



MANUAL DE UTILIZARE

nCommand Lite v2.4

Versiunea manualului: V.3



Cuprins

Capitolul 1	Introducere	4
Secțiune 1.1 -	Scop	4
Secțiune 1.2 -	Glosar	4
Secțiune 1.3 -	Descriere	5
1.3.1.	Utilizare.....	5
1.3.2.	Indicații de utilizare	6
1.3.3.	Populația de pacienți vizată.....	6
1.3.4.	Mediul de utilizare.....	6
1.3.5.	Contraindicații.....	6
1.3.6.	Capacitățile platformei	6
1.3.7.	Beneficii clinice	7
1.3.8.	Utilizatori vizați.....	7
1.3.9.	Mediul de operare.....	7
1.3.10.	Mediul unității medicale	8
1.3.11.	Cerințe minime	9
1.3.12.	Simboluri.....	11
1.3.13.	Durata de viață	11
1.3.14.	Îmbunătățire/Actualizare.....	12
Capitolul 2	Lista cu avertismente generale și precauții	13
Capitolul 3	Utilizarea platformei în fiecare locație.....	16
Secțiune 3.1 -	Accesarea și utilizarea nCommand Lite	16
Secțiune 3.2 -	Accesarea Platformei pentru prima dată	16
3.2.1.	Conectarea prin nCommand Lite.....	17
3.2.2.	Conectarea prin IdP extern.....	18
Secțiune 3.3 -	Gestionarea parolelor	19
Secțiune 3.4 -	Accesarea folosind profilul de operator local.....	22
Secțiune 3.5 -	Accesarea folosind profilul de tehnician la distanță.....	25
3.5.1.	Modul de acces	26
3.5.2.	Bara de redare în flux (Streaming)	29
3.5.3.	Camere video multiple.....	32
3.5.4.	Deschiderea altui dispozitiv	34
3.5.5.	Verificarea sistemului	36
Secțiune 3.6 -	Chat	37

Secțiune 3.7 -	Încheierea sesiunii pe platformă.....	41
Secțiune 3.8 -	Instruire operațională.....	43
Secțiune 3.9 -	Instrucțiuni de depanare	44
Secțiune 3.10 -	Metode de curățare a echipamentelor	49
Capitolul 4	Securitatea cibernetică și confidențialitatea	50
Secțiune 4.1 -	Riscurile de securitate și confidențialitatea.....	50
Secțiune 4.2 -	Protecția datelor cu caracter personal (conformitate cu GDPR/HIPAA).....	50
Secțiune 4.3 -	Gestionarea accesului și autentificarea.....	51
Secțiune 4.4 -	Controlul Accesului la verificarea sistemului	51
Secțiune 4.5 -	Segregarea regională a datelor și păstrarea jurnalelor	52
Secțiune 4.6 -	Securitatea și integritatea datelor	52
Secțiune 4.7 -	Răspunsul la incidentele de securitate	52
Capitolul 5	Canalele de servicii	53
Capitolul 6	Informațiile legale și de reglementare.....	54
Capitolul 7	Istoricul revizuirilor.....	57
Anexa I	- Lista de verificare pentru începerea lucrărilor de service.....	58

**ATENȚIE**

Legea federală restricționează vânzarea acestui dispozitiv doar de către sau la ordinul unui medic, așa cum este utilizat de un operator medical licențiat în statul în care practică.
(pentru Statele Unite ale Americii)

**ATENȚIE**

În Brazilia, acest software este autorizat de Anvisa pentru utilizare exclusivă cu dispozitive de imagistică prin rezonanță magnetică (RMN). Orice altă utilizare este interzisă.
(pentru utilizare în Brazilia)

**ATENȚIE**

Înainte de utilizare, asigurați-vă că sunteți la curent cu cerințele specifice ale țării sau regiunii dumneavoastră. Nerespectarea reglementărilor poate duce la riscuri pentru sănătate.

**ATENȚIE**

Asigurați-vă că versiunea acestui manual de utilizare corespunde cu versiunea platformei utilizate. Utilizarea unei versiuni incorecte poate duce la o funcționare incorectă sau la o interpretare greșită a funcțiilor.

Capitolul 1 Introducere

Secțiune 1.1 - Scop

Acest manual își propune să ofere operatorilor locali și la distanță o înțelegere cuprinzătoare a funcționalităților specifice ale sistemului nCommand Lite. Servind drept manual de utilizare, acest document oferă informații concise și practice, ghidând utilizatorii în ceea ce privește funcționalitățile și depanarea sistemului. Urmând acest manual, utilizatorii vor putea utiliza nCommand Lite în mod eficient, deoarece îi ajută în maximizarea productivității și reducerea dependenței de asistența tehnică.

Secțiune 1.2 - Glosar

**ATENȚIE**

Această etichetă se aplică condițiilor sau acțiunilor care prezintă potențial pericol. Puteți provoca vătămări sau daune materiale minore dacă ignorați aceste instrucțiuni.

**AVERTISMENT**

Această etichetă identifică condițiile sau acțiunile care au ca rezultat un pericol specific. Veți provoca vătămări corporale grave sau daune materiale substanțiale dacă ignorați aceste instrucțiuni.

Termen în platformă	Termen corespondent
Unitate de imagistică	Unitate medicală, Unitate, Unități mobile, Centru de asistență medicală, Unitate medicală
Unitate la distanță	Stație de lucru la distanță, Loc la distanță, Birou la distanță, Locație la distanță, Centru de comandă
Platformă	Aplicația web nCommand Lite
Sistem	nCommand Lite cu toate subsistemele
Dispozitiv	Scanner medical, Scanner, Echipament, Dispozitiv medical, Dispozitiv de imagistică, Echipament de imagistică
Operator local	Utilizator local, Operator local, Profesionist local în domeniul sănătății (LHP), Utilizator la fața locului

Secțiune 1.3 - Descriere

Sistemul nCommand Lite este un SaMD (software ca dispozitiv medical) care este orientat către client și permite accesul de la distanță printr-o aplicație web pentru vizualizarea/revizuirea imaginilor, precum și posibilitatea de a oferi de la distanță recomandări în timp real operatorului autorizat aflat lângă pacient (utilizator local) care operează dispozitivele de imagistică medicală în contextul instruirii sau evaluării procedurii, pentru scanere RMN, CT și PET/CT.

Utilizatorii de la distanță sunt operatori licențiați, care pot accesa un dispozitiv medical de imagistică de pe un computer care îndeplinește specificațiile minime necesare din orice loc, folosind o conexiune software securizată care transmite imagini video și permite accesul la tastatură și mouse. Acest lucru permite utilizatorilor de la distanță să asiste utilizatorii locali fără a fi împiedicați de distanță. Acest acces trebuie permis de utilizatorul local care folosește sistemul și poate fi, de asemenea, revocat în orice moment de către utilizatorul local, permițându-i astfel să mențină permanent controlul complet asupra sesiunii. De asemenea, fiecare sesiune la distanță este controlată printr-o acreditare securizată care este gestionată de utilizatorul local. Conexiunile la un dispozitiv medical sunt limitate la o singură sesiune de la distanță la un moment dat pentru a menține un control strict asupra celor care interacționează de la distanță cu sistemul. Imaginile revizuite de la distanță nu sunt destinate diagnosticării.

Sistemul nCommand Lite constă dintr-o soluție de instalare bazată pe hardware și software IT care permite mai multe sesiuni, oferind operatorilor la distanță posibilitatea de a accesa mai multe dispozitive de imagistică medicală, după cum este necesar. Scanerile compatibile cu sistemul nCommand Lite respectă un protocol comun, permițând gestionarea parametrilor de scanare și scanarea de la distanță.

1.3.1. Utilizare

Sistemul nCommand Lite oferă acces de la distanță pentru vizualizarea/revizuirea imaginilor, precum și posibilitatea de a oferi de la distanță îndrumări în timp real operatorului licențiat care lucrează cu scannerul. Aceste îndrumări includ instruirea, evaluarea procedurilor și gestionarea parametrilor de scanare.

1.3.2. Indicații de utilizare

Sistemul nCommand Lite permite accesul de la distanță pentru vizualizarea/revizuirea imaginilor, precum și posibilitatea de a oferi de la distanță îndrumări în timp real operatorului licențiat care operează un scanner RMN, CT sau PET/CT compatibil. Acest acces trebuie permis de către operatorul local licențiat care operează sistemul. Accesul de la distanță este disponibil numai pentru sistemele care au capacitatea de conectare de la distanță. Imaginile revizuite de la distanță nu sunt destinate diagnosticării.

1.3.3. Populația de pacienți vizată

Orice pacient căruia i se prescrie să efectueze investigații imagistice folosindu-se un dispozitiv medical de imagistică conectat.

1.3.4. Mediul de utilizare

Unități de imagistică care efectuează examene de imagistică prin rezonanță magnetică (RMN), tomografie computerizată (CT) și tomografie cu emisie de pozitroni – tomografie computerizată (PET/CT) și centre de comandă la distanță.

1.3.5. Contraindicații

Platforma nu ar trebui operată de utilizatori care nu sunt operatori licențiați și care nu au fost instruiți cu privire la utilizarea nCommand Lite.

1.3.6. Capacitățile platformei

- **Scanarea la distanță:** prezintă ecranul dispozitivului de imagistică medicală în timp real, permițând unui operator la distanță licențiat să participe la o examinare.
- **Chat:** face posibilă comunicarea între operatorii licențiați la distanță și cei locali prin mesaje text și vocale. Operatorii locali și la distanță pot efectua și primi apeluri vocale și video.
- **Camere video multiple:** facilitează observarea de la distanță a pacienților și a unității medicale în timpul procedurii. Operatorul la distanță poate accesa vizualizarea camerelor video prin filele partajate ale tuturor camerelor video și individual, pe fiecare în parte. Acest mecanism reproduce supravegherea vizuală pe care ar avea-o un profesionist din domeniul sănătății dacă s-ar afla în apropierea pacientului, introducând astfel un nivel sporit de siguranță.
- **Scanarea la distanță în sesiuni multiple** permite operatorului la distanță să acceseze mai multe dispozitive de imagistică medicală, după cum este necesar.
- **Modul de acces:** permite operatorului la distanță să aleagă între vizualizări sau să controleze dispozitivul. În modul Vizualizare, operatorii la distanță pot vedea doar ceea ce este transmis. În modul Control, aceștia dețin controlul asupra mouse-ului și tastaturii.
- **Gestionarea accesului operatorului la distanță:** permite operatorului local să controleze accesul operatorului la distanță și modul de acces al acestuia (Vizualizare sau Control). Pentru a permite conectarea operatorului la distanță, accesul trebuie acordat de către operatorul local care utilizează platforma și poate fi, de asemenea, revocat în orice moment de către operatorul local, permițându-i astfel să mențină în permanență controlul complet asupra sesiunii.
- **Dimensiunea fluxului:** operatorul la distanță poate vedea dimensiunea originală a fluxului și dimensiunea curentă a fluxului în pixeli. De asemenea, este notificat atunci când dimensiunea curentă a fluxului este mai mică decât cea originală.

- **Starea mouse-ului și a tastaturii:** operatorul la distanță primește feedback dacă mouse-ul și tastatura dispozitivului de imagistică medicală funcționează corect.
- **Detalii sesiune:** operatorii locali și la distanță pot accesa detalii despre sesiune.

1.3.7. Beneficii clinice

nCommand Lite optimizează imagistica de diagnostic permițând operarea de la distanță a sistemelor **RMN, CT și PET-CT**, asigurând o calitate constantă a imagisticii și respectarea protocoalelor. Permite operatorilor cu experiență să supravegheze și să asiste la scanări în timp real, optimizând eficiența fluxului de lucru și reducând erorile care ar putea afecta acuratețea diagnosticării. Sistemul facilitează colaborarea între operatori, sporind consecvența examinărilor și permițând luarea mai rapidă a deciziilor în cazuri complexe. Deoarece permite profesioniștilor de la distanță să folosească mai multe unități, **nCommand Lite** crește **disponibilitatea, varietatea și calitatea** examinărilor imagistice și, astfel, mai mulți pacienți au acces la diagnostice avansate, cu optimizarea, în același timp, a resurselor medicale. În plus, ajută la atenuarea deficitului de personal prin reducerea dependenței de specialiștii de la fața locului, menținând în același timp conformitatea cu standardele stricte de reglementare și de securitate a datelor.

1.3.8. Utilizatori vizați

- **Operator local**
Operatorul local este utilizatorul de la fața locului responsabil cu asistarea și îndrumarea fizică a pacienților în unitatea medicală. Acesta trebuie să aibă cunoștințele necesare pentru a efectua proceduri de scanare pentru un anumit dispozitiv de imagistică. În plus, acesta/aceasta controlează modul de acces al operatorului la distanță (Vizualizare sau Control), iar accesul la distanță trebuie acordat de către operatorul local prin intermediul platformei și poate fi revocat în orice moment.
- **Operator la distanță**
Un profesionist care efectuează operațiuni de la distanță, având acces și control asupra computerului dispozitivului. La fel ca operatorul local, operatorul la distanță trebuie să aibă cunoștințele necesare pentru a efectua proceduri de scanare pentru un anumit dispozitiv de imagistică.
- **Asistență/Utilizator IT**
Profesionist responsabil cu configurarea platformei (nu este inclusă în acest Manual de utilizare).

1.3.9. Mediul de operare

Următoarele specificații se referă la cerințele de mediu pentru computerul e-KVM.

- **Altitudine maximă (fără presurizare)**
 - Funcționare: Între 0 m (0 ft) și 3.048 m (10.000 ft)
 - Depozitare: Între 0 m (0 ft) și 12.192 m (40.000 ft)
- **Temperatură**
 - Funcționare: Între 10 °C (50 °F) și 35 °C (95 °F)
 - Depozitare: Între -10 °C (14 °F) și 50 °C (122 °F)

- **Umiditate relativă**
 - Funcționare: 20%-80% (fără condensare)
 - Depozitare: 10%-90% (fără condensare)

1.3.10. Mediul unității medicale

Platforma nCommand Lite are două tipuri diferite de locații fizice:

- **Unitate de imagistică:** Unități care efectuează examene de imagistică prin rezonanță magnetică (RMN), tomografie computerizată (CT) sau tomografie cu emisie de pozitroni – tomografie computerizată (PET/CT).
- **Unitate la distanță:** O locație unde operatori la distanță pot accesa și gestiona de la distanță dispozitivele (scanere RMN, CT sau PET/CT). Această stație de lucru poate fi utilizată în diverse medii, cum ar fi birouri, centre de comandă, locații îndepărtate sau chiar locații secundare din unitatea medicală. Stația de lucru la distanță poate fi amplasată în orice spațiu care oferă utilizatorului condiții adecvate pentru concentrare, conectivitate minimă și respectarea cerințelor de configurare a sistemului informatic.

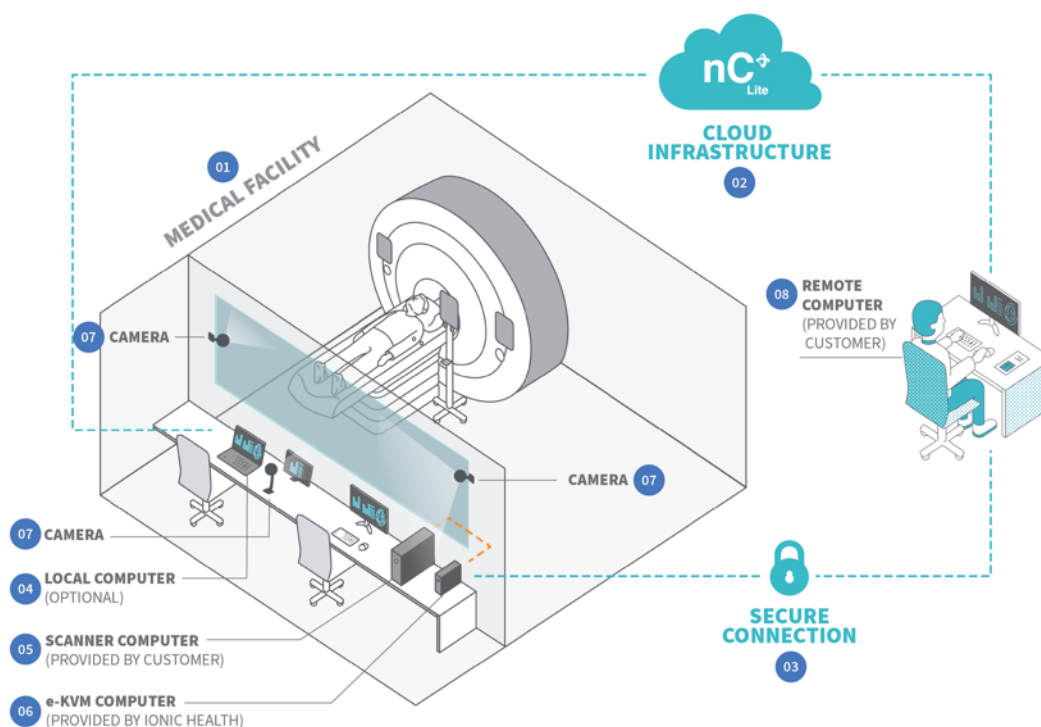


Figura 01: Prezentare generală a produsului și a conexiunilor acestuia printr-o conexiune securizată (de exemplu, VPN).

01 – Facilități medicale; 02 – Infrastructură Cloud; 03 – Conexiune securizată; 04 – Calculator local (opțional);
 05 – Calculator Scanner (Furnizat de Client); 06 – e-KVM (Furnizat de IONIC Health);
 07 – Cameră video; 08 - Computer la distanță (furnizat de client)

**ATENȚIE!****Compatibilitate cu scanarea de la distanță**

IONIC Health (IH) validează funcționalitatea de scanare de la distanță pe dispozitivele compatibile menționate. IH efectuează o evaluare completă a cerințelor IH de scanare de la distanță și testează sistemul în mediul vizat în timpul instalării. Acest lucru asigură compatibilitatea și performanța adecvată în momentul respectiv pentru scanarea de la distanță. Această verificare nu implică faptul că toate cerințele privind dispozitivul OEM (producător de echipamente originale) sunt îndeplinite în această configurație. Orice abatere de la cerințele OEM este responsabilitatea utilizatorului final.

Modificările aduse sistemului sau mediului după instalare trebuie raportate către IH pentru a se verifica compatibilitatea continuă. IH nu poate garanta performanța și nu își poate asuma responsabilitatea pentru configurațiile diferite de cele validate în timpul instalării.

1.3.11. Cerințe minime**• Computer local**

Acest computer este folosit de **operatorul local** pentru a autoriza și permite accesarea de la distanță a dispozitivului prin nCommand Lite®. De asemenea, permite comunicarea directă cu **operatorul la distanță** prin funcția de chat de pe platformă.

Specificațiile tehnice minime necesare sunt:

- Procesor: AMD® A4-9120C sau o versiune ulterioară sau un procesor similar
- Memorie: 4 GB sau mai mare
- Capacitate: 128 GB SSD sau mai mare
- Periferice: microfon și difuzor, sau căști și cameră video web
- Monitor: FHD 14" (1920 x 1080) sau o versiune ulterioară
- Sistem de operare: Chrome OS, Windows OS sau MAC OS
- Loc de instalare: acest computer trebuie să fie în apropierea computerului scannerului
- Rutina IT: Crearea unei comenzi rapide pentru nCommand Lite pe desktop-ul fiecărui utilizator
- Compatibilitatea browserului: Google Chrome sau Microsoft Edge.

