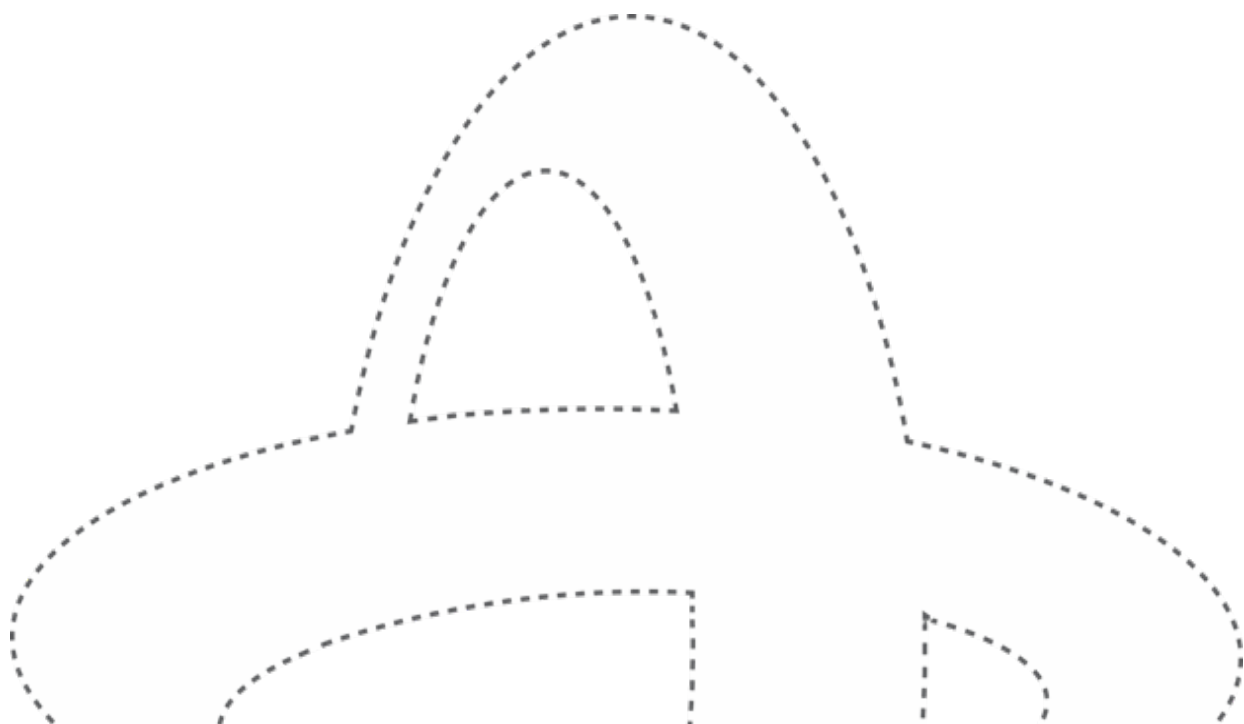




ПОТРЕБИТЕЛСКО РЪКОВОДСТВО

NCommand Lite v2.4

Версия на ръководството: V.3



Съдържание

Глава 1	Въведение	4
Раздел 1.1 -	Цел	4
Раздел 1.2 -	Речник	4
Раздел 1.3 -	Описание	5
1.3.1.	Употреба по предназначение	6
1.3.2.	Показания за употреба	6
1.3.3.	Предвидена популация от пациенти	6
1.3.4.	Среда на използване	6
1.3.5.	Противопоказания	6
1.3.6.	Възможности на платформата	6
1.3.7.	Клинични ползи	7
1.3.8.	Предвидени потребители	7
1.3.9.	Работна среда	8
1.3.10.	Среда на съоръжението	8
1.3.11.	Минимални изисквания	10
1.3.12.	Символи	11
1.3.13.	Експлоатационен живот	12
1.3.14.	Надстройка/Актуализация	12
Глава 2	Списък с общи предупреждения и предпазни мерки	13
Глава 3	Използване на платформата във всяко местоположение	16
Раздел 3.1 -	Достъп и използване на nCommand Lite	16
Раздел 3.2 -	Достъп до платформата за първи път	17
3.2.1.	Влезте чрез nCommand Lite	17
3.2.2.	Вход чрез външен IdP	19
Раздел 3.3 -	Управление на пароли	20
Раздел 3.4 -	Достъп с профил на местен технолог	23
Раздел 3.5 -	Достъп с профил на технолог от разстояние	26
3.5.1.	Режим на достъп	27
3.5.2.	Лента за стрийминг	30
3.5.3.	Многокамерно	33
3.5.4.	Отваряне на друго устройство	35
3.5.5.	Проверка на системата	37

Раздел 3.6 -	Чат.....	38
Раздел 3.7 -	Приключване на вашата сесия в платформата	42
Раздел 3.8 -	Оперативно обучение.....	44
Раздел 3.9 -	Указания за отстраняване на неизправности.....	45
Раздел 3.10 -	Методи за почистване на хардуера.....	51
Глава 4	Киберсигурност и поверителност	52
Раздел 4.1 -	Рискове за сигурността и поверителността.....	52
Раздел 4.2 -	Защита на личните данни (съответствие с GDPR/HIPAA)	52
Раздел 4.3 -	Управление на достъпа и удостоверяване	53
Раздел 4.4 -	Контрол на достъпа за проверка на системата.....	53
Раздел 4.5 -	Регионално разделяне на данни и съхранение на файлове с дневници	54
Раздел 4.6 -	Сигурност и цялост на данните	54
Раздел 4.7 -	Реакция при инциденти със сигурността	54
Глава 5	Канали за обслужване.....	56
Глава 6	Правна и регулаторна информация.....	57
Глава 7	История на редакциите	60
ПРИЛОЖЕНИЕ I -	Контролен списък за стартиране на услугата.....	61

**ВНИМАНИЕ**

Федералният закон ограничава това устройство до продажба от или по нареждане на лекар, както се използва от медицински технолог, лицензиран в щата, в който той/тя практикува.

(за Съединените американски щати)

**ВНИМАНИЕ**

В Бразилия този софтуер е оторизиран от Anvisa за използване изключително с устройство за ядрено-магнитен резонанс (ЯМР). Не е разрешена друга употреба.

(за използване в Бразилия)

**ВНИМАНИЕ**

Преди употреба се уверете, че сте наясно със специфичните изисквания на вашата страна или регион. Неспазването на разпоредбите може да доведе до рискове за здравето.

**ВНИМАНИЕ**

Уверете се, че версията на това ръководство за потребителя съответства на версията на използваната платформа. Използването на несъответстваща версия може да доведе до неправилна работа или неправилно тълкуване на функциите.

Глава 1 Въведение

Раздел 1.1 - Цел

Това ръководство има за цел да предостави на местните технолози и технолозите от разстояние, цялостно разбиране за специфичните функционалности на системата nCommand Lite. Служейки като ръководство за потребителя, този документ предоставя кратка и практична информация, насочвайки потребителите през функционалностите на системата и отстраняването на неизправности. Следвайки това ръководство, потребителите ще могат да използват nCommand Lite ефективно, което помага за увеличаване на производителността и намаляване на зависимостта от техническа поддръжка.

Раздел 1.2 - Речник

**ВНИМАНИЕ**

Този етикет се прилага за условия или действия, които представляват потенциална опасност. Може да причините леки наранявания или имуществени щети, ако пренебрегнете тези инструкции.

**ПРЕДУПРЕЖДЕНИЕ**

Този етикет идентифицира условия или действия, които водят до конкретна опасност. Ще причините тежки телесни наранявания или значителни имуществени щети, ако пренебрегнете тези инструкции.

Термин на платформата	Съответстващ термин
Съоръжение за образна диагностика	Медицинско заведение, звено, мобилни звена, здравно заведение, здравно звено
Дистанционно съоръжение	Отдалечена работна станция, Отдалечено място, Отдалечен офис, Отдалечено местоположение, Команден център
Платформа	Уеб приложение nCommand Lite
Система	nCommand Lite с всички подсистеми
Устройство	Медицински скенер, скенер, оборудване, медицинско изделие, изделие за образна диагностика, оборудване за образна диагностика
Местен технолог	Местен потребител, местен техник, местен здравен специалист (LHP), потребител на място

Раздел 1.3 - Описание

Системата nCommand Lite е SaMD (Софтуер като медицинско изделие), която е насочена към клиента и осигурява отдалечен достъп чрез уеб приложение за преглед/преглеждане на образна диагностика, както и възможност за дистанционно предоставяне на насоки в реално време на лицензирания технолог (локален потребител) до пациента, който работи с медицинските образни устройства в контекста на обучение или оценка на процедурата, за ЯМР, КТ и ПЕТ/КТ скенери.

Отдалечените потребители са лицензирани технолози, които могат да получат достъп до медицинско устройство за образна диагностика от компютър, който отговаря на минималните изисквани спецификации навсякъде, като използват защитена софтуерна връзка, която предава видео и осигурява достъп с клавиатура и мишка. Това позволява на отдалечените потребители да помагат на местните потребители, без разстоянието да е ограничение. Този достъп трябва да бъде предоставен от локалния потребител, използващ системата, и също така може да бъде отнет по всяко време от локалния потребител, като по този начин му позволява да поддържа пълен контрол върху сесията по всяко време. Освен това всяка отдалечена сесия се контролира чрез защитени идентификационни данни, които се управляват от локалния потребител. Връзките с медицинско изделие са ограничени до една отдалечена сесия наведнъж, за да се поддържа строг контрол върху това кой взаимодейства дистанционно със системата. Изображенията, прегледани дистанционно, не са за диагностична употреба.

Системата nCommand Lite се състои от ИТ хардуерно и софтуерно базирано инсталационно решение, което поддържа няколко сесии, позволявайки на технолози от разстояние да имат достъп до множество медицински изделия за образна диагностика при необходимост. Скенерите, които са съвместими със системата nCommand Lite, отговарят на общ протокол, позволяващ управление на параметри за сканиране и дистанционно сканиране.

1.3.1. Употреба по предназначение

Системата nCommand Lite осигурява отдалечен достъп за преглед/разглеждане на изображения, както и възможност за дистанционно предоставяне на насоки в реално време на лицензирания технолог, работещ със скенера. Това ръководство включва обучение, оценка на процедурите и управление на параметрите за сканиране.

1.3.2. Показания за употреба

Системата nCommand Lite позволява отдалечен достъп за преглед/разглеждане на изображения, както и възможност за дистанционно предоставяне на насоки в реално време на лицензирания технолог, работещ със съвместим ЯМР, КТ или ПЕТ/КТ скенер. Този достъп трябва да бъде предоставен от местния лицензиран технолог, който управлява системата. Отдалеченият достъп е наличен само за системи, поддържащи възможност за отдалечена свързаност. Изображенията, преглеждани дистанционно, не са за диагностична употреба.

1.3.3. Предвидена популация от пациенти

За всеки пациент е предписано да се подложи на образна диагностика чрез свързано медицинско изделие за образна диагностика.

1.3.4. Среда на използване

Съоръжения за образна диагностика, които извършват ядрено-магнитен резонанс (ЯМР), компютърна томография (КТ) и позитронно-емисионна томография – компютърна томография (ПЕТ/КТ) изследвания и отдалечени командни центрове.

1.3.5. Противопоказания

Платформата не трябва да се управлява от потребители, които не са лицензирани технолози и които не са преминали обучение за използване на nCommand Lite.

1.3.6. Възможности на платформата

- **Дистанционно сканиране:** показва екрана на медицинското изделие за изображения в реално време, което позволява на лицензиран технолог от разстояние да присъства на прегледа.
- **Чат:** прави комуникацията чрез текстови и гласови съобщения между местните лицензирани технолози и технолози от разстояние възможна. Местните технолози и технолозите от разстояние също могат да извършват и приемат гласови и видео разговори.
- **Мулти-камера:** улеснява дистанционното наблюдение на пациентите и медицинското заведение по време на процедурата. Технологът от разстояние може да получи достъп до изгледа на камерите чрез разделите, които са разделени между

всички раздели на камерата и отделните такива. Този механизъм възпроизвежда визуалния надзор, който би имал здравен специалист, ако се намира близо до пациента, като по този начин въвежда допълнителен слой на безопасност.

- **Многосесийното дистанционно сканиране** позволява на технолога от разстояние да получи достъп до множество медицински изделия за образна диагностика, ако е необходимо.
- **Режим на достъп:** позволява на технолога от разстояние да избира между изгледи или да управлява изделието. В режим на изглед, технолозите от разстояние могат да виждат само какво се предава. В режим на управление той/тя има контрол върху мишката и клавиатурата.
- **Управление на достъпа на технолог от разстояние:** позволява на местния технолог да контролира достъпа на технолога от разстояние и техния режим на достъп (Преглед или Управление). За да се позволи връзка на технолог от разстояние, достъпът трябва да бъде предоставен от местния технолог, използващ платформата, и също така може да бъде отменен по всяко време от местния технолог, като по този начин му позволява да поддържа пълен контрол върху сесията по всяко време.
- **Размер на стрийминга:** технологът от разстояние може да види оригиналния размер на стрийминга и текущия размер на стрийминга в пиксели. Той/тя също така се уведомява, когато текущият размер на стрийминг е по-малък от оригинала.
- **Състояние на мишката и клавиатурата:** технологът от разстояние има обратна връзка, ако мишката и клавиатурата на медицинското изделие за образна диагностика работят правилно.
- **Подробности за сесията:** местните и технолози и технолозите от разстояние могат да получат достъп до подробности за сесията.

1.3.7. Клинични ползи

nCommand Lite подобрява диагностичната образна диагностика, като позволява дистанционна работа на **ЯМР, КТ и ПЕТ-КТ** системи, осигурявайки постоянно качество на изображенията и спазване на протоколите. Тя позволява на опитни технолози да наблюдават и помагат при сканиранията в реално време, оптимизирайки ефективността на работния процес и намалявайки грешките, които биха могли да повлияят на точността на диагностиката. Системата улеснява сътрудничеството между технолозите, подобрявайки последователността на изпита и позволявайки по-бързо вземане на решения в сложни случаи. Като позволява на отдалечени специалисти да поддържат множество съоръжения, nCommand Lite увеличава **наличността, разнообразието и качеството** на образните изследвания, като гарантира, че повече пациенти имат достъп до усъвършенствана диагностика, като същевременно оптимизира здравните ресурси. Освен това помага за смекчаване на недостига на персонал чрез намаляване на зависимостта от специалисти на място, като същевременно поддържа съответствие със строги регулаторни стандарти и стандарти за сигурност на данните.

1.3.8. Предвидени потребители

- **Местен технолог**
Местният технолог е потребителят на място, отговорен за подпомагането и насочването на пациентите лично в медицинското заведение. Той/тя трябва да

притежава необходимите знания за извършване на процедури за сканиране на дадено изделие за образна диагностика. Освен това той/тя контролира режима на достъп на технолога от разстояние (Преглед или Управление) и отдалеченият достъп трябва да бъде предоставен от местния технолог чрез платформата и може да бъде отменен по всяко време.

- **Технолог от разстояние**

Професионалист, който извършва операции дистанционно, с достъп и контрол на компютъра на устройството. Подобно на местния технолог, технологът от разстояние също трябва да има необходимите познания за извършване на процедури за сканиране на дадено изделие за образна диагностика.

- **Поддръжка/ИТ потребител**

Професионалист, отговорен за настройката на платформата (не е включен в това ръководство за потребителя).

1.3.9. Работна среда

Следните спецификации се отнасят до екологичните изисквания на e-KVM компютъра.

- **Максимална надморска височина (без налягане)**

- Експлоатация: От 0 м (0 фута) до 3048 м (10 000 фута)
- Съхранение: От 0 м (0 фута) до 12 192 м (40 000 фута)

- **Температура**

- Експлоатация: От 10°C (50°F) до 35°C (95°F)
- Съхранение: От -10°C (14°F) до 50°C (122°F)

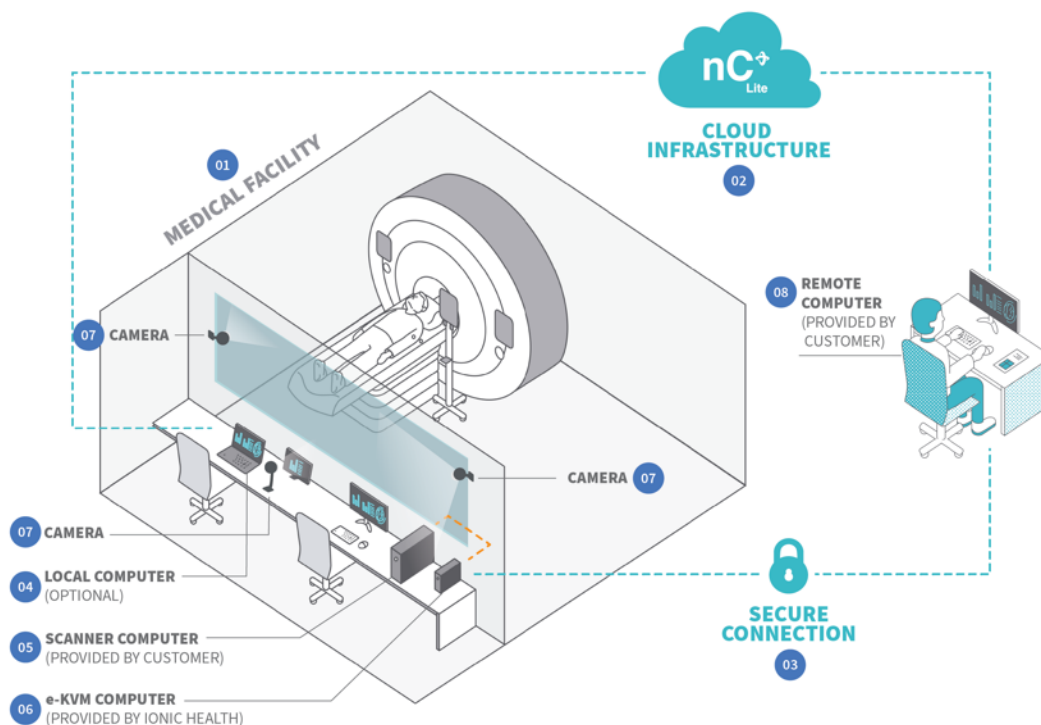
- **Относителна влажност**

- Експлоатация: 20%-80% (без кондензация)
- Съхранение: 10%–90% (без кондензация)

1.3.10. Среда на съоръжението

Платформата nCommand Lite има два различни типа местоположение на средата:

- **Съоръжение за образна диагностика:** Съоръжения, които извършват ядрено-магнитен резонанс (ЯМР), компютърна томография (КТ) или позитронно-емисионна томография – компютърна томография (ПЕТ/КТ) и изследвания.
- **Отдалечено съоръжение:** Място, където технолози от разстояние могат да получат достъп и дистанционно да управляват устройства (ЯМР, КТ или ПЕТ/КТ скенери). Тази работна станция може да се използва в различни среди като офиси, командни центрове, отдалечени места или дори второстепенни места в здравното заведение. Отдалечената работна станция може да бъде разположена във всяко пространство, което осигурява на потребителя подходящи условия за концентрация, минимална свързаност и изпълнение на изискванията за компютърна конфигурация.



