



BRUGERVEJLEDNING

nCommand Lite v2.4

Manuel version: V.3



Indhold

Kapitel 1	Introduktion.....	4
Afsnit 1.1 -	Formål	4
Afsnit 1.2 -	Ordliste	4
Afsnit 1.3 -	Beskrivelse	5
1.3.1.	Tilsigtet anvendelse	5
1.3.2.	Indikationer for brug.....	6
1.3.3.	Tilsigtet patientpopulation.....	6
1.3.4.	Brugsmiljø.....	6
1.3.5.	Kontraindikationer.....	6
1.3.6.	Platformens egenskaber.....	6
1.3.7.	Kliniske fordele	7
1.3.8.	Tilsigtede brugere.....	7
1.3.9.	Driftsmiljø.....	7
1.3.10.	Facilitetsmiljø.....	8
1.3.11.	Minimumskrav	9
1.3.12.	Symboler	10
1.3.13.	Levetid	11
1.3.14.	Opgrader / Opdater	11
Kapitel 2	Liste over generelle advarsler og forholdsregler	12
Kapitel 3	Platformbrug på hver lokalitet.....	14
Afsnit 3.1 -	Adgang til og brug af nCommand Lite	14
Afsnit 3.2 -	Adgang til platformen for første gang	14
3.2.1.	Log ind via nCommand Lite.....	15
3.2.2.	Login via ekstern IdP	16
Afsnit 3.3 -	Administration af adgangskoder	17
Afsnit 3.4 -	Adgang med lokal teknikerprofil	20
Afsnit 3.5 -	Adgang med fjernteknikerprofil.....	23
3.5.1.	Adgangstilstand	24
3.5.2.	Streaminglinje.....	27
3.5.3.	Multikamera	29
3.5.4.	Åbn en anden enhed	31
3.5.5.	Systemkontrol.....	33
Afsnit 3.6 -	Chat.....	35

Afsnit 3.7 - Afslutning af din session på platformen.....	38
Afsnit 3.8 - Undervisning i betjening	40
Afsnit 3.9 - Retningslinjer for fejlfinding	41
Afsnit 3.10 – Hardwarerengøringsmetoder	46
Kapitel 4 Cybersikkerhed og privatliv	47
Afsnit 4.1 - Sikkerheds- og privatlivsrisici	47
Afsnit 4.2 - Beskyttelse af personoplysninger (overholdelse af GDPR/HIPAA).....	47
Afsnit 4.3 - Adgangsstyring og godkendelse	48
Afsnit 4.4 - Systemkontrol Adgangskontrol.....	48
Afsnit 4.5 - Regional dataadskillelse og logopbevaring	49
Afsnit 4.6 - Datasikkerhed og -integritet.....	49
Afsnit 4.7 - Håndtering af sikkerhedshændelser	49
Kapitel 5 Servicekanaler.....	50
Kapitel 6 Juridiske og lovgivningsmæssige oplysninger	51
Kapitel 7 Revisionshistorik	54
BILAG I – Tjekliste til service	55

**FORSIGTIG**

I henhold til amerikansk føderal lovgivning må dette udstyr kun sælges af eller på ordination af en læge, som anvendt af en medicinsk tekniker, der er autoriseret i den stat, hvor denne praktiserer.

(gælder for USA)

**FORSIGTIG**

I Brasilien, er denne software godkendt af Anvisa til brug udelukkende med magnetisk resonansbilleddannelse (MRI) enhed. Enhver anden brug er ikke tilladt.

(Til brug i Brasilien)

**FORSIGTIG**

Før brug skal du sikre dig, at du er opmærksom på de specifikke krav i dit land eller din region. Manglende overholdelse af forordninger kan medføre sundhedsrisici.

**FORSIGTIG**

Sørg for, at versionen af denne brugervejledning matcher den version af platformen, der anvendes. Brug af en forkert version kan resultere i forkert betjening eller fejlfortolkning af funktioner.

Kapitel 1 Introduktion

Afsnit 1.1 - Formål

Denne vejledning har til formål at give lokale teknikere og fjernteknikere en omfattende forståelse af nCommand Lite-systemets specifikke funktionaliteter. Dette dokument fungerer som en brugervejledning og giver præcise og praktiske oplysninger, der guider brugerne gennem systemets funktionaliteter og fejlfinding. Ved at følge denne vejledning kan brugerne bruge nCommand Lite effektivt, hvilket hjælper med at maksimere produktivitet og reducere afhængighed af teknisk support.

Afsnit 1.2 - Ordliste

**FORSIGTIG**

Denne mærkning vedrører tilstande eller handlinger, der kan udgøre en potentiel fare. Du kan forårsage mindre personskade eller materiel skade, hvis du ignorerer disse anvisninger.

**ADVARSEL**

Denne mærkning identificerer tilstande eller handlinger, som resulterer i en specifik fare. Du vil forårsage alvorlig personskade eller væsentlig materiel skade, hvis du ignorerer disse anvisninger.

Platformens udtryk	Tilsvarende udtryk
Billeddiagnostisk facilitet	Medicinsk facilitet, Enhed, Mobile enheder, Sundhedsfacilitet, Sundhedsenhed
Fjernfacilitet	Ekstern arbejdsstation, Eksternt sted, Fjernkontor, Ekstern placering, Kommandocenter
Platform	nCommand Lite-webprogram
System	nCommand Lite med alle delsystemer
Apparat	Medicinsk scanner, Scanner, Udstyr, Medicinsk udstyr, Billeddannelsesapparat, Billeddannelsesudstyr
Lokal tekniker	Lokal bruger, Lokal tekniker, Lokal sundhedsperson, bruger på stedet

Afsnit 1.3 - Beskrivelse

nCommand Lite-systemet er en SaMD (software som medicinsk udstyr), der er kundeorienteret, og som giver fjernadgang via et webprogram til visning/gennemsyn af billeder samt evnen til på afstand at give vejledning i realtid til den patientnære, autoriserede tekniker (lokal bruger), der betjener det medicinske billeddannelsesudstyr i forbindelse med undervisning i eller procedurevurdering for MR-, CT- og PET/CT-scannere.

Fjernbrugere er autoriserede teknikere, som kan få adgang til et medicinsk billeddannelsesudstyr fra en computer, der opfylder de påkrævede minimumsspecifikationer hvor som helst, ved hjælp af en sikker softwareforbindelse, der streamer video og giver adgang til tastatur og mus. Dette gør det muligt for fjernbrugere at hjælpe lokale brugere uden at skulle tage hensyn til afstande. Denne adgang skal gives af den lokale bruger, der bruger systemet, og den kan også til enhver tid tilbagekaldes af den lokale bruger, så denne altid har den fulde kontrol over sessionen. Hver fjernsession styres endvidere ved hjælp af sikre legitimationsoplysninger, der administreres af den lokale bruger. Forbindelser til medicinsk udstyr er begrænset til én fjernsession ad gangen for at opretholde streng kontrol over, hvem der interagerer eksternt med systemet. Billeder, der gennemses eksternt, er ikke til diagnostisk brug.

nCommand Lite-systemet består af en IT-hardware- og softwarebaseret installationsløsning, der understøtter flere forskellige sessioner, så fjernteknikere har adgang til flere medicinske billeddannelsesenheder efter behov. Scannere, der er kompatible med nCommand Lite-systemet, overholder en fælles protokol, der giver mulighed for scanningsparameterstyring og fjernscanning.

1.3.1. Tilsigtet anvendelse

nCommand Lite-systemet giver fjernadgang til visning/gennemsyn af billeder samt mulighed for at give vejledning i realtid til den autoriserede tekniker, der betjener scanneren. Denne vejledning omfatter undervisning, procedurevurdering og administration af scanningsparametre.

1.3.2. Indikationer for brug

nCommand Lite-systemet muliggør fjernadgang til visning/gennemsyn af billeder samt mulighed for at give vejledning i realtid til den autoriserede tekniker, der betjener en kompatibel MR-, CT- eller PET/CT-scanner. Denne adgang skal gives af den lokale autoriserede tekniker, som betjener systemet. Fjernadgang er kun tilgængelig for systemer, der understøtter fjernforbindelse. Billeder, der gennemses eksternt, er ikke til diagnostisk brug.

1.3.3. Tilsigtet patientpopulation

For enhver patient, der ordineres til at få foretaget billeddannelse via tilsluttet medicinsk billeddannelsesudstyr.

1.3.4. Brugsmiljø

Medicinske faciliteter, der udfører MR-undersøgelser (magnetisk resonansscanning), CT-scanning (computertomografi) og positronemissionstomografi – computertomografi (PET/CT) samt eksterne kommandocentre.

1.3.5. Kontraindikationer

Platformen må ikke betjenes af brugere, der ikke er autoriserede teknikere, og som ikke har modtaget undervisning i brugen af nCommand Lite.

1.3.6. Platformens egenskaber

- **Fjernscanning:** Viser skærmen på det medicinske billeddannelsesudstyr i realtid, hvilket gør det muligt for en autoriseret fjerntekniker at deltage i en undersøgelse.
- **Chat:** Gør kommunikation tilgængelig mellem autoriserede fjernteknikere og autoriserede, lokale teknikere via tekst- og talebeskeder. Lokale teknikere og fjernteknikere kan også foretage og modtage stemme- og videoopkald.
- **Multikamera:** Muliggør fjernobservation af patienter og den medicinske facilitet under proceduren. Fjernteknikeren kan få adgang til visningen af kameraerne via fanerne, der er fordelt mellem alle kamerafaner og de individuelle faner. Denne mekanisme er en kopi af det visuelle overblik, som en sundhedsperson ville have, hvis denne befandt sig i nærheden af patienten og introducerer på den måde et ekstra element af sikkerhed.
- **Fjernscanning med flere sessioner** gør det muligt for fjernteknikeren at få adgang til forskelligt medicinsk billeddannelsesudstyr efter behov.
- **Adgangstilstand:** Giver fjernteknikeren mulighed for at vælge mellem visninger eller at betjene udstyret. I Vis-tilstanden kan fjernteknikere kun se det, der bliver streamet. I Kontroltilstand har vedkommende kontrol over musen og tastaturet.
- **Administrere fjernteknikeres adgang:** Giver den lokale tekniker mulighed for at styre fjernteknikeres adgang og deres adgangstilstand (Vis eller Kontrol). For at tillade fjernteknikerforbindelsen skal den lokale tekniker, som bruger platformen, give adgang. Adgang kan også til enhver tid blive trukket tilbage af den lokale tekniker, hvilket giver vedkommende mulighed for at opretholde den fulde kontrol over sessionen hele tiden.
- **Streamingstørrelse:** Fjernteknikeren kan se den oprindelige streamingstørrelse og den aktuelle streamingstørrelse i pixels. Vedkommende bliver også underrettet, hvis den aktuelle streamingstørrelse er mindre end den originale.
- **Status for mus og tastatur:** Fjernteknikeren får feedback, hvis det medicinske billeddannelsesudstyrs mus og tastatur fungerer korrekt.

- **Sessionsoplysninger:** Lokale teknikere og fjernteknikere kan få adgang til detaljer om sessionen.

1.3.7. Kliniske fordele

nCommand Lite forbedrer diagnostisk billeddannelse ved at muliggøre fjernbetjening af **MR-, CT- og PET-CT-systemer**, hvilket sikrer ensartet billedkvalitet og overholdelse af protokoller. Systemet giver erfarne teknikere mulighed for at overvåge og hjælpe med scanninger i realtid, optimere effektiviteten af arbejdsgange og reducere fejl, der kan påvirke den diagnostiske nøjagtighed. Systemet letter samarbejdet mellem teknikere, forbedrer ensartetheden af undersøgelser og muliggør hurtigere beslutningstagning i forbindelse med komplekse tilfælde. Ved at gøre det muligt for fjernpersonale at understøtte flere faciliteter øger **nCommand Lite tilgængeligheden, variationen og kvaliteten** af billeddiagnostiske undersøgelser, hvilket sikrer, at flere patienter har adgang til avanceret diagnostik samtidig med, at sundhedsressourcer optimeres. Derudover hjælper systemet med at afhjælpe personalemangel ved at reducere afhængigheden af specialister på stedet, og samtidig overholde strenge lovgivningsmæssige og datasikkerhedsstandarder.

1.3.8. Tilsigtede brugere

- **Lokal tekniker**
Den lokale tekniker er den bruger på stedet, der er ansvarlig for at hjælpe og vejlede patienter personligt på den medicinske facilitet. Vedkommende skal have den nødvendige viden til at udføre scanningsprocedurer med specifikt billeddannelsesudstyr. Derudover kontrollerer vedkommende fjernteknikerens adgangstilstanden (Vis eller Kontrol), og der skal gives fjernadgang af den lokale tekniker via platformen. Denne fjernadgang kan til enhver tid blive trukket tilbage.
- **Fjerntekniker**
En fagperson, der udfører fjernbetjening, med adgang til og kontrol over udstyrets computer. Ligesom den lokale tekniker skal fjernteknikeren også have den nødvendige viden til at udføre scanningsprocedurer for specifikt billeddannelsesudstyr.
- **Support/IT-bruger**
Fagperson, der er ansvarlig for opsætning af platformen (ikke inkluderet i denne brugervejledning).

1.3.9. Driftsmiljø

Følgende specifikationer henviser til de miljømæssige krav til e-KVM-computeren.

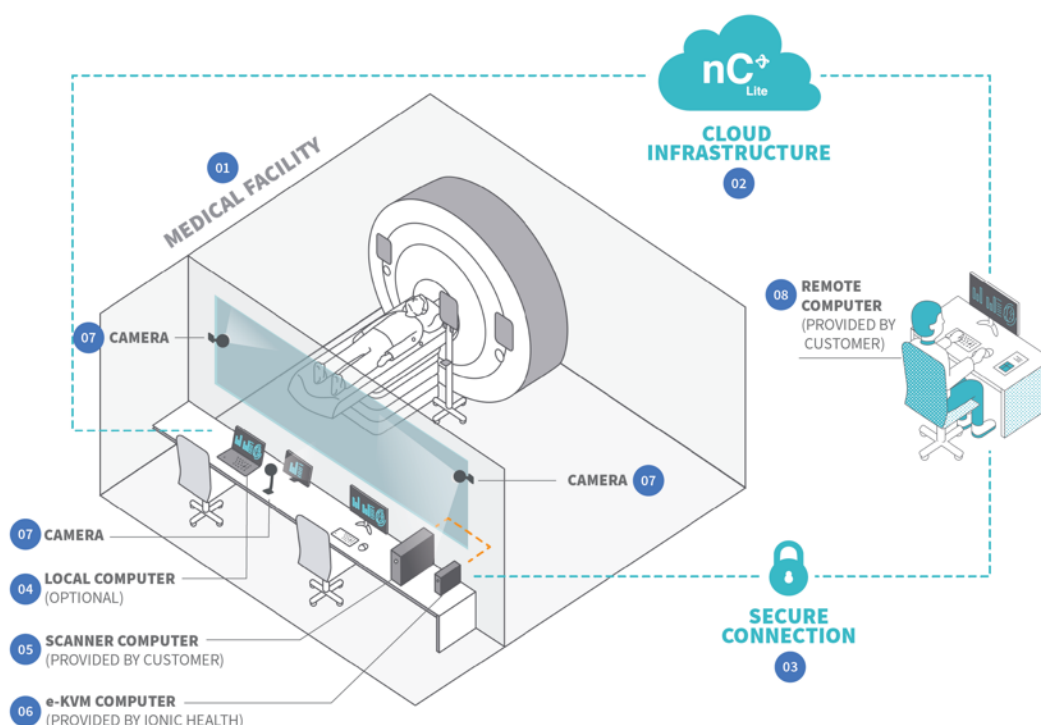
- **Maksimal højde (uden tryk)**
 - Drift: Fra 0 m (0 fod) til 3.048 m (10.000 fod)
 - Oplagring: Fra 0 m (0 fod) til 12.192 m (40.000 fod)
- **Temperatur**
 - Drift: Fra 10 °C (50 °F) til 35 °C (95 °F)
 - Oplagring: Fra -10 °C (14 °F) til 50 °C (122 °F)

- **Relativ luftfugtighed**
 - Drift: 20-80 % (ikke-kondenserende)
 - Oplagring: 10-90 % (ikke-kondenserende)

1.3.10. Facilitetsmiljø

nCommand Lite-plattformen har to lokalitetstyper, hvad miljøet angår:

- **Billeddiagnostisk facilitet:** Faciliteter, der udfører MR-scanning (magnetisk resonansscanning), CT-scanning (computertomografi) eller PET-/CT-scanninger (positronemissionstomografi – computertomografi).
- **Fjernfacilitet:** Et sted, hvor fjernteknikere kan få adgang til og fjernadministrere enheder (MR-, CT- eller PET/CT-scannere). Denne arbejdsstation kan bruges i forskellige miljøer såsom kontorer, kommandocentre, fjerntliggende placeringer og endda sekundære steder i sundhedsfaciliteten. Den eksterne arbejdsstation kan placeres i ethvert lokale, der tilbyder brugeren egnede forhold for koncentration samt de nødvendige minimumskrav til netværksforbindelse og computerkonfiguration.



Figur 01: Oversigt over produktet og dets opkoblinger via en sikker forbindelse (f.eks. VPN).
 01 – Medicinsk facilitet; 02 – Cloud-infrastruktur; 03 – Sikker forbindelse; 04 – Lokal computer (valgfrit);
 05 – Scanner Computer (leveret af kunden); 06 – e-KVM (leveret af IONIC Health);
 07 – Kamera; 08 - Fjerncomputer (leveret af kunden)

**ADVARSEL!****Kompatibilitet med fjernscanning**

IONIC Health (IH) validerer fjernscanningsfunktionaliteten på de anførte kompatible enheder. IH foretager en fuld vurdering af IH's krav til fjernscanning og tester systemet i målmiljøet under installationen. Dette sikrer kompatibilitet og korrekt ydeevne på tidspunktet for fjernscanningen. Denne verifikation betyder ikke, at alle OEM-enhedskrav (Original Equipment Manufacturer) er opfyldt i denne konfiguration. Enhver afvigelse fra OEM-kravene er slutbrugers ansvar.

Ændringer af systemet eller miljøet efter installationen skal meddeles til IH for at verificere fortsat kompatibilitet. IH kan ikke garantere ydeevne eller påtage sig ansvar for konfigurationer, der adskiller sig fra dem, der er valideret under installationen.

1.3.11. Minimumskrav

- **Lokal computer**

Denne computer bruges af den **lokale tekniker** til at godkende og understøtte fjernadgang til enheden via nCommand Lite®. Det giver også mulighed for direkte kommunikation med **fjernteknikeren** via chatfunktionen på platformen.

De minimalt påkrævede tekniske specifikationer er:

- Processor: AMD® A4-9120C eller højere eller lignende
- Hukommelse: 4 GB eller højere
- Oplagring: 128 GB SSD eller højere
- Eksterne enheder: mikrofon og højttaler eller headset og webcam
- Skærm: 14" FHD (1920 x 1080) eller højere
- Operativsystem: Chrome OS, Windows OS eller MAC OS
- Installationssted: Denne computer skal være i nærheden af scannercomputeren
- IT-rutine: Opret en nCommand Lite-genvej på hver brugers skrivebord
- Browser-kompatibilitet: Google Chrome eller Microsoft Edge.