• Stația de lucru la distanță

Această stație este utilizată de **operatorul la distanță** pentru a accesa și controla dispozitivul prin nCommand Lite®. Stația de lucru la distanță trebuie să stabilească o conexiune securizată la computerul e-KVM (furnizat de IONIC HEALTH®).

Clientul este responsabil pentru furnizarea computerului la distanță și va alege unul dintre cele două scenarii: primul este o funcționare 24x7, iar al doilea este o funcționare în timpul programului de lucru.

Pentru fiecare scenariu, veți găsi mai jos specificațiile adecvate pentru alegerea modelelor de computer:

Scenariul 1 (funcționare permanentă) - trebuie să îndeplinească următoarele specificații:

- Intel Xeon W-2223 (4 nuclee, 8 fire de execuție, memorie cache 8,25 MB, 3,90 GHz Turbo) sau o versiune ulterioară.
- RAM: 16 GB sau mai mult.
- Unitate grafică: NVIDIA RTX A2000 6 GB sau versiune ulterioară sau o unitate similară.
- Capacitate: 128 GB SSD sau mai mare.
- Sistem de operare: Windows 11 Pro 64B sau o versiune ulterioară.
- Cerințe minime pentru monitor: Dimensiune 27", raport de aspect 16:9, rezoluție 4k.
- Căști: BLACKWIRE 3200 sau similare.
- Compatibilitatea browserului: Google Chrome sau Microsoft Edge.

Scenariul 2 (funcționare în timpul programului de lucru) - trebuie să îndeplinească următoarele specificații:

- Intel® Core™ i7-12700k vPro® sau o versiune ulterioară.
- RAM: 16 GB sau mai mult.
- Unitate grafică: NVIDIA T400 GB sau versiune ulterioară sau o unitate similară.
- Capacitate: 128 GB SSD sau mai mare.
- Sistem de operare: Windows 11 Pro 64B sau o versiune ulterioară.
- Cerințe minime pentru monitor: Dimensiune 27", raport de aspect 16:9, rezoluție 4k.
- Căști: BLACKWIRE 3200 sau similare.
- Compatibilitatea browserului: Google Chrome sau Microsoft Edge.



AVERTISMENT!

Nerespectarea configurării adecvate și a cerințelor minime poate duce la o comunicare deficitară sau eșuată între utilizatori.

● **Configurații de rețea (cerințe minime)**

Pentru a permite sesiunea între utilizatorul la distanță și computerul e-KVM, comunicarea în rețea între cele două dispozitive trebuie să fie asigurată. Sistemul nCommand Lite utilizează arhitectura de rețea peer-to-peer (P2P) pentru a stabili conexiunea între utilizatorul local, utilizatorul la distanță și computerul e-KVM. Există trei scenarii posibile:

- **Scenariul 1** – rețea de corporație care utilizează unul dintre următoarele protocoale: LAN, LAN-to-LAN, MPLS sau VPN;
- **Scenariul 2** – rețea de corporație care utilizează WAN (rețea externă) de încredere și nu utilizează niciunul dintre următoarele protocoale: LAN, LAN-to-LAN, MPLS sau VPN;
- **Scenariul 3** – rețea publică pentru computerul la distanță (utilizatorul la distanță).

Configurațiile pentru fiecare scenariu sunt detaliate în documentația tehnică.

1.3.12. Simboluri

Simbol	Descriere	Referință
	Producător	ISO 15223-1, ISO 7000-3082
	Data fabricației	ISO 15223-1, ISO 7000-2497
	Simbolul indică faptul că acest produs este un dispozitiv medical	ISO 15223-1
	Identificator unic al dispozitivului	ISO 15223-1
	Număr de catalog	ISO 15223-1, ISO 7000-2493
	Importator	ISO 15223-1, ISO 7000-3725
	Consultați manualul de utilizare	ISO 15223-1, ISO 7000-1641
	Distribuitor	ISO 15223-1, ISO 7000-3724
	Atenție	ISO 15223-1, ISO 7000-0434A
	Avertisment	ISO 7010-W001
	Număr de serie (sau versiune de software)	ISO 15223-1, ISO 7000-2498
	Reprezentant autorizat în Comunitatea Europeană	ISO 15223-1
	Reprezentant autorizat în Elveția (CH-REP)	ISO 15223-1
	CE - marcaj de conformitate europeană; 2803 – desemnarea organismului notificat	Regulamentul UE 2017/745

1.3.13. Durata de viață

Durata de viață preconizată a produsului este de 5 ani, având în vedere durata de viață utilă a componentelor care alcătuiesc produsul. Această evaluare complexă se asigură că durata de viață a fiecărui component critic corespunde cu durata de viață totală, garantând performanțe și fiabilitate constante pe toată durata preconizată de utilizare a produsului.

1.3.14. Îmbunătățire/Actualizare

IONIC Health va actualiza sistemul nCommand Lite ca parte a întreținerii planificate sau a lansărilor de upgrade-uri. Aceste actualizări sunt concepute să asigure performanța și fiabilitatea continue fără a afecta versiunea implementată în acel moment la unitatea clientului. În funcție de natura actualizării, produsului i se poate face upgrade de la distanță sau poate fi necesară o vizită la fața locului din partea unui inginer de teren.

Capitolul 2 Lista cu avertismente generale și precauții



AVERTISMENT!

Vă rugăm să citiți toate avertismentele de mai jos înainte de a utiliza sistemul nCommand Lite.



ATENȚIE

Sistemul nCommand Lite nu poate fi supus lucrărilor de reparație sau întreținere în timp ce este utilizat pentru a controla un echipament RMN, CT sau PET-CT în prezența unui pacient.

- Acordați o atenție deosebită tuturor alertelor de sistem, deoarece acestea sunt esențiale pentru funcționarea în siguranță.
- Puneți pe primul loc siguranța și atenția în timpul tuturor operațiunilor.
- Legea federală restricționează vânzarea acestui dispozitiv doar de către sau la ordinul unui medic, așa cum este utilizat de un operator medical licențiat în statul în care practică.
- Sistemul nCommand Lite trebuie utilizat numai de operatori care au fost instruiți cu privire la utilizarea platformei.
- Utilizați acest sistem numai cu browsere web compatibile. Browserele compatibile sunt Google Chrome și Microsoft Edge.
- În caz de urgență, un operator instruit și licențiat trebuie să rămână în unitatea de imagistică pentru a efectua examinarea RMN, CT sau PET/CT fără nCommand Lite.
- Accesarea simultană a mai multor dispozitive necesită concentrare intensă și comunicare cu echipele locale.
- Evitați accesarea simultană a dispozitivelor cu aspect identic sau examinări ale aceleiași regiuni anatomice.
- Puteți vizualiza mai multe ecrane, dar controlul este limitat la un singur dispozitiv la un moment dat.
- Inițiați întotdeauna un chat atunci când vă conectați la un dispozitiv pentru o comunicare clară.
- Alerte de apel apar pe ecranul dispozitivului asociat; doar un singur apel poate fi activ la un moment dat.
- Testați comunicarea video atunci când accesați aplicația (înainte de a începe o sesiune de lucru) pentru a verifica dacă există vreo defecțiune în conexiunea de ieșire video a dispozitivelor de RMN, CT sau PET/CT sau a oricărui dispozitiv asociat fluxului video.
- Dispozitivul nu trebuie conectat la priză și/sau la sursa de alimentare neîntreruptă și stabilizată prin prelungitoare sau „prize cu prelungitor”.
- Dacă apar defecțiuni video, verificați conexiunea video dintre sistemul dispozitivului și computerul e-KVM.
- Dacă aplicația este lentă în timpul accesului de la distanță, reîmprospătați pagina cu comanda Ctrl+F5 în browserul computerului operatorului la distanță. Dacă problema persistă, contactați asistența tehnică.
- Ori de câte ori pagina browserului este reîmprospătată, conexiunea la dispozitiv este întreruptă, necesitând reluarea procesului de aprobare.
- Nu vă conectați folosind un alt browser când sunteți deja conectat.

- Unitatea de imagistică a clientului trebuie să aibă o legătură redundantă la internet cu un furnizor diferit de cel principal pentru schimbarea imediată în caz de pierdere a comunicării cu sistemul/platforma.
- În caz de pierdere a comunicării sau încetinire a mouse-ului, efectuați o „resincronizare a mouse-ului” pe pagina utilizată în browser.
- Asigurați-vă că computerele utilizate pentru controlul sistemului nCommand Lite, atât în unitatea de imagistică, cât și în centrul de comandă, îndeplinesc cerințele minime; în caz contrar, se poate produce o pierdere a performanței aplicației.
- QoS (calitatea serviciului) ar trebui aplicată legăturii principale și legăturii redundante pentru transmiterea de pe platformă, iar performanța legăturii ar trebui monitorizată.
- Înainte de utilizare, verificați în browser-ul web nivelurile de volum audio și pentru microfon, precum și permisiunea pentru transmisie audio și de la microfon.
- Înainte de utilizare, verificați funcționarea tastaturii și a mouse-ului; dacă acestea sunt lente sau nesincronizate, activați butonul „resincronizare mouse”. Verificați dacă computerul e-KVM este conectat și pornit.
- Asigurați-vă că tastatura de la unitatea la distanță are o configurație identică cu tastatura de la unitatea de imagistică.
- Dacă trebuie să schimbați locul în care este utilizată platforma, clientul trebuie să contacteze asistența tehnică pentru a efectua o nouă instalare. Nu reinstalați fără a contacta asistența tehnică.
- Înainte de a începe procesul de accesare de la distanță a dispozitivului RMN, CT sau PET/CT, este important ca echipele de tehnicieni să verifice toate aspectele necesare pentru buna funcționare a platformei, pentru a nu afecta examinarea. Aceste aspecte sunt enumerate în documentul „Lista de verificare la începutul serviciului”.
- Configurația firewall-ului unității de imagistică trebuie verificată lunar împreună cu echipa IT, asigurându-se că nu există probleme cu versiunea de firewall care ar putea compromite utilizarea nCommand Lite.
- Orice anomalie observată în utilizarea aplicației trebuie raportată imediat echipei de asistență înainte de a începe accesarea sau se va întrerupe accesul, dacă acesta a fost deja inițiat.
- Numai operatori licențiați instruiți cu privire la utilizarea nCommand Lite ar trebui să folosească aplicația.
- Accesul de la distanță prin intermediul platformei nu înlocuiește și nu concurează cu nicio altă procedură operațională pentru funcționarea RMN, CT sau PET/CT stabilită de producătorul dispozitivelor medicale și protocoalele și procedurile unității de îngrijire.
- Evitați îndoirea sau întinderea cablurilor echipamentelor.
- Dacă apar probleme cu comunicarea vocală sau prin chat, utilizați funcția de apel telefonic pentru a stabili comunicarea între operatorul local de la unitatea de imagistică și operatorul la distanță de la Centrul de Comandă. Urmați instrucțiunile descrise în secțiunea „Instrucțiuni în caz de defecțiune” și, dacă este necesar, contactați asistența tehnică pentru a efectua reparația.
- Dacă este necesară înlocuirea unui computer sau a oricărui alt echipament care influențează direct echipamentul nCommand Lite, contactați suportul tehnic, asigurând continuarea funcționării sistemului.
- Doar o singură persoană la un moment dat poate accesa de la distanță dispozitivul RMN, CT sau PET/CT.
- Nu atingeți niciun cablu video fizic cât timp computerul dispozitivului și sistemul nCommand Lite se află sub tensiune.

- Când accesați un dispozitiv suplimentar se va deschide o filă nouă. Trageți această filă pe un al doilea monitor, deoarece sistemul este conceput să fie utilizat cu un ecran separat pentru fiecare dispozitiv.
- Orice incident grav legat de utilizarea acestui dispozitiv trebuie raportat atât producătorului, cât și autorității sanitare/autorității competente din locul unde este instalat dispozitivul (*vedeți mai multe detalii în capitolul Canale de service*).

Capitolul 3 Utilizarea platformei în fiecare locație

Secțiune 3.1 - Accesarea și utilizarea nCommand Lite

**AVERTISMENT!**

În cazul apariției unor probleme, contactați asistența tehnică pentru suport.

**AVERTISMENT!**

Verificați aspectul tastaturii și asigurați-vă că aceasta este identică în ambele locații (unitate medicală și unitate la distanță). Aspectul diferit al tastaturii poate afecta experiența utilizatorului.

Acest capitol prezintă tot ceea ce trebuie să știți pentru a accesa și a începe să utilizați platforma nCommand Lite. Veți găsi instrucțiuni simple, pas cu pas, pentru a vă conecta, a naviga prin interfață și a înțelege principalele funcții. Indiferent dacă lucrați la fața locului sau de la distanță, acest ghid vă va ajuta să începeți utilizarea rapid și cu încredere.

Schimbarea limbii - sistemul este presetat în limba engleză în mod implicit, dar puteți schimba cu ușurință limba în funcție de preferințele dvs. Pe ecranul de conectare, faceți clic pe colțul din dreapta sus unde apare „English (en-US)”. Astfel se va deschide o listă derulantă cu limbile disponibile din care puteți selecta.

După conectare, puteți schimba limba făcând clic pe limba selectată în prezent în partea dreaptă a barei de sus. Astfel se va deschide o listă derulantă cu limbile disponibile din care puteți alege.

Vă rugăm să rețineți că, dacă schimbați limba în timp ce sunteți conectat la un dispozitiv, conexiunea curentă va fi încheiată automat și va trebui să vă reconectați.

Când accesați platforma, puteți alege limba preferată pe ecranul de conectare. Cu toate acestea, unele mesaje afișate în timpul procesului de conectare pot apărea în limba setată în browser-ul dvs. web, indiferent de limba selectată pe platformă. Pentru o experiență consecventă, vă recomandăm să aliniați setările de limbă ale browser-ului cu limba preferată pentru platformă.

Secțiune 3.2 - Accesarea Platformei pentru prima dată

Procesul de conectare la platformă se poate face în două moduri: prin nCommand Lite sau printr-un furnizor de identitate extern (External IdP). Utilizatorul se poate conecta folosind una dintre metodele preconfigurate. Dacă metoda configurată este furnizor de identitate extern (IdP extern), metoda nCommand Lite nu va funcționa și invers. Pentru a vă conecta prin IdP extern, accesați direct **subpunctul 3.2.2**.

3.2.1. Conectarea prin nCommand Lite

Notă: Această secțiune nu se aplică utilizatorilor care se conectează printr-un furnizor de identitate extern (IdP extern).

Porniți computerul și faceți dublu clic pe pictograma de comandă rapidă nCommand Lite, care se află de obicei pe desktop. De asemenea, puteți accesa adresa URL direct din browser.

Primul acces este un pas esențial pentru a începe să utilizați platforma în siguranță și eficient. Iată ce trebuie să știți:

1 - E-mail de bun venit: Veți primi un e-mail cu detaliile de conectare, inclusiv adresa dvs. personală de e-mail asociată, o parolă temporară și un link direct către platforma clientului. Acest e-mail este esențial pentru a vă începe parcursul pe nCommand Lite.

2 - Creare parolă: După accesarea link-ului va trebui să introduceți adresa de e-mail asociată și parola primită în e-mailul de bun venit. Dacă faceți clic pe „Sign in” (Conectare), veți fi direcționat către o altă pagină, pentru a crea o nouă parolă. Trebuie să introduceți parola veche, parola nouă și să confirmați parola nouă. Aceasta trebuie să fie puternică și sigură, cuprinzând cel puțin 3 elemente dintre următoarele: o literă mică, o literă mare, o cifră și un simbol și să aibă cel puțin 8 caractere. Dacă faceți clic pe „Continue” (Continuare) veți fi redirecționat către o altă pagină pentru a vă confirma din nou adresa de e-mail. După ce faceți clic pe „Continue” (Continuare) veți fi redirecționat către ecranul de pornire, care este personalizat în funcție de profilul dvs. de utilizator specific.

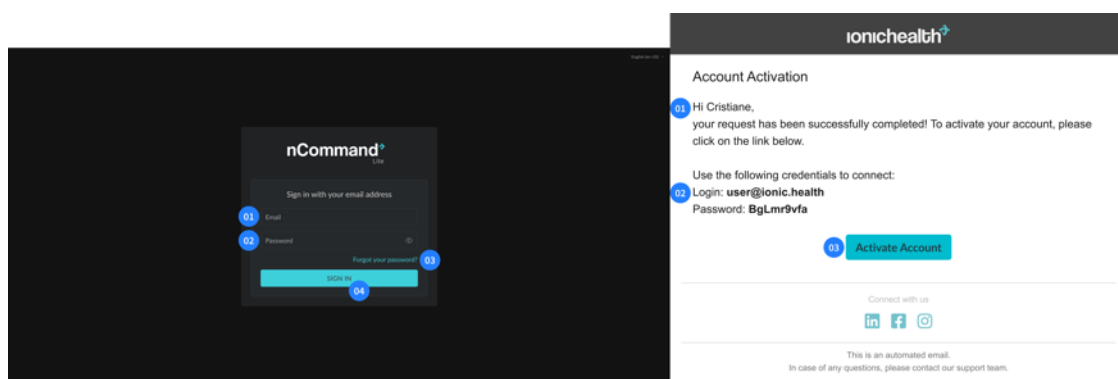


Figura 02: Prima Accesare

Stânga - Pagina de autentificare: 01 – Adresă de email; 02 – Parolă; 03 – "Ați uitat parola?"; 04 – Butonul de autentificare

Dreapta - E-mail de bun venit: 01 – Textul e-mailului de activare a contului; 02 – Acreditări de conectare; 03 – Butonul pentru activarea contului

Această procedură inițială este concepută să asigure securitatea maximă a contului dvs. încă de la început. Începând cu a doua accesare, procesul va fi optimizat, menținând același nivel de securitate, prin transmiterea unui cod de autentificare cu doi factori către adresa de e-mail asociată la fiecare conectare, pentru a garanta securitatea continuă a contului dumneavoastră..

După conectarea în nCommand Lite, sistemul vă va direcționa automat către ecranul de pornire, care este personalizat în funcție de profilul dvs. de utilizator specific. Indiferent dacă sunteți operator local sau operator la distanță, interfața este concepută astfel încât să satisfacă nevoile și accesul relevant pentru rolul dvs. Acest design intuitiv vă oferă toate instrumentele și

informațiile necesare pentru o experiență de utilizator eficientă, chiar din momentul în care vă conectați.

Notă: Când metoda de autentificare este configurată ca nCommand Lite, autentificarea trebuie realizată întotdeauna prin această opțiune. Chiar dacă pe ecranul de conectare apare un buton de IdP extern, acesta nu va funcționa pentru acești utilizatori. Fiecare cont de utilizator este înregistrat pe platformă cu o metodă specifică de autentificare — fie credențiale nCommand Lite, fie un serviciu External IdP. Dacă un utilizator încearcă să se autentifice folosind o metodă diferită de cea atribuită contului său, sistemul va afișa un mesaj de eroare care indică faptul că acel cont nu este autorizat pentru acel tip de autentificare.

