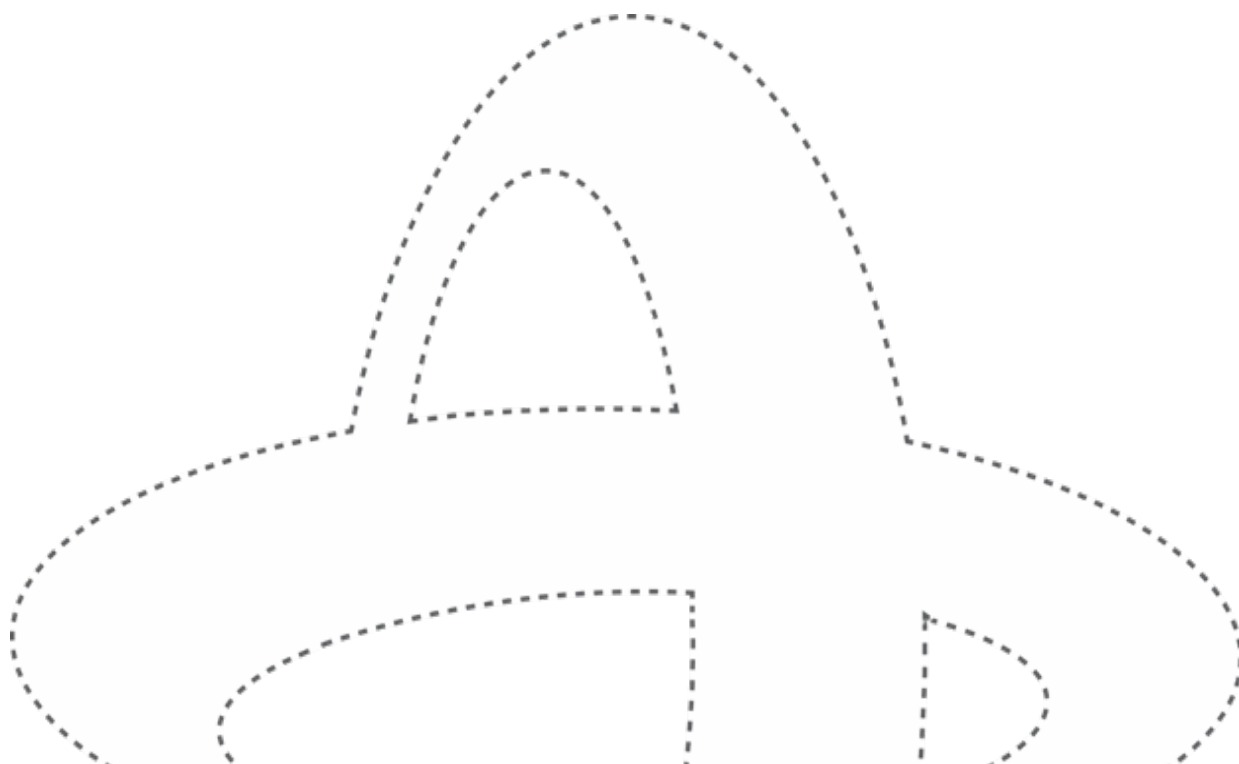




MANUALE D'USO

nCommand Lite v2.4

Versione del manuale: V.3



Indice

Capitolo 1	Introduzione.....	4
Sezione 1.1 -	Finalità.....	4
Sezione 1.2 -	Glossario.....	4
Sezione 1.3 -	Descrizione.....	5
1.3.1.	Uso previsto.....	6
1.3.2.	Indicazioni per l'uso.....	6
1.3.3.	Popolazione di pazienti prevista.....	6
1.3.4.	Ambiente di utilizzo.....	6
1.3.5.	Controindicazioni.....	6
1.3.6.	Funzionalità della piattaforma.....	6
1.3.7.	Benefici clinici.....	7
1.3.8.	Utenti previsti.....	7
1.3.9.	Ambiente operativo.....	8
1.3.10.	Ambiente della struttura.....	8
1.3.11.	Requisiti minimi.....	10
1.3.12.	Simboli.....	11
1.3.13.	Durata di servizio.....	12
1.3.14.	Rinnovo / Aggiornamento.....	12
Capitolo 2	Elenco delle avvertenze e precauzioni generali.....	13
Capitolo 3	Uso della piattaforma in ciascuna posizione.....	16
Sezione 3.1 -	Accesso al sistema nCommand Lite e utilizzo.....	16
Sezione 3.2 -	Primo accesso alla Piattaforma.....	16
3.2.1.	Accedi tramite nCommand Lite.....	17
3.2.2.	Login tramite IdP esterno.....	18
Sezione 3.3 -	Gestione della password.....	19
Sezione 3.4 -	Accesso con profilo Tecnologo locale.....	22
Sezione 3.5 -	Accesso con profilo di tecnologo da remoto.....	25
3.5.1.	Modalità di accesso.....	26
3.5.2.	Barra dello streaming.....	29
3.5.3.	Configurazione a più videocamere.....	32
3.5.4.	Apri un altro dispositivo.....	34
3.5.5.	Controllo sistema.....	36
Sezione 3.6 -	Chat.....	37

Sezione 3.7 -	Chiusura della sessione sulla piattaforma	41
Sezione 3.8 -	Formazione operativa	43
Sezione 3.9 -	Linee guida per la risoluzione dei problemi	44
Sezione 3.10 -	Metodi di pulizia dei componenti hardware	49
Capitolo 4	Sicurezza informatica e riservatezza	50
Sezione 4.1 -	Rischi per la sicurezza e la privacy	50
Sezione 4.2 -	Protezione dei dati personali (conformità GDPR / HIPAA)	50
Sezione 4.3 -	Gestione degli accessi e autenticazione	51
Sezione 4.4 -	Controllo degli accessi a System Check	51
Sezione 4.5 -	Segregazione dei dati regionali e conservazione dei registri	52
Sezione 4.6 -	Sicurezza e integrità dei dati	52
Sezione 4.7 -	Risposta agli incidenti di sicurezza	52
Capitolo 5	Canali di servizio	53
Capitolo 6	Informazioni legali e normative	54
Capitolo 7	Cronologia delle Revisioni	57
APPENDICE I -	Lista di controllo per l'avvio della manutenzione	58

**ATTENZIONE**

In ottemperanza alle leggi federali statunitensi, il presente dispositivo può essere venduto esclusivamente da personale medico o su prescrizione medica, secondo l'uso di un tecnico medico autorizzato nello Stato in cui opera.

(per gli Stati Uniti d'America)

**ATTENZIONE**

In Brasile questo software è autorizzato da Anvisa per essere utilizzato esclusivamente con dispositivi di risonanza magnetica (RM). Qualsiasi altro utilizzo non è consentito.

(per l'uso in Brasile)

**ATTENZIONE**

Prima dell'uso, assicurarsi di essere a conoscenza dei requisiti specifici vigenti nel proprio Paese o nella propria regione. La mancata osservanza delle normative può comportare rischi per la salute.

**ATTENZIONE**

Assicurarsi che la versione di questo manuale utente corrisponda alla versione della piattaforma in uso. L'utilizzo di una versione non corrispondente può causare un funzionamento errato o un'interpretazione errata delle funzionalità.

Capitolo 1 Introduzione

Sezione 1.1 - Finalità

Il presente manuale è stato redatto allo scopo di fornire ai tecnici che operano in locale e da remoto una conoscenza approfondita delle funzionalità specifiche del sistema nCommand Lite. Il documento, che costituisce il manuale d'uso, fornisce informazioni pratiche e concise, guidando l'utente attraverso le funzionalità del sistema e la procedura di risoluzione dei problemi. Attenendosi a quanto riportato nel presente manuale, l'utente potrà utilizzare il sistema nCommand Lite in modo efficiente, massimizzando la produttività e diminuendo la necessità di ricorrere a interventi di assistenza tecnica.

Sezione 1.2 - Glossario

**ATTENZIONE**

Questa etichetta si applica a condizioni o azioni potenzialmente pericolose. In caso di mancata osservanza delle istruzioni ivi riportate, vi è il rischio di causare lesioni personali o danni a cose di lieve entità.

**AVVERTENZA**

Questa etichetta identifica condizioni o azioni che comportano un pericolo specifico. In caso di mancata osservanza delle istruzioni ivi riportate, vi è il rischio di causare lesioni personali gravi o danni a cose di grande entità.

Termine usato sulla piattaforma	Termine corrispondente
Struttura di imaging	Struttura medica, Unità, Unità mobili, Struttura sanitaria, Unità sanitaria
Struttura da remoto	Postazione di lavoro remota, luogo remoto, ufficio remoto, posizione remota, centro di comando
Piattaforma	Applicazione web di nCommand Lite
Sistema	nCommand Lite con tutti i sottosistemi
Dispositivo	Scanner medico, Scanner, Attrezzatura, Dispositivo medico, Dispositivo di imaging, Attrezzatura di imaging
Tecnologo locale	Utente locale, Tecnico locale, Professionista sanitario locale (LHP), Utente in loco

Sezione 1.3 - Descrizione

Il sistema nCommand Lite è un dispositivo SaMD (“Software as a Medical Device”) orientato al cliente che consente di effettuare l’accesso da remoto tramite un’applicazione web ai fini della visualizzazione/consultazione delle immagini. Fornisce inoltre la possibilità di offrire da remoto una guida in tempo reale al tecnico autorizzato vicino al paziente (utente in locale) che opera i dispositivi di imaging medico nel contesto della formazione o della valutazione della procedura, per gli scanner RM, TC e PET/TC.

Gli utenti da remoto sono tecnici autorizzati che possono accedere a un dispositivo medico di diagnostica per immagini da qualsiasi computer che soddisfi le specifiche minime richieste, ovunque si trovino, utilizzando una connessione software sicura che trasmette video e offre l’accesso tramite tastiera e mouse. Questo sistema consente agli utenti da remoto di assistere gli utenti in locale indipendentemente dalla distanza che li separa. Questo tipo di accesso deve essere concesso dall’utente in locale che utilizza il sistema. Questo stesso utente ha anche facoltà di revocarlo in qualsiasi momento allo scopo di mantenere il pieno controllo della sessione in maniera continuativa. Ciascuna sessione remota viene inoltre controllata tramite credenziali protette gestite sempre dall’utente in locale. Le connessioni a un dispositivo medico sono limitate a una sessione da remoto alla volta, allo scopo di garantire un controllo rigoroso sulle parti che interagiscono da remoto con il sistema. Le immagini esaminate da remoto non sono destinate all’uso diagnostico.

Il sistema nCommand Lite è costituito da un componente hardware informatico e da una soluzione di installazione software che supporta più sessioni, consentendo ai tecnici da remoto di accedere a più dispositivi medici di diagnostica per immagini secondo necessità. Gli scanner compatibili con il sistema nCommand Lite sono conformi a un protocollo comune, che consente la gestione dei parametri di scansione e la scansione da remoto.

1.3.1. Uso previsto

Il sistema nCommand Lite consente di effettuare l'accesso da remoto finalizzato alla visualizzazione/consultazione delle immagini, oltre a offrire al tecnico autorizzato che utilizza lo scanner una funzione di guida da remoto in tempo reale. Questo strumento comprende opzioni di formazione, valutazione della procedura e gestione dei parametri di scansione.

1.3.2. Indicazioni per l'uso

Il sistema nCommand Lite consente di effettuare l'accesso da remoto finalizzato alla visualizzazione/consultazione delle immagini, oltre a offrire al tecnico autorizzato, che utilizza uno scanner compatibile per RM, TC o PET/TC, una funzione di guida da remoto in tempo reale. L'accesso deve essere concesso dal tecnico autorizzato in locale che utilizza il sistema. L'accesso da remoto è disponibile solo per i sistemi che supportano la funzionalità di connettività da remoto. Le immagini esaminate da remoto non sono destinate all'uso diagnostico.

1.3.3. Popolazione di pazienti prevista

Qualsiasi paziente a cui sia stato prescritto di sottoporsi a un esame di diagnostica per immagini tramite un dispositivo medico di diagnostica per immagini collegato.

1.3.4. Ambiente di utilizzo

Strutture di diagnostica per immagini che eseguono esami di risonanza magnetica per immagini (RM), tomografia computerizzata (TC) e tomografia a emissione di positroni/tomografia computerizzata (PET/TC) e centri di comando da remoto.

1.3.5. Controindicazioni

La piattaforma non deve essere utilizzata da utenti che non sono tecnici autorizzati e che non hanno ricevuto alcun tipo di formazione sull'uso del sistema nCommand Lite.

1.3.6. Funzionalità della piattaforma

- **Scansione da remoto:** consente di visualizzare la schermata del dispositivo medico di diagnostica per immagini in tempo reale, offrendo a un tecnico autorizzato la possibilità di assistere a un esame da remoto.
- **Chat:** rende possibile la comunicazione tra tecnici autorizzati da remoto e tecnici autorizzati in locale tramite messaggi vocali e di testo. I tecnici locali e i tecnici da remoto possono anche effettuare e ricevere chiamate vocali e videochiamate.
- **Configurazione a più videocamere:** questa funzione agevola l'osservazione da remoto dei pazienti e della struttura sanitaria durante la procedura. Il tecnologo da remoto può accedere alla visualizzazione delle videocamere attraverso le schede, che sono suddivise in due gruppi: tutte le schede della videocamera e schede singole. Questo meccanismo replica la supervisione visiva che l'operatore sanitario avrebbe se si trovasse vicino al paziente, introducendo così un livello di sicurezza aumentato.
- **La scansione da remoto multisessione** consente al tecnologo da remoto di accedere a più dispositivi medici di diagnostica per immagini secondo necessità.
- **Modalità di accesso:** consente al tecnologo da remoto di scegliere tra visualizzazioni e controllo del dispositivo. In modalità "View" (Visualizzazione) i tecnologi da remoto possono visualizzare solo i contenuti in streaming. In modalità "Control" (Controllo) il paziente ha il controllo del mouse e della tastiera.

- **Gestione dell'accesso da parte del Tecnologo da remoto:** consente al Tecnologo locale di controllare l'accesso del Tecnologo da remoto e la relativa modalità di accesso ("View" [Visualizzazione] o "Control" [Controllo]). Per consentire al tecnologo da remoto di effettuare la connessione, il tecnologo locale che utilizza la piattaforma deve concedere l'accesso. Questo stesso tecnico ha anche facoltà di revocarlo in qualsiasi momento, allo scopo di mantenere il pieno controllo della sessione in maniera continuativa.
- **Dimensione dello streaming:** il tecnologo da remoto può visualizzare la dimensione (espressa in pixel) dello streaming originale e dello streaming in corso. Il tecnico viene inoltre avvisato quando la dimensione dello streaming in corso è inferiore a quella originale.
- **Stato del mouse e della tastiera:** il tecnologo da remoto riceve un feedback se il mouse e la tastiera del dispositivo medico di diagnostica per immagini funzionano correttamente.
- **Dettagli della sessione:** i tecnologi locali e i tecnologi da remoto possono accedere ai dettagli della sessione.

1.3.7. Benefici clinici

Lo strumento **nCommand Lite** migliora la diagnostica per immagini rendendo possibile il funzionamento da remoto dei sistemi **RM, TC e PET-TC** e garantendo costantemente la qualità delle immagini e la conformità ai protocolli. Consente a tecnici esperti di supervisionare e prestare assistenza nello svolgimento di esami in tempo reale, ottimizzando l'efficienza del flusso di lavoro e riducendo gli errori che potrebbero interferire con l'accuratezza diagnostica. Il sistema agevola la collaborazione tra i tecnici, aumentando la coerenza degli esami e accelerando il processo decisionale nei casi complessi. Consentendo ai professionisti che operano da remoto di supportare più strutture, il sistema **nCommand Lite** aumenta **la disponibilità, la varietà e la qualità** degli esami di diagnostica per immagini, assicurando l'accesso a dispositivi di diagnostica avanzata a un maggior numero di pazienti e ottimizzando nel contempo le risorse sanitarie. Questo strumento contribuisce inoltre a mitigare le carenze di personale riducendo la dipendenza da specialisti in loco e preservando nel contempo la conformità a rigorosi standard normativi e di sicurezza dei dati.

1.3.8. Utenti previsti

- **Tecnologo locale**
Il tecnologo locale è l'utente che opera in loco, responsabile di assistere e guidare i pazienti di persona presso la struttura sanitaria. Deve avere le conoscenze necessarie a eseguire le procedure di scansione per un determinato dispositivo di diagnostica per immagini. Controlla inoltre la modalità di accesso del tecnologo da remoto (View [Visualizzazione] o Control [Controllo]). L'accesso da remoto deve essere concesso dal tecnologo locale tramite la piattaforma e può essere revocato in qualsiasi momento.
- **Tecnologo da remoto**
Professionista che esegue le operazioni da remoto attraverso l'accesso al computer del dispositivo e il controllo dello stesso. Similmente al tecnologo locale, anche il tecnologo da remoto deve possedere le conoscenze necessarie a eseguire le procedure di scansione per un determinato dispositivo di diagnostica per immagini.
- **Utente addetto all'assistenza/Utente di sistemi informatici**
Professionista responsabile della configurazione della piattaforma (non inclusa nel presente Manuale d'uso).

1.3.9. Ambiente operativo

Le seguenti specifiche fanno riferimento ai requisiti ambientali del computer e-KVM.