- **Ekstern arbejdsstation**

Denne station bruges af **fjernteknikeren** til at få adgang til og styre enheden via nCommand Lite®. Den eksterne arbejdsstation skal etablere en sikker forbindelse til e-KVM-computeren (leveret af IONIC HEALTH®).

Kunden er ansvarlig for at levere fjerncomputeren og vil beslutte sig for et af to scenarier: det første er en 24x7-drift, og det andet er en drift i åbningstiden.

For hvert scenarie finder du nedenfor de korrekte specifikationer for valg af computermodeller:

Scenarie 1 (24x7-drift) – Skal opfylde følgende specifikationer:

- Intel Xeon W-2223 (4 kerner, 8 tråde, 8,25 MB cache, 3,90 GHz Turbo) eller højere.
- RAM: 16 GB eller højere.
- Grafik: NVIDIA RTX A2000 6 GB eller højere eller lignende.
- Oplagring: 128 GB SSD eller højere.

- Operativsystem: Windows 11 Pro 64 B eller højere.
- Overvåg minimumskrav: Størrelse 27", Billedformat 16:9, opløsning 4k.
- Headset: BLACKWIRE 3200 eller lignende.
- Browser-kompatibilitet: Google Chrome eller Microsoft Edge.

Scenarie 2 (drift i åbningstiden) – Skal opfylde følgende specifikationer:

- Intel® Core™ i7-12700k vPro® eller højere.
- RAM: 16 GB eller højere.
- Grafik: NVIDIA T400 GB eller højere eller lignende.
- Oplagring: 128 GB SSD eller højere.
- Operativsystem: Windows 11 Pro 64 B eller højere.
- Overvåg minimumskrav: Størrelse 27", Billedformat 16:9, opløsning 4k.
- Headset: BLACKWIRE 3200 eller lignende.
- Browser-kompatibilitet: Google Chrome eller Microsoft Edge.



ADVARSEL!

Hvis de relevante opsætnings- og minimumskrav ikke opfyldes, kan det medføre forringet eller manglende kommunikation mellem brugere.

• Netværkskonfigurationer (minimumskrav)

For at etablere sessionen mellem fjernbrugeren og e-KVM-computeren skal netværkskommunikation mellem de to enheder sikres. nCommand Lite-systemet bruger peer-to-peer (P2P) til at etablere forbindelse mellem lokale bruger, fjern-bruger og e-KVM-computer. Der er tre kompatible scenarier:

- **Scenario 1** – Virksomhedsnetværk, der bruger en af følgende protokoller: LAN, LAN-til-LAN, MPLS eller VPN;
- **Scenario 2** – Virksomhedsnetværk, der bruger et betroet WAN (eksternt netværk) og ikke bruger nogen af følgende protokoller: LAN, LAN-til-LAN, MPLS eller VPN;
- **Scenario 3** – Offentligt netværk på fjerncomputersiden (fjernbruger).

Konfigurationerne for hvert scenarie er beskrevet i den tekniske dokumentation.

1.3.12. Symboler

Symbol	Beskrivelse	Reference
	Fabrikant	ISO 15223-1, ISO 7000-3082
	Fremstillingsdato	ISO 15223-1, ISO 7000-2497
	Symbolet angiver, at dette produkt er medicinsk udstyr	ISO 15223-1
	Unik udstyrsidentifikation	ISO 15223-1

	Modelreference	ISO 15223-1, ISO 7000-2493
	Importør	ISO 15223-1, ISO 7000-3725
	Se brugervejledningen	ISO 15223-1, ISO 7000-1641
	Distributør	ISO 15223-1, ISO 7000-3724
	Forsigtig	ISO 15223-1, ISO 7000-0434A
	Advarsel	ISO 7010-W001
	Serienummer <i>(eller softwareversion)</i>	ISO 15223-1, ISO 7000-2498
	Bemyndiget repræsentant i Det Europæiske Fællesskab	ISO 15223-1
	Autoriseret repræsentant i Schweiz (CH-REP)	ISO 15223-1
	CE – Europæisk overensstemmelsesmærkning; 2803 – Udpeget bemyndiget organ	EU-forordning 2017/745

1.3.13. Levetid

Produktets forventede levetid er 5 år under hensyntagen til holdbarheden af komponenterne i produktet. Denne omfattende evaluering sikrer, at hver kritisk komponents levetid stemmer overens med den samlede levetid og således garanterer ensartet ydeevne og pålidelighed i produktets fulde, tilsigtede levetid.

1.3.14. Opgrader / Opdater

IONIC Health vil opdatere nCommand Lite-systemet som en del af planlagte vedligeholdelses- eller opgraderingsudgivelser. Disse opdateringer er designet til at sikre fortsat ydeevne og pålidelighed uden at afbryde den aktuelt installerede version på kunders websteder. Afhængigt af opdateringens art kan produktet opgraderes eksternt eller kan kræve et besøg på stedet af en felttekniker.

Kapitel 2 Liste over generelle advarsler og forholdsregler



ADVARSEL!

Læs alle advarslerne nedenfor, inden nCommand Lite-systemet tages i brug.



FORSIGTIG

nCommand Lite-systemet kan ikke repareres eller vedligeholdes, mens det anvendes til at styre et MR-, CT- eller PET-CT-udstyr i nærværelse af en patient.

- Vær meget opmærksom på alle systemadvarsler, da de er afgørende for sikker betjening.
- Prioritér sikkerhed og opmærksomhed under enhver drift.
- I henhold til amerikansk føderal lovgivning må dette udstyr kun sælges af eller på ordination af en læge og anvendes af medicinske teknikere, der er autoriseret i den stat, hvor de praktiserer.
- nCommand Lite-systemet må kun anvendes af teknikere, som har modtaget undervisning i brugen af platformen.
- Brug kun dette system sammen med compatible webbrowsere. Understøttede browsere er Google Chrome og Microsoft Edge.
- I tilfælde af uforudsete situationer skal en uddannet, autoriseret tekniker forblive på den billeddiagnostiske facilitet for at udføre MR-, CT- eller PET/CT-scanningerne uden nCommand Lite.
- Adgang til flere enheder samtidig kræver intenst fokus og kommunikation med det lokale personale.
- Undgå at tilgå enheder med identiske layouts eller undersøgelser af samme anatomiske område på samme tid.
- Du kan se flere skærbilleder, men kontrollen er begrænset til én enhed ad gangen.
- Start altid en chat, når du er blevet forbundet til udstyret, for at opnå klar kommunikation.
- Alarmer for taleopkald vises på den tilknyttede enheds skærm. Kun ét opkald kan være aktivt ad gangen.
- Test videokommunikationen, når du åbner programmet (før starten af en arbejds-session) for at kontrollere, om der er fejl i videoudgangsforbindelsen til MRI-, CT- eller PET/CT-udstyret eller andet udstyr relateret til videostreaming.
- Udstyret må ikke tilsluttes stikkontakten og/eller den uafbrydelige og stabiliserede strømforsyning ved brug af forlængerledninger eller strømskinner.
- Hvis der opstår videofejl, skal videoforbindelsen mellem udstyrssystemet og e-KVM-computeren kontrolleres.
- Hvis programmet er langsomt ved fjernadgang, skal siden opdateres med kommandoerne Ctrl+F5 i browseren på fjernteknikerens computer. Kontakt teknisk support, hvis problemet fortsætter.
- Når browsersiden opdateres, bliver forbindelsen til udstyret afbrudt, hvilket kræver, at godkendelsesprocessen skal udføres igen.
- Log ikke på med en anden browser, hvis du allerede er logget på.
- Kundens billeddiagnostiske facilitet skal have et redundant internetlink fra en anden leverandør end den primære til øjeblikkeligt skift i tilfælde af tab af system-/platformskommunikation.

- I tilfælde af kommunikationssvigt eller langsom mus, skal du udføre en "musesynkronisering" på den side, der bruges i browseren.
- Sørg for, at de computere, der bruges til nCommand Lite-systemkontrol, både på den billeddiagnostiske facilitet og i kommandocentret, opfylder minimumskravene. Ellers kan der være tab af ydeevne i programmet.
- Servicekvalitet (Quality of Service, QoS) skal anvendes på hovedforbindelsen og den redundante forbindelse til overførsel af platformen, og linkets ydeevne skal monitoreres.
- Før brug skal lyd- og mikrofonlydstyrkeniveauerne og lyd- og mikrofontilladelsen i webbrowseren kontrolleres.
- Før brug skal du kontrollere tastaturets og musens funktion. Hvis de er langsomme eller ude af synkronisering, skal du aktivere knappen "musesynkronisering". Kontrollér, om e-KVM-computeren er tilsluttet og tændt.
- Sørg for, at tastaturlayoutet på fjernfaciliteten er identisk med tastaturlayoutet på Imaging Facility.
- Hvis det er nødvendigt at ændre stedet, hvor platformen bruges, skal klienten kontakte teknisk support for at foretage en ny installation. Platformen må ikke geninstalleres, uden at teknisk support kontaktes.
- Før du starter fjernadgangsprocessen for MRI-, CT- eller PET/CT-udstyret, er det vigtigt, at teknikereholderne kontrollerer alle dele, der er nødvendige for, at platformen fungerer korrekt, så undersøgelsen ikke påvirkes. Disse dele er anført i dokumentet "Service Start Checklist".
- Den billeddiagnostiske facilitets firewallkonfiguration skal kontrolleres månedligt med IT-teamet for at bekræfte, at der ikke er problemer med firewall-frigivelsen, som kan kompromittere brugen af nCommand Lite.
- Enhver uregelmæssighed, der observeres under brugen af applikationen, skal straks indberettes til supportteamet, inden adgang påbegyndes, eller brugen afbrydes, hvis den allerede er startet.
- Kun autoriserede teknikere, der er uddannet i brugen af nCommand Lite, må bruge programmet.
- Fjernadgang via platformen erstatter eller konkurrerer ikke med andre driftsprocedurer for MR-, CT- eller PET/CT-betjening, der er fastlagt af fabrikanten af det medicinske udstyr og plejefacilitetens protokoller og procedurer.
- Undgå at bøje eller strække hardwarekablerne.
- Hvis der opstår problemer med stemme- eller chatkommunikation, skal du bruge telefonfunktionen til at etablere kommunikation mellem den lokale tekniker på den billeddiagnostiske facilitet og fjernteknikeren på Kommandocentret. Følg anvisningerne i afsnittet "Retningslinjer i tilfælde af fejl", og kontakt om nødvendigt teknisk support for at udføre reparationen.
- Hvis det er nødvendigt at udskifte en computer eller andet udstyr, der direkte påvirker installationen af nCommand Lite, skal teknisk support aktiveres, så videreføringen af systemets drift kan garanteres.
- Kun én person ad gangen kan få fjernadgang til MRI-, CT- eller PET/CT-udstyret.
- Rør ikke ved fysiske videokabler, mens udstyrets computer og nCommand Lite-systemet er tændt.
- Når du får adgang til andet udstyr, åbnes der en ny fane. Træk denne fane til en anden skærm, da systemet er designet til at blive brugt med en separat skærm til hver enhed.
- Enhver alvorlig hændelse relateret til brugen af dette udstyr skal rapporteres til både fabrikanten og sundhedsmyndigheden/den kompetente myndighed, hvor udstyret er installeret (se yderligere oplysninger i kapitlet Servicekanaler).

Kapitel 3 Platformbrug på hver lokalitet

Afsnit 3.1 - Adgang til og brug af nCommand Lite

**ADVARSEL!**

I tilfælde af problemer, kontaktes teknisk support for assistance.

**ADVARSEL!**

Kontrollér tastaturlayoutet, og sørg for, at det er det samme på begge lokaliteter (medicinsk facilitet og fjernfacilitet). Forskellige tastaturlayouts kan hindre brugeroplevelsen.

Dette kapitel indeholder alt, hvad du behøver at vide for at få adgang til og begynde at bruge nCommand Lite-platformen. Du finder enkle, trinvis instruktioner til at logge på platformen, navigere på grænsefladen og forstå hovedfunktionerne. Uanset om du arbejder på stedet eller eksternt, vil denne vejledning hjælpe dig med at komme i gang hurtigt og trygt.

Ændring af sprog – Systemet er forudindstillet til engelsk som standard, men du kan nemt ændre sproget efter din præference. På login-skærmen skal du klikke i øverste højre hjørne, hvor der står "English (en-US)" (Engelsk (en-USA)) vises. Dette åbner en rulleliste over tilgængelige sprog, som du kan vælge imellem.

Når du har logget på, kan du også ændre sproget ved at klikke på det aktuelt valgte sprog i højre side på den øverste linje. Dette åbner en rulleliste over tilgængelige sprog, som du kan vælge imellem.

Bemærk: Hvis du ændrer sprog, mens du har forbindelse til udstyr, vil den aktuelle forbindelse automatisk blive afbrudt, og du skal oprette forbindelse igen.

Når du får adgang til platformen, kan du vælge dit foretrukne sprog på loginskærmen. Dog kan nogle meddelelser under login-processen blive vist på det sprog, der er indstillet i din webbrowser, uanset hvilket sprog der er valgt på platformen. For at få en ensartet oplevelse anbefaler vi, at du tilpasser dine browsersprogindstillinger til dit foretrukne platformssprog.

Afsnit 3.2 - Adgang til platformen for første gang

Login-processen på platformen kan udføres på to måder: via nCommand Lite eller via en ekstern identitetsudbyder (ekstern IdP). Brugeren kan logge ind ved hjælp af en af de forudkonfigurerede metoder. Hvis den konfigurerede metode er ekstern identitetsudbyder (External IdP), vil nCommand Lite-metoden ikke fungere, og omvendt. For at logge ind via ekstern identitetsudbyder skal du gå direkte til **underafsnit 3.2.2**.

3.2.1. Log ind via nCommand Lite

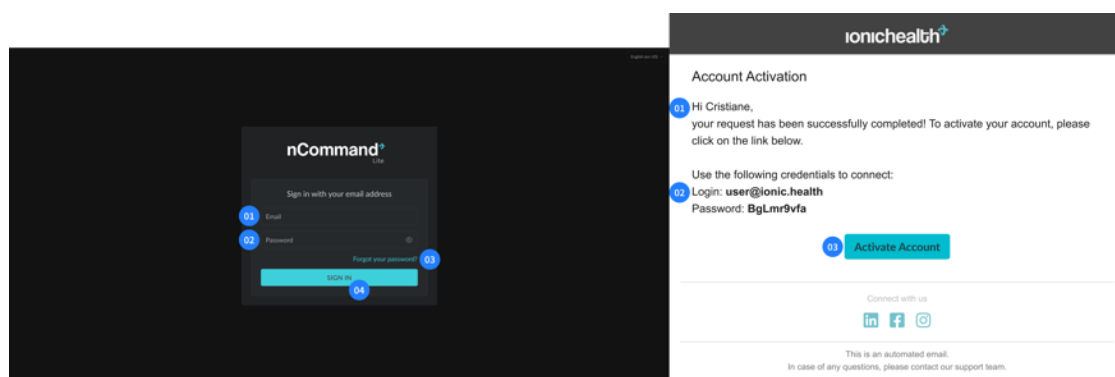
Bemærk: Dette afsnit gælder ikke for brugere, der logger på via en ekstern identitetsudbyder (External IdP).

Tænd for computeren, og dobbeltklik på genvejsikonet til nCommand Lite, som normalt findes på skrivebordet. Du kan også få adgang til URL'en direkte i browseren.

Din første adgang er et afgørende trin, der gør, at du kan begynde at bruge platformen sikkert og effektivt. Her er, hvad du skal vide:

1 – Velkomstmil: Du vil modtage en e-mail med dine loginoplysninger, herunder din tilknyttede personlige e-mailadresse, en midlertidig adgangskode og et direkte link til klientplatformen. Denne e-mail er afgørende for, at du kan påbegynde dit forløb med nCommand Lite.

2 – Oprettelse af adgangskode: Efter at du har åbnet linket, skal du indtaste din tilknyttede e-mailadresse og den adgangskode, du modtog i velkomstmilen. Ved at klikke på "Sign in" (Log på) vil du blive sendt videre til en side, hvor du kan oprette en ny adgangskode. Du skal indtaste den gamle adgangskode, den nye adgangskode og bekræftelsen af den nye adgangskode. Den skal være stærk og sikker og indeholde mindst 3 af følgende: et lille bogstav, et stort bogstav, et tal og et symbol, og være på mindst 8 tegn. Når du klikker på "Continue" (Fortsæt) bliver du sendt videre til en side, hvor du skal bekræfte din e-mail igen. Ved at klikke på "Continue" (Fortsæt) bliver du nu sendt til startskærmen, som er tilpasset i henhold til din specifikke brugerprofil.



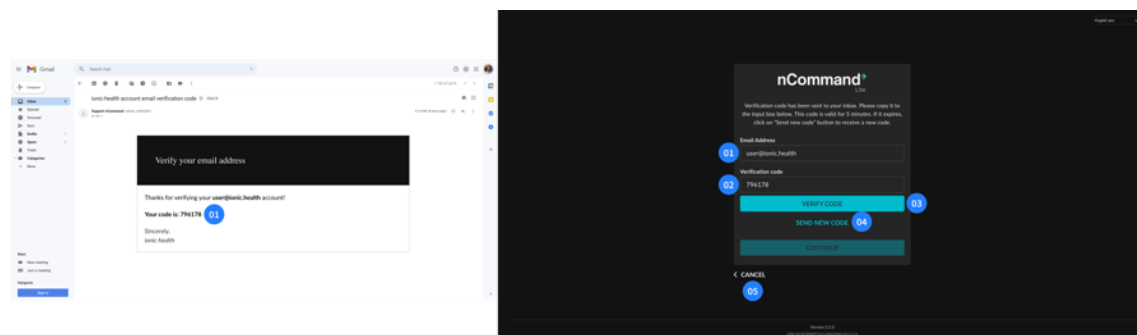
Figur 02: Første adgang

Venstre - Log ind-side: 01 – E-mailadresse; 02 – Adgangskode; 03 – "Glemst din adgangskode?"; 04 – Sign In knap
Højre – Velkomstmil: 01 – E-mailtekst til kontoaktivering; 02 – Loginoplysninger; 03 – Aktiv konto knap

Denne indledende procedure er designet til at sikre maksimal sikkerhed for din konto fra starten. Fra og med dit andet login vil processen blive mere strømlinet, men forblive lige så sikker, idet en tofaktorgodkendelseskode sendes til din tilknyttede e-mail ved hvert login for at opretholde den fortsatte sikkerhed for din konto.

Når du har logget på nCommand Lite, leder systemet dig automatisk til startskærmen, som tilpasses i henhold til din specifikke brugerprofil. Uanset om du er lokal tekniker eller fjerntekniker, er grænsefladen designet til at opfylde de behov og den adgang, der er relevant for din rolle. Dette intuitive design sikrer, at du har alle de værktøjer og oplysninger, der er nødvendige for en effektiv brugeroplevelse fra det øjeblik, du logger på.