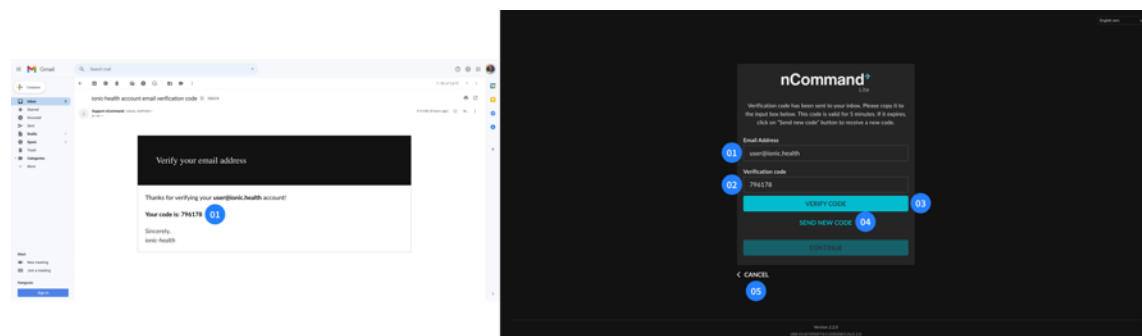


Figura 03: Autentificare în doi pași (2-FA)

Stânga – E-mail: 01 – 2-FA Cod

Dreapta - Pagina de autentificare cu doi factori: **01** – Adresă de e-mail; **02** – Cod de verificare; **03** – Buton cod de verificare confirmare; **04** – Trimitere cod nou; **05** – Anulare

3.2.2. Conectarea prin IdP extern

În unele cazuri, utilizatorii se pot conecta la platformă printr-un furnizor de identitate (IdP) extern, care le permite să folosească serviciul de autentificare existent al organizației lor, un mecanism cunoscut și sub numele de Autentificare unică (SSO). Prin această metodă, utilizatorul preînregistrat nu va primi un e-mail de bun venit. Serviciul IT local trebuie să verifice compatibilitatea, să configureze metoda și să informeze utilizatorul care e-mail (IdP extern) trebuie utilizat.

Când este disponibilă această opțiune, utilizatorul trebuie să se conecteze întotdeauna folosind IdP extern (de exemplu, Amazon Cognito, Microsoft Entra ID, Microsoft AD B2C). Metoda de conectare prin nCommand Lite nu va fi disponibilă pentru utilizatorii de IdP extern.

Pentru a vă conecta folosind IdP extern, faceți clic pe butonul cu numele IdP și urmați instrucțiunile furnizate de autentificatorul extern. Dacă instituția dvs. are integrat mai mult de un IdP extern, nu uitați să confirmați furnizorul la care sunteți înregistrat. Alți furnizori nu vor funcționa. Dacă aveți întrebări sau întâmpinați dificultăți, contactați serviciul IT local.

În scenariile în care utilizatorii partajează același aparat și utilizează Autentificarea unică (SSO), se recomandă ca fiecare utilizator să selecteze opțiunea „do not stay signed in” (nu rămâneți conectat) în timpul conectării cu IdP extern (dacă este disponibilă) sau să se deconecteze de la furnizorul extern după ce s-a deconectat de la nCommand Lite.

Pentru această opțiune de conectare, procesul complet de conectare și deconectare — inclusiv politicile de creare și expirare a parolelor, autentificarea cu mai mulți factori (MFA) și blocările contului — este gestionat în întregime de echipa IT a clientului care a configurat IdP extern.

Când vă conectați printr-un IdP extern, funcțiile „Forgot Password” (Am uitat parola) și „Change Password” (Schimbare parolă) trebuie efectuate conform procesului pentru IdP extern.

Notă: Opțiunea „Forgot Password” (Am uitat parola) va fi afișată în continuare pe ecranul de autentificare, însă nu va fi funcțională pentru acești utilizatori. Opțiunea vă poate direcționa către următorii pași ai procesului, dar nu îl va finaliza. Dacă trebuie să vă recuperați parola, urmați instrucțiunile de la IdP extern.

Important: Chiar și atunci când se folosește un IdP extern, utilizatorul trebuie să fie preînregistrat în platforma nCommand Lite pentru a i se permite accesul.

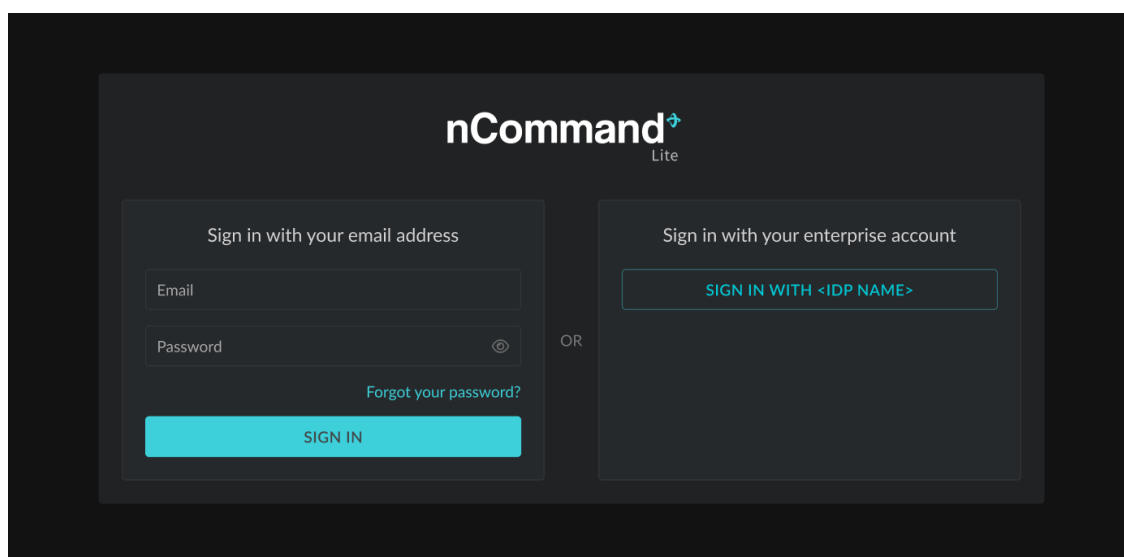


Figura 04: Ecranul de autentificare prin External IdP (Exemplu)

Secțiune 3.3 - Gestionarea parolelor

După prima accesare a platformei, utilizatorii își pot schimba parola sau, dacă au uitat-o, pot seta o parolă nouă.

Notă: Când conectarea se realizează prin IdP extern, funcțiile ***Forgot password (Am uitat parola)*** și ***Change password (Schimbare parolă)*** trebuie efectuate conform procesului pentru IdP extern.

- **Recuperarea parolei:** Permite utilizatorilor să recupereze accesul la cont în cazul în care își uită parola. Pur și simplu faceți clic pe linkul „Forgot your password?” (Ați uitat parola?) de pe pagina de conectare, introduceți adresa de e-mail asociată și trimiteți informațiile. Sistemul va trimite apoi un e-mail care conține un cod de verificare. După ce introduceți codul și faceți clic pe „Verify code” (Verificare cod), utilizatorilor li se va cere să confirme adresa de e-mail asociată.

Dacă dau clic pe „Continue” (Continuare), utilizatorii sunt direcționați către o pagină unde pot introduce o parolă nouă și pot confirma parola nouă. Dacă parola nouă îndeplinește cerințele de sistem, utilizatorii o pot înregistra cu succes și ulterior se pot conecta cu acreditările actualizate.

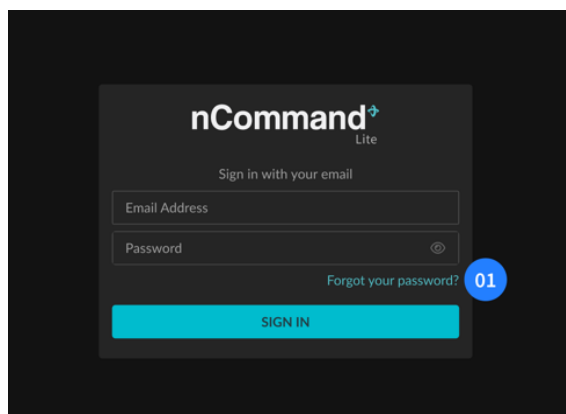


Figura 05: Link către pagina de resetare a parolei
01 – Ați uitat parola?

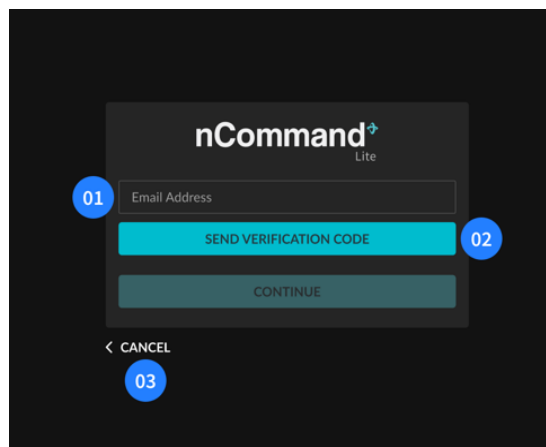


Figura 06: Pagina de resetare a parolei
01 – Adresă de e-mail; 02 – Trimitere cod de verificare; 03 – Anulare

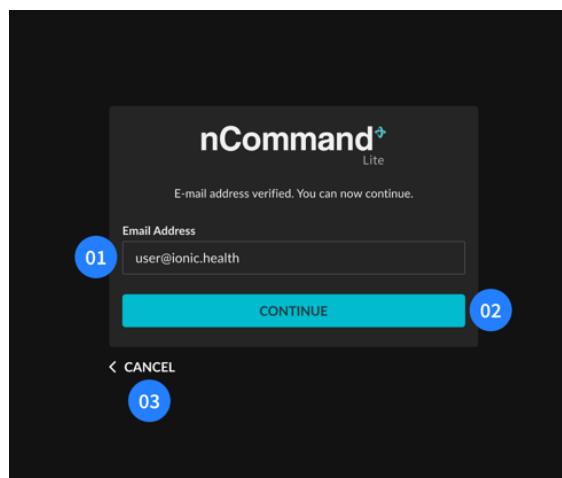
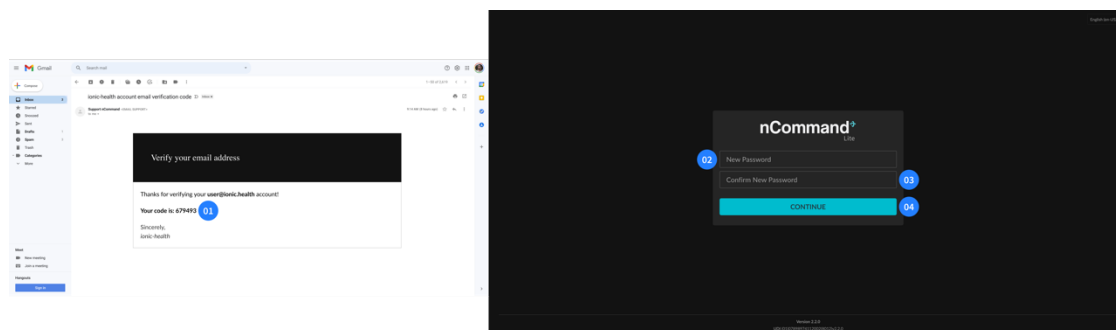
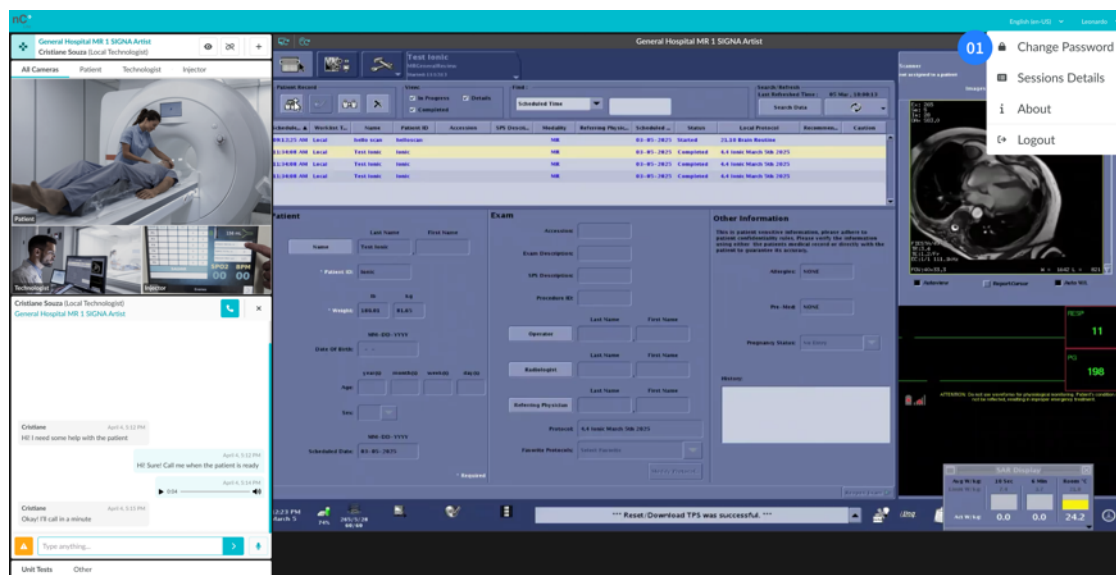


Figura 07: Confirmare pe email
01 – Adresă de e-mail; 02 – Butonul de continuare; 03 – Anulare



**Figura 08: Email cu cod pentru a înregistra parola nouă (stânga) - 01 – Cod 2-FA
Pagina Schimbare parolă (dreapta) - 02 – Parolă nouă; 03 – Confirmare parolă nouă; 04 – Butonul de continuare**

- Schimbarea parolei:** Permite utilizatorilor să își actualizeze parola respectând criteriile specifice, inclusiv cel puțin 3 elemente din următoarele: o literă mică, o literă mare, o cifră și un simbol și trebuie să aibă cel puțin 8 caractere. Sistemul verifică dacă parola nouă îndeplinește aceste criterii și îi transmite un mesaj utilizatorului în caz contrar. În plus, utilizatorii trebuie să confirme parola nouă pentru a preveni erorile de introducere. Pentru a schimba parola, utilizatorul, după procesul de conectare, trebuie să facă clic pe pictograma din colțul din dreapta sus și să aleagă meniul „Change Password” (Schimbare parolă). Acesta va fi deconectat de la platformă și direcționat către o pagină pentru a confirma adresa de e-mail asociată. Sistemul va trimite apoi un e-mail care conține un cod de verificare. După ce completează codul și dau clic pe „Verify code” (Verificare cod), utilizatorii sunt redirecționați spre un ecran unde pot introduce parola nouă.



**Figura 09: Element meniu derulant Schimbare parolă
01 – Schimbare parolă**

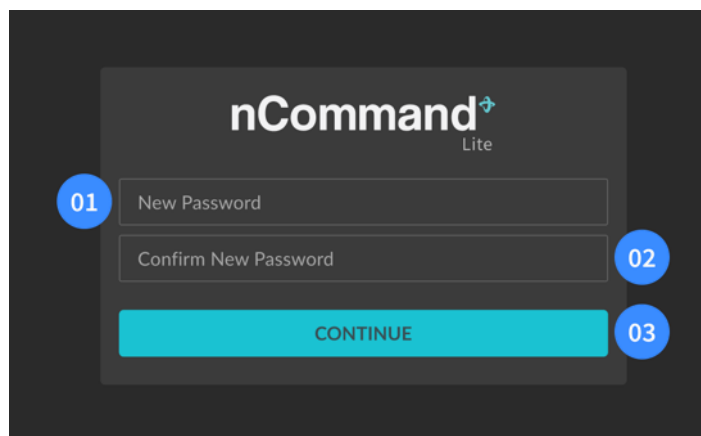


Figura 10: Pagina de schimbare a parolei
 01 – Parolă nouă; 02 – Confirmare parolă nouă; 03 – Buton continuare

Secțiune 3.4 - Accesarea folosind profilul de operator local



AVERTISMENT!

Înainte de a utiliza platforma, contactați telefonic operatorul la distanță.



AVERTISMENT!

Pentru a evita supraîncălzirea, nu așezați niciun obiect în fața ventilatorului computerului e-KVM și, pentru a preveni orice deteriorare, nu așezați niciun obiect pe acesta.



AVERTISMENT!

În timpul sesiunilor de la distanță, operatorul local este responsabil de gestionarea și respectarea regulilor locale de siguranță pentru fiecare tip de examinare și cerințele specifice aferente. Rămâneți întotdeauna prezent în camera de control și/sau în camera de examinare pentru a asigura siguranța, atât a pacientului, cât și a profesioniștilor implicați.



AVERTISMENT!

Mișcările mesei în timpul sesiunii trebuie efectuate numai de către operatorul local atunci când sunt solicitate de sistem. Înainte de a părăsi camera de examinare, operatorul local trebuie să revoce întotdeauna accesul operatorului la distanță.



AVERTISMENT!

Doar operatorul local are dreptul să mute masa pentru a poziționa pacientul în interiorul dispozitivului și pentru a-i permite să iasă în siguranță. Înainte de a părăsi camera de examinare, operatorul local trebuie să revoce întotdeauna accesul utilizatorului de la distanță.

După conectarea la platformă, continuați prin a selecta dispozitivul dorit în caseta Device Selection (Selectare dispozitiv). Dvs. veți fi răspunzător pentru acest dispozitiv, astfel încât să

puteți examina solicitarea operatorului la distanță de a accesa dispozitivul. Când un operator la distanță dorește să acceseze dispozitivul, va apărea o fereastră pop-up ce vă permite să revizuiți toate informațiile prezentate înainte de a accepta sau refuza accesul. Fiți atenți la solicitările primite de la un operator la distanță. Este extrem de important să verificați cu atenție fiecare detaliu. În cazul în care informațiile furnizate nu sunt recunoscute, nu permiteți accesul.

Operatorul la distanță poate accesa dispozitivul folosind unul dintre cele două moduri de acces: **Control** sau **Vizualizare**:

- **Modul Control (Control)** - permite operatorului la distanță să controleze mouse-ul și tastatura, precum și să vizualizeze transmisia dispozitivului. Cu toate acestea, operatorul local nu pierde controlul asupra mouse-ului și tastaturii locale și poate prelua controlul în orice moment.
- **Modul View (Vizualizare)** - permite operatorului la distanță doar să vizualizeze ecranul dispozitivului și să utilizeze chatul pentru comunicare.

După selectarea dispozitivului, utilizatorul are acces la funcția de chat, facilitând comunicarea cu ceilalți utilizatori prin mesaje text, mesaje audio, apel vocal și video.



Figura 11: Ecranul principal al Operatorului local cu notificare de solicitare de acces

01 – Titlu (Solicitare de acces); **02** - Numele solicitantului, rolul și descrierea tipului de acces;
03 – Mesaj: „Do you approve this request?” (Aprobați această cerere?); **04** – Butonul de respingere; **05** – Butonul de aprobare

După aprobare, operatorul local poate revoca accesul operatorului la distanță în orice moment, dând clic pe butonul REVOKE (REVOCARE).