- **Altitudine massima (senza pressurizzazione)**
 - In servizio: Da 0 m (0 piedi) a 3048 m (10.000 piedi)
 - Archiviazione: Da 0 m (0 piedi) a 12192 m (40.000 piedi)
- **Temperatura**
 - In servizio: Da 10°C (50°F) a 35°C (95°F)
 - Archiviazione: Da -10°C (14°F) a 50°C (122°F)
- **Umidità relativa**
 - In servizio: 20%-80% (senza condensa)
 - Archiviazione: 10%-90% (senza condensa)

1.3.10. Ambiente della struttura

La piattaforma nCommand Lite prevede due diversi tipi di posizioni di utilizzo:

- **Struttura di Imaging:** Strutture che eseguono esami di risonanza magnetica per immagini (RM), tomografia computerizzata (TC) o tomografia a emissione di positroni/tomografia computerizzata (PET/TC).
- **Struttura da remoto:** Una posizione in cui i tecnici remoti possono accedere e gestire da remoto i dispositivi (scanner MRI, TC o PET/TC). Questa postazione di lavoro può essere utilizzata in vari ambienti, come uffici, centri di comando, sedi remote o persino sedi secondarie all'interno della struttura sanitaria. La postazione di lavoro remota può essere collocata in qualsiasi spazio che fornisca all'utente le condizioni appropriate per la concentrazione, la connettività minima e i requisiti di configurazione del computer.

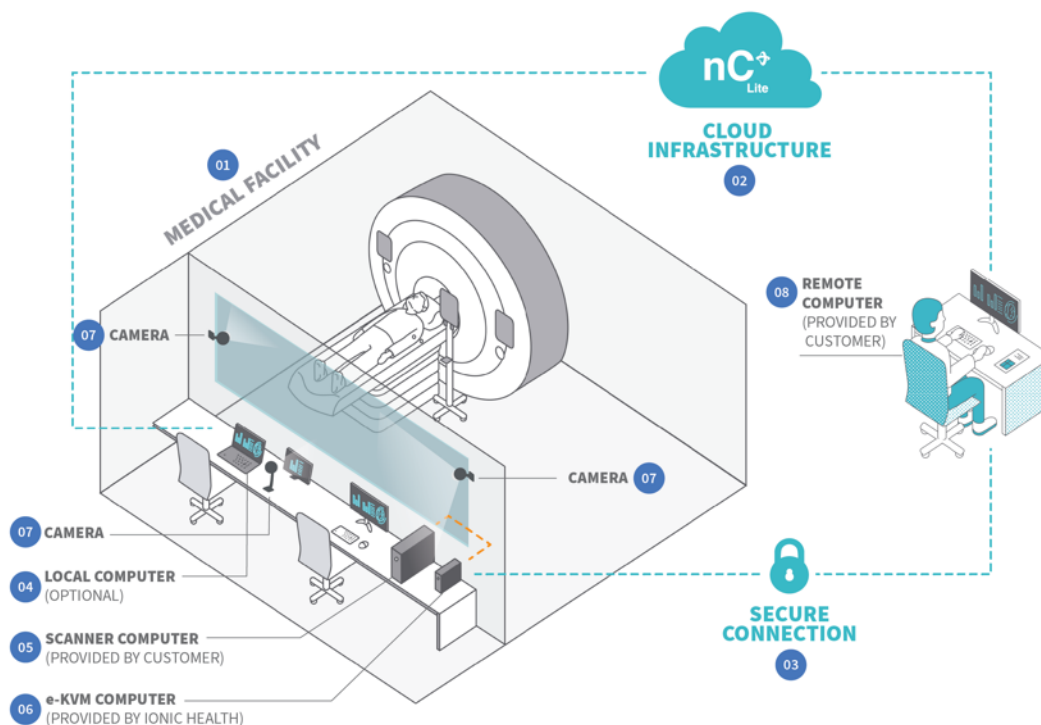


Figura 01: Panoramica del prodotto e delle sue connessioni tramite una connessione sicura (ad esempio VPN).

01 – Struttura medica; **02** – Infrastruttura cloud; **03** – Connessione sicura; **04** – Computer locale (Opzionale);
05 – Computer scanner (fornito dal cliente); **06** – e-KVM (Fornito da IONIC Health);
07 – Fotocamera; **08** - Computer remoto (fornito dal cliente))



AVVERTENZA!

Compatibilità con la scansione remota

IONIC Health (IH) convalida la funzionalità di scansione remota sui dispositivi compatibili elencati. IH esegue una valutazione completa dei requisiti di scansione remota IH e testa il sistema nell'ambiente di destinazione durante l'installazione. Ciò garantisce la compatibilità e le prestazioni adeguate in quel momento per la scansione remota. Questa verifica non implica che tutti i requisiti del dispositivo OEM (Original Equipment Manufacturer) siano soddisfatti in questa configurazione. Qualsiasi deviazione dai requisiti OEM è responsabilità dell'utente finale.

Eventuali modifiche al sistema o all'ambiente apportate dopo l'installazione devono essere segnalate a IH per verificarne la compatibilità continua. IH non può garantire le prestazioni né assumersi la responsabilità per configurazioni diverse da quelle convalidate durante l'installazione.

1.3.11. Requisiti minimi

- **Computer locale**

Questo computer viene utilizzato dal **Tecnologo locale** per autorizzare e supportare l'accesso remoto del dispositivo tramite nCommand Lite®. Consente inoltre la comunicazione diretta con il **Tecnologo da remoto** tramite la funzione chat sulla piattaforma.

Le specifiche tecniche minime richieste sono:

- Processore: AMD® A4-9120C o superiore, oppure simile
- Memoria: 4 GB o superiore
- Archiviazione: SSD 128 GB o superiore
- Periferiche: microfono e altoparlante, oppure cuffie e webcam
- Monitor: 14" FHD (1920 x 1080) o superiore
- Sistema operativo: Chrome OS, Windows OS o MAC OS
- Luogo di installazione: questo computer deve essere vicino al computer scanner
- Routine IT: Crea il collegamento nCommand Lite nel desktop di ogni utente
- Compatibilità con il browser: Google Chrome o Microsoft Edge.

- **Workstation remota**

Questa stazione viene utilizzata dal **tecnologo da remoto** per accedere e controllare il dispositivo tramite nCommand Lite®. La stazione di lavoro remota deve stabilire una connessione sicura al computer e-KVM (fornito da IONIC HEALTH®).

Il cliente è responsabile della fornitura del computer remoto e deciderà in base a uno dei due scenari: il primo è un'operazione 24 ore su 24, 7 giorni su 7 e il secondo è un'operazione durante l'orario di ufficio.

Per ogni scenario troverai di seguito le specifiche corrette per la scelta dei modelli di computer:

Scenario 1 (24x7 Operazione) - Deve soddisfare le seguenti specifiche:

- Intel Xeon W-2223 (4 core, 8 thread, 8,25 MB di cache, 3,90 GHz Turbo) o superiore.
- RAM: 16 GB o superiore.
- Scheda grafica: NVIDIA RTX A2000 6GB o superiore o simile.
- Archiviazione: SSD 128 GB o superiore.
- Sistema operativo: Windows 11 Pro 64B o versioni successive.
- Requisiti minimi per il monitor: Dimensioni 27", proporzioni 16:9, risoluzione 4k.
- Auricolari: BLACKWIRE 3200 o similari.
- Compatibilità con il browser: Google Chrome o Microsoft Edge.

Scenario 2 (Operazione orario lavorativo) - Deve soddisfare le seguenti specifiche:

- Intel® Core™ i7-12700k vPro® o superiore.
- RAM: 16 GB o superiore.
- Scheda grafica: NVIDIA T400 GB o superiore o simile.
- Archiviazione: SSD 128 GB o superiore.
- Sistema operativo: Windows 11 Pro 64B o versioni successive.
- Requisiti minimi per il monitor: Dimensioni 27", proporzioni 16:9, risoluzione 4k.
- Auricolari: BLACKWIRE 3200 o similari.
- Compatibilità con il browser: Google Chrome o Microsoft Edge.

**AVVERTENZA!**

Il mancato rispetto della configurazione appropriata e dei requisiti minimi potrebbe causare problemi o interruzioni della comunicazione tra gli utenti.

- **Configurazioni di rete (requisiti minimi)**

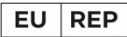
Per stabilire la sessione tra l'utente remoto e il computer e-KVM, è necessario garantire la comunicazione di rete tra i due dispositivi. Il sistema nCommand Lite utilizza il peer-to-peer (P2P) per stabilire la connessione tra utente locale, utente remoto e computer e- KVM. Esistono tre scenari compatibili:

- **Scenario 1** – Rete aziendale che utilizza uno dei seguenti protocolli: LAN, LAN-to-LAN, MPLS o VPN;
- **Scenario 2** – Rete aziendale che si affida a una rete WAN (esterna) fidata e non utilizza nessuno dei seguenti protocolli: LAN, LAN-to-LAN, MPLS o VPN;
- **Scenario 3** – rete pubblica dal lato del computer remoto (utente remoto).

Le configurazioni per ogni scenario sono descritte in dettaglio nella documentazione tecnica.

1.3.12. Simboli

Simbolo	Descrizione	Riferimento
	Produttore	ISO 15223-1, ISO 7000-3082
	Data di produzione	ISO 15223-1, ISO 7000-2497
	Il simbolo indica che questo prodotto è un dispositivo medico	ISO 15223-1
	Identificativo univoco del dispositivo	ISO 15223-1
	Riferimento del modello	ISO 15223-1, ISO 7000-2493
	Importatore	ISO 15223-1, ISO 7000-3725
	Consultare il Manuale d'uso	ISO 15223-1, ISO 7000-1641
	Distributore	ISO 15223-1, ISO 7000-3724
	Attenzione	ISO 15223-1, ISO 7000-0434A
	Avvertenza	ISO 7010-W001

	Numero di serie (o versione del software)	ISO 15223-1, ISO 7000-2498
	Rappresentante autorizzato nella Comunità europea	ISO 15223-1
	Rappresentante autorizzato in Svizzera (CH-REP)	ISO 15223-1
	CE – Marchio di conformità europea; 2803 – Designazione dell'organismo notificato	Regolamento UE 2017/745

1.3.13. Durata di servizio

La durata prevista del prodotto è di 5 anni, considerando la vita utile dei componenti che compongono il prodotto. Questa valutazione globale garantisce che la durata di ciascun componente fondamentale sia in linea con la durata complessiva, assicurando prestazioni e affidabilità costanti per l'intera durata prevista del prodotto.

1.3.14. Rinnovo / Aggiornamento

IONIC Health aggiornerà il sistema nCommand Lite come parte di una manutenzione pianificata o di rilasci di aggiornamento. Questi aggiornamenti sono progettati per garantire prestazioni e affidabilità costanti senza interrompere la versione attualmente distribuita presso le sedi dei clienti. A seconda della natura dell'aggiornamento, il prodotto potrebbe essere aggiornato da remoto oppure potrebbe richiedere una visita in loco da parte di un tecnico sul campo.

Capitolo 2 Elenco delle avvertenze e precauzioni generali



AVVERTENZA!

Leggere tutte le avvertenze riportate di seguito prima di utilizzare il sistema nCommand Lite.



ATTENZIONE

Il sistema nCommand Lite non può essere sottoposto a riparazione o manutenzione durante l'utilizzo per controllare un'apparecchiatura MRI, TC o PET-CT in presenza di un paziente.

- Prestare particolare attenzione a tutti gli allarmi di sistema, in quanto sono fondamentali ai fini di un funzionamento sicuro.
- Dare priorità alla sicurezza e all'attenzione durante tutte le operazioni.
- In ottemperanza alle leggi federali statunitensi, questo dispositivo può essere venduto esclusivamente da personale medico o su prescrizione medica, secondo l'utilizzo da parte di tecnici medici autorizzati nello Stato in cui operano.
- Il sistema nCommand Lite deve essere utilizzato solo da tecnici che abbiano ricevuto una formazione adeguata sull'uso della piattaforma.
- Utilizzare questo sistema solo con browser Web compatibili. I browser supportati sono Google Chrome e Microsoft Edge.
- In caso di necessità, un tecnico qualificato e autorizzato deve rimanere nella struttura di imaging per eseguire l'operazione di RM, TC o PET/TC senza il sistema nCommand Lite.
- L'accesso simultaneo a più dispositivi richiede la dovuta concentrazione e una comunicazione efficace con i team che operano in locale.
- Evitare di accedere contemporaneamente a dispositivi con layout o esami identici della stessa regione anatomica.
- È possibile visualizzare più schermate, ma il controllo è limitato a un dispositivo alla volta.
- Ai fini di una comunicazione efficace, avviare sempre una chat in caso di connessione a un dispositivo.
- Gli avvisi di chiamata vengono visualizzati sullo schermo del dispositivo associato; è possibile attivare una sola chiamata alla volta.
- Verificare la comunicazione video quando si accede all'applicazione (prima dell'inizio di una sessione di lavoro) per escludere eventuali guasti della connessione dell'uscita video dei dispositivi RM, TC o PET/TC o di qualsiasi dispositivo correlato allo streaming video.
- Il dispositivo non deve essere collegato alla presa e/o all'alimentazione elettrica ininterrotta e stabilizzata tramite prolunghe o multiprese.
- Se si verificano errori video, controllare la connessione video tra il sistema del dispositivo e il computer e-KVM.
- Se l'accesso da remoto all'applicazione è lento, aggiorna la pagina con il comando Ctrl+F5 nel browser del computer del tecnologo da remoto. Se il problema persiste, contattare l'assistenza tecnica.
- Ogni volta che la pagina del browser viene aggiornata, la connessione al dispositivo viene interrotta e il processo di approvazione deve essere eseguito nuovamente.

- Se è già stato effettuato l'accesso, non accedere con un browser diverso.
- La struttura di Imaging del cliente deve disporre di un collegamento Internet ridondante con un fornitore diverso da quello principale per consentire un cambio immediato in caso di perdita della comunicazione sistema/piattaforma.
- In caso di perdita di comunicazione o di rallentamento del mouse, eseguire una "risincronizzazione del mouse" nella pagina utilizzata nel browser.
- Assicurarsi che i computer utilizzati per il controllo del sistema nCommand Lite, sia nella struttura di imaging sia nel Centro di comando, soddisfino i requisiti minimi; in caso contrario, l'applicazione potrebbe subire un calo in termini di prestazioni.
- La qualità del servizio (Quality of Service, QoS) deve essere applicata al collegamento principale e al collegamento ridondante ai fini della trasmissione della piattaforma e le prestazioni del collegamento devono essere monitorate.
- Prima dell'uso, controllare i livelli di volume dell'audio e del microfono, nonché l'autorizzazione all'utilizzo dell'audio e del microfono nel browser web.
- Prima dell'uso, verificare il funzionamento della tastiera e del mouse. In caso di eccessiva lentezza o di mancata sincronizzazione, attivare il pulsante "mouse resync" (Risincronizzazione mouse). Controllare se il computer e-KVM è collegato e acceso.
- Assicurarsi che il layout della tastiera presso la struttura remota sia identico a quello della tastiera nella struttura di imaging.
- Se è necessario modificare il luogo di utilizzo della piattaforma, il cliente deve contattare l'assistenza tecnica per provvedere a una nuova installazione. Non eseguire la reinstallazione senza aver contattato l'assistenza tecnica.
- Prima di avviare il processo di accesso da remoto del dispositivo RM, TC o PET/TC, è importante che i team di tecnici controllino tutti gli elementi necessari per il corretto funzionamento della piattaforma, in modo da non ostacolare l'esame. Queste voci sono elencate nel documento "Lista di controllo per l'avvio della manutenzione".
- La configurazione del firewall della struttura di diagnostica per immagini deve essere verificata mensilmente con il team del reparto informatico, allo scopo di escludere la presenza di problemi relativi alla versione del firewall che potrebbero compromettere l'uso del sistema nCommand Lite.
- Qualsiasi anomalia osservata durante l'uso dell'applicazione deve essere immediatamente segnalata al team addetto all'assistenza prima di avviare la procedura di accesso o di interromperla se già avviata.
- L'applicazione deve essere utilizzata esclusivamente da tecnici autorizzati addestrati all'uso del sistema nCommand Lite.
- L'accesso da remoto tramite la piattaforma non sostituisce né compete con altre procedure operative per RM, TC o PET/TC stabilite dal fabbricante del dispositivo medico e dai protocolli e procedure della struttura sanitaria.
- Evitare di piegare o allungare i cavi dei componenti hardware.
- Se si verificano problemi con la comunicazione vocale o tramite chat, utilizzare la funzione di telefonata per stabilire la comunicazione tra il tecnologo locale della struttura di imaging e il tecnologo da remoto del Centro di comando. Attenersi alle istruzioni descritte nella sezione "Linee guida in caso di guasto" e, se necessario, contattare l'assistenza tecnica per la riparazione.
- Se è necessario sostituire un computer o qualsiasi altra apparecchiatura che influisca direttamente sull'installazione di nCommand Lite, attivare l'assistenza tecnica, garantendo la conservazione del funzionamento del sistema.
- Solo una persona alla volta può accedere da remoto al dispositivo RM, TC o PET/TC.
- Non toccare alcun cavo video fisico mentre il computer del dispositivo e il sistema nCommand Lite sono accesi.

- Quando si accede a un dispositivo aggiuntivo, si apre una nuova scheda. Trascinare questa scheda su un secondo monitor poiché il sistema è progettato per essere utilizzato con uno schermo separato per ciascun dispositivo.
- Qualsiasi incidente grave correlato all'uso di questo dispositivo deve essere segnalato sia al produttore sia all'autorità sanitaria/autorità competente presso cui è installato il dispositivo (*per ulteriori dettagli, consultare il capitolo "Canali di servizio"*).

Capitolo 3 Uso della piattaforma in ciascuna posizione

Sezione 3.1 - Accesso al sistema nCommand Lite e utilizzo

**AVVERTENZA!**

In caso di problemi, contattare l'assistenza tecnica.

**AVVERTENZA!**

Controllare il layout della tastiera e assicurarsi che sia identico in entrambe le posizioni (struttura sanitaria e struttura da remoto). Eventuali discrepanze tra i layout potrebbero compromettere l'esperienza dell'utente.