Фигура 01: Преглед на продукта и неговите връзки чрез защитена връзка (напр. VPN).
01 – Медицинско съоръжение; **02** – Облачна инфраструктура; **03** – Сигурна връзка; **04** – Локален компютър (по желание);
05 – Компютър скенер (предоставен от клиента); **06** – e-KVM (предоставено от IONIC Health);
07 – Камера; **08** - Отдалечен компютър (предоставен от Клиента)



ПРЕДУПРЕЖДЕНИЕ!

Съвместимост с дистанционно сканиране

IONIC Health (IH) валидира функционалността за дистанционно сканиране на изброените съвместими устройства. IH извършва пълна оценка на изискванията за дистанционно сканиране на IH и тества системата в целевата среда по време на инсталация. Това гарантира съвместимост и правилна работа по това време за дистанционно сканиране. Тази проверка не означава, че всички изисквания за OEM (производител на оригинално оборудване) устройства са изпълнени в тази конфигурация. Всяко отклонение от изискванията на OEM е отговорност на крайния потребител.

Промените в системата или околната среда след инсталирането трябва да бъдат докладвани на IH, за да се провери продължаващата съвместимост. IH не може да гарантира производителност или да поеме отговорност за конфигурации, различни от тези, валидирани по време на инсталацията.

1.3.11. Минимални изисквания

- **Локален компютър**

Този компютър се използва от **местния технолог** за разрешаване и поддръжка на отдалечения достъп до устройството чрез nCommand Lite®. Той също така позволява директна комуникация с **технолога от разстояние** чрез функцията за чат на платформата.

Минимално необходимите технически спецификации са:

- Процесор: AMD® A4-9120C или по-висока версия, или подобна
- Памет: 4 GB или повече
- Съхранение: 128 GB SSD или повече
- Периферни устройства: микрофон и високоговорител, или слушалки и уеб камера
- Монитор: 14" FHD (1920 x 1080) или по-висок
- Операционна система: Chrome OS, Windows OS или MAC OS
- Място за инсталиране: този компютър трябва да е близо до компютъра на скенера
- ИТ рутина: Създайте пряк път на nCommand Lite на работния плот на всеки потребител
- Съвместимост с браузъра: Google Chrome или Microsoft Edge.

- **Отдалечена работна станция**

Тази станция се използва от **технолога от разстояние** за достъп и управление на устройството чрез nCommand Lite®. Отдалечената работна станция трябва да установи защитена връзка с e-KVM компютъра (предоставен от IONIC HEALTH®).

Клиентът е отговорен за предоставянето на отдалечения компютър и ще вземе решение за един от двата сценария: първият е работа 24x7, а вторият е работа в работно време.

За всеки сценарий по-долу ще намерите подходящите спецификации за избор на модели компютри:

Сценарий 1 (Работа 24x7) - Трябва да отговаря на следните спецификации:

- Intel Xeon W-2223 (4 ядра, 8 нишки, 8,25 MB кеш, 3,90 GHz Turbo) или по-висок.
- RAM: 16 GB или повече.
- Графика: NVIDIA RTX A2000 6GB или по-нова версия, или подобна.
- Съхранение: 128 GB SSD или повече.
- Операционна система: Windows 11 Pro 64B или по-нова версия.
- Минимални изисквания за монитор: Размер 27", съотношение на страните 16:9, разделителна способност 4k.
- Слушалки: BLACKWIRE 3200 или подобни.
- Съвместимост с браузъра: Google Chrome или Microsoft Edge.

Сценарий 2 (Работа в работно време) - Трябва да отговаря на следните спецификации:

- Intel® Core™ i7-12700k vPro® или по-нова версия.
- RAM: 16 GB или повече.
- Графика: NVIDIA T400 GB или по-нова версия, или подобна.
- Съхранение: 128 GB SSD или повече.

- Операционна система: Windows 11 Pro 64B или по-нова версия.
- Минимални изисквания за монитор: Размер 27", съотношение на страните 16:9, разделителна способност 4k.
- Слушалки: BLACKWIRE 3200 или подобни.
- Съвместимост с браузъра: Google Chrome или Microsoft Edge.

**ПРЕДУПРЕЖДЕНИЕ!**

Неспазването на подходящата настройка и минималните изисквания може да доведе до влошена или неуспешна комуникация между потребителите.

- **Мрежови конфигурации (минимални изисквания)**

За да се установи сесията между отдалечения потребител и е-KVM компютъра, трябва да се осигури мрежова комуникация между двете устройства. Системата nCommand Lite използва peer-to-peer (P2P) за установяване на връзка между локален потребител, отдалечен потребител и е-KVM компютър. Има три съвместими сценария:

- **Сценарий 1** – Корпоративна мрежа, която използва един от следните протоколи: LAN, LAN-to-LAN, MPLS или VPN;
- **Сценарий 2** – Корпоративна мрежа, която използва надеждна WAN (външна мрежа) и не използва нито един от следните протоколи: LAN, LAN-to-LAN, MPLS или VPN;
- **Сценарий 3** – Обществена мрежа от страна на отдалечения компютър (отдалечен потребител).

Конфигурациите за всеки сценарий са подробно описани в техническата документация.

1.3.12. Символи

Символ	Описание	Препратка
	Производител	ISO 15223-1, ISO 7000-3082
	Дата на производство	ISO 15223-1, ISO 7000-2497
	Символът показва, че този продукт е медицинско изделие	ISO 15223-1
	Уникален идентификатор на устройството	ISO 15223-1
	Справка за модела	ISO 15223-1, ISO 7000-2493
	Вносител	ISO 15223-1, ISO 7000-3725

	Консултирайте се с ръководството за потребителя	ISO 15223-1, ISO 7000-1641
	Дистрибутор	ISO 15223-1, ISO 7000-3724
	Внимание	ISO 15223-1, ISO 7000-0434A
	Предупреждение	ISO 7010-W001
	Сериен номер <i>(или версия на софтуера)</i>	ISO 15223-1, ISO 7000-2498
	Упълномощен представител в Европейската общност	ISO 15223-1
	Швейцарски оторизиран представител (CH-REP)	ISO 15223-1
	CE - Европейска маркировка за съответствие; 2803 – Наименование на нотифициран орган	Регламент 2017/745 на ЕС

1.3.13. Експлоатационен живот

Очакваният експлоатационен живот на продукта е 5 години, като се има предвид полезният живот на компонентите, които съставляват продукта. Тази цялостна оценка гарантира, че продължителността на живота на всеки критичен компонент е в съответствие с общия експлоатационен живот, гарантирайки постоянна производителност и надеждност през цялата предвидена продължителност на продукта.

1.3.14. Надстройка/Актуализация

IONIC Health ще актуализира системата nCommand Lite като част от планираните версии за поддръжка или надстройка. Тези актуализации са предназначени да осигурят непрекъсната производителност и надеждност, без да нарушават текущо внедрената версия на клиентските обекти. В зависимост от естеството на актуализацията, продуктът може да бъде надстроен дистанционно или може да изисква посещение на място от полеви инженер.

Глава 2 Списък с общи предупреждения и предпазни мерки



ПРЕДУПРЕЖДЕНИЕ!

Моля, прочетете всички предупреждения по-долу, преди да използвате системата nCommand Lite.



ВНИМАНИЕ

Системата nCommand Lite не може да се подлага на ремонт или поддръжка, докато се използва за управление на ЯМР, КТ или ПЕТ-КТ оборудване в присъствието на пациент.

- Обърнете голямо внимание на всички системни сигнали, тъй като те са от решаващо значение за безопасната работа.
- Дайте приоритет на безопасността и вниманието по време на всички операции.
- Федералният закон ограничава това устройство до продажба от или по нареждане на лекар, като се използва от медицински технолози, лицензирани в щата, в който той/тя практикува.
- Системата nCommand Lite трябва да се използва само от технолози, които са преминали обучение за използване на платформата.
- Използвайте тази система само със съвместими уеб браузъри. Поддържаните браузъри са Google Chrome и Microsoft Edge.
- В случай на извънредни ситуации, обучен, лицензиран технолог трябва да остане в съоръжението за образна диагностика, за да извърши операцията ЯМР, КТ или ПЕТ/КТ без nCommand Lite.
- Достъпът до множество устройства едновременно изисква интензивен фокус и комуникация с местните екипи.
- Избягвайте достъпа до устройства с идентично оформление или изследвания на една и съща анатомична област едновременно.
- Можете да преглеждате няколко екрана, но управлението е ограничено до едно устройство в даден момент.
- Винаги инициирайте чат, когато сте свързани с устройство за ясна комуникация.
- Сигналите за обаждания се появяват на екрана на свързаното устройство; само едно обаждане може да бъде активно в даден момент.
- Тествайте видео комуникацията при достъп до приложението (преди началото на работна сесия), за да проверите дали има повреда във връзката за видео изход на устройствата за ЯМР, КТ или ПЕТ/КТ или на друго устройство, свързано с видео стрийминг.
- Устройството не трябва да се включва в контакта и/или непрекъсваемото и стабилизирано захранване чрез удължителни кабели или "щепселни ленти".
- Ако възникнат повреди на видеото, проверете видео връзката между системата на устройството и e-KVM компютъра.

- Ако приложението е бавно в отдалечения си достъп, опреснете страницата с командите Ctrl+F5 в брауъра на компютъра на технолога от разстояние. Ако проблемът продължава, свържете се с техническата поддръжка.
- Всеки път, когато страницата на брауъра се обнови, връзката с устройството се прекъсва, което изисква процесът на одобрение да се извърши отново.
- Не влизайте с помощта на друг брауър, когато вече сте влезли.
- Съоръжението за изображения на клиента трябва да има резервна интернет връзка с доставчик, различен от основния, за незабавна промяна в случай на загуба на комуникация със системата/платформата.
- В случай на загуба на комуникация или забавяне на мишката, извършете „ресинхронизиране с мишката“ на страницата, използвана в брауъра.
- Уверете се, че компютрите, използвани за управление на системата nCommand Lite, както в съоръжението за образна диагностика, така и в командния център, отговарят на минималните изисквания; в противен случай може да има загуба на ефективност на приложението.
- QoS (качество на услугата) следва да се прилага към основната връзка и резервната връзка за предаване на платформата, а ефективността на връзката да се наблюдава.
- Преди употреба проверете нивата на звука и микрофона, както и разрешението за аудио и микрофон в уеб брауъра.
- Преди употреба проверете функционирането на клавиатурата и мишката; ако са бавни или не са синхронизирани, активирайте бутона "повторно синхронизиране с мишката". Проверете дали e-KVM компютърът е свързан и включен.
- Уверете се, че клавиатурната подредба в отдалеченото съоръжение е идентична с клавиатурната подредба в изделието за образна диагностика.
- Ако е необходимо да се промени мястото, където се използва платформата, клиентът трябва да се обади на техническата поддръжка, за да направи нова инсталация. Не преинсталирайте, без да се свържете с техническата поддръжка.
- Преди да започнат процеса на отдалечен достъп до устройството за ЯМР, КТ или ПЕТ/КТ, е важно екипите на технолозите да проверят всички елементи, необходими за правилното функциониране на платформата, за да не възпрепятстват изпита. Тези елементи са изброени в документа "Контролен списък за стартиране на услугата".
- Конфигурацията на защитната стена на съоръжението за образна диагностика трябва да се проверява ежемесечно с ИТ екипа, като се потвърди, че няма проблеми с изданието на защитната стена, които биха могли да компрометират използването на nCommand Lite.
- Всяка аномалия, наблюдавана при използването на приложението, трябва незабавно да бъде съобщена на екипа за поддръжка, преди да започне достъпът или да бъде прекратен, ако вече е започнал.
- Само лицензирани технолози, обучени за използване на nCommand Lite, трябва да работят с приложението.
- Отдалеченият достъп чрез платформата не замества и не се конкурира с никоя друга оперативна процедура за ЯМР, КТ или ПЕТ/КТ операция, установена от производителя на медицинското изделие и протоколите и процедурите на лечебното заведение.
- Избягвайте да огъвате или разтягате хардуерните кабели.
- Ако възникнат проблеми с гласовата или чат комуникацията, използвайте функцията за телефонно обаждане, за да установите комуникация между местния технолог в съоръжението за изображения и технолога от разстояние в командния център. Следвайте

инструкциите, описани в раздела "Насоки в случай на повреда" и, ако е необходимо, свържете се с техническата поддръжка, за да извършите ремонта.

- Ако е необходимо да се подмени компютър или друго оборудване, което пряко влияе върху инсталацията на nCommand Lite, активирайте техническата поддръжка, като гарантирате запазването на работата на системата.
- Само един човек в даден момент може да получи отдалечен достъп до ЯМР, КТ или ПЕТ/КТ устройството.
- Не докосвайте никакви физически видео кабели, докато компютърът на устройството и системата nCommand Lite са включени.
- При достъп до допълнително устройство ще се отвори нов раздел. Плъзнете този раздел към втори монитор, тъй като системата е проектирана да се използва с отделен екран за всяко устройство.
- Всеки сериозен инцидент, свързан с използването на това устройство, трябва да бъде докладван както на производителя, така и на здравния орган/компетентния орган, където е инсталирано устройството (*Вижте повече подробности в главата Канали за обслужване*).

Глава 3 Използване на платформата във всяко местоположение

Раздел 3.1 - Достъп и използване на nCommand Lite



ПРЕДУПРЕЖДЕНИЕ!

В случай на възникване на проблеми, свържете се с техническата поддръжка за съдействие.



ПРЕДУПРЕЖДЕНИЕ!

Проверете подредбата на клавиатурата и се уверете, че е идентична и на двете места (медицинско заведение и отдалечено заведение). Различните клавиатурни подредби могат да попречат на потребителското изживяване.

Тази глава предоставя всичко, което трябва да знаете, за да получите достъп и да започнете да използвате платформата nCommand Lite. Ще намерите прости инструкции стъпка по стъпка за влизане, навигация в интерфейса и разбиране на основните функции. Независимо дали работите на място или дистанционно, това ръководство ще ви помогне да започнете бързо и уверено.

Промяна на езика - Системата е предварително настроена на английски по подразбиране, но можете лесно да промените езика според вашите предпочитания. На екрана за вход щракнете върху горния десен ъгъл, където се показва "English (en-US)". Това ще отвори падащ списък с налични езици, от които можете да избирате.

След като влезете, можете също да промените езика, като щракнете върху текущо избрания език от дясната страна на горната лента. Това ще отвори падащ списък с налични езици, от които можете да избирате.

Моля, имайте предвид, че ако промените езика, докато сте свързани с устройство, текущата връзка ще бъде прекратена автоматично и ще трябва да се свържете отново.

Когато влизате в платформата, можете да изберете предпочитания от вас език на екрана за вход. Въпреки това, някои съобщения, показани по време на процеса на влизане, може да се появят на езика, зададен във вашия уеб браузър, независимо от езика, избран в платформата. За последователно изживяване препоръчваме да приведете езиковите настройки на браузъра си в съответствие с предпочитания от вас език на платформата.

Раздел 3.2 - Достъп до платформата за първи път

Процесът на влизане в платформата може да се извърши по два начина: чрез nCommand Lite или чрез външен доставчик на самоличност (външен IdP). Потребителят може да влезе с помощта на един от предварително конфигурираните методи. Ако конфигурираният метод е външен доставчик на самоличност (външен IdP), методът nCommand Lite няма да работи и обратно. За да влезете чрез External IdP, отидете директно на **поделемент 3.2.2.**

3.2.1. Влезте чрез nCommand Lite

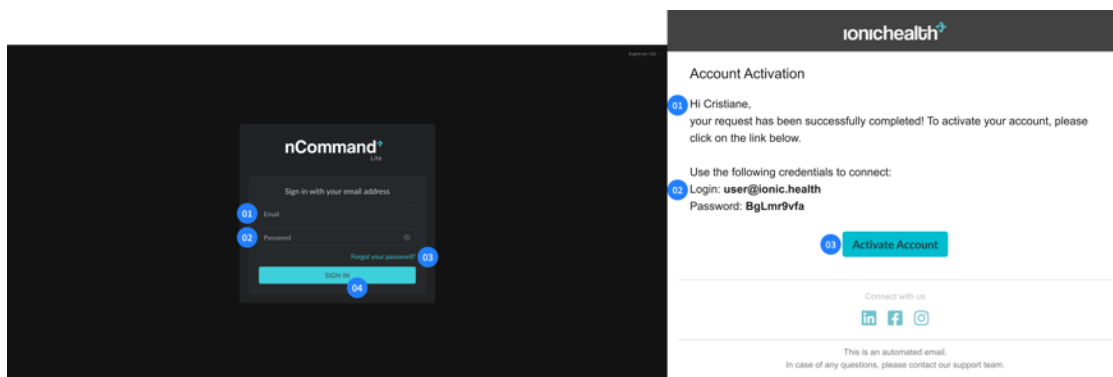
Забележка: Този раздел не се прилага за потребители, които влизат чрез външен доставчик на самоличност (външен IDP).

Включете компютъра и щракнете двукратно върху иконата за пряк път nCommand Lite, която обикновено е на работния плот. Можете също така да получите достъп до URL адреса директно в браузъра.

Първият ви достъп е решаваща стъпка, за да започнете да използвате платформата безопасно и ефективно. Ето какво трябва да знаете:

1 - Имейл за добре дошли: Ще получите имейл с вашите данни за достъп, включително свързания с вас личен имейл, временна парола и директен линк към клиентската платформа. Този имейл е от съществено значение, за да започнете работата си с nCommand Lite.

2 - Създаване на парола: При достъп до връзката ще трябва да въведете свързания имейл и паролата, получена в имейла за добре дошли. Като щракнете върху "Вход", ще бъдете насочени към страница за създаване на нова парола. Трябва да въведете старата, новата парола и потвърждението на новата парола. Тя трябва да е здрава и сигурна, включваща поне 3 елемента от следното: малка буква, главна буква, цифра и символ, и да е най-малко 8 знака дълга. Като щракнете върху "Продължи", ще бъдете пренасочени към страница, за да потвърдите имейла си отново. Като щракнете върху "Продължи", ще бъдете пренасочени към началния екран, който е персонализиран според вашия конкретен потребителски профил.