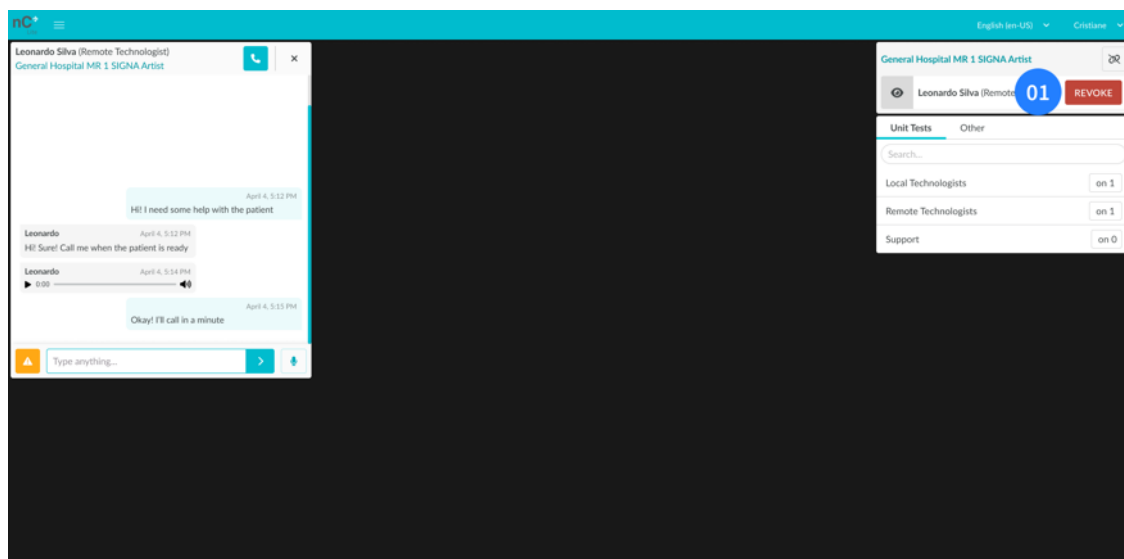


Figura 12: Ecranul principal al Operatorului Local atunci când este conectat la un dispozitiv 01 – Butonul de revocare

În timpul sesiunii de la distanță, operatorul la distanță poate solicita o schimbare a modului de accesare. Pe ecran va apărea o fereastră pop-up de solicitare. O puteți aproba sau respinge. Fiți atenți la prerogativele pe care fiecare mod de acces le permite operatorului la distanță.

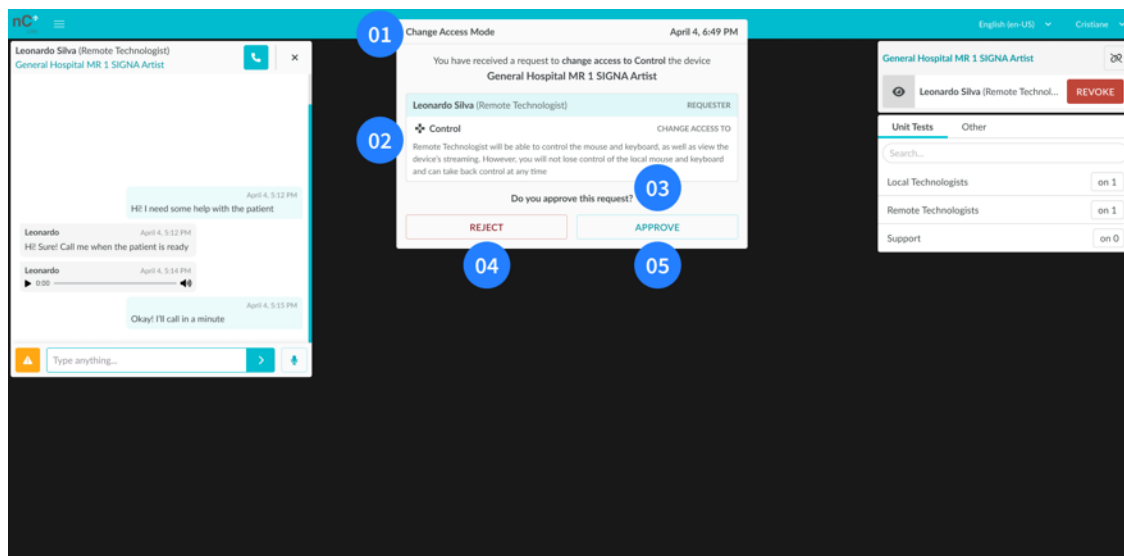


Figura 13: Ecranul principal al Operatorului local cu Solicitare de modificare a modului de acces
01 – Titlu (Schimbare mod de acces); 02 - Numele solicitantului, rolul și descrierea tipului de acces;
03 – Mesaj: „Aprobați această cerere?”; 04 – Butonul de respingere; 05 – Butonul de aprobare

**ATENȚIE!**

În cazul pierderii conexiunii la computerul local, operatorul de la distanță are în continuare acces la *dispozitiv*. Contactați **imediat** operatorul la distanță și cereți-i să se **deconecteze** SAU să se conecteze la un alt computer și **revocați accesul** operatorului la distanță SAU **apăsăți butonul de pornire** pentru a opri computerul e-KVM.

**ATENȚIE!****În cazul întreținerii scannerului:**

Înainte ca inginerul de teren să înceapă orice procedură (fie pe dispozitiv, fie în camera de control), informați operatorul la distanță și revocați-i accesul dând clic pe butonul „REVOKE ACCESS” (REVOCARE ACCES). Apoi, deconectați-vă de pe platforma nCommand Lite.

Dacă nu este conectat niciun operator la distanță, deconectați-vă de pe platforma nCommand Lite înainte de a începe operațiunile de întreținere.

Secțiune 3.5 - Accesarea folosind profilul de tehnician la distanță

**AVERTISMENT!**

Utilizatorul computerului dispozitivului și parola root: ambele trebuie să fie deținute de gazda locală care va primi echipa de instalare.

**AVERTISMENT!**

Mișcările mesei în timpul sesiunii trebuie efectuate numai de către operatorul local atunci când sunt solicitate de sistem. Înainte de a părăsi sala de examinare, operatorul local trebuie să revoce întotdeauna accesul operatorului la distanță.

**AVERTISMENT!**

Doar operatorul local are dreptul să mute masa pentru a poziționa pacientul în interiorul dispozitivului și pentru a-i permite să iasă în siguranță. Înainte de a părăsi camera de examinare, operatorul local trebuie să revoce întotdeauna accesul utilizatorului de la distanță.

**AVERTISMENT!**

Fiți întotdeauna atenți la situația din încăperea prin intermediul camerei video și asigurați comunicarea cu operatorul local înainte de a desfășura orice activitate.

**AVERTISMENT!**

În cazul pierderii conexiunii la computerul local, contactați imediat operatorul local și deconectați-vă.

**AVERTISMENT!****În cazul întreținerii scannerului:**

După ce ați fost notificat cu privire la începerea mentenanței dispozitivului, asigurați-vă că accesul a fost revocat de către operatorul local și deconectați-vă de pe platforma nCommand Lite. Dacă accesul nu a fost revocat, deconectați-vă de la platforma nCommand Lite și contactați imediat operatorul local pentru a-l informa.

**AVERTISMENT!**

Pentru a controla mouse-ul și tastatura de la distanță, modul de acces selectat trebuie să fie Control; în modul View, operatorul la distanță are permisiunea doar de a vizualiza camerele video de redare în flux și locale.

**AVERTISMENT!**

Dacă răspunsul la solicitarea dvs. întârzie mai mult decât era de așteptat, contactați operatorul local prin chat sau telefon.

Locul de muncă al operatorului la distanță include echipamente precum un computer, monitoare (de obicei trei), un mouse, o tastatură și o cască audio.

În fluxul de lucru clinic, *operatorii locali* au contact direct cu pacientul. Aceștia sunt responsabili pentru interacțiunea cu pacientul, poziționare și asigurarea siguranței și a respectării protocolului în timpul procedurilor RMN, CT sau PET/CT, conform standardelor instituționale și de reglementare.

3.5.1. Modul de acces

După conectarea la platformă, selectați dispozitivul la care doriți să vă conectați în caseta Device Selection (Selectare dispozitiv). Se va deschide o fereastră pop-up pentru a alege modul de acces între **Control (Control)** și **View (Vizualizare)**:

- **Modul Control (Control)**– În acest mod, controlul mouse-ului și al tastaturii este activat în plus față de vizualizarea ecranului. Profesioniștii locali păstrează accesul deplin la mouse-ul și tastatura locale și pot prelua controlul în orice moment.
- **Modul View (Vizualizare)** – se poate doar vizualiza ecranul dispozitivului și utiliza chatul pentru comunicare.

Prin selectarea modului de acces, va fi afișată o casetă „Waiting for approval” (Se așteaptă aprobarea), indicând că este necesară aprobarea din partea operatorului local conectat pentru a continua. Acest operator local are autoritate deplină de a aproba sau respinge accesul și de a revoca accesul în orice moment, în cazul în care consideră necesar. Această măsură este esențială pentru a asigura un control strict și pentru a menține siguranța atunci când utilizați dispozitivul.

După selectarea dispozitivului, utilizatorul are acces la funcția de chat, permițând comunicarea prin mesaje text, mesaje audio, apel vocal și video cu ceilalți utilizatori. Utilizatorul nu trebuie să fie aprobat pentru a accesa chat-ul.

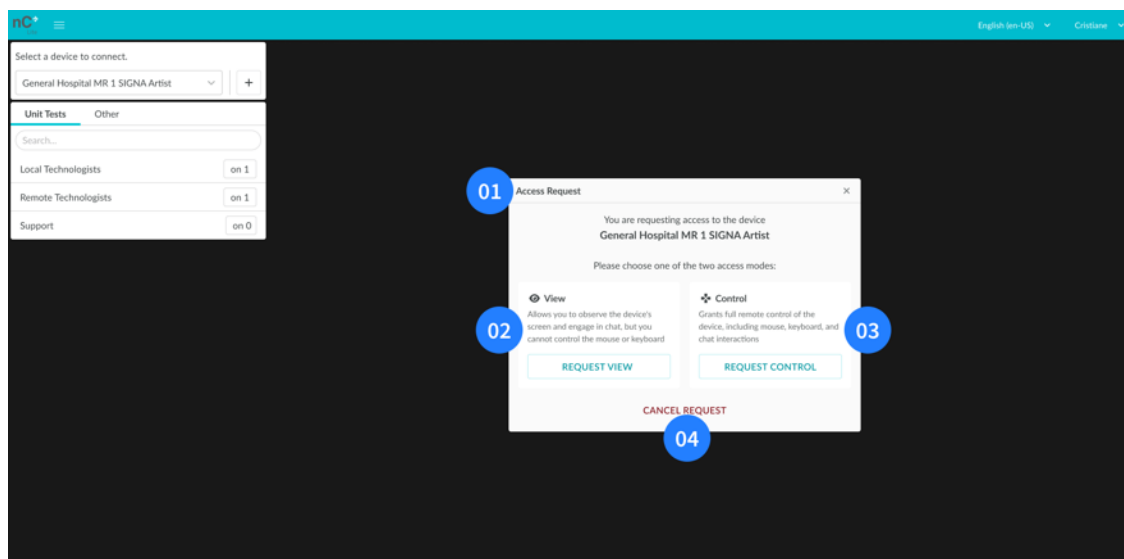


Figura 14: Dialog de solicitare acces pentru Operatorul la distanță

01 – Titlu (Cerere de acces); **02** - Descrierea modului de vizualizare și butonul de solicitare a vizualizării;
03 – Descrierea modului de control și butonul de solicitare a controlului; **04** – Anularea solicitării

După ce accesul la dispozitiv a fost autorizat de către operatorul local, interfața operatorului la distanță va fi actualizată pentru a afișa fluxul video în timp real al dispozitivului și al camerelor asociate. Dacă modul de acces selectat este Control, va fi activată funcționalitatea de operare de la distanță a dispozitivului.

Acest proces asigură o interacțiune eficientă și sigură, permițând utilizarea de la distanță în siguranță a dispozitivului, fără a compromite integritatea sau siguranța pacientului.

Pentru a solicita o modificare a modului de acces în timpul unei sesiuni la distanță, faceți clic pe pictograma corespunzătoare. Operatorul local poate accepta sau respinge solicitarea:

- **Acceptare** – fluxul se va reîncărca, iar conținutul chatului nu se va pierde. Dacă sunteți într-un apel vocal și video, acesta se va încheia și va trebui să fie reluat de unul dintre utilizatori.
- **Refuzare** - va apărea o fereastră pop-up care vă va comunica respingerea din partea operatorului local și accesul curent va rămâne activ.

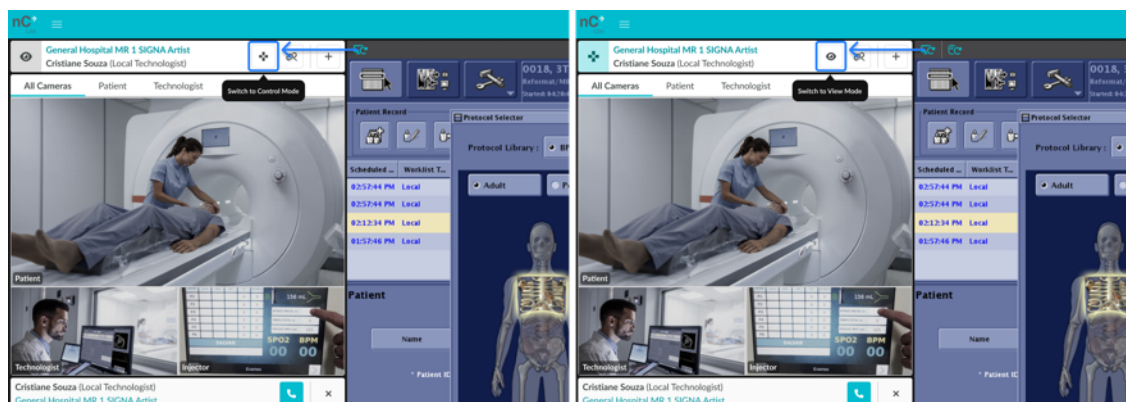


Figura 15: Schimbarea modului de acces

Stânga - Comută la pictograma și tooltip-ul Mod Control / **Dreapta** - Comută la pictograma și tooltip-ul Mod Vizualizare

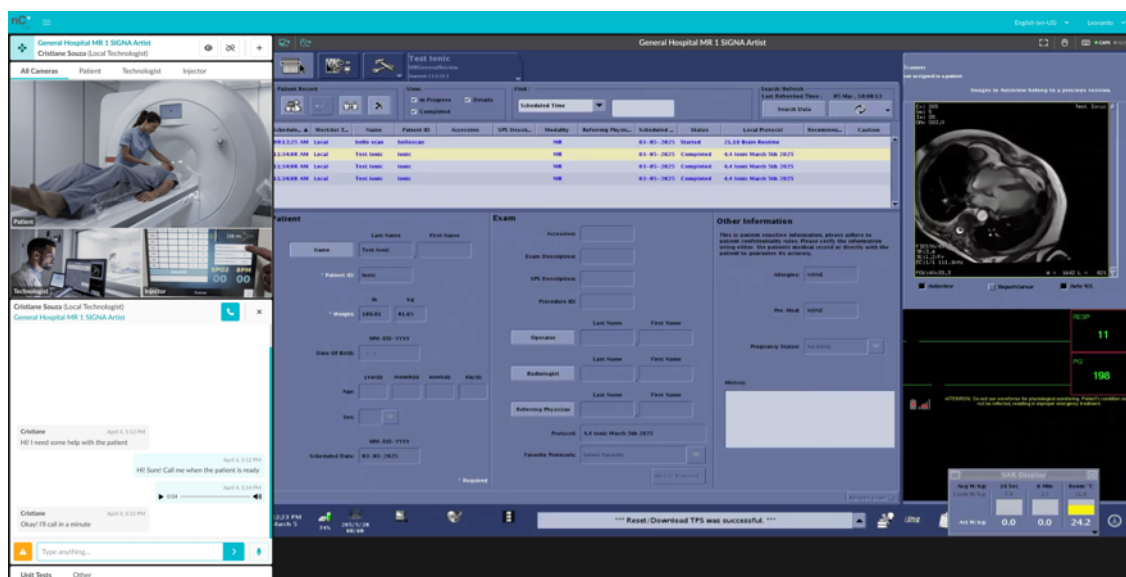


Figura 16: Ecranul principal al Operatorului la distanță atunci când este conectat la un dispozitiv

Când operatorul la distanță solicită accesul și niciun operator local nu este conectat la dispozitiv, platforma afișează un avertisment pop-up. După ce operatorul local se conectează, platforma îl informează pe operatorul la distanță că poate solicita din nou accesul.

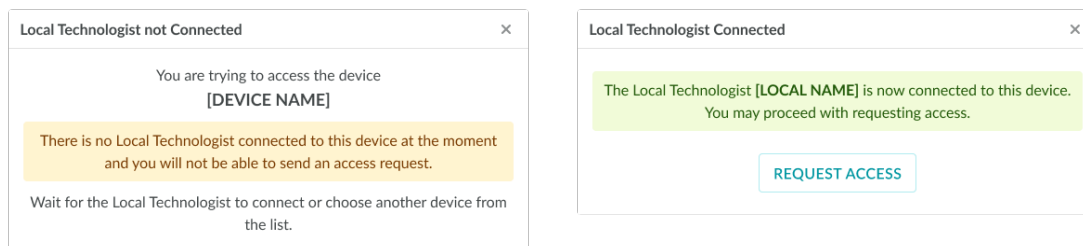


Figura 17: Avertizări ale Operatorului la distanță privind starea conexiunii Operatorului local
Stânga - Notificare care indică faptul că s-a făcut o încercare de accesare a dispozitivului, dar nu este conectat în prezent niciun Operator local.

Dreapta - Notificare care confirmă faptul că operatorul local s-a conectat la dispozitiv după ce anterior nu a fost conectat.

3.5.2. Bara de redare în flux (Streaming)

Bara de redare în flux afișează informații și comenzi cheie legate de sesiunea de redare în flux a dispozitivului. Include butoanele „Reload Streaming” (Reîncărcare redare în flux) și „Mouse Resync” (Resincronizare mouse), numele dispozitivului, rezoluția ecranului și starea curentă a mouse-ului și tastaturii computerului la distanță.

1 - Reîncărcare redare în flux

Această funcție permite operatorilor la distanță să recupereze accesul la dispozitive în cazul unei pierderi de conexiune sau al unei scăderi de performanță. Dacă apare orice tip de deconectare sau desincronizare a ecranului pe computerul dispozitivului, puteți face clic pe pictograma „Reload Streaming” (Reîncărcare redare în flux) situată în bara de redare în flux. Această acțiune va determina platforma să se reconecteze la computerul dispozitivului și să reîncarce, de asemenea, camerele sistemului.