In questo capitolo troverai tutto ciò che devi sapere per accedere e iniziare a utilizzare la piattaforma nCommand Lite. Troverai istruzioni semplici e dettagliate per effettuare l'accesso, navigare nell'interfaccia e comprendere le funzionalità principali. Che tu stia lavorando in sede o da remoto, questa guida ti aiuterà a iniziare in modo rapido e sicuro.

Modifica della lingua: il sistema compare in lingua inglese come impostazione predefinita, ma offre anche la possibilità di modificare facilmente questo parametro in base alle specifiche preferenze dell'utente. Nella schermata di accesso, fai clic sull'angolo in alto a destra in cui viene visualizzata la dicitura "English (en-US)" (Inglese, us-US). Si aprirà un elenco a discesa delle lingue disponibili tra le quali poter scegliere.

Una volta effettuato l'accesso, è anche possibile modificare la lingua facendo clic sulla lingua selezionata sul lato destro della barra superiore. Si aprirà un elenco a discesa delle lingue disponibili tra le quali poter scegliere.

Si noti che, se si cambia la lingua mentre si è connessi a un dispositivo, la connessione attuale verrà automaticamente interrotta e sarà necessario riconnettersi.

Quando accedi alla piattaforma, puoi scegliere la lingua preferita nella schermata di accesso. Tuttavia, alcuni messaggi visualizzati durante la procedura di accesso potrebbero apparire nella lingua impostata nel browser web, indipendentemente dalla lingua selezionata sulla piattaforma. Per un'esperienza coerente, ti consigliamo di allineare le impostazioni della lingua del tuo browser con la lingua della tua piattaforma preferita.

Sezione 3.2 - Primo accesso alla Piattaforma

Il processo di accesso alla piattaforma può essere effettuato in due modi: tramite nCommand Lite o tramite un provider di identità esterno (External IdP). L'utente può effettuare l'accesso utilizzando uno dei metodi preconfigurati. Se il metodo configurato è l'External Identity Provider (External IdP), il metodo nCommand Lite non funzionerà e viceversa. Per accedere tramite IdP esterno, andare direttamente a **sottovoce 3.2.2.**

3.2.1. Accedi tramite nCommand Lite

Nota: Questa sezione non riguarda gli utenti che accedono tramite un provider di identità esterno (IdP esterno).

Accendere il computer e fare doppio clic sull'icona di scelta rapida del sistema nCommand Lite, solitamente presente sul desktop. È inoltre possibile accedere all'URL direttamente nel browser.

Il primo accesso è un passaggio fondamentale per iniziare a utilizzare la piattaforma in modo sicuro ed efficiente. Ecco cosa devi sapere:

1 - Email di benvenuto: Riceverai un'e-mail con i tuoi dati di accesso, inclusa la tua e-mail personale associata, una password temporanea e un collegamento diretto alla piattaforma client. Questa email è fondamentale per avviare la navigazione sul sistema nCommand Lite.

2 - Creazione della password: Dopo aver effettuato l'accesso al link, sarà necessario inserire l'indirizzo e-mail associato e la password ricevuta nell'e-mail di benvenuto. Facendo clic su "Sign in" (Accedi), l'utente verrà indirizzato alla pagina di impostazione di una nuova password. Sarà quindi necessario inserire la password precedente, la nuova password e la conferma della nuova password. Deve essere complessa e sicura, includendo almeno 3 dei seguenti elementi: una lettera minuscola, una lettera maiuscola, un numero e un simbolo, e avere una lunghezza minima di 8 caratteri. Facendo clic su "Continue" (Continua), l'utente verrà reindirizzato a una pagina per confermare nuovamente l'indirizzo e-mail. Facendo clic su "Continue" (Continua), l'utente verrà reindirizzato alla schermata iniziale, personalizzata in base al profilo specifico.

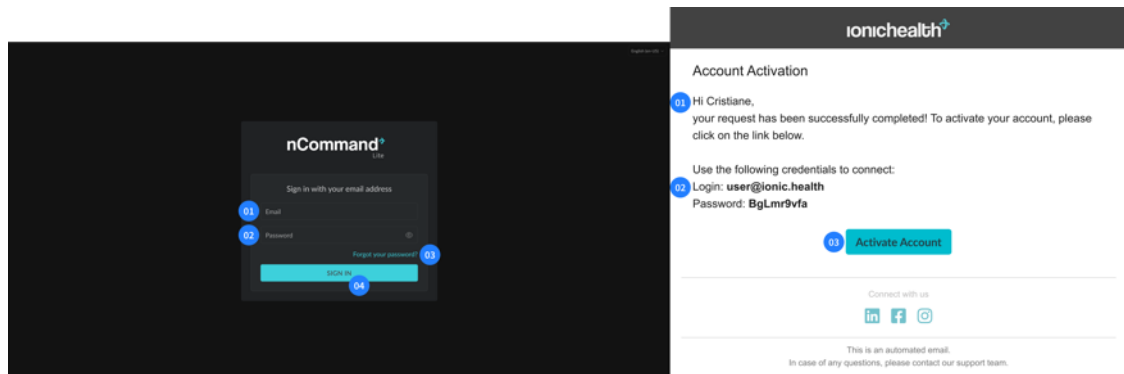


Figura 02: Primo Accesso

Sinistra - Pagina di accesso: 01 – Indirizzo e-mail; 02 – Password; 03 – “Hai dimenticato la password?”; 04 – Pulsante “Accedi”

Destra - Email di benvenuto: 01 – Testo dell'e-mail di attivazione dell'account; 02 – Credenziali di accesso; 03 – Pulsante “Attiva account”

Questa procedura è stata concepita allo scopo di garantire la massima sicurezza dell'account sin dai primi passaggi. Dal secondo accesso in poi, la procedura sarà semplificata ma altrettanto sicura, con un codice di autenticazione a due fattori inviato all'e-mail associata a ogni accesso per garantire la continua sicurezza del tuo account.

Dopo aver effettuato l'accesso a nCommand Lite, il sistema ti indirizzerà automaticamente alla schermata iniziale, personalizzata in base al tuo profilo specifico. Che si tratti di un tecnologo locale o di un tecnologo da remoto, l'interfaccia è stata progettata allo scopo di soddisfare le

esigenze in termini di utilizzo e di accesso in base al ruolo. Questa configurazione intuitiva garantisce la disponibilità di tutti gli strumenti e le informazioni necessari ai fini di un'esperienza utente efficace ed efficiente sin dal momento dell'accesso.

Nota: Quando il metodo di accesso è configurato come nCommand Lite, l'accesso deve sempre essere effettuato tramite questa opzione. Anche se nella schermata di accesso viene visualizzato un pulsante IdP esterno, tale pulsante non sarà operativo per questi utenti. Ogni account utente è registrato sulla piattaforma con un metodo di autenticazione specifico — o credenziali nCommand Lite o un servizio IdP esterno. Se un utente tenta di accedere utilizzando un metodo diverso da quello assegnato al proprio account, il sistema visualizzerà un messaggio di errore che indica che l'account non è autorizzato per quel tipo di autenticazione.

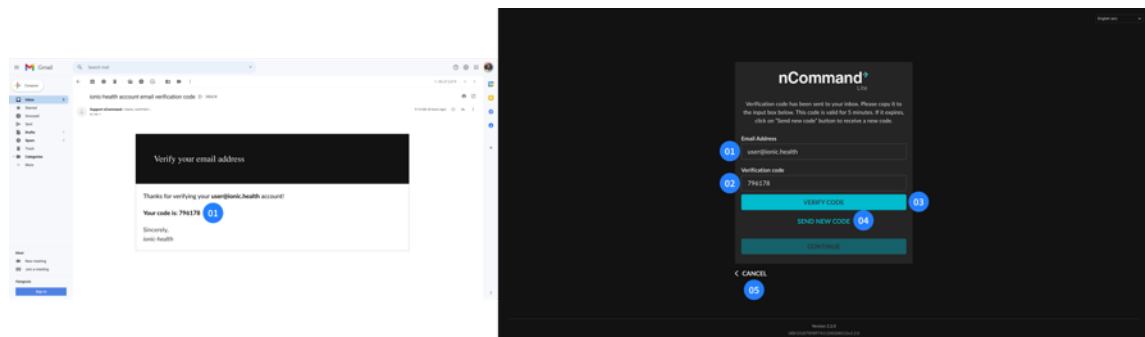


Figura 03: Autenticazione a due fattori (2-FA)

Sinistra – Email: 01 – 2-FA Codice

Destra - Pagina di autenticazione a due fattori: **01** – Indirizzo e-mail; **02** – Codice di verifica; **03** – Pulsante di verifica conferma; **04** – Invia nuovo codice; **05** – Annulla

3.2.2. Login tramite IdP esterno

In alcuni casi, gli utenti possono accedere alla piattaforma tramite un provider di identità esterno (IdP), che consente loro di utilizzare il servizio di autenticazione esistente della propria organizzazione, un meccanismo noto anche come Single Sign On (SSO). Con questo metodo l'utente preregistrato non riceverà alcuna email di benvenuto. Il servizio IT locale deve verificare la compatibilità, configurare il metodo e comunicare all'utente quale indirizzo email (IdP esterno) deve essere utilizzato.

Quando questa opzione è disponibile, l'utente deve sempre effettuare l'accesso utilizzando l'IdP esterno (ad esempio, Amazon Cognito, Microsoft Entra ID, Microsoft AD B2C). Il metodo di accesso tramite nCommand Lite non sarà disponibile per gli utenti IdP esterni.

Per accedere tramite l'IdP esterno, fare clic sul pulsante con il nome dell'IdP e seguire le istruzioni fornite dall'autenticatore esterno. Se il tuo istituto ha più di un IdP esterno integrato, assicurati di confermare con quale provider sei registrato. Altri provider non funzioneranno. In caso di domande o difficoltà, contattare il servizio IT locale.

Negli scenari in cui gli utenti condividono lo stesso computer e utilizzano Single Sign-On (SSO), si consiglia che ogni utente selezioni l'opzione "non rimanere connesso" durante l'accesso all'IdP esterno (se disponibile) o che si disconnetta dal provider esterno dopo aver effettuato la disconnessione da nCommand Lite.

Per questa opzione di accesso, l'intero processo di accesso e disconnessione, inclusi i criteri di creazione e scadenza delle password, l'autenticazione a più fattori (MFA) e i blocchi degli account, è gestito interamente dal team IT del cliente che ha configurato l'IdP esterno.

Quando si effettua l'accesso tramite IdP esterno, le funzioni "Password dimenticata" e "Modifica password" devono essere eseguite secondo la procedura dell'IdP esterno.

Nota: L'opzione "Password dimenticata" continuerà a comparire nella schermata di accesso, ma non sarà operativa per questi utenti. Potrebbe indirizzare verso le fasi successive del processo, ma non lo completerà. Se hai bisogno di recuperare la tua password, segui le istruzioni del tuo IdP esterno.

Importante: Anche quando si utilizza un IdP esterno, l'utente deve essere preregistrato nella piattaforma nCommand Lite per ottenere l'accesso.

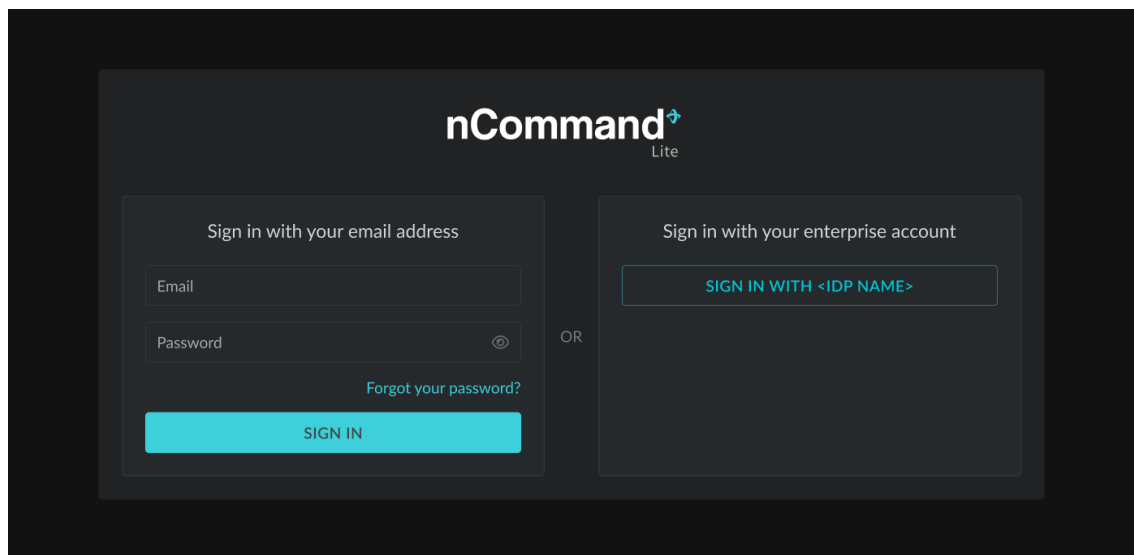


Figura 04: Schermata di login tramite IdP esterno (Esempio)

Sezione 3.3 - Gestione della password

Dopo aver effettuato il primo accesso alla piattaforma, gli utenti possono modificare la propria password o, se è stata dimenticata, impostarne una nuova.

Nota: Quando si accede tramite IdP esterno, le funzioni **Password dimenticata** e **Cambia password** devono essere eseguite in base al processo dell'IdP esterno.

- **Recupera password:** Consente all'utente di recuperare l'accesso all'account se dimentica la password. Sarà sufficiente fare clic sul link "Forgot your password?" (Hai dimenticato la password?) nella pagina di accesso, inserire l'indirizzo e-mail associato e inviare le informazioni. Il sistema invierà quindi un'e-mail contenente un codice di verifica. Una volta inserito il codice e dopo aver fatto clic su "Verify code" (Verifica codice), all'utente verrà richiesto di confermare l'indirizzo e-mail associato. Facendo clic su "Continue" (Continua), l'utente viene

indirizzato a una pagina in cui può inserire una nuova password e confermarla. Se la nuova password soddisfa i requisiti di sistema, l'utente può registrarla e successivamente accedere con le credenziali aggiornate.

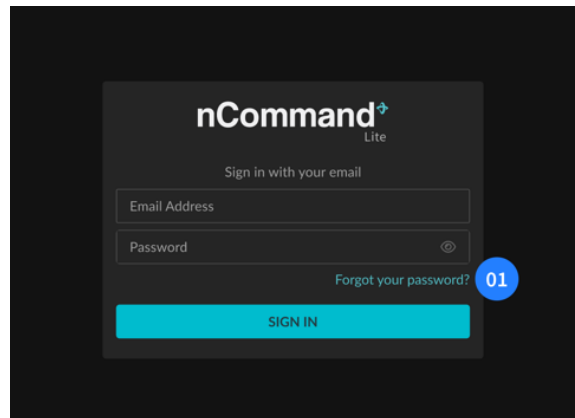


Figura 05: Link alla pagina di reset della password
01 – Hai dimenticato la password?

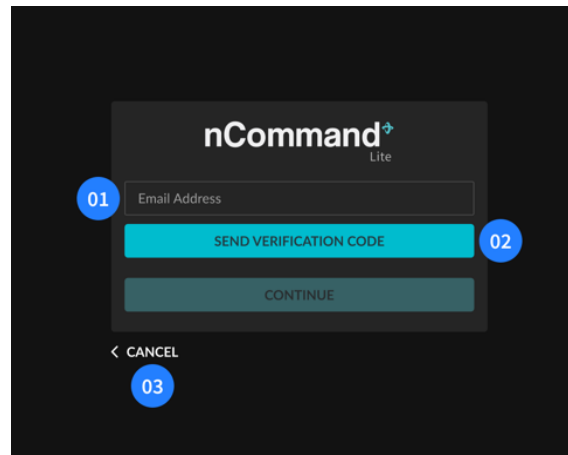


Figura 06: Pagina di reset della password
01 – Indirizzo e-mail; 02 – Invia codice di verifica; 03 – Annulla