Фигура 02: Първи достъп

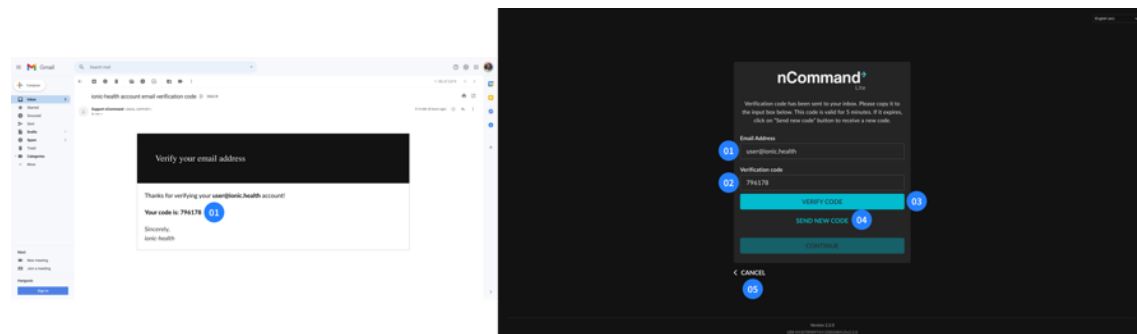
Ляво - страница за вход: 01 – Имейл адрес; 02 – Парола; 03 – "Забравихте паролата си?"; 04 – Бутон за вход

Дясно - Имейл за добре дошли: 01 – Имейл текст за активиране на акаунта; 02 – Идентификационни данни за вход; 03 – Бутон за активен акаунт

Тази първоначална процедура е предназначена да гарантира максимална сигурност на вашия акаунт от самото начало. От втория ви достъп нататък процесът ще бъде опростен, но също толкова сигурен, като при всяко влизане ще бъде изпращан двуфакторен код за удостоверяване на свързания ви имейл, за да се гарантира постоянната сигурност на вашия акаунт.

След като влезете в nCommand Lite, системата автоматично ще ви насочи към началния екран, който е персонализиран според вашия конкретен потребителски профил. Независимо дали сте местен технолог или технолог от разстояние, интерфейсът е проектиран да отговори на нуждите и достъпа, свързани с вашата роля. Този интуитивен дизайн гарантира, че разполагате с всички инструменти и информация, необходими за ефективно и ефикасно потребителско изживяване от момента, в който влезете.

Забележка: Когато методът за влизане е конфигуриран като nCommand Lite, влизането винаги трябва да се извършва чрез тази опция. Дори ако на екрана за вход се появи бутон за външен IdP, той няма да работи за тези потребители. Всеки потребителски акаунт се регистрира в платформата с конкретен метод за удостоверяване — или nCommand Lite идентификационни данни, или External IdP услуга. Ако потребител се опита да влезе с различен от този метод назначен на акаунта му, системата ще покаже съобщение за грешка, което показва, че акаунтът не е разрешен за този тип удостоверяване.



Фигура 03: Двухфакторно удостоверяване (2-FA)

Легенда – Имейл: 01 – 2-FA Код

Видно - Страница за двухфакторно удостоверяване: 01 – Имейл адрес; 02 – Код за потвърждение;
03 – Бутон за потвърждаване на кода за проверка; 04 – Изпрати нов код; 05 – Отказ

3.2.2. Вход чрез външен IdP

В някои случаи потребителите могат да влязат в платформата чрез външен доставчик на самоличност (IdP), който им позволява да използват съществуващата услуга за удостоверяване на организацията си, механизъм, известен още като Single Sign On (SSO). По този начин предварително регистрираният потребител няма да получи имейл за добре дошли. Локалната ИТ услуга трябва да провери съвместимостта, да конфигурира метода и да информира потребителя кой имейл (External IdP) трябва да се използва.

Когато тази опция е налична, потребителят винаги трябва да влиза с помощта на външния идентификатор (напр. Amazon Cognito, Microsoft Entra ID, Microsoft AD B2C). Методът за влизане чрез nCommand Lite няма да бъде достъпен за външни потребители на IdP.

За да влезете с помощта на външния идентификатор, щракнете върху бутона с името на IdP и следвайте инструкциите, предоставени от външния удостоверявател. Ако вашата институция има повече от един интегриран външен IdP, не забравяйте да потвърдите при кой доставчик сте регистрирани. Други доставчици няма да работят. Ако имате въпроси или срещнете затруднения, свържете се с местната ИТ служба.

В сценарии, в които потребителите споделят една и съща машина и използват еднократна идентификация (SSO), се препоръчва всеки потребител да избере опцията „не оставяй влизан“ по време на вход във външен IdP (ако е налично) или да се отпише от външния доставчик след излизане от nCommand Lite.

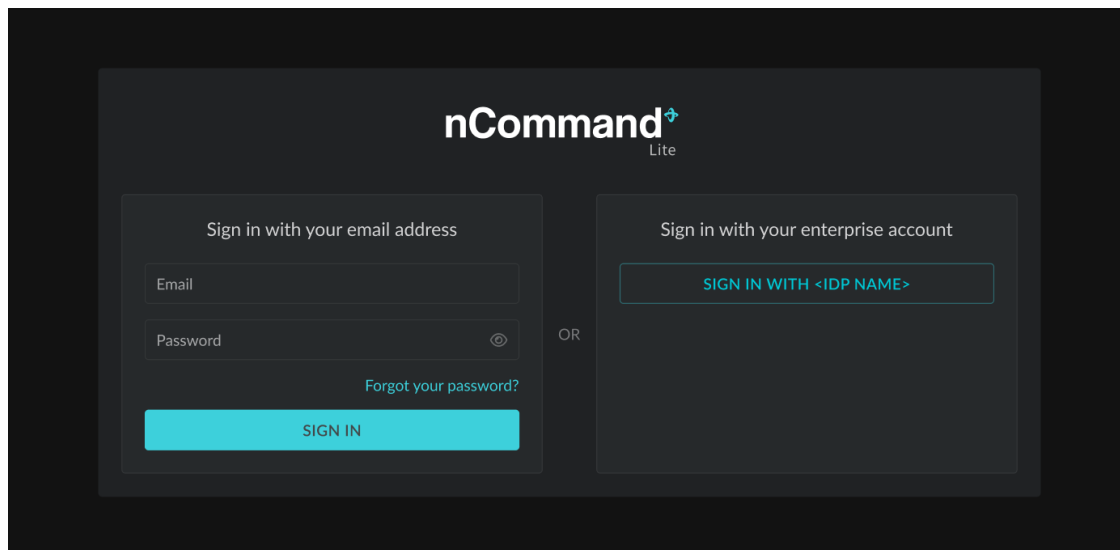
За тази опция за влизане пълният процес на влизане и излизане – включително правила за създаване и изтичане на парола, многофакторно удостоверяване (MFA) и заключване на акаунти – се управлява изцяло от ИТ екипа на клиента, който е конфигурирал външния IdP.

При влизане чрез външен IDP функциите „Забравена парола“ и „Промяна на парола“ трябва да се изпълняват според процеса на външния IDP.

Забележка: Опцията „Забравена парола“ ще продължи да се показва на екрана за вход, но няма да бъде активна за тези потребители. Той може да насочи към следващите

стъпки от процеса, но няма да го завърши. Ако трябва да възстановите паролата си, следвайте инструкциите от вашия външен идентификатор.

Важно: Дори когато използва външен IdP, потребителят трябва да бъде предварително регистриран в платформата nCommand Lite, за да получи достъп.



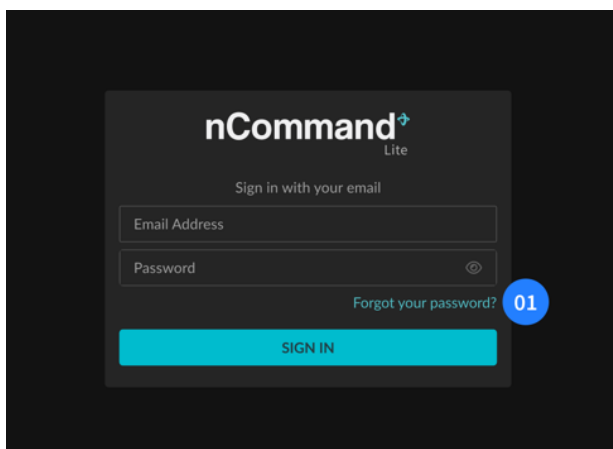
Фигура 04: Екран за вход чрез външен IdP (Пример)

Раздел 3.3 - Управление на пароли

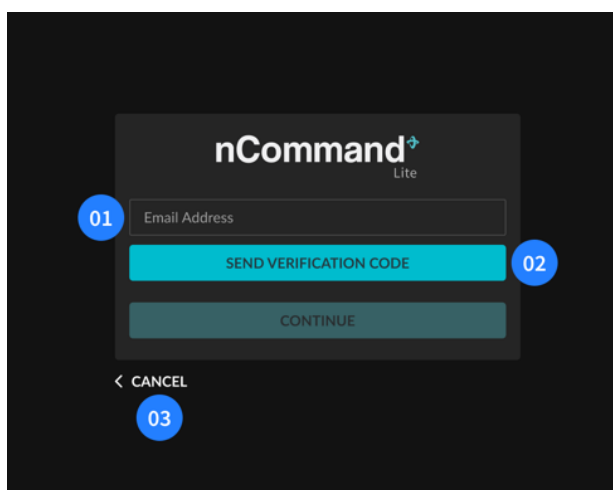
След като влязат в платформата за първи път, потребителите могат да променят паролата си или, ако е забравена, да зададат нова парола.

Забележка: При влизане чрез външен IdP, функциите **Забравена парола** и **Промяна на парола** трябва да се изпълняват според процеса на външния IdP.

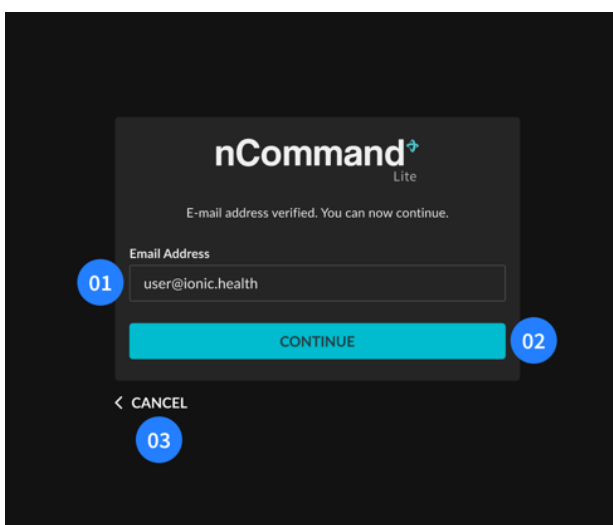
- **Възстановяване на парола:** Позволява на потребителите да възстановят достъпа до акаунта в случай на забравяне на паролата си. Просто щракнете върху връзката "Забравена парола?" на страницата за вход, въведете свързания имейл адрес и изпратете информацията. След това системата ще изпрати имейл, съдържащ код за потвърждение. Когато попълват кода и щракват върху "Потвърждаване на кода", потребителите ще бъдат помолени да потвърдят свързания имейл. Като кликнат върху "Продължи", потребителите се насочват към страница, където могат да въведат нова парола и потвърждение на новата парола. Ако новата парола отговаря на системните изисквания, потребителите могат успешно да я регистрират и впоследствие да влязат с актуализираните идентификационни данни.



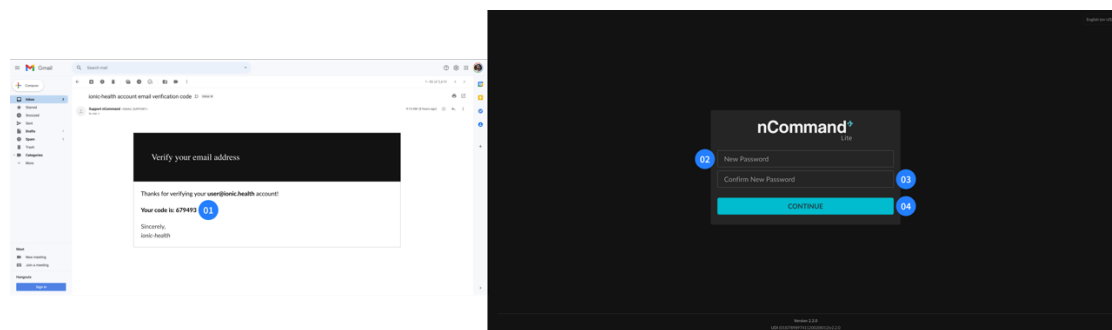
Фигура 05: Връзка към страницата за нулиране на парола
01 – Забравили сте паролата си?



Фигура 06: Страница за нулиране на парола
01 – Имейл адрес; 02 – Изпращане на код за потвърждение; 03 – Отказ

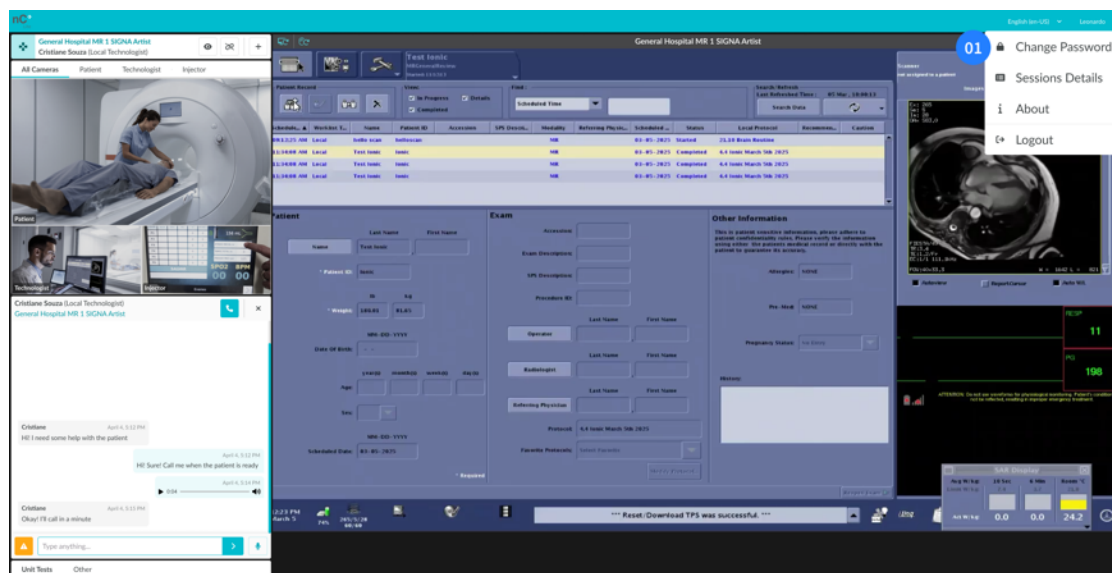


Фигура 07: Имейл потвърждение
01 – Имейл адрес; 02 – Продължи; 03 – Отказ

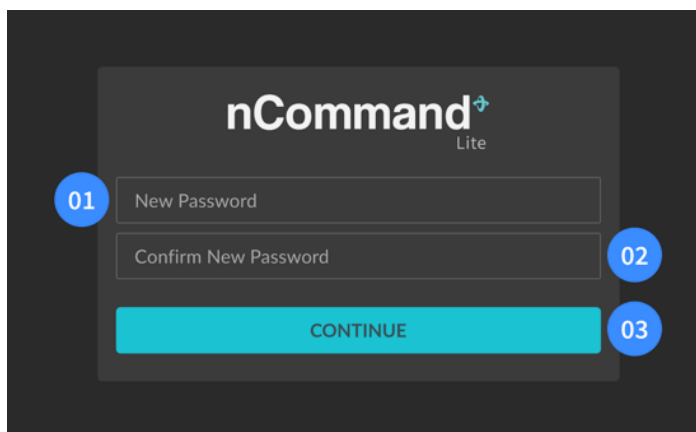


Фигура 08: Имейл с код за регистрация на нова парола (вляво) - 01 – 2-FA код
Страница за промяна на парола (вдясно) - 02 – нова парола; 03 – Потвърждаване на новата парола; 04 –
Бутон Продължи

- Промяна на паролата:** Позволява на потребителите да актуализират паролата си, като се придържат към определени критерии, включително поне 3 елемента от следното: малка буква, главна буква, цифра и символ и да бъде дълга най-малко 8 знака. Системата проверява дали новата парола отговаря на тези критерии и подканва потребителя със съобщение, ако не отговаря. Освен това потребителите трябва да потвърдят новата парола, за да предотвратят грешки при въвеждане. За да промени паролата, потребителят, след процеса на влизане, трябва да щракне върху иконата в горния десен ъгъл и да избере менюто "Промяна на паролата". Той/тя ще бъде прекъснат от платформата и ще бъде насочен към страница за потвърждаване на свързания имейл. След това системата ще изпрати имейл, съдържащ код за потвърждение. Когато попълват кода и щракнат върху "Проверка на кода", потребителите се пренасочват към екран, където могат да въведат нова парола.



Фигура 09: Промяна на парола, падащо меню елемент
01 – Промяна на паролата



Фигура 10: Страница за промяна на парола
01 – Нова парола; 02 – Потвърдете новата парола; 03 – Бутон Продължи

Раздел 3.4 - Достъп с профил на местен технолог



ПРЕДУПРЕЖДЕНИЕ!

Преди да използвате платформата, свържете се с технолога от разстояние по телефона.



ПРЕДУПРЕЖДЕНИЕ!

За да избегнете прегряване, моля, не поставяйте никакви предмети пред въздушния охладител на e-KVM компютъра и за да предотвратите повреда, не поставяйте никакви предмети върху него.



ПРЕДУПРЕЖДЕНИЕ!

По време на дистанционните сесии местният технолог отговаря за управлението и прилагането на местните правила за безопасност за всеки вид изпит и неговите специфични изисквания. Винаги оставайте в контролната зала и/или стаята за преглед, за да гарантирате безопасността както на пациента, така и на участващите специалисти.



ПРЕДУПРЕЖДЕНИЕ!

Движенията на масата по време на сесията трябва да се извършват от местния технолог само по искане на системата. Преди да напусне операционната, местният технолог винаги трябва да отнема достъпа на технолога от разстояние.



ПРЕДУПРЕЖДЕНИЕ!

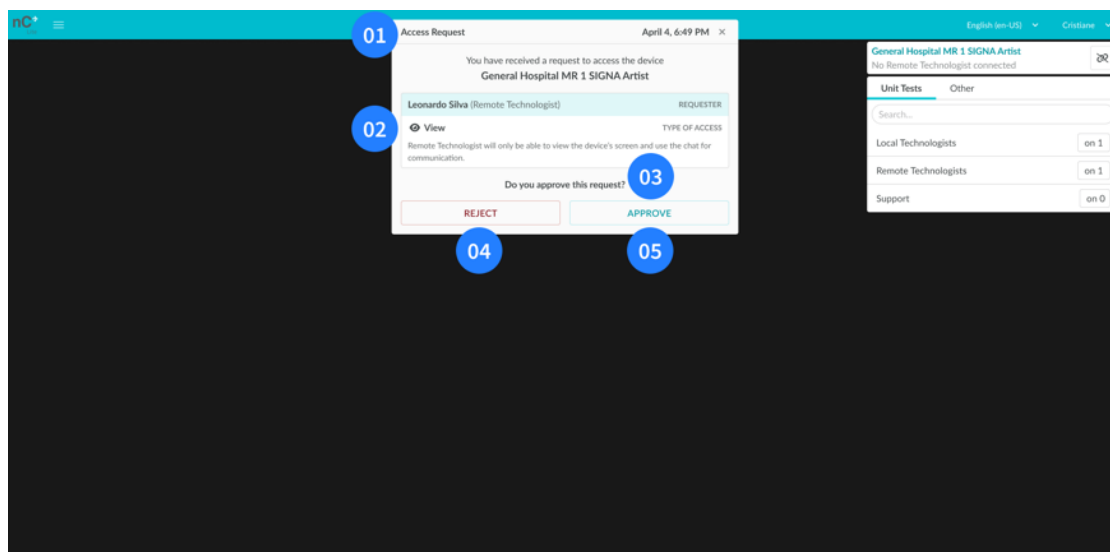
Само местният технолог има право да премести масата, за да позиционира пациента вътре в устройството и да освободи пациента безопасно. Преди да напусне операционната, местният технолог винаги трябва да отнема достъпа на отдалечения потребител.