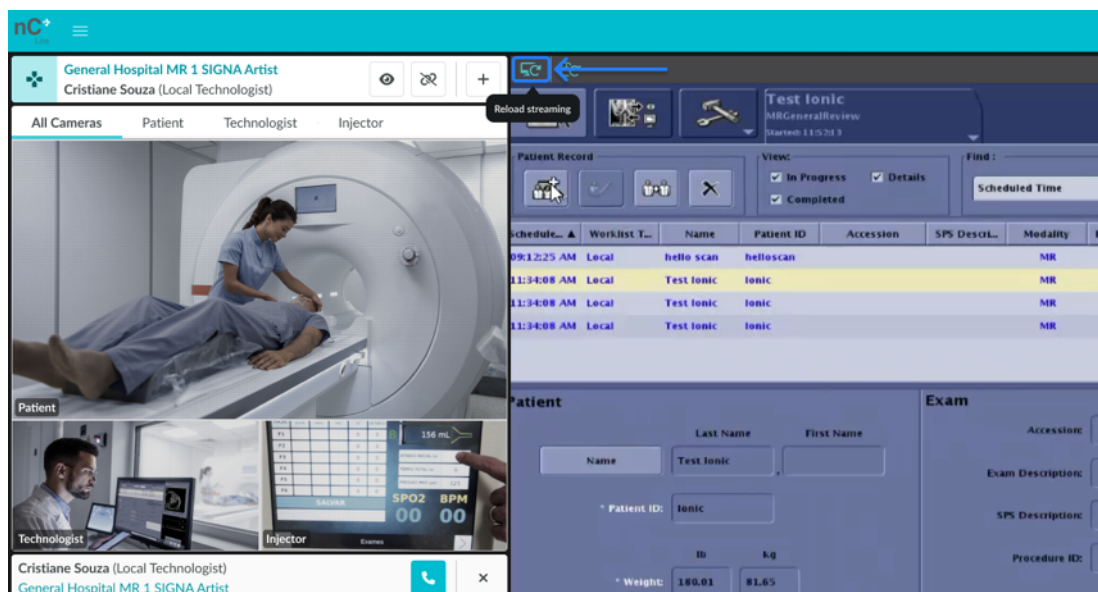


Figura 18: Butonul de reîncărcare a redării în flux

2 - Resincronizare mouse

În cazul în care mouse-ul reacționează lent sau este nealiniat, vă rugăm să faceți clic pe butonul „Mouse Resync” (Resincronizare mouse) aflat pe bara de deasupra ferestrei de streaming pentru a resincroniza mouse-ul dispozitivului cu computerul e-KVM.

O alternativă este să mutați cursorul mouse-ului în afara zonei de streaming și apoi să-l aduceți înapoi, astfel sistemul va resincroniza automat mouse-ul fără a fi nevoie de nicio acțiune suplimentară. De asemenea, puteți apăsa și elibera butonul de scroll al mouse-ului (când există) pentru a declanșa resincronizarea automat. Totuși, această metodă s-ar putea să nu funcționeze pe dispozitive cu două sau mai multe ecrane dacă indicatoarele de la mouse-ul local și al celui de la distanță sunt pe ecrane diferite.

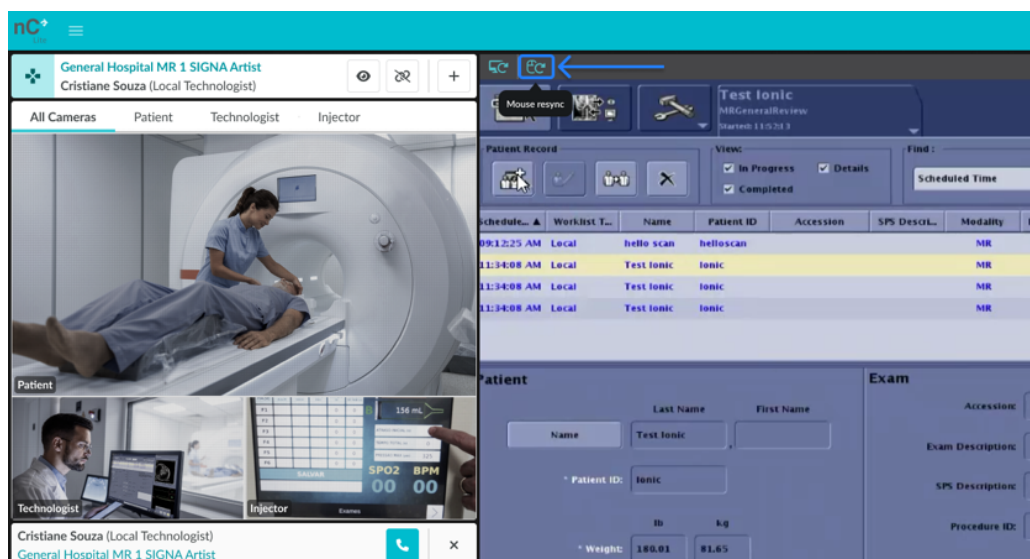


Figura 19: Butonul de resincronizare a mouse-ului

3 - Afișaj redare în flux

Această funcție oferă operatorului la distanță informații despre rezoluția redării în flux originale (de pe dispozitiv) și rezoluția curentă în pixeli afișată pe stația de lucru la distanță.

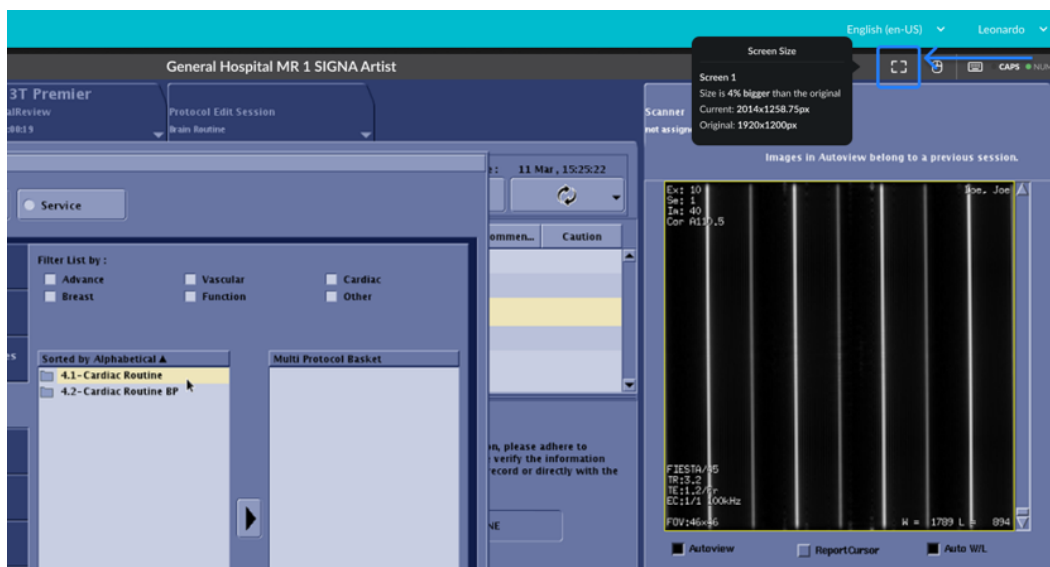


Figura 20: Tooltip pentru informații de redare în flux

4 - Starea mouse-ului și a tastaturii

Această funcție informează operatorul la distanță dacă mouse-ul și tastatura funcționează corect. Împreună cu starea tastaturii, utilizatorul poate vedea dacă tastele de pe tastatură **Caps lock** și **Num lock** de la computerul dispozitivului sunt activate sau dezactivate. Cu toate acestea, această funcționalitate depinde de computerul dispozitivului care furnizează informațiile respective; în scenariile în care aceste informații nu sunt puse la dispoziție de sistemul dispozitivului, starea tastelor **Caps Lock** și **Num Lock** nu va fi afișată. Atât starea mouse-ului, cât și a tastaturii se afișează numai atunci când utilizatorul are acces de tip Control.

Când vă conectați la un dispozitiv, o discrepanță între indicatorii **Caps Lock** și **Num Lock** de pe computerul la distanță și dispozitiv poate duce la un comportament de tastare inconsecvent. Dacă indicatorii apar activați pe dispozitiv, dar nu sunt în fapt activi pe computerul de la distanță, utilizatorul poate tasta cu majuscule pe dispozitiv în timp ce textul apare cu litere mici în chat sau invers. În mod similar, dacă **Caps Lock** este activat pe computerul la distanță, dar dezactivat pe dispozitiv, aceeași problemă va apărea invers.

Pentru a preveni această problemă, asigurați-vă că **Caps Lock** și **Num Lock** sunt fie ambele activate, fie ambele dezactivate înainte de a vă conecta la dispozitiv. Dacă apare o discrepanță, utilizatorul trebuie să se deconecteze de la dispozitiv, să ajusteze starea tastei pe computerul la distanță și apoi să se reconecteze.

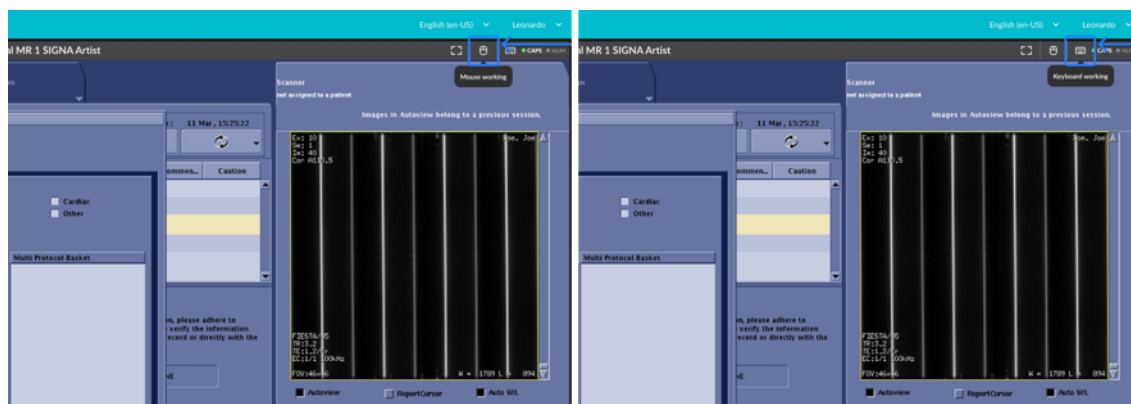


Figura 21: Bară de streaming (redare în flux)
Stânga - Informații despre starea mouse-ului
Dreapta - Informații despre starea tastaturii

3.5.3. Camere video multiple

Această funcție permite operatorului la distanță să vizualizeze mai multe camere în același timp. Dacă sunt disponibile mai multe camere, este posibil să vizualizați doar una și să comutați între ele făcând clic pe meniul cu numele desemnat al fiecărei camere video. Dacă selectați „ALL CAMERAS” (TOATE CAMERELE), toate camerele disponibile vor fi afișate în cadru, iar una dintre ele va fi evidențiată. Pentru a schimba camera evidențiată, trebuie doar să treceți cu mouse-ul peste una dintre camerele din cadrul mai mic și să faceți clic pe „SWITCH CAMERA” (SCHIMBARE CAMERĂ).

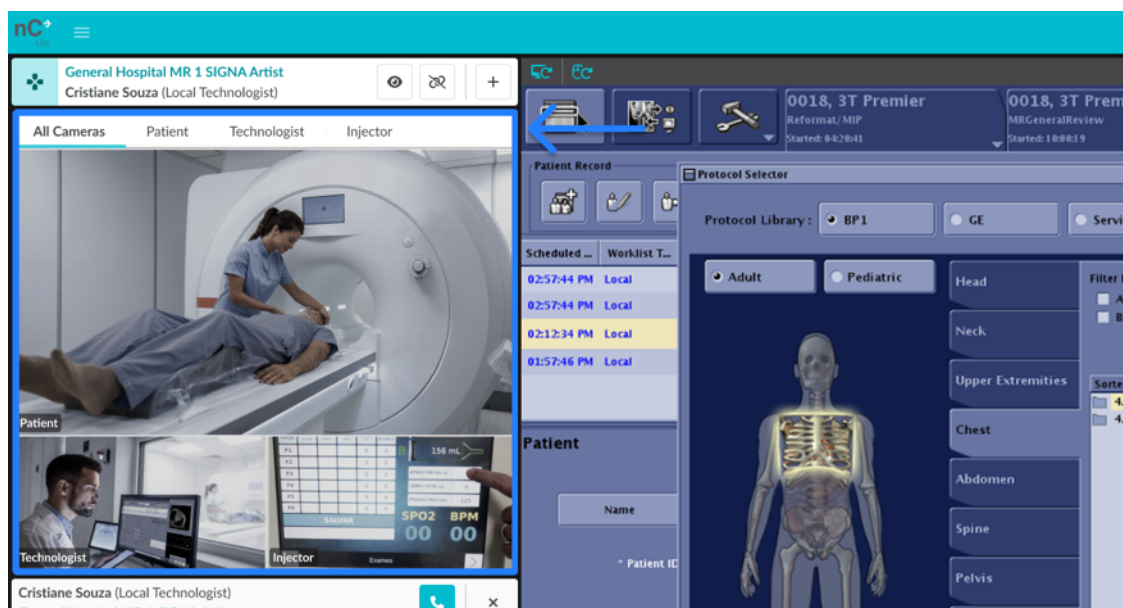


Figura 22: Vedere a cadrului camere multiple

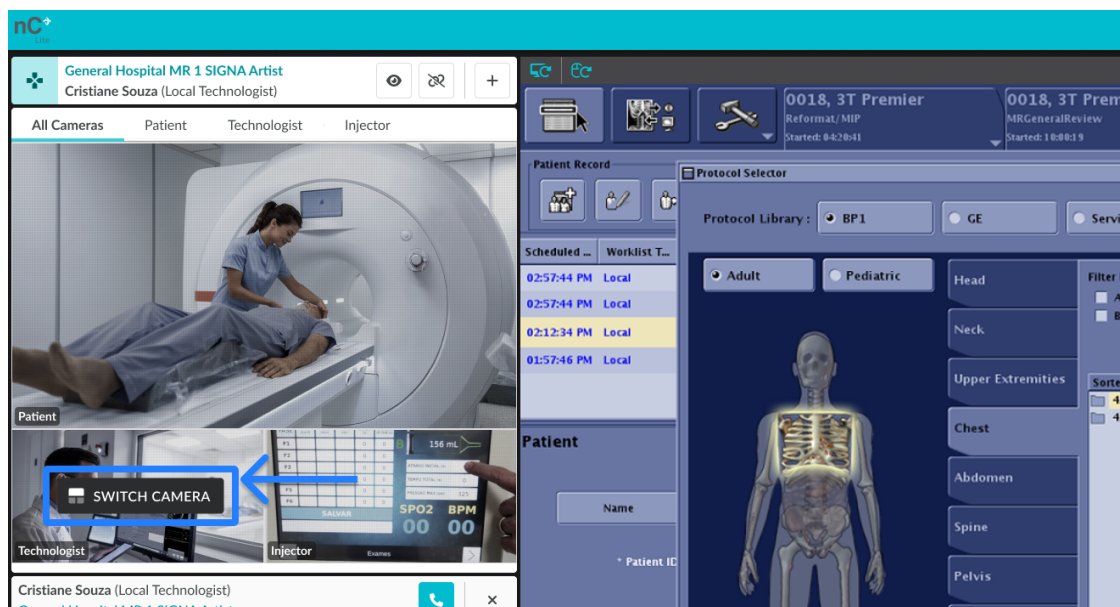


Figura 23: Buton flotant camere multiple „SCHIMBARE CAMERA”

În timpul unei sesiuni active de la distanță, dacă operatorul la distanță o accesează ca **Vizualizare**, există o opțiune de a opri una sau mai multe camere trecând mouse-ul peste camera aleasă și făcând clic pe „TURN OFF CAMERA” (OPRIRE CAMERĂ). Pentru a vizualiza din nou camera, trebuie doar să repetați procesul și să faceți clic pe „TURN ON CAMERA” (PORNIRE CAMERĂ).

NOTĂ: Opțiunea de oprire a camerelor video este disponibilă numai în modul de vizualizare; în modul de control nu este posibilă oprirea camerelor.

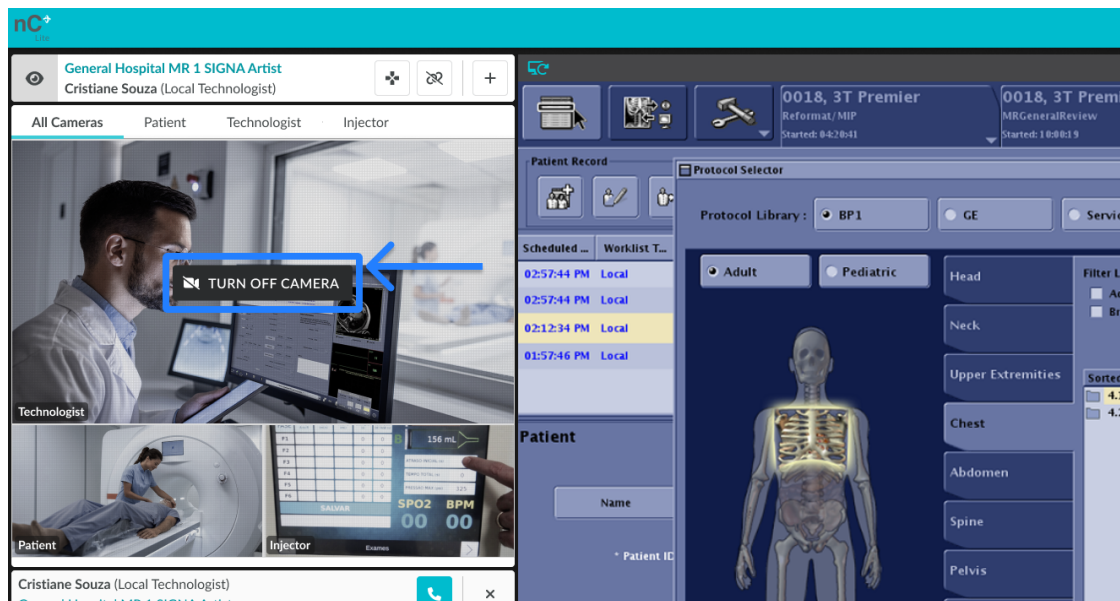


Figura 24: Buton flotant camere multiple "OPRIRE CAMERĂ" în Modul Vizualizare

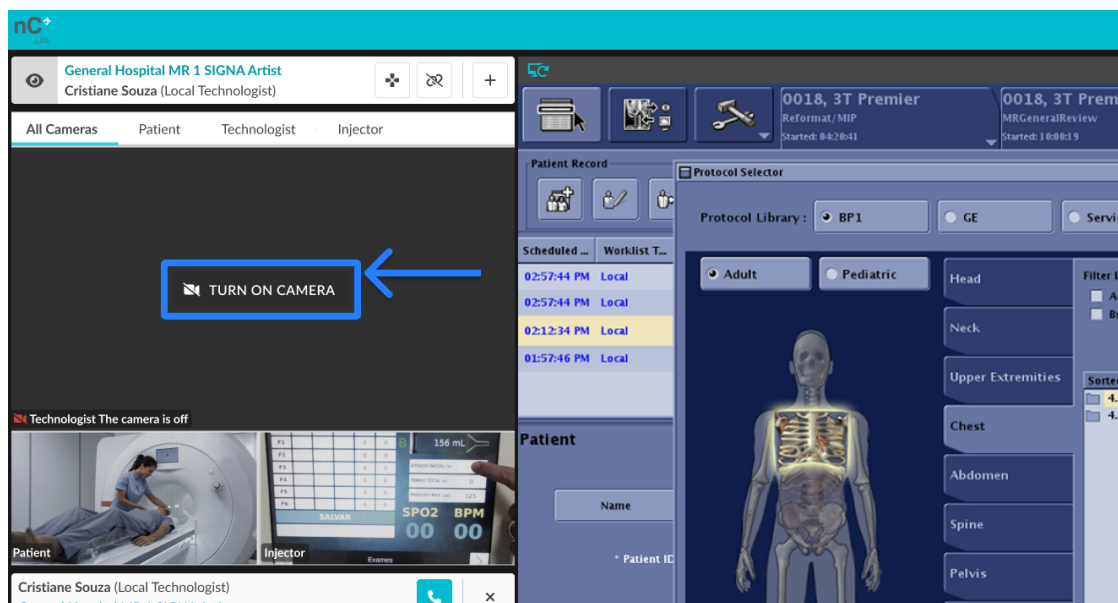


Figura 25: Butonul flotant „PORNIRE CAMERĂ” pentru camere multiple în modul Vizualizare

3.5.4. Deschiderea altui dispozitiv

Permite operatorului la distanță să deschidă o nouă filă de browser a nCommand Lite, permițând astfel utilizatorului să selecteze un dispozitiv nou pentru a efectua simultan mai multe scanări de la distanță. Pentru a deschide un dispozitiv nou pentru acces, trebuie doar să faceți clic pe butonul „Open Another Device” (Deschidere alt dispozitiv) și apoi apare un avertisment pentru ca dvs. să puteți efectua în siguranță această operațiune simultană. Trebuie să citiți avertismentul înainte de a accesa această nouă fereastră.

