



ANVÄNDARHANDBOK

nCommand Lite v2.4

Handbokens version: V.3



Innehåll

Kapitel 1	Introduktion.....	4
Avsnitt 1.1 -	Syfte	4
Avsnitt 1.2 -	Ordlista	4
Avsnitt 1.3 -	Beskrivning.....	5
1.3.1.	Avsedd användning	5
1.3.2.	Indikationer för användning	6
1.3.3.	Avsedd patientpopulation	6
1.3.4.	Användningsmiljö	6
1.3.5.	Kontraindikationer.....	6
1.3.6.	Plattformens funktioner.....	6
1.3.7.	Klinisk nytta	7
1.3.8.	Avsedda användare.....	7
1.3.9.	Driftsmiljö.....	7
1.3.10.	Inrättningsmiljö	8
1.3.11.	Minimikrav	9
1.3.12.	Symboler	10
1.3.13.	Livslängd	11
1.3.14.	Uppgradera/uppdatera	11
Kapitel 2	Lista över allmänna varningar och försiktighetsåtgärder	12
Kapitel 3	Användning av plattformen på varje plats	14
Avsnitt 3.1 -	Åtkomst till och användning av nCommand Lite.....	14
Avsnitt 3.2 -	Öppna plattformen för första gången.....	14
3.2.1.	Logga in via nCommand Lite.....	15
3.2.2.	Logga in via extern IdP	16
Avsnitt 3.3 -	Lösenordshantering.....	17
Avsnitt 3.4 -	Åtkomst med lokal teknikerprofil.....	20
Avsnitt 3.5 -	Åtkomst med fjärrteknikerprofil	23
3.5.1.	Åtkomstläge	24
3.5.2.	Streamingfält	26
3.5.3.	Multikamera	28
3.5.4.	Öppna en annan enhet.....	30
3.5.5.	Systemkontroll	32
Avsnitt 3.6 -	Chatt	34

Avsnitt 3.7 - Avsluta din session på plattformen.....	37
Avsnitt 3.8 - Användarutbildning.....	39
Avsnitt 3.9 - Felsökningsriktlinjer.....	40
Avsnitt 3.10 – Rengöringsmetoder för maskinvara	45
Kapitel 4 Cybersäkerhet och sekretess	46
Avsnitt 4.1 - Säkerhets- och integritetsrisker	46
Avsnitt 4.2 - Skydd av personuppgifter (efterlevnad av GDPR / HIPAA).....	46
Avsnitt 4.3 - Åtkomsthantering och autentisering	47
Avsnitt 4.4 - Åtkomst till systemkontroller	47
Avsnitt 4.5 - Regional datasegregering och logglagring	48
Avsnitt 4.6 - Datasäkerhet och integritet.....	48
Avsnitt 4.7 - Åtgärder vid säkerhetsincidenter	48
Kapitel 5 Servicekanaler.....	49
Kapitel 6 Juridisk och regulatorisk information	50
Kapitel 7 Versionshistorik	53
BILAGA I - Checklista för servicestart.....	54

**FÖRSIKTIGHET**

Enligt federal lag får denna enhet endast säljas av läkare eller på läkares ordination samt användas av en medicinsk tekniker som är legitimerad i det land där hen är verksam.
(för USA)

**FÖRSIKTIGHET**

I Brasilien är den här programvaran endast godkänd av Anvisa för användning med magnetisk resonanstomografi (MRI). All annan användning är förbjuden.
(för användning i Brasilien)

**FÖRSIKTIGHET**

Se till att du känner till de specifika kraven i ditt land eller din region före användning. Underlåtenhet att följa förordningarna kan leda till hälsorisker.

**FÖRSIKTIGHET**

Se till att versionen av den här bruksanvisningen matchar den version av plattformen som används. Om du använder en inkompatibel version kan det leda till felaktig användning eller feltolkning av funktioner.

Kapitel 1 Introduktion

Avsnitt 1.1 - Syfte

Syftet med denna handbok är att förse lokala tekniker och fjärrtekniker med en omfattande förståelse av de specifika funktionerna i nCommand Lite-systemet. Detta dokument fungerar som en användarhandbok och ger kortfattad och praktisk information för att vägleda användare genom systemets funktioner och felsökning. Genom att följa denna handbok kommer användare att kunna använda nCommand Lite effektivt, vilket bidrar till att maximera produktiviteten och minska beroendet av teknisk support.

Avsnitt 1.2 - Ordlista

**FÖRSIKTIGHET**

Denna märkning gäller förhållanden eller åtgärder som medför potentiell fara. Du kan orsaka lindrig personskada eller egendomsskada om du ignorerar dessa instruktioner.

**VARNING**

Denna märkning identifierar förhållanden eller åtgärder som resulterar i en specifik fara. Du kommer att orsaka allvarlig personskada eller väsentlig egendomsskada om du ignorerar dessa instruktioner.

Plattformsuttryck	Motsvarande uttryck
Anläggning för bildbehandling	Medicinsk anläggning, Enhet, Mobila Enheter, Vårdinrättning, Hälso- och sjukvårdsenhet
Fjärrinrättning	Fjärransluten arbetsstation, fjärrplacering, fjärrkontor, fjärrlokalisering, kommandocenter
Plattform	nCommand Lite-webbapplikation
System	nCommand Lite med alla delsystem
Enhet	Medicinsk skanner, skanner, utrustning, medicinsk utrustning, bildbehandlingsenhet, bildutrustning
Lokal tekniker	Lokal användare, lokal tekniker, lokal sjukvårdspersonal (LHP), användare on-site

Avsnitt 1.3 - Beskrivning

nCommand Lite är ett SaMD-system (Software as a Medical Device) som är kundinriktat och ger fjärråtkomst via en webbapplikation för visning/granskning av bilder samt möjligheten att ge vägledning på distans i realtid till den patientnära legitimerade teknikern (lokal användare) som använder de medicintekniska produkterna för bildbehandling i samband med utbildning eller procedurutvärdering, i MRT-, DT- och PET/DT-skannrar.

Fjärranvändare är legitimerade tekniker med åtkomst till en medicinteknisk produkt för bildbehandling från en dator var som helst som uppfyller de minsta nödvändiga specifikationerna, med en säker programvaruanslutning som streamar video och ger åtkomst till tangentbord och mus. Detta gör det möjligt för fjärranvändare att hjälpa lokala användare utan att begränsas av avståndet. Denna åtkomst måste beviljas av den lokala användaren som använder systemet, och den kan också återkallas när som helst av den lokala användaren, vilket gör att han/hon hela tiden kan upprätthålla fullständig kontroll över sessionen. Dessutom styrs varje fjärrsession via en säker inloggning som hanteras av den lokala användaren. Anslutningar till en medicinteknisk produkt är begränsade till en fjärrsession i taget för att upprätthålla strikt kontroll över vem som interagerar med systemet på distans. Bilder som fjärrgranskas är inte avsedda för diagnostisk användning.

nCommand Lite-systemet består av en IT-baserad maskinvaru- och programvaruinstallationslösning som stöder flera sessioner, vilket ger fjärrtekniker åtkomst till flera medicintekniska produkter för bildbehandling efter behov. Skannrar som är kompatibla med nCommand Lite-systemet följer ett gemensamt protokoll, vilket möjliggör hantering av skanningsparametrar och fjärrskanning.

1.3.1. Avsedd användning

nCommand Lite-systemet ger fjärråtkomst för visning/granskning av bilder samt möjlighet att vägleda den legitimerade teknikern som använder skannern i realtid. Denna vägledning innefattar utbildning, bedömning av procedur och hantering av skanningsparametrar.

1.3.2. Indikationer för användning

nCommand Lite-systemet möjliggör fjärråtkomst för visning/granskning av bilder samt möjlighet att vägleda den legitimerade teknikern som använder en kompatibel MRT-, DT- eller PET/DT-skanner i realtid. Denna åtkomst måste beviljas av den lokala legitimerade teknikern som använder systemet. Fjärråtkomst är endast tillgänglig för system som stöder fjärranslutningsfunktion. Bilder som fjärrgranskas är inte avsedda för diagnostisk användning.

1.3.3. Avsedd patientpopulation

För alla patienter som ordinerats att genomgå avbildning via en ansluten medicinteknisk produkt för bildbehandling.

1.3.4. Användningsmiljö

Bilddiagnostiska anläggningar som utför undersökningar med magnetisk resonanstomografi (MRT), datortomografi (DT) och positronemissionstomografi – datortomografi (PET/CT) samt ledningscentraler på distans.

1.3.5. Kontraindikationer

Plattformen ska inte användas av användare som inte är legitimerade tekniker och som inte har genomgått utbildning i att använda nCommand Lite.

1.3.6. Plattformens funktioner

- **Fjärrskanning:** visar skärmen på medicinteknisk produkt för bildbehandling i realtid, vilket gör det möjligt för en legitimerad fjärrtekniker att närvara vid en undersökning.
- **Chatt:** tillgängliggör kommunikation mellan fjärrtekniker och lokala legitimerade tekniker via text- och röstmeddelanden. Lokala tekniker och fjärrtekniker kan också ringa och ta emot röst- och videosamtal.
- **Multikamera:** underlättar fjärrobservation av patienter och sjukvårdsinrättningen under proceduren. Fjärrteknikern har åtkomst till kameravyerna via flikarna som är uppdelade mellan samtliga kameraflikar och de enskilda. Denna mekanism replikerar den visuella översikten som hälso- och sjukvårdspersonal skulle ha om de är placerade nära patienten. Detta medför därmed ett förstärkt säkerhetsskikt.
- **Fjärrskanning med flera sessioner** ger fjärrteknikern åtkomst till flera medicinska bildbehandlingsenheter efter behov.
- **Åtkomstläge:** gör det möjligt för fjärrteknikern att välja mellan att visa eller kontrollera enheten. I visningsläge kan fjärrtekniker endast se streamingen. I kontrolläge har han/hon kontroll över musen och tangentbordet.
- **Hantera åtkomst för fjärrtekniker:** gör att en lokal tekniker kan kontrollera fjärrteknikerns åtkomst och åtkomstläge (View (Visning) eller Control (Kontroll)). För att fjärrteknikern ska kunna ansluta måste åtkomst beviljas av den lokala teknikern som använder plattformen, och den kan också återkallas när som helst av den lokala teknikern, vilket möjliggör fullständig och kontinuerlig kontroll över sessionen.
- **Storlek på streaming:** fjärrteknikern kan se den ursprungliga storleken på streamingen och den nuvarande storleken på streamingen i pixlar. Han/hon meddelas också när den nuvarande storleken på streamingen är mindre än den ursprungliga.
- **Mus- och tangentbordsstatus:** fjärrteknikern får feedback om mus och tangentbord till den medicintekniska produkten för bildbehandling fungerar korrekt.
- **Sessionsinformation:** lokal och fjärrtekniker har åtkomst till information om sessionen.

1.3.7. Klinisk nytta

nCommand Lite förbättrar diagnostisk avbildning genom att möjliggöra fjärrstyrning av **MRT-, CT- och PET-CT-system**, vilket säkerställer konsekvent avbildningskvalitet och följsamhet av protokoll. Det gör det möjligt för erfarna tekniker att övervaka och hjälpa till med skanningar i realtid, optimera arbetsflödets effektivitet och minska fel som kan påverka diagnostisk noggrannhet. Systemet underlättar samarbete mellan tekniker, förbättrar undersökningskonsekvens och möjliggör snabbare beslutsfattande i komplexa fall. Genom att göra det möjligt för fjärrpersonal att stödja flera inrättningar ökar **nCommand Lite tillgängligheten, variationen och kvaliteten** på avbildningsundersökningar, vilket säkerställer att fler patienter har tillgång till avancerad diagnostik samtidigt som sjukvårdsresurser optimeras. Dessutom hjälper det till att minska personalbristen genom att minska beroendet av specialister på plats, samtidigt som efterlevnaden av strikta regulatoriska och datasäkerhetsstandarder upprätthålls.

1.3.8. Avsedda användare

- **Lokal tekniker**

Den lokala teknikern är den användare på plats som ansvarar för att hjälpa och vägleda patienter personligen på sjukvårdsinrättningen. Han/hon måste ha nödvändig kunskap för att utföra skanningsprocedurer i en viss avbildningsenhet. Dessutom kontrollerar han/hon fjärrteknikerns åtkomstläge (View (Visning) eller Control (Kontroll)) och fjärråtkomsten måste beviljas av den lokala teknikern via plattformen, och den kan återkallas när som helst.

- **Fjärrtekniker**

Personal som utför åtgärder på distans, med åtkomst till och kontroll över enhetsdatorn. Liksom den lokala teknikern måste fjärrteknikern också ha nödvändig kunskap för att utföra skanningsprocedurer i en viss avbildningsenhet.

- **Support/IT-användare**

Personal som är ansvarig för att installera plattformen (ingår inte i denna användarhandbok).

1.3.9. Driftsmiljö

Följande specifikationer avser miljökraven för e-KVM-datorn.

- **Maximal altitud (utan trycksättning)**

- Drift: Från 0 m (0 fot) till 3 048 m (10 000 fot)
- Lagringsutrymme: Från 0 m (0 fot) till 12 192 m (40 000 fot)

- **Temperatur**

- Drift: Från 10 °C (50 °F) till 35 °C (95 °F)
- Lagringsutrymme: Från -10 °C (14 °F) till 50 °C (122 °F)

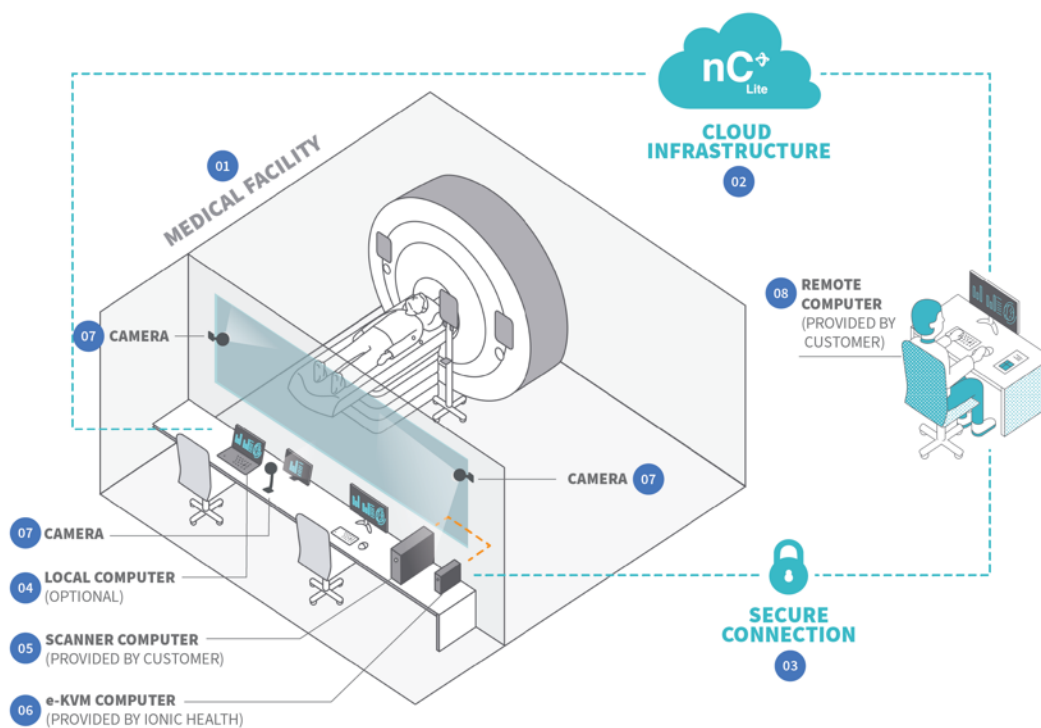
- **Relativ luftfuktighet**

- Drift: 20 %–80 % (icke-kondenserande)
- Lagringsutrymme: 10 %–90 % (icke-kondenserande)

1.3.10. Inrättningsmiljö

nCommand Lite-plattformen har två olika typer av miljöplatser:

- **Anläggning för medicinsk bilddiagnostik** Anläggningar som utför undersökningar med magnetisk resonanstomografi (MRT), datortomografi (DT) eller positronemissionstomografi – datortomografi (PET/CT).
- **Fjärranläggning:** En plats där fjärrtekniker kan få åtkomst till och fjärrhantera enheter (MRI-, CT- eller PET/CT-skannrar). Denna arbetsstation kan användas i olika miljöer som kontor, kommandocentraler, avlägsna platser eller till och med sekundära platser inom vårdinrättningen. Fjärrarbetsstationen kan placeras i vilket utrymme som helst som ger användaren lämpliga förutsättningar för koncentration och minimal anslutning samt krav på datorkonfiguration.



Figur 01: Översikt över produkten och dess anslutningar via en säker anslutning (t.ex. VPN).

01 – Sjukvårdsinrättning, 02 – Molninfrastruktur, 03 – Säker anslutning, 04 – Lokal dator (valfritt),
05 – Skannerdator (tillhandahålls av kund), 06 – e-KVM (tillhandahålls av IONIC Health),
07 – Kamera, 08 - Fjärrdator (tillhandahålls av kund)

**WARNING!****Kompatibilitet med fjärrskanning**

IONIC Health (IH) validerar fjärrskanningsfunktioner på de listade kompatibla enheterna. IH genomför en fullständig bedömning av IH:s krav på fjärrskanning och testar systemet i målmiljön under installationen. Detta säkerställer kompatibilitet och korrekt prestanda vid den tidpunkten för fjärrskanning. Den här verifieringen innebär inte att alla OEM-enhetskrav (Original Equipment Manufacturer) uppfylls i den här konfigurationen. Eventuella avvikelser från OEM-kraven är slutanvändarens ansvar.

Ändringar av systemet eller miljön efter installationen måste rapporteras till IH för att verifiera fortsatt kompatibilitet. IH kan inte garantera prestanda eller ta ansvar för konfigurationer som skiljer sig från de som validerades under installationen.

1.3.11. Minimikrav**• Lokal dator**

Den här datorn används av **lokal tekniker** för att auktorisera och stödja fjärråtkomst till enheten via nCommand Lite®. Den används också för direkt kommunikation med **fjärtekniker** via chattfunktionen på plattformen.

De lägsta tekniska specifikationerna som krävs är:

- Processor: Minst AMD® A4-9120C eller motsvarande
- Minne: 4 GB eller mer
- Lagringsutrymme: 128 GB SSD eller högre
- Kringutrustning: mikrofon och högtalare eller headset och webbkamera
- Bildskärm: 14" FHD (1920 x 1080) eller högre
- Operativsystem: Chrome OS, Windows OS eller MAC OS
- Installationsplats: den här datorn måste vara i närheten av skannerdatorn
- IT-rutin: Skapa nCommand Lite-genväg på varje användares skrivbord
- Kompatibla webbläsare: Google Chrome eller Microsoft Edge.