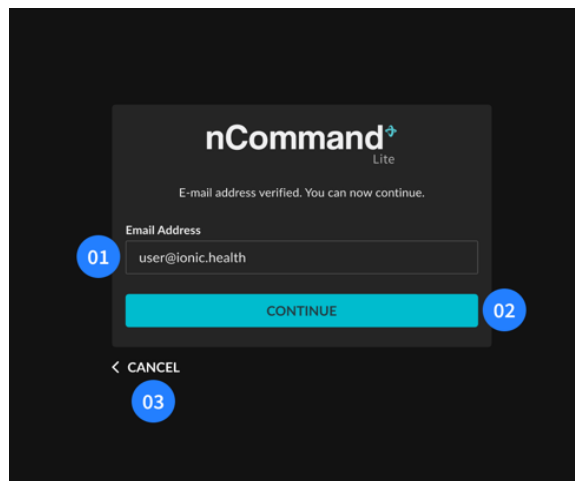
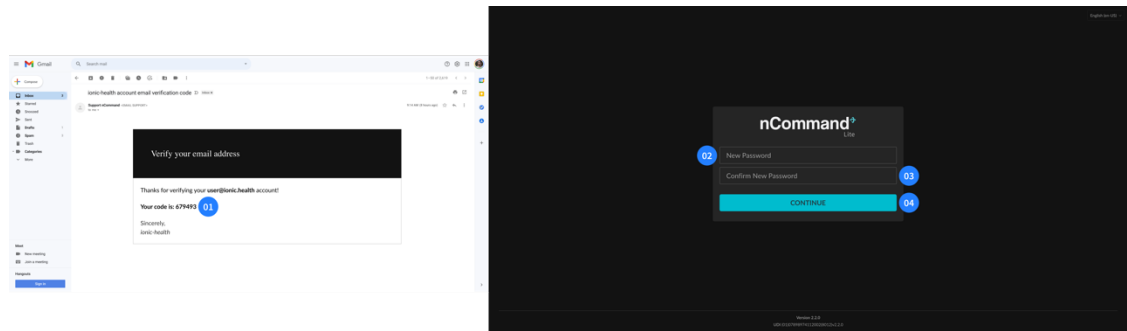
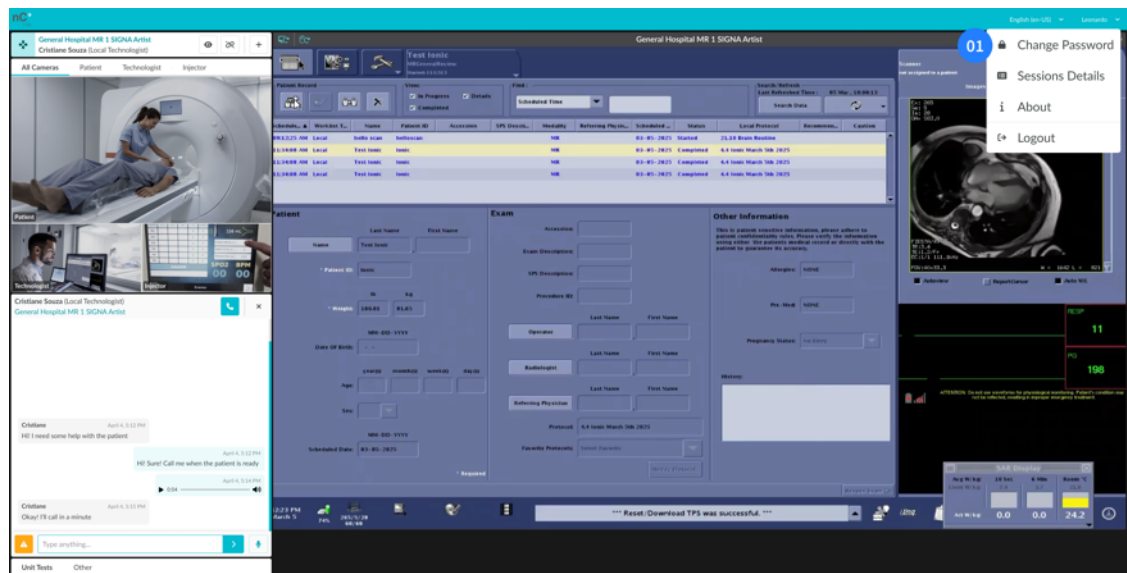


Figura 07: Conferma via email
01 – Indirizzo e-mail; 02 – Pulsante "Continua"; 03 – Annulla



**Figura 08: Email con codice per registrare nuova password (sinistra) - 01 – 2-Codice FA
Pagina Cambia password (destra) - 02 – Nuova password; 03 – Conferma nuova password; 04 – Pulsante “Continua”**

- Modifica password:** Consente agli utenti di aggiornare la propria password rispettando criteri specifici, tra cui almeno 3 elementi tra i seguenti: una lettera minuscola, una lettera maiuscola, un numero e un simbolo, e deve essere lunga almeno 8 caratteri. Il sistema verifica se la nuova password soddisfa questi criteri e, in caso contrario, informa l'utente con un messaggio. Inoltre, gli utenti devono confermare la nuova password per evitare errori di inserimento. Per modificare la password, l'utente, dopo aver effettuato l'accesso, deve fare clic sull'icona nell'angolo in alto a destra e scegliere il menu “Modifica Password”. A questo punto verrà effettuata la disconnessione dalla piattaforma seguita dal reindirizzamento a una pagina per confermare l'indirizzo e-mail associato. Il sistema invierà quindi un'e-mail contenente un codice di verifica. Una volta inserito il codice e dopo aver fatto clic su “Verify code” (Verifica codice), l'utente viene reindirizzato a una schermata in cui può immettere una nuova password.



**Figura 09: Voce del menu a tendina Cambia password
01 – Cambia password**

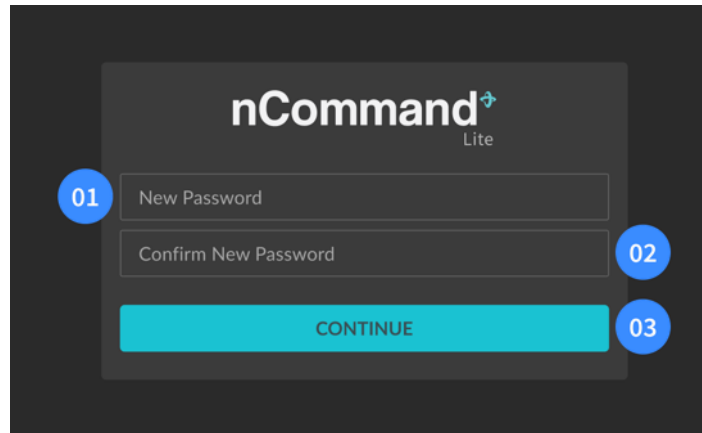


Figura 10: Pagina Cambia password
 01 – Nuova password; 02 – Conferma la nuova password; 03 – Pulsante “Continua”

Sezione 3.4 - Accesso con profilo Tecnologo locale



AVVERTENZA!

Prima di utilizzare la piattaforma, contattare telefonicamente il tecnologo da remoto.



AVVERTENZA!

Non collocare oggetti né davanti alla ventola del computer e-KVM, onde evitarne il surriscaldamento, né sopra il computer, per evitare eventuali danni.



AVVERTENZA!

Durante le sessioni da remoto, il tecnico in locale è responsabile della gestione e dell'applicazione delle norme di sicurezza locali vigenti per ciascun tipo di esame e dei relativi requisiti specifici. Per garantire la sicurezza del paziente e dei professionisti coinvolti, rimanere sempre presenti nella sala di controllo e/o nella sala in cui viene eseguito l'esame.



AVVERTENZA!

Eventuali spostamenti del tavolo con sessione in corso possono essere effettuati solo dal tecnologo locale quando richiesto dal sistema. Prima di uscire dalla sala operatoria, il tecnologo locale deve sempre revocare l'accesso al tecnologo da remoto.



AVVERTENZA!

Solo il tecnologo locale può spostare il tavolo per posizionare il paziente all'interno del dispositivo e rimuoverlo in sicurezza. Prima di uscire dalla sala operatoria, il tecnologo locale deve sempre revocare l'accesso all'utente da remoto.

Dopo aver effettuato l'accesso alla piattaforma, procedere alla selezione del dispositivo di interesse nella casella Device Selection (Selezione del dispositivo). Sarai responsabile di questo dispositivo, quindi potrai esaminare la richiesta del tecnologo da remoto di accedere al dispositivo. Quando un tecnologo da remoto chiede di accedere al dispositivo, viene visualizzata

una finestra a comparsa che consente di verificare tutte le informazioni presentate prima di concedere o negare l'accesso. Monitorare l'arrivo di richieste provenienti da un tecnologo da remoto. È estremamente importante verificare attentamente ogni dettaglio. In caso di mancato riconoscimento delle informazioni fornite, non concedere l'accesso.

Il tecnologo da remoto può accedere al dispositivo utilizzando una delle due modalità di accesso:

Controllo o Visualizza:

- **Modalità Control (Controllo)** - consente al tecnologo da remoto di controllare il mouse e la tastiera, nonché di visualizzare lo streaming del dispositivo. Tuttavia, il tecnologo locale non perde il controllo del mouse e della tastiera locali e può riprenderne il controllo in qualsiasi momento.
- **Modalità View (Visualizza)** - consente al tecnologo da remoto di visualizzare solo lo schermo del dispositivo e di utilizzare la chat per la comunicazione

Dopo aver selezionato il dispositivo, l'utente può accedere alla funzione chat, che permette di comunicare con gli altri utenti tramite messaggi di testo, messaggi audio, chiamate vocali e videochiamate.

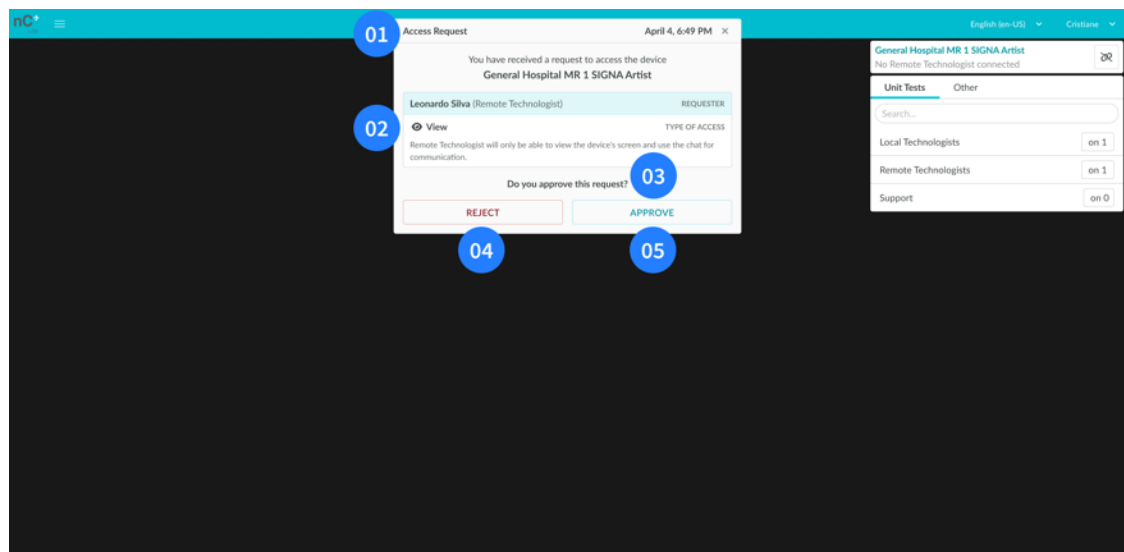


Figura 11: Schermata principale del Tecnologo locale con notifica di richiesta di accesso

01 – Titolo (Richiesta di accesso); **02** – Nome del richiedente, ruolo e descrizione del tipo di accesso;
03 – Richiesta: "Do you approve this request?" (Approvare questa richiesta?); **04** – Pulsante Reject (Rifiuta); **05** – Pulsante Approve (Approva)

Dopo l'approvazione, il tecnologo locale può revocare l'accesso del tecnologo da remoto in qualsiasi momento facendo semplicemente clic sul pulsante REVOKE (REVOCA).

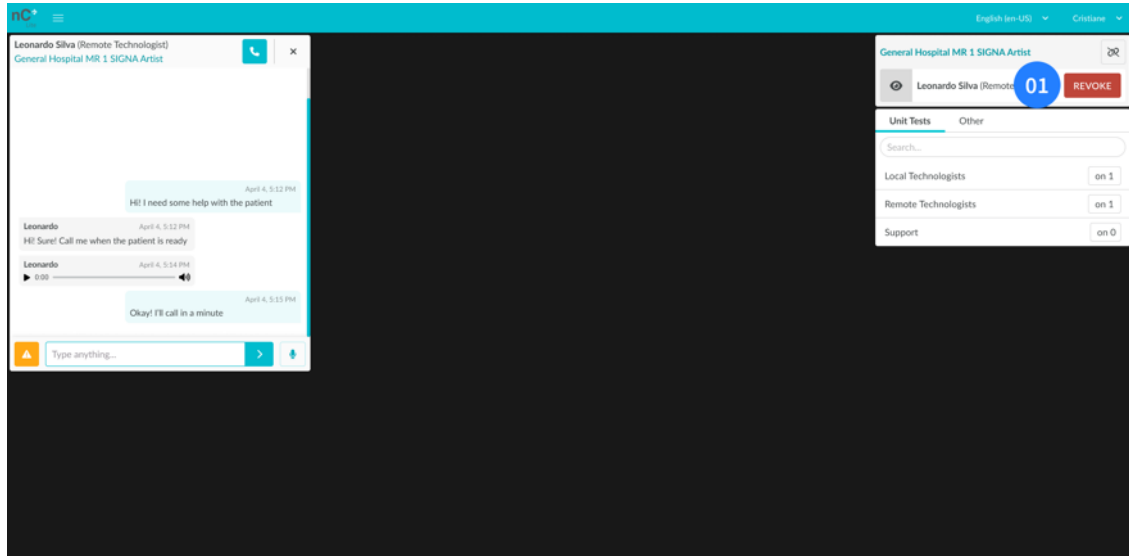


Figura 12: Schermata principale del Tecnologo locale quando è connesso a un dispositivo
01 – Pulsante Revoke (Revoca)

Durante la sessione da remoto, il tecnologo da remoto può chiedere di cambiare la modalità di accesso. La richiesta verrà visualizzata sullo schermo all'interno di una finestra a comparsa. La richiesta può essere approvata o respinta. Si tengano presenti i diritti riconosciuti da ciascuna modalità di accesso al tecnologo da remoto.

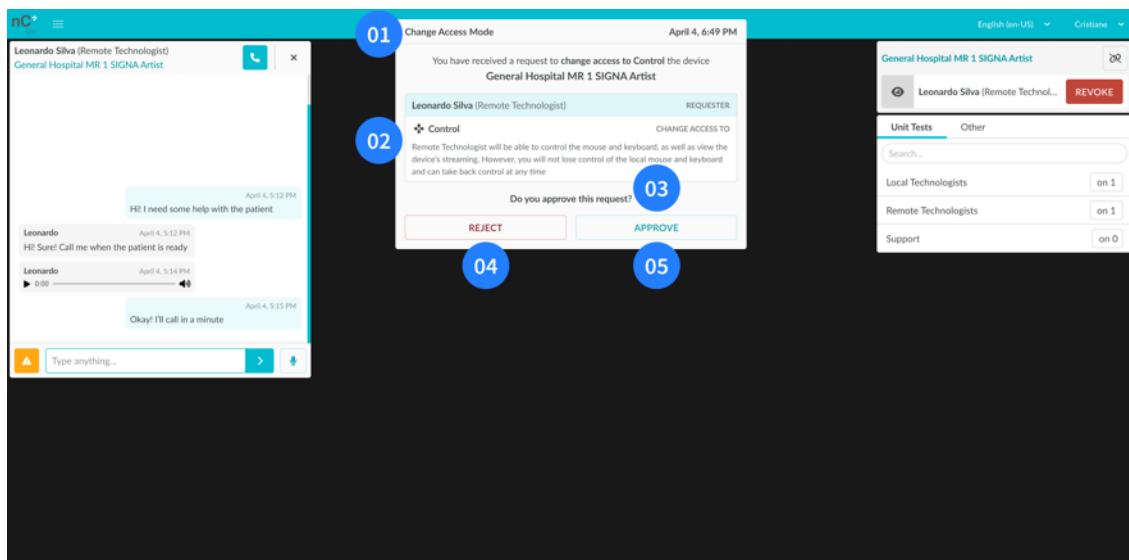


Figura 13: Schermata principale del Tecnologo locale con richiesta di modifica della modalità di accesso
01 – Titolo (Modifica modalità di accesso); 02 – Nome del richiedente, Descrizione del ruolo e del tipo di accesso;
03 – Richiesta: "Do you approve this request?" (Approvi questa richiesta?); 04 – Pulsante Reject (Rifiuta);
05 – Pulsante Approve (Approva)

**AVVERTENZA!**

In caso di perdita della connessione sul computer in locale, il tecnologo da remoto mantiene l'accesso al *dispositivo*. Contattare **immediatamente** il tecnologo da remoto e chiedere di **effettuare la disconnessione** OPPURE accedere a un altro computer e **revocare l'accesso** del tecnologo da remoto OPPURE **premere il pulsante di accensione** per spegnere il computer e-KVM.

**AVVERTENZA!****In caso di manutenzione dello scanner:**

Prima che il tecnico addetto alla manutenzione avvii qualsiasi procedura (sul dispositivo o in sala di controllo), informare il tecnologo da remoto e revocare l'accesso facendo clic sul pulsante "REVOKE ACCESS" (REVOCA ACCESSO). Effettuare quindi la disconnessione dalla piattaforma nCommand Lite.

In assenza di tecnologi da remoto connessi, effettuare la disconnessione dalla piattaforma nCommand Lite prima di avviare la manutenzione.

Sezione 3.5 - Accesso con profilo di tecnologo da remoto

**AVVERTENZA!**

Utente del computer del dispositivo e password di root: entrambi devono essere conservati dall'host in loco che riceverà il team di installazione.

**AVVERTENZA!**

Eventuali spostamenti del tavolo con sessione in corso possono essere effettuati solo dal tecnologo locale quando richiesto dal sistema. Prima di uscire dalla sala operatoria, il tecnologo locale deve sempre revocare l'accesso al tecnologo da remoto.

**AVVERTENZA!**

Solo il tecnologo locale può spostare il tavolo per posizionare il paziente all'interno del dispositivo e rimuoverlo in sicurezza. Prima di uscire dalla sala operatoria, il tecnologo locale deve sempre revocare l'accesso all'utente da remoto.

**AVVERTENZA!**

Monitorare sempre la sala attraverso la videocamera e assicurarsi di comunicare con il tecnologo locale prima di eseguire qualsiasi attività.

**AVVERTENZA!**

In caso di perdita della connessione sul computer in locale, contattare immediatamente il tecnologo locale ed effettuare la disconnessione.

**AVVERTENZA!****In caso di manutenzione dello scanner:**

Dopo essere stati avvisati dell'inizio della manutenzione del dispositivo, assicurarsi che l'accesso sia stato revocato dal tecnologo locale e disconnettersi dalla piattaforma nCommand Lite. Se l'accesso non è stato revocato, disconnettersi dalla piattaforma nCommand Lite e contattare immediatamente il tecnologo locale per informarlo.

