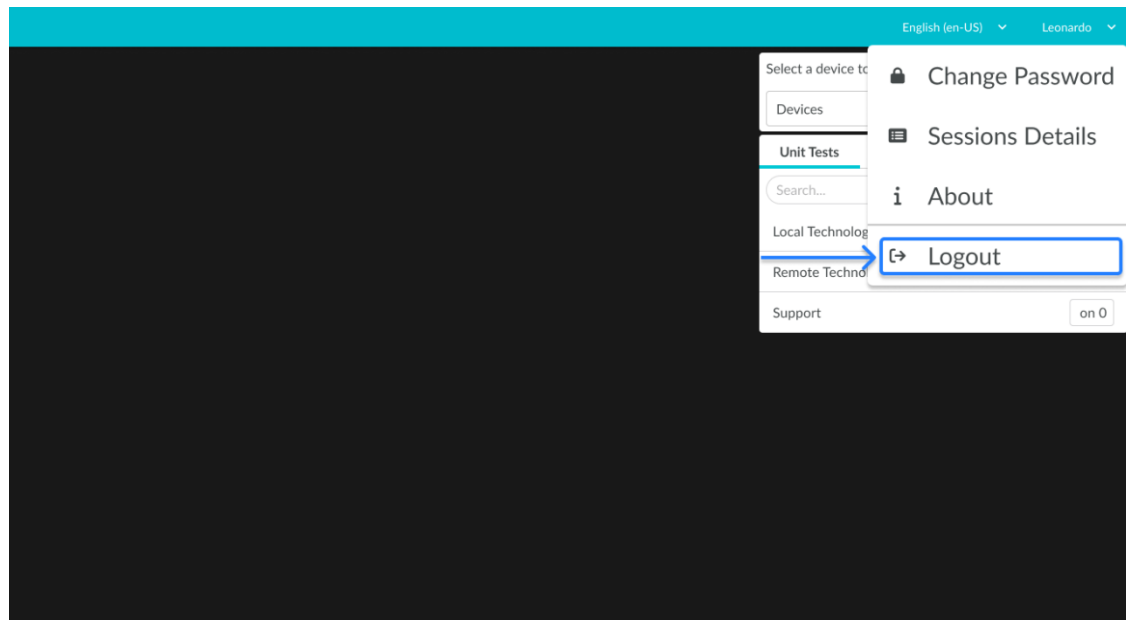


Figure 35: Logout Dropdown Menu Item



WARNING!

When using an external identity provider on a shared or public computer, after login out of the platform, also logout from the identity provider. For more information on how to proceed, contact your organization's IT support team.

Section 3.8 - Operational Training

Participation in the training program is mandatory for all users of the nCommand Lite System. User registration on the platform is managed by the IONIC Health team and is only initiated after confirmation that the user has successfully completed the required LMS training and is properly qualified to operate the platform. This process ensures that all users possess a thorough understanding of the system's functionalities and are prepared to use the platform efficiently and safely. To initiate the training enrollment process, please contact your sales representative.

Section 3.9 - Troubleshooting Guidelines

USER AND PASSWORD	
Password Change	Validate that the password requirements have been met, the password must be strong and secure, including at least one lowercase letter, one uppercase letter, one special character and be at least 8 characters long.
Forgot My Password	Check your Email Inbox: Ensure you are using the correct email address and that the password recovery email has not been filtered into your spam or junk folder. Try Again: Wait a few minutes and request another password recovery email by clicking "Did you Forget your password?". Check Internet Connection: Make sure you are connected to the internet.
Welcome Email Not Received	Check to see whether the email is in your spam folder. If it is not there, contact an admin user to ensure that the email provided in your registration is correct. If it is not correct, the admin should update it and resend the welcome email.
Two-Factor Authentication Code Not Received	Click on 'Resend Code' and check your spam folder. If you do not receive it, please contact an admin user to verify whether the email registered in the Access Control is correct.
Exceeded login attempts	If you exceed the allowed number of login attempts, you must wait for a period before trying again.
EXTERNAL IDENTITY PROVIDER	
Issues Logging In to the Product	If you encounter login issues while using an external Identity Provider (IdP), please note that the authentication process is managed entirely by the IdP and not by the product provider i.e: Ionic Health. As such, the product cannot assist with account credentials, access policies, authentication errors or account lockout. In these cases, you should contact your organization's IT support team, who can