Bemærk: Når login-metoden er konfigureret som nCommand Lite, skal login altid foretages via denne mulighed. Selvom knappen *External IdP* (ekstern identitetsudbyder) vises på login-skærmen, vil den ikke fungere for disse brugere. Hver brugerkonto er registreret på platformen med en specifik autentificeringsmetode — enten nCommand Lite legitimationsoplysninger eller en *External IdP*-tjeneste. Hvis en bruger forsøger at logge ind med en anden metode end den, der er tildelt deres konto, vil systemet vise en fejlmeddelelse, der indikerer, at kontoen ikke er autoriseret til den autentificeringstype.



Figur 03: Tofaktoraутenticering (2-FA)

Venstre – E-mail: 01 – 2-FA Kode

Højre – Tofaktorgodkendelsesside: 01 – E-mail Address (E-mailadresse); 02 – Bekræftelseskode; 03 – Bekræft knap til bekræftelseskode; 04 – Send ny kode; 05 – Annuller

3.2.2. Login via ekstern IdP

I nogle tilfælde kan brugere logge ind på platformen via en ekstern identitetsudbyder (IdP), som giver dem mulighed for at bruge deres organisations eksisterende godkendelsestjeneste, en mekanisme også kendt som Single Sign-On (SSO). Med denne metode vil den forudregistrerede bruger ikke modtage en velkomstmil. Den lokale it-tjeneste skal kontrollere kompatibiliteten, konfigurere metoden og informere brugeren om, hvilken e-mail (ekstern identitetsudbyder) der skal bruges.

Når denne mulighed er tilgængelig, skal brugeren altid logge ind ved hjælp af den eksterne identitetsudbyder (f.eks. Amazon Cognito, Microsoft Entra ID, Microsoft AD B2C). Login-metoden via nCommand Lite vil ikke være tilgængelig for eksterne IdP-brugere.

For at logge ind med den eksterne identitetsudbyder skal du klikke på knappen med identitetsudbydernavnet og følge instruktionerne fra den eksterne autentifikator. Hvis din institution har mere end én ekstern identitetsudbyder integreret, skal du sørge for at bekræfte, hvilken udbyder du er registreret hos. Andre udbydere vil ikke fungere. Hvis du har spørgsmål eller støder på problemer, kan du kontakte din lokale IT-service.

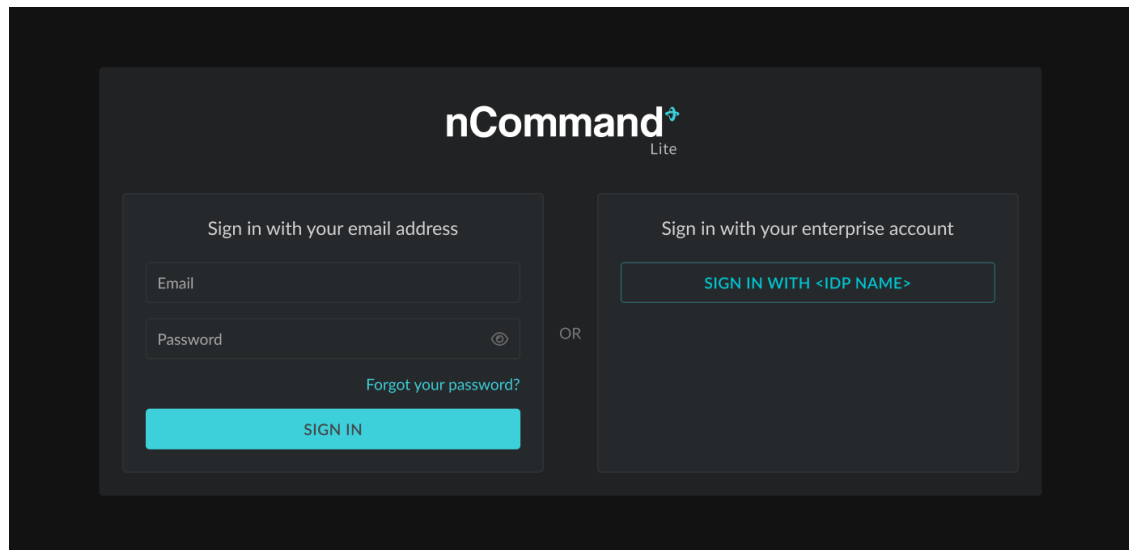
I scenarier, hvor brugere deler den samme maskine og bruger Single Sign-On (SSO), anbefales det, at hver bruger vælger indstillingen "do not stay signed in" (forbliv ikke logget på) under eksternt identitetsudbyder-login (hvis tilgængeligt) eller logger ud af den eksterne udbyder efter at have logget ud af nCommand Lite.

For denne login-mulighed administreres hele login- og logout-processen – herunder politikker for oprettelse og udløb af adgangskoder, multifaktorgodkendelse (MFA) og kontospærring – udelukkende af kundens it-team, der konfigurerede den eksterne identitetsudbyder.

Når du logger ind via ekstern identitetsudbyder, skal funktionerne "Forgot Password" (Glemmt adgangskode) og "Change Password" (Skift adgangskode) udføres i henhold til den eksterne identitetsudbyders proces.

Bemærk: Valgmuligheden "Glemmt adgangskode" vil stadig vises på loginskærmen, men den vil ikke fungere for disse brugere. Det vil muligvis gå videre til de næste trin i processen, men vil ikke fuldføre dem. Hvis du har brug for at gendanne din adgangskode, skal du følge instruktionerne fra din eksterne identitetsudbyder.

Vigtigt: Selv når du bruger en ekstern identitetsudbyder, skal brugeren være forudregistreret på nCommand Lite-plattformen for at få adgang.



Figur 04: Login-skærm via ekstern IdP (Eksempel)

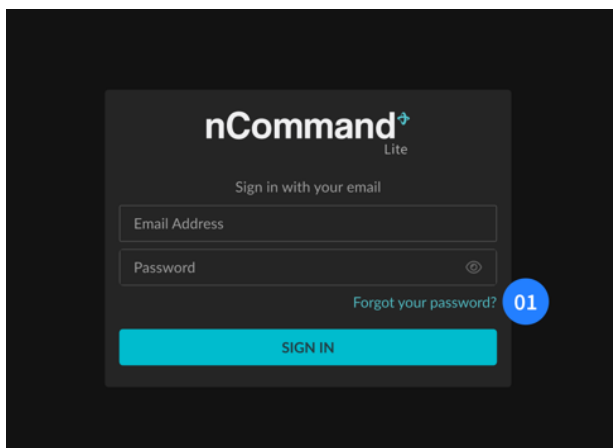
Afsnit 3.3 - Administration af adgangskoder

Efter at have tilgået platformen for første gang kan brugerne ændre deres adgangskode eller, hvis den blev glemt, indstille en ny adgangskode.

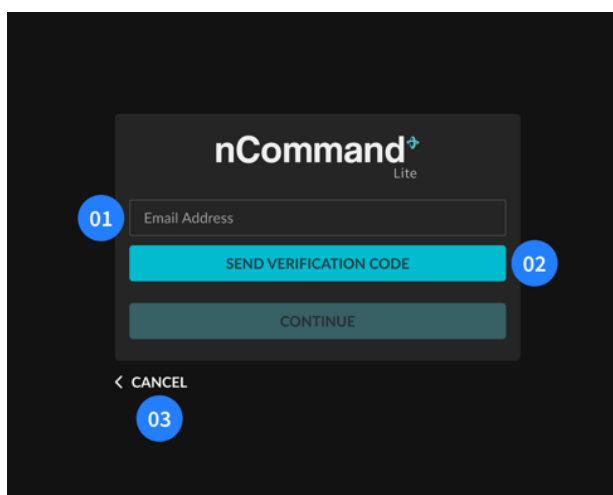
Bemærk: Når du logger ind via ekstern identitetsudbyder, skal funktionerne **Forgot Password** (Glemmt adgangskode) og **Change Password** (Skift adgangskode) udføres i henhold til den eksterne identitetsudbyders proces.

- **Gendan adgangskode:** Gør det muligt for brugere at gendanne kontoadgang, skulle de glemme deres adgangskode. Du skal blot klikke på linket "Forgot your password?" (Har du glemt din adgangskode?) på login-siden, indtast den tilknyttede e-mailadresse, og send oplysningerne. Systemet sender derefter en e-mail med en bekræftelseskode. Når du udfylder

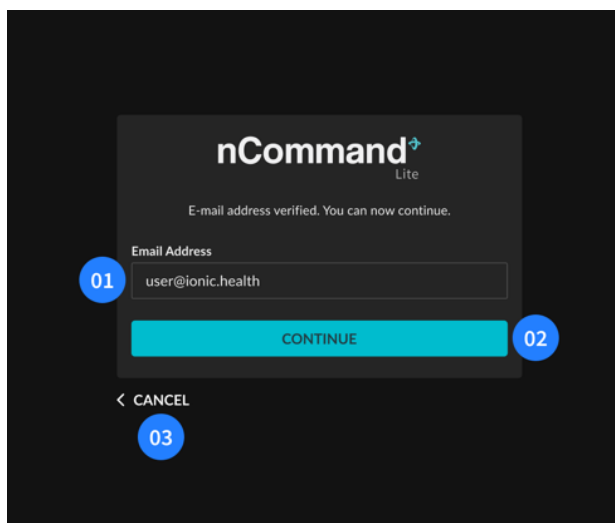
koden og klikker på "Verify Code" (Bekræft kode), vil brugerne blive bedt om at bekræfte den tilknyttede e-mail. Ved at klikke på "Continue" (Fortsæt) dirigeres brugerne til en side, hvor de kan indtaste en ny adgangskode og bekræfte den nye adgangskode. Hvis den nye adgangskode opfylder systemkravene, kan brugerne registrere den og derefter logge på med de opdaterede brugeroplysninger.



Figur 05: Link til siden for nulstilling af adgangskode
01 – Har du glemt din adgangskode?

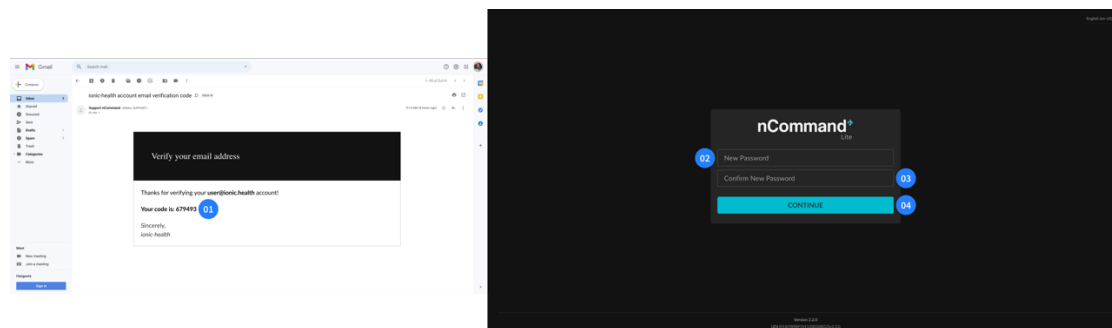


Figur 06: Side for nulstilling af adgangskode
01 – E-mailadresse; 02 – Send bekræftelseskode; 03 – Annuller



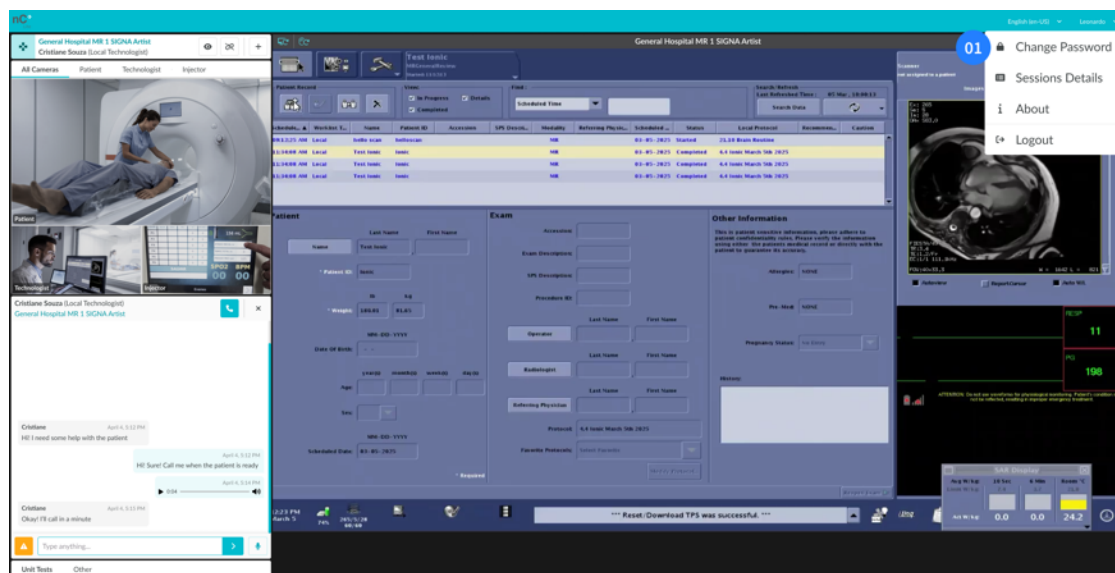
Figur 07: E-mail bekræftelse

01 – E-mail Address (E-mailadresse); **02** – Knappen Continue (Fortsæt); **03** – Cancel (Annuller)

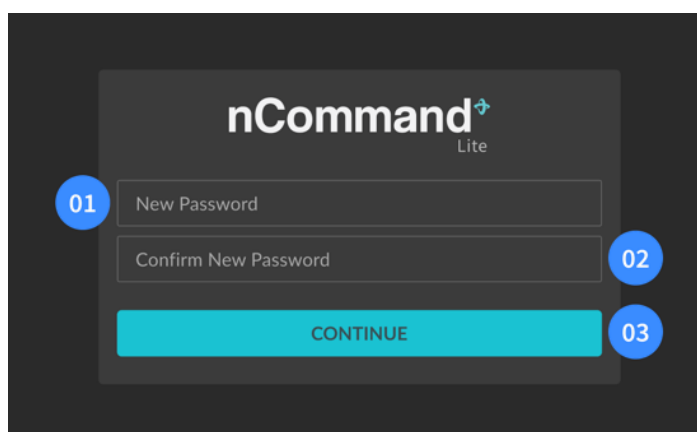


Figur 08: Send en e-mail med kode til Registrer Ny Adgangskode (venstre) - 01 – 2-FA Kode Ændre kodeord-siden (højre) - 02 – Ny adgangskode; 03 – Bekræft ny adgangskode; 04 – Fortsæt knappen

- Skift adgangskode:** Gør det muligt for brugere at opdatere deres adgangskode ved at overholde specifikke kriterier, herunder mindst 3 elementer af følgende: et lille bogstav, et stort bogstav, et tal og et symbol og være på mindst 8 tegn. Systemet kontrollerer, om den nye adgangskode opfylder disse kriterier og sender brugeren en meddelelse, hvis adgangskoden ikke opfylder disse kriterier. Brugere skal desuden bekræfte den nye adgangskode for at forhindre indtastningsfejl. Brugeren skal klikke på ikonet i øverste højre hjørne og vælge menuen "Change Password" (Skift adgangskode) for at skifte adgangskoden. Vedkommende kobles fra platformen og sendes til en side med henblik på at bekræfte den tilknyttede e-mail. Systemet sender derefter en e-mail med en bekræftelseskode. Når brugere tilføjer koden og klikker på "Verify code" (Bekræft kode), sendes de til et skærbillede, hvor de kan indtaste en ny adgangskode.



Figur 09: Skift adgangskode rullemenu-element
01 – Skift adgangskode



Figur 10: Skift adgangskodeside
01 – Ny adgangskode; 02 – Bekræft ny adgangskode; 03 – Fortsæt knappen

Afsnit 3.4 - Adgang med lokal teknikerprofil



ADVARSEL!

Inden platformen tages i brug, skal fjernteknikeren kontaktes telefonisk.



ADVARSEL!

For at undgå overophedning må der ikke placeres genstande foran blæseren på e-KVM-computeren, og for at undgå beskadigelse må der ikke placeres genstande oven på den.

**ADVARSEL!**

Under fjernsessioner er den lokale tekniker ansvarlig for at styre og håndhæve lokale sikkerhedsregler for hver type undersøgelse og for undersøgelsens specifikke krav. Bliv altid i kontrolrummet og/eller undersøgelsesrummet for at sikre sikkerheden for både patienten og de involverede fagpersoner.

**ADVARSEL!**

Enhver bevægelse af bordet under sessionen må kun udføres af den lokale tekniker, når systemet anmoder om det. Inden lokalet forlades, skal den lokale tekniker altid tilbagekalde fjernteknikerens adgang.

**ADVARSEL!**

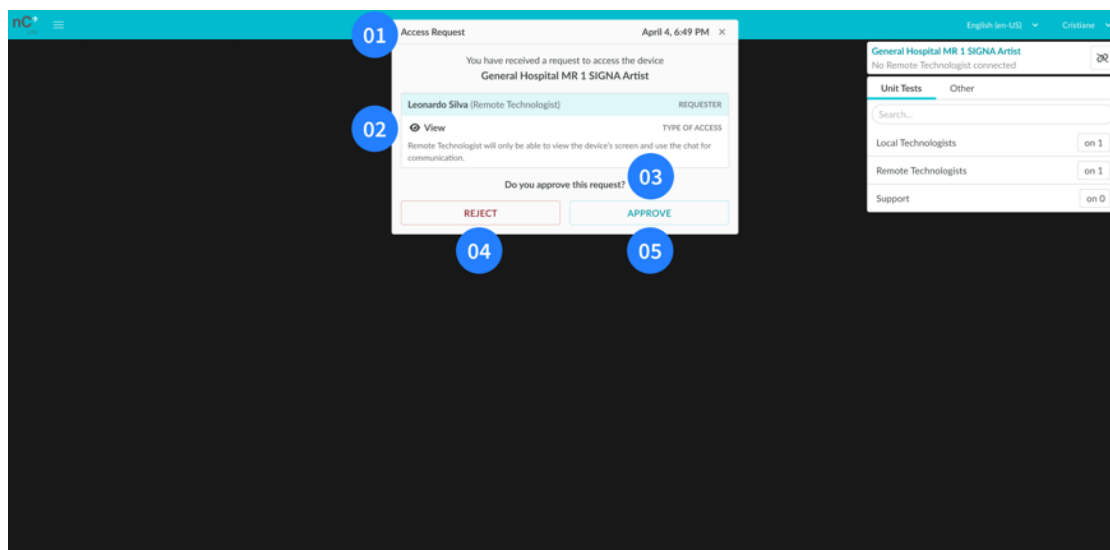
Kun den lokale tekniker har lov til at flytte bordet med henblik på at placere patienten i udstyret og for at frigøre patienten sikkert. Inden lokalet forlades, skal den lokale tekniker altid tilbagekalde fjernbrugerens adgang.

Når du har logget på platformen, skal du fortsætte med at vælge det ønskede udstyr i feltet Device Selection (Valg af udstyr). Du vil være ansvarlig for denne enhed, så du kan gennemgå fjernteknikerens anmodning om at få adgang til enheden. Når en fjerntekniker ønsker at få adgang til udstyret, vises et pop op-vindue, der giver dig mulighed for at gennemgå alle de viste oplysninger, før du giver eller afviser adgang. Vær opmærksom på en indgående anmodning fra en fjerntekniker. Det er yderst vigtigt, at du omhyggeligt fører kontrol med hver detalje. I tilfælde hvor de angivne oplysninger ikke bliver registreret, må du ikke give adgang.