След като влезете в платформата, продължете да изберете желаното устройство в полето за избор на устройство. Вие ще носите отговорност за това устройство, така че можете да прегледате заявката на технолога от разстояние за достъп до устройството. Когато технолог от разстояние иска да получи достъп до устройството, ще се появи изскачащ прозорец, който ви позволява да прегледате цялата представена информация, преди да предоставите или откажете достъп. Бъдете нащрек за входяща заявка от технолог от разстояние. От изключителна важност е внимателно да проверите всеки детайл. В случаите, когато предоставената информация не се признава, не предоставяйте достъп.

Технологът от разстояние може да получи достъп до устройството с помощта на един от двата режима на достъп: **Контрол** или **Преглед**:

- **Режим на управление** - позволява на технолога от разстояние да управлява мишката и клавиатурата, както и да преглежда стрийминга на устройството. Местният технолог обаче не губи контрол над локалната мишка и клавиатура и може да поеме контрола по всяко време.
- **Режим на преглед** - позволява на технолога от разстояние да преглежда само екрана на устройството и да използва чата за комуникация

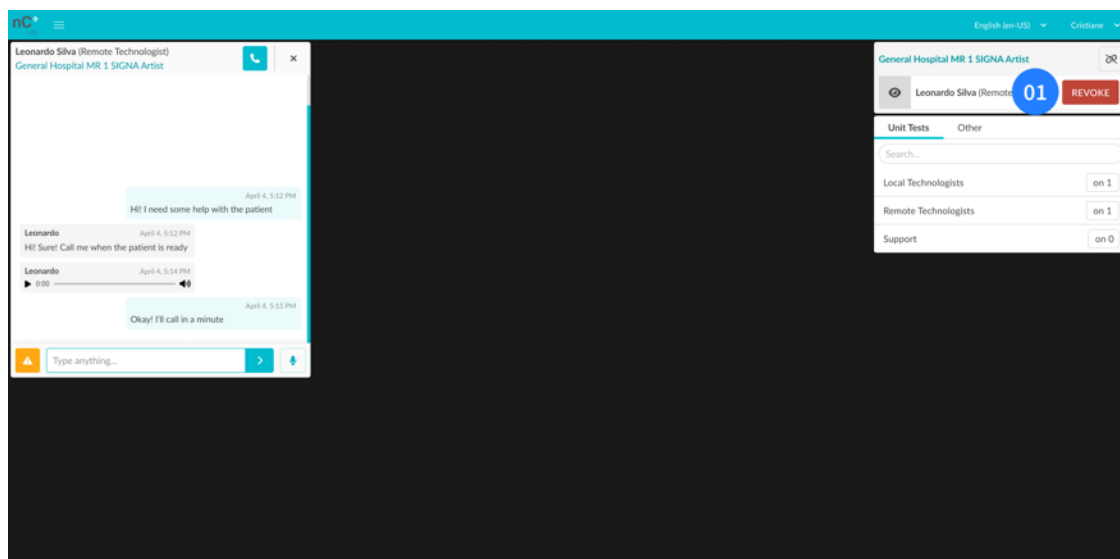
След като избере устройството, потребителят има достъп до функцията за чат, позволяваща комуникация чрез текстови, аудио съобщения, гласови и видео разговори с останалите потребители.



Фигура 11: Екран на Местен технолог с известие за заявка за достъп

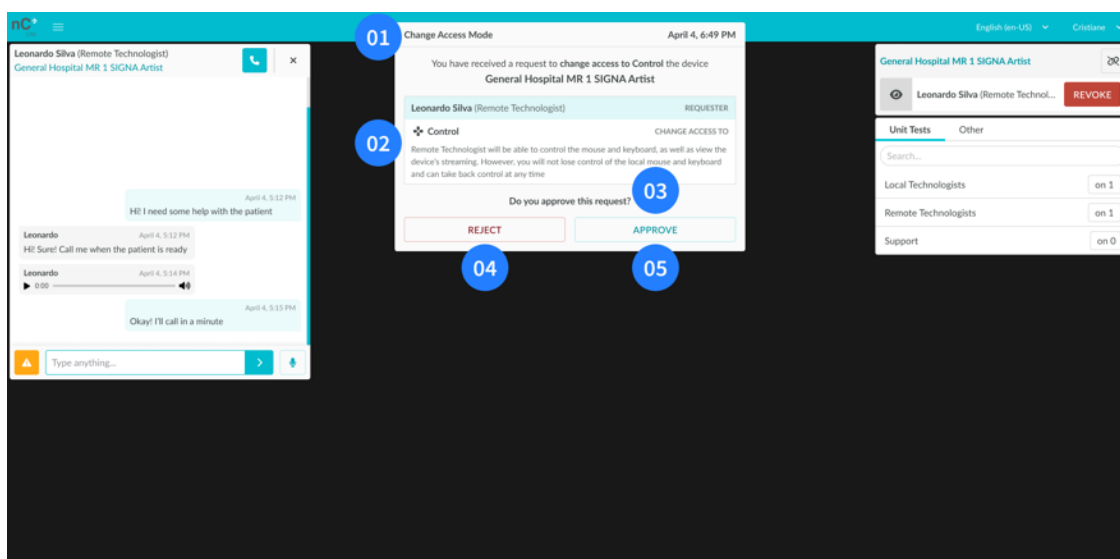
01 – Заглавие (Заявка за достъп); **02** - Име на заявителя, роля и описание на типа достъп;
03 – Подкана: "Одобрявате ли това искане?"; **04** – Бутон Отхвърляне; **05** – Бутон Одобряване

След одобрение, местният технолог може да отмени достъпа на технолога от разстояние по всяко време, като просто щракне върху бутона ОТМЯНА.



Фигура 12: Основен екран на Местен технолог при свързване към устройство
01 – Бутон за отмяна

По време на дистанционната сесия, технолога от разстояние може да поиска промяна на режима на достъп. На екрана ще се появи изскачащ прозорец за заявка. Можете да го одобрите или отхвърлите. Имайте предвид привилегиите, които всеки режим на достъп позволява на технолога от разстояние.



Фигура 13: Основен екран на Местен технолог с Искане за промяна на режима на достъп
01 – Заглавие (промяна на режима на достъп); 02 - Име на заявителя, роля и описание на типа достъп;
03 – Подкана: "Одобрявате ли това искане?"; 04 – Бутон за отхвърляне; 05 – Бутон одобряване

**ПРЕДУПРЕЖДЕНИЕ!**

В случай на загуба на връзка на локалния компютър, технолога от разстояние все още има достъп до *устройството*. **Незабавно** се свържете с технолога от разстояние и го помолете да **прекъсне връзката** ИЛИ да влезе в друг компютър и **отмени достъпа** на технолога от разстояние ИЛИ **натиснете бутона за захранване**, за да изключите e-KVM компютъра.

**ПРЕДУПРЕЖДЕНИЕ!****В случай на поддръжка на скенера:**

Преди полевият инженер да започне каквито и да било процедури (на устройството или в контролната зала), информирайте технолога от разстояние и отменете достъпа, като щракнете върху бутона "ОТМЕНИ ДОСТЪП". След това излезте от платформата nCommand Lite.

Ако няма свързан технолог от разстояние, излезте от платформата nCommand Lite, преди да започнете поддръжката.

Раздел 3.5 - Достъп с профил на технолог от разстояние

**ПРЕДУПРЕЖДЕНИЕ!**

Потребител на компютъра на устройството и главна парола: и двете трябва да се съхраняват от хоста на място, който ще получи инсталационния екип.

**ПРЕДУПРЕЖДЕНИЕ!**

Движенията на масата по време на сесията трябва да се извършват от местния технолог само по искане на системата. Преди да напусне операционната, местният технолог винаги трябва да отнема достъпа на технолога от разстояние.

**ПРЕДУПРЕЖДЕНИЕ!**

Само местният технолог има право да премести масата, за да позиционира пациента вътре в устройството и да освободи пациента безопасно. Преди да напусне операционната, местният технолог винаги трябва да отнема достъпа на отдалечения потребител.

**ПРЕДУПРЕЖДЕНИЕ!**

Винаги следете състоянието на стаята чрез видеокамерата и осигурете връзка с местен технолог, преди да пристъпите към каквито и да било действия.

**ПРЕДУПРЕЖДЕНИЕ!**

В случай на загуба на връзка на локалния компютър, незабавно се свържете с местния технолог и прекъснете връзката.

**ПРЕДУПРЕЖДЕНИЕ!****В случай на поддръжка на скенера:**

След като бъдете уведомени за началото на поддръжката на устройството, уверете се, че достъпът е прекратен от местен технолог и излезте от платформата nCommand Lite.

Ако достъпът не е отменен, излезте от платформата nCommand Lite и незабавно се свържете с местен технолог, за да го уведомите.

**ПРЕДУПРЕЖДЕНИЕ!**

За да управлявате мишката и клавиатурата дистанционно, избраният режим на достъп трябва да бъде Управление; в режим Преглед на технолога от разстояние е позволено само да гледа стрийминг и локални камери.

**ПРЕДУПРЕЖДЕНИЕ!**

Ако отговорът на вашето запитване отнема повече време от очакваното, свържете се с местен технолог чрез чат или телефон.

Работното място на технолога от разстояние включва оборудване като компютър, монитори (обикновено три), мишка, клавиатура и слушалки.

В клиничния работен процес *местните технологии* имат пряк контакт с пациента. Те са отговорни за взаимодействието с пациентите, позиционирането и осигуряването на безопасност и съответствие с протоколите по време на ЯМР, КТ или ПЕТ/КТ процедури, в съответствие с институционалните и регулаторните стандарти.

3.5.1. Режим на достъп

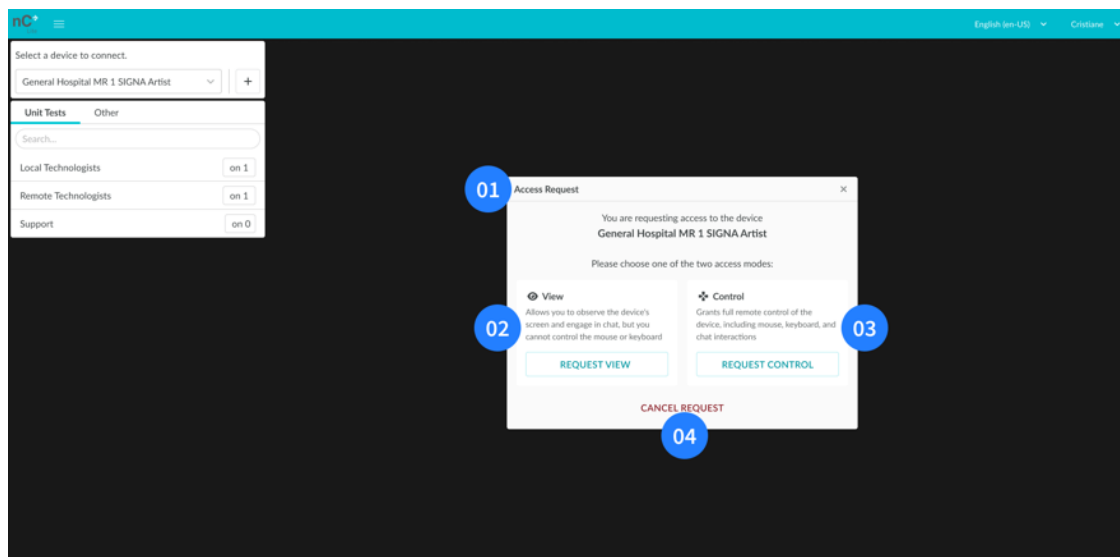
След като влезете в платформата, изберете устройството, към което искате да се свържете, в полето за избор на устройство. Ще се отвори изскачащ прозорец за избор на режим на достъп между *Управление* и *Преглед*:

- **Режим на управление** – В този режим управлението с мишката и клавиатурата е разрешено в допълнение към гледането на екрана. Местните професионалисти запазват пълен достъп до локалната мишка и клавиатура и могат да си върнат контрола по всяко време.
- **Режим на преглед** – Възможно е само да видите екрана на устройството и да използвате чата за комуникация.

При избиране на режим на достъп ще се покаже поле "Изчакване на одобрение", което показва, че е необходимо одобрение от свързания местен технолог, за да продължите. Този местен технолог има пълни правомощия да одобрява или отхвърля достъпа и да отменя достъпа по всяко време, ако сметне за необходимо. Тази мярка е от съществено значение за осигуряване на строг контрол и поддържане на безопасност при използване на устройството.

След като избере устройството, потребителят има достъп до функцията за чат, позволяваща комуникация чрез текст, аудио съобщения, гласови и видео обаждания с

другите потребители. Потребителят не е необходимо да бъде одобрен, за да има достъп до чата.



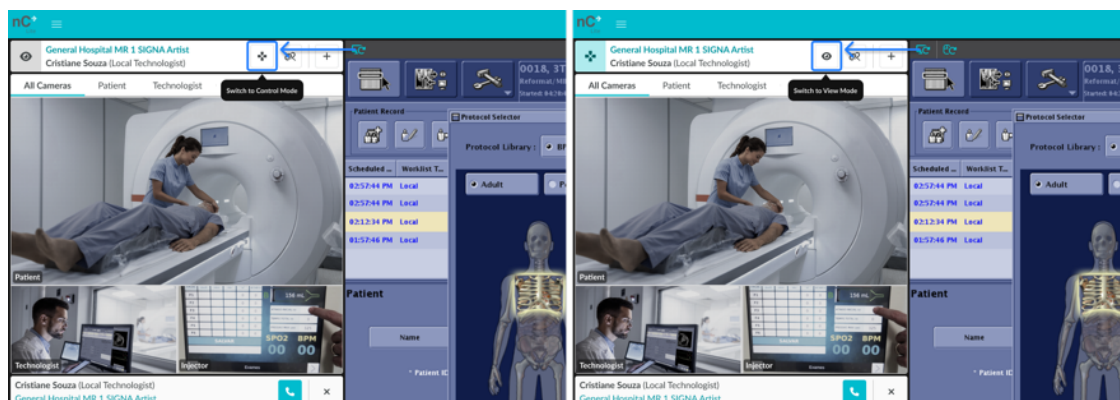
Фигура 14: Диалогов прозорец за заявка за достъп за технолог от разстояние
01 – Заглавие (заявка за достъп); 02 - Преглед на описанието на режима и бутон за заявка за преглед; 03 – Описание на режима за управление и бутон за заявка за управление; 04 – Отказ на заявката

След като достъпът до устройството бъде разрешен от местния технолог, интерфейсът на технолога от разстояние ще бъде актуализиран, за да се показва предаването на живо на устройството и свързаните с него камери. Ако избраният режим на достъп е Управление, възможността за дистанционно управление на устройството ще бъде активирана.

Този процес осигурява ефективно и сигурно взаимодействие, позволявайки безопасно дистанционно използване на устройството, без да се компрометира неговата цялост или безопасността на пациента.

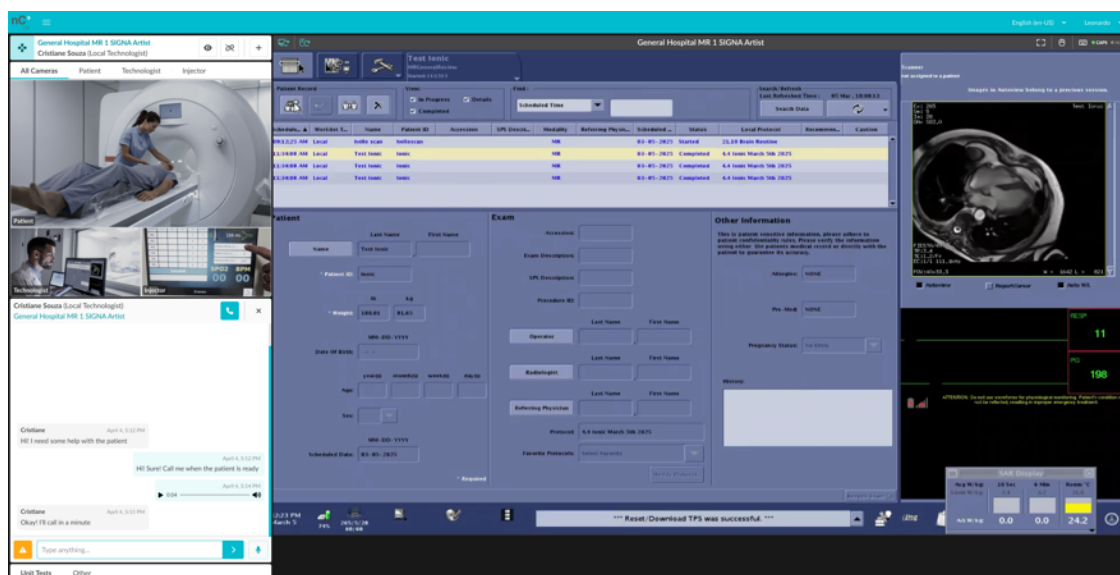
За да поискате промяна в режима на достъп по време на отдалечена сесия, щракнете върху съответната икона. Местният технолог може да приеме или отхвърли заявката:

- **Приеман** – стриймингът ще се презареди, но съдържанието на чата няма да бъде загубено. Ако сте в гласов и видео разговор, той ще приключи и ще трябва да бъде рестартиран от един от потребителите.
- **Отказ** - ще се появи изскачащ прозорец, който ви уведомява за отхвърлянето от местния технолог и текущият достъп ще остане активен



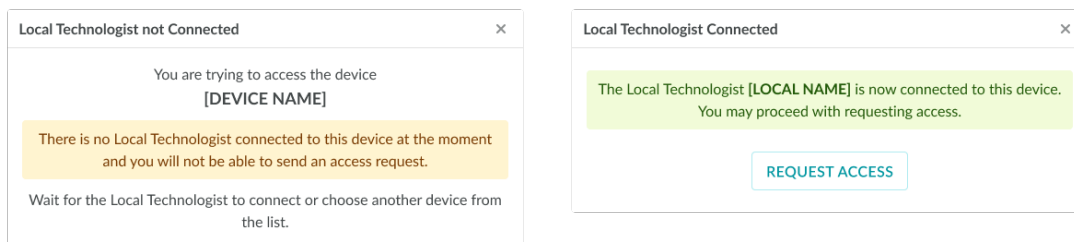
Фигура 15: Промяна на режима на достъп

Ляво - Превключване към икона и подсказка за контрол/Дясно - Превключване към икона и подсказка за режим на преглед



Фигура 16: Основен екран на Технолож от разстояние при свързване към устройство

Когато технолог от разстояние поиска достъп и няма местен технолог, свързан към устройството, платформата показва изскачащо предупреждение. Веднага след като местният технолог се свърже, платформата информира технолога от разстояние, че може да поиска достъп отново.