• Fjärrarbetsstation

Den här stationen används av **fjärtekniker** för att komma åt och styra enheten via nCommand Lite®. Fjärrarbetsstationen måste upprätta en säker anslutning till e-KVM-datorn (tillhandahålls av IONIC HEALTH®).

Kunden ansvarar för att tillhandahålla fjärrdatorn och kan välja ett av två scenarier: det första är 24x7-drift och det andra är drift på kontorstid.

Nedan anges specifikationerna som krävs för varje scenario när ni väljer datormodeller:

Scenario 1 (24x7-drift) – måste uppfylla följande specifikationer:

- Intel Xeon W-2223 (4 kärnor, 8 trådar, 8,25 MB cacheminne, 3,90 GHz Turbo) eller högre.
- RAM: 16 GB eller högre.
- Grafik: Minst NVIDIA RTX A2000 6 GB eller motsvarande.

- Lagringsutrymme: 128 GB SSD eller högre.
- Operativsystem: Windows 11 Pro 64B eller senare.
- Minimikrav för bildskärm: Storlek 27", bildförhållande 16:9, upplösning 4k.
- Headset: BLACKWIRE 3200 eller liknande.
- Kompatibla webbläsare: Google Chrome eller Microsoft Edge.

Scenario 2 (drift under kontorstid) – måste uppfylla följande specifikationer:

- Intel® Core™ i7-12700k vPro® eller högre.
- RAM: 16 GB eller högre.
- Grafik: Minst NVIDIA T400 GB eller motsvarande.
- Lagringsutrymme: 128 GB SSD eller högre.
- Operativsystem: Windows 11 Pro 64B eller senare.
- Minimikrav för bildskärm: Storlek 27", bildförhållande 16:9, upplösning 4k.
- Headset: BLACKWIRE 3200 eller liknande.
- Kompatibla webbläsare: Google Chrome eller Microsoft Edge.



WARNING!

Om du inte uppfyller lämpliga inställningar och minimikrav kan det leda till försämrad eller misslyckad kommunikation mellan användare.

• Nätverkskonfigurationer (minimikrav)

För att upprätta sessionen mellan fjärranvändaren och e-KVM-datorn måste nätverkskommunikationen mellan de två enheterna säkerställas. nCommand Lite-systemet använder P2P (peer-to-peer) för att upprätta en anslutning mellan lokala användare, fjärranvändare och e-KVM-datorn. Det finns tre kompatibla scenarier:

- **Scenario 1** – företagsnätverk som använder något av följande protokoll: LAN, LAN-till-LAN, MPLS eller VPN;
- **Scenario 2** – företagsnätverk som använder betrott WAN (externt nätverk) och inte använder något av följande protokoll: LAN, LAN-till-LAN, MPLS eller VPN;
- **Scenario 3** – offentligt nätverk på fjärrdatorsidan (fjärranvändare).

Konfigurationerna för varje scenario beskrivs i den tekniska dokumentationen.

1.3.12. Symboler

Symbol	Beskrivning	Referens
	Tillverkare	ISO 15223-1, ISO 7000-3082
	Tillverkningsdatum	ISO 15223-1, ISO 7000-2497
	Symbolen anger att denna produkt är en medicinteknisk produkt	ISO 15223-1
	Unik produktidentifiering	ISO 15223-1

	Modellreferens	ISO 15223–1, ISO 7000–2493
	Importör	ISO 15223–1, ISO 7000–3725
	Se användarhandboken	ISO 15223–1, ISO 7000–1641
	Distributör	ISO 15223–1, ISO 7000–3724
	Försiktighet	ISO 15223–1, ISO 7000–0434A
	Varning	ISO 7010-W001
	Serienummer (eller programversion)	ISO 15223–1, ISO 7000–2498
	Auktoriserad representant i Europeiska gemenskapen	ISO 15223-1
	Auktoriserad representant i Schweiz (CH-REP)	ISO 15223-1
	CE – Europeisk överensstämmelsemärkning; 2803 – Utnämning av anmält organ	EU-förordning 2017/745

1.3.13. Livslängd

Produktens förväntade livslängd är 5 år, med hänsyn till livslängden för de komponenter som produkten består av. Denna omfattande utvärdering säkerställer att varje kritisk komponents livslängd överensstämmer med den totala livslängden, vilket garanterar konsekvent prestanda och tillförlitlighet under produktens avsedda varaktighet.

1.3.14. Uppgradera/uppdatera

IONIC Health uppgraderar nCommand Lite-systemet som en del av planerat underhåll eller via uppgraderingar. Dessa uppdateringar är utformade för att säkerställa fortsatt prestanda och tillförlitlighet utan att störa den nuvarande versionen som är installerad hos kunderna. Beroende på uppdateringens karaktär kan produkten uppgraderas på distans eller genom ett besök på plats av en fältingenjör.

Kapitel 2 Lista över allmänna varningar och försiktighetsåtgärder



VARNING!

Läs alla varningar nedan innan du använder nCommand Lite-systemet.



FÖRSIKTIGHET

nCommand Lite-systemet kan inte repareras eller underhållas när det används för att styra en MRI-, CT- eller PET-CT-utrustning i närvaro av en patient.

- Var speciellt uppmärksam på alla systemvarningar, då de är avgörande för säker drift.
- Prioritera säkerhet och uppmärksamhet under all drift.
- Enligt federal lag får denna enhet endast säljas av läkare eller på läkares ordination. Används av medicinska tekniker som är legitimerade i det land där hen är verksamma.
- nCommand Lite-systemet får endast användas av tekniker som har utbildats i användningen av plattformen.
- Använd endast detta system med kompatibla webbläsare. Webbläsare som stöds är Google Chrome och Microsoft Edge.
- Om en oförutsedd händelse skulle uppstå måste en utbildad, legitimerad tekniker vara kvar på bilddiagnostikavdelningen för att utföra MRT-, CT- eller PET/CT-proceduren utan nCommand Lite.
- Tillgång till flera enheter samtidigt kräver intensivt fokus och kommunikation med lokala team.
- Undvik att koppla upp till enheter med identiska layouter eller undersökningar av samma anatomiska region vid samma tidpunkt.
- Du kan visa flera skärmar, men kontroll är begränsad till en enhet åt gången.
- Starta alltid en chatt när du är ansluten till en enhet för en tydlig kommunikation.
- Samtalsvarningar visas på den associerade enhetens skärm – endast ett samtal kan vara aktivt åt gången.
- Testa videokommunikationen när du öppnar applikationen (innan en arbetssession påbörjas) för att kontrollera om det finns något fel i videoutgångsanslutningen för MRT-, CT- eller PET/CT-enheterna eller någon enhet som är relaterad till videostreaming.
- Enheten ska inte anslutas till uttaget och/eller den avbrottsfria och stabiliserade strömförsörjningen genom förlängningssladdar eller "flerkontaktdosor".
- Om videofel uppstår, kontrollera videoanslutningen mellan enhetssystemet och e-KVM-datorn.
- Om applikationen har en långsam fjärråtkomst ska du uppdatera sidan med kommandona Ctrl+F5 i fjärrteknikerdatorns webbläsare. Kontakta teknisk support om problemet kvarstår.
- När webbläsarsidan uppdateras avbryts anslutningen till enheten, vilket kräver att godkännandeprocessen måste utföras igen.
- Logga inte in via en annan webbläsare när du redan är inloggad.
- Kundens bilddiagnostikavdelning måste ha en redundant internetanslutning från en annan leverantör än den huvudsakliga för att kunna byta omedelbart i händelse av förlust av system-/plattformkommunikation.
- I händelse av kommunikationsförlust eller långsam mus ska du "synka om musen" på den sida som används i webbläsaren.

- Se till att datorerna som används för kontroll av nCommand Lite-systemet uppfyller minimikraven, både på bilddiagnostikavdelningen och i ledningscentralen. Annars kan applikationsprestanda förloras.
- QoS (Quality of Service) ska tillämpas på huvudlänken och den redundanta länken för överföring av plattformen, och länkens prestanda ska övervakas.
- Kontrollera volymnivåerna på ljud och mikrofon samt behörigheten för ljud och mikrofon i webbläsaren före användning.
- Om de är långsamma eller inte synkade ska du aktivera knappen "mouse resync" (synka om musen). Kontrollera att e-KVM-datorn är ansluten och påslagen.
- Se till att tangentbordets layout på fjärrinrättningen är identisk med tangentbordets layout på bilddiagnostikinrättningen.
- Om det är nödvändigt att ändra platsen där plattformen används måste kunden ringa teknisk support för att göra en ny installation. Installera inte om utan att kontakta teknisk support.
- Innan fjärråtkomstprocessen för MRT-, CT- eller PET/CT-enheten påbörjas är det viktigt att teknikerns team kontrollerar alla objekt som krävs för att plattformen ska fungera korrekt, så att undersökningen inte störs. Dessa objekt anges i dokumentet "Kontrollista för servicestart".
- Bildbehandlingsanläggningens brandväggskonfiguration måste kontrolleras varje månad med IT-teamet för att verifiera att det inte finns några problem med brandväggsversionen som kan äventyra användningen av nCommand Lite.
- Alla avvikelser som observeras vid användning av applikationen måste omedelbart meddelas till supportteamet innan du startar åtkomsten. Avbryt om den redan har startats.
- Endast legitimerade tekniker med utbildning i användning av nCommand Lite får använda applikationen.
- Fjärråtkomst via plattformen ersätter eller konkurrerar inte med någon annan procedur för MRT-, CT- eller PET/CT-drift som fastställts av den medicintekniska produktens tillverkare och vårdinrättningens protokoll och rutiner.
- Undvik att böja eller tänja ut maskinvarukablarna.
- Om det uppstår problem med röst- eller chattkommunikationen ska du använda funktionen för telefonsamtal för att upprätta kommunikation mellan den lokala teknikern på bildbehandlingsanläggningen och fjärrteknikern på ledningscentralen. Följ instruktionerna som beskrivs i avsnittet "Riktlinjer vid fel" och kontakta teknisk support vid behov för att utföra reparationen.
- Om en dator eller annan utrustning behöver bytas ut, som direkt påverkar installationen av nCommand Lite, ska du aktivera teknisk support för att garantera att systemets drift upprätthålls.
- Endast en person åt gången kan få fjärråtkomst till MRT-, DT- eller PET/CT-enheten.
- Rör inte några fysiska videokablar medan enhetens dator och nCommand Lite-systemet är påslagna.
- Vid åtkomst till ytterligare en enhet, kommer en ny flik att öppnas. Dra denna flik till en andra bildskärm, då systemet är utformat för att användas med en separat skärm för varje enhet.
- Alla allvarliga tillbud relaterade till användningen av denna enhet ska rapporteras till både tillverkaren och den hälso- och sjukvårdsmyndighet/behörig myndighet där enheten är installerad (se mer information i kapitlet *Servicekanaler*).

Kapitel 3 Användning av plattformen på varje plats

Avsnitt 3.1 - Åtkomst till och användning av nCommand Lite

**WARNING!**

Kontakta teknisk support för hjälp vid eventuella problem.

**WARNING!**

Kontrollera tangentbordets layout och se till att det är identiskt på båda platserna (sjukvårdsinrättning och fjärrinrättning). Olika tangentbordslayouter kan försvåra användarupplevelsen.

Det här kapitlet innehåller allt du behöver veta för att komma åt och börja använda nCommand Lite-plattformen. Du hittar enkla, steg-för-steg-instruktioner för att logga in, navigera i gränssnittet och förstå huvudfunktionerna. Oavsett om du arbetar på plats eller på distans hjälper den här guiden dig att komma igång snabbt och säkert.

Ändra språk – Systemet är inställt på engelska som standard, men du kan enkelt ändra språket enligt dina önskemål. På inloggningsskärmen klickar du längst upp till höger där "English (en-US)" (engelska) visas. Då öppnas en rullgardinslista med tillgängliga språk som du kan välja bland.

När du har loggat in kan du också ändra språk genom att klicka på det aktuella valda språket till höger i det övre fältet. Då öppnas en rullgardinslista med tillgängliga språk som du kan välja bland.

Observera att om du ändrar språk när du är ansluten till en enhet kommer den aktuella anslutningen att avslutas automatiskt, och du måste ansluta igen.

När du kopplar upp dig till plattformen kan du välja önskat språk på inloggningsskärmen. Vissa meddelanden som visas under inloggningsprocessen kan dock visas på det språk som är inställt i din webbläsare, oavsett vilket språk som valts på plattformen. För en konsekvent upplevelse rekommenderar vi att du justerar webbläsarens språkställningar med det språk du föredrar på plattformen.

Avsnitt 3.2 - Öppna plattformen för första gången

Inloggningsprocessen på plattformen kan göras på två sätt: via nCommand Lite eller via en extern identitetsleverantör (External IdP). Användaren kan logga in med en av de förkonfigurerade metoderna. Om den konfigurerade metoden är External Identity Provider (External IdP) kommer nCommand Lite-metoden inte att fungera och vice versa. För att logga in via Extern IdP, gå direkt till **sub-item 3.2.2**.

3.2.1. Logga in via nCommand Lite

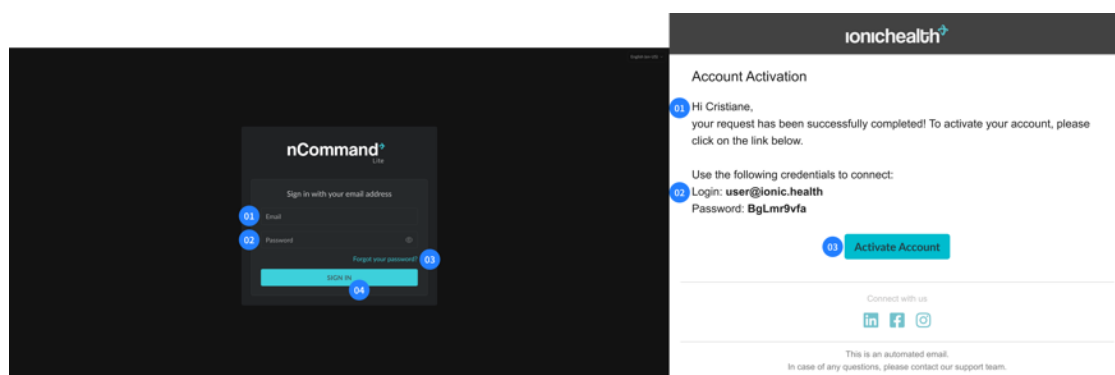
Observera: Det här avsnittet gäller inte för användare som loggar in via en extern identitetsleverantör (extern IdP).

Slå på datorn och dubbelklicka på genvägsikonen nCommand Lite, som vanligtvis finns på skrivbordet. Du kan också koppla upp dig till webbadressen direkt i webbläsaren.

Den första åtkomsten är ett avgörande steg för att börja använda plattformen på ett säkert och effektivt sätt. Här är vad du behöver veta:

1 – E-post med välkomstmeddelande: Du kommer att få ett e-postmeddelande med dina inloggningsuppgifter, inklusive tillhörande personliga e-postadress, ett tillfälligt lösenord och en direktlänk till kundplattformen. Detta e-postmeddelande är avgörande för att börja använda nCommand Lite.

2 – Skapa lösenord: När du öppnat länken måste du ange din tillhörande e-postadress och lösenordet som du fick i välkomstmeddelandet. Genom att klicka på "Sign in" (logga in) kommer du till en sida där du kan skapa ett nytt lösenord. Du måste ange det gamla, det nya lösenordet och bekräfta det nya lösenordet. Det måste vara starkt och säkert, inklusive minst 3 av följande: en liten bokstav, en stor bokstav, en siffra och en symbol och vara minst 8 tecken långt. När du klickar på "Continue" (fortsätt) omdirigeras du till en sida för att bekräfta din e-postadress igen. När du klickar på "Continue" (fortsätt) omdirigeras du nu till startskärmen, som är anpassad efter din specifika användarprofil.



Figur 02: Första åtkomst

Vänster - Inloggningssida: 01 – Email Address (e-postadress), 02 – Password (lösenord), 03 – Forgot your password? (har du glömt ditt lösenord?), 04 – Knappen Sign In (logga in)

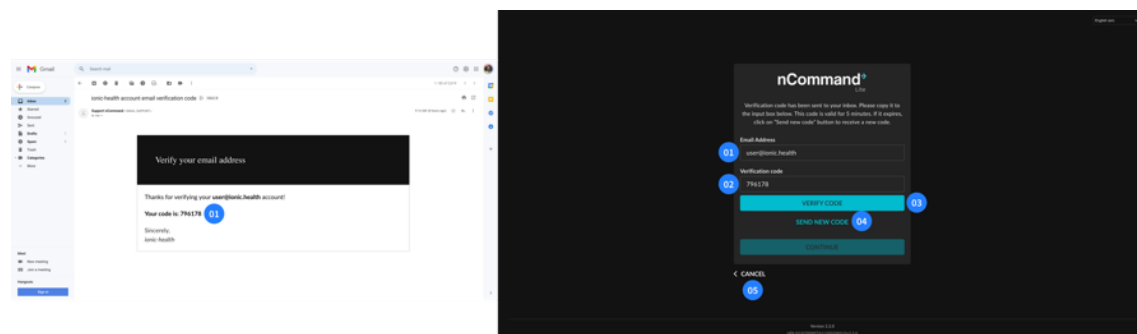
Höger – E-post med välkomstmeddelande: 01 – E-postmeddelande med kontoaktivering, 02 – Inloggningsuppgifter, 03 – Knappen Activate Account (aktivera konto)

Denna inledande procedur är utformad för att säkerställa maximal säkerhet för ditt konto från början. Vid framtida åtkomstillfällen är processen enklare men lika säker med en kod för tvåfaktorsautentisering som skickas till din kopplade e-postadress vid varje inloggning för att säkerställa den löpande säkerheten för ditt konto.

När du har loggat in på nCommand Lite leder systemet dig automatiskt till startskärmen, som är anpassad efter din specifika användarprofil. Oavsett om du är en lokal tekniker eller en fjärrtekniker är gränssnittet utformat för att uppfylla de behov och den åtkomst som är relevant

för din roll. Denna intuitiva design säkerställer att du har alla verktyg och all information som behövs för en effektiv och ändamålsenlig användarupplevelse från det ögonblick du loggar in.