Fjernteknikeren kan få adgang til udstyret ved hjælp af en af to adgangstilstande: **Kontrol** eller **Vis**:

- **Kontroltilstand** – giver fjernteknikeren mulighed for at kontrollere musen og tastaturet samt se udstyrets streaming. Den lokale tekniker mister imidlertid ikke kontrollen over den lokale mus og det lokale tastatur og kan til enhver tid tage kontrollen.
- **Visningstilstand** – giver fjernteknikeren mulighed for kun at se udstyrets skærm og bruge chatten til kommunikation

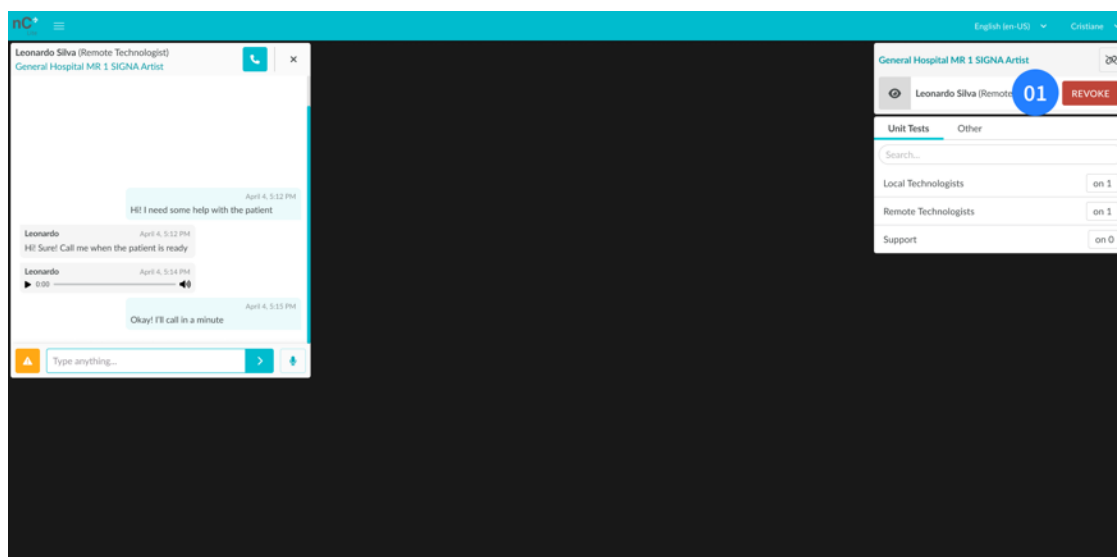
Efter valg af udstyr får brugeren adgang til chatfunktionen, hvilket muliggør kommunikation via tekst, lydbeskeder, tale- og videoopkald med de øvrige brugere.



Figur 11: Lokal tekniker hovedskærm med adgangsmodningsmeddelelse

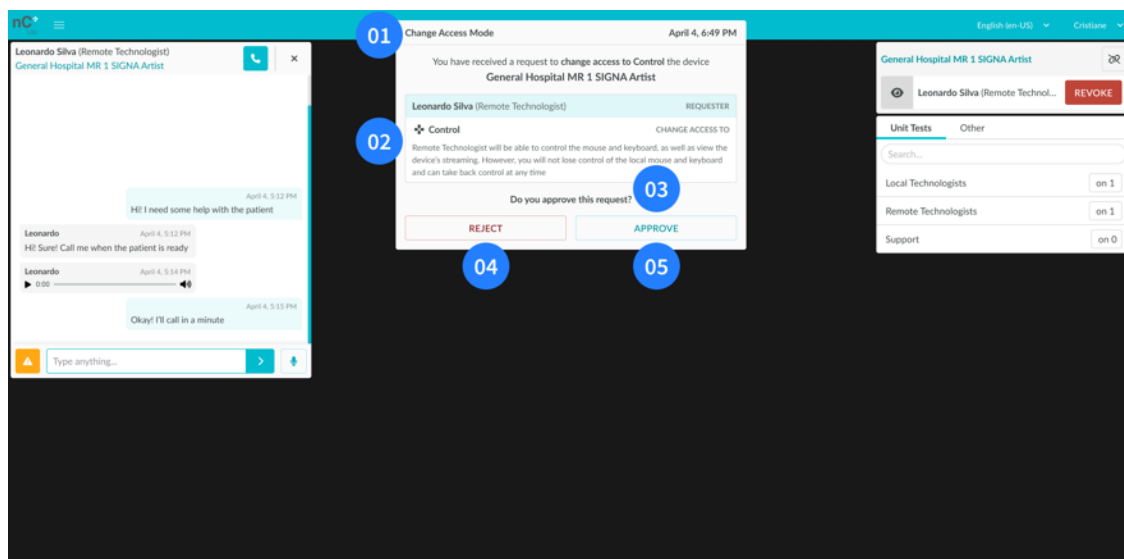
01 – Titel (Access Request (Anmodning om adgang)); **02** – Navn på anmoder, rolle og beskrivelse af adgangstype; **03** – Prompt: "Do you approve this request?" (Godkender du denne anmodning?); **04** – Knappen Reject (Afvis); **05** – Knappen Approve (Godkend)

Efter godkendelsen kan den lokale tekniker til enhver tid tilbagekalde fjernteknikerens adgang ved blot at klikke på knappen REVOKE (TILBAGEKALD).



Figur 12: Lokal tekniker hovedskærm ved tilslutning til en enhed
01 – Tilbagekald knap

Under fjernsessionen kan fjernteknikeren anmode om en ændring af adgangstilstand. Der vises en pop op-anmodning på skærmen. Du kan godkende eller afvise den. Vær opmærksom på de privilegier, som hver adgangstilstand giver fjernteknikeren.



Figur 13: Lokal tekniker hovedskærm med anmodning om at ændre adgangstilstand
 01 – Titel (Skift adgangstilstand); 02 – Navn på anmoder, rolle og beskrivelse af adgangstype;
 03 – Prompt: "Godkender du denne anmodning?"; 04 – Afvisningsknap; 05 – Godkend knap



ADVARSEL!

I tilfælde af en mistet forbindelse på den lokale computer har fjernteknikeren stadig adgang til *udstyret*. Kontakt **straks** fjernteknikeren, og bed vedkommende om at **afbryde** forbindelsen til ELLER logge på en anden computer og **tilbagekalde** adgangen for fjernteknikeren, ELLER tryk på **tænd/sluk-knappen** for at lukke e-KVM-computeren ned.



ADVARSEL!

I tilfælde af scannervedligeholdelse:

Inden feltteknikeren påbegynder nogen procedurer (enten på udstyret eller i kontrolrummet), skal fjernteknikeren informeres, og adgangen skal tilbagekaldes ved at klikke på knappen "REVOKE ACCESS" (TILBAGEKALD ADGANG). Log derefter af nCommand Lite-plattformen. Hvis der ikke er forbundet en fjerntekniker, skal du logge af nCommand Lite-plattformen, før du starter vedligeholdelse.

Afsnit 3.5 - Adgang med fjernteknikerprofil



ADVARSEL!

Udstyrscomputerens bruger- og rodadgangskode: Begge skal opbevares af den vært på stedet, som modtager installationsteamet.



ADVARSEL!

Enhver bevægelse af bordet under sessionen må kun udføres af den lokale tekniker, når systemet anmoder om det. Inden lokalet forlades, skal den lokale tekniker altid tilbagekalde fjernteknikerens adgang.



ADVARSEL!

Kun den lokale tekniker har lov til at flytte bordet med henblik på at placere patienten i udstyret og for at frigøre patienten sikkert. Inden lokalet forlades, skal den lokale tekniker altid tilbagekalde fjernbrugerens adgang.

-  **ADVARSEL!** Hold altid øje med lokalet via videokameraet, og sikre kommunikation med Lokal tekniker, før der udføres nogen aktiviteter.
-  **ADVARSEL!** Hvis forbindelsen til den lokale computer mistes, skal du straks kontakte Lokal tekniker og afbryde forbindelsen.
-  **ADVARSEL!** **I tilfælde af scannervedligeholdelse:**
Efter at være blevet informeret om påbegyndelsen af vedligeholdelsen af udstyret, skal du sikre, at adgangen er blevet tilbagekaldt af Lokal tekniker, og logge af nCommand Lite-plattformen.
Hvis adgangen ikke er blevet tilbagekaldt, skal du logge af nCommand Lite-plattformen og straks kontakte Lokal tekniker for at underrette vedkommende.
-  **ADVARSEL!** For at fjernstyre musen og tastaturet skal den valgte adgangstilstand være Kontrol; i Visningstilstand har Fjerntekniker kun tilladelse til at se streaming og lokale kameraer.
-  **ADVARSEL!** Hvis svaret på din anmodning tager længere tid end forventet, skal du kontakte den lokale tekniker via chat eller telefon.

Fjernteknikerens arbejdsområde inkluderer udstyr som en computer, skærme (typisk tre), en mus, et tastatur og et headset.

I det kliniske arbejdsforløb har *lokale teknikere* direkte kontakt med patienten. De er ansvarlige for patientkontakt, positionering samt for at sikre sikkerhed og overholdelse af protokoller under MR-, CT- eller PET/CT-undersøgelser i overensstemmelse med institutionelle og lovmæssige standarder.

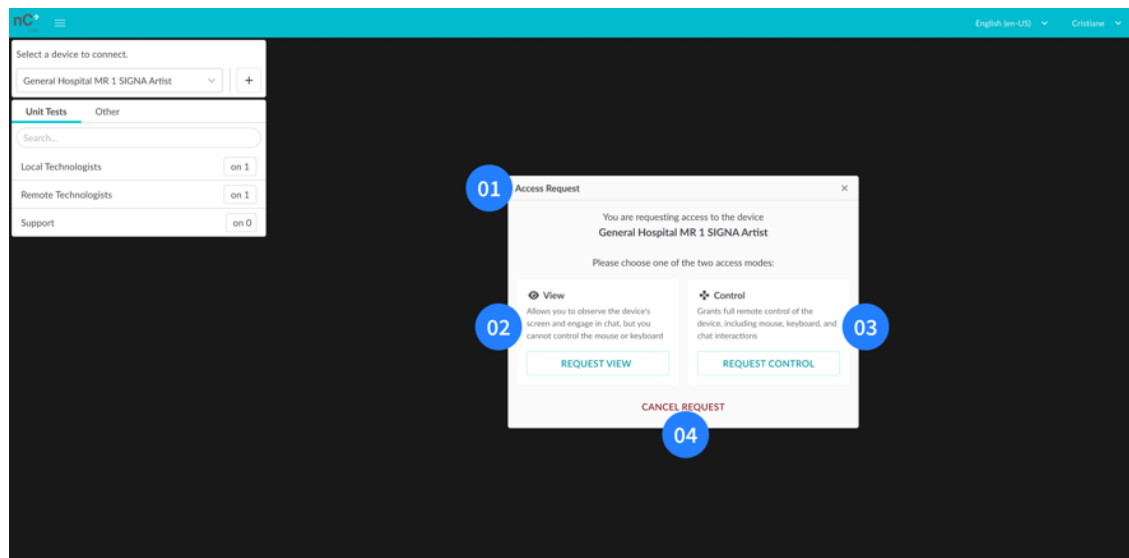
3.5.1. Adgangstilstand

Når du har logget på platformen, skal du vælge det udstyr, du vil oprette forbindelse til, i feltet Device Selection (Valg af udstyr). Et pop op-vindue åbner, så du kan vælge adgangstilstand mellem **Kontrol** og **Vis**:

- **Kontroltilstand** – I denne tilstand er både mus- og tastaturkontrol og skærmvisning aktiveret. Lokale fagfolk bevarer fuld adgang til den lokale mus og det lokale tastatur og kan til enhver tid tage kontrollen.
- **Visningstilstand** – Her er det kun muligt at se udstyrets skærm og kommunikere via chatfunktionen.

Når der vælges adgangstilstand, bliver der vist et felt med meddelelsen "Waiting for approval" (Afventer godkendelse), som angiver, at godkendelsen fra den lokale, tilsluttede tekniker er påkrævet for at fortsætte. Denne lokale tekniker har fuld bemyndigelse til når som helst at godkende eller afvise adgang og tilbagekalde adgang, hvis det skønnes nødvendigt. Denne foranstaltning er afgørende for at sikre streng kontrol og opretholde sikkerhed, når udstyret anvendes.

Efter valg af udstyr har brugeren adgang til chatfunktionen, hvilket muliggør kommunikation via tekst, lydbeskeder, stemme- og videoopkald med de andre brugere. Brugeren behøver ikke at være godkendt for at have adgang til chat-funktionen.



Figur 14: Adgangsanmodningsdialog for Fjerntekniker

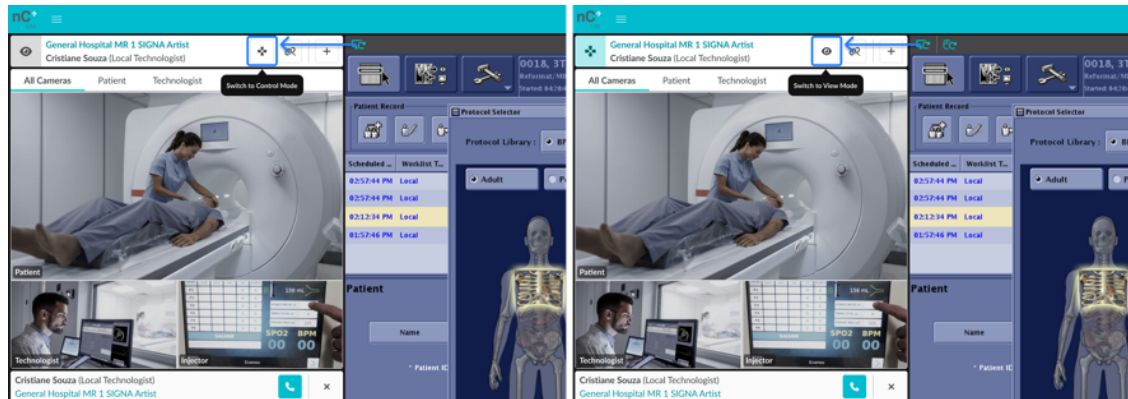
01 – Titel (Anmodning om adgang); **02** – Beskrivelse af visningstilstand og knappen Anmod om visning; **03** – Beskrivelse af kontroltilstand og knappen Anmod om kontrol; **04** – Annuller anmodning

Når adgang til udstyret er blevet godkendt af den lokale tekniker, vil fjernteknikerens grænseflade blive opdateret, så den viser live-feed for udstyret og dets tilknyttede kameraer. Hvis den valgte adgangstilstand er Control (Kontrol), aktiveres muligheden for fjernbetjening af udstyret.

Denne proces sikrer effektiv og sikker interaktion, hvilket muliggør sikker fjernbetjening af udstyret uden at kompromittere dets integritet eller patientsikkerheden.

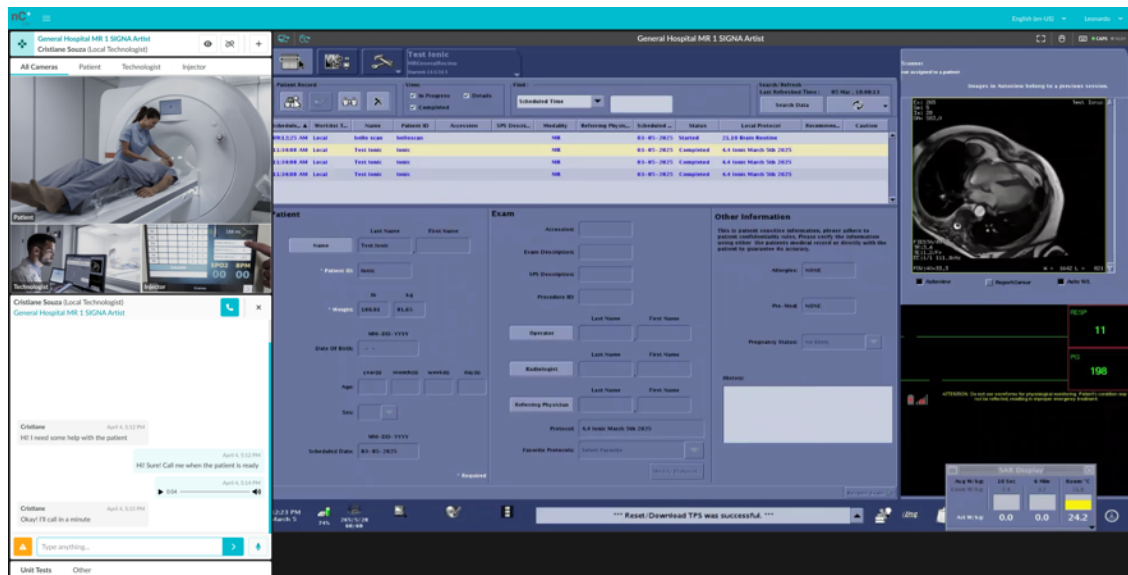
Klik på det tilsvarende ikon for at anmode om et skift af adgangstilstand under en fjernsession. Den lokale tekniker kan acceptere eller afvise anmodningen:

- **Accepter** – streaming genindlæses, uden at chatindhold går tabt. Hvis du er i gang med et tale- og videoopkald, afsluttes det og skal genstartes af en af brugerne.
- **Afvis** – der vises et popup-vindue, der giver dig besked om den lokale teknikers afvisning, og den aktuelle adgang forbliver aktiv



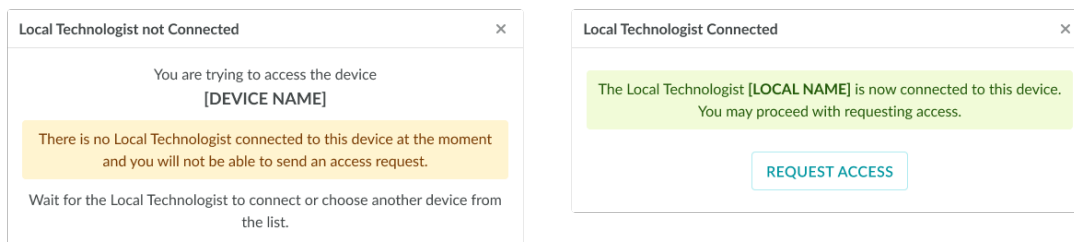
Figur 15: Skift adgangstilstand

Venstre - Skift til kontroltilstand ikon og værktøjstip / **Højre** - Skift til visningstilstand ikon og værktøjstip



Figur 16: Fjernteknikerens hovedskærm ved tilslutning til en enhed

Når fjernteknikeren anmoder om adgang, og der ikke er forbindelse til en lokal tekniker på udstyret, viser platformen en pop up-advarsel. Så snart den lokale tekniker opretter forbindelse, informerer platformen fjernteknikeren om, at de kan anmode om adgang igen.



Figur 17: Advarsler fra Fjerntekniker om Lokal teknikers forbindelsesstatus

Venstre - Meddelelse, der angiver, at der blev gjort et forsøg på at få adgang til enheden, men at der ikke er tilknyttet en Lokal tekniker i øjeblikket.