	review the IdP configuration and help resolve the issue.
Credential Issues	Any credential-related issues (e.g., forgotten password, password change) must be resolved directly with your organization's IT support team. They can review the IdP configuration and provide the necessary assistance.
Multi-factor authenticator (MFA) issues	Any multi-factor authenticator (MFA) related issues (e.g., MFA expiration issues, MFA not working, login without requesting MFA) must be resolved directly with your organization's IT support team. They can review the IdP configuration and provide the necessary assistance.
Credentials not working on the platform	When using external identity providers (IdP), login to the product only using the IdP. Using the IdP credentials directly on the login page of the product will result in unsuccessful login.
SCANNER COMPUTER MONITOR	
Does Not Turn On	Check the monitor's connections to the computer and the electrical outlet. Disconnections may occur. Press the monitor's power button again.
PLATFORM	
Unreachable	Check the network connection. Check whether the platform has started and whether the login has occurred.
Platform Latency	Refresh the page by pressing Ctrl+F5. Check if the unit's (medical facility's) chat is open in more than one tab. If so, close the tab that is not being used. If the issue persists, try logging out of the platform, clearing the cache, closing the browser and then logging back in.
Malfunctioning Features	Before trying other troubleshooting procedures, clear the browser cache (look for instructions on your current browser) after login, then close and reopen the browser, log back into the platform, and retry the action.
Upgrade	After the platform has been upgraded, clear your browser cache (refer to the instructions for your browser) before logging in to the new version.

AUDIO	
No Sound	Ensure that the unit's (medical facility's) microphone and speaker volumes are adjusted to appropriate levels. Check if the browser has permission to use audio and microphone. Check if the headset is connected and functioning properly.
Sound Latency	Check the equipment's electrical and network connections. Refresh the browser page by pressing Ctrl+F5 and log in again. If the issue persists, try logging out of the platform, clearing the cache, closing the browser and then logging back in.
CHAT	
Chat Does Not Appear	Make sure the browser is not minimized. Otherwise, open the chat after logging into the nCommand Lite platform. Check that the unit (medical facility) has been selected and the user is authorized to enable chat communication. Make sure your browser's audio and microphone permissions are accepted. Check the cable connections, which may be disconnected. Refresh the browser page by pressing Ctrl+F5 and reconnect to the platform. Check if the site's chat is open in more than one tab. If so, close the tab that is not being used.
Chat Delay	Refresh the browser page by pressing Ctrl+F5 and reconnect to the platform. If the issue persists, try logging out of the platform, clearing the cache, closing the browser and then logging back in. Check the cable connections, which may be disconnected.

Trouble Sending Audio Messages	Check browser permissions for audio and microphone and ensure that both microphone and audio devices are connected to the computer. If browser permissions need to be adjusted, press Ctrl+F5 to prompt the browser to recognize the changes upon page reload.
Voice Call Failed to Initiate	Check your internet connection and see if any notification explaining the reason for the call not starting was displayed. Ensure that you have an audio device connected and that audio and microphone permissions are allowed in the browser. If the issue persists, refresh the page with Ctrl+F5 to try again.
User Not Found in Chat	If you are unable to locate a user in the chat, click on the 'Others' tab to ensure they are not listed there. Users associated with other contracts appear separately in the contact list. If your user does not appear in the contact list after selecting the device, press Ctrl+F5 to refresh the screen and select again. Ensure you have an internet connection.
REQUESTING ACCESS TO DEVICE	
Platform did not recognize that the local technologist is connected	Check under the 'Others' option to confirm whether the local user is connected. If the user is indeed connected but you are still receiving the message that the local user is not connected to the scanner, refresh the screen by pressing Ctrl+F5, and ask the local user to repeat the same instruction. Then, select the device again and ask the local user to select the device again as well. If the issue persists, contact support to check the network.
Access request is not being sent	Refresh the page by pressing Ctrl+F5 and confirm with the local user via chat if the access request is being received. If the issue persists, please contact support for further assistance.
STREAMING DEVICE (e-KVM COMPUTER)	
Streaming Device (e-KVM COMPUTER) Not Working	Click the "Reload streaming" button on the platform.