NOTĂ: Pentru o vizualizare optimă în timpul accesului simultan, se recomandă ca, după ce faceți clic pe „OPEN ANOTHER DEVICE” (DESCHIDERE ALT DISPOZITIV) și confirmați avertismentele cu „OK” și să mutați noua filă pe un alt monitor disponibil.



AVERTISMENT!

Avertisment de siguranță pentru accesarea mai multor scanere

- **Cerință de concentrare intensă:** Accesul simultan necesită o concentrare intensă și comunicare eficientă cu echipele locale.
- **Alegere a diferitelor aspecte:** Evitați accesarea simultană a dispozitivelor cu layout identic sau efectuarea examinării aceleiași regiuni anatomice în același timp.
- **Tragere filă pe alt monitor:** Când accesați un dispozitiv suplimentar, se va deschide o filă nouă. Trageți această filă pe un al doilea monitor, deoarece sistemul este proiectat să fie utilizat cu un ecran separat pentru fiecare dispozitiv.
- **Atenție la alerte:** Acordați o atenție deosebită tuturor alertelor de sistem, deoarece acestea sunt esențiale pentru operarea în condiții de siguranță.
- **Control pe rând:** Puteți vizualiza mai multe ecrane, însă controlul este posibil doar asupra unui singur dispozitiv, la un moment dat.
- **Deschidere chat:** Inițiați întotdeauna chatul atunci când sunteți conectați la un dispozitiv, pentru a asigura o comunicare clară.

- **Câte un apel pe rând:** Alertele de apel vocal apar pe ecranul dispozitivului asociat; doar un singur apel poate fi activ la un moment dat.
- **Siguranță și vigilență:** Acordați prioritate siguranței și mențineți-vă vigilența pe parcursul tuturor operațiunilor.

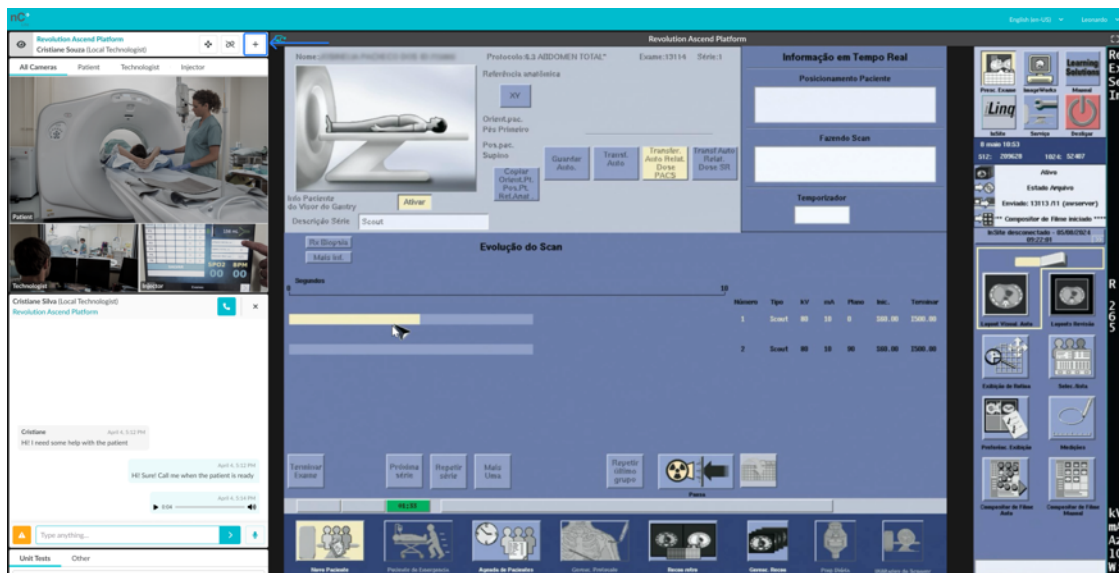


Figura 26: Buton Deschidere alt dispozitiv (+)

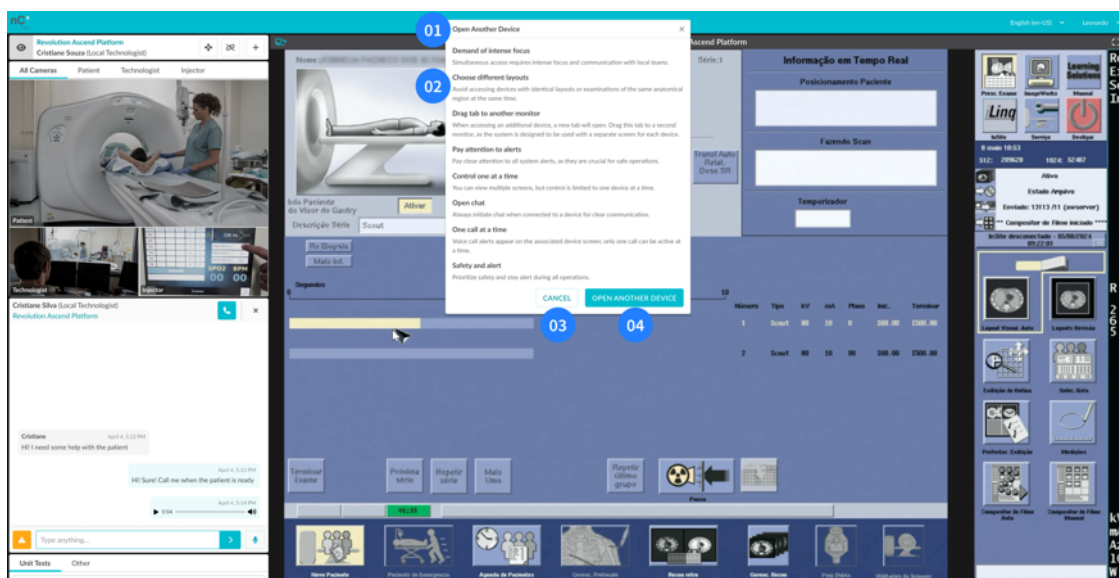


Figura 27: Avertismente privind accesul de pe mai multe dispozitive

- 01 – Titlu (Deschidere alt dispozitiv); 02 – Avertismente de siguranță operațională; 03 – Buton de anulare;
04 – Butonul de deschidere a altui dispozitiv

3.5.5. Verificarea sistemului

Funcția System Check ajută la verificarea faptului că dispozitivul curent, rețeaua și conectivitatea la internet îndeplinesc cerințele pentru utilizarea corectă a nCommand Lite. Se efectuează un test automat rapid care verifică elemente esențiale, precum calitatea internetului, accesul la serverele necesare și stabilitatea conexiunii. Acest instrument poate fi folosit înainte de a începe o sesiune, în timpul instalării sau când se suspectează orice problemă de conexiune. Ajută la asigurarea faptului că platforma va funcționa conform așteptărilor și asistă echipa tehnică dacă este nevoie de depanare.

Notă: Verificarea sistemului ar trebui folosită, de preferat, cu suportul sau la cererea unui profesionist IT. Rularea acestui instrument fără îndrumare tehnică poate duce la interpretarea greșită a rezultatelor.

Pentru a accesa System Check, operatorii locali și operatorii la distanță trebuie să deschidă opțiunea Detalii sesiune din meniul derulant disponibil sub numele de utilizator, situat în colțul din dreapta sus al ecranului principal. Apoi, apasă pe **Open** lângă unealta *System Check*. Odată ce pagina este afișată, faceți clic pe **Run Test** pentru a începe procesul de verificare.

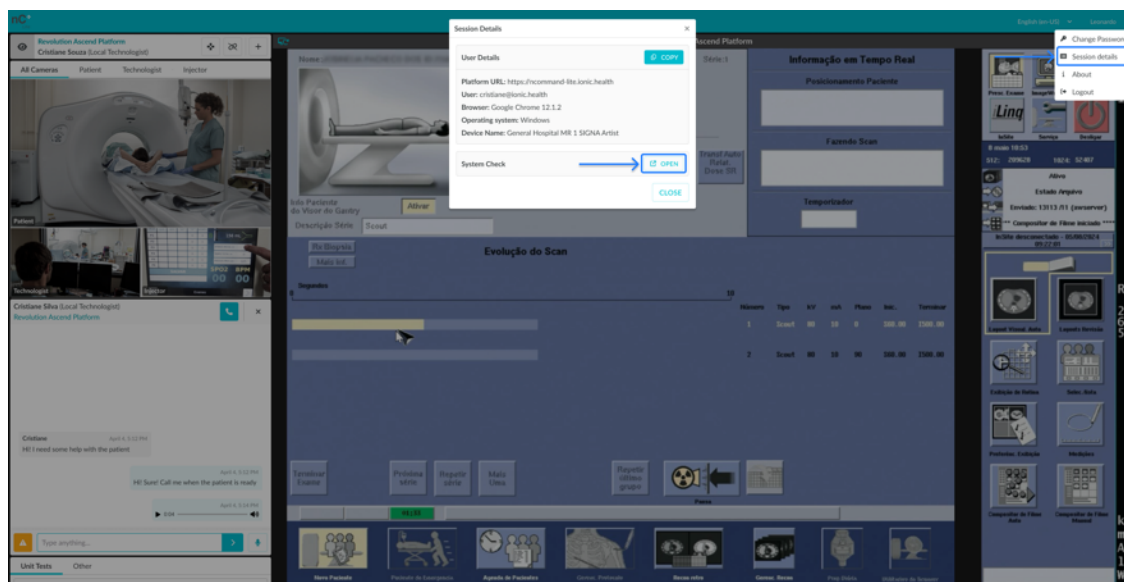


Figura 28: Accesarea verificării sistemului

La utilizarea operatorului la distanță, este posibil să selectați un dispozitiv din ecranul principal al instrumentului pentru a fi inclus în rezultatele testului.



AVERTISMENT!

Înainte de a începe testul, asigurați-vă că dispozitivul selectat nu este folosit în prezent.

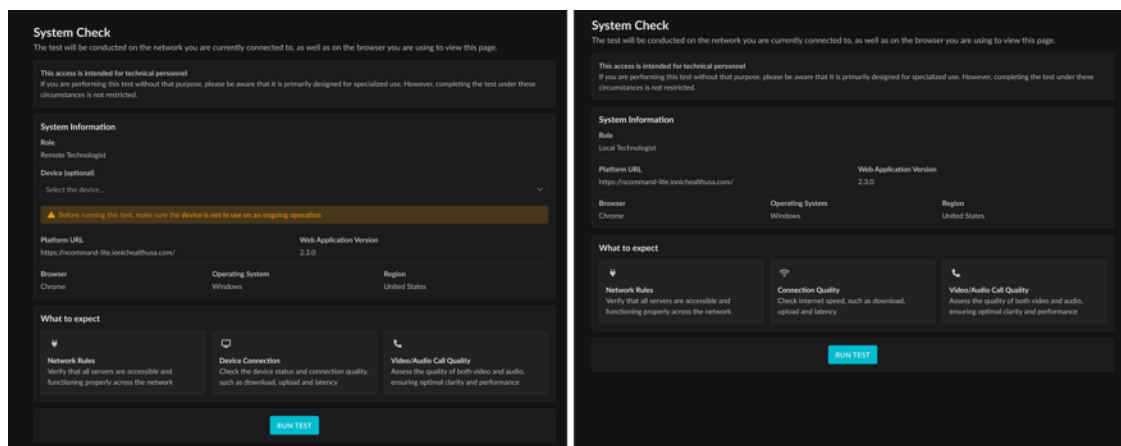


Figura 29: Verificare sistem ecranul principal
Stânga - Operator la distanță / Dreapta - Operator local

După finalizarea testului, pe ecran este afișat un rezumat al rezultatelor. Profesioniștii IT pot analiza aceste informații pentru a identifica posibile probleme care afectează performanța sistemului.

Secțiune 3.6 - Chat

Platforma oferă funcționalități de chat și apel în timp real, cu opțiuni de voce și video, utilizate pentru comunicare eficientă între operatori autorizați. Prin intermediul acestor funcții, operatorii autorizați pot comunica pe toate subiectele legate de fluxul de lucru al sesiunii.



AVERTISMENT!

În caz de defecțiuni, contactați telefonic operatorul local.

La conectarea la un dispozitiv, veți avea acces imediat la lista utilizatorilor de chat, organizată în două file. Pentru clienții cu mai multe centre, fiecare sucursală poate fi configurată drept contract separat. Când este activată, utilizatorii sunt grupați în funcție de contract, utilizatorii din alte contracte apărând în fila „Others” (Altele).

Pentru a iniția o conversație, faceți dublu clic pe numele unui utilizator pentru a deschide interfața de chat, care suportă atât mesageria text, cât și apelurile vocale. Asigurați-vă că sesiunea selectată corespunde dispozitivului corect. Platforma informează utilizatorii dacă conexiunea la rețea devine lentă sau instabilă.



AVERTISMENT!

Înainte de a iniția contactul, verificați numele dispozitivului afișat sub numele utilizatorului, deoarece unii operatori la distanță pot fi conectați la mai multe dispozitive.

Iată instrumentele disponibile pentru comunicare în cadrul platformei:

1. **Apeluri vocale și video:** Faceți clic pe pictogramă pentru a iniția un apel vocal și video de până la 60 de minute între un operator la distanță și un operator local. Conexiunile între utilizatorii cu același profil (Local-Local sau La distanță-La distanță) nu sunt acceptate.

Când un operator local inițiază un apel, operatorul la distanță poate opta să îl accepte sau să îl refuze. În schimb, atunci când un operator la distanță inițiază apelul, acesta este conectat automat, iar operatorul local este notificat—aceste funcții acționează ca un mecanism de siguranță pentru a asigura că operatorul la distanță poate comunica întotdeauna cu persoana prezentă fizic la locație, ca și cum ar fi acolo în persoană.

În mod implicit, microfonul este activ la începutul apelului, în timp ce camera rămâne oprită. Fiecare operator își poate porni sau opri manual microfonul și camera video, în orice moment.

Pentru a efectua cu succes un apel, ambii utilizatori trebuie să aibă un microfon și o ieșire audio funcționale, cu permisiuni de browser activate corespunzător. Dacă lipsește oricare dintre aceste componente, sistemul va informa ambii utilizatori și apelul nu va fi finalizat. O cameră video este opțională—dacă nu este disponibilă sau nu este detectată, sistemul va actualiza pictograma pentru a reflecta faptul că apelul video nu este posibil.

Este permis un singur apel activ per utilizator. Dacă un operator încearcă să inițieze un nou apel în timp ce este deja implicat într-unul, sistemul va bloca încercarea și va afișa o notificare. În mod similar, dacă un utilizator este deja implicat într-un apel și primește un alt apel, apelantul va fi informat că destinatarul nu este disponibil în prezent, iar utilizatorul aflat în apelul în curs va primi o alertă care indică faptul că cineva a încercat să îl contacteze.

2. **Închiderea chaturilor:** Când unul dintre utilizatori închide chatul făcând clic pe butonul de închidere, celuilalt utilizator îi este trimis un mesaj automat și fila de chat este închisă. Acest lucru asigură faptul că ambele părți sunt informate că respectiva conversație s-a încheiat. Când fereastra de chat este închisă, toate mesajele dispar. Dacă o redeschideți în timpul sesiunii, conversația va fi reluată fără mesajele anterioare.
3. **Mesaje text:** Trimiteți mesaje text în câmpul desemnat. Când este trimis un mesaj, apare o pictogramă cu o bifă gri, iar când mesajul este primit de destinatar, este afișată o altă pictogramă cu două bife albastre. Acest lucru permite o comunicare scrisă sigură, clară și concisă între cele două părți.
4. **Atenționare:** Atrageți atenția celuilalt utilizator făcând clic pe butonul cu un semn de exclamare. Această acțiune aplică un efect de vibrație vizuală ferestrei celuilalt utilizator timp de câteva secunde și se trimite automat un mesaj, semnalând urgența sau importanța.
5. **Mesaje audio:** Trimiteți mesaje audio dând clic pe butonul microfon. Acesta este folosit atunci când doriți să transmiteți un mesaj mai personal sau când nu este adecvată tastarea.