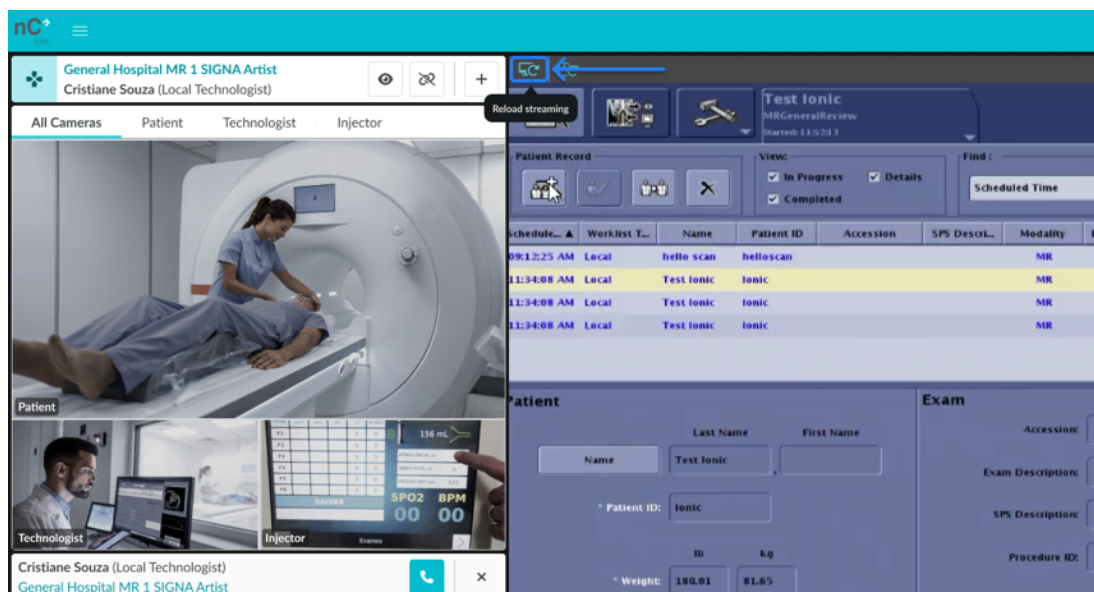
Højre - Meddelelse, der bekræfter, at Lokal tekniker har oprettet forbindelse til udstyret, efter at der tidligere ikke var forbindelse.

3.5.2. Streaminglinje

Streaminglinjen viser vigtige oplysninger og kontroller relateret til enhedens streamingssession. Det inkluderer knapperne "Reload Streaming" (Genindlæs streaming) og "Mouse Resync" (Resynkronisering af mus), enhedens navn, skærmopløsningen og den aktuelle status for fjerntcomputerens mus og tastatur.

1 – Genindlæs streaming

Denne funktion giver fjernteknikere mulighed for at genoprette adgangen til udstyr i tilfælde af forbindelsesfejl eller nedsat ydeevne. Hvis du oplever nogen former for afbrydelse eller skærmforsinkelse på enhedens computer, kan du klikke på ikonet "Reload Streaming" (Genindlæs streaming) i streaminglinjen. Dette vil bede platformen om at genoprette forbindelsen til enhedens computer samt genindlæse systemkameraerne.

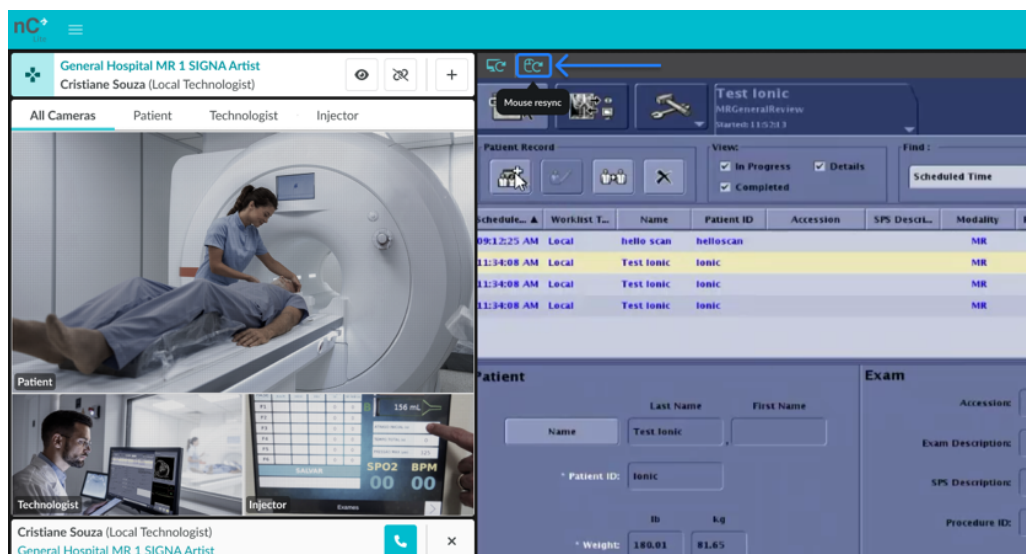


Figur 18: Genindlæs streaming-knap

2 – Mouse Resync (Resynkronisering af mus)

I tilfælde af en langsom eller forkert justeret mus klikker du på knappen "Mouse Resync" (Resynkronisering af mus) på linjen over streamingvinduet for at resynkronisere udstyrets mus ved hjælp af e-KVM-computeren.

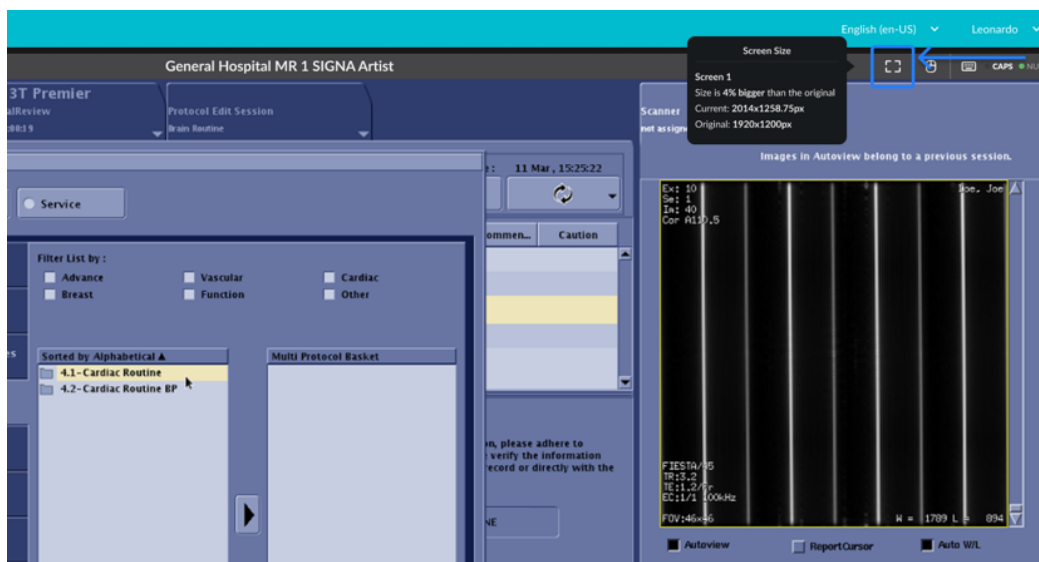
Et alternativ er at flytte musemarkøren uden for streamingområdet og derefter bringe den tilbage, systemet vil automatisk gensynkronisere musen uden yderligere handling. Du kan også klikke og slippe musehjulsknappen (når det er tilgængeligt) for automatisk at aktivere resynkroniseringen. Dog virker denne metode muligvis ikke på enheder med to eller flere skærme, hvis de lokale og fjernstyrede musemarkører er på forskellige skærme.



Figur 19: Muse-resynkroniseringsknap

3 – Streamingvisning

Denne funktion giver fjernteknikeren oplysninger om den oprindelige streamingopløsning (fra enheden) og den aktuelle opløsning i pixels, der vises på den eksterne arbejdsstation.



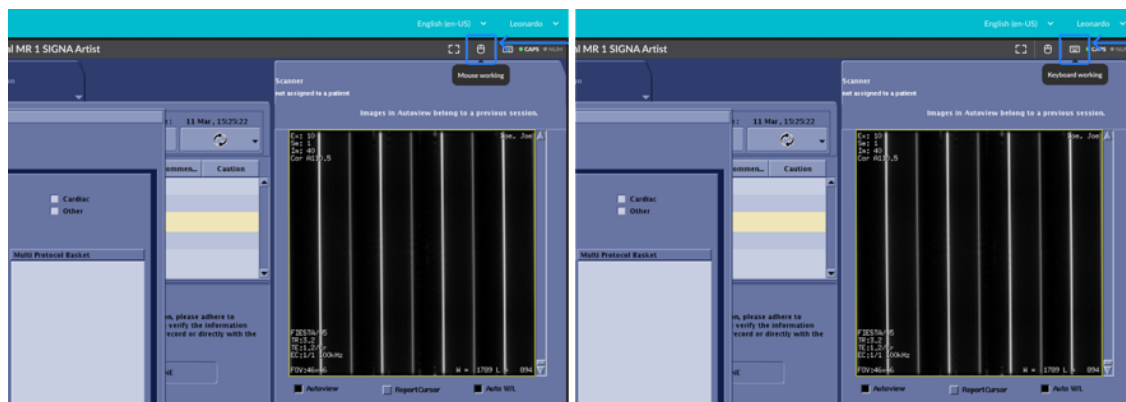
Figur 20: Værktøjstip til streaminginformation

4 – Status for mus og tastatur

Denne funktion informerer fjernteknikeren om, hvorvidt musen og tastaturet fungerer korrekt. Sammen med tastaturstatus kan brugeren se, om tastaturetasterne **Caps lock** og **Num Lock** på udstyrets computer er tændt eller slukket. Denne funktionalitet afhænger imidlertid af, at computerudstyret leverer disse oplysninger. I situationer, hvor disse oplysninger ikke gøres tilgængelige af udstyrssystemet, vises status for tasterne **Caps Lock** og **Num Lock** ikke. Både musens og tastaturets status vises kun, når brugeren anvender adgangstypen Kontrol.

Når der oprettes forbindelse til udstyr, kan en uoverensstemmelse mellem **Caps Lock**- og **Num Lock**-indikatorerne på fjerncomputeren og udstyret føre til usammenhængende indtastninger. Hvis indikatorerne ser ud til at være aktiveret på udstyret, men ikke er aktive på fjerncomputeren, kan brugeren eventuelt foretage indtastninger med store bogstaver på udstyret, mens denne tekst vises med små bogstaver i chat-funktionen eller omvendt. Hvis **Caps Lock** er aktiveret på fjerncomputeren, men deaktiveret på udstyret, vil det samme problem opstå i omvendt rækkefølge.

For at forhindre dette problem skal det sikres, at **Caps Lock** og **Num Lock** enten begge er aktiveret, eller begge er deaktiveret, før der logges på udstyret. Hvis der opstår en uoverensstemmelse, skal brugeren afbryde forbindelsen til udstyret, justere nøglestatus på fjerncomputeren og derefter oprette forbindelse igen.

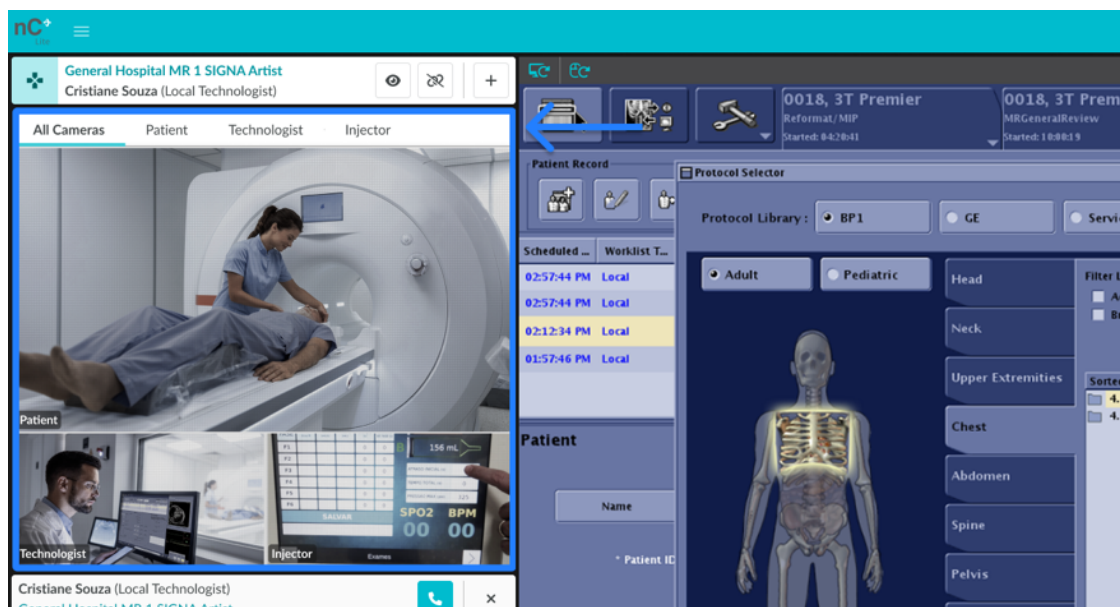


Figur 21: Streaming Bar

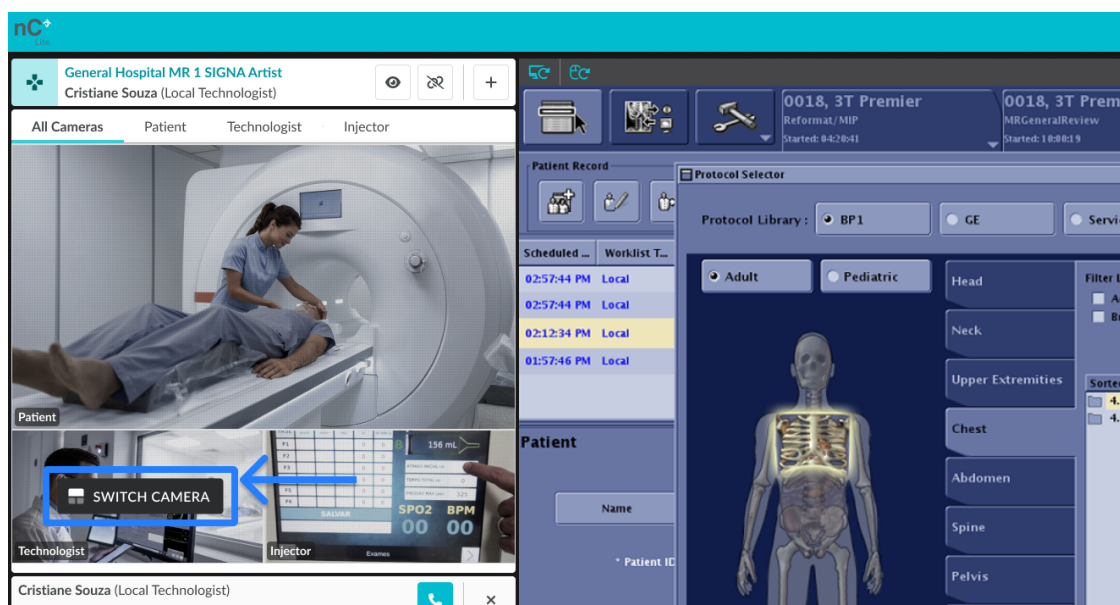
*Venstre - Musestatus-værktøjstipinformation
Højre - Tastaturstatus Tooltip-information*

3.5.3. Multikamera

Denne funktion gør det muligt for fjernteknikeren at se flere kameraer på samme tid. Hvis der er mere end ét kamera tilgængeligt, er det muligt kun at se ét kamera og skifte mellem dem ved at klikke på menuen med det navn, der er angivet for hvert kamera. Ved at vælge "ALL CAMERAS" (ALLE KAMERAER) vises alle tilgængelige kameraer i billedrammen, hvor ét af dem er fremhævet. Der skiftes til det fremhævede kamera ved at holde musen hen over et af kameraerne i den lille ramme og klikke på "SWITCH CAMERA" (Skift kamera).



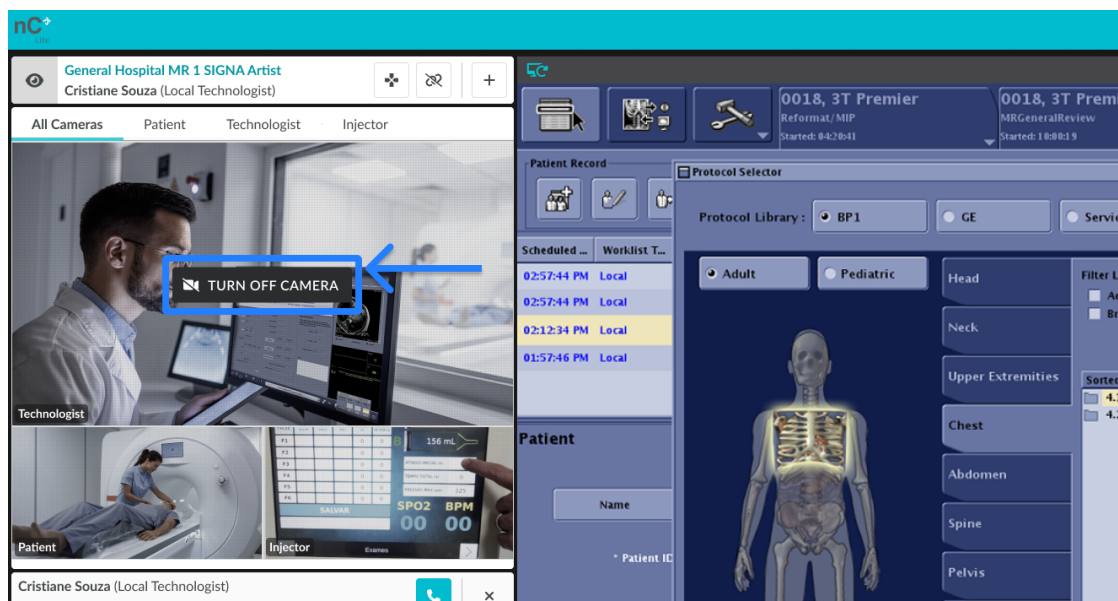
Figur 22: Multi-kamera rammevisning



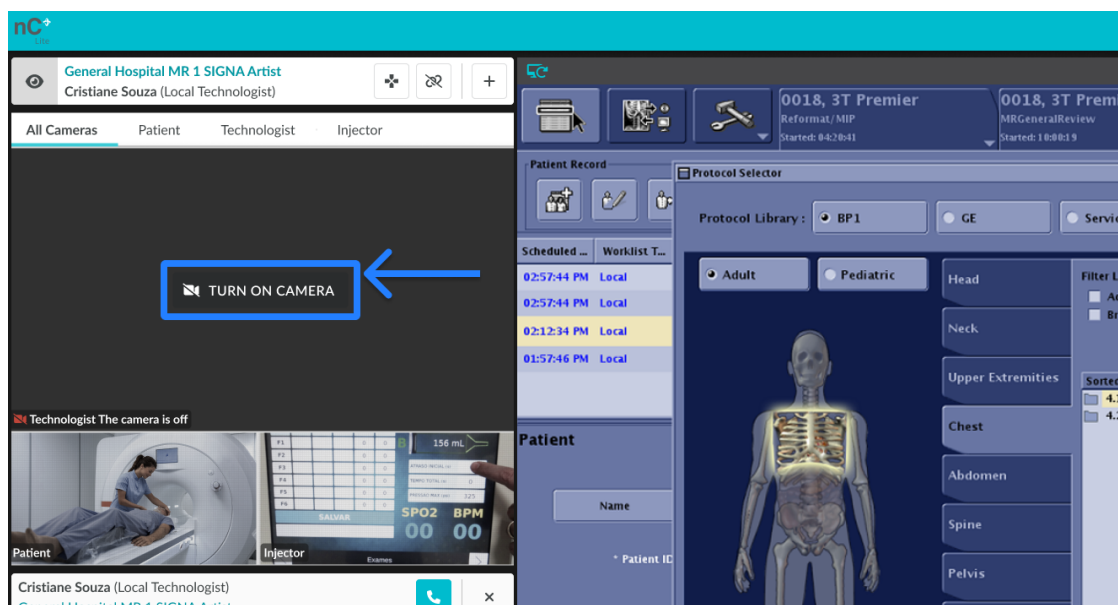
Figur 23: Multi-kamera "SWITCH CAMERA" Hover-knap

Hvis fjerneteknikeren under en aktiv fjernsession skaffer adgang som **Vis**, er det muligt at slukke for et eller flere kameraer ved at holde musen over det valgte kamera og klikke på "TURN OFF" (SLUK). Hvis du vil se kameraet igen, skal du blot gentage processen og klikke på "TURN ON CAMERA" (Tænd kamera).