	Ensure that the uninterruptable and stabilized power supply (medical facility) and/or streaming device are correctly connected and turned on. Turn off the streaming device and all other equipment and turn it on again. Refresh the platform.
Streaming Device Slow	Click the "Reload streaming" button on the platform. Refresh the page with Ctrl+F5 and reconnect to the platform. Check the quality of your network connection. To validate the network status, it is possible to conduct a ping test to the device to check for packet loss. After internet issues, the platform may not operate as intended. Refresh the webpage and request access to the local user again.
Loss of video output	It is admissible that an electrostatic discharge causes loss of image. After a restart of the system, the communication and video streaming should be automatically reestablished.

Section 3.10 - Hardware Cleaning Methods

- Before starting the cleaning process, ensure all equipment is disconnected from the electrical outlet.
- Do not use abrasive products.
- Do not immerse any equipment or peripheral in any type of liquid.
- Dispose of cleaning materials according to regulations for disposing of hazardous waste.
- It is not advisable to use spray disinfectant as vapor may enter the equipment and cause a short circuit or corrosion.
- This product is non-sterile

Chapter 4 Cybersecurity and Privacy

Section 4.1 - Security and Privacy Risks

The **nCommand Lite System** implements multiple technical and organizational measures to protect processed information.

The system has been certified under ISO/IEC 27001 and ISO/IEC 27701 and follows a privacy-by-design approach. Supports compliance with healthcare data protection laws and cybersecurity regulations applicable in the EU, US, UK, Switzerland, Brazil, UAE, Saudi Arabia, Australia and New Zealand.

However, users must adopt best practices to prevent unnecessary exposure of sensitive data.

- Avoid sharing personal or sensitive information unless strictly necessary.
- Ensure that communications and system access occur in secure environments.
- If you suspect any malicious activity, immediately notify the responsible team.

Section 4.2 - Personal Data Protection (GDPR / HIPAA Compliance)

The **nCommand Lite System** complies with all applicable privacy and data protection laws and regulations in the regions where it operates, including, but not restricted to, GDPR, HIPAA, LGPD, and ISO/IEC 27701 requirements. All data processing activities are performed under the “**Processor**” and “**Sub-Processor**” roles as defined by GDPR, with strict regional data segregation to ensure compliance and prevent unauthorized cross-border data transfers

What data is collected?

- **Users:** Name, email, and company (strictly for authentication and access management).
- **Patient data:** Only medical exam transmissions via streaming in real time, with no data storage

How is data used and protected?

- Data is used exclusively for **authentication, access control, and session traceability**.
- Information transmission is secured through **AES-256 encryption for storage** and **TLS 1.3 for data in transit**.
- **Access is restricted** and follows the **principle of least privilege (RBAC)**.
- End-to-end encryption ensured for P2P video and control streams via WebRTC.
- Authorized cloud providers (e.g., Microsoft Azure) process limited data under strict contractual safeguards.

Users are granted the following rights:

- **Access and correction** of personal information.
- **Request for data deletion**, where applicable.

If you have any questions, email privacy@ionic.health to reach the Ionic Health DPO. All requests are handled within 30 days, extendable per GDPR.

Section 4.3 - Access Management and Authentication

Users are responsible for defining **access roles and permissions** for their teams, ensuring periodic reviews and documentation of granted access.