Observera: När inloggningsmetoden är konfigurerad som nCommand Lite måste inloggningen alltid utföras via detta alternativ. Även om en extern IdP-knapp visas på inloggningsskärmen kommer den inte att fungera för dessa användare. Varje användarkonto är registrerat på plattformen med en specifik autentiseringsmetod – antingen nCommand Lite-uppgifter eller en extern IdP-tjänst. Om en användare försöker logga in med en annan metod än den som är tilldelad deras konto, kommer systemet att visa ett felmeddelande som indikerar att kontot inte är auktoriserat för den autentiseringstypen.



Figur 03: Tvåfaktorsautentisering (2-FA)

Vänster – E-post: 01 – 2-FA Kod

Höger – Sida för tvåfaktorsautentisering: 01 – E-mail Address (e-postadress), 02 – Verification Code (verifieringskod),

03 – Bekräftelseknapp för verifieringskod, 04 – Send New Code (Skicka ny kod), 05 – Cancel (Avbryt)

3.2.2. Logga in via extern IdP

I vissa fall kan användare logga in på plattformen via en extern identitetsleverantör (IdP), vilket gör att de kan använda organisationens befintliga autentiseringstjänst, en mekanism som även kallas enkel inloggning (SSO). Med denna metod kommer den förregistrerade användaren inte att få ett välkomstmeddelande. Den lokala IT-tjänsten måste kontrollera kompatibiliteten, konfigurera metoden och informera användaren om vilken e-post (extern IdP) som ska användas.

När det här alternativet är tillgängligt måste användaren alltid logga in med den externa IdP:n (t.ex. Amazon Cognito, Microsoft Entra ID, Microsoft AD B2C). Inloggningsmetoden via nCommand Lite kommer inte att vara tillgänglig för externa IdP-användare.

För att logga in med den externa IdP:n, klicka på knappen med IdP:ns namn och följ instruktionerna från den externa autentiseraren. Om din institution har mer än en extern IdP integrerad, se till att bekräfta vilken leverantör du är registrerad hos. Andra leverantörer kommer inte att fungera. Om du har några frågor eller stöter på problem, kontakta din lokala IT-tjänst.

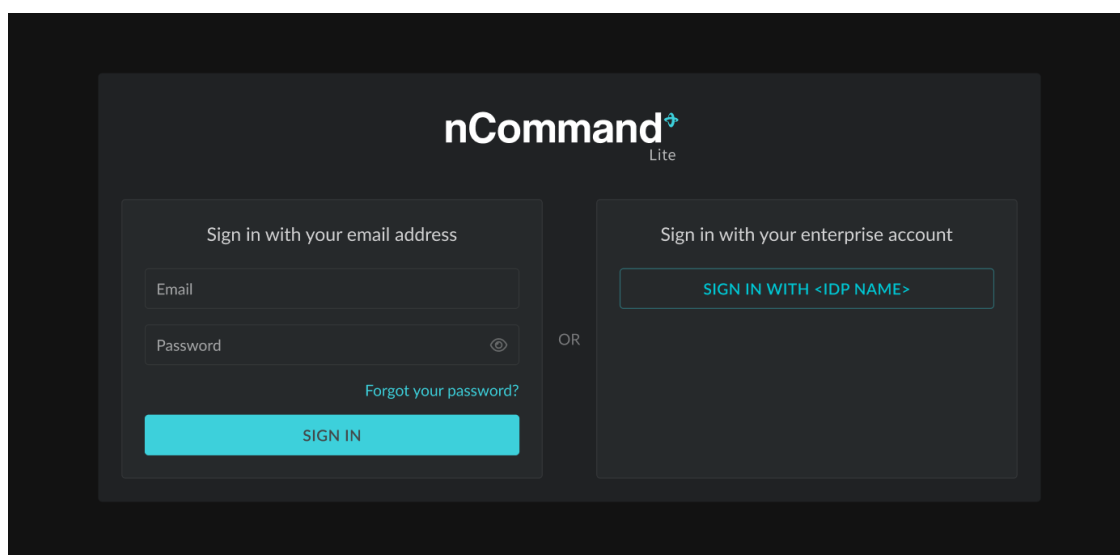
I scenarier där användare delar samma maskin och använder Single Sign-On (SSO), rekommenderas det att varje användare väljer alternativet "Do not stay signed in" under extern IdP-inloggning (om tillgängligt) eller loggar ut från den externa leverantören efter att ha loggat ut från nCommand Lite.

För det här inloggningsalternativet hanteras hela inloggnings- och utloggningsprocessen – inklusive policyer för att skapa och förfalla lösenord, multifaktorautentisering (MFA) och kontolåsningar – helt och hållet av klientens IT-team som konfigurerade den externa IdP:n.

Vid inloggning via Extern IdP måste funktionerna "Glömt lösenord" och "Ändra lösenord" utföras enligt den Externa IdP:ns process.

Observera: Alternativet *Forgot Password* (glömt lösenord) kommer fortfarande att visas på inloggningsskärmen, men det kommer inte att vara tillgängligt för dessa användare. Den kan leda till nästa steg i processen, men kommer inte att slutföra den. Om du behöver återställa ditt lösenord följer du instruktionerna från din externa IdP.

Viktigt: Även när du använder en extern IdP måste användaren vara förregistrerad på nCommand Lite-plattformen för att få åtkomst.



Figur 04: Inloggningsskärm via extern IdP (exempel)

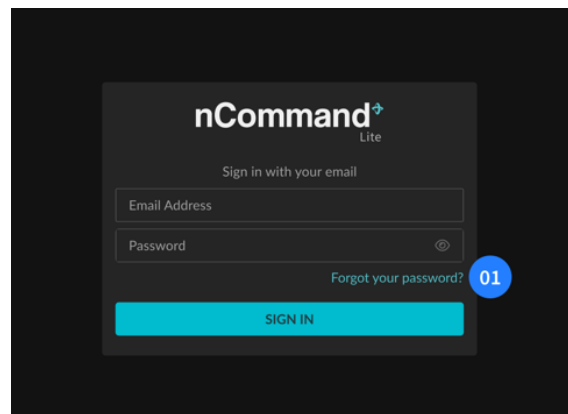
Avsnitt 3.3 - Lösenordshantering

Efter att ha öppnat plattformen för första gången kan användare byta lösenord eller, om det glömdes, ställa in ett nytt lösenord.

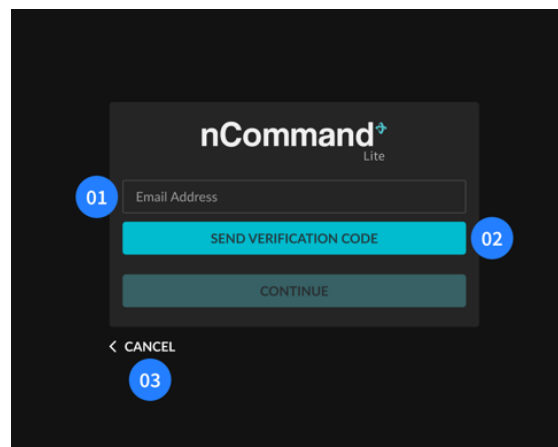
Observera: När du loggar in via extern IdP måste funktionerna **Glömt lösenord** och **Ändra lösenord** utföras enligt den externa IdP:ns process.

- **Återställa lösenord:** Gör det möjligt för användare att återställa åtkomst till kontot om han/hon glömmet sitt lösenord. Klicka bara på länken "Forgot your password?" (har du glömt ditt lösenord?) på inloggningssidan, ange tillhörande e-postadress och skicka informationen. Systemet skickar sedan ett e-postmeddelande med en verifieringskod. När du fyller i koden och klickar på "Verify code" (verifiera kod) blir användaren ombedd att bekräfta den tillhörande e-postadressen. Genom att klicka på "Continue" (fortsätt) skickas användaren till en sida där

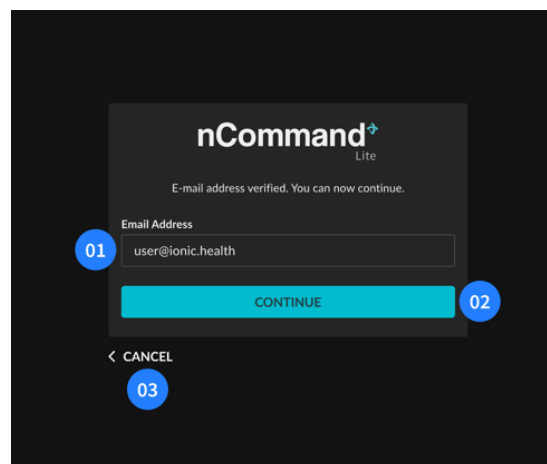
denne kan ange ett nytt lösenord och bekräfta det nya lösenordet. Om det nya lösenordet uppfyller systemkraven kan användaren registrera det och därefter logga in med de uppdaterade uppgifterna.



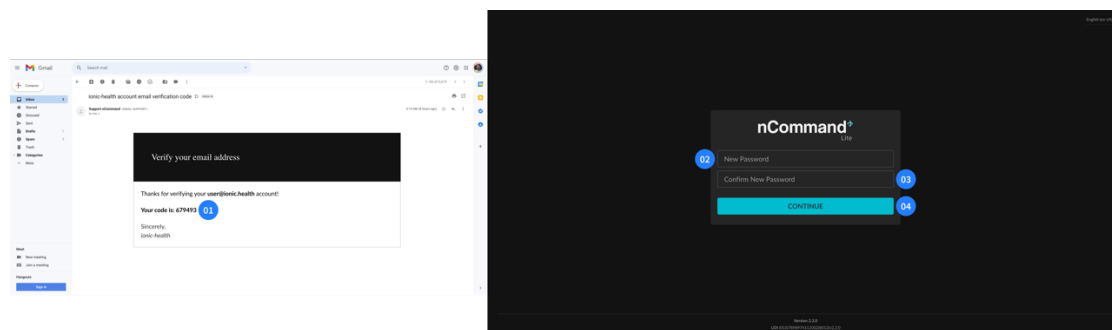
Figur 05: Länk till sidan för återställning av lösenordet
01 – Forgot your password? (Glömt ditt lösenord?)



Figur 06: Sidan för lösenordsåterställning
01 – E-mail Address (e-postadress), 02 – Send Verification Code (skicka verifieringskod), 03 – Cancel (avbryt)

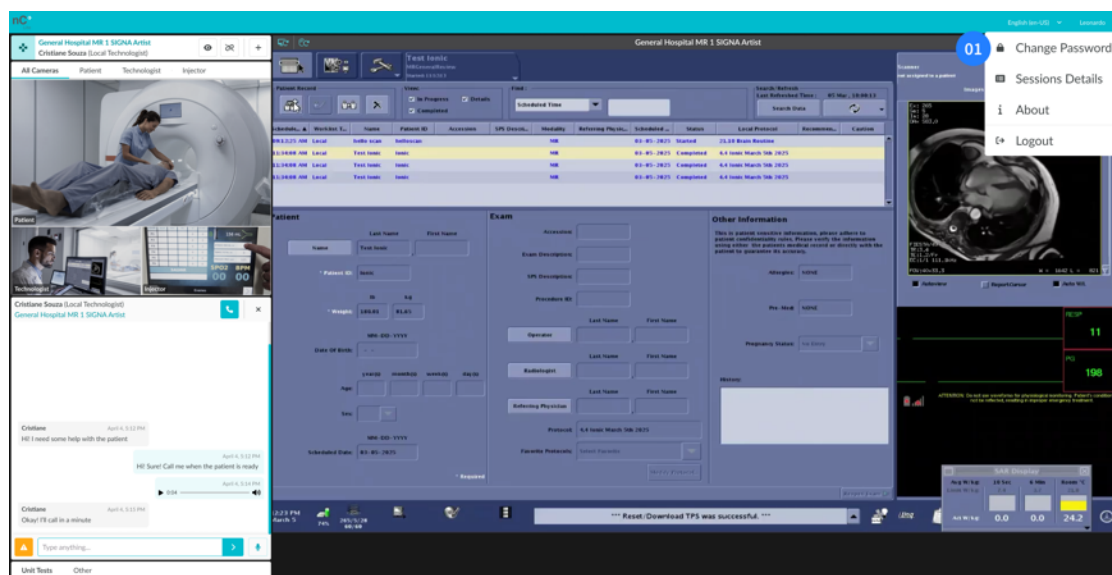


Figur 07: E-postbekräftelse
01 – E-mail Address (e-postadress); 02 – Knappen Continue (fortsätt); 03 – Cancel (avbryt)

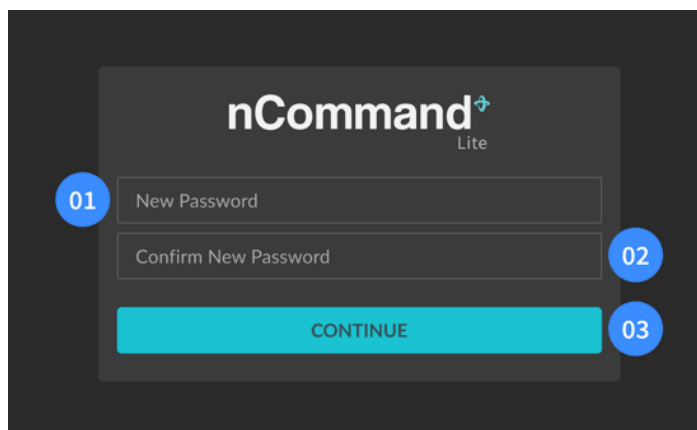


**Figur 08: E-post med kod för att registrera nytt lösenord (vänster) - 01 – 2-FA-kod
Sida för att byta lösenord (höger) – 02 – New Password (nytt lösenord), 03 – Confirm New Password (bekräfta nytt lösenord), 04 – Knappen Continue (fortsätt)**

- **Ändra lösenord:** Gör det möjligt för användare att uppdatera sitt lösenord genom att följa specifika kriterier, inklusive minst 3 objekt med följande: en liten bokstav, en stor bokstav, en siffra och en symbol och vara minst 8 tecken långt. Systemet kontrollerar om det nya lösenordet uppfyller dessa kriterier och uppmanar användaren i ett meddelande om det inte gör det. Dessutom måste användaren bekräfta det nya lösenordet för att förhindra inmatningsfel. För att byta lösenordet efter inloggningsprocessen måste användaren klicka på ikonen längst upp till höger och välja menyn "Change Password" (Ändra lösenord). Han/hon kommer att kopplas bort från plattformen och dirigeras till en sida för att bekräfta den tillhörande e-postadressen. Systemet skickar sedan ett e-postmeddelande med en verifieringskod. När du fyller i koden och klickar på "Verify code" (verifiera koden) omdirigeras användaren till en skärm där de kan ange ett nytt lösenord.



**Figur 09: Menyalternativet Change Password (byt lösenord)
01 – Change Password (byt lösenord)**



Figur 10: Sidan Change Password (byt lösenord)

01 – New Password (nytt lösenord), **02** – Confirm New Password (bekräfta nytt lösenord), **03** – Knappen Continue (fortsätt)

Avsnitt 3.4 - Åtkomst med lokal teknikerprofil



WARNING!

Fjärrteknikern ska kontaktas per telefon innan du använder plattformen.



WARNING!

För att undvika överhettning får inga föremål placeras framför e-KVM-datorns luftkylare, och för att förhindra skador får inga föremål placeras ovanpå den.



WARNING!

Under fjärrsessioner är den lokala teknikern ansvarig för att hantera och genomdriva lokala säkerhetsregler för varje typ av undersökning och dess specifika krav. Var alltid närvarande i kontrollrummet och/eller undersökningsrummet för att säkerställa säkerheten för både patienten och den medicinska personalen som deltar.



WARNING!

Bordsflyttningar under sessionen får endast utföras av den lokala teknikern på begäran av systemet. Innan den lokala teknikern lämnar operationssalen ska han/hon alltid återkalla fjärrteknikerns åtkomst.



WARNING!

Endast den lokala teknikern får flytta bordet för att placera patienten inuti enheten och för att frigöra patienten på ett säkert sätt. Innan den lokala teknikern lämnar salen ska han/hon alltid återkalla fjärranvändarens åtkomst.

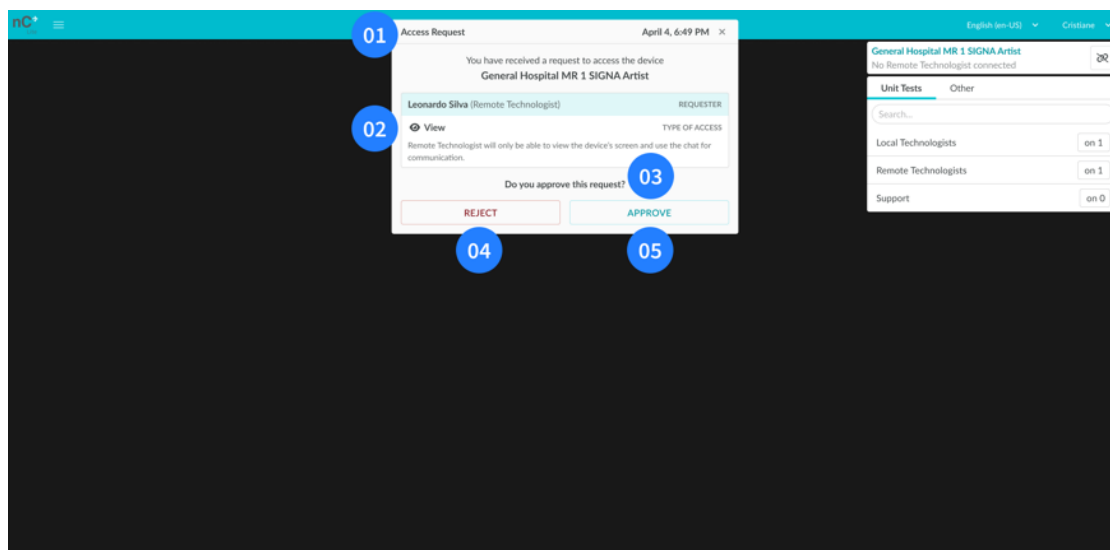
När du har loggat in på plattformen fortsätter du med att välja önskad enhet i rutan Device Selection (val av enhet). Du kommer att vara ansvarig för denna enhet, så att du kan gå igenom fjärrteknikerns begäran om att få åtkomst till enheten. När en fjärrtekniker vill få åtkomst till enheten visas ett popup-fönster där du kan gå igenom all information som visas innan du ger

eller nekar åtkomst. Var uppmärksam på en inkommande begäran från en fjärrtekniker. Det är ytterst viktigt att noggrant kontrollera varje detalj. Om du inte känner igen den tillhandahållna informationen ska du inte ge åtkomst.