BEMÆRK: Muligheden for at slukke for kameraer er kun tilgængelig i tilstanden Vis. I kontroltilstand er det ikke muligt at slukke for kameraerne.



Figur 24: Multi-kamera "SLUK KAMERA" Hover-knap i visningstilstand



Figur 25: Multi-kameraets "TURN ON CAMERA" hoverknap i tilstanden Vis

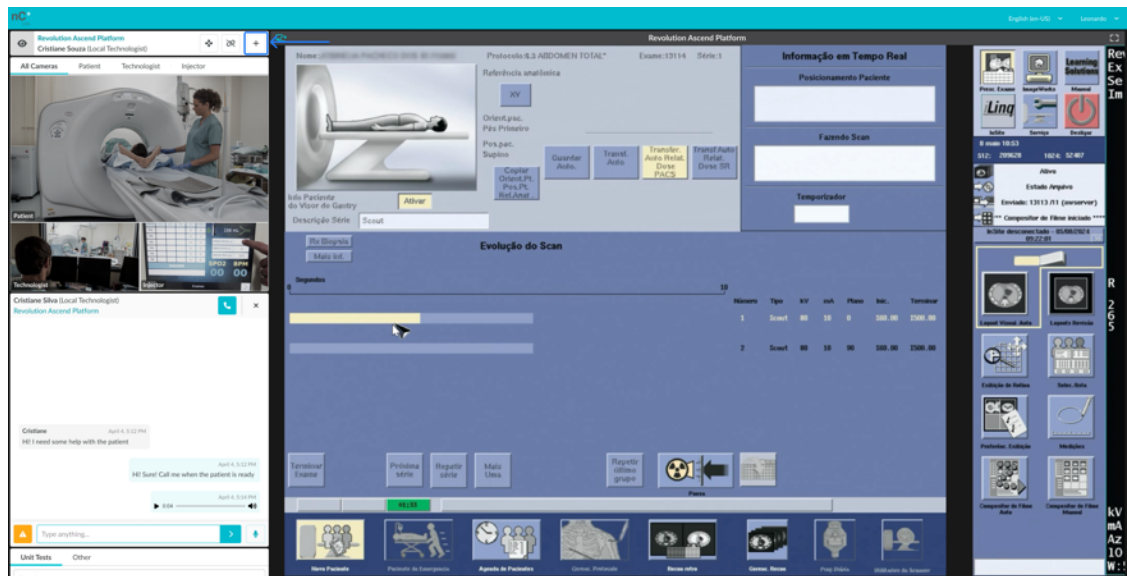
3.5.4. Åbn en anden enhed

Giver fjern teknikeren mulighed for at åbne en ny browserfane i nCommand Lite, hvilket gør det muligt for brugeren at vælge nyt udstyr for at udføre mere end én fjernscanning samtidigt. Hvis du vil åbne for nyt udstyr og få adgang, skal du blot klikke på knappen "Open Another Device" (Åbn en anden enhed), hvorefter du får vist en advarsel, så du kan udføre denne samtidige handling på sikker vis. Du skal læse advarslen, før du åbner dette nye vindue.

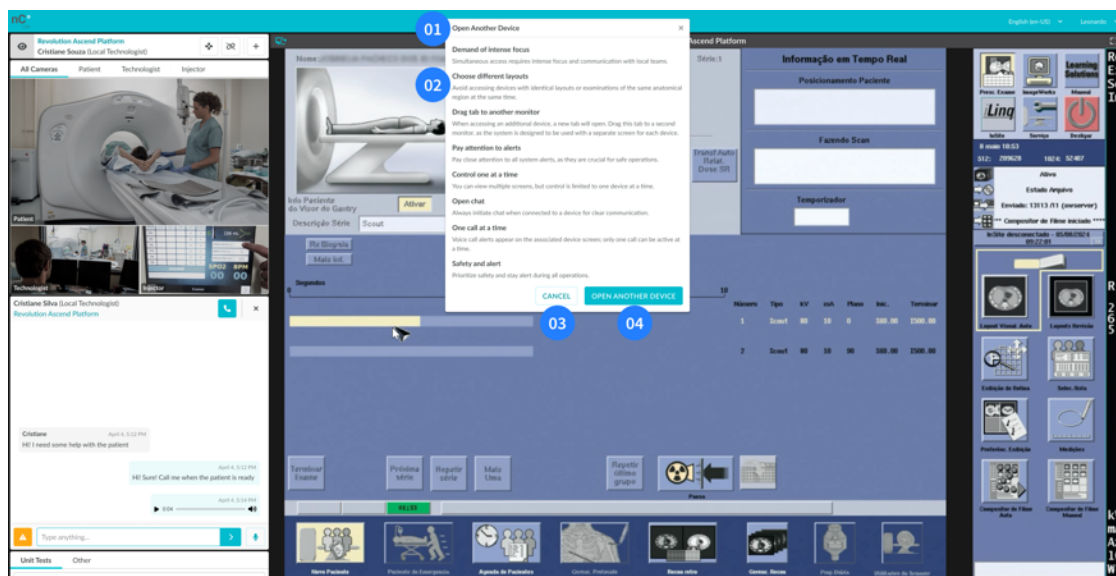
BEMÆRK: For bedre visning under samtidig adgang anbefales det, at du, efter at du har klikket på "ÅBN EN ANDEN ENHED" og klikket på "OK" i advarslerne, trækker den nye fane til en anden tilgængelig skærm..

**ADVARSEL!****Sikkerhedsadvarsel for adgang til flere scannere**

- **Demand of intense focus (Behov for intenst fokus):** Samtidig adgang kræver intens fokus og kommunikation med lokale teams.
- **Choose different layouts (Vælg forskellige layouts):** Undgå at få adgang til enheder med identiske layouts eller undersøgelser af det samme anatomiske område på samme tid.
- **Drag tab to another monitor (Træk fanen til en anden skærm):** Når du får adgang til andet udstyr, åbnes der en ny fane. Træk denne fane til en anden skærm, da systemet er designet til at blive brugt med en separat skærm til hver enhed.
- **Pay attention to alerts (Vær opmærksom på advarsler):** Vær meget opmærksom på alle systemadvarsler, da de er afgørende for sikker drift.
- **Control one at a time (Kontrollér én ad gangen):** Du kan se flere skærbilleder, men styringen er begrænset til én enhed ad gangen.
- **Open chat (Åbn chat):** Start altid chatten, når du er forbundet til en enhed, for at sikre tydelig kommunikation.
- **One call at a time (Ét opkald ad gangen):** Alarmer for taleopkald vises på den tilknyttede enheds skærm; kun ét opkald kan være aktivt ad gangen.
- **Safety and alert (Sikkerhed og opmærksomhed):** Prioritér sikkerheden, og vær opmærksom under alle procedurer.



Figur 26: Åbn knappen Anden enhed (+)



Figur 27: Advarsler om adgang fra flere enheder

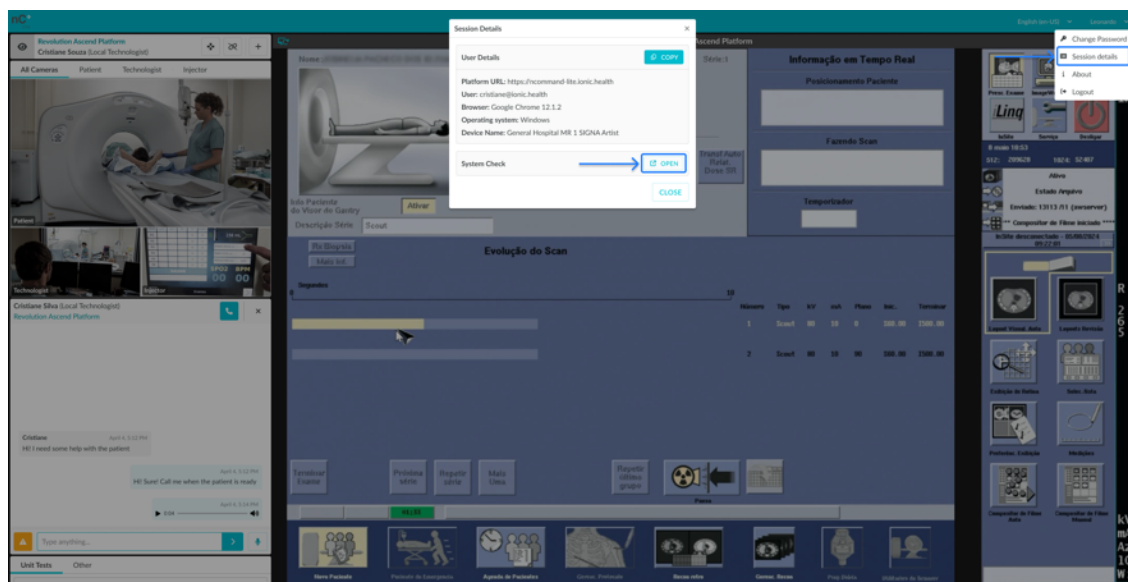
01 – Titel (Åbn en anden enhed); **02** – Advarsler om driftssikkerhed; **03** – Aannuler knappen
04 – Knappen Open Another Device (Åbn en anden enhed)

3.5.5. Systemkontrol

Systemkontrollfunktionen hjælper med at verificere, at den aktuelle enhed, netværk og internetforbindelse opfylder kravene til korrekt brug af nCommand Lite. Den udfører en hurtig automatisk test, der tjekker væsentlige elementer som internetkvalitet, adgang til nødvendige servere og forbindelsesstabilitet. Dette værktøj kan bruges før start af en session, under installationen, eller når der er mistanke om forbindelsesproblemer. Det hjælper med at sikre, at platformen fungerer som forventet, og assisterer det tekniske team, hvis fejlfinding er nødvendig.

Bemærk: Systemkontrollen bør helst bruges med support eller efter anmodning fra en IT-professionel. At køre dette værktøj uden teknisk vejledning kan føre til fejltolkning af resultaterne.

For at få adgang til Systemkontrol skal lokale teknikere og Fjerntekniker åbne Session Details-muligheden fra rullemenuen under deres brugernavn, som findes i øverste højre hjørne af hovedskærmen. Klik derefter på **Open** ved siden af **Systemkontrol**-værktøjet. Når værktøjssiden vises, klik på **Kør Test** for at starte verifikationsprocessen.

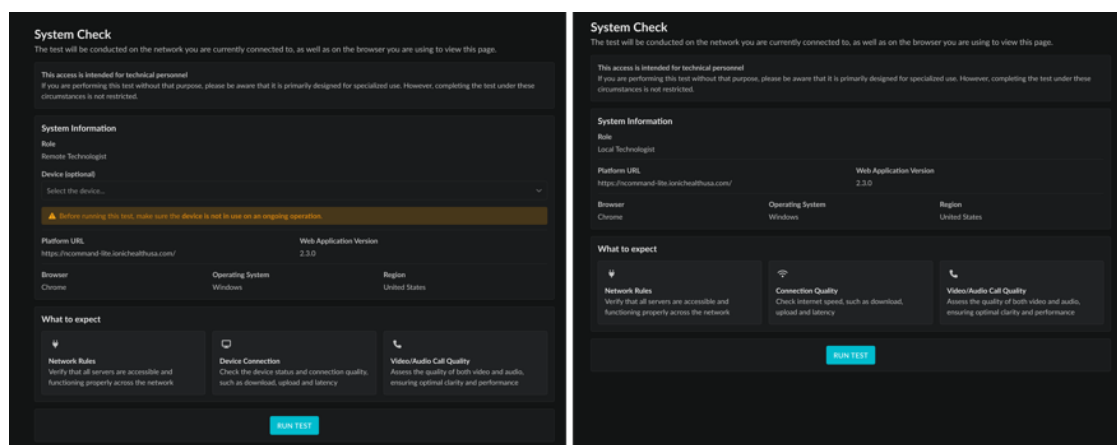


Figur 28: Adgang til Systemkontrol

Når man bruger fjernteknikeren, er det muligt at vælge en enhed på værktøjets hovedskærm, så den inkluderes i testresultaterne.

**ADVARSEL!**

Før du starter testen, skal du sikre dig, at den valgte enhed ikke er i brug lige nu.



Figur 29: Systemkontrol hovedskærm
Venstre - Fjerntekniker / Højre - Lokal tekniker

Når testen er afsluttet, vises et resumé af resultaterne på skærmen. IT-professionelle kan gennemgå disse oplysninger for at identificere mulige problemer, der påvirker systemets ydeevne.

Afsnit 3.6 - Chat

Platformen tilbyder en chat- og opkaldsfunktion i realtid med stemme- og videoegenskaber, som anvendes til effektiv kommunikation mellem autoriserede teknikere. Gennem disse funktioner kan de autoriserede teknikere kommunikere om alle forhold, der vedrører arbejdsgangen for sessionen.

**ADVARSEL!**

I tilfælde af fejl skal du ringe til den lokale tekniker.

Når du opretter forbindelse til en enhed, får du øjeblikkelig adgang til chatbrugerlisten, der er organiseret i to faner. For kunder med flere lokationer kan hver filial konfigureres som en separat kontrakt. Når den er aktiveret, grupperes brugere efter kontrakt, hvor brugere fra andre kontrakter vises under fanen "Andre".

For at starte en samtale skal du dobbeltklikke på en brugers navn for at åbne chatgrænsefladen, som understøtter både tekstbeskeder og taleopkald. Sørg for, at den valgte session svarer til den korrekte enhed. Platformen giver brugerne besked, hvis netværksforbindelsen bliver langsom eller ustabil.

**ADVARSEL!**

Før du starter kontakten, skal du kontrollere enhedens navn, der er vist under brugerens navn, da nogle fjernteknikere kan være forbundet til flere enheder.

Her er de tilgængelige værktøjer til kommunikation inden for platformen:

1. **Stemme- og videoopkald:** Klik på ikonet for at starte et tale- og videoopkald på op til 60 minutter mellem en fjerntekniker og en Lokal tekniker. Forbindelser mellem brugere med samme profil (Lokal-Lokal eller Fjern-Fjern) understøttes ikke.

Når en lokal tekniker starter et opkald, kan fjernteknikeren vælge at acceptere eller afslå. Omvendt, når en Fjerntekniker initierer opkaldet, forbindes det automatisk, og Lokal tekniker bliver underrettet—disse funktioner fungerer som en sikkerhedsmekanisme for at sikre, at Fjerntekniker altid kan kommunikere med den person, der fysisk er til stede på stedet, som var de til stede personligt.

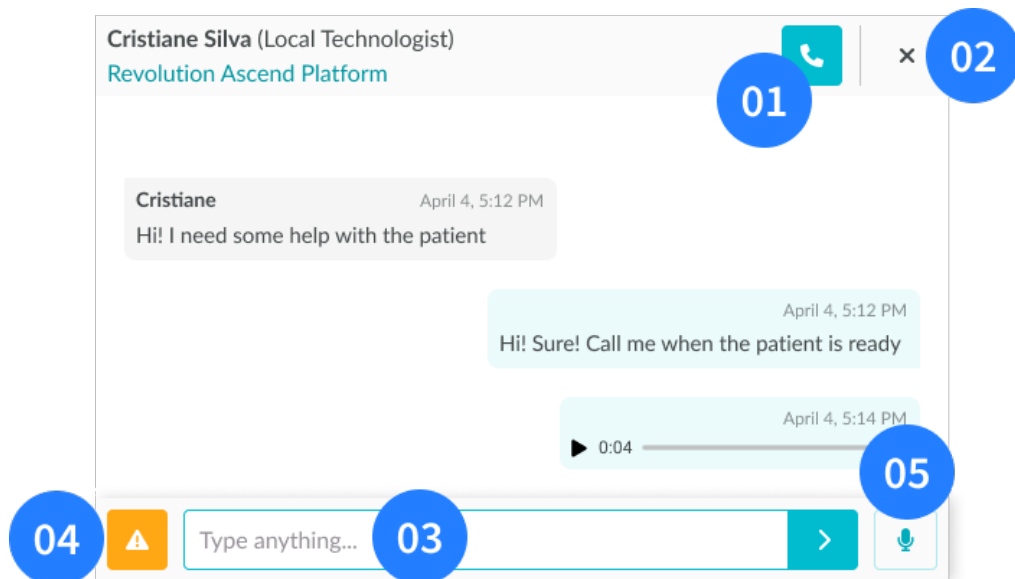
Som standard er mikrofonen aktiv fra starten af opkaldet, mens kameraet er slukket. Den enkelte tekniker kan til enhver tid manuelt tænde eller slukke for mikrofon og kamera.

For at kunne foretage et opkald skal begge brugere have en fungerende mikrofon og lydudgang med korrekt aktiverede browsertilladelser. Hvis en eller flere af disse komponenter mangler, vil systemet give begge brugere besked, og opkaldet vil ikke blive gennemført. Kamera er valgfrit – hvis det ikke er tilgængeligt eller ikke registreres, vil systemet opdatere ikonet for at afspejle, at video ikke understøttes.