**AVVERTENZA!**

Per controllare il mouse e la tastiera da remoto, la modalità di accesso selezionata deve essere Control (Controllo); in modalità View (Visualizzazione), il Tecnologo da remoto può visualizzare solo lo streaming e le videocamere locali.

**AVVERTENZA!**

Se la risposta alla tua richiesta richiede più tempo del previsto, contatta il tecnologo locale tramite chat o telefono.

L'area di lavoro del tecnologo da remoto include apparecchiature quali computer, monitor (di solito tre), mouse, tastiera e cuffie.

Nel flusso di lavoro clinico, il *Tecnologo locale* ha un contatto diretto con il paziente. Sono responsabili dell'interazione con il paziente, del posizionamento e della garanzia della sicurezza e del rispetto del protocollo durante le procedure di risonanza magnetica, TC o PET/TC, secondo gli standard istituzionali e normativi.

3.5.1. Modalità di accesso

Dopo aver effettuato l'accesso alla piattaforma, selezionare il dispositivo al quale si desidera connettersi nella casella di selezione del dispositivo. Si aprirà una finestra popup per scegliere la modalità di accesso tra **Controllo** e **Visualizza**:

- **Controllo** - In questa modalità, oltre alla visualizzazione dello schermo, è abilitato il controllo del mouse e della tastiera. I professionisti locali mantengono il pieno accesso al mouse e alla tastiera locali e possono riprenderne il controllo in qualsiasi momento.
- **Modalità View (Visualizza)** – È possibile solo visualizzare lo schermo del dispositivo e utilizzare la chat per comunicare.

Selezionando la modalità di accesso, compare la casella di "Waiting for approval" (In attesa di approvazione), che indica la necessità di approvazione del tecnologo locale connesso per procedere. Il tecnologo locale ha piena facoltà di approvare o respingere l'accesso e revocarlo in qualsiasi momento, qualora lo ritenga necessario. Questa misura è essenziale allo scopo di garantire un controllo rigoroso e di preservare la sicurezza durante il periodo di utilizzo del dispositivo.

Dopo aver selezionato il dispositivo, l'utente ha accesso alla funzione della chat, che consente di comunicare con gli altri utenti tramite messaggi di testo e audio, chiamate vocali e videochiamate. L'utente non ha bisogno dell'approvazione per accedere alla chat.

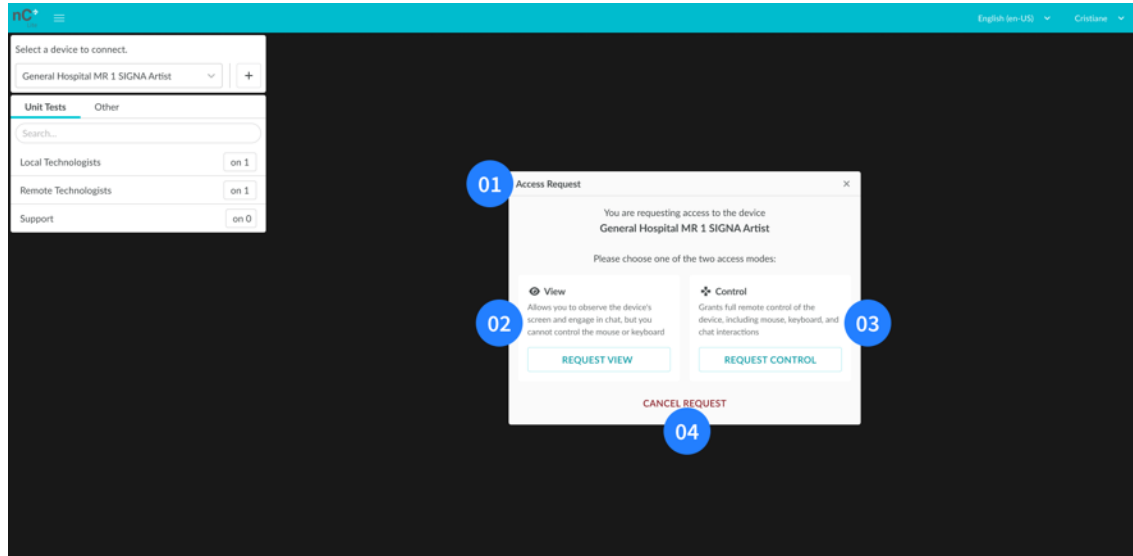


Figura 14: Finestra di richiesta di accesso per Tecnologo da remoto

01 – Titolo (Richiesta di Accesso); **02** - Visualizza la Descrizione della Modalità e pulsante Richiedi Visualizzazione; **03** – Descrizione Controllo e pulsante Richiedi controllo; **04** – Annulla Richiesta

Una volta che l'accesso al dispositivo è stato autorizzato dal tecnico in locale, l'interfaccia del tecnico da remoto verrà aggiornata allo scopo di visualizzare in tempo reale e il dispositivo le relative videocamere. Se la modalità di accesso scelta è Control (Controllo), sarà abilitata l'opzione di funzionamento da remoto del dispositivo.

Questo processo garantisce un'interazione efficace e sicura, consentendo l'uso remoto sicuro del dispositivo senza comprometterne l'integrità o la sicurezza del paziente.

Per richiedere una modifica della modalità di accesso durante una sessione remota, cliccare sull'icona corrispondente. Il tecnologo locale può accettare o respingere la richiesta:

- **Accetta** – lo streaming verrà ricaricato, ma il contenuto della chat non andrà perso. Se sei impegnato in una chiamata vocale e video, questa terminerà e dovrà essere riavviata da uno degli utenti.
- **Decline (Rifiuta)** - apparirà una finestra popup che notificherà il rifiuto del tecnologo locale e l'accesso attuale rimarrà attivo

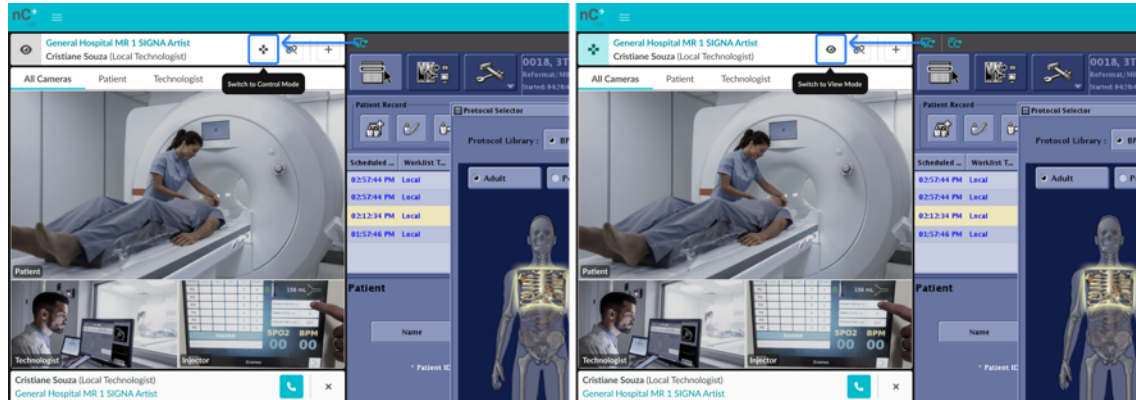


Figura 15: Cambia modalità di accesso

Sinistra - Passa all'icona Controllo e Descrizione comando/ **Destra** - Passa all'icona Visualizza e Descrizione comando

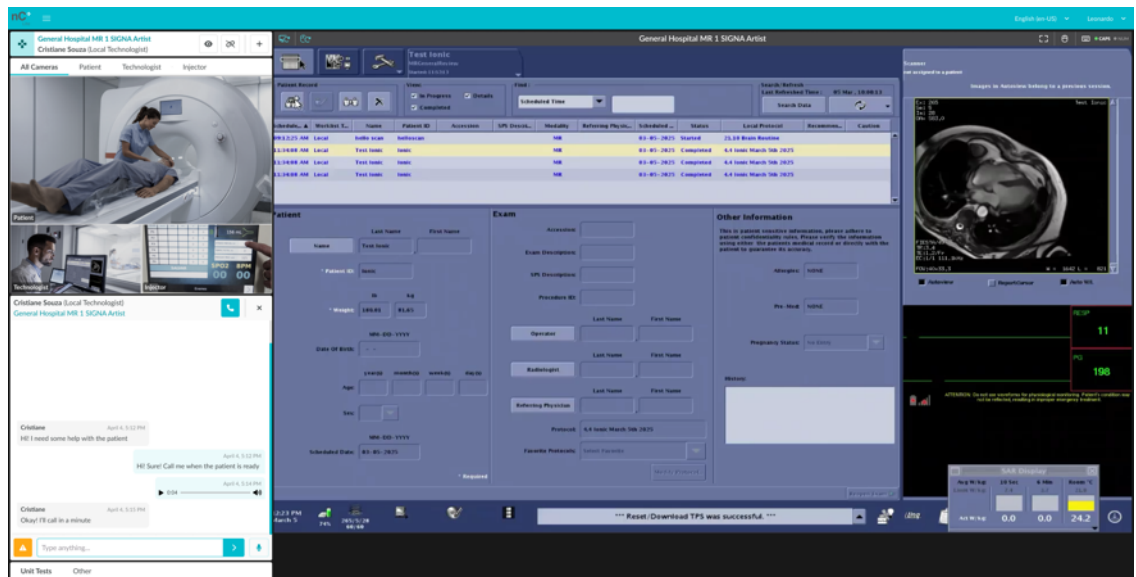


Figura 16: Schermata principale del Tecnologo da remoto quando è connesso a un dispositivo

Quando il tecnologo da remoto richiede l'accesso e non sono presenti tecnologi locali connessi al dispositivo, sulla piattaforma compare una finestra a comparsa con un'avvertenza. Non appena il tecnologo locale effettua la connessione, la piattaforma informa il tecnologo da remoto che può richiedere nuovamente l'accesso.

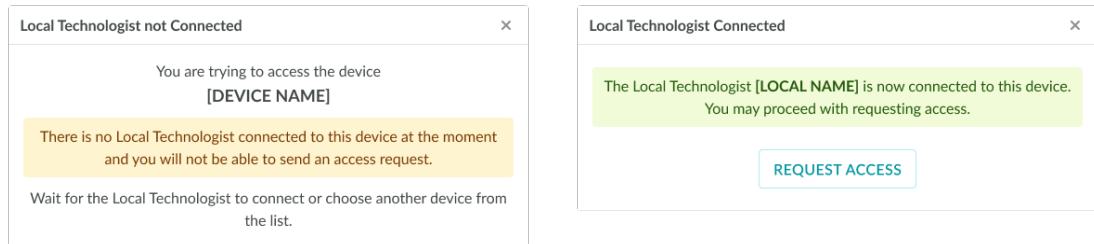


Figura 17: Avvisi del Tecnologo Remoto sullo stato della connessione del Tecnologo Locale
Sinistra - Notifica che indica che è stato effettuato un tentativo di accesso al dispositivo, ma al momento non è connesso alcun Tecnologo locale.
Destra - Notifica che conferma che il Tecnologo locale si è connesso al dispositivo dopo un periodo di disconnessione.

3.5.2. Barra dello streaming

La barra dello streaming mostra le informazioni chiave e i controlli relativi alla sessione di streaming del dispositivo. Include i pulsanti "Ricarica streaming" e "Risincronizzazione mouse", il nome del dispositivo, la risoluzione dello schermo e lo stato corrente del mouse e della tastiera del computer remoto.

1 – Reload Streaming (Ricarica streaming)

Questa funzionalità consente ai tecnologi da remoto di ripristinare l'accesso ai dispositivi in caso di interruzione della connessione o rallentamento delle prestazioni. Se si verifica qualsiasi tipo di disconnessione o ritardo dello schermo sul computer del dispositivo, è possibile fare clic sull'icona "Ricarica streaming" situata nella barra di streaming. Ciò richiederà alla piattaforma di riconnettersi al computer del dispositivo e di ricaricare anche le telecamere di sistema.

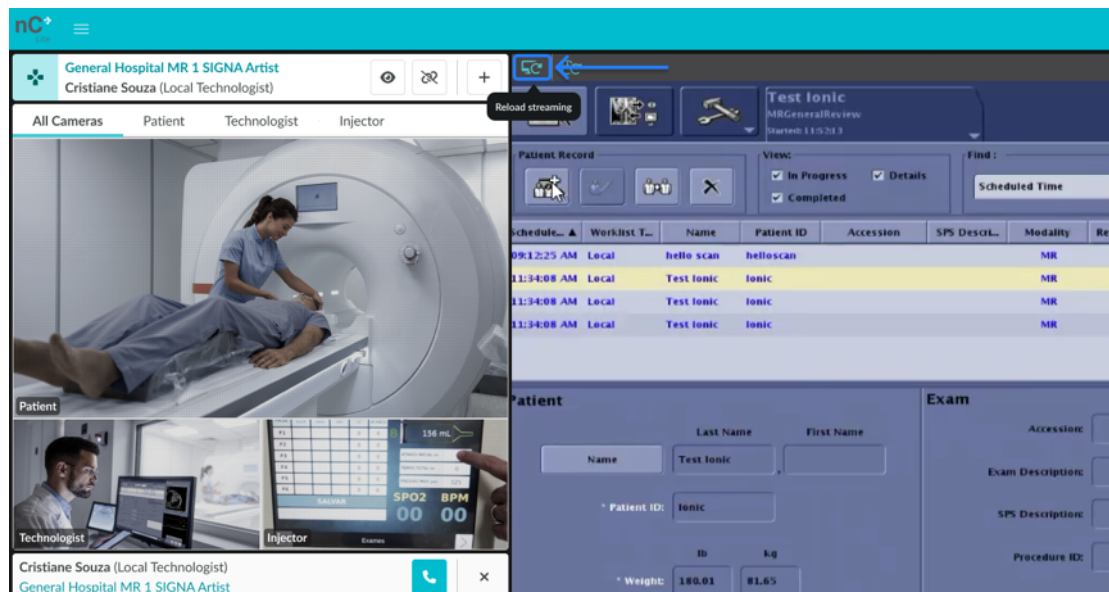


Figura 18: Pulsante Ricarica Streaming

2 – Mouse Resync (Risincronizzazione del mouse)

In caso di rallentamento o disallineamento del mouse, fare clic sul pulsante “Mouse Resync” (Risincronizzazione del mouse) situato sulla barra sopra la finestra dello streaming per risincronizzare il mouse del dispositivo con il computer e-KVM.

Un'alternativa è quella di spostare il puntatore del mouse fuori dall'area di streaming e poi riportarlo dentro: il sistema risincronizzerà automaticamente il mouse senza bisogno di ulteriori azioni. È anche possibile fare clic e rilasciare la rotellina del mouse (se disponibile) per attivare automaticamente la risincronizzazione. Tuttavia, questo metodo potrebbe non funzionare su dispositivi con due o più schermi se i puntatori del mouse locale e remoto si trovano su schermi diversi.

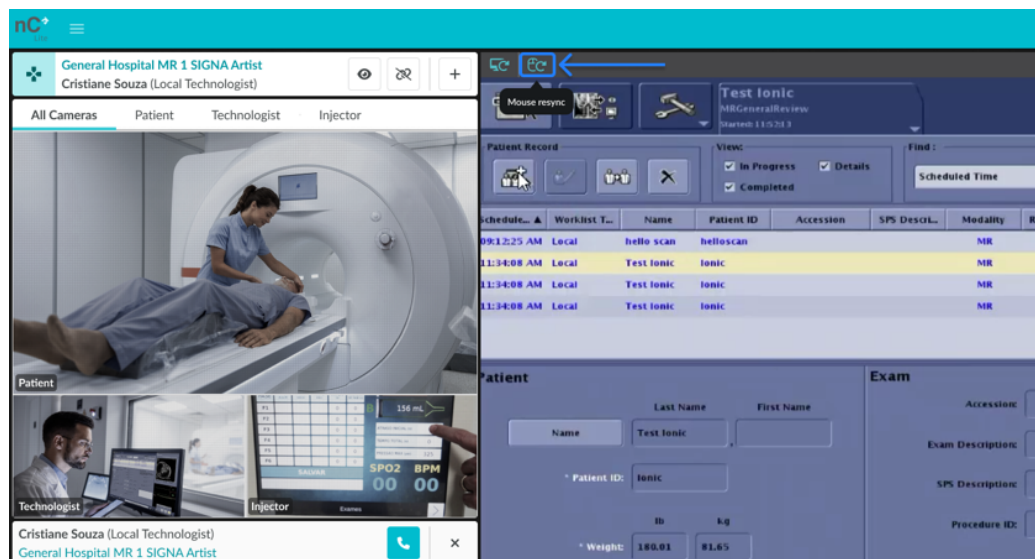


Figura 19: Pulsante di Risincronizzazione del mouse

3 – Streaming Display (Visualizzazione dello streaming)

Questa funzione fornisce al tecnologo da remoto informazioni sulla risoluzione di streaming originale (dal dispositivo) e sulla risoluzione corrente in pixel visualizzata sulla workstation remota.