Фигура 17: Предупреждения от технолог от разстояние относно състоянието на връзката на местен технолог

Ляво - Известие, показващо, че е направен опит за достъп до устройството, но в момента не е свързан местен технолог.

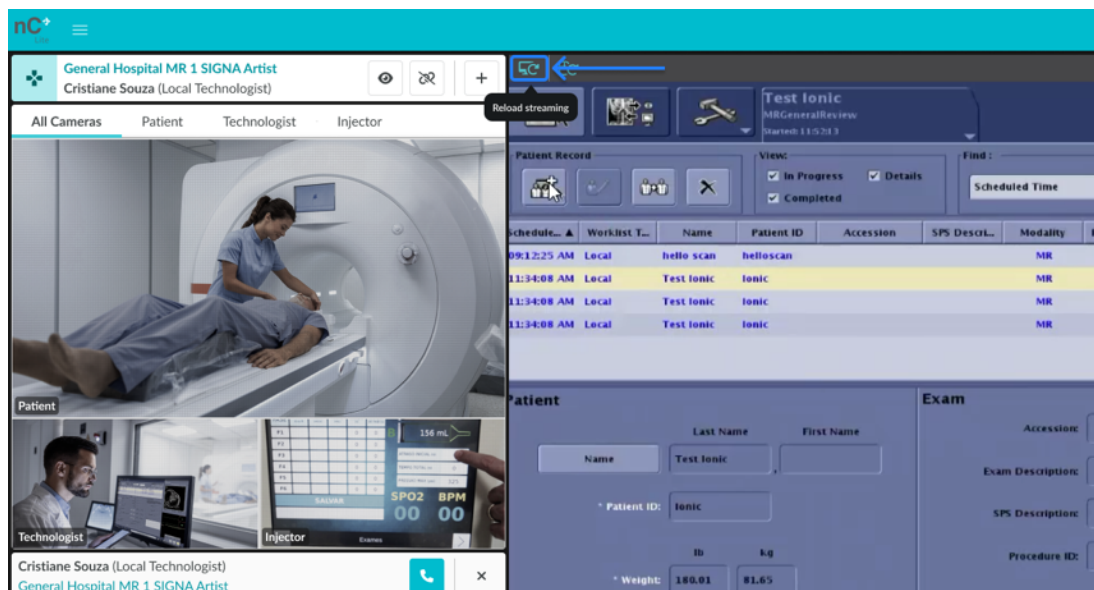
Дясно - Известие, потвърждаващо, че Местен технолог се е свързал с устройството, след като преди това не е бил свързан.

3.5.2. Лента за стрийминг

Лентата за стрийминг показва ключова информация и контроли, свързани със сесията за поточно предаване на устройството. Той включва бутоните "Презареждане на стрийминг" и "Синхронизиране с мишката", името на устройството, разделителната способност на екрана и текущото състояние на мишката и клавиатурата на отдалечения компютър.

1 - Презареждане на стрийминг

Тази функция позволява на технологите от разстояние да възстановят достъпа до устройствата при прекъсване на връзката или забавяне на производителността. Ако получите някакъв вид прекъсване на връзката или забавяне на екрана на компютъра на устройството, можете да щракнете върху иконата "Презареждане на стрийминг", разположена в лентата за стрийминг. Това ще накара платформата да се свърже отново с компютъра на устройството и също така да презареди системните камери.

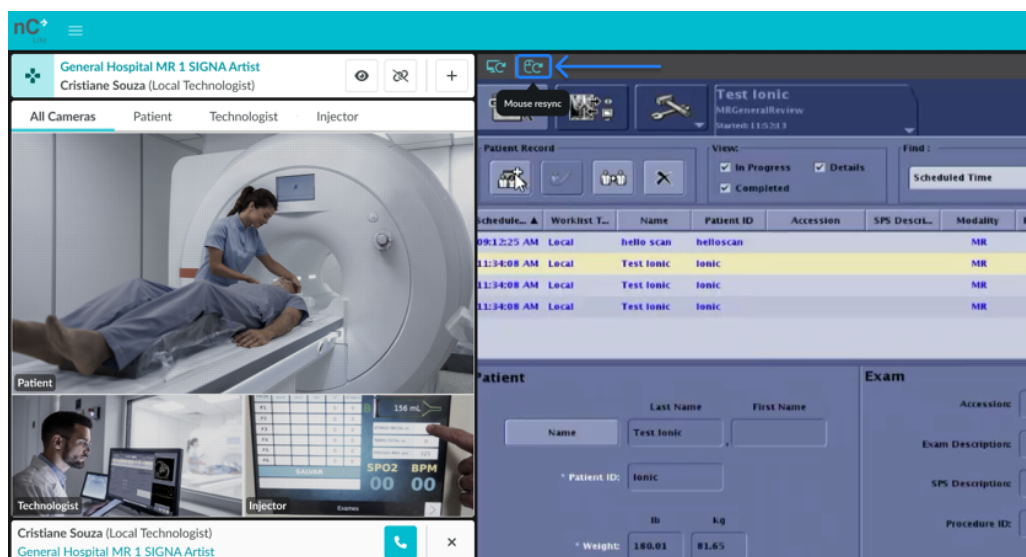


Фигура 18: Бутон за презареждане на поточно предаване

2 - Повторно синхронизиране с мишката

В случай на забавяне на мишката или несъответствие, моля, щракнете върху бутона „Синхронизиране на мишката“, разположен на лентата над прозореца за стрийминг, за да синхронизирате мишката на устройството с компютъра e-KVM.

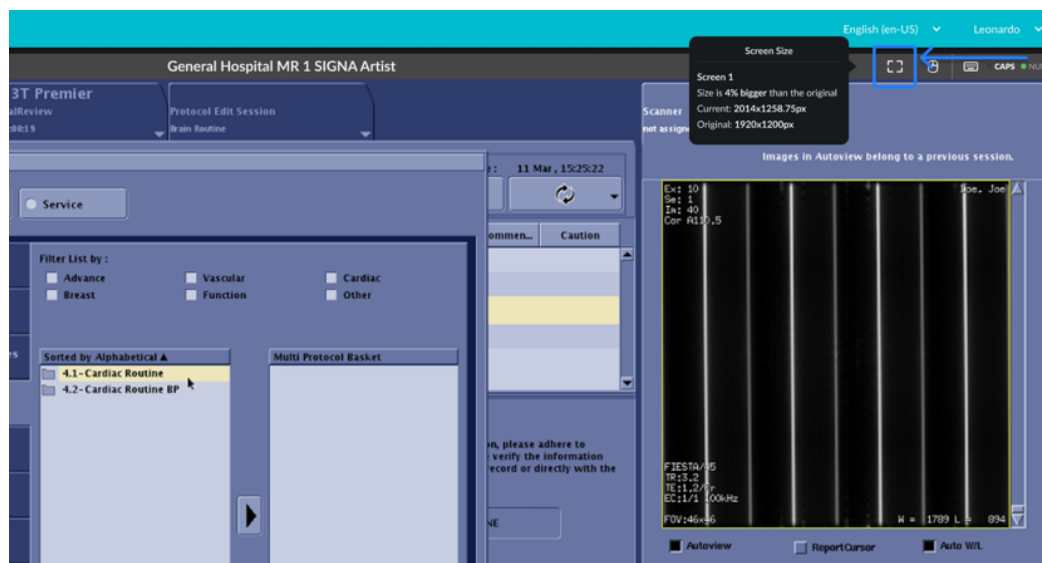
Алтернатива е да преместите показалеца на мишката извън зоната за стрийминг и след това да го върнете обратно, системата автоматично ще синхронизира мишката без нужда от допълнителни действия. Можете също да щракнете и отпуснете бутона на колелцето за превъртане на мишката (когато е наличен), за да задействате автоматично повторното синхронизиране. Въпреки това, този метод може да не работи на устройства с два или повече екрана, ако локалният и отдалеченият указател на мишката са на различни екрани.



Фигура 19: Бутон за повторно синхронизиране на мишката

3 - Стрийминг дисплей

Тази функция предоставя на технолога от разстояние информация за оригиналната разделителна способност на поточно предаване (от устройството) и текущата разделителна способност в пиксели, която се показва на отдалечената работна станция.



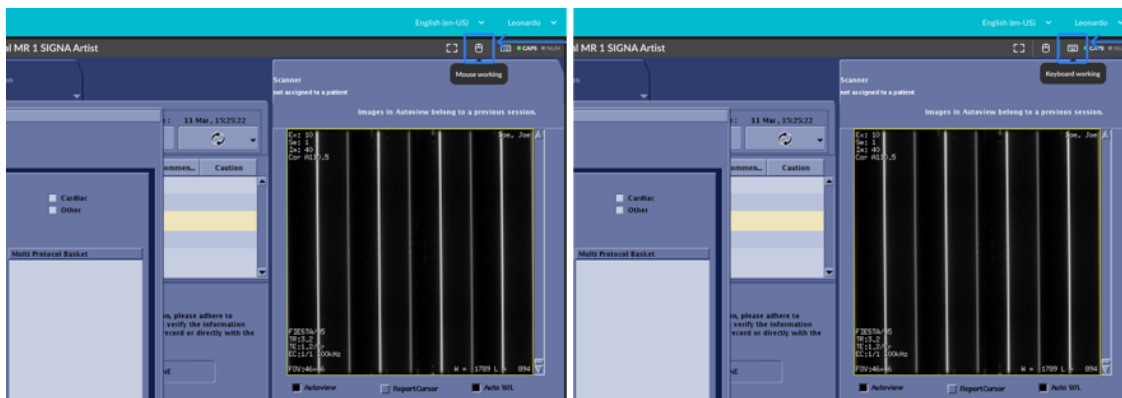
Фигура 20: Подсказка за информация за стрийминг

4 - Състояние на мишката и клавиатурата

Тази функция информира технолога от разстояние дали мишката и клавиатурата работят правилно. Заедно със състоянието на клавиатурата, потребителят може да види дали клавишите на клавиатурата **Caps lock** и **Num lock** на компютъра на устройството са включени или изключени. Тази функционалност обаче зависи от компютъра на устройството, предоставящ тази информация; в сценарии, при които тази информация не е предоставена от системата на устройството, състоянието на клавишите **Caps Lock** и **Num Lock** няма да се показва. Състоянията на мишката и клавиатурата се показват само когато потребителят има контролен тип достъп.

Когато се свързвате с устройство, несъответствие между индикаторите **Caps Lock** и **Num Lock** на отдалечения компютър и устройството може да доведе до непоследователно поведение при писане. Ако индикаторите се показват активирани на устройството, но всъщност не са активни на отдалечения компютър, потребителят може да пише с главни букви на устройството, докато текстът се появява с малки букви в чата, или обратно. По същия начин, ако **Caps Lock** е включен на отдалечения компютър, но изключен на устройството, същият проблем ще се появи обратно.

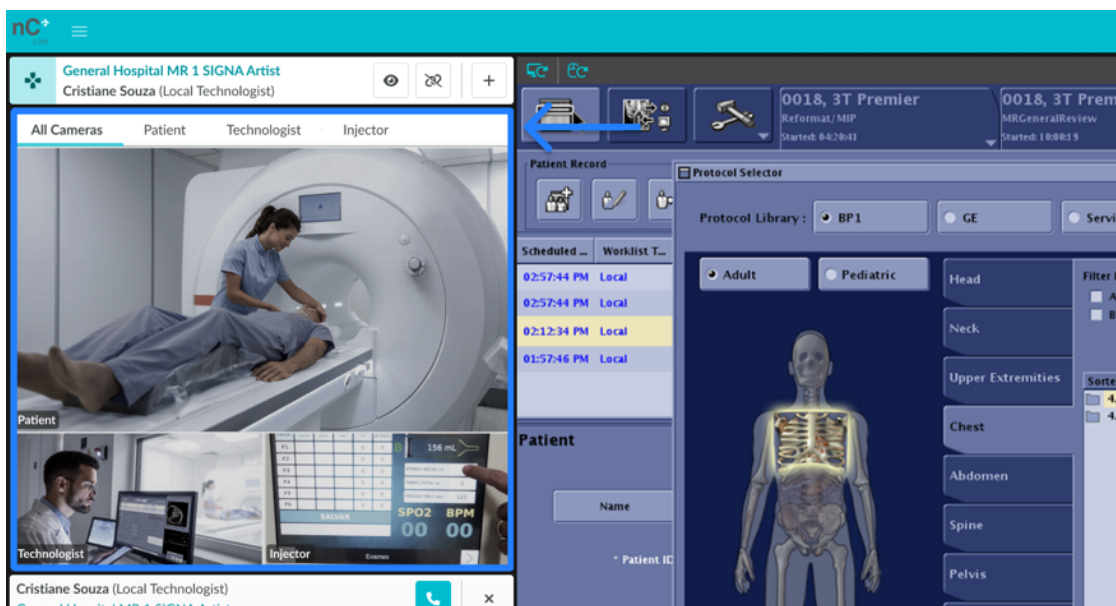
За да предотвратите този проблем, уверете се, че **Caps Lock** и **Num Lock** са или и двете активирани, или и двете деактивирани, преди да влезете в устройството. Ако възникне несъответствие, потребителят трябва да изключи връзката с устройството, да регулира състоянието на ключа на отдалечения компютър и след това да се свърже отново.



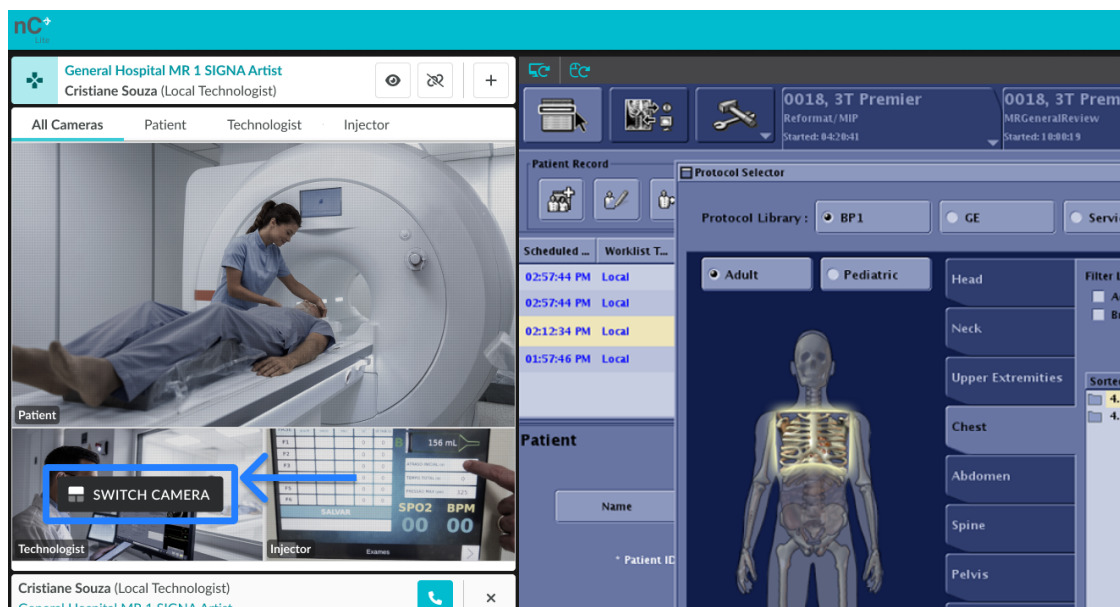
Фигура 21: Лента за поточно предаване
Ляво - Информация за състоянието на мишката
Точно - Информация за подсказката за състоянието на клавиатурата

3.5.3. Многокамерно

Тази функция позволява на технолога от разстояние да преглежда няколко камери едновременно. Ако има повече от една камера, е възможно да видите само една и да превключвате между тях, като щракнете върху менюто с определеното име за всяка камера. Като изберете "ВСИЧКИ КАМЕРИ", всички налични камери ще бъдат показани в рамката, като една от тях ще бъде маркирана. За да превключите маркираната камера, просто задръжте курсора на мишката върху една от камерите в по-малкия кадър и щракнете върху "ПРЕВКЛЮЧВАНЕ КАМЕРА".