Fjärrteknikern kan få åtkomst till enheten med något av två åtkomstlägen: **Kontroll** eller **Visning**:

- **Kontrollläge** - låter fjärrteknikern styra musen och tangentbordet, samt se enhetens streaming. Den lokala teknikern förlorar dock inte kontrollen över den lokala musen och tangentbordet och kan när som helst ta kontrollen.
- **Visningsläge** - låter fjärrteknikern endast visa enhetens skärm och använda chatten för kommunikation

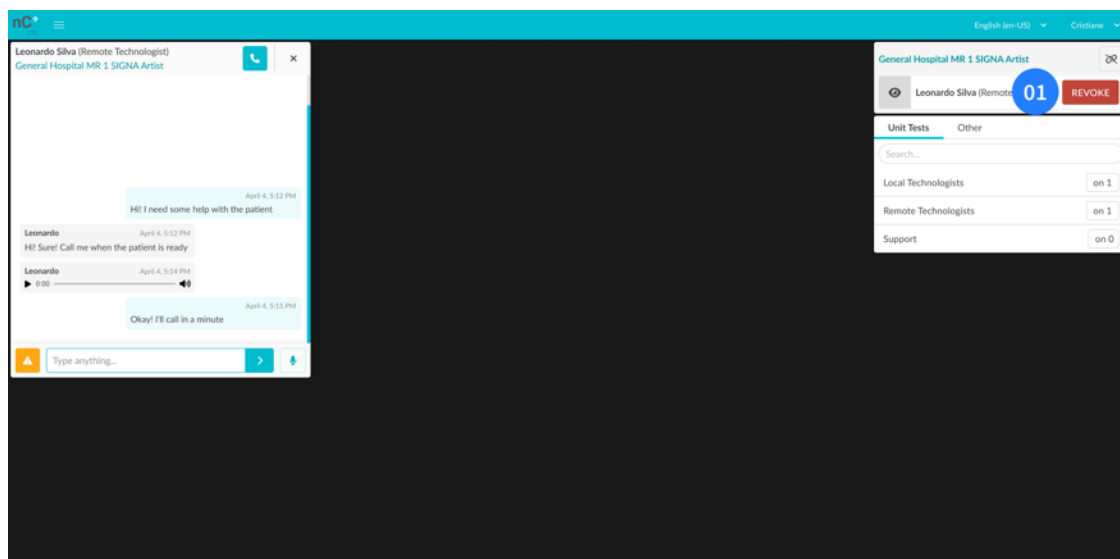
Efter att ha valt enheten får användaren tillgång till chattfunktionen som möjliggör kommunikation via text, ljudmeddelanden, röst- och videosamtal med de andra användarna.



Figur 11: Huvudskärm med avisering om åtkomstförfrågan för lokal tekniker

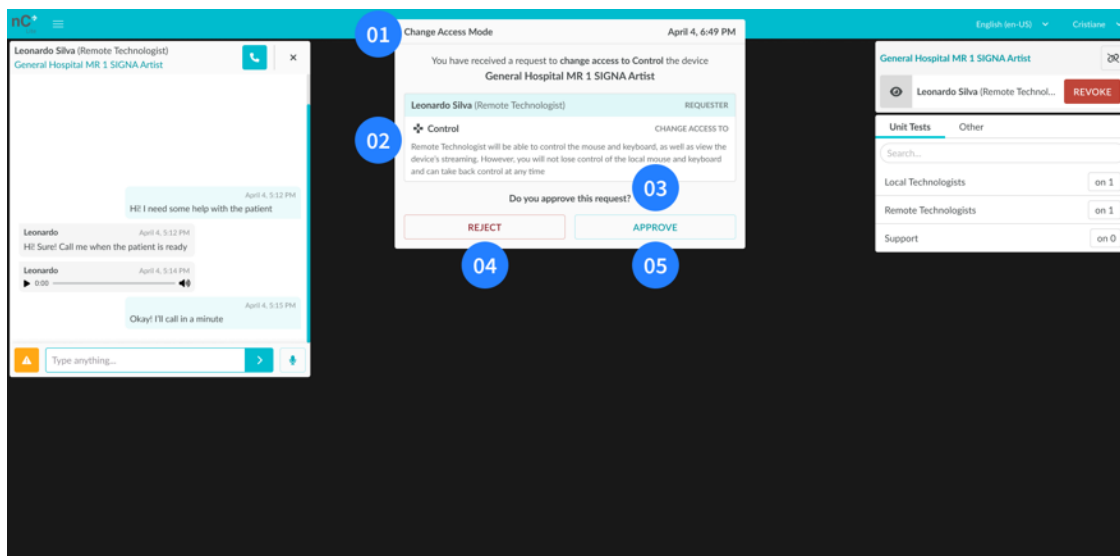
01 – Titel (Åtkomstförfrågan), **02** – Namn på den som begär, roll och beskrivning av åtkomsttyp, **03** – Fråga: "Do you approve this request? (Godkänner du denna begäran?)"; **04** – Knappen Reject (avvisa); **05** – Knappen Approve (godkänn)

Efter godkännande kan den lokala teknikern när som helst återkalla fjärrteknikerns åtkomst genom att helt enkelt klicka på knappen REVOKE (ÅTERKALLA).



Figur 12: Huvudskärm för lokal tekniker vid anslutning till en enhet
01 – Knappen Revoke (återkalla)

Under fjärrsessionen kan fjärrteknikern begära en ändring av åtkomstläget. Ett popup-meddelande om begäran visas på skärmen. Du kan godkänna eller avvisa den. Tänk på de privilegier som varje åtkomstläge ger fjärrteknikern.



Figur 13: Huvudskärm för lokal tekniker med begäran om att ändra åtkomstläge
01 – Titel (Change Access Mode (ändra åtkomstläge)), 02 – Namn på den som begär, roll och beskrivning av åtkomsttyp, 03 – Fråga: "Do you approve this request?" (Godkänner du denna begäran?), 04 – Knappen Reject (avvisa), 05 – Knappen Approve (godkänn)

**WARNING!**

Om anslutningen till den lokala datorn bryts har fjärrteknikern fortfarande åtkomst till *enheten*. Kontakta fjärrteknikern **omedelbart** och be honom/henne att **koppla från** ELLER logga in på en annan dator och **återkalla fjärrteknikerns åtkomst** ELLER **tryck på strömknappen** för att stänga av e-KVM-datorn.

**WARNING!****Vid underhåll av skanner:**

Innan fjärrteknikern påbörjar några procedurer (antingen på enheten eller i kontrollrummet) ska du informera fjärrteknikern och återkalla åtkomsten genom att klicka på knappen "REVOKE ACCESS" (ÅTERKALLA ÅTKOMST). Logga sedan ut från nCommand Lite-plattformen.

Om ingen fjärrtekniker är ansluten ska du logga ut från nCommand Lite-plattformen innan underhåll påbörjas.

Avsnitt 3.5 - Åtkomst med fjärrteknikerprofil

**WARNING!**

Användare av enhetsdator och rotlösenord: båda måste förvaras av värden på platsen som tar emot installationsteamet.

**WARNING!**

Bordsflyttningar under sessionen får endast utföras av den lokala teknikern på begäran av systemet. Innan den lokala teknikern lämnar operationssalen ska han/hon alltid återkalla fjärrteknikerns åtkomst.

**WARNING!**

Endast den lokala teknikern får flytta bordet för att placera patienten inuti enheten och för att frigöra patienten på ett säkert sätt. Innan den lokala teknikern lämnar salen ska han/hon alltid återkalla fjärranvändarens åtkomst.

**WARNING!**

Ha alltid uppsikt över rummet genom videokameran och säkerställ kommunikation med den lokala teknikern innan några åtgärder utförs.

**WARNING!**

Om anslutningen till den lokala datorn bryts ska du kontakta den lokala teknikern omedelbart och koppla från.

**WARNING!****Vid underhåll av skanner:**

Efter att ha blivit informerad om att enhetens underhåll har påbörjats ska du säkerställa att åtkomst har återkallats av den lokala teknikern och logga ut från nCommand Lite-plattformen.

Om åtkomst inte har återkallats ska du logga ut från nCommand Lite-plattformen och omedelbart kontakta den lokala teknikern för att informera denne.

**WARNING!**

För att fjärrstyra musen och tangentbordet måste det valda åtkomstläget vara kontroll, i visningsläge får fjärrteknikern bara se streaming och lokala kameror.

**WARNING!**

Om svaret på din begäran tar längre tid än förväntat kan du kontakta den lokala teknikern via chatt eller telefon.

Fjärrteknikerns arbetsplats innefattar utrustning som en dator, bildskärmar (vanligtvis tre), en mus, ett tangentbord och ett headset.

I det kliniska arbetsflödet har *lokala tekniker* direktkontakt med patienten. De ansvarar för patientinteraktion, positionering och för att säkerställa säkerhet och protokollefterlevnad under MRI-, CT- eller PET/CT-procedurer, i enlighet med institutionella och regulatoriska standarder.

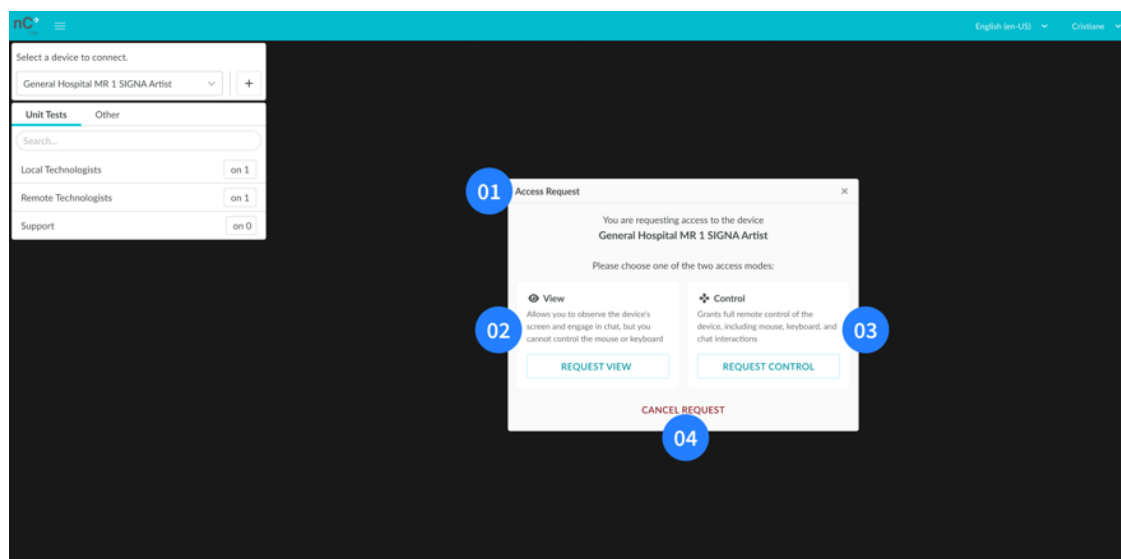
3.5.1. Åtkomstläge

När du har loggat in på plattformen väljer du enheten som du vill ansluta till i rutan Device Selection (val av enhet). Ett popup-fönster öppnas för att välja åtkomstläge mellan **Control** och **View**:

- **Kontrollläge** – I det här läget är mus- och tangentbordskontroll aktiverad utöver skärmvisning. Lokala yrkespersoner behåller full tillgång till den lokala musen och tangentbordet och kan när som helst ta tillbaka kontrollen.
- **Visningsläge** – Det är endast möjligt att se enhetens skärm och använda chatten för kommunikation.

Genom att välja åtkomstläget visas en ruta med "Waiting for approval" (väntar på godkännande) som indikerar att godkännande från den lokala teknikern som är ansluten krävs för att fortsätta. Denna lokala teknikern har full befogenhet att godkänna eller avvisa åtkomst och återkalla åtkomst när som helst om det anses nödvändigt. Denna åtgärd är nödvändig för att säkerställa strikt kontroll och upprätthålla säkerheten när enheten används.

Efter att ha valt enheten har användaren åtkomst till chattfunktionen, vilket möjliggör kommunikation via text, ljudmeddelanden, röst- och videosamtal med de andra användarna. Användaren behöver inte vara godkänd för att få åtkomst till chatten.



Figur 14: Åtkomstbegäran – dialog för fjärrtekniker

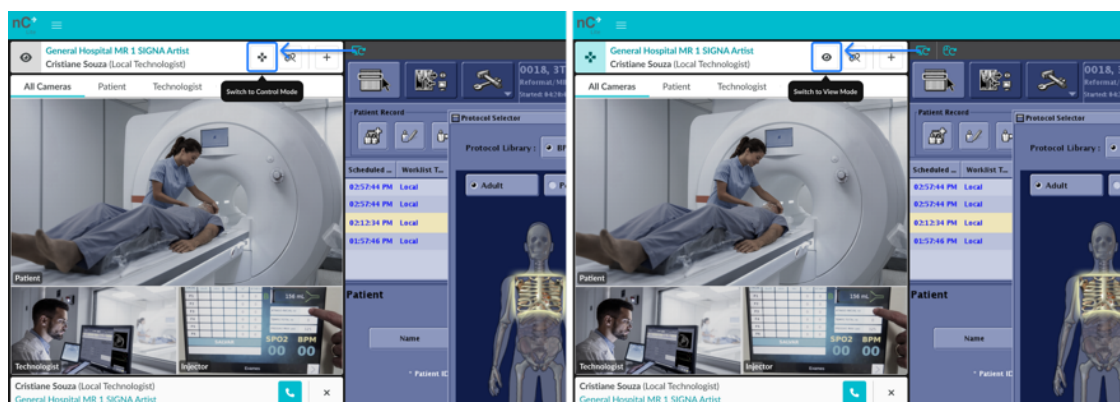
01 – Titel (Access Request – åtkomstbegäran), **02** – Beskrivning av visningsläge och knappen Request View (begär vy), **03** – Beskrivning av styrläge och knappen Request Control (begär styrning), **04** – Cancel Request (avbryt begäran)

När åtkomsten till enheten har godkänts av den lokala teknikern uppdateras fjärrteknikerns gränssnitt för att visa enhetens livesändning och dess tillhörande kameror. Om det valda åtkomstläget är kontroll, kommer funktionen för fjärrstyrning av enheten att aktiveras.

Denna process säkerställer effektiv och säker interaktion, vilket möjliggör säker fjärranvändning av enheten utan att äventyra dess integritet eller patientsäkerhet.

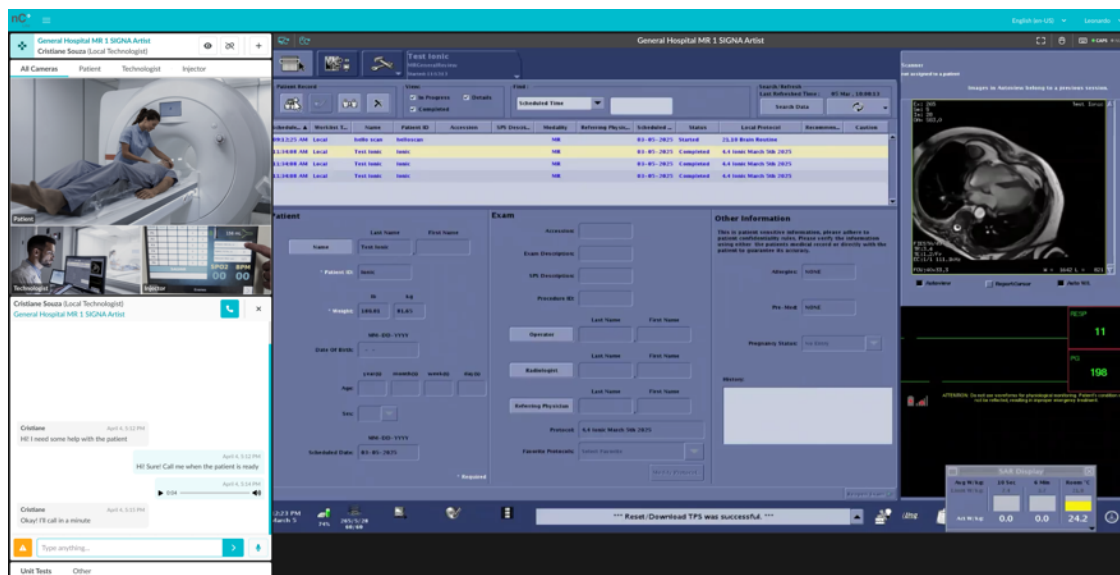
För att begära en ändring i åtkomstläget under en fjärrsession, klicka på den motsvarande ikonen. Den lokala teknikern kan godkänna eller avvisa begäran:

- **Accept (godkänn)** – streamingen kommer att laddas om, men chattinnehållet kommer inte att gå förlorat. Om du deltar i ett röst- och videosamtal kommer det att avslutas och måste startas om av en av användarna.
- **Decline (avslag)** - en popup kommer att visas som meddelar dig om den lokala teknikerns avslag och den aktuella åtkomsten kommer att förbli aktiv



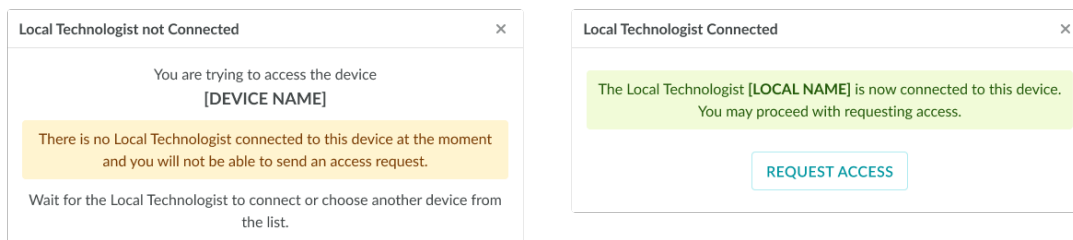
Figur 15: Ändra åtkomstläge

Vänster – Byt till styrlägesikon och verktygstips / Höger – Byt till visningslägesikon och verktygstips



Figur 16: Huvudskärm för fjärrtekniker vid anslutning till en enhet

När fjärrteknikern begär åtkomst och det inte finns någon lokal tekniker ansluten till enheten visar plattformen en popup-varning. Så snart den lokala tekniker ansluter informerar plattformen fjärrteknikern om att denne kan begära åtkomst igen.



Figur 17: Fjärrtekniker – varningar om lokal teknikers anslutningsstatus

Vänster – Meddelande som indikerar att ett försök att komma åt enheten gjordes, men att en lokal tekniker inte är ansluten för närvarande.