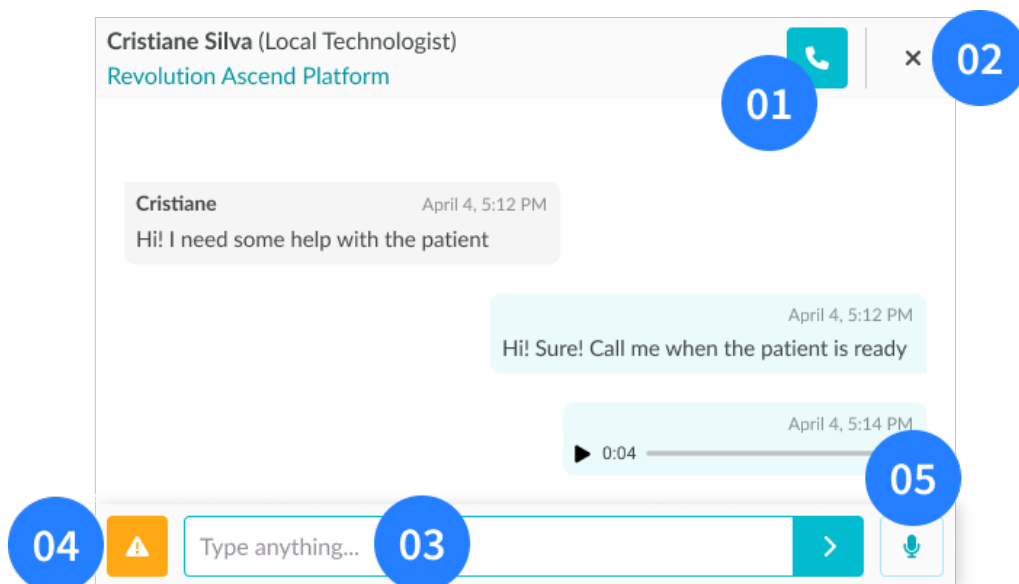


Figura 30: Aspectul ferestrei de chat

01 – Butonul de apel vocal și video; 02 – Butonul de închidere chat; 03 – Caseta pentru mesaje text;
04 – Butonul de atenționare; 05 – Butonul de înregistrare a mesajului audio

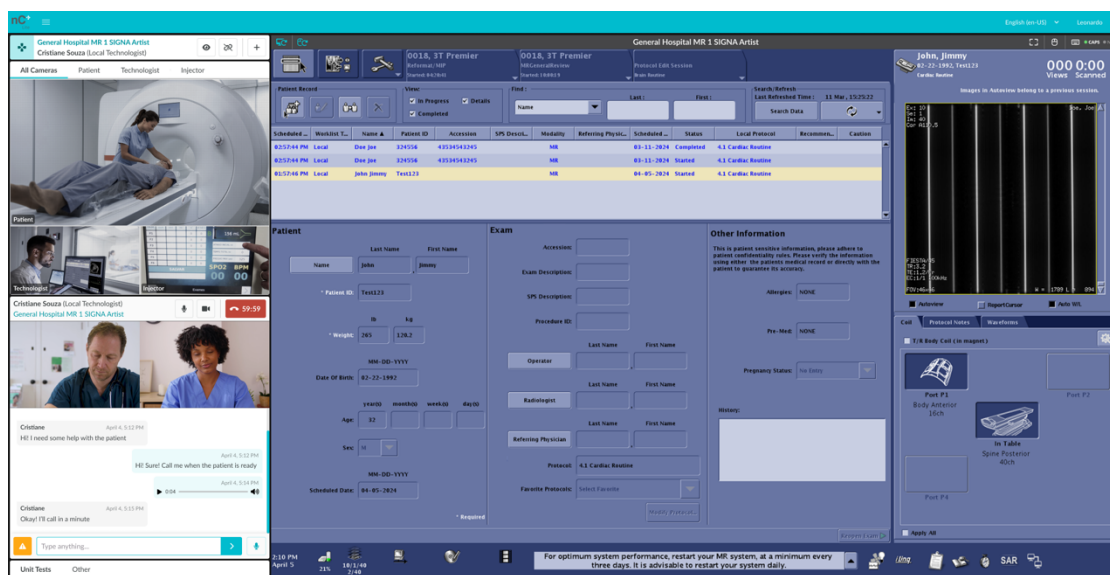


Figura 31: Ecranul principal al operatorului la distanță - Fereastră de chat (colțul din stânga jos)

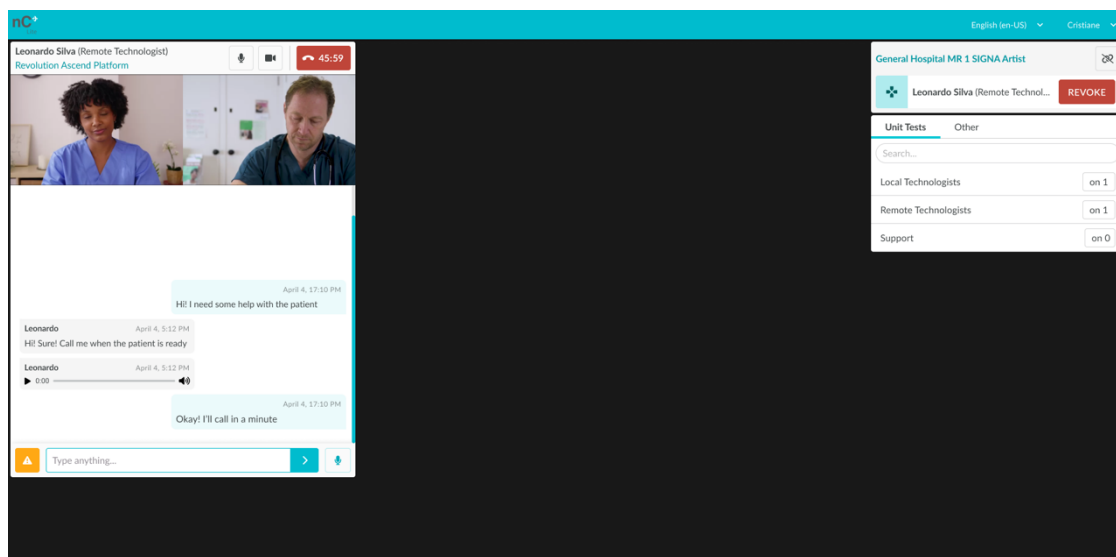


Figura 32: Ecranul principal al operatorului local - fereastră de chat

Probleme cu conexiunea la internet - când unul dintre operatori întâmpină probleme de conexiune la rețea, sistemul va afișa un mesaj și va încerca reconectarea. Dacă conexiunea este restabilită, sistemul va afișa un mesaj **ONLINE**, iar sesiunea la distanță va continua ca de obicei. Cu toate acestea, după mai multe încercări de reconectare, dacă conexiunea nu este restabilită, sistemul va încheia sesiunea activă și va notifica operatorul că a fost deconectat din cauza problemelor legate de internet. În același timp, va notifica și celălalt operator că omologul său a fost deconectat din cauza problemelor de internet.

Secțiune 3.7 - Încheierea sesiunii pe platformă

La sfârșitul sarcinii sale, operatorul autorizat trebuie să se deconecteze de la dispozitiv și să se deconecteze de la platformă.



AVERTISMENT!

Operatorii autorizați nu trebuie să uite să se deconecteze de pe platformă înainte de încheierea serviciului.

Pentru a vă deconecta de la dispozitiv, trebuie să faceți clic pe pictograma de deconectare situată în caseta dispozitivului. Notă: Dacă lucrați ca operator local, asigurați-vă că ați revocat orice acces al operatorului la distanță înainte de a vă deconecta de la dispozitiv.

Pentru a asigura siguranța, veți primi o notificare pentru a confirma că doriți să vă deconectați de la dispozitiv. După confirmare, veți fi redirecționat către ecranul principal, fără niciun dispozitiv selectat.

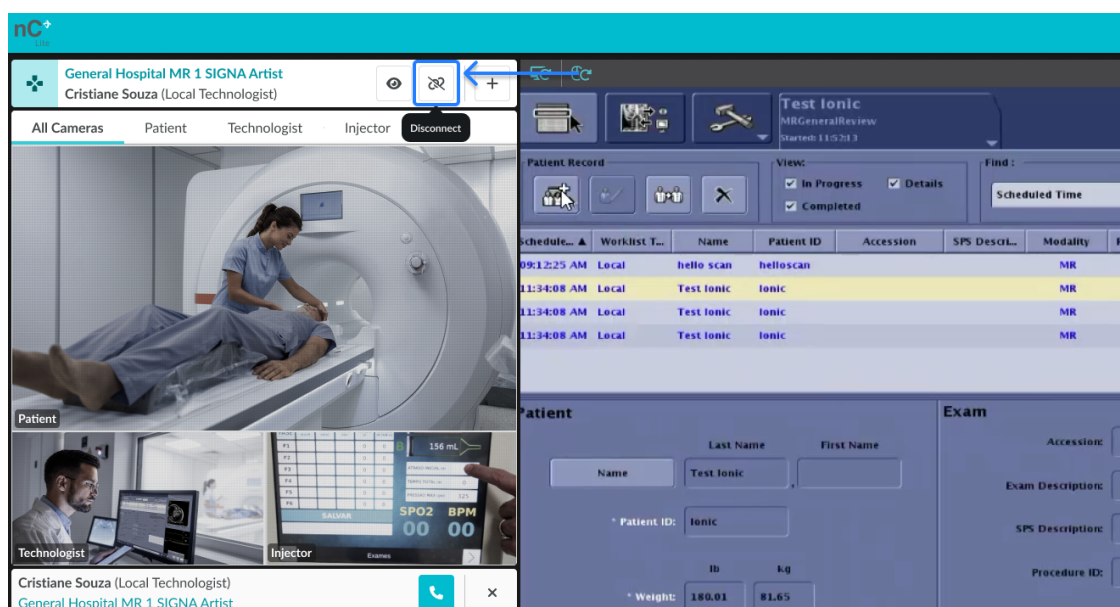


Figura 33: Buton de deconectare - ecranul principal al operatorului la distanță

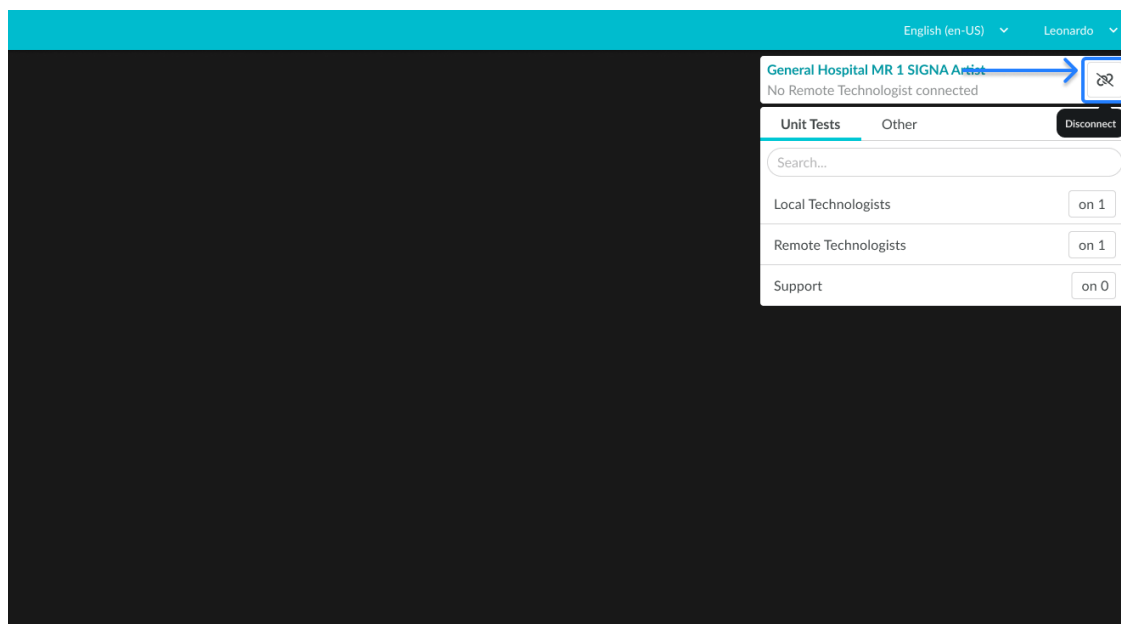


Figura 34: Buton de deconectare - ecran principal operator local



AVERTISMENT!

Înainte de a vă deconecta, asigurați-vă că toate filele suplimentare care au fost deschise sunt acum închise.

Pentru a încheia sesiunea pe platformă, faceți clic pe numele de utilizator situat în colțul din dreapta sus al ecranului și selectați opțiunea „Logout” (Deconectare). Veți primi o notificare pentru a confirma că doriți să părăsiți centrul medical în care lucrați. După confirmare, veți fi redirecționat către pagina de conectare a aplicației, încheind astfel în siguranță activitatea.

nCommand Lite nu controlează sesiunea utilizatorului pe IdP extern și, prin urmare, nu poate efectua o deconectare la nivel de IdP. În situațiile în care utilizatorii partajează același echipament și utilizează conectarea unică (SSO), se recomandă ca fiecare utilizator să selecteze opțiunea „do not stay signed in” (nu rămâneți conectat) în timpul autentificării la IdP extern (dacă este disponibilă) sau să se deconecteze de la IdP după deconectarea din nCommand Lite. Astfel este sigur că niciun utilizator ulterior de pe același dispozitiv nu poate reutiliza accidental o sesiune activă.

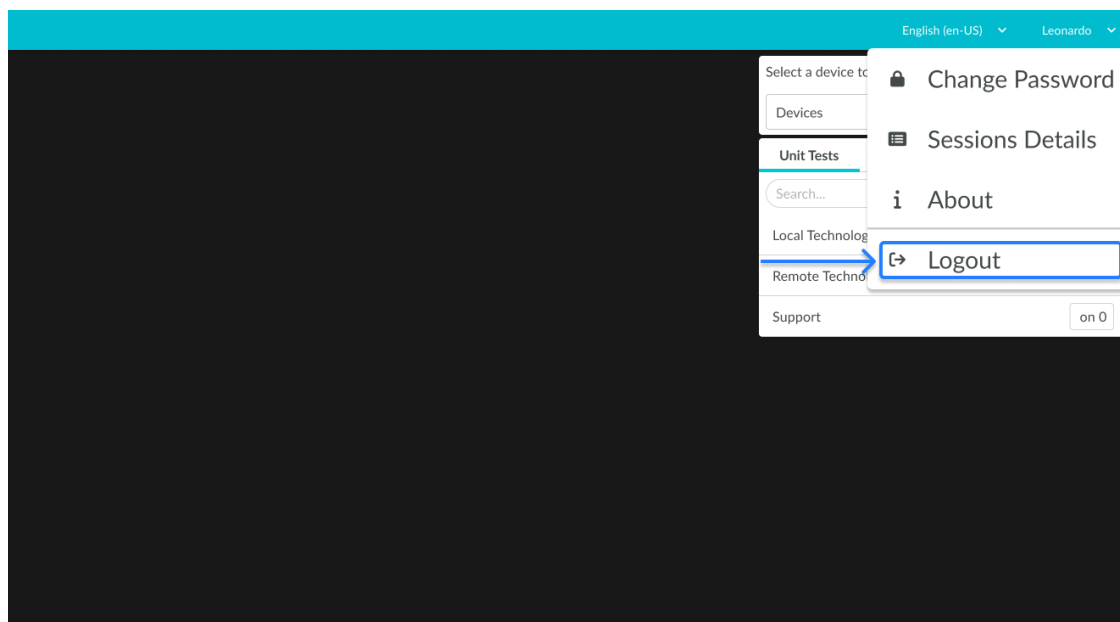


Figura 35: Element meniu derulant Deconectare



AVERTISMENT!

Când utilizați un furnizor de identitate extern pe un computer partajat sau public, după ce v-ați deconectat de la platformă, deconectați-vă și de la furnizorul de identitate. Pentru mai multe informații privind procedura, contactați echipa de asistență IT a organizației dumneavoastră.

Secțiune 3.8 - Instruire operațională

Participarea la programul de instruire este obligatorie pentru toți utilizatorii sistemului nCommand Lite. Înregistrarea utilizatorilor pe platformă este gestionată de echipa IONIC Health și este inițiată numai după confirmarea faptului că utilizatorul a finalizat cu succes instruirea LMS obligatorie și este calificat corespunzător pentru a opera platforma. Acest proces asigură faptul că toți utilizatorii dețin o înțelegere aprofundată a funcționalităților sistemului și sunt pregătiți să utilizeze platforma eficient și în siguranță. Pentru a iniția procesul de înscriere la instruire, vă rugăm să contactați reprezentantul dumneavoastră de vânzări.

Secțiune 3.9 - Instrucțiuni de depanare

UTILIZATOR ȘI PAROLĂ	
Schimbare parolă	Validează îndeplinirea cerințelor privind parola; parola trebuie să fie puternică și sigură, incluzând cel puțin o literă mică, o literă mare, un caracter special și să aibă cel puțin 8 caractere.
Am uitat parola	Verificați-vă căsuța de e-mail: asigurați-vă că utilizați adresa de e-mail corectă și că e-mailul de recuperare a parolei nu a fost filtrat în folderul de spam sau junk. Încercați din nou: Așteptați câteva minute și solicitați un alt e-mail de recuperare a parolei făcând clic pe „Did you Forget your password?” (Ați uitat parola?). Verificați conexiunea la internet: asigurați-vă că aveți conexiune la internet.
Nu am primit e-mailul de bun venit	Verificați dacă e-mailul a ajuns în folderul de spam. Dacă nu este acolo, contactați un utilizator administrator pentru a vă asigura că e-mailul furnizat în înregistrare este corect. Dacă nu este corect, administratorul ar trebui să îl actualizeze și să retransmită e-mailul de bun venit.
Nu am primit codul de autentificare cu doi factori	Faceți clic pe „Resend Code” (Retrimiteră cod) și verificați folderul de spam. Dacă nu îl primiți, contactați un utilizator administrator pentru a verifica dacă e-mailul înregistrat în controlul accesului este corect.
Încercări de conectare depășite	Dacă depășiți numărul permis de încercări de conectare, trebuie să așteptați o perioadă de timp înainte de a încerca din nou.
FURNIZOR DE IDENTITATE EXTERN	
Probleme la conectarea la produs	Dacă întâmpinați probleme la conectare atunci când utilizați un furnizor de identitate extern (IdP), rețineți faptul că procesul de autentificare este gestionat în întregime de IdP și nu de furnizorul produsului, adică: Ionic Health. Ca atare, produsul nu poate ajuta în ceea ce privește acreditările contului, politicile de

	acces, erorile de autentificare sau blocarea contului. În aceste cazuri, ar trebui să contactați echipa de asistență IT a organizației dvs., care poate revizui configurația IdP și vă poate ajuta să rezolvați problema.
Probleme cu acreditările	Orice problemă legată de acreditări (de ex.: parolă uitată, schimbare parolă) trebuie soluționată direct cu echipa de asistență IT a organizației dvs. Aceștia pot revizui configurația IdP și pot asigura asistența necesară.
Probleme cu autentificatorul cu mai mulți factori (MFA)	Orice problemă legată de autentificatorul cu mai mulți factori (MFA) (de ex.: probleme de expirare MFA, MFA nu funcționează, conectare fără a se solicita MFA) trebuie soluționată direct cu echipa de asistență IT a organizației dvs. Aceștia pot revizui configurația IdP și pot asigura asistența necesară.
Acreditările nu funcționează pe platformă	Când utilizați furnizori de identitate externi (IdP), conectați-vă la produs folosind doar IdP. Utilizarea acreditărilor IdP direct pe pagina de conectare a produsului va duce la o conectare nereușită.
MONITORUL COMPUTERULUI SCANNERULUI	
Nu pornește	Verificați conexiunile monitorului la computer și la priza de curent. Se pot produce deconectări. Apăsați din nou butonul de pornire al monitorului.
PLATFORMĂ	
Inaccessibilă	Verificați conexiunea la rețea. Verificați dacă platforma a pornit și dacă a avut loc conectarea.
Latență platformă	Reîmprospătați pagina apăsând Ctrl+F5. Verificați dacă chat-ul unității (unități medicale) este deschis în mai multe file. Dacă da, închideți fila care nu este utilizată. Dacă problema persistă, încercați să vă deconectați de la platformă, să ștergeți memoria cache, să închideți browser-ul și apoi să vă conectați din nou.
Funcții defectuoase	Înainte de a încerca alte proceduri de depanare, ștergeți memoria cache a browser-ului (căutați instrucțiuni pe

	browser-ul curent) după conectare, apoi închideți și redeschideți browser-ul, conectați-vă din nou la platformă și încercați din nou acțiunea.
Upgrade (Îmbunătățire)	După ce platforma a fost actualizată, ștergeți memoria cache a browser-ului (consultați instrucțiunile pentru browser-ul dvs.) înainte de a vă conecta la noua versiune.
AUDIO	
Fără sunet	Asigurați-vă că volumele microfonului și difuzorului unității (unități medicale) sunt reglate la nivelurile adecvate. Verificați dacă browser-ul are permisiunea de a utiliza sistemul audio și microfonul. Verificați căștile să fie conectate și să funcționeze corect.
Latență sunet	Verificați conexiunile electrice și de rețea ale echipamentului. Reîmprospătați pagina browser-ului apăsând Ctrl+F5 și conectați-vă din nou. Dacă problema persistă, încercați să vă deconectați de la platformă, să ștergeți memoria cache, să închideți browser-ul și apoi să vă conectați din nou.
CHAT	
Nu apare chatul	Asigurați-vă că browserul nu este minimizat. În caz contrar, deschideți chatul după ce vă conectați la platforma nCommand Lite. Verificați dacă unitatea (unitatea medicală) a fost selectată și dacă utilizatorul este autorizat să activeze comunicarea prin chat. Asigurați-vă că permisiunile audio și pentru microfon ale browser-ului sunt acceptate.