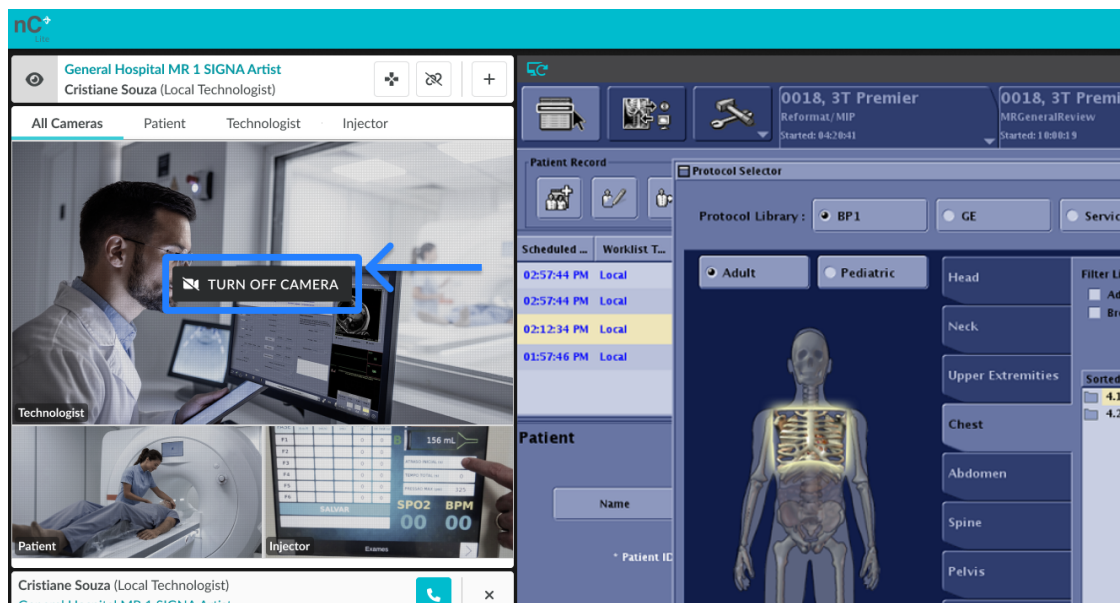
Фигура 22: Многокамерен кадърен поглед



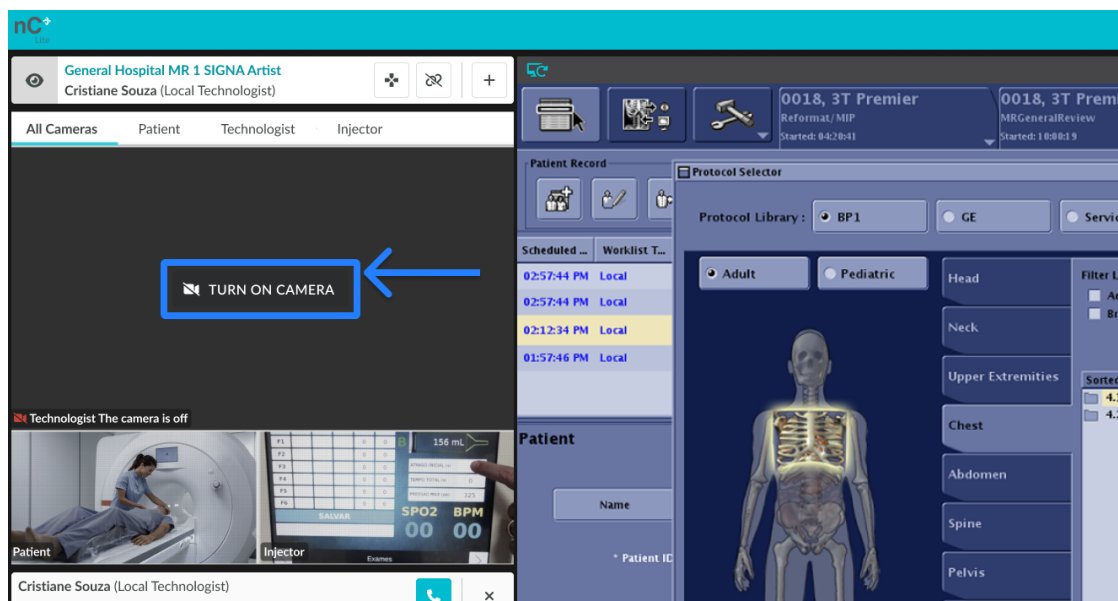
Фигура 23: Бутон „ПРЕВКЛЮЧВАНЕ НА КАМЕРАТА“ за много камери при задържане на курсора на мишката

По време на активна отдалечена сесия, ако технолог от разстояние има достъп като **Преглед**, има опция да изключи една или повече камери, като задържи курсора на мишката върху избраната камера и щракне върху "ИЗКЛЮЧВАНЕ НА КАМЕРАТА." За да видите камерата отново, просто повторете процеса и щракнете върху "ВКЛЮЧВАНЕ НА КАМЕРАТА".

БЕЛЕЖКА: Опцията за изключване на камерите е налична само в режим на преглед; в режим на управление не е възможно да изключите камерите.



Фигура 24: Бутон „ИЗКЛЮЧВАНЕ НА КАМЕРАТА“ за много камери с задържане на курсора в режим на преглед



Фигура 25: Бутон „ВКЛЮЧВАНЕ НА КАМЕРАТА“ за много камери с задържане на курсора в режим на преглед

3.5.4. Отваряне на друго устройство

Позволява на технолога от разстояние да отвори нов раздел на браузъра на nCommand Lite, като по този начин позволява на потребителя да избере ново устройство за извършване на повече от едно дистанционно сканиране едновременно. За да отворите ново устройство за достъп, просто щракнете върху бутона "Отваряне на друго устройство" и е предоставено предупреждение, за да можете безопасно да извършите тази едновременна операция. Трябва да прочетете предупреждението, преди да отворите този нов прозорец.

БЕЛЕЖКА: За оптимален преглед при едновременен достъп се препоръчва, след като щракнете върху „ОТВАРЯНЕ НА ДРУГО УСТРОЙСТВО“ и потвърдите с „ОК“ предупрежденията, да преместите новия раздел на друг наличен монитор.

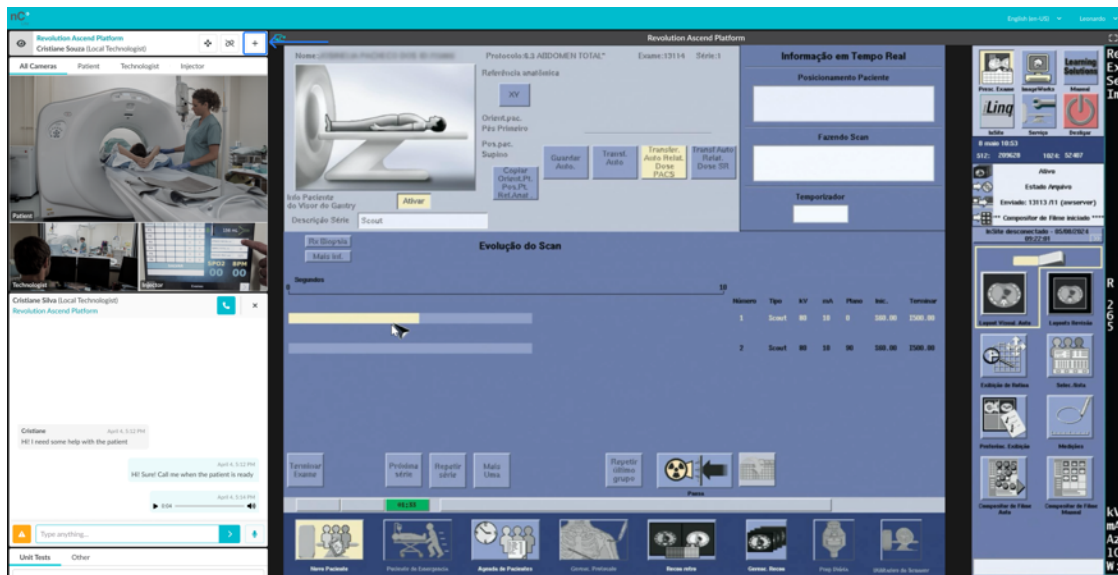


ПРЕДУПРЕЖДЕНИЕ!

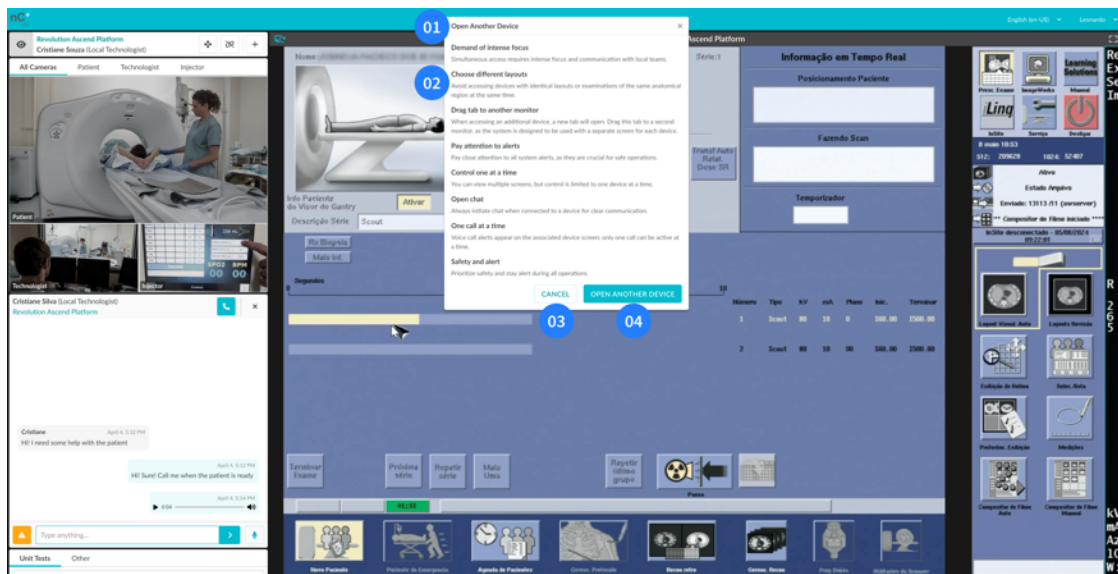
Предупреждение за безопасност при достъп с множество скенери

- **Изискване за интензивен фокус:** Едновременният достъп изисква интензивен фокус и комуникация с местните екипи.
- **Изберете различни оформления:** Избягвайте достъпа до устройства с идентично оформление или изследвания на една и съща анатомична област едновременно.
- **Плъзгане на раздела към друг монитор:** При достъп до допълнително устройство ще се отвори нов раздел. Плъзнете този раздел към втори монитор, тъй като системата е проектирана да се използва с отделен екран за всяко устройство.
- **Обърнете внимание на сигналите:** Обърнете голямо внимание на всички системни сигнали, тъй като те са от решаващо значение за безопасната работа.

- **Контролирайте един по един:** Можете да преглеждате няколко екрана, но управлението е ограничено до едно устройство в даден момент.
- **Отвори чат:** Винаги инициирайте чат, когато сте свързани с устройство за ясна комуникация.
- **Едно по едно обаждания:** Сигналите за гласови повиквания се появяват на екрана на свързаното устройство; само едно обаждане може да бъде активно в даден момент.
- **Безопасност и предупреждение:** Дайте приоритет на безопасността и бъдете нащрек по време на всички операции.



Фигура 26: Бутон за отваряне на друго устройство (+)



Фигура 27: Предупреждения за достъп до множество устройства

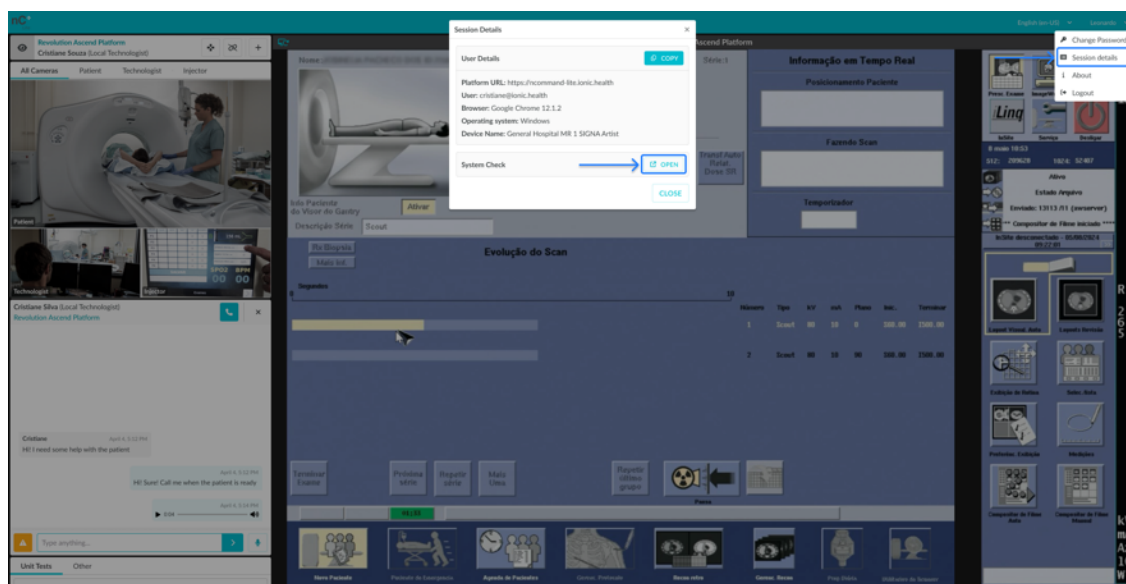
- 01 – Заглавие (Отваряне на друго устройство); 02 – Предупреждения за експлоатационна безопасност;
03 – Бутон за отказ; 04 – Бутон за отваряне на друго устройство

3.5.5. Проверка на системата

Функцията Проверка на системата помага да се провери дали текущото устройство, мрежата и интернет връзката отговарят на изискванията за правилно използване на nCommand Lite. Той извършва бърз автоматичен тест, който проверява основни елементи като качество на интернет връзката, достъп до необходимите сървъри и стабилност на връзката. Този инструмент може да се използва преди започване на сесия, по време на инсталация или при подозрение за проблем с връзката. Това помага да се гарантира, че платформата ще работи както се очаква, и подпомага техническия екип, ако е необходимо отстраняване на проблеми.

Забележка: Системната проверка е за предпочитане да се използва с поддръжката или по заявка на ИТ специалист. Използването на този инструмент без технически насоки може да доведе до погрешно тълкуване на резултатите.

За да получат достъп до Проверка на системата, локалните и отдалечените технолози трябва да отворят опцията Подробности за сесията от падащото меню, достъпно под потребителското им име, разположено в горния десен ъгъл на главния екран. След това щракнете на **Отвори** до инструмента *Проверка на системата*. След като страницата на инструмента се покаже, щракнете **Стартиране на тест**, за да започнете процеса на верификация.



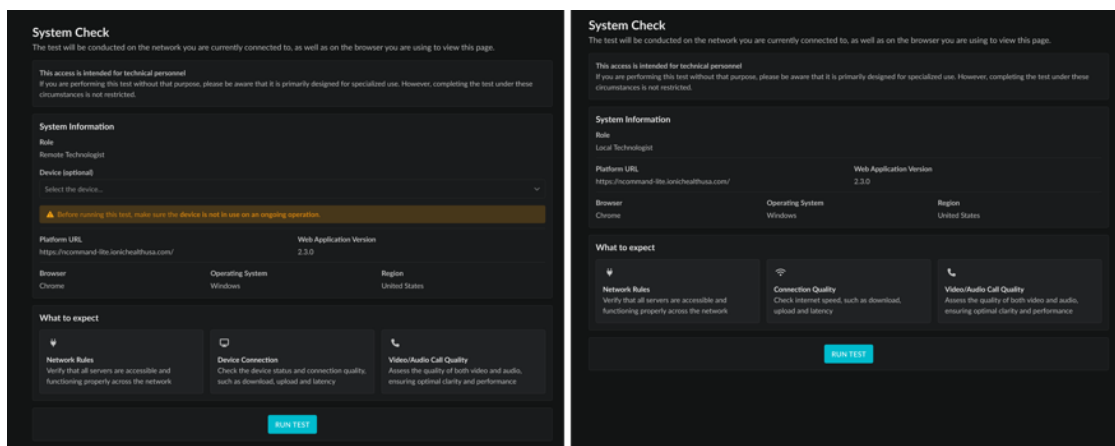
Фигура 28: Достъп до Проверка на системата

Когато използвате технолог от разстояние, е възможно да изберете устройство от основния екран на инструмента, така че то да бъде включено в резултатите от теста.



ПРЕДУПРЕЖДЕНИЕ!

Преди да започнете теста, уверете се, че избраното устройство в момента не се използва.



Фигура 29: Проверка на основния екран за Проверка на системата
Ляво – Технолог от разстояние/Дясно – Местен технолог

След приключване на теста, на екрана се показва обобщение на резултатите. ИТ специалистите могат да прегледат тази информация, за да идентифицират възможни проблеми, влияещи на работата на системата.

Раздел 3.6 - Чат

Платформата предоставя чат и разговори в реално време с гласови и видео функции, които се използват за ефективна комуникация между лицензирани технолози. Чрез тези функции лицензираните технолози могат да взаимодействат по всички въпроси, свързани с работния процес на сесията.



ПРЕДУПРЕЖДЕНИЕ!

В случай на повреда се обадете на местния технолог по телефона.

След като се свържете с устройство, ще имате незабавен достъп до списъка с потребители в чата, организиран в два раздела. За клиенти с няколко обекта всеки клон може да бъде конфигуриран като отделен договор. Когато е активирано, потребителите се групират по договор, като потребителите от други договори се показват в раздела "Други".

За да започнете разговор, щракнете двукратно върху името на потребител, за да отворите интерфейса за чат, който поддържа както текстови съобщения, така и гласови повиквания. Уверете се, че избраната сесия съответства на правилното устройство. Платформата уведомява потребителите, ако мрежовата връзка стане бавна или нестабилна.



ПРЕДУПРЕЖДЕНИЕ!

Преди да започнете контакт, проверете името на устройството, показано под името на потребителя, тъй като някои технолози от разстояние може да са свързани към множество устройства.

Ето наличните инструменти за комуникация в рамките на платформата:

Уведомление за поверителност: Този документ е предназначен само за използване от местните технолози и технолозите от разстояние

1. **Гласови и видео разговори:** Щракнете върху иконата, за да започнете гласов и видео разговор с продължителност до 60 минути между технолог от разстояние и местен технолог. Връзките между потребители с един и същ профил (локално–локално или отдалечено–отдалечено) не се поддържат.

Когато местен технолог инициира обаждане, технолог от разстояние може да избере да приеме или да откаже. От друга страна, когато технолог от разстояние инициира разговора, той автоматично се свързва и се уведомява местен технолог. Използвайте тези функции като механизъм за безопасност, за да се гарантира, че технолог от разстояние винаги може да комуникира с всеки, който физически присъства на мястото, сякаш е там лично.

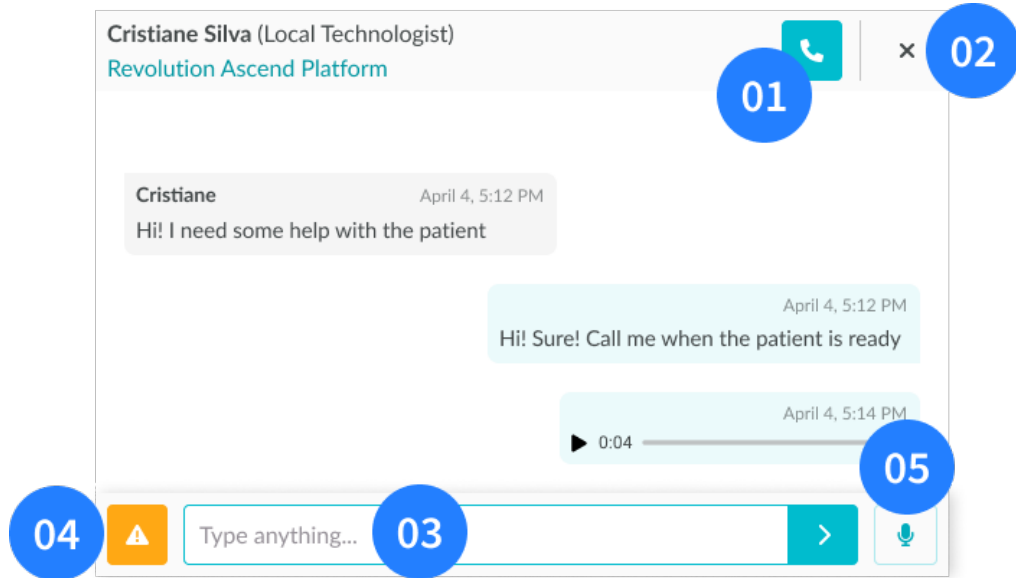
По подразбиране микрофонът е активен в началото на разговора, докато камерата остава изключена. Всеки технолог може ръчно да включи или изключи своя микрофон и камера по всяко време.