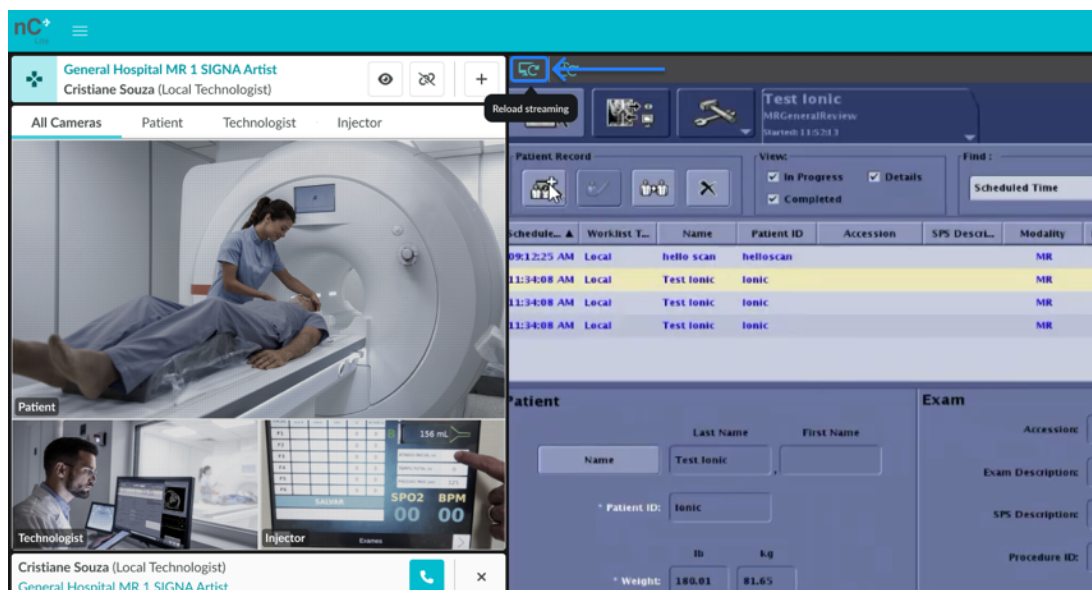
Höger – Meddelande som bekräftar att en lokal tekniker har anslutit till enheten efter att inte varit ansluten.

3.5.2. Streamingfält

I streamingfältet visas viktig information och kontroller som är relaterade till enhetens streaming-session. Den innehåller knapparna "Reload Streaming" och "Mouse Resync", enhetens namn, skärmapplösning och aktuell status för fjärrdatorns mus och tangentbord.

1 – Reload Streaming (Ladda om streaming)

Denna funktion gör att fjärrtekniker kan återställa åtkomst till enheter vid anslutningsfel eller prestandaproblem. Om du upplever någon typ av fränkoppling eller skärmfördröjning på enhetens dator kan du klicka på ikonen "Reload Streaming" i streamingfältet. Det gör att plattformen återansluter till enhetens dator och även laddar om systemkamerorna.

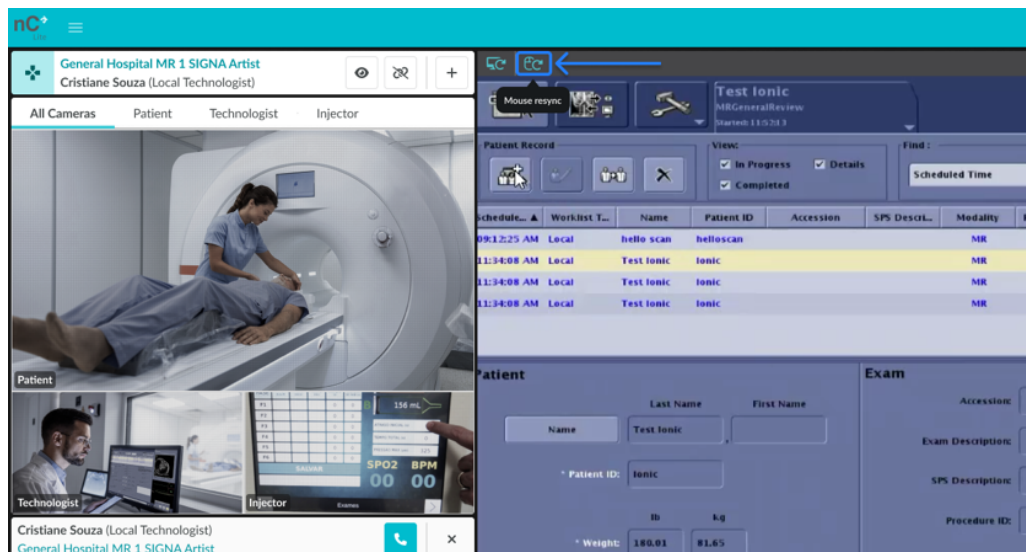


Figur 18: Knappen Reload Streaming (ladda om streaming)

2 – Omsynkronisering av mus

Om musen är långsam eller felinriktad ska du klicka på knappen "Mouse Resync" (Omsynkronisering av mus) som finns i fältet ovanför streamingfönstret för att synka om enhetens mus med e-KVM-datorn.

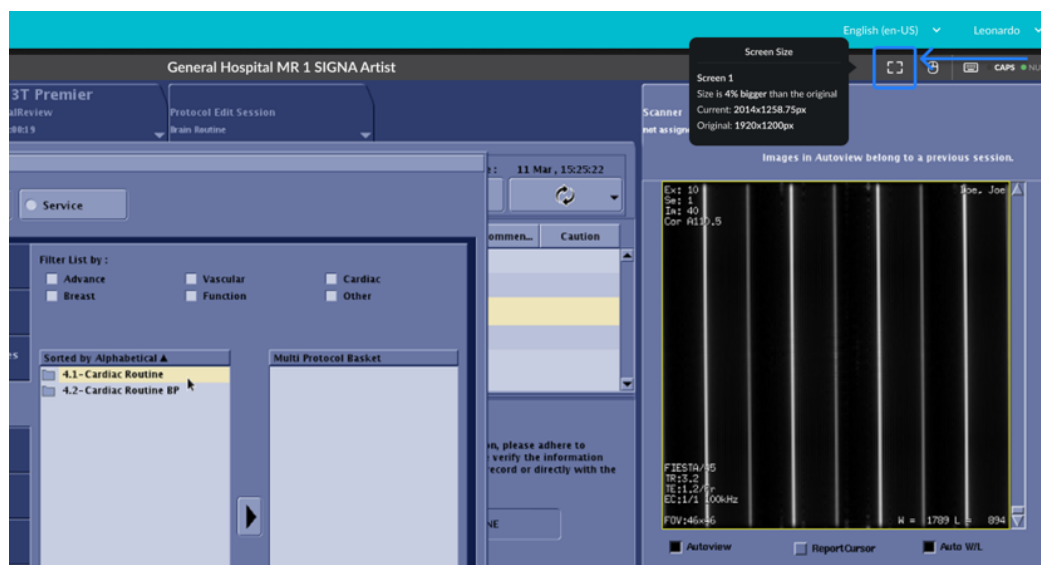
Ett alternativ är att flytta muspekaren utanför streamingområdet och sedan föra in den igen. Då kommer systemet automatiskt att synkronisera musen utan att någon ytterligare åtgärd behövs. Du kan också klicka och släppa rullningshjulet (när det är tillgängligt) för att aktivera en omsynkronisering. Det kanske inte fungerar på enheter med två eller fler skärmar om den lokala och fjärrstyrda muspekaren är på olika skärmar.



Figur 19: Musens omsynkroniseringsknapp

3 – Streamingskärm

Den här funktionen ger fjärrteknikern information om den ursprungliga streamingupplösningen (från enheten) och den aktuella upplösningen i pixlar som visas på fjärrarbetsstationen.



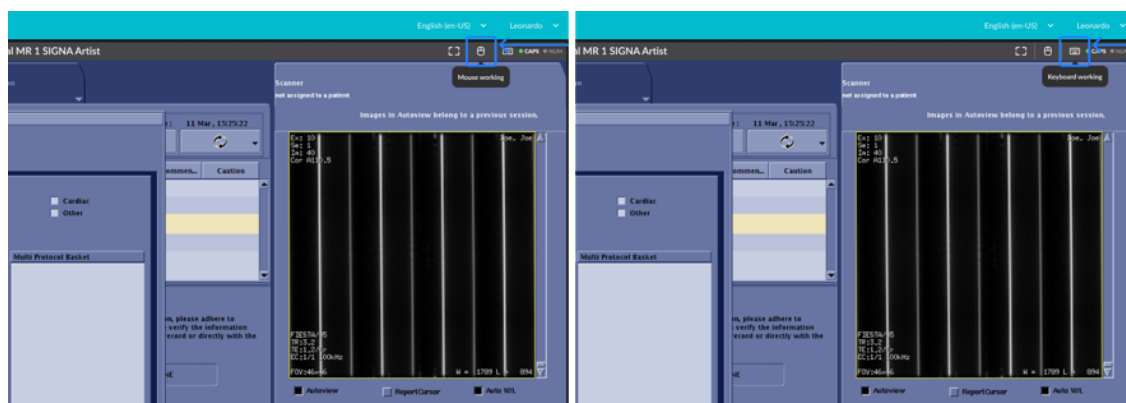
Figur 20: Verktystips för streaminginformation

4 – Mus- och tangentbordsstatus

Denna funktion informerar fjärrteknikern om huruvida musen och tangentbordet fungerar korrekt. Förutom tangentbordets status kan användaren se om tangenterna **Caps Lock** och **Num Lock** på enhetsdatorn är på eller av. Denna funktion beror dock på vilken enhetsdator som tillhandahåller denna information. I scenarier där denna information inte görs tillgänglig av enhetssystemet visas inte status för knapparna **Caps Lock** och **Num Lock**. Både mus- och tangentbordsstatus visas endast när användaren har åtkomst av typen Kontroll.

När du ansluter till en enhet kan en felmatchning mellan indikatorerna för **Caps Lock** och **Num Lock** på fjärrdatorn och enheten leda till inkonsekvent tangentbordsinmatning. Om indikatorerna visas aktiverade på enheten men inte faktiskt är aktiva på fjärrdatorn kan användaren skriva med versaler på enheten medan texten visas med gemener i chatten, eller tvärtom. På samma sätt, om **Caps Lock** är aktiverat på fjärrdatorn men inaktiverat på enheten, kommer samma problem att uppstå i omvänd ordning.

För att förhindra detta problem ska du säkerställa att **Caps Lock** och **Num Lock** är antingen aktiverade, eller inaktiverade innan du loggar in på enheten. Om en felmatchning inträffar ska användaren koppla från enheten, justera tangentstatusen på fjärrdatorn och sedan återansluta.



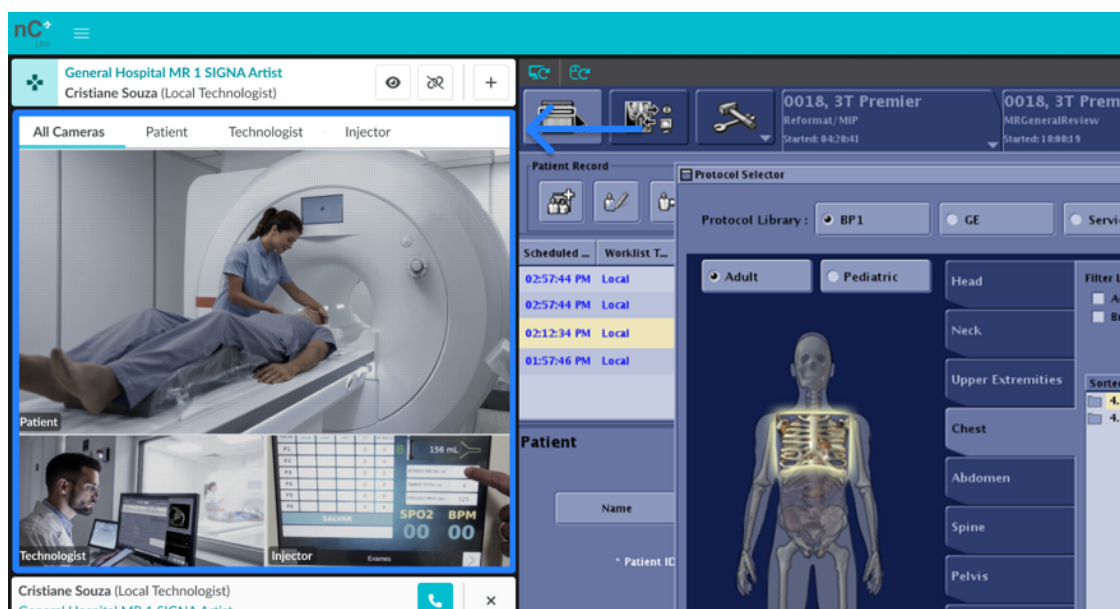
Figur 21: Streamingfält

Vänster – Musstatus, information i verktygstips

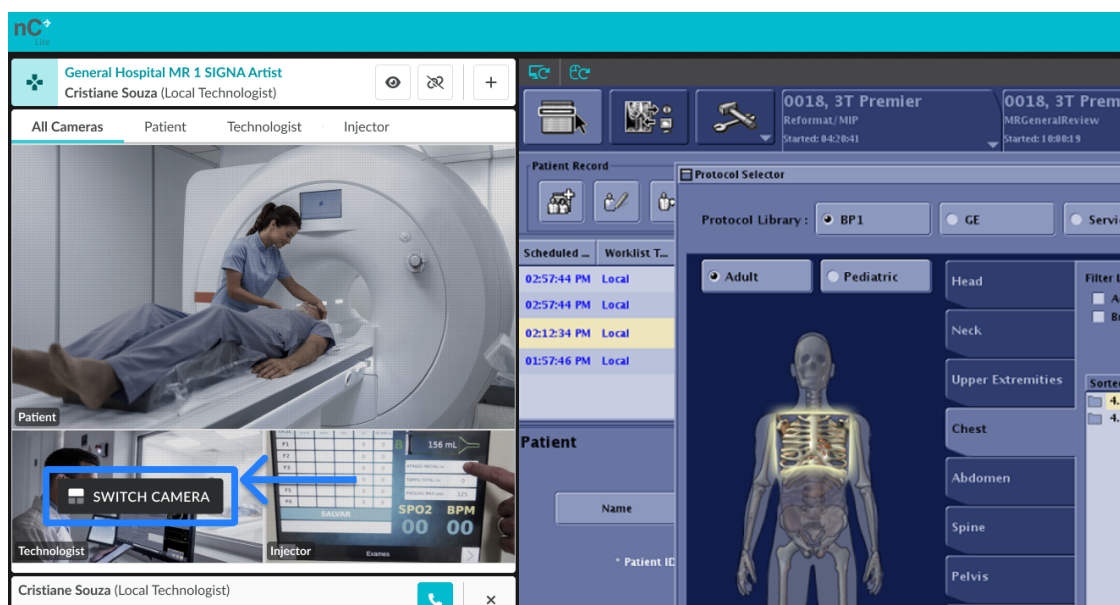
Höger – Tangentbordsstatus, information i verktygstips

3.5.3. Multikamera

Denna funktion gör det möjligt för fjärrteknikern att visa flera kameror samtidigt. Om fler än en kamera är tillgänglig kan du visa endast en kamera och växla mellan dem genom att klicka på menyn med det angivna namnet för varje kamera. När du väljer "ALL CAMERAS" (SAMTLIGA KAMEROR) visas alla tillgängliga kameror i ramen, med en av dem markerad. För att växla från den markerade kameran håller du bara muspekaren över en av kamerorna i den mindre ramen och klickar på "SWITCH CAMERA" (BYT KAMERA).



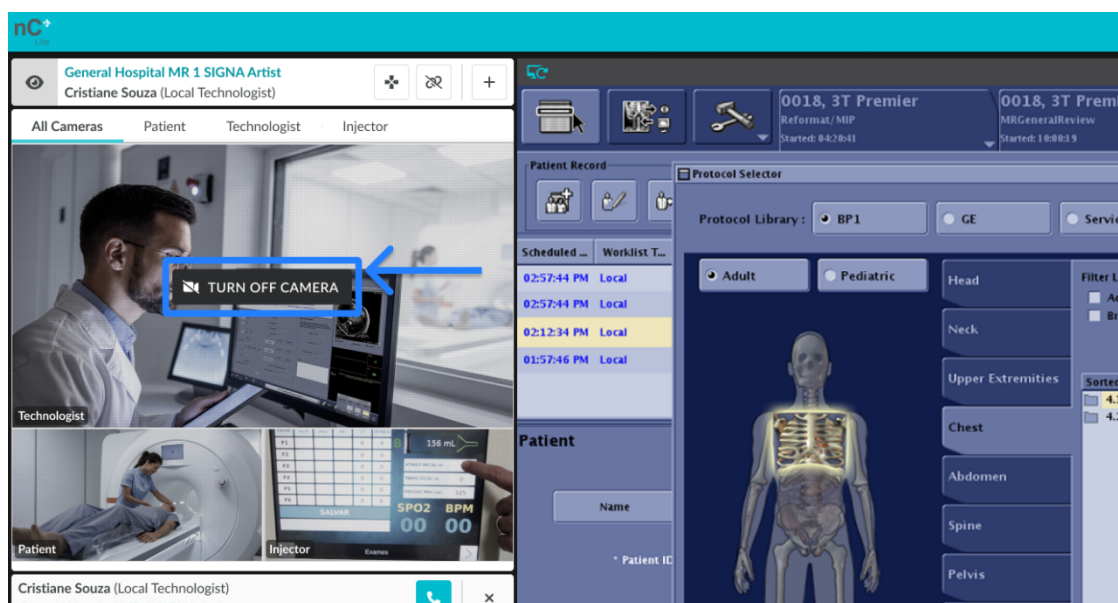
Figur 22: Multikameravvy



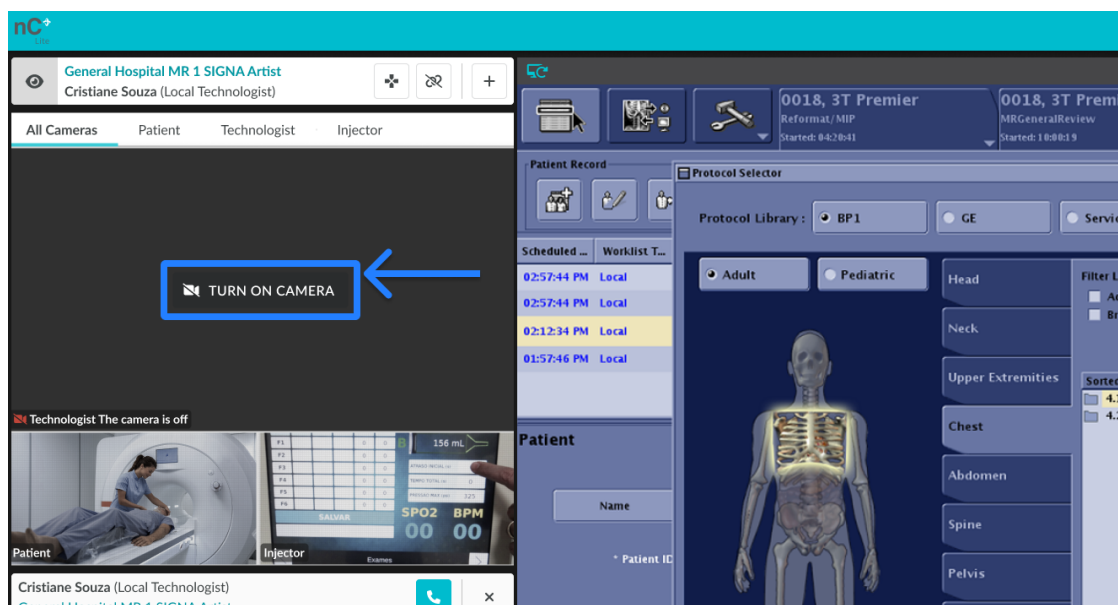
Figur 23: Hovringsknapp "SWITCH CAMERA" (byt kamera) för multikamera

Om fjärrteknikern har åtkomsten **View (visning)** under en aktiv fjärrsession finns det ett alternativ att stänga av en eller flera kameror genom att hålla muspekaren över den valda kameran och klicka på "TURN OFF CAMERA" (STÄNG AV KAMERA). Om du vill visa kameran igen upprepar du bara processen och klickar på "TURN ON CAMERA" (AKTIVERA KAMERA).