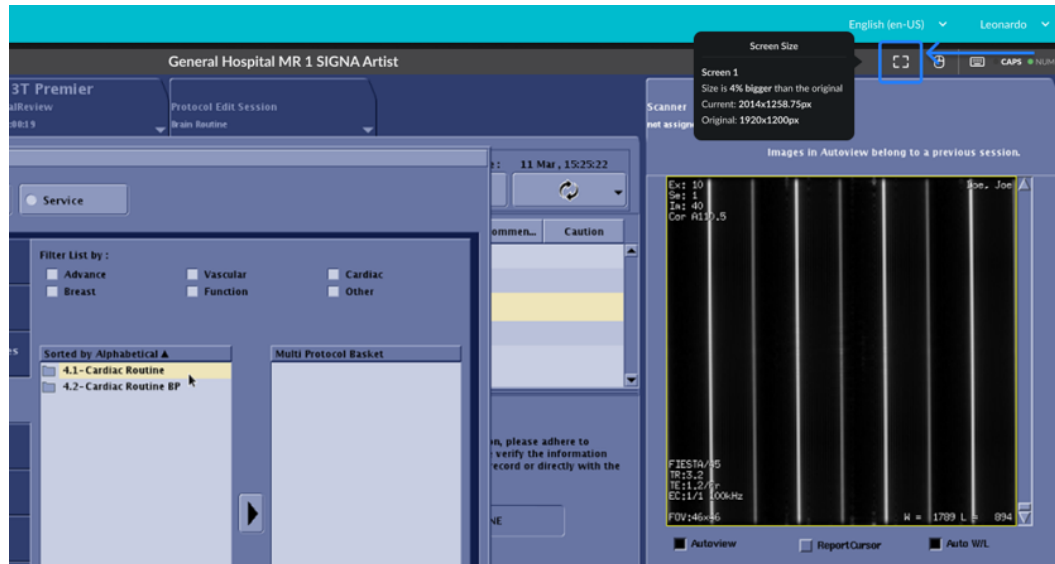


Figura 20: Descrizione comando sulle Informazioni in streaming

4 – Mouse and Keyboard Status (Stato del mouse e della tastiera)

Questa funzione informa il tecnologo da remoto se il mouse e la tastiera funzionano correttamente. Insieme allo stato della tastiera, l'utente può verificare se i tasti **Caps lock** e **Num lock** della tastiera del computer del dispositivo sono attivati o disattivati. Questa funzione dipende tuttavia dal computer del dispositivo che fornisce queste informazioni. Nei casi in cui questi dati non sono resi disponibili dal sistema del dispositivo, lo stato dei tasti **Caps Lock** e **Num Lock** non sarà visualizzato. Gli stati del mouse e della tastiera vengono visualizzati solo quando l'utente dispone dell'accesso in modalità Control (Controllo).

Nel tentativo di connessione a un dispositivo, una discrepanza tra gli indicatori **Bloc Maiusc** e **Bloc Num** sul computer da remoto e il dispositivo potrebbe causare incongruenze di digitazione. Se gli indicatori vengono visualizzati come abilitati sul dispositivo ma non sono effettivamente attivi sul computer da remoto, l'utente può scrivere in maiuscolo sul dispositivo, ma il testo nella chat compare in minuscolo o viceversa. Analogamente, se la funzione **Bloc Maiusc** è abilitata sul computer da remoto, ma disabilitata sul dispositivo, lo stesso problema si verificherà al contrario.

Per ovviare a questa eventualità, prima di accedere al dispositivo, assicurarsi che le funzioni **Bloc Maiusc** e **Bloc Num** siano o entrambe abilitate, oppure entrambe disabilitate. In caso di mancata corrispondenza, l'utente deve disconnettersi dal dispositivo, modificare lo stato della tastiera sul computer remoto e poi riconnettersi.

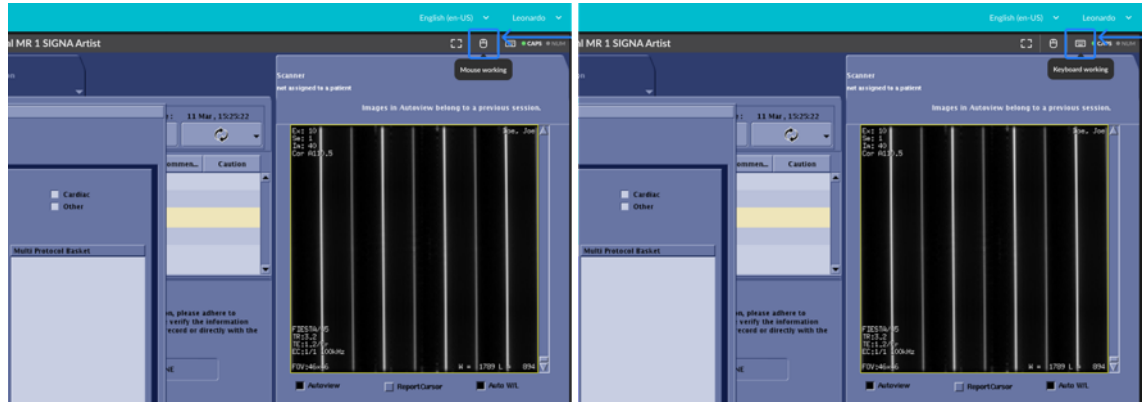


Figura 21: Barra dello streaming

Sinistra - Informazioni sulla descrizione comando per lo Stato del mouse

Bene - Informazioni sulla Descrizione comando per lo Stato della tastiera

3.5.3. Configurazione a più videocamere

Questa funzione consente al tecnologo da remoto di visualizzare più videocamere contemporaneamente. Se è disponibile più di una videocamera, è possibile visualizzarne una sola e passare da una videocamera all'altra facendo clic sul menu con il nome assegnato a ciascuna di esse. Selezionando "ALL CAMERAS" (TUTTE LE VIDEOCAMERE), nel riquadro saranno visualizzate tutte le videocamere disponibili e solo una sarà evidenziata. Per cambiare la videocamera evidenziata, basta passare il mouse su una delle fotocamere nel riquadro più piccolo e cliccare su "SWITCH CAMERA" (CAMBIA VIDEOCAMERA).

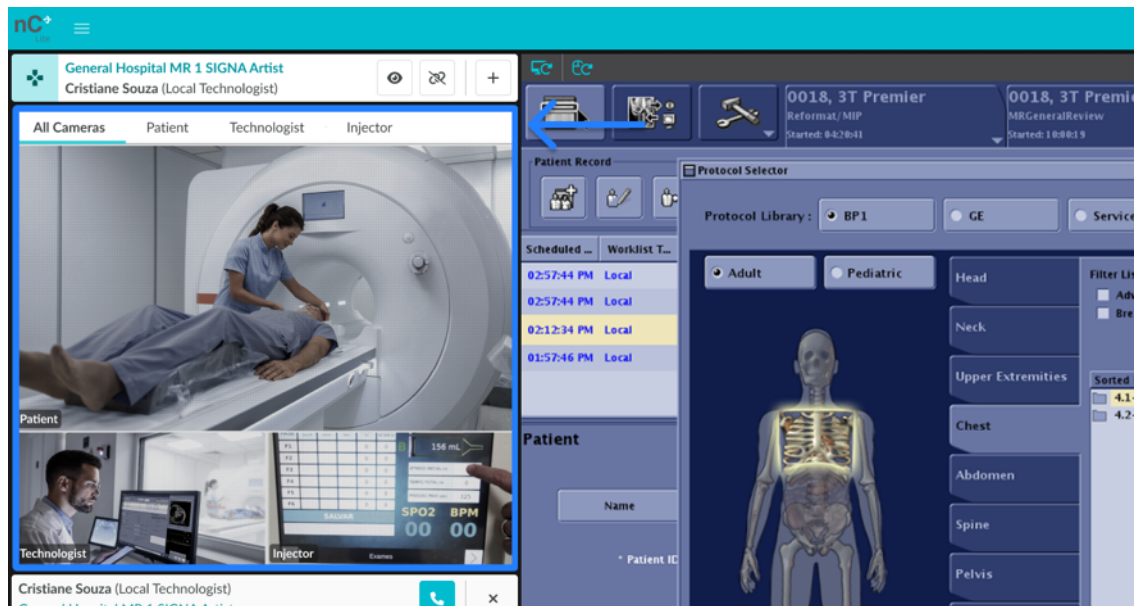


Figura 22: Visualizzazione multi-camera

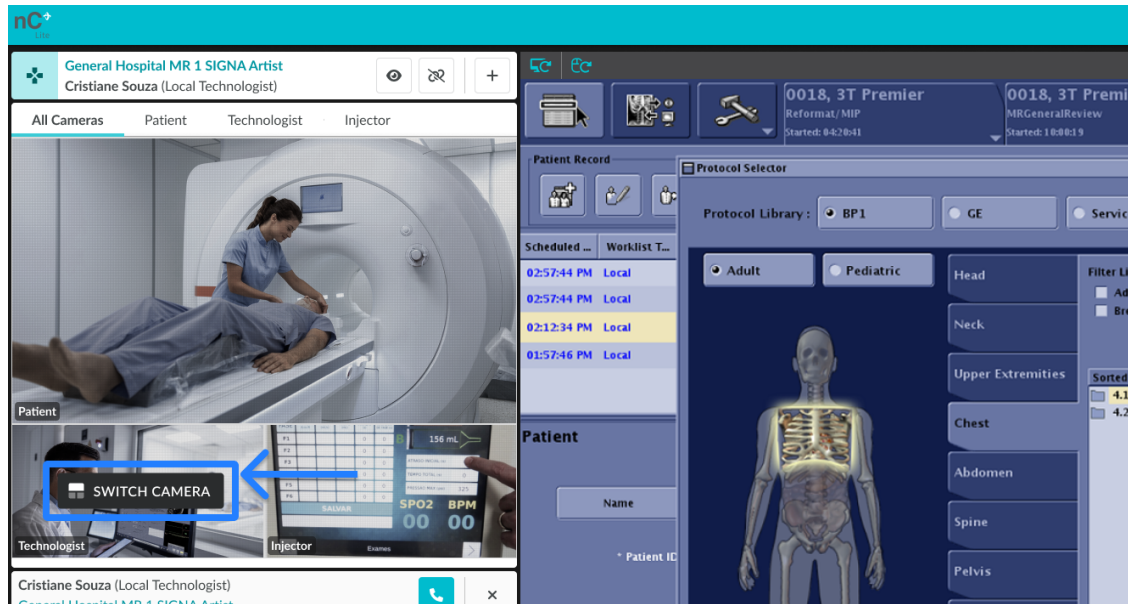


Figura 23: Pulsante sensibile al passaggio del mouse "SWITCH CAMERA" (CAMBIA VIDEOCAMERA)

Durante una sessione da remoto attiva, se il tecnologo da remoto effettua l'accesso in modalità **View (Visualizza)**, è disponibile un'opzione per spegnere una o più videocamere passando il mouse sulla videocamera scelta e facendo clic su "TURN OFF CAMERA" (SPEGNI VIDEOCAMERA). Per visualizzare nuovamente la videocamera, sarà sufficiente ripetere la procedura e fare clic su "TURN ON CAMERA" (ATTIVA VIDEOCAMERA).

NOTA: La funzione di spegnimento delle videocamere è disponibile solo in modalità View (Visualizza); in modalità Control (Controllo) non è possibile spegnere le videocamere.

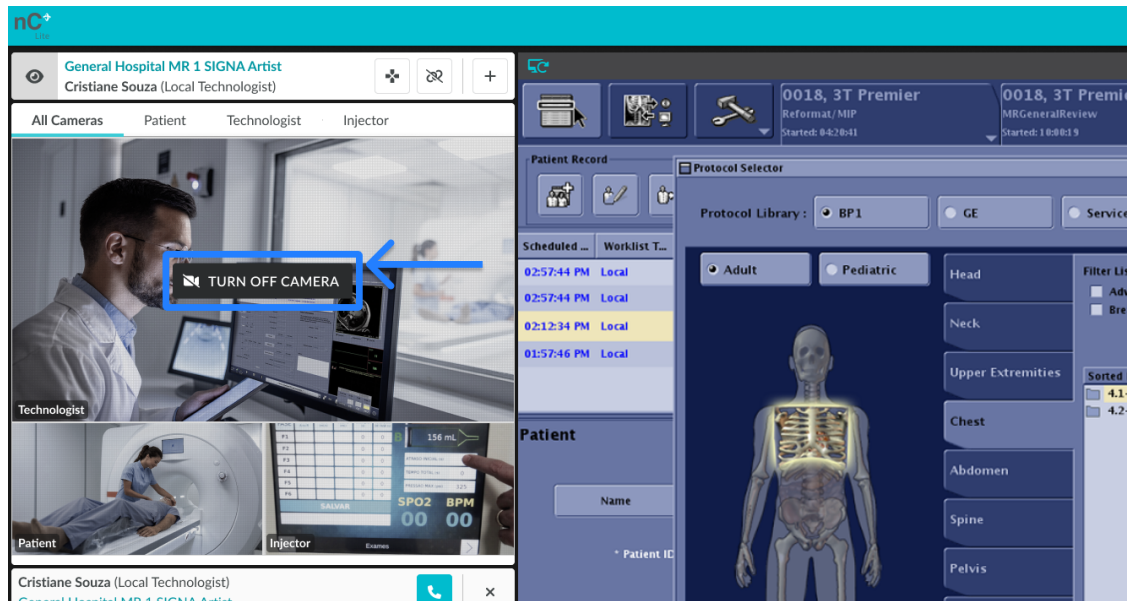


Figura 24: Pulsante sensibile al passaggio del mouse "SPEGNI VIDEOCAMERA" nella sezione a più telecamere in modalità di visualizzazione

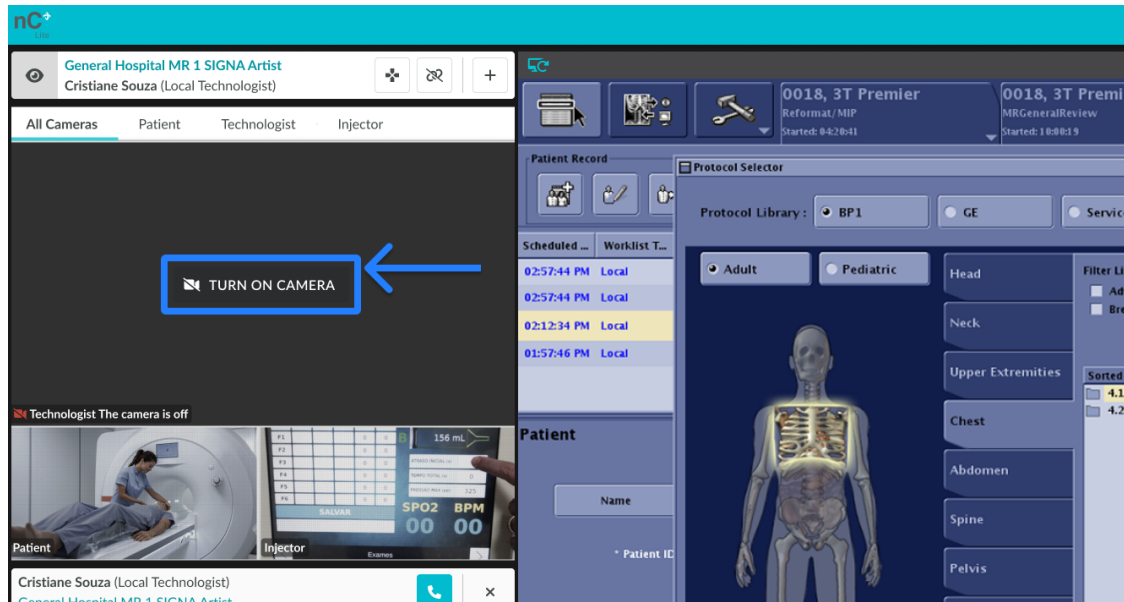


Figura 25: Pulsante sensibile al passaggio del mouse "TURN ON CAMERA" (ACCENDI VIDEOCAMERA) nella modalità di visualizzazione a più videocamere

3.5.4. Apri un altro dispositivo

Consente al tecnologo da remoto di aprire una nuova scheda del browser del sistema nCommand Lite, permettendo così all'utente di selezionare un nuovo dispositivo per eseguire simultaneamente più di una scansione da remoto. Per aprire un nuovo dispositivo al quale effettuare l'accesso, è sufficiente fare clic sul pulsante "Open Another Device" (Apri un altro dispositivo). A questo punto, viene visualizzato un avviso che consente di eseguire questa operazione simultanea in sicurezza. Leggere l'avvertenza prima di accedere a questa nuova finestra.

NOTA: Per una migliore visualizzazione durante l'accesso simultaneo, si consiglia, dopo aver selezionato "OPEN ANOTHER DEVICE" (APRI UN ALTRO DISPOSITIVO) e aver cliccato su "OK" negli avvisi, di trascinare la nuova scheda su un altro monitor disponibile.



AVVERTENZA!

Avvertenza di sicurezza per l'accesso a più scanner

- **Richiesta di concentrazione intensa:** L'accesso simultaneo richiede un'intensa concentrazione e una comunicazione efficace con i team locali.
- **Scegliere layout differenti:** Evitare di accedere contemporaneamente a dispositivi con layout o esami identici della stessa regione anatomica.
- **Trascina la scheda su un altro monitor:** Quando si accede a un dispositivo aggiuntivo, si apre una nuova scheda. Trascinare questa scheda su un secondo monitor, poiché il sistema è progettato per essere utilizzato con uno schermo separato per ciascun dispositivo.
- **Prestare attenzione agli avvisi:** Prestare particolare attenzione a tutti gli avvisi di sistema, in quanto sono essenziali per garantire la sicurezza delle operazioni.

- **Controllare uno alla volta:** È possibile visualizzare più schermate, ma il controllo è limitato a un dispositivo alla volta.
- **Apri chat:** Ai fini di una comunicazione efficace, avviare sempre una chat in caso di connessione a un dispositivo.
- **Una chiamata alla volta:** Gli avvisi di chiamata vocale vengono visualizzati sullo schermo del dispositivo associato; è possibile avere una sola chiamata attiva alla volta.
- **Sicurezza e avvisi:** Dare priorità alla sicurezza e rimanere vigili durante tutte le operazioni.