Kun ét aktivt opkald pr. bruger er tilladt. Hvis en tekniker forsøger at foretage et nyt opkald, hvor vedkommende allerede er i gang med et, blokerer systemet forsøget og viser en meddelelse. På samme måde er det, hvis en bruger allerede er i gang med et opkald og modtager et andet indgående opkald, vil opkalderen blive informeret om, at modtageren i

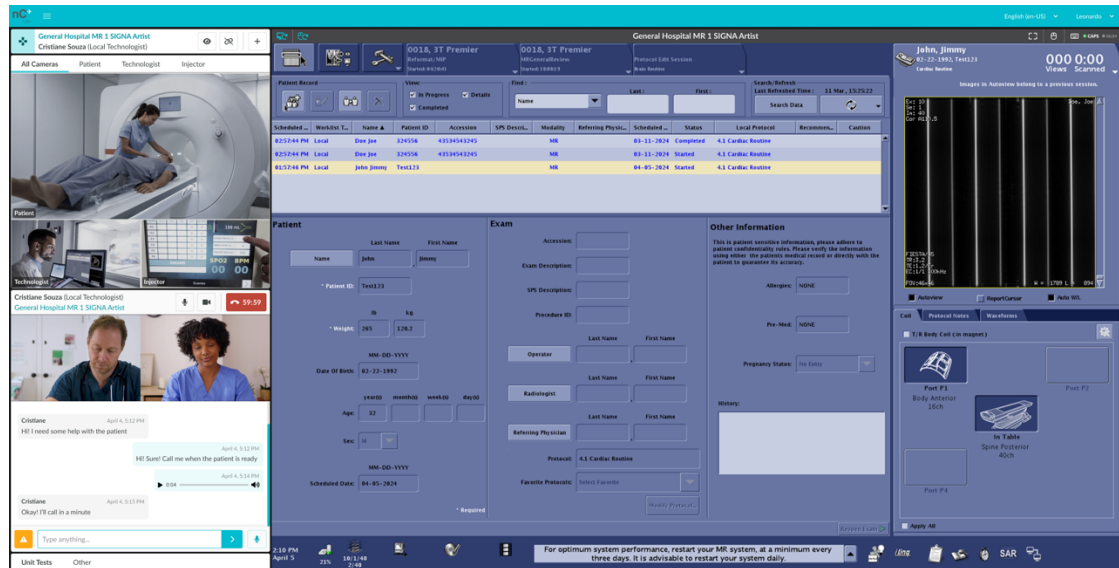
øjeblikket ikke er tilgængelig, og brugeren i det igangværende opkald vil modtage en advarsel, der angiver, at nogen har forsøgt at kontakte brugeren.

2. **Lukning af chats:** Når en af brugerne lukker chatten ved at klikke på lukkeknappen, sendes der automatisk en meddelelse til den anden bruger, og chatfanen lukkes. Dette sikrer, at begge parter informeres om, at samtalen er afsluttet. Når chatvinduet lukkes, forsvinder alle meddelelser. Hvis du åbner det igen under sessionen, starter samtalen igen uden de tidligere meddelelser.
3. **Tekstbeskeder:** Send tekstbeskeder i det angivne felt. Når der sendes en besked, vises der et ikon med et gråt flueben, og når beskeden er blevet modtaget af modtageren, vises et andet ikon med to blå flueben. Dette giver mulighed for sikker, klar og præcis skriftlig kommunikation mellem de to parter.
4. **Tilkald opmærksomhed:** Tiltræk den anden brugers opmærksomhed ved at klikke på knappen med et udråbstegn. Denne handling anvender en visuel vibrationseffekt i den anden brugers vindue i et par sekunder, og der sendes automatisk en besked, som signalerer, at det haster eller er vigtigt.
5. **Lydbeskeder:** Send lydbeskeder ved at klikke på mikrofonknappen. Dette bruges, når du ønsker at viderebringe en besked mere personligt, eller når det ikke er praktisk at skrive.

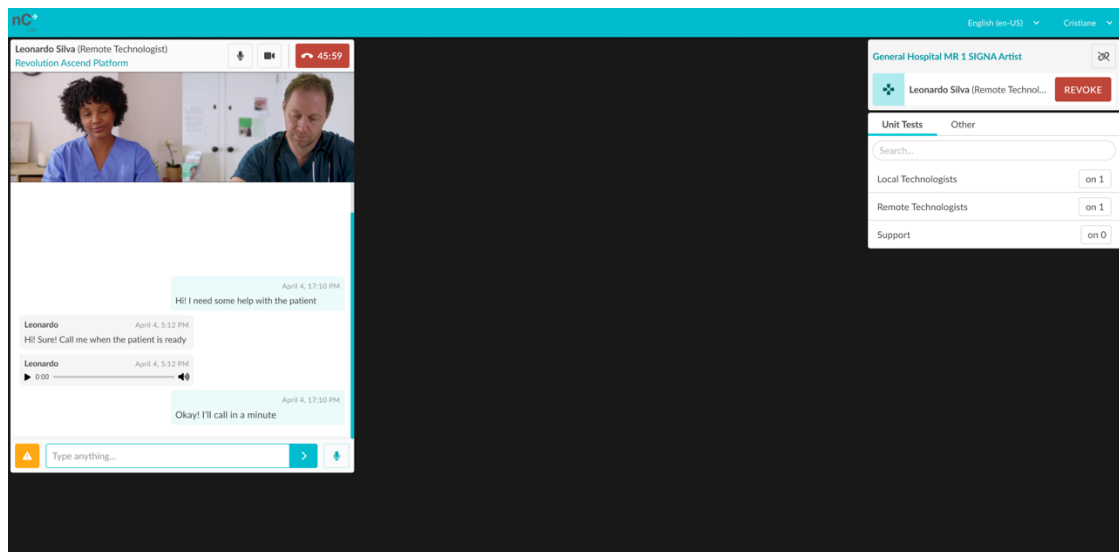


Figur 30: Chatvinduesvisning

- 01** – Knappen Voice and Video Call (Tale- og videoopkald); **02** - Knappen Close Chat (Luk chat);
03 – Beskedtekstboks; **04** – Knappen Call for attention (Tilkald opmærksomhed);
05 – Knappen Record Audio Message (Optag lydbesked)



Figur 31: Fjernteknikerens hovedskærm – Chatvindue (nederste venstre hjørne)



Figur 32: Lokal tekniker hovedskærm - chatvindue

Problemer med internetforbindelse – Hvis en af teknikerne oplever problemer med netværksforbindelsen, viser systemet en meddelelse og forsøger at genoprette forbindelsen. Hvis forbindelsen genoprettes, viser systemet en **ONLINE**-meddelelse, og fjernsessionen fortsætter som normalt. Hvis der ikke er genoprettet forbindelse efter flere forsøg, afslutter systemet imidlertid den aktive session og underretter teknikeren om, at forbindelsen er blevet afbrudt på grund af internetproblemer. Samtidig vil systemet også underrette den anden tekniker om, at vedkommendes modpart er blevet frakoblet på grund af internetproblemer.

Afsnit 3.7 - Afslutning af din session på platformen

Ved afslutningen af arbejdet skal den licenserede tekniker afbryde forbindelsen til udstyret og logge af platformen.

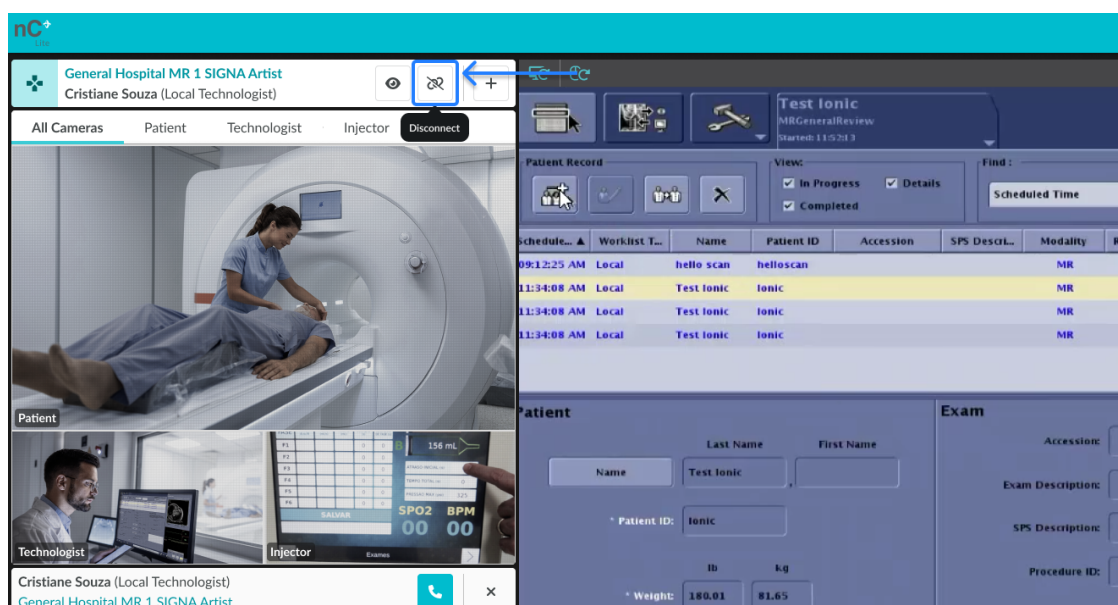


ADVARSEL!

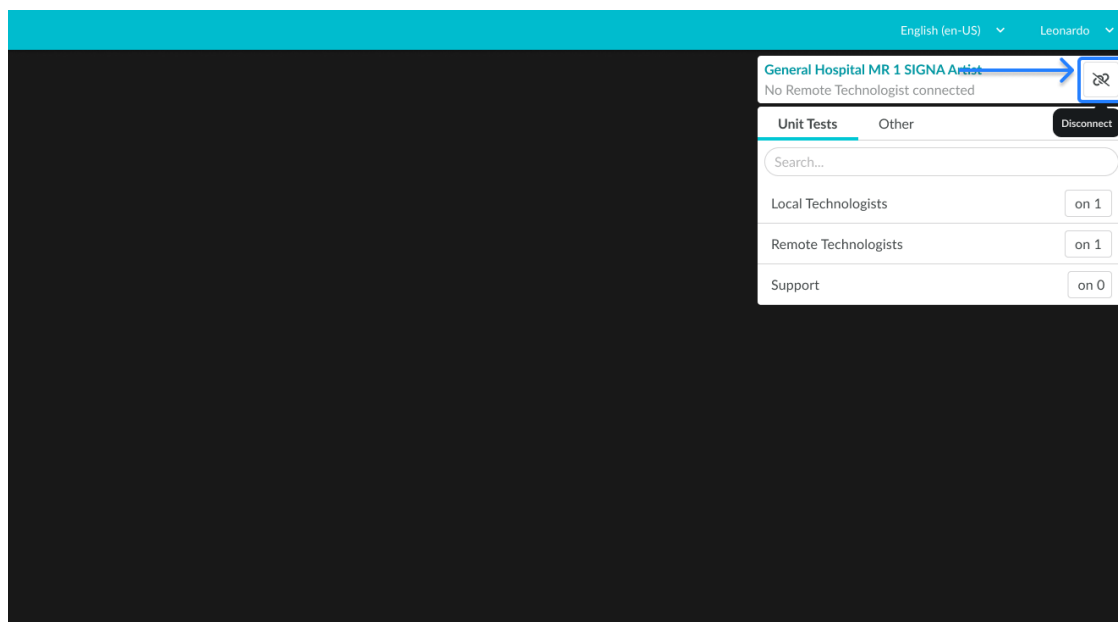
Autoriserede teknikere må ikke glemme at logge ud af platformen, når deres arbejde er slut.

For at afbryde forbindelsen til udstyret skal du klikke på forbindelsesikonet i udstyrsfeltet. Bemærk: Hvis du arbejder som lokal tekniker, skal du sikre dig, at du har tilbagekaldt al fjerntekniker-adgang, inden du afbryder forbindelsen til udstyret.

Af sikkerhedshensyn vil du modtage en meddelelse til bekræftelse af, at du ønsker at afbryde forbindelsen til udstyret. Efter bekræftelsen bliver du sendt videre til startskærmen, uden at der er valgt noget udstyr.



Figur 33: Afbryd-knap - Fjernteknikerens hovedskærm



Figur 34: Afbryd-knap – Lokal tekniker hovedskærm

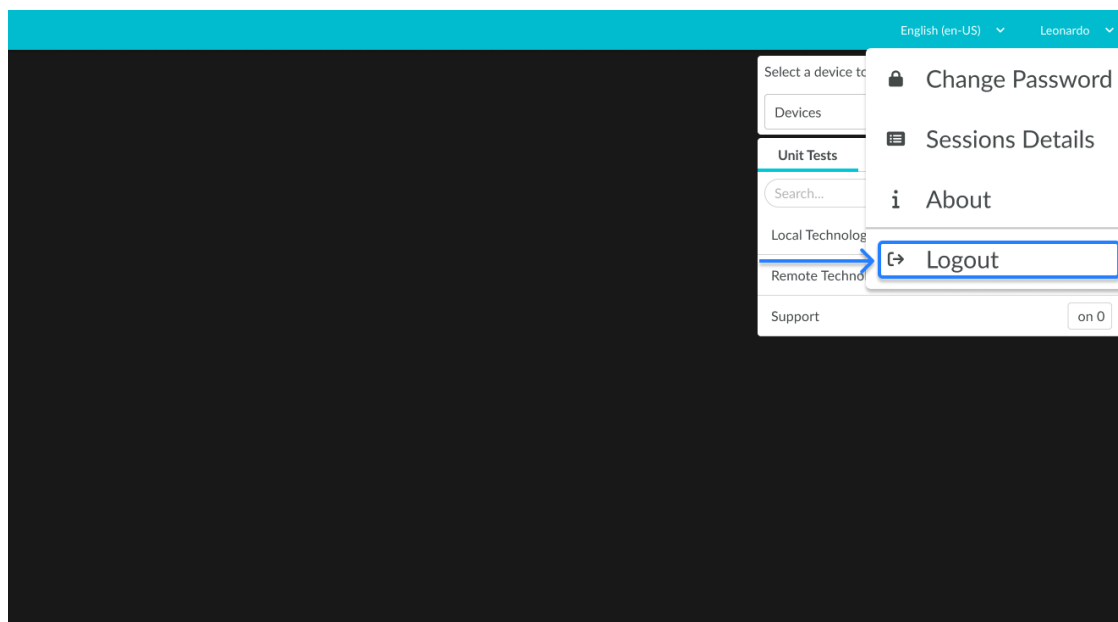


ADVARSEL!

Før du logger af, skal du sikre dig, at alle yderligere faner, der blev åbnet, er lukket.

For at afslutte din session på platformen skal du klikke på dit brugernavn i øverste højre hjørne af skærmen, og vælge valgmuligheden "Logout" (Log ud). Du vil modtage en meddelelse om at bekræfte, at du ønsker at forlade faciliteten, hvor du arbejder. Når du har bekræftet, vil du blive sendt videre til programmets login-side, hvilket er en bekræftelse på, at dit arbejde er sikkert afsluttet.

nCommand Lite styrer ikke brugerens session på den eksterne identitetsudbyder og kan derfor ikke udføre en logout på identitetsudbyderniveau. I scenarier, hvor brugere deler den samme maskine og bruger Single Sign-On (SSO), anbefales det, at hver bruger vælger indstillingen "do not stay signed in" (forbliv ikke logget på) under eksternt identitetsudbyder-login (hvis tilgængeligt) eller logger ud af identitetsudbyderen efter at have logget ud af nCommand Lite. Dette sikrer, at ingen efterfølgende bruger på den samme enhed utilsigtet kan genbruge en aktiv session.



Figur 35: Log ud-dropdownmenupunkt



ADVARSEL!

Når du bruger en ekstern identitetsudbyder på en delt eller offentlig computer, skal du også logge af identitetsudbyderen efter at have logget ud af platformen. Du kan få flere oplysninger om, hvordan du fortsætter, ved at kontakte organisationens it-supportteam.

Afsnit 3.8 - Undervisning i betjening

Deltagelse i undervisningsprogrammet er obligatorisk for alle brugere af nCommand Lite-systemet. Brugerregistrering på platformen administreres af IONIC Health-teamet og igangsættes først, når det er bekræftet, at brugeren har gennemført det krævede LMS-kursus og er behørigt kvalificeret til at betjene platformen. Denne proces sikrer, at alle brugere har en grundig forståelse af systemets funktionaliteter og er forberedt på at bruge platformen effektivt og sikkert. Kontakt din salgsrepræsentant for at starte tilmeldingsprocessen.

Afsnit 3.9 - Retningslinjer for fejlfinding

BRUGER OG ADGANGSKODE	
Ændring af adgangskode	Bekræft, at kravene til kodeordet er opfyldt; kodeordet skal være stærkt og sikkert og indeholde mindst ét lille bogstav, ét stort bogstav, ét specialtegn og skal være på mindst 8 tegn.
Har glemt min adgangskode	Tjek din e-mailindbakke: Sørg for, at du bruger den korrekte e-mailadresse, og at e-mailen til genoprettelse af adgangskoden ikke er blevet sendt til mapper med uønsket mail. Prøv igen: Vent et par minutter, og anmod om en ny e-mail vedrørende gendannelse af adgangskode ved at klikke på "Did you Forget your password?" (Har du glemt din adgangskode?). Kontrollér internetforbindelsen: Sørg for, at du er koblet på internettet.
Velkomstmil ikke modtaget	Tjek, om e-mailen er i din spammappe. Hvis den ikke er der, skal du kontakte en admin-bruger for at sikre, at den e-mail, du oplyste ved registrering, er korrekt. Hvis den ikke er korrekt, skal administratoren opdatere den og sende en ny velkomstmil.
Kode til tofaktorgodkendelse blev ikke modtaget	Klik på "Resend Code" (Send kode igen), og tjek din spammappe. Hvis du ikke modtager den, bedes du kontakte en admin-bruger for at bekræfte, om den e-mail, der er registreret i Adgangskontrol, er korrekt.
For mange loginforsøg	Hvis du har overskredet det tilladte antal loginforsøg, skal du vente et stykke tid, før du kan forsøge igen.
EKSTERN IDENTITETSUDBYDER	
Problemer med at logge ind på produktet	Hvis du støder på login-problemer, mens du bruger en ekstern identitetsudbyder (IdP), skal du være opmærksom på, at godkendelsesprocessen udelukkende administreres af identitetsudbyderen og ikke af produktudbyderen, dvs.: Ionisk

	sundhed. Som sådan kan produktet ikke hjælpe med kontooplysninger, adgangspolitikker, godkendelsesfejl eller kontospærring. I sådanne tilfælde skal du kontakte din organisations it-supportteam, som kan gennemgå identitetsudbyderkonfigurationen og hjælpe med at løse problemet.
Problemer med login-oplysninger	Eventuelle login-relaterede problemer (<i>f.eks.</i> , glemt adgangskode, ændring af adgangskode) skal løses direkte hos din organisations it-supportteam. De kan gennemgå identitetsudbyderkonfigurationen og yde den nødvendige hjælp.
Problemer med multifaktorgodkendelse (MFA)	Eventuelle problemer med multifaktorgodkendelse (MFA) (<i>f.eks.</i> problemer med udløb af MFA, MFA, der ikke fungerer, login uden at anmode om MFA) skal løses direkte hos din organisations it-supportteam. De kan gennemgå identitetsudbyderkonfigurationen og yde den nødvendige hjælp.
Login-oplysninger virker ikke på platformen	Når du bruger eksterne identitetsudbydere (IdP), kan du kun logge på produktet ved hjælp af identitetsudbyderen. Brug af login-oplysningerne til identitetsudbyder direkte på produktets login-side vil resultere i mislykket login.
SCANNERCOMPUTERENS SKÆRM	
Tænder ikke	Kontrollér skærmens forbindelser til computeren og stikkontakten. Der kan forekomme afbrydelser. Tryk på skærmens tænd/sluk-knap igen.
PLATFORM	
Ikke tilgængelig	Kontrollér netværksforbindelsen. Kontrollér, om platformen er startet, og om login har fundet sted.
Platformsventetid	Opdater siden ved at trykke på Ctrl+F5. Kontrollér, om enhedens (medicinsk facilitets) chat er åben på mere end én fane. Hvis det er tilfældet, skal du lukke den fane, der ikke er i brug. Hvis problemet fortsætter, skal du prøve at logge af platformen, rydde cachen,

	lukke browseren og derefter logge på igen.
Funktionsfejl	Før du prøver andre fejlfindingprocedurer, skal du rydde browserens cache (se efter instruktioner i din nuværende browser) efter login, derefter lukke og genåbne browseren, logge ind på platformen igen og prøve handlingen igen.
Opgrader	Når platformen er blevet opgraderet, skal du rydde din browsers cache (se instruktionerne til din browser), før du logger ind i den nye version.
LYD	
Ingen lyd	Sørg for, at lydstyrken i enhedens (medicinsk facilitets) mikrofon og højttalere er justeret til passende niveauer. Kontrollér, om browseren har tilladelse til at bruge lyd og mikrofon. Kontrollér, om headsettet er tilsluttet og fungerer korrekt.
Lydventetid	Kontrollér udstyrets elektriske forbindelser og netværksforbindelser. Opdater browsersiden ved at trykke på Ctrl+F5, og log på igen. Hvis problemet fortsætter, skal du prøve at logge af platformen, rydde cachen, lukke browseren og derefter logge på igen.
CHAT	
Chat vises ikke	Sørg for, at browseren ikke er minimeret. Ellers kan du åbne chatten, efter du har logget på nCommand Lite-platformen. Kontrollér, at enheden (medicinsk facilitet) er valgt, og at brugeren er autoriseret til at aktivere chatkommunikation. Sørg for, at din browsers lyd- og mikrofонтilladelser er blevet godkendt.