За да установят успешно разговор, и двамата потребители трябва да имат функциониращ микрофон и аудио изход, с правилно активирани разрешения на брауъра. Ако някой от тези компоненти липсва, системата ще уведоми и двамата потребители и разговорът няма да бъде завършен. Камерата не е задължителна – ако не е налична или не е открита, системата ще актуализира иконата, за да отрази, че видеото не се поддържа.

Разрешено е само едно активно обаждане на потребител. Ако технолог се опита да започне ново повикване, докато вече е в такова, системата ще блокира опита и ще покаже известие. По същия начин, ако потребителят вече е в разговор и получи друго входящо повикване, обажданият ще бъде информиран, че получателят в момента не е на разположение, а потребителят в текущия разговор ще получи известие, че някой е опитал да се свърже с него.

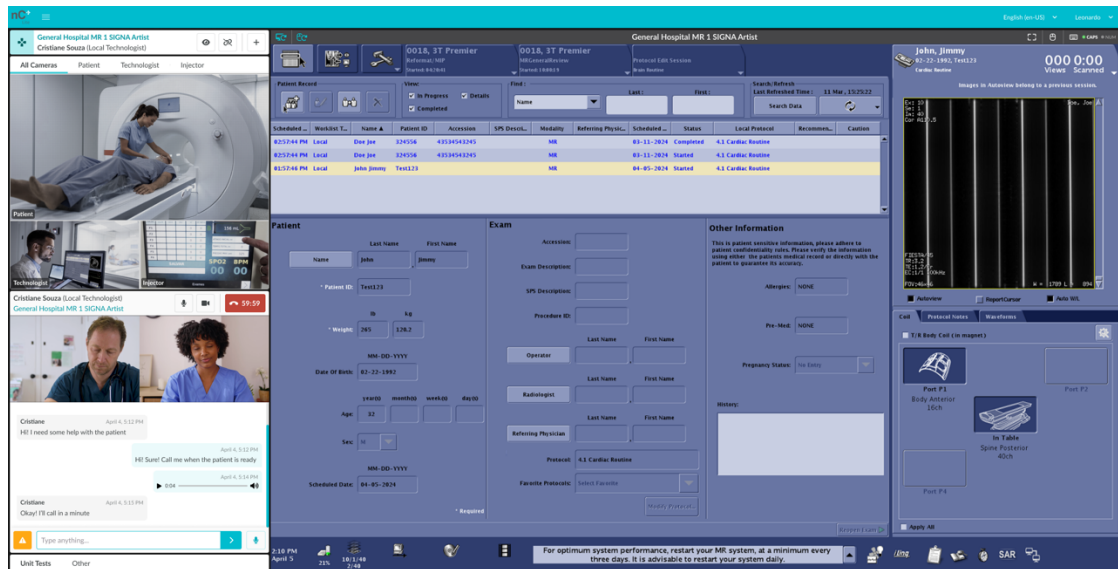
2. **Затваряне на чатове:** Когато един от потребителите затвори чата, като щракне върху бутона за затваряне, до другия потребител се изпраща автоматично съобщение и разделът за чат се затваря. Това гарантира, че и двете страни са информирани, че разговорът е приключил. Когато прозорецът за чат е затворен, всички съобщения изчезват. Ако го отворите отново по време на сесията, разговорът се рестартира без предишни съобщения.
3. **Текстови съобщения:** Изпращайте текстови съобщения в определеното поле. Когато се изпрати съобщение, се появява икона със сива отметка, а когато съобщението бъде получено от получател, се показва друга икона с две сини отметки. Това позволява безопасна, ясна и кратка писмена комуникация между двете страни.
4. **Призив за внимание:** Привлечете вниманието на другия потребител, като щракнете върху бутона с удивителен знак. Това действие прилага ефект на визуална вибрация към прозореца на другия потребител за няколко секунди и автоматично се изпраща съобщение, сигнализиращо за спешност или важност.

- Аудио съобщения:** Изпращайте аудио съобщения, като щракнете върху бутона за микрофон. Това се използва, когато искате да предадете съобщение по-лично или когато писането не е удобно.

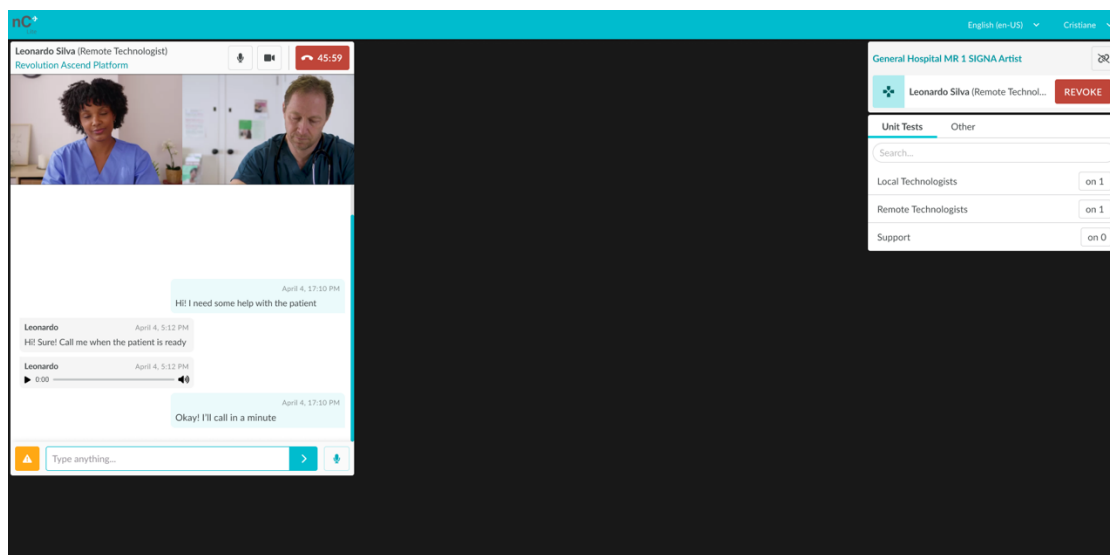


Фигура 30: Изглед на чат прозореца

- 01** – Бутон за гласово и видео повикване; **02** - Бутон за затваряне на чата; **03** – Текстово поле за съобщение;
04 – Бутон за призоваване на внимание; **05** – Запис Бутон за аудио съобщение



Фигура 31: Основен екран на технолог от разстояние – Прозорец за чат (долен ляв ъгъл)



Фигура 32: Основен екран на местен технолог – прозорец за чат

Проблеми с интернет връзката - Когато някой от технологите изпита проблеми с мрежовата връзка, системата ще покаже съобщение и ще се опита да се свърже отново. Ако връзката бъде възстановена, системата ще покаже съобщение **ONLINE** и отдалечената сесия ще продължи както обикновено. Въпреки това, след няколко опита за повторно свързване, ако връзката не бъде възстановена, системата ще прекрати активната сесия и ще уведоми технолога, че е прекъснат поради проблеми с интернет. В същото време системата ще уведоми и другия технолог, че неговият колега е бил прекъснат поради проблеми с интернет връзката.

Раздел 3.7 - Приключване на вашата сесия в платформата

В края на задълженията си лицензираният технолог трябва да изключи връзката с устройството и да излезе от платформата.

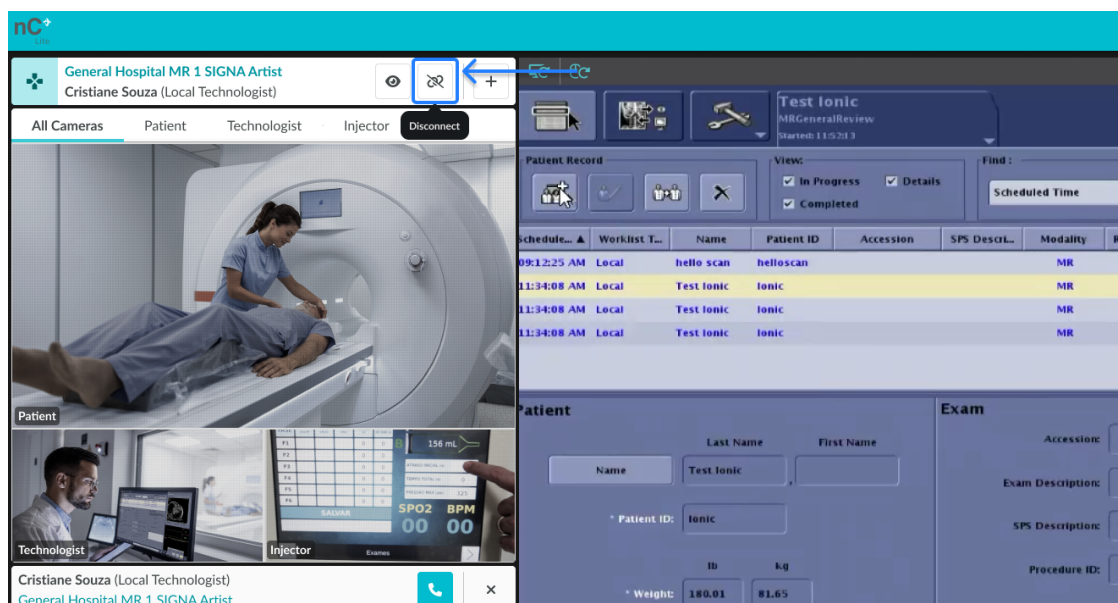


ПРЕДУПРЕЖДЕНИЕ!

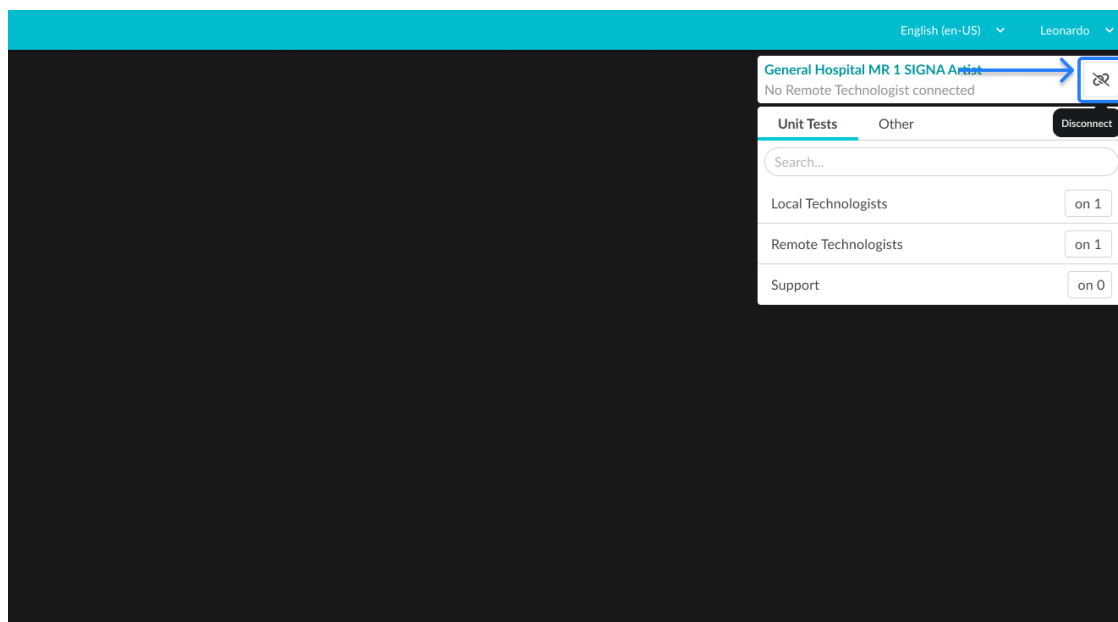
Лицензираните технологи не трябва да забравят да излязат от платформата, преди да приключат задълженията си.

За да прекъснете връзката с устройството, трябва да кликнете върху иконата за прекъсване на връзката, разположена в полето за устройство. Бележка: Ако работите като местен технолог, уверете се, че сте прекратили достъпа на всички технологии от разстояние, преди да прекъснете връзката с устройството.

За да гарантирате безопасността, ще получите известие, за да потвърдите, че искате да прекъснете връзката с устройството. След потвърждение ще бъдете пренасочени към началния екран, без да е избрано устройство.



Фигура 33: Бутон за прекъсване на връзката – основен екран на технолог от разстояние



Фигура 34: Бутон за прекъсване на връзката – основен екран на местен технолог

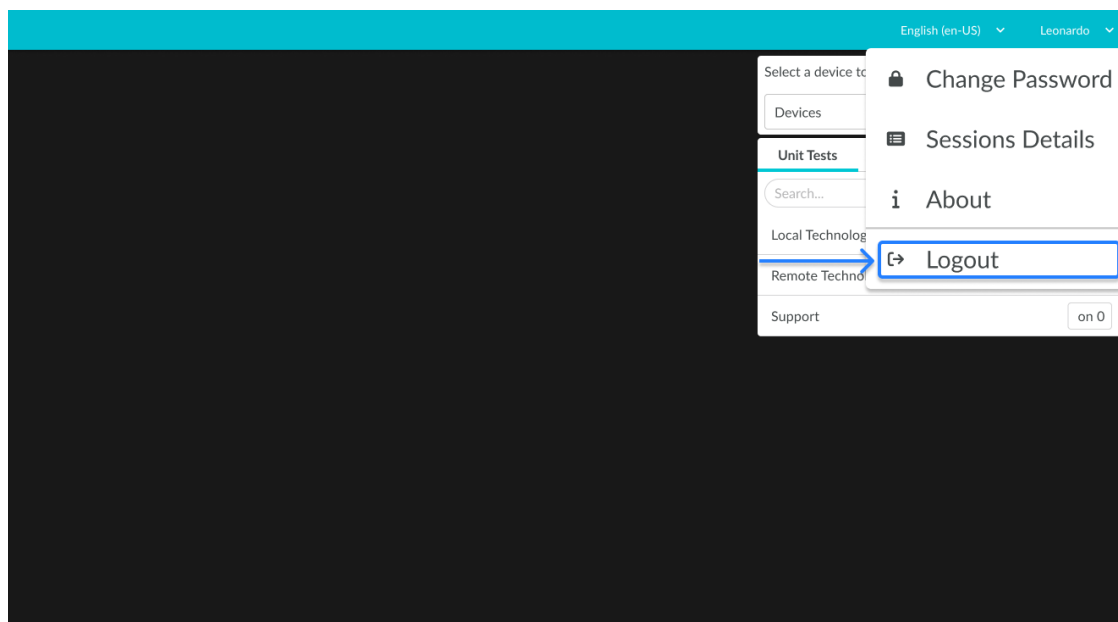


ПРЕДУПРЕЖДЕНИЕ!

Преди да излезете, уверете се, че всички допълнителни раздели, които са отворени, са затворени.

За да прекратите сесията си в платформата, щракнете върху потребителското си име, разположено в горния десен ъгъл на екрана, и изберете опцията „Излизане“. Ще получите известие, за да потвърдите, че желаете да напуснете медицинския център, в който сте работили. След потвърждение ще бъдете пренасочени към страницата за вход в приложението, като по този начин безопасно ще приключите работното си пътуване.

nCommand Lite не контролира сесията на потребителя на външния IdP и следователно не може да извърши излизане на ниво IdP. В сценарии, в които потребителите споделят една и съща машина и използват еднократно влизане (SSO), се препоръчва всеки потребител да избере опцията „не оставай влизан“ по време на вход във външен IdP (ако е налично) или да излезе от IdP след като излезе от nCommand Lite. Това гарантира, че никой следващ потребител на същото устройство не може неволно да използва повторно активна сесия.



Фигура 35: Елемент от падащото меню за излизане



ПРЕДУПРЕЖДЕНИЕ!

Когато използвате външен доставчик на самоличност на споделен или публичен компютър, след като излезете от платформата, излезте и от доставчика на самоличност. За повече информация как да продължите, се свържете с екипа за ИТ поддръжка на вашата организация.

Раздел 3.8 - Оперативно обучение

Участието в програмата за обучение е задължително за всички потребители на системата nCommand Lite. Регистрацията на потребителите в платформата се управлява от екипа на IONIC Health и се инициира само след потвърждение, че потребителят успешно е завършил необходимото LMS обучение и е подходящо квалифициран да работи с платформата. Този процес гарантира, че всички потребители притежават задълбочено разбиране за функционалностите на системата и са готови да използват платформата ефективно и безопасно. За да започнете процеса на записване за обучение, моля, свържете се с вашия търговски представител.