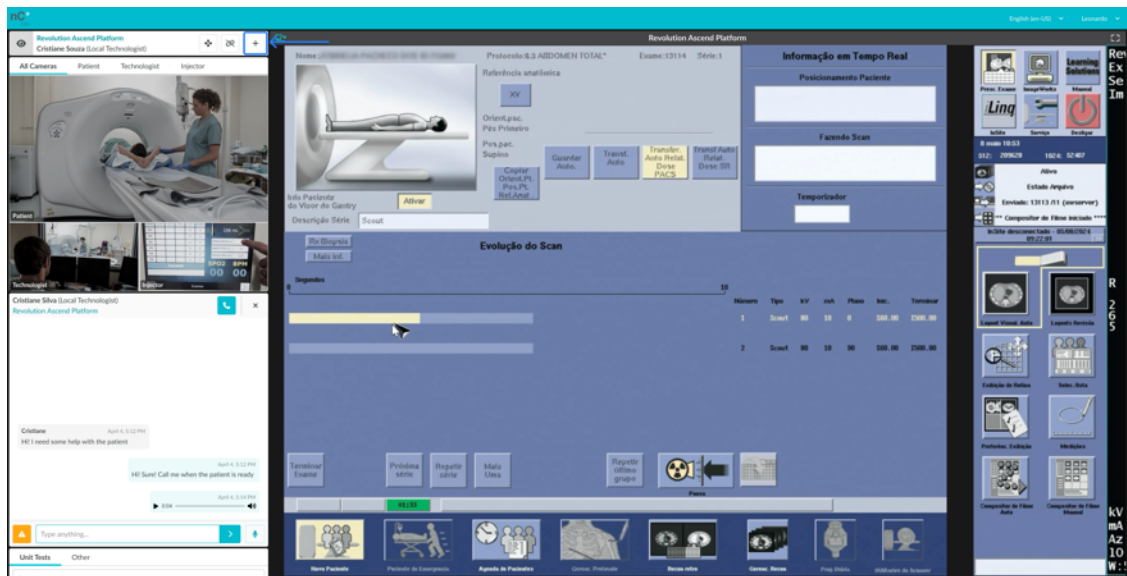


Figura 26: Pulsante Apri un altro dispositivo (+)

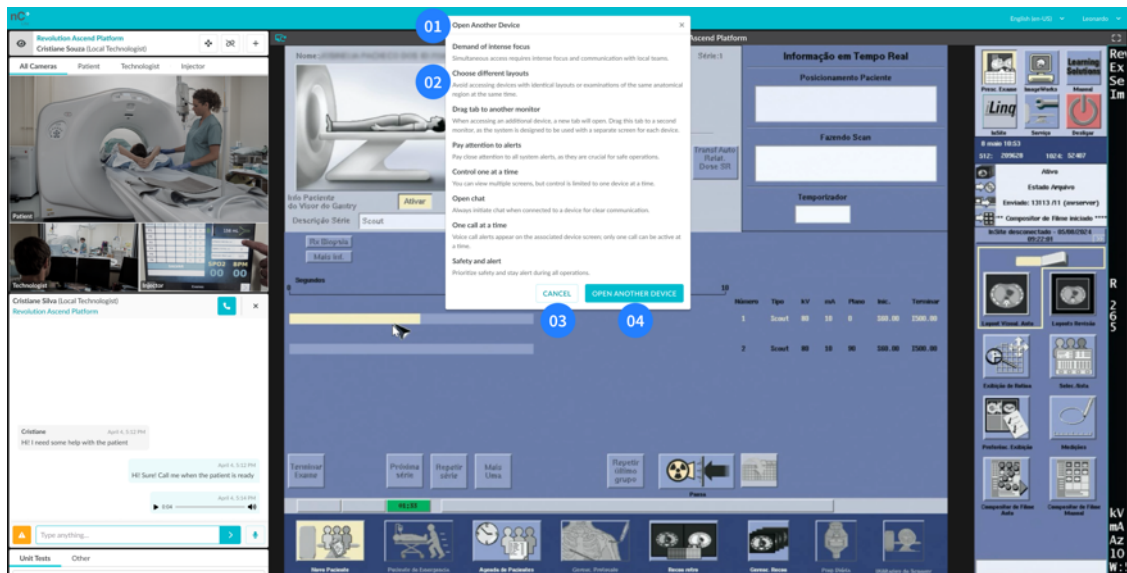


Figura 27: Avvisi di accesso a più dispositivi

01 – Titolo (Open Another Device [Apri un altro dispositivo]); 02 – Operational Safety Warnings (Avvertenze sulla sicurezza operativa); 03 – Pulsante Annulla; 04 – Pulsante Apri un altro dispositivo

3.5.5. Controllo sistema

La funzione "System Check" (Controllo sistema) consente di verificare che il dispositivo, la rete e la connettività Internet attuali soddisfino i requisiti per utilizzare correttamente nCommand Lite. Esegue un rapido test automatico che verifica elementi essenziali come la qualità di Internet, l'accesso ai server richiesti e la stabilità della connessione. Questo strumento può essere utilizzato prima di iniziare una sessione, durante l'installazione o quando si sospetta un problema di connessione. Aiuta a garantire il corretto funzionamento della piattaforma e supporta il team tecnico in caso di necessità di risoluzione dei problemi.

Nota: La funzione *System Check* dovrebbe essere utilizzata preferibilmente con il supporto o su richiesta di un professionista IT. L'esecuzione di questo strumento senza una guida tecnica potrebbe portare a un'interpretazione errata dei risultati.

Per accedere a System Check, i tecnici locali e remoti devono aprire l'opzione Dettagli sessione dal menu a discesa disponibile sotto il loro nome utente, situato nell'angolo in alto a destra della schermata principale. Quindi, fare clic su **Open** (Apri) accanto allo strumento *System Check*. Una volta visualizzata la pagina dello strumento, fare clic su **Run Test** (Esegui test) per avviare il processo di verifica.

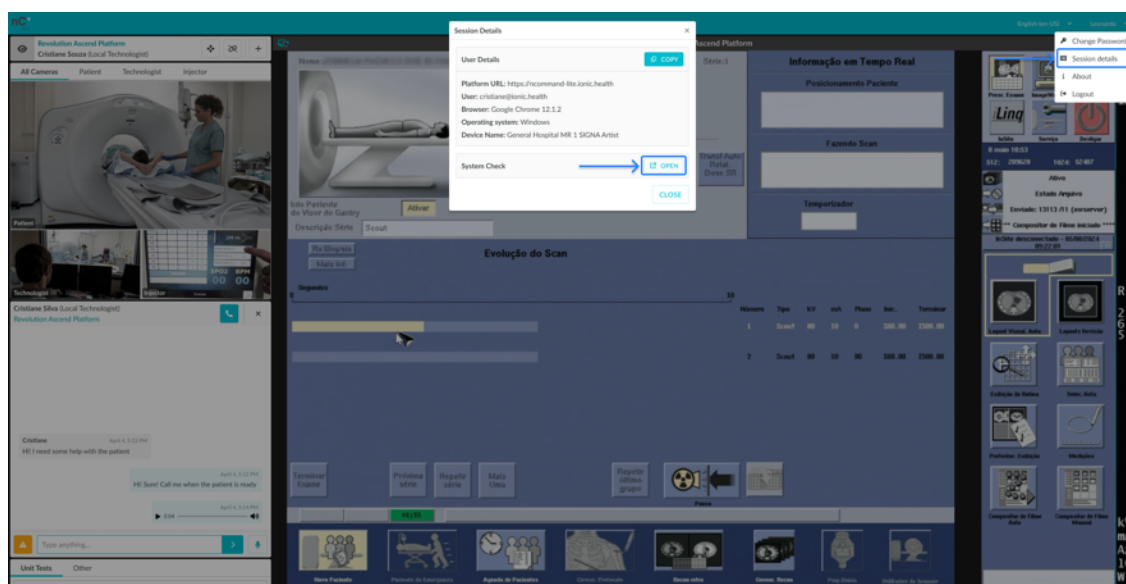


Figura 28: Accesso a System Check

Utilizzando il tecnologo da remoto, è possibile selezionare un dispositivo nella schermata principale dello strumento in modo che venga incluso nei risultati del test.



AVVERTENZA!

Prima di iniziare il test, assicurarsi che il dispositivo selezionato non sia attualmente in uso.

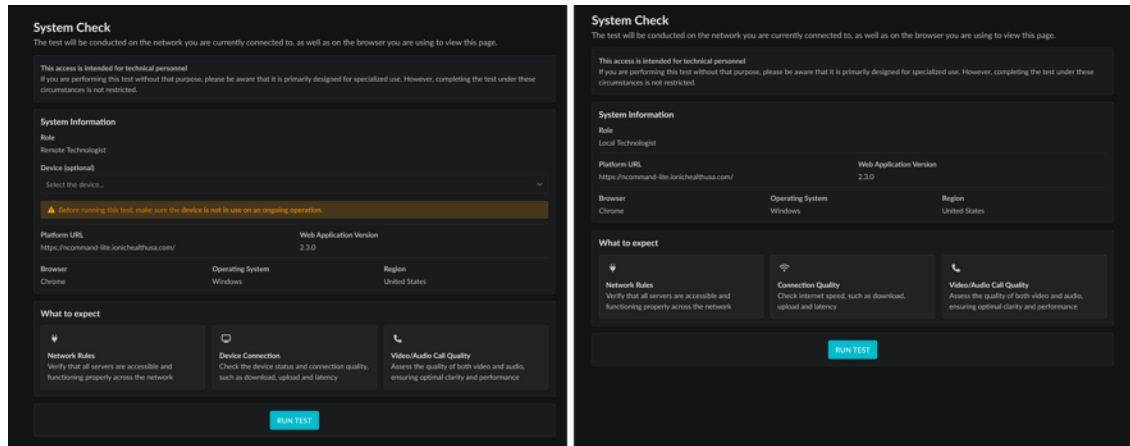


Figura 29: Schermata principale del System Check
Sinistra - Tecnologo da remoto / Destra - Tecnologo locale

Una volta completato il test, sullo schermo viene visualizzato un riepilogo dei risultati. I professionisti IT possono esaminare queste informazioni per identificare possibili problemi che incidono sulle prestazioni del sistema.

Sezione 3.6 - Chat

La piattaforma offre una chat e una chiamata in tempo reale con funzionalità vocali e video, utilizzate per una comunicazione efficace tra tecnici autorizzati. Grazie a queste funzionalità, i tecnici autorizzati possono interagire su tutti gli aspetti relativi al flusso di lavoro della sessione.



AVVERTENZA!

In caso di guasto, contattare telefonicamente il tecnologo locale.

Dopo esserti connesso a un dispositivo, avrai accesso immediato all'elenco degli utenti della chat, organizzato in due schede. Per i clienti multi-sede, ogni filiale può essere configurata come un contratto separato. Se abilitata, gli utenti vengono raggruppati in base al contratto, mentre gli utenti di altri contratti vengono visualizzati nella scheda "Altri".

Per avviare una conversazione, fare doppio clic sul nome di un utente per aprire l'interfaccia della chat, che supporta sia la messaggistica di testo che le chiamate vocali. Assicurarsi che la sessione selezionata corrisponda al dispositivo corretto. La piattaforma avvisa gli utenti se la connessione di rete diventa lenta o instabile.



AVVERTENZA!

Prima di avviare il contatto, verificare il nome del dispositivo visualizzato sotto il nome dell'utente, poiché alcuni tecnologi da remoto potrebbero essere connessi a più dispositivi.

Ecco gli strumenti disponibili per la comunicazione all'interno della piattaforma:

1. **Chiamate vocali e video:** Fare clic sull'icona per avviare una chiamata vocale e video della durata massima di 60 minuti tra un tecnologo da remoto e un tecnologo locale. Le connessioni tra utenti con lo stesso profilo (Locale-Locale o Remoto-Remoto) non sono supportate.

Quando un tecnologo locale avvia una chiamata, il tecnologo da remoto può scegliere se accettare o rifiutare. Al contrario, quando un tecnologo da remoto avvia la chiamata, viene automaticamente connesso e il tecnologo locale viene avvisato queste funzioni costituiscono un meccanismo di sicurezza per garantire che il tecnologo da remoto possa sempre comunicare con chiunque sia fisicamente presente sul posto, come se fosse lì di persona.

Per impostazione predefinita, il microfono è attivo all'inizio della chiamata, mentre la fotocamera rimane spenta. Ogni tecnologo può accendere o spegnere manualmente il microfono e la telecamera in qualsiasi momento.

Per stabilire una chiamata correttamente, entrambi gli utenti devono disporre di un microfono e di un'uscita audio funzionanti, con le autorizzazioni del browser correttamente abilitate. Se uno di questi componenti risulta mancante, il sistema avviserà entrambi gli utenti e la chiamata non verrà completata. La presenza di una telecamera è facoltativa: se non è disponibile o non viene rilevata, il sistema aggiornerà l'icona per indicare che il video non è supportato.

È consentita una sola chiamata attiva per utente. Se un tecnologo tenta di avviare una nuova chiamata mentre ne è già impegnata in un'altra, il sistema bloccherà il tentativo e visualizzerà una notifica. Allo stesso modo, se un utente è già impegnato in una chiamata e riceve un'altra chiamata in arrivo, il chiamante verrà informato che il destinatario non è attualmente disponibile e l'utente nella chiamata in corso riceverà un avviso che indica che qualcuno ha tentato di contattarlo.

2. **Chiusura delle chat:** Quando uno degli utenti chiude la chat cliccando sul pulsante Chiudi, viene inviato un messaggio automatico all'altro utente e la scheda della chat viene chiusa. Questo tipo di funzionamento garantisce che entrambe le parti siano informate che la conversazione è terminata. Quando la finestra della chat viene chiusa, tutti i messaggi scompaiono. Se si riapre la chat durante la sessione, la conversazione si riavvia senza i messaggi precedenti.
3. **Messaggi di testo:** Inviare messaggi di testo nel campo designato. Quando viene inviato un messaggio, compare un'icona con un segno di spunta grigio e, quando il messaggio viene ricevuto dal destinatario, compare un'altra icona con due segni di spunta blu. Questo sistema garantisce una comunicazione scritta sicura, chiara e concisa tra le due parti.
4. **Richiamo all'attenzione:** Attira l'attenzione dell'altro utente cliccando sul pulsante con il punto esclamativo. Questa azione applica un effetto visivo di vibrazione alla finestra dell'altro utente per alcuni secondi e invia automaticamente un messaggio che segnala urgenza o importanza.
5. **Messaggi audio:** Invia messaggi audio facendo clic sul pulsante del microfono. Questa funzione viene utilizzata per trasmettere un messaggio in modo più personale o quando scrivere non è conveniente.

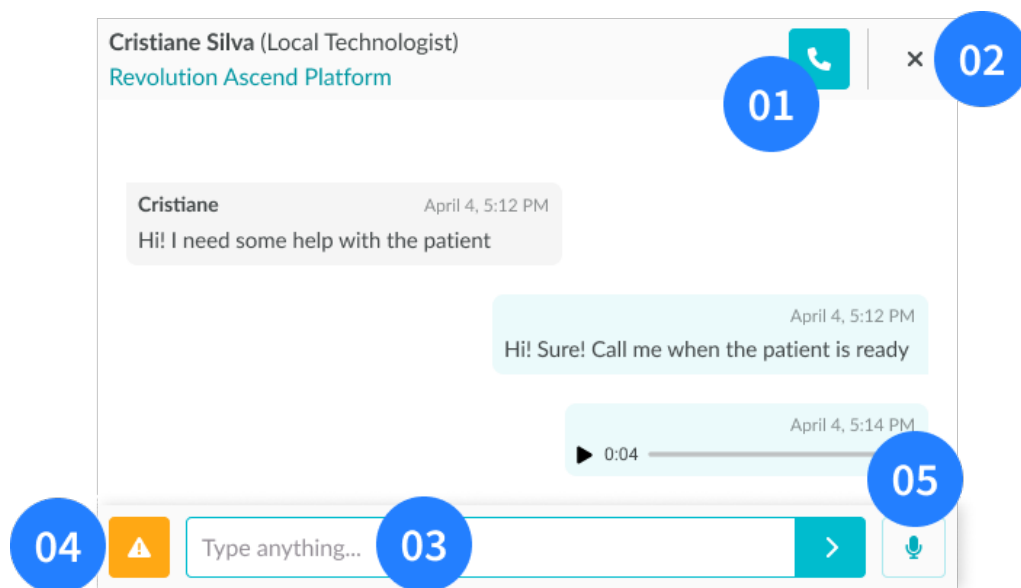


Figura 30: Visualizzazione finestra chat

01 – Pulsante Chiamata vocale e video; **02** - Pulsante Chiudi chat; **03** – Casella di testo del messaggio; **04** – Pulsante Chiama l'attenzione; **05** – Registra Pulsante Messaggio áudio