	Kontrollér kabelforbindelser, der kan være blevet frakoblet. Opdater browsersiden ved at trykke på Ctrl+F5, og opret forbindelse til platformen igen. Kontrollér, om webstedets chat er åben på mere end én fane. Hvis det er tilfældet, skal du lukke den fane, der ikke er i brug.
Chatforsinkelse	Opdater browsersiden ved at trykke på Ctrl+F5, og opret forbindelse til platformen igen. Hvis problemet fortsætter, skal du prøve at logge af platformen, rydde cachen, lukke browseren og derefter logge på igen. Kontrollér kabelforbindelser, der kan være blevet frakoblet.
Problemer med at sende lydmeddelelser	Kontrollér browsertilladelser for lyd og mikrofon, og sørg for, at både mikrofon og lydenheder er koblet til computeren. Hvis browsertilladelser skal justeres, skal du trykke på Ctrl+F5 for at bede browseren om at godkende ændringerne, når siden genindlæses.
Stemmeopkald kunne ikke startes	Kontrollér din internetforbindelse, og se, om der er blevet vist en meddelelse, der forklarer årsagen til det opkald, der ikke startede. Sørg for, at der er tilsluttet en lydenhed, og at lyd- og mikrofontilladelser er tilladt i browseren. Hvis problemet fortsætter, skal du opdatere siden med Ctrl+F5 for at prøve igen.
Bruger ikke fundet i chat	Hvis du ikke kan finde en bruger i chatten, skal du klikke på fanen "Others" (Andre) for at sikre, at de ikke er angivet der. Brugere, der er tilknyttet andre kontrakter, vises særskilt på kontaktlisten. Hvis din bruger ikke er vist på kontaktlisten efter, at du har valgt

	udstyret, skal du trykke på Ctrl+F5 for at opdatere skærbilledet og vælge igen. Sørg for, at du har internetforbindelse.
ANMODNING OM ADGANG TIL UDS TYRET	
Platformen registrerede ikke, at den lokale tekniker er tilsluttet	Kontrollér under valgmuligheden "Others" (Andre) for at bekræfte, om den lokale bruger er tilsluttet. Hvis brugeren er tilsluttet, men du modtager stadig meddelelsen om, at den lokale bruger ikke er tilsluttet scanneren, skal du opdatere skærmen ved at trykke på Ctrl+F5 og bede den lokale bruger om at følge den samme anvisning igen. Vælg derefter udstyret igen, og bed den lokale bruger om også at vælge udstyret igen. Hvis problemet fortsætter, skal du kontakte support for at kontrollere netværket.
Anmodning om adgang bliver ikke sendt	Opdater siden ved at trykke på Ctrl+F5, og bekræft med den lokale bruger via chat, om adgangsanmodningen bliver modtaget. Hvis problemet fortsætter, skal du kontakte support for yderligere assistance.
STREAMINGUDSTYR (e-KVM-COMPUTER)	
Streamingudstyr (e-KVM-COMPUTER) virker ikke	Klik på knappen "Reload streaming" (Genindlæs streaming) på platformen. Sørg for, at den uafbrydelige og stabiliserede strømforsyning (medicinsk facilitet) og/eller streamingudstyret er korrekt tilsluttet og tændt. Sluk for streamingudstyret og alt andet udstyr, og tænd for det igen. Opdater platformen.
Streamingudstyret er langsomt	Klik på knappen "Reload streaming" (Genindlæs streaming) på platformen. Opdater siden med Ctrl+F5, og tilslut systemet til platformen igen. Kontrollér kvaliteten af netværksforbindelsen. For at validere netværksstatus er det muligt at udføre en ping-test på udstyret

	for at kontrollere, om der er tab af pakker (packet loss). Efter internetproblemer vil platformen muligvis ikke fungere efter hensigten. Opdater websiden, og anmod om adgang til den lokale bruger igen.
Tab af videoudgang	Det er tilladt, at elektrostatisk udladning vil forårsage billedtab. Efter genstart af systemet bør kommunikationen og videostreaming automatisk være genetableret.

Afsnit 3.10 – Hardwarerengøringsmetoder

- Inden rengøringsprocessen startes, skal det sikres, at alt udstyr er koblet fra stikkontakten.
- Brug ikke slibende produkter.
- Udstyr eller perifert udstyr må ikke nedsænkes i nogen form for væske.
- Bortskaf rengøringsmaterialer i henhold til reglerne for bortskaffelse af farligt affald.
- Det anbefales ikke at bruge desinfektionsmiddel i sprayform, da dampe kan trænge ind i udstyret og forårsage kortslutning eller korrosion.
- Dette produkt er ikke sterilt

Kapitel 4 Cybersikkerhed og privatliv

Afsnit 4.1 - Sikkerheds- og privatlivsrisici

nCommand Lite-systemet implementerer flere tekniske og organisatoriske foranstaltninger for at beskytte de behandlede oplysninger.

Systemet er certificeret i henhold til ISO/IEC 27001 og ISO/IEC 27701 og følger en tilgang baseret på privatlivsdesign. Understøtter overholdelse af databeskyttelseslove inden for sundhedsvæsenet og cybersikkerhedsregler, der gælder i EU, USA, Storbritannien, Schweiz, Brasilien, UAE, Saudi-Arabien, Australien og New Zealand.

Brugerne skal dog anvende bedste praksis for at forhindre unødvendig eksponering af følsomme data.

- Undgå at dele personlige eller følsomme oplysninger, medmindre det er strengt nødvendigt.
- Sørg for, at kommunikation og systemadgang foregår i sikre miljøer.
- Hvis du har mistanke om skadelig aktivitet, skal du straks underrette det ansvarlige team.

Afsnit 4.2 - Beskyttelse af personoplysninger (overholdelse af GDPR/HIPAA)

nCommand Lite System overholder alle gældende privatlivs- og databeskyttelseslove og -regler i de regioner, hvor det opererer, herunder, men ikke begrænset til, GDPR, HIPAA, LGPD og ISO/IEC 27701-krav. Alle databehandlingsaktiviteter udføres under rollerne "**Processor**" og "**Sub-Processor**" roller som defineret i GDPR, med streng regional dataadskillelse for at sikre overholdelse og forhindre uautoriserede grænseoverskridende dataoverførsler

Hvilke oplysninger indsamles?

- **Brugere:** Navn, e-mailadresse og firma (udelukkende til godkendelse og adgangsstyring)).
- **Patientdata:** Kun overførsler af medicinske undersøgelser via streaming i realtid, uden datalagring

Hvordan bruges og beskyttes oplysninger?)

- Oplysningerne bruges udelukkende til **godkendelse, adgangskontrol og sporing af sessioner.**
- Informationsoverførsel sikres med **AES-256-kryptering til lagring** og **TLS 1.3 til oplysninger i transit..**
- **Adgangen er begrænset** og følger **princippet om minimering af autorisation (RBAC).**
- End-to-end-kryptering sikret til P2P-video og kontrolstreams via WebRTC.
- Autoriserede cloududbydere (f.eks. Microsoft Azure) behandler begrænsede data under strenge kontraktmæssige sikkerhedsforanstaltninger.

Brugere gives følgende rettigheder:

- **Adgang til og rettelse** af personoplysninger.
- **Anmodning om sletning af oplysninger**, hvor det er relevant.

Hvis du har spørgsmål, kan du sende en e-mail til privacy@ionic.health for at kontakte Ionic Healths databeskyttelsesrådgiver. Alle anmodninger behandles inden for 30 dage, hvilket kan forlænges i henhold til GDPR.

Afsnit 4.3 - Adgangsstyring og godkendelse

Brugerne er ansvarlige for at definere **adgangsroller og tilladelser** for deres teams og for at sikre regelmæssig gennemgang og dokumentation af den tildelte adgang).

Bedste praksis og kontroller

- Følg **princippet om minimering af autorisation (RBAC)**, og sørg for, at brugerne kun har den nødvendige adgang).
- **Multifaktorgodkendelse (MFA)** er obligatorisk for administrativ adgang og anbefales for alle brugere).
- Der kræves **stærke adgangskoder** med mindst **8 tegn, herunder store og små bogstaver, tal og symboler**.
- **Del ikke login-oplysninger**.
- Adgangstilladelser overvåges og gennemgås med jævne mellemrum.

Overvågning: Adgang, ændring af tilladelser og vigtige aktiviteter dokumenteres i systemets sikkerhedslogfiler. Logfiler opbevares i mindst 7 år i overensstemmelse med HIPAA, GDPR og andre gældende regler. De understøtter intern revision, retsmedicinsk analyse og lovpligtig rapportering. Logfiler er beskyttet mod manipulation og opbevares i sikre miljøer med adgangskontrol.

Afsnit 4.4 - Systemkontrol Adgangskontrol

Systemkontrollfunktionen er udelukkende tilgængelig via **nCommand Lite Web Application** og kræver gyldige legitimationsoplysninger for login. Adgang er begrænset til autoriserede roller — *Fjerntekniker, Lokal tekniker, Admin, Rolleansvarlig og Systemkontrolbruger*.

Systemkontrolbruger-rollen er designet med begrænsede tilladelser, der kun tillader adgang til diagnostiske funktioner relateret til netværksvalidering og forbindelsesverifikation. Dette sikrer, at netværksdetaljer, whitelisting-information og systemmålinger aldrig bliver eksponeret for uautoriserede personer.

Alle adgangsanmodninger autentificeres via Azure AD B2C, med Multi-Factor Authentication (MFA) og adaptive betingede adgangspolitikker, der administreres af Microsoft Entra ID. Adgangskodekompleksitet følger organisationens sikkerhedspolitik og kræver mindst otte tegn, herunder både store og små bogstaver, tal og symboler. Adgangskoder udløber hver 90. dag, og sessioner logger automatisk ud efter 24 timers inaktivitet, hvilket kan forlænges i op til 90 dage ved kontinuerlig brug.

Afsnit 4.5 - Regional dataadskillelse og logopbevaring

nCommand Lite platformen opretholder streng regional adskillelse af data for at forhindre uautoriserede eller unødvendige grænseoverskridende overførsler. Miljøerne er isoleret pr. region, hvilket sikrer overholdelse af gældende regler.

Alle adgangslogfiler, aktivitetsregistre og sikkerhedshændelser opbevares i minimum syv (7) år i overensstemmelse med gældende databeskyttelses- og sundhedsregler. Logfiler opbevares i sikre, adgangskontrollerede miljøer og er beskyttet mod manipulation. Disse oplysninger understøtter retsmedicinske undersøgelser, overholdelsesrevisioner og regulatorisk rapportering.

Afsnit 4.6 - Datasikkerhed og -integritet

nCommand Lite-systemet sikrer fortrolighed, integritet og tilgængelighed af data gennem sikkerhedspraksisser, der er i overensstemmelse med branchestandarderne.

Brugerne skal sørge for at overholde sikkerhedsprotokoller, regelmæssigt gennemgå adgangspolitikker og rapportere eventuelle uregelmæssigheder. Systemet overvåger løbende aktiviteter, og administratorer skal håndhæve sikkerhedspolitikker for at opretholde et robust forsvar mod potentielle trusler.

Systemet er beskyttet af 24/7 overvågning via et dedikeret Security Operations Center (SOC) med SIEM-funktioner til trusseldetektion og -respons.

Afsnit 4.7 - Håndtering af sikkerhedshændelser

Systemet omfatter en dokumenteret Incident Response Plan, der er i overensstemmelse med ISO 27035 og NIST CSF.

I tilfælde af sikkerhedshændelser, f.eks. uautoriseret adgang eller systemfejl, skal brugerne følge disse trin:

Hvordan identificerer man en hændelse?

- **Uautoriseret adgang** opdaget i aktivitetslogfiler.
- **Mistænkelige forsøg på at logge ind** eller gentagne godkendelsesfejl.
- **Usædvanlig systemadfærd**, f.eks. uventede handlinger eller funktionsfejl.

Hvordan rapporterer man en hændelse?

Registrer omgående hændelsen via de tilgængelige supportkanaler (kapitel 5).

Hvis et brud på persondatasikkerheden bekræftes, vil IONIC, der fungerer som underdatabehandler, underrette GE som databehandler inden for 48 timer og fremlægge al relevant dokumentation, detaljer om konsekvens og afbødende foranstaltninger. GE er til gengæld ansvarlig for at underrette den dataansvarlige (kunden) i overensstemmelse med gældende juridiske og kontraktlige krav.

Kapitel 5 Servicekanaler

Uanset om du har brug for hjælp til et teknisk problem, et uklart trin i processen eller yderligere vejledning, er vores team klar til at hjælpe. Du kan kontakte os via telefon, e-mail eller ITSM-plattformen alt efter, hvad der er mest bekvemt for dig. Vores specialister er uddannet til at give dig personlig assistance, hvilket sikrer, at ethvert problem kan blive løst hurtigt og effektivt.

Telefonnumre

USA	+1 (216) 2421223
Brasilien	+55 12 3600 0181
Europa (Portugal)	+351 (300) 528 410
Australien	+1 (216) 2421223
New Zealand	+1 (216) 2421223

ITSM-plattform

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

E-mail

helpdesk@ionic.health



ADVARSEL!

Enhver alvorlig hændelse relateret til brugen af dette udstyr skal rapporteres til både fabrikanten og sundhedsmyndigheden/den kompetente myndighed, hvor udstyret er installeret.

Rapportering til fabrikanten: Kontakt enten den lokale servicerepræsentant eller rapporter til:
helpdesk@ionic.health

Oplys følgende:

- Systemets versionsnummer, der vises på logonskærmen,
- Dato for hændelse,
- Beskrivelse af hændelse, herunder enhver indvirkning/skade på patient eller bruger,
- Dine kontaktoplysninger (facilitet, adresse, kontaktnavn, titel og telefonnummer).

Kapitel 6 Juridiske og lovgivningsmæssige oplysninger

Fabrikant



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
Brasilien

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

Ansvarlig tekniker

Alexandre Seiji Fukuda Ribas
CREA-SP: 5071085437

ANVISA

82585300004

Importør (USA)



nCommand Lite System

IONIC HEALTH USA INC.

11201 Cedar Avenue, STE 600
Cleveland, OH 44106
USA

+1 (216) 242 1223

EU-repræsentant/importør



nCommand Lite



Identifikationsnummer for bemyndiget
organ: 2803

EUROPE IONIC HEALTH DIGITAL TECHNOLOGIES, LDA

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

+351 (300) 528 410

Schweizisk autoriseret repræsentant (CH-REP) / Importør**CH REP****REF**

nCommand Lite

FREYR LIFE SCIENCES GMBH

Bahnhofplatz
CH-6300 Zug
Schweiz

UK Ansvarlig Person / Importør**REF**

nCommand Lite

FREYR LIFE SCIENCES LTD

9 Greyfriars Road
Reading, Berkshire
RG1 1NU
England, Storbritannien

Australsk sponsor**REF**

nCommand Lite

TAEVAS LIFE SCIENCES PTY LTD

46 Dora St
Blacktown NSW 2148
Australien

New Zealandsk sponsor**REF**

nCommand Lite

TAEVAS LIFE SCIENCES LIMITED

Niveau 3, 1 Margaret Street
Lower Hutt 5010
New Zealand

Grundlæggende UDI-DI: 7898974112NCLITE2L**Anmodning om en papirkopi**

Papirkopier af brugervejledningen til nCommand Lite kan rekvireres uden yderligere omkostninger. Kontakt din lokale repræsentant, og anmod om en papirkopi af brugervejledningen.

Fremstillingsdato

Dato for softwarefrigivelse findes på nCommand Lite loginsiden i formatet MÅNED/ÅR.

Kapitel 7 Revisionshistorik

Revision	Ændr beskrivelse	Dato
0	Opdateret vejledningsversion fra 2.3 v1 til 2.4	25. november 2025
1	Opdatering af etiketter i kapitel 6	4. december 2025
2	Fjernede kravet om en statisk IP-adresse fra den lokale computerkonfiguration i underafsnit 1.3.11 Opdateret EU-repræsentantsymbolet i underafsnit 1.3.12 Fjernet bemærkning fra underpunkt 1.3.14 Opdaterede indholdet i kapitel 2 Opdaterede EU-repræsentantsymbolet i kapitel 6	28. januar 2026
3	Oversættelsen af "Ansvarlig tekniker" i kapitel 6 blev gennemgået.	9. februar 2026

BILAG I – Tjekliste til service

1. *Bekræft elektriske forbindelser og netværksforbindelser:*

Sørg for, at de elektriske forbindelser og netværkspunkterne er etableret korrekt på e-KVM-computeren, scannercomputeren og den lokale computer.

2. *Kontrollér strømstatus:*

Kontrollér, at den uafbrydelige og stabiliserede strømforsyning og e-KVM-computeren er tændt og fungerer korrekt.

3. *Hurtig adgang til nC Lite-plattformen:*

Bekræft tilstedeværelsen af genvejen til nC Lite-plattformen på skrivebordet for hurtig adgang.

4. *Adgang og login på nC Lite-plattformen:*

Åbn nCommand-plattformen, og log på for at sikre fuld adgang og korrekt funktionalitet.

5. *Konfiguration af chatprogram:*

Åbn chat-programmet på nC Lite-plattformen i kun én fane, og undgå at minimere den for problemfri kommunikation.