Best Practices and Controls

- Follow the **principle of least privilege (RBAC)**, ensuring users have only the necessary access.
- **Multi-Factor Authentication (MFA)** is mandatory for administrative access and recommended for all users.
- **Strong passwords** are required, with at least **8 characters, including uppercase and lowercase letters, numbers, and symbols**.
- **Do not share credentials**.
- Access permissions are monitored and reviewed periodically.

Monitoring: Access, permission modifications, and important activities are documented in the system's security logs. Logs are retained for a minimum of 7 years, in alignment with HIPAA, GDPR, and other applicable regulations. They support internal auditing, forensic analysis, and regulatory reporting. Logs are protected against tampering and stored in secure environments with access control.

Section 4.4 - System Check Access Control

The System Check feature is accessible exclusively through the **nCommand Lite Web Application** and requires valid credentials for login. Access is limited to authorized roles only — *Remote Technologist, Local Technologist, Admin, Role Supervisor* and *System Check User*.

The *System Check User* role is designed with restricted permissions, allowing access solely to diagnostic features related to network validation and connectivity verification. This ensures that network details, whitelisting information, and system metrics are never exposed to unauthorized individuals.

All access requests are authenticated via Azure AD B2C, with Multi-Factor Authentication (MFA) and adaptive conditional access policies managed by Microsoft Entra ID. Password complexity follows the organizational security policy, requiring at least eight characters, including uppercase and lowercase letters, numbers, and symbols. Passwords expire every 90 days, and sessions automatically log out after 24 hours of inactivity, extendable for up to 90 days with continuous use.

Section 4.5 - Regional Data Segregation and Log Retention

The **nCommand Lite** platform maintains strict regional segregation of data to prevent unauthorized or unnecessary cross-border transfers. Environments are isolated per region, ensuring compliance with applicable regulations.

All access logs, activity records, and security events are retained for a minimum of seven (7) years, in accordance with applicable data protection and healthcare regulations. Logs are stored in secure, access-controlled environments and protected against tampering. This information supports forensic investigations, compliance audits, and regulatory reporting.

Section 4.6 - Data Security and Integrity

The **nCommand Lite System** ensures the confidentiality, integrity, and availability of data through industry-standard security practices.

Users should ensure compliance with security protocols, regularly review access policies, and report any anomalies. The system continuously monitors activities, and administrators must enforce security policies to maintain a robust defense against potential threats.

The system is protected by 24/7 monitoring through a dedicated Security Operations Center (SOC) with SIEM capabilities for threat detection and response.

Section 4.7 - Security Incident Response

The system includes a documented Incident Response Plan, aligned with ISO 27035 and NIST CSF.

In the event of security incidents, such as unauthorized access or system failures, users must follow these steps:

How to Identify an Incident?

- **Unauthorized access** detected in activity logs.
- **Suspicious login attempts** or repeated authentication failures.
- **Unusual system behavior**, such as unexpected actions or malfunctions.

How to Report an Incident?

Immediately record the event through the available support channels (Chapter 5).

If a personal data breach is confirmed, IONIC, acting as a sub-processor, will notify GE as the Processor within 48 hours, providing all relevant evidence, impact details, and mitigation measures. GE, in turn, is responsible for notifying the Controller (the customer) in accordance with applicable legal and contractual requirements.

Chapter 5 Service Channels

Whether you need help with a technical issue, an unclear step in the process, or further guidance, our team is ready to assist. You can contact us via phone, email, or the ITSM Platform, whichever is more convenient for you. Our specialists are trained to offer personalized assistance, ensuring that any problem is resolved quickly and efficiently.

Phone numbers

United States	+1 (216) 2421223
Brazil	+55 12 3600 0181
Europe (Portugal)	+351 (300) 528 410
Australia	+1 (216) 2421223
New Zealand	+1 (216) 2421223

ITSM Platform

<https://ionichealth.desk.ms/?LoginPortal>

Email

helpdesk@ionic.health



WARNING!