OBSERVERA: Alternativet att stänga av kamerorna är endast tillgängligt i läget View (visning); i läget Control (kontroll) går det inte att stänga av kamerorna.



Figur 24: Hovringsknapp "TURN OFF CAMERA" (stäng av kamera) för multikamera i visningsläge



Figur 25: Hovringsknapp "TURN ON CAMERA" (slå på kamera) för multikamera i visningsläge

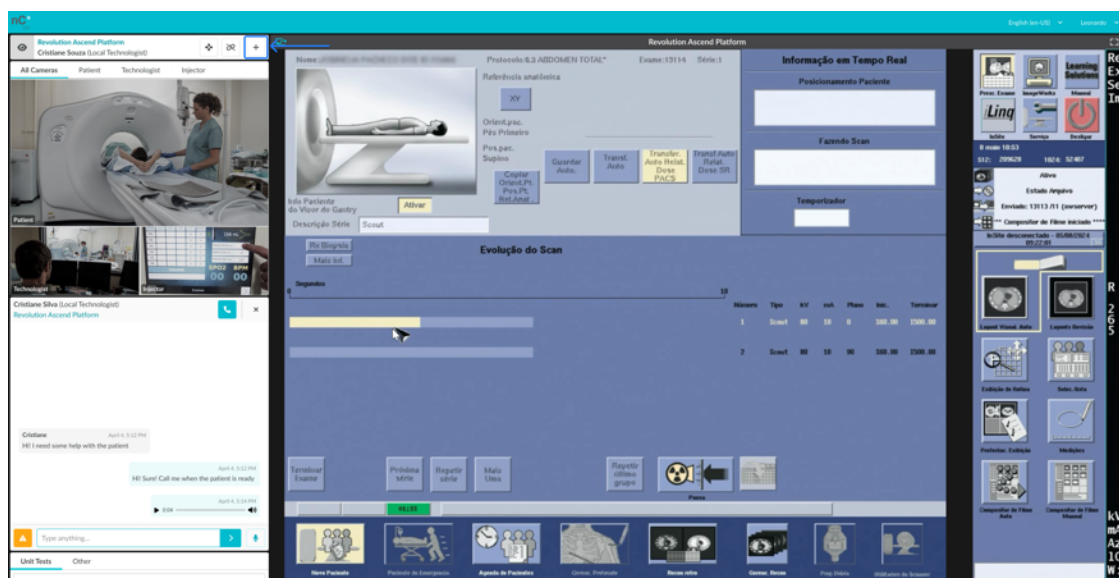
3.5.4. Öppna en annan enhet

Gör det möjligt för fjärrteknikern att öppna en ny webbläsarflik i nCommand Lite, vilket tillåter användaren att välja en ny enhet för att utföra fler än en fjärrskanning samtidigt. För att öppna en ny enhet för åtkomst klickar du bara på knappen "Open Another Device" (öppna en annan enhet) och en varning visas så att du säkert kan utföra denna samtidiga åtgärd. Du bör läsa varningen innan du öppnar detta nya fönster.

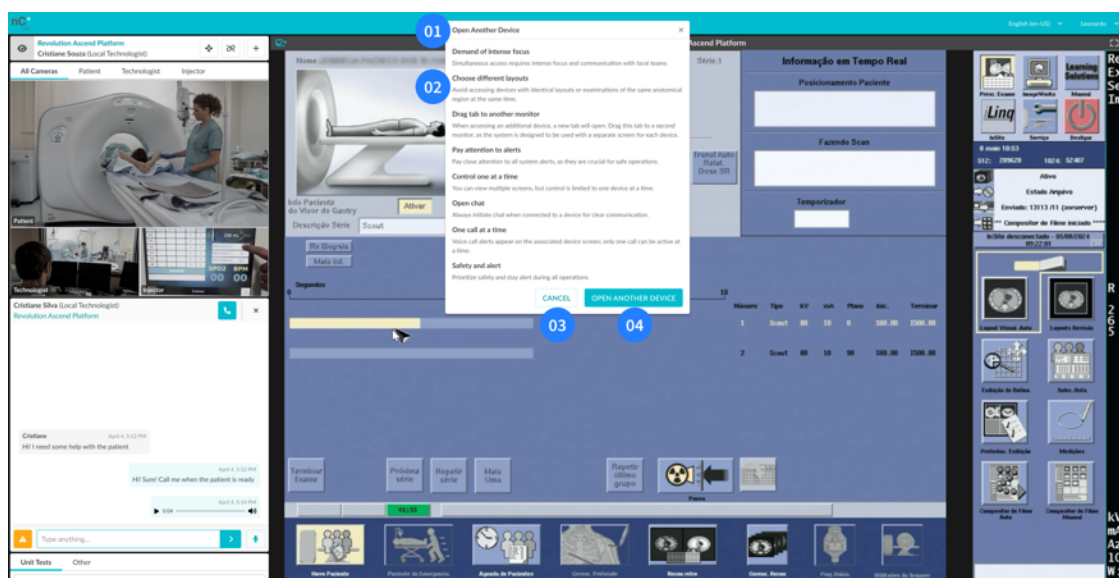
OBSERVERA: För bättre visning under samtidig åtkomst rekommenderas det att du drar den nya fliken till en annan tillgänglig bildskärm efter att ha klickat på "OPEN ANOTHER DEVICE" (ÖPPNA EN ANNAN ENHET) och klickat på "OK" i varningarna.

**WARNING!****Säkerhetsvarning om åtkomst till flera skannrar**

- **Demand of intense focus (krav på intensivt fokus):** Samtidig åtkomst kräver intensivt fokus och kommunikation med lokala team.
- **Välj olika layouter:** Undvik att koppla upp till enheter med identiska layouter eller undersökningar av samma anatomiska region vid samma tidpunkt.
- **Dra fliken till en annan bildskärm:** Vid åtkomst till ytterligare en enhet, kommer en ny flik att öppnas. Dra den här fliken till en annan bildskärm, eftersom systemet är utformat för att användas med en separat skärm för varje enhet.
- **Var uppmärksam på varningar:** Var speciellt uppmärksam på alla systemvarningar, de är avgörande för säker drift.
- **Styr en åt gången:** Du kan visa flera skärmar, men kontrollen är begränsad till en enhet åt gången.
- **Öppna chatt:** Starta alltid chatten när du är ansluten till en enhet för tydlig kommunikation.
- **Ett samtal åt gången:** Röstsamtalsvarningar visas på den associerade enhetens skärm – endast ett samtal kan vara aktivt åt gången.
- **Säkerhet och uppmärksamhet:** Prioritera säkerhet och var alltid uppmärksam när enheterna är i drift.



Figur 26: Knappen Open Another Device (öppna en annan enhet) (+)



Figur 27: Varningar om åtkomst från flera enheter

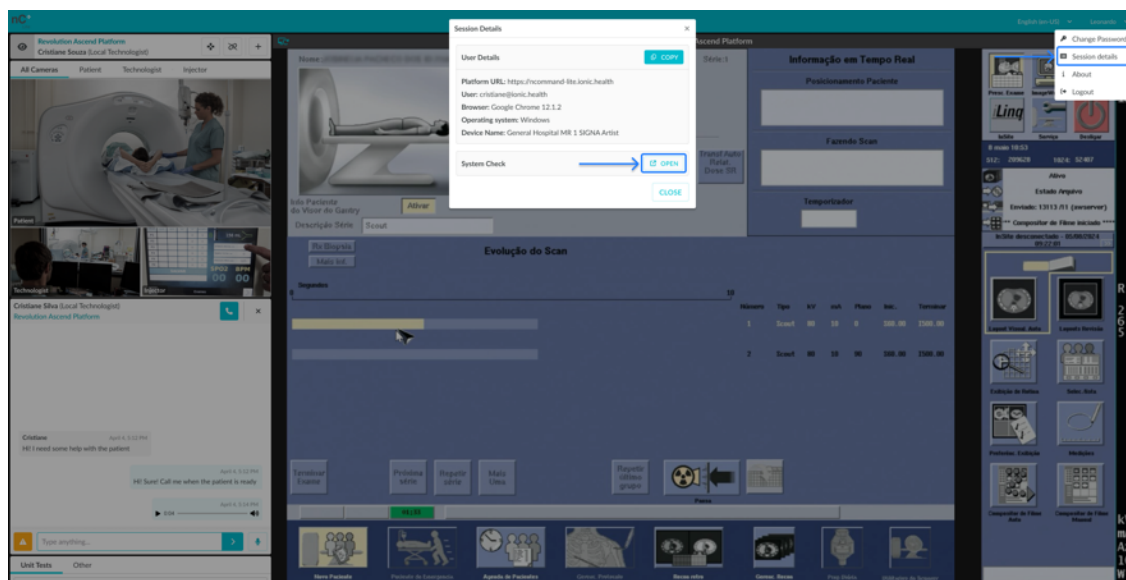
01 – Titel (Open Another Device (öppna en annan enhet)), **02** – Varningar om driftsäkerhet, **03** – Knappen Cancel (avbryt), **04** – Knappen Öppna en annan enhet

3.5.5. Systemkontroll

Systemkontrollen hjälper till att verifiera att den aktuella enheten, nätverket och internetanslutningen uppfyller kraven för att använda nCommand Lite korrekt. Den utför ett snabbt automatiskt test som kontrollerar viktiga saker som internetkvalitet, tillgång till nödvändiga servrar och anslutningens stabilitet. Verktøget kan användas innan en session startas, under installationen eller när anslutningsproblem misstänks. Det hjälper till att säkerställa att plattformen fungerar som förväntat och hjälper det tekniska teamet om felsökning behövs.

Observera: Systemkontrollen bör helst användas med hjälp av eller på begäran av en IT-ansvarig. Att använda detta verktyg utan teknisk vägledning kan leda till feltolkning av resultaten.

För att få åtkomst till systemkontrollen kan lokala tekniker och fjärrtekniker öppna alternativet Session Details (sessionsuppgifter) på rullgardinsmenyn under användarnamnet överst till höger på huvudskärmen. Klicka sedan på **Open** (öppna) bredvid verktyget **System Check** (systemkontroll). När verktygssidan visas klickar du på **Run Test** (Kör test) för att starta verifieringsprocessen.

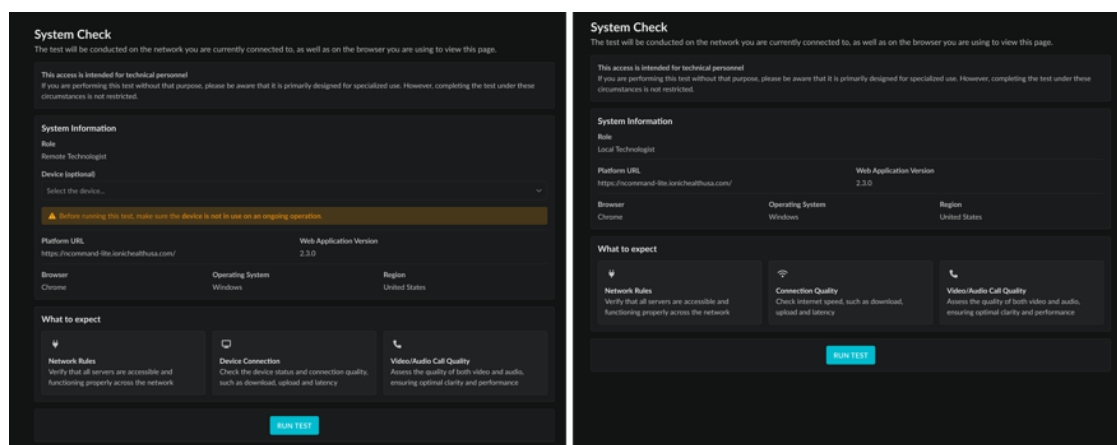


Figur 28: Åtkomst till systemkontroll

När en fjärrtekniker arbetar går det att välja en enhet på verktygets huvudsida så att det inkluderas i testresultaten.

**WARNING!**

Innan du startar testet ska du se till att den valda enheten inte används.



Figur 29: Systemkontroll, huvudskärm
Vänster – Fjärrtekniker / Höger – Lokal tekniker

När testet är klart visas en sammanfattning av resultaten på skärmen. IT-ansvariga kan granska informationen för att identifiera möjliga problem som påverkar systemets prestanda.

Avsnitt 3.6 - Chatt

Plattformen har en chatt- och samtalsfunktion i realtid med röst- och videofunktioner som används för effektiv kommunikation mellan legitimerade tekniker. Genom dessa funktioner kan legitimerade tekniker kommunicera om alla frågor som rör sessionens arbetsflöde.

**WARNING!**

Vid fel, ring den lokala teknikern per telefon.

När du ansluter till en enhet får du omedelbar tillgång till chattens användarlista, organiserad i två flikar. För kunder med flera platser kan varje gren konfigureras som ett separat kontrakt. När det är aktiverat grupperas användare efter avtal, med användare från andra avtal som visas under fliken "Övriga".

För att starta en konversation kan du dubbelklicka på en användares namn för att öppna chattgränssnittet som har stöd för både textmeddelanden och röstsamtal. Se till att den valda sessionen motsvarar rätt enhet. Plattformen meddelar användarna om nätverksanslutningen blir långsam eller instabil.

**WARNING!**

Innan du påbörjar kontakten, kontrollera enhetsnamnet som visas under användarens namn, eftersom vissa fjärrtekniker kan vara anslutna till flera enheter.

Här är verktygen som finns tillgängliga för kommunikation inom plattformen:

1. **Röst- och videosamtal:** Klicka på ikonerna för att starta ett röst- och videosamtal på upp till 60 minuter mellan en fjärrtekniker och en lokal tekniker. Anslutningar mellan användare med samma profil (lokal-lokal eller fjärr-fjärr) stöds inte.

När en lokal tekniker initierar ett samtal kan fjärrteknikern välja att acceptera eller avslå. Omvänt, när en fjärrtekniker initierar samtalet, ansluts det automatiskt och den lokala teknikern meddelas. Det fungerar som en säkerhetsmekanism för att säkerställa att fjärrteknikern alltid kan kommunicera med den som är fysiskt närvarande på platsen.

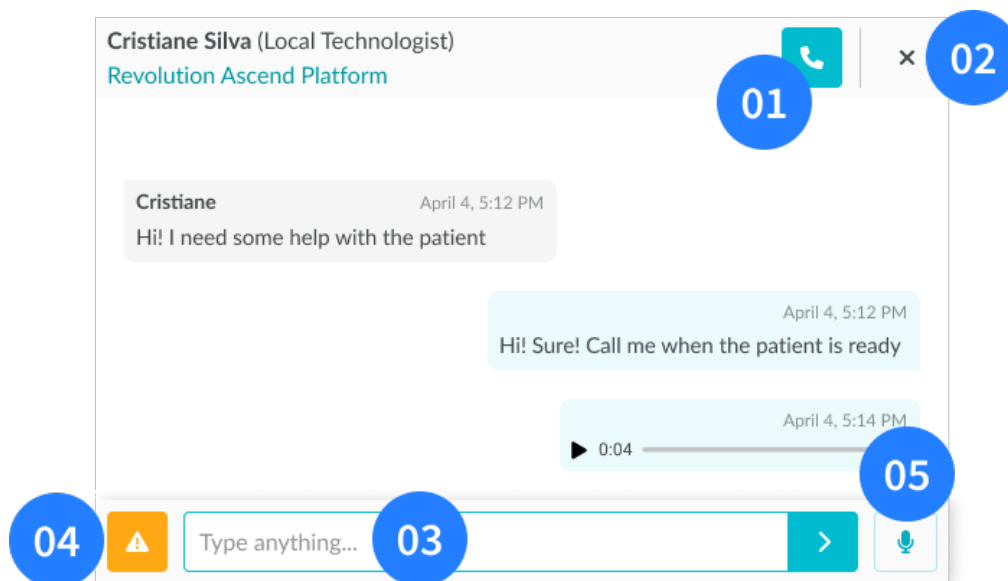
Som standard är mikrofonen aktiv i början av samtalet, medan kameran är avstängd. Varje tekniker kan när som helst manuellt slå på eller av sin mikrofon och kamera.

För att lyckas upprätta ett samtal måste båda användarna ha en fungerande mikrofon och ljudutgång, med webbläsarbehörigheter korrekt aktiverade. Om någon av dessa komponenter saknas kommer systemet att meddela båda användarna och samtalet kommer inte att kopplas. En kamera är valfri – om den inte är tillgänglig eller inte upptäcks kommer systemet att uppdatera ikonerna för att återspegla att video inte stöds.