	Verificați conexiunile cablului, care poate fi deconectat. Reîmprospătați pagina browser-ului apăsând Ctrl+F5 și reconectați-vă la platformă. Verificați dacă chatul unității este deschis în mai multe file. Dacă da, închideți fila care nu este utilizată.
Întârziere chat	Reîmprospătați pagina browser-ului apăsând Ctrl+F5 și reconectați-vă la platformă. Dacă problema persistă, încercați să vă deconectați de la platformă, să ștergeți memoria cache, să închideți browser-ul și apoi să vă conectați din nou. Verificați conexiunile cablului, care poate fi deconectat.
Probleme la trimiterea mesajelor audio	Verificați permisiunile browser-ului pentru sistemul audio și microfon și asigurați-vă că atât microfonul, cât și dispozitivele audio sunt conectate la computer. Dacă permisiunile browser-ului trebuie ajustate, apăsați Ctrl+F5 pentru a solicita browser-ului să recunoască modificările după reîncărcarea paginii.
Apelul vocal nu putut fi inițiat	Verificați conexiunea la internet și vedeți dacă a fost afișată vreo notificare care explică motivul pentru care apelul nu a fost inițiat. Asigurați-vă că aveți un dispozitiv audio conectat și că permisiunile pentru sistemul audio și microfon sunt active în browser. Dacă problema persistă, reîmprospătați pagina folosind Ctrl+F5 pentru a încerca din nou.
Utilizatorul nu este găsit în chat	Dacă nu puteți localiza un utilizator în chat, faceți clic pe fila „Others” (Altele) pentru a vă asigura că nu este afișat acolo. Utilizatorii asociați cu alte contracte apar separat în lista de contacte. Dacă utilizatorul nu apare în lista de contacte după selectarea dispozitivului,

	apăsați Ctrl+F5 pentru a reîmprospăta ecranul și selectați din nou. Asigurați-vă că aveți conexiune la internet.
SOLICITAREA ACCESULUI LA DISPOZITIV	
Platforma nu a recunoscut că operatorul local este conectat	Verificați sub opțiunea „Others” (Altele) pentru a confirma dacă utilizatorul local este conectat. Dacă utilizatorul este într-adevăr conectat, dar primiți în continuare mesajul că utilizatorul local nu este conectat la scanner, reîmprospătați ecranul apăsând Ctrl+F5 și solicitați utilizatorului local să repete aceeași instrucțiune. Apoi, selectați din nou dispozitivul și cereți utilizatorului local să selecteze din nou dispozitivul. Dacă problema persistă, contactați asistența pentru a verifica rețeaua.
Cererea de acces nu este trimisă	Reîmprospătați pagina apăsând Ctrl+F5 și confirmați cu utilizatorul local prin chat că cererea de acces este primită. Dacă problema persistă, contactați asistența pentru asistență suplimentară.
DISPOZITIV DE REDARE ÎN FLUX (COMPUTER E-KVM)	
Dispozitivul de redare în flux - streaming (COMPUTER e-KVM) nu funcționează	Faceți clic pe butonul „Reîncărcare redare în flux” de pe platformă. Asigurați-vă că sursa de alimentare neîntreruptă și stabilizată (unitate medicală) și/sau dispozitivul de redare în flux sunt conectate și pornite corect. Opriți dispozitivul de streaming și toate celelalte echipamente și porniți din nou. Reîmprospătați platforma.
Dispozitiv de redare în flux lent	Faceți clic pe butonul „Reîncărcare redare în flux” de pe platformă. Reîmprospătați pagina folosind Ctrl+F5 și reconectați-vă la platformă. Verificați calitatea conexiunii la rețea. Pentru a valida starea rețelei, este posibil să se efectueze un test ping pe dispozitiv pentru a verifica pierderea pachetelor. Dacă există probleme legate de internet, este posibil ca platforma să nu

	funcționeze așa cum doriți. Reîmprospătați pagina web și solicitați din nou acces utilizatorului local.
Pierderea ieșirii video	Este posibil ca o descărcare electrostatică să ducă la pierderea imaginii. După o repornire a sistemului, comunicarea și redarea în flux video ar trebui să fie restabilite automat.

Secțiune 3.10 - Metode de curățare a echipamentelor

- Înainte de a începe procesul de curățare, asigurați-vă că toate echipamentele sunt deconectate de la priza de curent.
- Nu utilizați produse abrazive.
- Nu scufundați niciun echipament sau periferic în niciun tip de lichid.
- Eliminați materialele de curățare conform reglementărilor pentru eliminarea deșeurilor periculoase.
- Nu se recomandă să folosiți dezinfectant prin pulverizare, deoarece vaporii pot pătrunde în echipament și pot provoca un scurtcircuit sau coroziune.
- Acest produs nu este steril.

Capitolul 4 Securitatea cibernetică și confidențialitatea

Secțiune 4.1 - Riscurile de securitate și confidențialitatea

Sistemul nCommand Lite implementează mai multe măsuri tehnice și organizatorice pentru a proteja informațiile procesate.

Sistemul a fost certificat conform ISO/IEC 27001 și ISO/IEC 27701 și urmează o abordare de confidențialitate din faza de concepere. Susține conformitatea cu legislația privind protecția datelor medicale și reglementările de securitate cibernetică aplicabile în UE, SUA, Regatul Unit, Elveția, Brazilia, Emiratele Arabe Unite, Arabia Saudită, Australia și Noua Zeelandă.

Cu toate acestea, utilizatorii trebuie să adopte cele mai bune practici pentru a preveni expunerea inutilă a datelor sensibile.

- Evitați partajarea informațiilor personale sau sensibile, cu excepția cazului în care este strict necesară.
- Asigurați-vă că comunicațiile și accesul la sistem au loc în medii securizate.
- Dacă suspectați orice activitate rău intenționată, anunțați imediat echipa responsabilă.

Secțiune 4.2 - Protecția datelor cu caracter personal (conformitate cu GDPR/HIPAA)

Sistemul **nCommand Lite** respectă toate legile și reglementările aplicabile privind confidențialitatea și protecția datelor din regiunile în care operează, inclusiv, dar fără a se limita la, cerințele GDPR, HIPAA, LGPD și ISO/IEC 27701. Toate activitățile de procesare a datelor se desfășoară sub rolurile "**Procesator**" și "**Sub-Procesator**" așa cum sunt definite de GDPR, cu o segregare regională strictă pentru a asigura conformitatea și a preveni transferurile transfrontaliere neautorizate de date.

Ce date sunt colectate?

- **Utilizatori:** Nume, adresă de e-mail și companie (strict pentru autentificare și gestionarea accesului).
- **Datele pacientului:** Doar transmisiile examinărilor medicale prin redare în flux în timp real, fără stocarea datelor.

Cum sunt utilizate și protejate datele?

- Datele sunt utilizate exclusiv pentru **autentificare, controlul accesului și trasabilitatea sesiunii**.
- Transmiterea informațiilor este securizată prin **criptarea AES-256 pentru stocare și TLS 1.3 pentru datele aflate în tranzit**.
- **Accesul este restricționat** și urmează **principiul privilegiului minim (RBAC)**.

- Criptare integrală asigurată pentru fluxuri video și de control P2P prin WebRTC.
- Furnizorii de cloud autorizați (de exemplu, Microsoft Azure) prelucrează date limitate în baza unor garanții contractuale stricte.

Utilizatorilor li se acordă următoarele drepturi:

- **Acces și corectare** a informațiilor personale.
- **Cerere de ștergere a datelor**, dacă este cazul.

Dacă aveți întrebări, trimiteți un e-mail la privacy@ionic.health pentru a contacta DPO Ionic Health. Toate solicitările sunt rezolvate în termen de 30 de zile, care se poate prelungi conform GDPR.

Secțiune 4.3 - Gestionarea accesului și autentificarea

Utilizatorii sunt responsabili pentru definirea **rolurilor și permisiunilor de acces** pentru echipele lor, asigurând revizuii periodice și documentarea accesului permis.

Cele mai bune practici și controale

- Respectați **principiul privilegiului minim (RBAC)**, asigurându-vă că utilizatorii au doar accesul necesar.
- **Autentificarea cu mai mulți factori (MFA)** este obligatorie pentru accesul administrativ și recomandat pentru toți utilizatorii.
- **Parolele puternice** sunt obligatorii, cu cel puțin **8 caractere, inclusiv litere mari și mici, cifre și simboluri**.
- **Nu partajați acreditările**.
- Permisele de acces sunt monitorizate și revizuite periodic.

Monitorizarea: accesul, modificările permisiunilor și activitățile importante sunt documentate în jurnalele de securitate ale sistemului. Jurnalul este păstrat timp de cel puțin 7 ani, în conformitate cu HIPAA, GDPR și alte reglementări aplicabile. Acestea sunt utile pentru auditul intern, analiza criminalistică și raportarea de reglementare. Jurnalul este protejat împotriva manipularii și stocat în medii securizate cu control al accesului.

Secțiune 4.4 - Controlul Accesului la verificarea sistemului

Funcția System Check este accesibilă exclusiv prin **nCommand Lite Web Application** și necesită acreditări valide pentru autentificare. Accesul este permis exclusiv rolurilor autorizate — *Operator la distanță, Operator local, Admin, Supraveghetor de rol și Utilizator verificare sistem*.

Rolul *Utilizator verificare sistem* este conceput cu permisiuni restricționate, oferind acces exclusiv la funcții de diagnostic legate de validarea rețelei și verificarea conectivității. Acest lucru asigură că detaliile rețelei, informațiile de pe lista albă și datele tehnice ale sistemului nu sunt niciodată expuse persoanelor neautorizate.

Toate cererile de acces sunt autentificate prin Azure AD B2C, cu autentificare multi-factor (MFA) și politici adaptive de acces condiționat gestionate de Microsoft Entra ID. Complexitatea parolei urmează politica de securitate a organizației, necesitând cel puțin opt caractere, inclusiv litere

mari și mici, cifre și simboluri. Parolele expiră la fiecare 90 de zile, iar sesiunile se deconectează automat după 24 de ore de inactivitate, extensibil până la 90 de zile cu utilizare continuă.

Secțiune 4.5 - Segregarea regională a datelor și păstrarea jurnalelor

Platforma **nCommand Lite** menține o segregare regională strictă a datelor pentru a preveni transferurile transfrontaliere neautorizate sau inutile. Mediile sunt izolate pe regiuni, asigurând conformitatea cu reglementările aplicabile.

Toate jurnalele de acces, înregistrările de activitate și evenimentele de securitate sunt păstrate pentru minimum șapte (7) ani, în conformitate cu reglementările aplicabile privind protecția datelor în domeniul sănătății. Jurnalele sunt stocate în medii sigure, cu acces controlat și protejate împotriva accesului nepermis. Aceste informații susțin investigațiile criminalistice, auditurile de conformitate și raportarea de reglementare.

Secțiune 4.6 - Securitatea și integritatea datelor

Sistemul nCommand Lite asigură confidențialitatea, integritatea și disponibilitatea datelor prin practici de securitate standard pentru domeniul respectiv.

Utilizatorii ar trebui să asigure conformitatea cu protocoalele de securitate, să revizuiască în mod regulat politicile de acces și să raporteze orice anomalii. Sistemul monitorizează continuu activitățile, iar administratorii trebuie să aplice politicile de securitate pentru a menține o apărare puternică împotriva potențialelor amenințări.

Sistemul este protejat prin monitorizare continuă, 24/7, realizată de un Centru de Operațiuni de Securitate (SOC) dedicat, dotat cu funcționalități SIEM pentru detectarea și gestionarea amenințărilor.

Secțiune 4.7 - Răspunsul la incidentele de securitate

Sistemul include un plan documentat de răspuns la incidente, aliniat la ISO 27035 și NIST CSF. În cazul unor incidente de securitate, cum ar fi accesul neautorizat sau erorile de sistem, utilizatorii trebuie să urmeze acești pași:

Cum se identifică un incident?

- **Acces neautorizat** detectat în jurnalele de activitate.
- **Încercări suspecte de conectare** sau eșecuri de autentificare repetate.
- **Comportament neobișnuit al sistemului**, cum ar fi acțiuni neașteptate sau defecțiuni.

Cum se raportează un incident?

Înregistrați imediat evenimentul prin canalele de asistență disponibile (Capitolul 5).

Dacă se confirmă o breșă de date personale, IONIC, acționând ca subprocesator, va notifica GE în calitate de Procesator în termen de 48 de ore, furnizând toate dovezile relevante, detaliile de impact și măsurile de atenuare. La rândul său, GE este responsabilă pentru notificarea Controlorului (clientul) în conformitate cu cerințele legale și contractuale aplicabile.

Capitolul 5 Canalele de servicii

Indiferent dacă aveți nevoie de ajutor cu o problemă tehnică, cu un pas neclar al procesului sau pentru îndrumări suplimentare, echipa noastră este gata să vă ajute. Ne puteți contacta prin telefon, e-mail sau prin platforma ITSM, oricare variantă vă este mai la îndemână. Specialiștii noștri sunt instruiți să ofere asistență personalizată, asigurându-se că orice problemă este rezolvată rapid și eficient.

Numere de telefon

Statele Unite ale Americii	+1 (216) 2421223
Brazilia	+55 12 3600 0181
Europa (Portugalia)	+351 (300) 528 410
Australia	+1 (216) 2421223
Noua Zeelandă	+1 (216) 2421223

Platforma ITSM

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

E-mail

helpdesk@ionic.health



AVERTISMENT!

Orice incident grav legat de utilizarea acestui dispozitiv trebuie raportat atât producătorului, cât și autorității sanitare/autorității competente din regiunea unde este instalat dispozitivul.

Pentru a raporta producătorului: fie contactați reprezentantul local de service, fie raportați la: helpdesk@ionic.health

Vă rugăm să furnizați următoarele informații:

- Numărul de versiune a sistemului, afișat pe ecranul de conectare;
- Data incidentului;
- Descrierea incidentului, inclusiv orice impact/vătămare a pacientului sau utilizatorului;
- Datele dvs. de contact (unitate, adresă, nume, funcție și număr de telefon al persoanei de contact).

Capitolul 6 Informațiile legale și de reglementare

Producător



nCommand Lite

IONIC HEALTH TECHNOLOGIES S.A.

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

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

Tehnician responsabil

Alexandre Seiji Fukuda Ribas
CREA-SP: 5071085437

ANVISA

82585300004

Importator (SUA)



nCommand Lite System

IONIC HEALTH USA INC.

11201 Cedar Avenue, STE 600
Cleveland, OH 44106
SUA

+1 (216) 242 1223

Reprezentant UE/Importator



nCommand Lite



Numărul de identificare al organismului
notificat: 2803

EUROPE IONIC HEALTH DIGITAL TECHNOLOGIES, LDA

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

+351 (300) 528 410

Reprezentant autorizat în Elveția (CH-REP)/Importator**CH REP****REF**

nCommand Lite

FREYR LIFE SCIENCES GMBH

Bahnhofplatz
CH-6300 Zug
Elveția

Persoană responsabilă / Importator Regatul Unit**REF**

nCommand Lite

FREYR LIFE SCIENCES LTD

9 Greyfriars Road
Reading, Berkshire
RG1 1NU
Anglia, Regatul Unit

Sponsor din Australia**REF**

nCommand Lite

TAEVAS LIFE SCIENCES PTY LTD

46 Dora St
Blacktown NSW 2148
Australia

Sponsor din Noua Zeelandă**REF**

nCommand Lite

TAEVAS LIFE SCIENCES LIMITED

Nivelul 3, 1 Margaret Street
Lower Hutt 5010
Noua Zeelandă

UDI-DI DE BAZĂ: 7898974112NCLITE2L**Solicitarea unui exemplar tipărit**

Exemplarele tipărite ale Manualului de utilizare nCommand Lite vor fi furnizate la cerere, fără costuri suplimentare. Contactați reprezentantul local și solicitați un exemplar tipărit al Manualului de utilizare.

Data fabricației

Data versiunii de software se găsește pe pagina de autentificare nCommand Lite, în format LUNĂ/AN.

Capitolul 7 Istoricul revizuirilor

Revizuire	Descrierea modificării	Data
0	S-a actualizat versiunea manualului de la 2.3 v1 la 2.4	25 noiembrie 2025
1	S-au actualizat etichetele din Capitolul 6	04 decembrie 2025
2	A fost eliminată cerința pentru o adresă IP statică din configurația computerului local în subsecțiunea 1.3.11 S-a actualizat simbolul Reprezentantului Autorizat al UE în subsecțiunea 1.3.12 S-a eliminat nota de la subpunctul 1.3.14 S-a actualizat conținutul din Capitolul 2 S-a actualizat simbolul Reprezentantului Autorizat UE în Capitolul 6	28 ianuarie 2026
3	A fost revizuită traducerea termenului „Tehnician responsabil” în capitolul 6.	9 februarie 2026

Anexa I - Lista de verificare pentru începerea lucrărilor de service

1. Verificați conexiunile electrice și de rețea:

Asigurați-vă că conexiunile electrice și punctele de rețea sunt stabilite corect pe computerul e-KVM, pe computerul scannerului și pe computerul local.

2. Verificați starea alimentării cu energie:

Verificați dacă sursa de alimentare neîntreruptă și stabilizată și computerul e-KVM sunt pornite și funcționează corect.

3. Accesarea rapidă a platformei nC Lite:

Confirmați prezența comenzii rapide pentru platforma nC Lite pe desktop pentru acces rapid.

4. Accesarea și conectarea la platforma nC Lite:

Deschideți platforma nCommand și conectați-vă pentru a asigura accesul complet și funcționalitatea adecvată.

5. Configurarea aplicației de chat:

Deschideți aplicația de chat din platforma nC Lite într-o singură filă și evitați minimizarea acesteia pentru o comunicare fără probleme.