Раздел 3.9 - Указания за отстраняване на неизправности

ПОТРЕБИТЕЛ И ПАРОЛА	
Промяна на паролата	Уверете се, че изискванията за парола са изпълнени, паролата трябва да е силна и сигурна, включително поне една малка буква, една главна буква, един специален знак и да е дълга най-малко 8 знака.
Забравена парола	Проверете входящата си поща: Уверете се, че използвате правилния имейл адрес и че имейлът за възстановяване на парола не е филтриран във вашата папка за спам или нежелана поща. Опитайте отново: Изчакайте няколко минути и поискайте друг имейл за възстановяване на паролата, като щракнете върху "Забравихте ли паролата си?". Проверете интернет връзката: Уверете се, че сте свързани с интернет.
Имейлът за добре дошли не е получен	Проверете дали имейлът е в папката „Спам“. Ако го няма, свържете се с администраторски потребител, за да се уверите, че имейлът, предоставен във вашата регистрация, е правилен. Ако не е правилно, администраторът трябва да го актуализира и да изпрати отново имейла за добре дошли.
Код за двуфакторно удостоверяване не е получен	Щракнете върху "Повторно изпращане на кода" и проверете папката си за спам. Ако не го получите, моля, свържете се с администраторски потребител, за да проверите дали имейлът, регистриран в контрола на достъпа, е правилен.
Превишени опити за влизане	Ако надвишите допустимия брой опити за влизане, трябва да изчакате определен период, преди да опитате отново.
ВЪНШЕН ДОСТАВЧИК НА ИДЕНТИФИКАЦИЯ	
Проблеми с влизането в продукта	Ако срещнете проблеми с влизането, докато използвате външен доставчик

	на самоличност (IdP), моля, имайте предвид, че процесът на удостоверяване се управлява изцяло от IdP, а не от доставчика на продукта, т.е.: Ionic Health. Поради това продуктът не може да помогне с идентификационни данни за акаунт, правила за достъп, грешки при удостоверяване или заключване на акаунта. В тези случаи трябва да се свържете с екипа за ИТ поддръжка на вашата организация, който може да прегледа конфигурацията на IdP и да помогне за разрешаването на проблема.
Проблеми с идентификационните данни	Всички проблеми, свързани с идентификационните данни (<i>напр.</i> , забравена парола, промяна на парола), трябва да бъдат разрешени директно с екипа за ИТ поддръжка на вашата организация. Те могат да прегледат конфигурацията на IdP и да предоставят необходимата помощ.
Проблеми с многофакторния удостоверител (MFA)	Всички проблеми, свързани с многофакторния удостоверител (MFA) (<i>напр.</i> , проблеми с изтичане на MFA, MFA не работи, влизане без искане на MFA), трябва да бъдат разрешени директно с екипа за ИТ поддръжка на вашата организация. Те могат да прегледат конфигурацията на IdP и да предоставят необходимата помощ.
Идентификационните данни не работят на платформата	Когато използвате външни доставчици на самоличност (IdP), влизайте в продукта само с помощта на IdP. Използването на идентификационните данни за IdP директно на страницата за вход в продукта ще доведе до неуспешно влизане.
МОНИТОР НА СКЕНЕРА	
Не се включва	Проверете връзките на монитора към компютъра и електрическия контакт. Може да възникнат прекъсвания на връзката. Натиснете отново бутона за захранване на монитора.
ПЛАТФОРМА	

Недостъпни	Проверете мрежовата връзка. Проверете дали платформата е стартирана и дали влизането е извършено.
Латентност на платформата	Обновете страницата, като натиснете Ctrl+F5. Проверете дали чатът на устройството (на медицинското заведение) е отворен в повече от един раздел. Ако е така, затворете раздела, който не се използва. Ако проблемът продължава, опитайте да излезете от платформата, да изчистите кеша, да затворите браузъра и след това да влезете отново.
Неизправни функции	Преди да опитате други процедури за отстраняване на неизправности, изчистете кеша на браузъра (потърсете инструкции в текущия си браузър) след влизане, след това затворете и отворете отново браузъра, влезте отново в платформата и опитайте действието отново.
Надстройка	След като платформата бъде надстроена, изчистете кеша на браузъра си (вижте инструкциите за вашия браузър), преди да влезете в новата версия.
АУДИО	
Няма звук	Уверете се, че силата на звука на микрофона и високоговорителите на устройството (на медицинското заведение) са настроени на подходящи нива. Проверете дали браузърът има разрешение за използване на аудио и микрофон. Проверете дали слушалките са свързани и функционират правилно.
Забавяне на звука	Проверете електрическите и мрежовите връзки на оборудването. Опреснете страницата на браузъра,

	като натиснете Ctrl+F5 и влезте отново. Ако проблемът продължава, опитайте да излезете от платформата, да изчистите кеша, да затворите браузъра и след това да влезете отново.
ЧАТ	
Чатът не се появява	Уверете се, че браузърът не е минимизиран. В противен случай отворете чата, след като влезете в платформата nCommand Lite. Проверете дали устройството (медицинското заведение) е избрано и потребителят е упълномощен да активира комуникация в чата. Уверете се, че разрешенията за аудио и микрофон на браузъра ви са приети. Проверете кабелните връзки, които може да са изключени. Обновете страницата на браузъра, като натиснете Ctrl+F5 и се свържете отново с платформата. Проверете дали чатът на сайта е отворен в повече от един раздел. Ако е така, затворете раздела, който не се използва.
Забавяне на чата	Обновете страницата на браузъра, като натиснете Ctrl+F5 и се свържете отново с платформата. Ако проблемът продължава, опитайте да излезете от платформата, да изчистите кеша, да затворите браузъра и след това да влезете отново. Проверете кабелните връзки, които може да са изключени.
Проблеми с изпращането на аудио съобщения	Проверете разрешенията на браузъра за аудио и микрофон и се уверете, че

	микрофонът и аудио устройствата са свързани към компютъра. Ако разрешенията на браузъра трябва да бъдат коригирани, натиснете Ctrl+F5, за да подканите браузъра да разпознае промените при презареждане на страницата.
Гласовото повикване не успя да се инициира	Проверете интернет връзката си и вижте дали е показано известие, обясняващо причината за нестартиране на повикването. Уверете се, че имате свързано аудиоустройство и че разрешенията за аудио и микрофон са разрешени в браузъра. Ако проблемът продължава, обновете страницата с Ctrl+F5, за да опитате отново.
Потребителят не е намерен в чата	Ако не можете да намерите потребител в чата, щракнете върху раздела „Други“, за да се уверите, че не е в списъка там. Потребителите, свързани с други договори, се показват отделно в списъка с контакти. Ако вашият потребител не се появи в списъка с контакти, след като изберете устройството, натиснете Ctrl+F5, за да опресните екрана и изберете отново. Уверете се, че имате интернет връзка.
ЗАЯВКА ЗА ДОСТЪП ДО УСТРОЙСТВОТО	
Платформата не разпозна, че местният технолог е свързан	Проверете под опцията „Други“, за да потвърдите дали локалният потребител е свързан. Ако потребителят наистина е свързан, но все още получавате съобщение, че локалният потребител не е свързан към скенера, обновете екрана, като натиснете Ctrl+F5, и помолете локалният потребител да повтори същата инструкция. След това изберете устройството отново и помолете местния потребител също да избере устройството отново. Ако проблемът продължава, свържете се с поддръжката, за да проверите мрежата.

Заявката за достъп не се изпраща	Обновете страницата, като натиснете Ctrl+F5 и потвърдете с локалния потребител чрез чат дали е получена заявката за достъп. Ако проблемът продължава, моля, свържете се с поддръжката за допълнителна помощ.
УСТРОЙСТВО ЗА СТРИЙМИНГ (е-KVM КОМПЮТЪР)	
Устройството за стрийминг (е-KVM КОМПЮТЪР) не работи	Щракнете върху бутона "Презареждане на стрийминга" на платформата. Уверете се, че непрекъсваемото и стабилизирано захранване (медицинско заведение) и/или устройството за поточно предаване са правилно свързани и включени. Изключете устройството за стрийминг и цялото друго оборудване и го включете отново. Освежете платформата.
Стрийминг на устройството бавно	Щракнете върху бутона "Презареждане на стрийминга" на платформата. Обновете страницата с Ctrl+F5 и се свържете отново с платформата. Проверете качеството на вашата мрежова връзка. За да се потвърди състоянието на мрежата, е възможно да се проведе пинг тест на устройството, за да се провери за загуба на пакети. След проблеми с интернет платформата може да не работи по предназначение. Обновете уеб страницата и поискайте достъп до локалния потребител отново.
Загуба на видео изход	Допустимо е електростатичният разряд да причини загуба на изображение. След рестартиране на системата, комуникацията и видео стриймингът трябва автоматично да бъдат възстановени.

Раздел 3.10 - Методи за почистване на хардуера

- Преди да започнете процеса на почистване, уверете се, че цялото оборудване е изключено от електрическия контакт.
- Не използвайте абразивни продукти.
- Не потапяйте оборудване или периферни устройства в какъвто и да е вид течност.
- Изхвърлете почистващите материали в съответствие с разпоредбите за изхвърляне на опасни отпадъци.
- Не е препоръчително да използвате спрей-дезинфектант, тъй като парите могат да влязат в оборудването и да причинят късо съединение или корозия.
- Този продукт е нестерилен

Глава 4 Киберсигурност и поверителност

Раздел 4.1 - Рискове за сигурността и поверителността

Системата **nCommand Lite** прилага множество технически и организационни мерки за защита на обработената информация.

Системата е сертифицирана по ISO/IEC 27001 и ISO/IEC 27701 и следва подход за поверителност още при проектиране. Поддържа спазването на законите за защита на данните в здравеопазването и разпоредбите за киберсигурност, приложими в ЕС, САЩ, Обединеното кралство, Швейцария, Бразилия, ОАЕ, Саудитска Арабия, Австралия и Нова Зеландия.

Потребителите обаче трябва да възприемат най-добрите практики, за да предотвратят ненужното излагане на чувствителни данни.

- Избягвайте споделянето на лична или чувствителна информация, освен ако не е строго необходимо.
- Уверете се, че комуникациите и системният достъп се осъществяват в защитени среди.
- Ако подозирате каквато и да е злонамерена дейност, незабавно уведомете отговорния екип.

Раздел 4.2 - Защита на личните данни (съответствие с GDPR/HIPAA)

Системата **nCommand Lite** отговаря на всички приложими закони и регулации за поверителност и защита на данните в регионите, в които оперира, включително, но не само, изискванията на GDPR, HIPAA, LGPD и ISO/IEC 27701. Всички дейности по обработка на данни се извършват под ролите „Обработващ“ и „Подобработващ“, както са определени от GDPR, със строга регионална сегрегация на данните, за да се гарантира съответствие и да се предотвратят неоторизирани трансгранични трансфери на данни

Какви данни се събират?

- **Потребители:** Име, имейл и фирма (строго за удостоверяване и управление на достъпа).
- **Данни за пациента:** Само предаване на медицински преглед чрез стрийминг в реално време, без съхранение на данни

Как се използват и защитават данните?

- Данните се използват изключително за **удостоверяване, контрол на достъпа и проследимост на сесиите**.
- Предаването на информация е защитено чрез **AES-256 криптиране за съхранение и TLS 1.3 за данни в пренос**.
- **Достъпът е ограничен** и следва **принципа на най-малката привилегия (RBAC)**.

- Осигурено криптиране от край до край за P2P видео и контролни потоци чрез WebRTC.
- Оторизирани доставчици на облачни услуги (напр. Microsoft Azure) обработват ограничени данни при строги договорни гаранции.

Потребителите получават следните права:

- **Достъп и коригиране** на лична информация.
- **Искане за изтриване на данни**, където е приложимо.

Ако имате някакви въпроси, изпратете имейл на privacy@ionic.health, за да се свържете с DPO на Ionic Health. Всички заявки се обработват в рамките на 30 дни, с възможност за удължаване съгласно GDPR.

Раздел 4.3 - Управление на достъпа и удостоверяване

Потребителите са отговорни за дефиниране на **роли и разрешения за достъп** за своите екипи, като осигуряват периодични прегледи и документиране на предоставения достъп.

Най-добри практики и контрол

- Следвайте **принципа на най-малките привилегии (RBAC)**, като гарантирате, че потребителите имат само необходимия достъп.
- **Многофакторното удостоверяване (MFA)** е задължително за административен достъп и се препоръчва за всички потребители.
- **Надеждни пароли** трябва да бъдат избрани, с поне **8 знаци, включително главни и малки букви, цифри и символи**.
- **Не споделяйте идентификационни данни**.
- Разрешенията за достъп се наблюдават и преглеждат периодично.

Мониторинг: Достъпът, модификациите на разрешенията и важните дейности се документират в регистрационните файлове за сигурност на системата. Дневниците се съхраняват минимум 7 години, в съответствие с HIPAA, GDPR и други приложими разпоредби. Те поддържат вътрешен одит, криминалистичен анализ и регулаторно отчитане. Дневниците са защитени срещу подправяне и се съхраняват в защитени среди с контрол на достъпа.

Раздел 4.4 - Контрол на достъпа за проверка на системата

Функцията Проверка на системата е достъпна само чрез **уеб приложението nCommand Lite** и изисква валидни идентификационни данни за вход. Достъпът е ограничен само до оторизирани роли — *Технолог от разстояние*, *Местен технолог*, *Администратор*, *Супервайзор на роли* и *Потребител за системна проверка*.

Ролята *Потребител за проверка на системата* е проектирана с ограничени права, позволяващи достъп единствено до диагностични функции, свързани с валидиране на мрежата и верификация на свързаността. Това гарантира, че мрежовите данни, информацията в белия списък и системните показатели никога не се излагат на неупълномощени лица.

Всички заявки за достъп се удостоверяват чрез Azure AD B2C, с многофакторно удостоверяване (MFA) и адаптивни политики за условен достъп, управлявани от Microsoft Entra ID. Сложността на паролата следва политиката за сигурност на организацията, изискваща поне осем знака, включително главни и малки букви, цифри и символи. Паролите изтичат на всеки 90 дни, а сесиите автоматично се прекратяват след 24 часа неактивност, като може да се удължи до 90 дни при непрекъсната употреба.

Раздел 4.5 - Регионално разделяне на данни и съхранение на файлове с дневници

Платформата **nCommand Lite** поддържа строга регионална сегрегация на данните, за да предотврати неоторизирани или ненужни трансгранични трансфери. Средите са изолирани по региони, което гарантира съответствие с приложимите регулации.

Всички регистрационни файлове за достъп, записи за дейности и събития, свързани със сигурността, се съхраняват за минимум седем (7) години, в съответствие с приложимите разпоредби за защита на данните и здравеопазване. Дневниците се съхраняват в защитени среди с контролиран достъп и са защитени от несанкционирана промяна. Тази информация е в помощ на криминалистичните разследвания, одитите за съответствие и регулаторните отчети.

Раздел 4.6 - Сигурност и цялост на данните

nCommand Lite System гарантира поверителността, целостта и наличността на данните чрез стандартни за индустрията практики за сигурност.

Потребителите трябва да гарантират спазването на протоколите за сигурност, редовно да преглеждат политиките за достъп и да докладват за всякакви аномалии. Системата непрекъснато следи дейностите и администраторите трябва да прилагат политики за сигурност, за да поддържат стабилна защита срещу потенциални заплахи.

Системата е защитена от 24/7 мониторинг чрез специализиран Център за операции по сигурност (SOC) със SIEM възможности за откриване и реагиране на заплахи.

Раздел 4.7 - Реакция при инциденти със сигурността

Системата включва документиран план за реакция при инциденти, приведен в съответствие с ISO 27035 и NIST CSF.

В случай на инциденти със сигурността, като неоторизиран достъп или системни повреди, потребителите трябва да изпълнят следните стъпки:

Как да разпознаем инцидент?

- **Неоторизиран достъп**, открит в регистрационни файлове на активността.
- **Подозрителни опити за влизане** или повтарящи се грешки при удостоверяване.

- **Необичайно поведение на системата**, като неочаквани действия или неизправности.

Как да съобща за инцидент?

Незабавно запишете събитието чрез наличните канали за поддръжка (глава 5).

Ако бъде потвърдено нарушение на сигурността на лични данни, IONIC, действайки като подизпълнител, ще уведоми GE като обработващ в рамките на 48 часа, като предостави всички съответни доказателства, подробности за въздействието и мерки за смекчаване на последствията. GE, от своя страна, е отговорна за уведомяването на Администратора (клиента) в съответствие с приложимите закони и договорни изисквания.

Глава 5 Канали за обслужване

Независимо дали имате нужда от помощ при технически проблем, неясна стъпка в процеса или допълнителни насоки, нашият екип е готов да ви помогне. Можете да се свържете с нас по телефона, имейл или платформата ITSM, което е по-удобно за вас. Нашите специалисти са обучени да предлагат персонализирана помощ, като гарантират, че всеки проблем се решава бързо и ефективно.

Телефонни номера

САЩ	+1 (216) 2421223
Бразилия	+55 12 3600 0181
Европа (Португалия)	+351 (300) 528 410
Австралия	+1 (216) 2421223
Нова Зеландия	+1 (216) 2421223

ITSM платформа

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

Имейл

helpdesk@ionic.health



ПРЕДУПРЕЖДЕНИЕ!

Всеки сериозен инцидент, свързан с използването на това устройство, трябва да бъде докладван както на производителя, така и на здравния орган/компетентния орган, където е инсталирано устройството.

За да докладвате на производителя: свържете се с местния сервизен представител или докладвайте на: helpdesk@ionic.health

Моля, посочете следната информация:

- Номерът на версията на системата, показан на екрана за вход;
- Дата на инцидента;
- Описание на инцидента, включително всяко въздействие/нараняване на пациент или потребител;
- Вашата информация за контакт (съоръжение, адрес, име за контакт, дял и телефонен номер).

Глава 6 Правна и регулаторна информация

Производител



REF

nCommand Lite

IONIC HEALTH TECHNOLOGIES S.A.

Estrada Dr. Altino Bondesan, 500, Sala 1103-A
Еуженио Де Мело
Сао Жозе дос Кампос-SP
12247-016
Бразилия

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

Отговорен техник

Алешандре Сейджи Фукуда Рибас
CREA-SP: 5071085437

ANVISA

82585300004

Вносител (САЩ)



REF

Система nCommand Lite

IONIC HEALTH USA INC.

11201 Cedar Avenue, STE 600
Cleveland, OH 44106
САЩ

+1 (216) 242 1223

Представител/вносител в ЕС



EU REP

REF

nCommand Lite



Идентификационен номер на
нотифицирания орган: 2803

EUROPE IONIC HEALTH DIGITAL TECHNOLOGIES, LDA

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

+351 (300) 528 410

Упълномощен представител в Швейцария (CH-REP)/Вносител



CH REP

REF

nCommand Lite

FREYR LIFE SCIENCES GMBH

Bahnhofplatz
CH-6300 Zug
Швейцария

Представител/вносител в Обединеното кралство



REF

nCommand Lite

FREYR LIFE SCIENCES LTD

9 Greyfriars Road
Reading, Berkshire
RG1 1NU
Англия, Обединеното кралство

Австралийски спонсор

REF

nCommand Lite

TAEVAS LIFE SCIENCES PTY LTD

46 Dora St
Blacktown NSW 2148
Австралия

Новозеландски спонсор

REF

nCommand Lite

TAEVAS LIFE SCIENCES LIMITED

Level 3, 1 Margaret Street
Lower Hutt 5010
Нова Зеландия

ОСНОВЕН UDI-DI: 7898974112NCLITE2L

Заявка за хартиено копие

Хартиени копия на ръководството за потребителя на nCommand Lite ще бъдат предоставени при поискване без допълнително заплащане. Свържете се с вашия местен представител и поискайте хартиено копие на ръководството за потребителя.

Дата на производство

Датата на пускане на софтуера се намира на страницата за вход в nCommand Lite, във формат МЕСЕЦ/ГОДИНА.

Глава 7 История на редакциите

Редакция	Промяна на описанието	Дата
0	Актуализирана версия на ръководството от 2.3 v1 до 2.4	25 ноември 2025 г.
1	Актуализирани етикети на глава 6	04 декември 2025 г.
2	Премахнато е изискването за статичен IP адрес от конфигурацията на локалния компютър в подраздел 1.3.11 Актуализиран е символът на упълномощения представител на ЕС в подраздел 1.3.12 Премахната е бележката от подточка 1.3.14 Актуализирано е съдържанието в Глава 2 Актуализиран е символът на упълномощения представител на ЕС в Глава 6	28 януари 2026 г.
3	Прегледан е преводът на „Отговорен техник“ в глава 6.	09 февруари 2026 г.

ПРИЛОЖЕНИЕ I - Контролен списък за стартиране на услугата

1. Проверете електрическите и мрежовите връзки:

Уверете се, че електрическите връзки и мрежовите точки са правилно установени на е-KVM компютъра, скенера и локалния компютър.

2. Проверете състоянието на захранването:

Проверете дали непрекъсваемото и стабилизираното захранване и е-KVM компютърът са включени и функционират правилно.

3. Бърз достъп до платформата nC Lite:

Потвърдете наличието на пряк път на платформата nC Lite на работния плот за бърз достъп.

4. Достъп и влизане в nC Lite Platform:

Отворете платформата nCommand и влезте в системата, за да осигурите пълен достъп и правилна функционалност.

5. Настройка на приложението за чат:

Отворете приложението за чат в платформата nC Lite само в един раздел и избягвайте да го минимизирате за безпроблемна комуникация.