Endast ett aktivt samtal tillåts per användare. Om en tekniker försöker starta ett nytt samtal under ett pågående, kommer systemet att blockera försöket och visa ett meddelande. På samma sätt, om en användare redan är i ett samtal och tar emot ett annat inkommande samtal, kommer den som ringer att informeras om att mottagaren för närvarande inte är

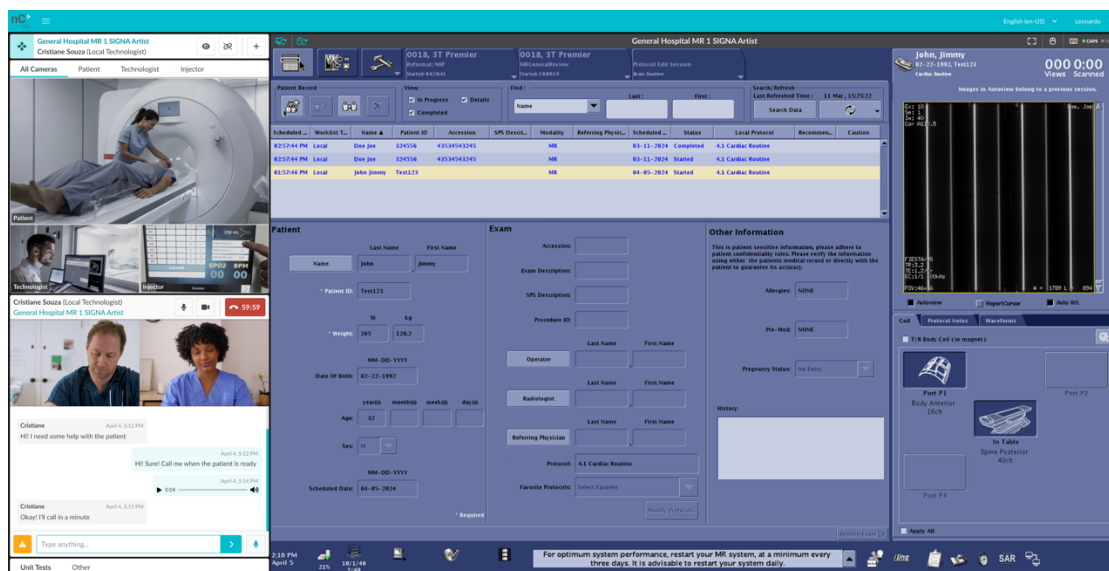
tillgänglig, och användaren i det pågående samtalet kommer att få en avisering som anger att någon försökte kontakta dem.

2. **Stänga chattar:** När en av användarna stänger chatten genom att klicka på stängningsknappen skickas ett automatiskt meddelande till den andra användaren, och chattfliken stängs. Detta säkerställer att båda parter informeras om att samtalet har avslutats. När chattfönstret stängs försvinner alla meddelanden. Om du öppnar samtalet igen under sessionen startas det om utan de tidigare meddelandena.
3. **Textmeddelanden:** Skicka textmeddelanden i det avsedda fältet. När ett meddelande skickas visas en ikon med en grå bock, och när meddelandet tas emot av mottagaren visas en annan ikon med två blå bockar. Detta möjliggör säker, tydlig och kortfattad skriftlig kommunikation mellan de två parterna.
4. **Uppmärksamhetsanrop:** Klicka på knappen med ett utropstecken för att få den andra användarens uppmärksamhet. Denna åtgärd avger en visuell vibrationseffekt på den andra användarens skärm i några sekunder och ett meddelande skickas automatiskt, vilket signalerar brådskandegrad eller vikt.
5. **Ljudmeddelanden:** Skicka ljudmeddelanden genom att klicka på mikrofonknappen. Använd detta när du vill framföra ett meddelande mer personligt eller när det inte är lämpligt att skriva.

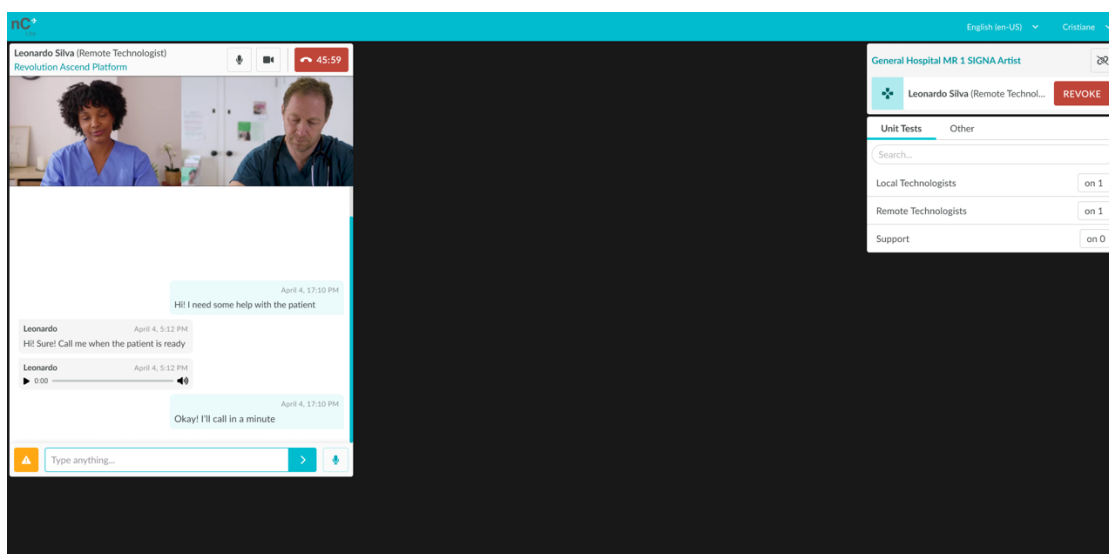


Figur 30: Vy över chattfönster

01 – Knapp för röst- och videosamtal; **02** - Stäng chatt-knapp; **03** – Textfält för meddelande;
04 – Knapp för att påkalla uppmärksamhet; **05** – Spela in Knapp för ljudmeddelande



Figur 31: Fjärrteknikerns huvudskärm – chattfönster (nere till vänster)



Figur 32: Huvudskärm för lokal tekniker – chattfönster

Problem med internetanslutning – När en av teknikerna har problem med nätverksanslutningen visar systemet ett meddelande och försöker återansluta. Om anslutningen återställs visar systemet ett meddelande om **ONLINE** och fjärrsessionen fortsätter som vanligt. Om anslutningen inte återupprättas efter flera försök till återanslutning kommer systemet dock att avsluta den aktiva sessionen och meddela teknikern att denne har kopplats bort på grund av internetproblem. Samtidigt kommer den också att meddela den andra teknikern att dennes motpart har kopplats bort på grund av internetproblem.

Avsnitt 3.7 - Avsluta din session på plattformen

När hans/hennes arbete är avslutat måste den legitimerade teknikern koppla bort från enheten och logga ut från plattformen.

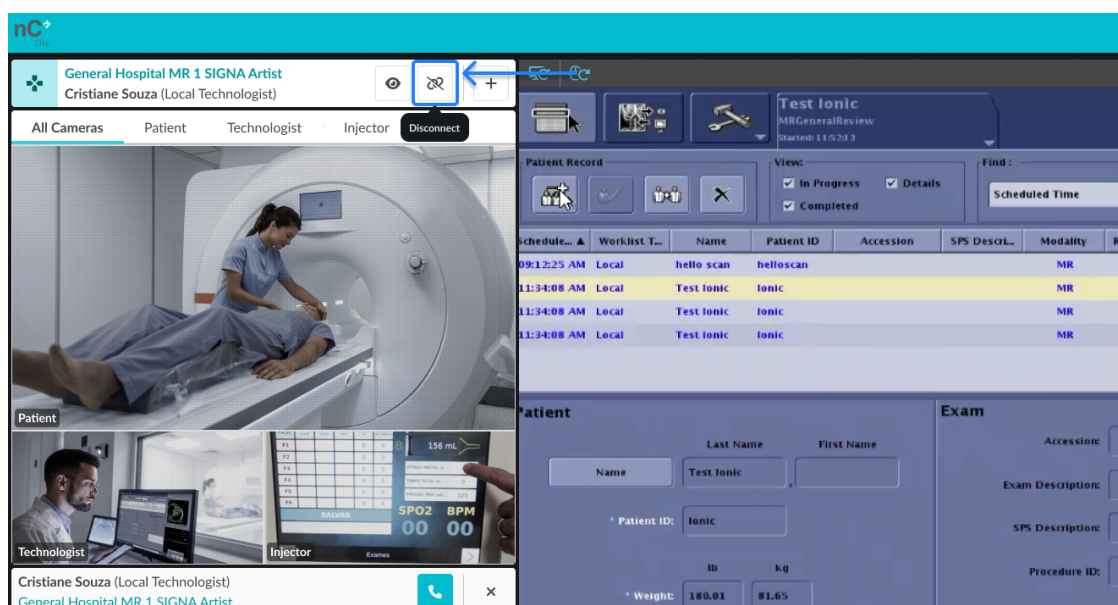


WARNING!

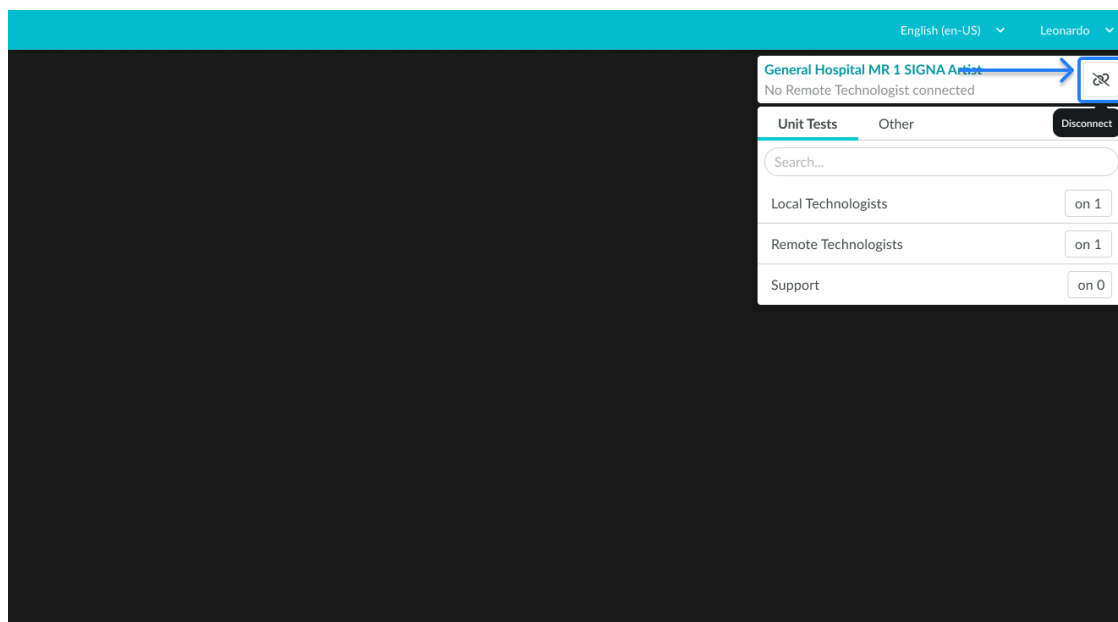
De legitimerade teknikerna får inte glömma att logga ut från plattformen innan arbetet avslutas.

För att koppla från enheten behöver du klicka på fränkopplingsikonen som finns i enhetsrutan. Observera: Om du arbetar som lokal tekniker ska du säkerställa att all åtkomst för fjärrtekniker har återkallats innan du kopplar bort enheten.

För att säkerställa säkerheten kommer du att få ett meddelande där du ombes att bekräfta att du vill koppla bort enheten. När du har bekräftat omdirigeras du till startskärmen utan att någon vald enhet.



Figur 33: Knappen Disconnect (koppla från) – fjärrteknikerns huvudskärm



Figur 34: Knappen Disconnect (koppla från) – den lokala teknikerns huvudskärm

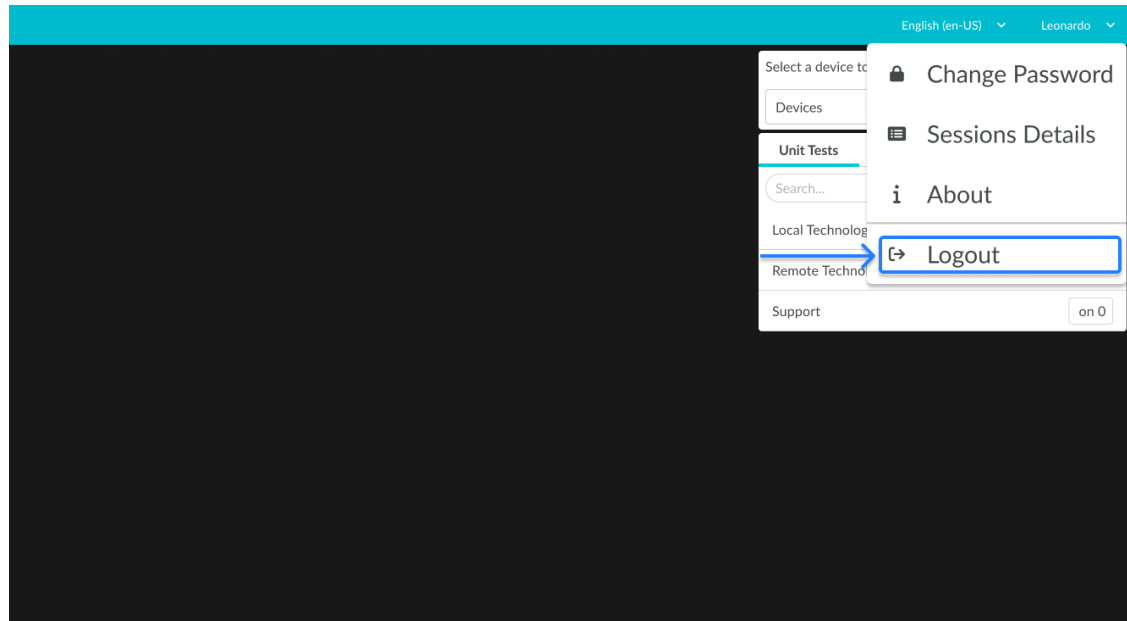


WARNING!

Innan du loggar ut måste du se till att alla ytterligare flikar som öppnades är stängda.

För att avsluta din session på plattformen ska du klicka på ditt användarnamn längst upp till höger på skärmen och välja alternativet "Logout" (logga ut). Du kommer att få ett meddelande där du ombes att bekräfta att du vill lämna sjukvårdsinrättningen där du arbetade. När du har bekräftat omdirigeras du till applikationens inloggningssida, där du kan slutföra ditt arbete på ett säkert sätt.

nCommand Lite kontrollerar inte användarens session på den externa IdP:n och kan därför inte utföra en utloggning på IdP-nivå. I scenarier där användare delar samma maskin och använder Single Sign-On (SSO), rekommenderas det att varje användare väljer alternativet "Do not stay signed in" under extern IdP-inloggning (om tillgängligt) eller loggar ut från IdP:n efter att ha loggat ut från nCommand Lite. Detta säkerställer att ingen efterföljande användare på samma enhet oavsiktligt kan återanvända en aktiv session.



Figur 35: Menyalternativet Logout (Logga ut)



WARNING!

När du använder en extern identitetsleverantör på en delad eller offentlig dator, efter att du loggat ut från plattformen, logga även ut från identitetsleverantören. För mer information om hur du går vidare, kontakta organisationens IT-supportteam.

Avsnitt 3.8 - Användarutbildning

Deltagande i utbildningsprogrammet är obligatoriskt för alla användare av nCommand Lite-systemet. Användarregistreringen på plattformen hanteras av IONIC Health-teamet och initieras först efter bekräftelse på att användaren framgångsrikt har slutfört den obligatoriska LMS-utbildningen och är korrekt kvalificerad att använda plattformen. Denna process säkerställer att alla användare har en grundlig förståelse för systemets funktioner och är beredda att använda plattformen effektivt och säkert. Kontakta en säljare för att påbörja registreringsprocessen för utbildningen.

Avsnitt 3.9 - Felsökningsriktlinjer

ANVÄNDARE OCH LÖSENORD	
Byta lösenord	Bekräfta att lösenordskraven har uppfyllts. Lösenordet måste vara starkt och säkert, och innehålla minst en liten bokstav, en stor bokstav, ett specialtecken och vara minst 8 tecken långt.
Glömt mitt lösenord	Kontrollera din e-postinkorg: Säkerställ att du använder rätt e-postadress och att e-postmeddelandet för återställning av lösenord inte har filtrerats in i din skräppostmapp. Försök igen: Vänta några minuter och begär ett nytt e-postmeddelande för återställning av lösenord genom att klicka på "Did you Forget your password? (Har du glömt ditt lösenord?)." Kontrollera internetanslutning: Se till att du är ansluten till internet.
Välkomstmeddelande ej mottaget	Kontrollera om e-postmeddelandet finns i din skräppostmapp. Om det inte finns där ska du kontakta en administratör för att säkerställa att e-postadressen i din registrering är korrekt. Om den inte är korrekt ska administratören uppdatera den och skicka välkomstmeddelandet igen.
Kod för tvåstegsautentisering ej mottagen	Klicka på "Resend Code" (skicka kod igen) och kontrollera din skräppostmapp. Om du inte får den ska du kontakta en administratör för att kontrollera om e-postmeddelandet som registrerats i åtkomstkontrollen är korrekt.
För många inloggningsförsök	Om du överskrider det tillåtna antalet inloggningsförsök måste du vänta en stund innan du försöker igen.
EXTERN IDENTITETSLIVERANTÖR	
Problem med att logga in på produkten	Om du stöter på inloggningsproblem när du använder en extern identitetsleverantör (IdP), observera att autentiseringsprocessen hanteras helt av IdP:n och inte av produktleverantören, dvs. Ionic Health. Som sådan kan

	produkten inte hjälpa till med kontouppgifter, åtkomstpolicyer, autentiseringsfel eller kontoutelåsning. I dessa fall bör du kontakta organisationens IT-supportteam, som kan granska IdP-konfigurationen och hjälpa till att lösa problemet.
Problem med autentiseringsuppgifter	Eventuella problem med autentiseringsuppgifter (<i>t.ex.</i> , glömt lösenord, lösenordsändring) måste lösas direkt med din organisations IT-supportteam. De kan granska IdP-konfigurationen och ge nödvändig hjälp.
Problem med multifaktorautentisering (MFA)	Eventuella problem med multifaktorautentisering (MFA) (<i>t.ex.</i> , problem med MFA-förfalldatum, MFA fungerar inte, inloggning utan att begära MFA) måste lösas direkt med din organisations IT-supportteam. De kan granska IdP-konfigurationen och ge nödvändig hjälp.
Autentiseringsuppgifter fungerar inte på plattformen	När du använder externa identitetsleverantörer (IdP) loggar du endast in på produkten med IdP:n. Om du använder IdP-uppgifterna direkt på produktens inloggningssida kommer inloggningen att misslyckas.
SKANNINGSDATORNS BILDSKÄRM	
Startar inte	Kontrollera bildskärmens anslutningar till datorn och eluttaget. Frånkopplingar kan förekomma. Tryck på bildskärmens strömknapp igen.
PLATTFORM	
Oåtkomlig	Kontrollera nätverksanslutningen. Kontrollera om plattformen har startat och om inloggningen har skett.
Plattformens svarstid	Uppdatera sidan genom att trycka på Ctrl+F5. Kontrollera om avdelningens (sjukvårdsinrättningens) chatt är öppen i fler än en flik. Om så är fallet, stäng fliken som inte används. Om problemet kvarstår ska du försöka logga ut från plattformen, rensa cacheminnet, stänga webbläsaren och sedan logga in igen.
Ej fungerande funktioner	Innan du provar andra felsökningsprocedurer, rensa

	webbläsarens cache (leta efter instruktioner i din nuvarande webbläsare) efter inloggning, stäng och öppna sedan webbläsaren igen, logga in på plattformen igen och försök igen.
Uppgradera	Efter att plattformen har uppgraderats, rensa webbläsarens cache (se instruktionerna för din webbläsare) innan du loggar in på den nya versionen.
LJUD	
Inget ljud	Se till att volymerna på avdelningens (sjukvårdsinrättningens) mikrofon och högtalare justeras till lämpliga nivåer. Kontrollera om webbläsaren har behörighet att använda ljud och mikrofon. Kontrollera om headsetet är anslutet och fungerar korrekt.
Ljutfördröjning	Kontrollera utrustningens elektriska anslutningar och nätverksanslutningar. Uppdatera webbläsarsidan genom att trycka på Ctrl+F5 och logga in igen. Om problemet kvarstår ska du försöka logga ut från plattformen, rensa cacheminnet, stänga webbläsaren och sedan logga in igen.
CHATT	
Chatten visas inte	Kontrollera om webbläsaren är minimerad. Annars öppnar du chatten efter inloggning i nCommand Lite-plattformen. Kontrollera att avdelningen (sjukvårdsinrättningen) har valts och att användaren har behörighet att aktivera chattkommunikation. Se till att din webbläsares ljud- och mikrofonbehörigheter är godkända. Kontrollera kabelanslutningarna, de kan vara fränkopplade.