Any serious incident related to the use of this device should be reported to both the manufacturer and the health authority/competent authority where the device is installed.

To report to the manufacturer: either contact your local service representative or report to: helpdesk@ionic.health

Please provide the following information:

- The system version number, displayed on the login screen;
- Date of incident;
- Description of incident, including any patient or user impact/injury;
- Your contact information (facility, address, contact name, title, and telephone number).

Chapter 6 Legal and Regulatory Information

Manufacturer



REF

nCommand Lite

IONIC HEALTH TECHNOLOGIES S.A.

Estrada Dr. Altino Bondesan, 500, Sala 1103-A
Eugênio De Melo
São José Dos Campos-SP
12247-016
Brasil

CNPJ: 35.594.747/0001-08
+55 12 3600-0181
contato@ionic.health

Responsible technician:

Alexandre Seiji Fukuda Ribas
CREA-SP: 5071085437

ANVISA

82585300004

Importer (USA)



REF

nCommand Lite System

IONIC HEALTH USA INC.

11201 Cedar Avenue, STE 600
Cleveland, OH 44106
USA

+1 (216) 242 1223

EU Representative / Importer



EU REP

REF

nCommand Lite



Notified Body identification number: 2803

EUROPE IONIC HEALTH DIGITAL TECHNOLOGIES, LDA

Rua de Raimundo Durães Magalhães, Lote 6/9
4475-189 Maia
Portugal

+351 (300) 528 410

Swiss Authorized Representative (CH-REP) / Importer**CH REP****REF**

nCommand Lite

FREYR LIFE SCIENCES GMBH

Bahnhofplatz
CH-6300 Zug
Switzerland

UK Responsible Person / Importer**REF**

nCommand Lite

FREYR LIFE SCIENCES LTD

9 Greyfriars Road
Reading, Berkshire
RG1 1NU
England, United Kingdom

Australian Sponsor**REF**

nCommand Lite

TAEVAS LIFE SCIENCES PTY LTD

46 Dora St
Blacktown NSW 2148
Australia

New Zealand Sponsor**REF**

nCommand Lite

TAEVAS LIFE SCIENCES LIMITED

Level 3, 1 Margaret Street
Lower Hutt 5010
New Zealand

BASIC UDI-DI: 7898974112NCLITE2L

Request for a hard copy

Hard copies of the nCommand Lite User Manual will be provided upon request at no additional cost. Contact your local representative and request a hard copy of the User Manual.

Manufacturing Date

Date of software release is found on the nCommand Lite login page, in a MONTH/YEAR format.

Chapter 7 Revision History

Revision	Change Description	Date
0	Updated manual version from 2.3 v1 to 2.4	25 November 2025
1	Updated Chapter 6 labels	04 December 2025
2	Removed the requirement for a static IP address from the local computer configuration in subsection 1.3.11 Updated the EU Authorized Representative symbol in subsection 1.3.12 Removed Note from Subitem 1.3.14 Updated the content in Chapter 2 Updated the EU Authorized Representative symbol in Chapter 6	28 January 2026
3	Reviewed the translation of “Responsible Technician” in Chapter 6	09 February 2026

APPENDIX I - Service Start Checklist

1. *Verify Electrical and Network Connections:*

Make sure that the electrical connections and network points are properly established on the e-KVM Computer, Scanner Computer, and the Local Computer.

2. *Check Power Status:*

Verify that the uninterruptable and stabilized power supply and the e-KVM Computer are turned on and functioning correctly.

3. *Quick access to the nC Lite platform:*

Confirm the presence of the nC Lite platform shortcut on the desktop for quick access.

4. *Access and Login to nC Lite Platform:*

Open the nCommand platform and log in to ensure full access and proper functionality.

5. *Chat Application Setup:*

Open the chat application within the nC Lite platform in only one tab and avoid minimizing it for seamless communication.