	Uppdatera webbläsarsidan genom att trycka på Ctrl+F5 och återanslut till plattformen. Kontrollera om inrättningens chatt är öppen i fler än en flik. Om så är fallet, stäng fliken som inte används.
Chattfördröjning	Uppdatera webbläsarsidan genom att trycka på Ctrl+F5 och återanslut till plattformen. Om problemet kvarstår ska du försöka logga ut från plattformen, rensa cacheminnet, stänga webbläsaren och sedan logga in igen. Kontrollera kabelanslutningarna, de kan vara fränkopplade.
Problem med att skicka ljudmeddelanden	Kontrollera webbläsarbehörigheter för ljud och mikrofon och säkerställ att både mikrofon och ljudenheter är anslutna till datorn. Om webbläsarbehörigheterna behöver justeras trycker du på Ctrl+F5 för att uppmana webbläsaren att känna igen ändringarna när sidan laddas om.
Kunde inte starta röstsamtal	Kontrollera din internetanslutning och se om något meddelande visades som förklarar orsaken till att samtalet inte startade. Säkerställ att du har en ansluten ljudenhet och att ljud- och mikrofonbehörigheter är tillåtna i webbläsaren. Om problemet kvarstår ska du uppdatera sidan med Ctrl+F5 för att försöka igen.
Användare hittades inte i chatt	Om du inte kan hitta en användare i chatten ska du klicka på fliken "Others" (övriga) för att kontrollera om de finns där. Användare som är associerade med andra avtal visas separat i kontaktlistan. Om användaren inte visas i kontaktlistan efter att du har valt enheten ska du trycka på Ctrl+F5 för att uppdatera skärmen och välja igen. Se till att du har en internetanslutning.
BEGÄRA ÅTKOMST TILL ENHETEN	

Plattformen upptäckte inte att den lokala teknikern är ansluten	Kontrollera under alternativet "Others" (övriga) för att bekräfta om den lokala användaren är ansluten. Om användaren verkligen är ansluten men du fortfarande får meddelandet att den lokala användaren inte är ansluten till skannern ska du uppdatera skärmen genom att trycka på Ctrl+F5 och be den lokala användaren att göra samma sak. Välj sedan enheten igen och be den lokala användaren att också välja enheten igen. Kontakta support för att kontrollera nätverket om problemet kvarstår.
Åtkomstbegäran skickas inte	Uppdatera sidan genom att trycka på Ctrl+F5 och bekräfta med den lokala användaren via chatt om åtkomstbegäran tas emot. Kontakta support för ytterligare hjälp om problemet kvarstår.
STREAMINGENHET (e-KVM-DATOR)	
Streamingenhet (e-KVM-DATOR) fungerar inte	Klicka på knappen "Reload streaming" (ladda om streaming) på plattformen. Se till att den avbrottsfria och stabiliserade strömförsörjningen (sjukvårdsinrättning) och/eller streamingenheten är korrekt anslutna och påslagna. Stäng av streamingenheten och all annan utrustning och slå på den igen. Uppdatera plattformen.
Streamingenhet långsam	Klicka på knappen "Reload streaming" (ladda om streaming) på plattformen. Uppdatera sidan med Ctrl+F5 och återanslut till plattformen. Kontrollera kvaliteten på din nätverksanslutning. För att validera nätverksstatusen är det möjligt att utföra ett pingtest i enheten för att göra en kontroll avseende paketförlust. Efter internetproblem kanske plattformen inte fungerar som avsett. Uppdatera

	webbsidan och begär åtkomst till den lokala användaren igen.
Förlorad videoutmatning	Att en elektrostatisk urladdning orsakar förlust av bild är känt. Efter en omstart av systemet ska kommunikationen och videostreamingen återupprättas automatiskt.

Avsnitt 3.10 – Rengöringsmetoder för maskinvara

- Innan rengöringsprocessen påbörjas ska du se till att all utrustning är bortkopplad från eluttaget.
- Använd inte slipande produkter.
- Sänk inte ned någon utrustning eller kringutrustning i någon typ av vätska.
- Kassera rengöringsmaterial enligt förordningarna om kassering av farligt avfall.
- Det är inte tillrådligt att använda spraydesinfektionsmedel eftersom ånga kan komma in i utrustningen och orsaka kortslutning eller korrosion.
- Denna produkt är icke-steril

Kapitel 4 Cybersäkerhet och sekretess

Avsnitt 4.1 - Säkerhets- och integritetsrisker

nCommand Lite System implementerar flera tekniska och organisatoriska åtgärder för att skydda bearbetad information.

Systemet har certifierats enligt ISO/IEC 27001 och ISO/IEC 27701 och följer en privacy-by-design-strategi. Stöder efterlevnad av lagar om dataskydd inom hälso- och sjukvården samt cybersäkerhetsbestämmelser som gäller i EU, USA, Storbritannien, Schweiz, Brasilien, Förenade Arabemiraten, Saudiarabien, Australien och Nya Zeeland.

Användarna måste emellertid tillämpa bästa praxis för att förhindra onödig exponering av känsliga uppgifter.

- Undvik att dela personlig eller känslig information om det inte är absolut nödvändigt.
- Se till att kommunikation och systemåtkomst sker i säkra miljöer.
- Informera omedelbart det ansvariga teamet om du misstänker någon skadlig aktivitet.

Avsnitt 4.2 - Skydd av personuppgifter (efterlevnad av GDPR / HIPAA)

nCommand Lite System följer alla tillämpliga integritets- och dataskyddslagar och regler i de regioner där det används, inklusive, men inte begränsat till, GDPR, HIPAA, LGPD och ISO/IEC 27701-krav. All databehandling utförs under rollerna "**Personuppgiftsbiträde**" och "**underordnat personuppgiftsbiträde**" enligt GDPR, med strikt regional datasegregering för att säkerställa efterlevnad och förhindra obehöriga gränsöverskridande dataöverföringar

Vilka uppgifter samlas in?

- **Användare:** Namn, e-postadress och företag (endast för autentisering och åtkomsthantering).
- **Patientdata:** Endast överföringar av medicinska undersökningar via direktsändning i realtid, utan datalagring

Hur används och skyddas data?

- Data används uteslutande för **autentisering, åtkomstkontroll och spårbarhet av sessioner**.
- Informationsöverföring säkras genom **AES-256-kryptering för lagring** och **TLS 1.3 för data i överföring**.
- **Åtkomsten är begränsad** och följer **principen om begränsad behörighet (RBAC)**.
- End-to-end-kryptering säkerställs för P2P-video och kontrollströmmar via WebRTC.
- Auktoriserade molnleverantörer (t.ex. Microsoft Azure) behandlar begränsade data under strikta avtalsmässiga skyddsåtgärder.

Användare beviljas följande rättigheter:

- **Åtkomst till och rättelse** av personuppgifter.
- **Begäran om radering av uppgifter**, i tillämpliga fall.

Om du har frågor kan du skicka ett e-postmeddelande till privacy@ionic.health för komma i kontakt med Ionic Healths dataskyddsombud. Alla förfrågningar hanteras inom 30 dagar, vilket kan förlängas enligt GDPR.

Avsnitt 4.3 - Åtkomsthantering och autentisering

Användarna ansvarar för att definiera **åtkomstroller och behörigheter** för sina team och för att säkerställa regelbundna granskningar och dokumentation av beviljad åtkomst.

Bästa praxis och kontroller

- Följ **principen om begränsad behörighet (RBAC)** och se till att användarna endast har nödvändig åtkomst.
- **Flerfaktorsautentisering (MFA)** är obligatorisk för administrativ åtkomst och rekommenderas för alla användare.
- **Starka lösenord** krävs, med minst **8 tecken, inklusive stora och små bokstäver, siffror och symboler**.
- **Dela inte inloggningsuppgifter**.
- Åtkomstbehörigheter övervakas och granskas med jämna mellanrum.

Övervakning: Åtkomst, ändringar av behörigheter och viktiga aktiviteter dokumenteras i systemets säkerhetsloggar. Loggar sparas i minst 7 år, i enlighet med HIPAA, GDPR och andra tillämpliga bestämmelser. De stöder internrevision, kriminalteknisk analys och lagstadgad rapportering. Loggarna är skyddade mot manipulering och lagras i säkra miljöer med åtkomstkontroll.

Avsnitt 4.4 - Åtkomst till systemkontroller

Systemkontrollen är enbart tillgänglig via **nCommand Lite Web Application** och kräver giltiga inloggningsuppgifter. Åtkomst begränsas till behöriga roller – *Fjärrtekniker, Lokal tekniker, Admin, Rollansvarig* och *Systemkontrollanvändare*.

Rollen systemkontrollanvändare har begränsade behörigheter som endast ger tillgång till diagnostiska funktioner relaterade till nätverksvalidering och verifiering av anslutning. Det säkerställer att obehöriga personer aldrig kommer åt nätverksuppgifter, vitlistningsinformation och systemmätvärden.

Alla åtkomstförfrågningar autentiseras via Azure AD B2C med flerfaktorsautentisering (MFA) och adaptiva villkorsbetingade åtkomstpolicyer som hanteras via Microsoft Entra ID. Lösenordskomplexiteten följer organisationens säkerhetspolicy och kräver minst åtta tecken, inklusive stora och små bokstäver, siffror och symboler. Lösenord går ut var 90:e dag och sessioner loggas automatiskt ut efter 24 timmars inaktivitet, vilket kan förlängas i upp till 90 dagar vid kontinuerlig användning

Avsnitt 4.5 - Regional datasegregering och logglagring

nCommand Lite-plattformen upprätthåller strikt regional segregering av data för att förhindra obehöriga eller onödiga gränsöverskridande överföringar. Miljöerna är isolerade per region, vilket säkerställer efterlevnad av gällande regler.

Alla åtkomstloggar, aktivitetsregister och säkerhetshändelser sparas i minst sju (7) år, i enlighet med tillämpliga dataskydds- och hälsoföreskrifter. Loggar lagras i säkra, åtkomstkontrollerade miljöer och skyddas mot manipulering. Informationen stödjer forensiska undersökningar, efterlevnadsrevisioner och regulatorisk rapportering.

Avsnitt 4.6 - Datasäkerhet och integritet

nCommand Lite System säkerställer uppgifternas konfidentialitet, integritet och tillgänglighet genom säkerhetsrutiner enligt branschstandard.

Användarna bör se till att säkerhetsprotokollen följs, regelbundet se över åtkomstpolicyerna och rapportera eventuella avvikelser. Systemet övervakar kontinuerligt aktiviteter och administratörer måste tillämpa säkerhetspolicyer för att upprätthålla ett robust försvar mot potentiella hot.

Systemet är skyddat av dygnet runt-övervakning via ett dedikerat Security Operations Center (SOC) med SIEM-funktioner för hotdetektering och incidentrespons.

Avsnitt 4.7 - Åtgärder vid säkerhetsincidenter

Systemet innehåller en dokumenterad incidenthanteringsplan, i linje med ISO 27035 och NIST CSF.

I händelse av säkerhetsincidenter, såsom obehörig åtkomst eller systemfel, måste användarna följa dessa steg:

Hur identifieras en incident?

- **Obehörig åtkomst** upptäcks i aktivitetsloggar.
- **Misstänkta inloggningsförsök** eller upprepade autentiseringsfel.
- **Ovanligt systembeteende**, t.ex. oväntade åtgärder eller funktionsstörningar.

Hur rapporterar jag en incident?

Registrera omedelbart händelsen via tillgängliga supportkanaler (kapitel 5).

Om en personuppgiftsincident bekräftas kommer IONIC, som underbiträde, att meddela GE som personuppgiftsbiträde inom 48 timmar och tillhandahålla bevis, information om påverkan samt information om åtgärder. GE ansvarar i sin tur för att meddela den personuppgiftsansvariga (kunden) i enlighet med tillämpliga juridiska och kontraktsmässiga krav.

Kapitel 5 Servicekanaler

Vårt team är redo att hjälpa till oavsett om du behöver hjälp med ett tekniskt problem, ett oklart steg i processen eller ytterligare vägledning. Du kan kontakta oss via telefon, e-post eller ITSM-plattformen, beroende på vilket som passar dig bäst. Våra specialister är utbildade i att erbjuda personlig hjälp, vilket säkerställer att alla problem löses snabbt och effektivt.

Telefonnummer

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

ITSM-plattform

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

E-post

helpdesk@ionic.health



WARNING!

Alla allvarliga tillbud relaterade till användningen av denna enhet ska rapporteras till både tillverkaren och den hälso- och sjukvårdsmyndighet/behörig myndighet där enheten är installerad.

För att rapportera till tillverkaren: kontakta antingen din lokala servicerepresentant eller rapportera till: helpdesk@ionic.health

Ange följande information:

- Systemets versionsnummer, som visas på inloggningsskärmen;
- Datum för tillbudet;
- Beskrivning av tillbudet, inklusive eventuell påverkan/skada hos patient eller användare;
- Dina kontaktuppgifter (inrättning, adress, kontaktnamn, titel och telefonnummer).

Kapitel 6 Juridisk och regulatorisk information

Tillverkare



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

Ansvarig tekniker

Alexandre Seiji Fukuda Ribas
CREA-SP: 5071085437

ANVISA

82585300004

Importör (USA)



nCommand Lite System

IONIC HEALTH USA INC.

11201 Cedar Avenue, STE 600
Cleveland, OH 44106
USA

+1 (216) 242 1223

EU-representant/importör



nCommand Lite



Identifieringsnummer för anmält organ:
2803

EUROPE IONIC HEALTH DIGITAL TECHNOLOGIES, LDA

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

+351 (300) 528 410

Auktoriserad representant i Schweiz (CH-REP) / Importör

nCommand Lite

FREYR LIFE SCIENCES GMBH

Bahnhofplatz
CH-6300 Zug
Switzerland

Ansvarig Person i Storbritannien / Importör

nCommand Lite

FREYR LIFE SCIENCES LTD

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

Sponsor i Australien

nCommand Lite

TAEVAS LIFE SCIENCES PTY LTD

46 Dora St
Blacktown NSW 2148
Australien

Sponsor i Nya Zeeland

nCommand Lite

TAEVAS LIFE SCIENCES LIMITED

Level 3, 1 Margaret Street
Lower Hutt 5010
Nya Zeeland

Grundläggande UDI-DI: 7898974112NCLITE2L**Begäran om papperskopia**

Papperskopior av användarhandboken till nCommand Lite kommer att tillhandahållas på begäran utan extra kostnad. Kontakta din lokala representant och begär en papperskopia av användarhandboken.

Tillverkningsdatum

Datum för programutgivning finns på nCommand Lite-inloggningssidan, i formatet MÅNAD/ÅR.

Kapitel 7 Versionshistorik

Version	Beskrivning av ändringar	Datum
0	Handboken har uppdaterats från 2.3 v1 till 2.4	25 november 2025
1	Etiketter i kapitel 6 har uppdaterats	4 december 2025
2	Kravet på statisk IP-adress har tagits bort från den lokala datorkonfigurationen i underavsnitt 1.3.11 Symbolen för EU:s auktoriserade representant har uppdaterats i underavsnitt 1.3.12 En anmärkning har tagits bort från underpunkt 1.3.14 Innehållet i kapitel 2 har uppdaterats Symbolen för EU:s auktoriserade representant har uppdaterats i kapitel 6	28 januari 2026
3	Översättningen av "Ansvarig tekniker" i kapitel 6 granskades.	9 februari 2026

BILAGA I - Checklista för servicestart

1. Verifiera elektriska anslutningar och nätverksanslutningar:

Se till att de elektriska anslutningarna och nätverkspunkterna är korrekt upprättade i e-KVM-datorn, skannerdatorn och den lokala datorn.

2. Kontrollera strömstatus:

Kontrollera att den avbrottsfria och stabiliserade strömförsörjningen och e-KVM-datorn är påslagna och fungerar korrekt.

3. Snabb åtkomst till nC Lite-plattformen:

Bekräfta att genvägen till nC Lite-plattformen finns på skrivbordet för snabb åtkomst.

4. Åtkomst och inloggning till nC Lite-plattformen:

Öppna nCommand-plattformen och logga in för att säkerställa fullständig åtkomst och korrekt funktion.

5. Installation av chattapplikation:

Öppna chattapplikationen i nC Lite-plattformen i endast en flik och undvik att minimera den för en smidig kommunikation.