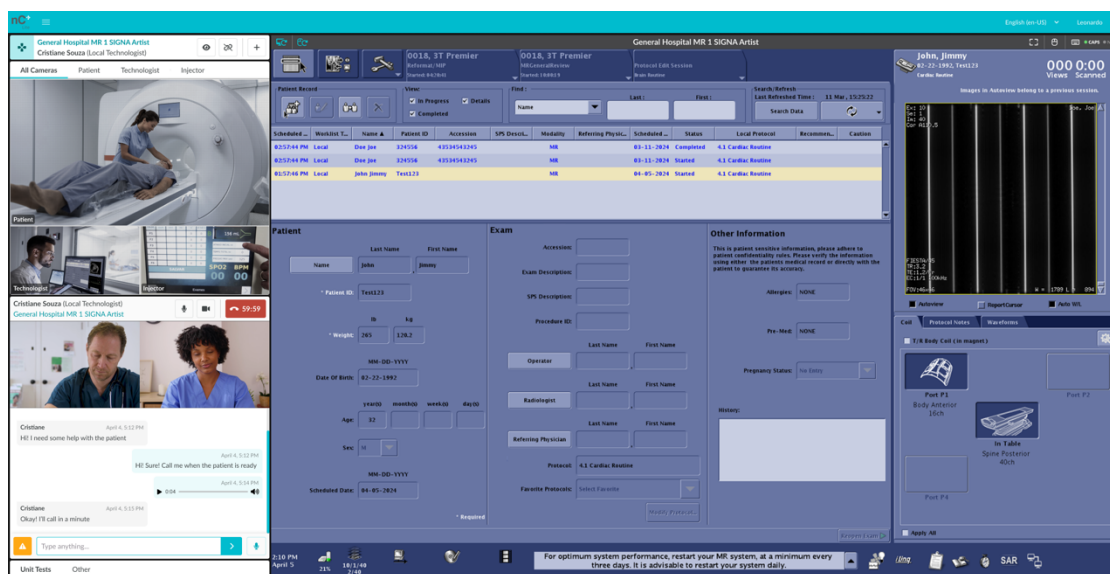


Figura 31: Schermata principale del Tecnologo da remoto - Finestra della chat (angolo in basso a sinistra)

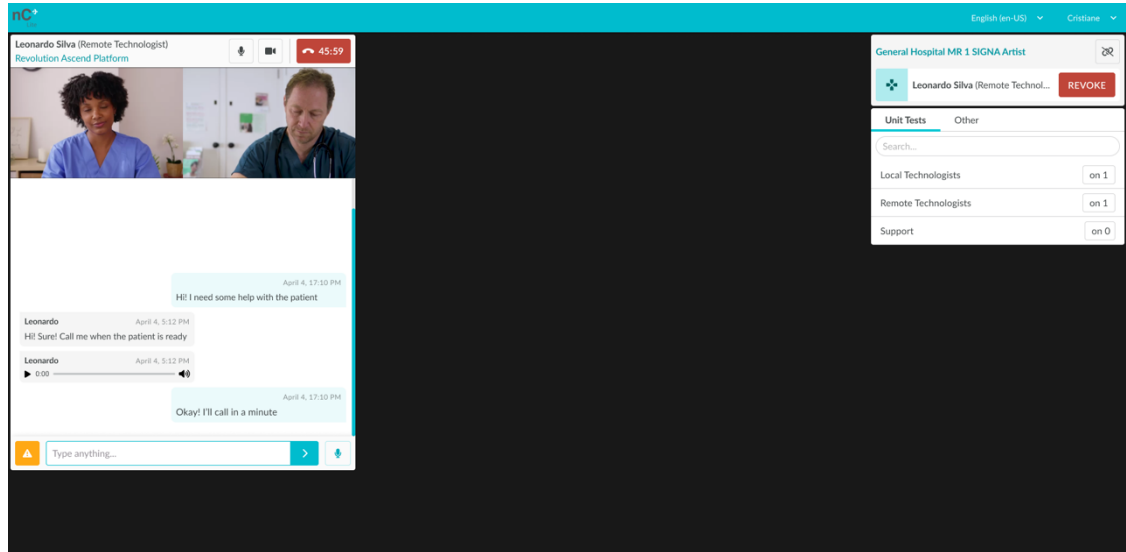


Figura 32: Schermata principale del Tecnologo locale - finestra della chat

Problemi di connessione a Internet: quando uno dei tecnici riscontra problemi di connessione di rete, sul sistema compare un messaggio e viene effettuato un nuovo tentativo di connessione. Se la connessione viene ripristinata, sul sistema comparirà il messaggio **ONLINE** e la sessione da remoto continuerà come di consueto. Tuttavia, dopo vari tentativi di riconnessione, se la connessione non viene ristabilita, il sistema terminerà la sessione attiva e notificherà al tecnico che è stato disconnesso a causa di problemi con Internet. Allo stesso tempo, informerà anche l'altro tecnico che la controparte è stata disconnessa a causa di problemi con Internet.

Sezione 3.7 - Chiusura della sessione sulla piattaforma

Al termine del servizio, il tecnico autorizzato deve effettuare la disconnessione dal dispositivo e uscire dalla piattaforma.



AVVERTENZA!

I tecnici autorizzati non devono dimenticarsi di effettuare la disconnessione dalla piattaforma prima della fine dell'intervento.

Per disconnettersi dal dispositivo, è necessario fare clic sull'icona di disconnessione situata nella casella Dispositivo. Nota: Se si opera come Tecnologo locale, assicurarsi di aver revocato qualsiasi accesso al Tecnologo da remoto prima di disconnettersi dal dispositivo.

Per garantire la sicurezza, si riceverà una notifica per confermare l'intenzione di effettuare la disconnessione dal dispositivo. Dopo la conferma, l'utente verrà reindirizzato alla schermata iniziale, senza selezionare alcun dispositivo.

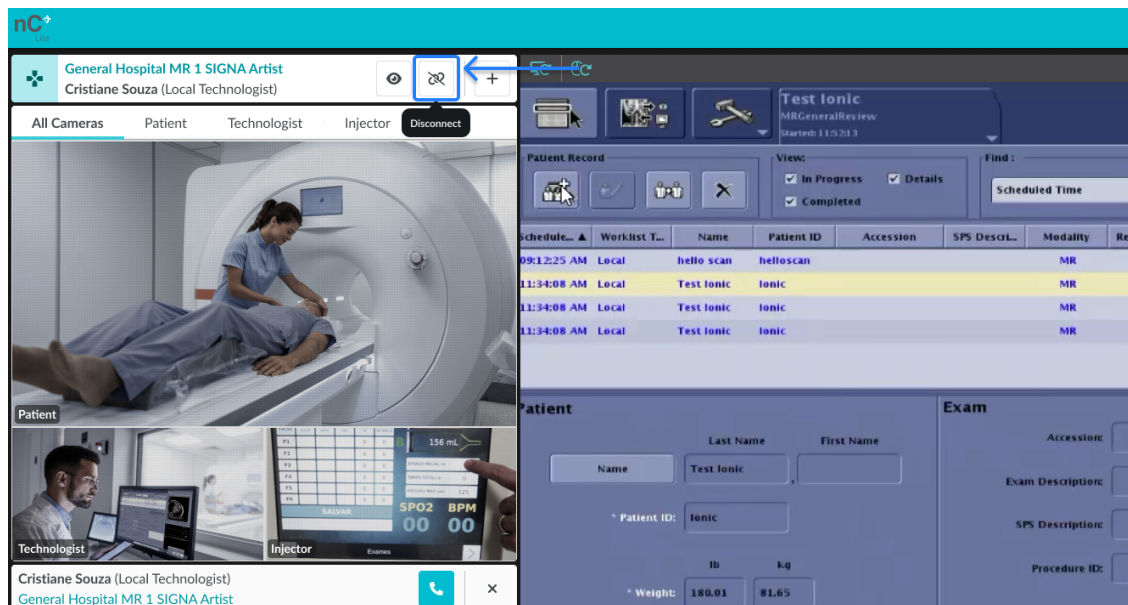


Figura 33: Pulsante Disconnetti - schermata principale Tecnologo da remoto

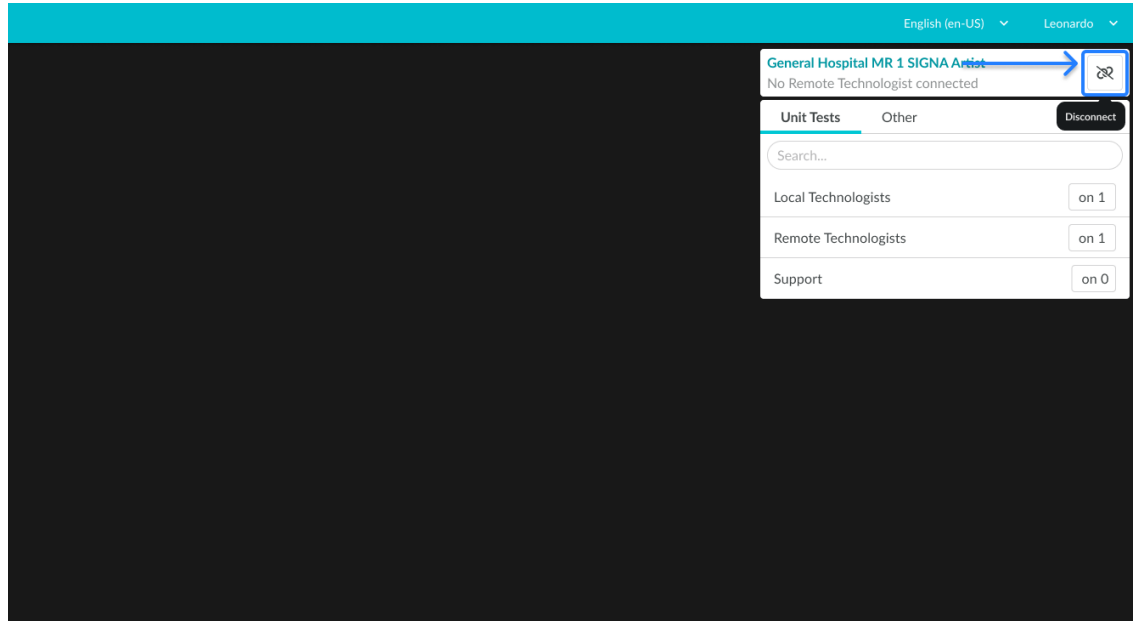


Figura 34: Pulsante Disconnetti - schermata principale del Tecnologo locale



AVVERTENZA!

Prima di effettuare la disconnessione, assicurarsi che tutte le schede aggiuntive aperte siano state chiuse.

Per chiudere la sessione sulla piattaforma, fare clic sul nome utente nell'angolo in alto a destra dello schermo e selezionare l'opzione "Logout" (Disconnettersi). L'utente riceverà una notifica per confermare l'intenzione di uscire dal centro medico in cui stava operando. Dopo la conferma, l'utente verrà reindirizzato alla pagina di accesso dell'applicazione, concludendo così il lavoro in modo sicuro.

nCommand Lite non controlla la sessione dell'utente sull'IdP esterno e pertanto non può eseguire una disconnessione a livello di IdP. Negli scenari in cui gli utenti condividono lo stesso computer e utilizzano Single Sign-On (SSO), si consiglia che ogni utente selezioni l'opzione "non rimanere connesso" durante l'accesso all'IdP esterno (se disponibile) o che si disconnetta dall'IdP dopo essersi disconnesso da nCommand Lite. In questo modo si garantisce che nessun utente successivo sullo stesso dispositivo possa riutilizzare involontariamente una sessione attiva.

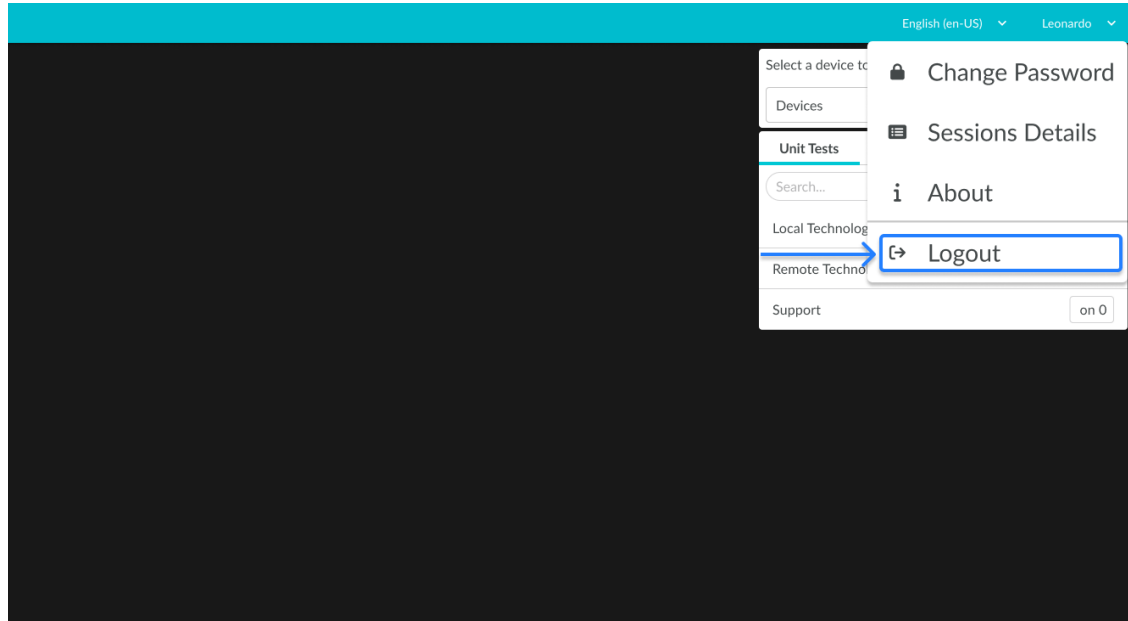


Figura 35: Voce di menu a discesa Logout (Esci)



AVVERTENZA!

Quando si utilizza un provider di identità esterno su un computer condiviso o pubblico, dopo aver effettuato il logout dalla piattaforma, è necessario disconnettersi anche dal provider di identità. Per ulteriori informazioni su come procedere, contattare il team di supporto IT della propria organizzazione.

Sezione 3.8 - Formazione operativa

La partecipazione al programma di formazione è obbligatoria per tutti gli utenti del sistema nCommand Lite. La registrazione dell'utente sulla piattaforma è gestita dal team IONIC Health e viene avviata solo dopo la conferma che l'utente ha completato con successo la formazione LMS richiesta ed è adeguatamente qualificato per utilizzare la piattaforma. Questo processo garantisce che tutti gli utenti abbiano una conoscenza approfondita delle funzionalità del sistema e siano preparati a utilizzare la piattaforma in modo efficiente e sicuro. Per avviare la procedura di iscrizione al corso di formazione, contattare il proprio rappresentante commerciale.

Sezione 3.9 - Linee guida per la risoluzione dei problemi

UTENTE E PASSWORD	
Modifica della password	Verificare che i requisiti della password siano stati soddisfatti e che la password sia complessa e sicura, includendo almeno una lettera minuscola, una lettera maiuscola, un carattere speciale e abbia una lunghezza minima di 8 caratteri.
Password dimenticata	Controlla la tua casella di posta elettronica: Assicurati di utilizzare l'indirizzo email corretto e che l'email di recupero della password non sia stata filtrata nella cartella spam o posta indesiderata. Riprova: Attendere qualche minuto e richiedere un'altra e-mail di recupero della password facendo clic su "Did you Forget your password?" (Hai dimenticato la password?). Controllare la connessione Internet: Assicurarsi di aver effettuato la connessione a Internet.
E-mail di benvenuto non ricevuta	Verificare se l'e-mail si trova nella cartella dello Spam. Se non è presente, contattare un utente con diritti di amministratore per assicurarsi che l'indirizzo e-mail fornito al momento della registrazione sia corretto. Se non è corretto, l'amministratore deve aggiornarlo e inviare nuovamente l'e-mail di benvenuto.
Codice di autenticazione a due fattori non ricevuto	Fare clic su "Resend Code" (Rinvia codice) e controllare la cartella Spam. In caso di mancata ricezione, contattare un utente con diritti amministratore per verificare se l'indirizzo e-mail registrato nella sezione Controllo accesso è corretto.
Numero di tentativi di accesso superato	Se si supera il numero consentito di tentativi di accesso, deve trascorrere un certo lasso di tempo prima di poter riprovare.
FORNITORE ESTERNO DI IDENTITY	

Problemi di accesso al prodotto	Se si riscontrano problemi di accesso durante l'utilizzo di un Identity Provider (IdP) esterno, tener presente che il processo di autenticazione è gestito interamente dall'IdP e non dal fornitore del prodotto, ovvero: Ionic Health. Pertanto, il prodotto non può fornire assistenza per le credenziali dell'account, i criteri di accesso, gli errori di autenticazione o il blocco dell'account. In questi casi, occorre contattare il team di supporto IT della propria organizzazione, che potrà esaminare la configurazione dell'IdP e aiutarti a risolvere il problema.
Problemi relativi alle credenziali	Eventuali problemi relativi alle credenziali (<i>ad es.</i> , password dimenticata, modifica della password) devono essere risolti direttamente con il team di supporto IT dell'organizzazione. Il team può rivedere la configurazione dell'IdP e fornire l'assistenza necessaria.
Problemi con l'autenticatore a più fattori (MFA)	Eventuali problemi relativi all'autenticazione a più fattori (MFA) (<i>ad esempio</i> , problemi di scadenza dell'MFA, l'MFA non funzionante, l'accesso senza richiedere l'MFA) devono essere risolti direttamente con il team di supporto IT della propria organizzazione. Il team può rivedere la configurazione dell'IdP e fornire l'assistenza necessaria.
Credenziali non funzionanti sulla piattaforma	Quando si utilizzano provider di identità esterni (IdP), accedere al prodotto solo tramite l'IdP. L'utilizzo delle credenziali IdP direttamente nella pagina di accesso del prodotto comporterà l'accesso non riuscito.
MONITOR DEL COMPUTER DELLO SCANNER	
Mancata accensione	Verificare i collegamenti del monitor al computer e alla presa elettrica. Potrebbe essersi verificata una disconnessione di uno o più componenti. Premere nuovamente il pulsante di accensione del monitor.
PIATTAFORMA	
Non raggiungibile	Verificare la connessione di rete. Verificare se la piattaforma è stata

	avviata e se l'accesso è andato a buon fine.
Latenza della piattaforma	Aggiornare la pagina premendo Ctrl+F5. Verificare se la chat dell'unità (struttura medica) è aperta in più di una scheda. In questo caso, chiudere la scheda che non viene utilizzata. Se il problema persiste, provare a effettuare la disconnessione dalla piattaforma, svuotare la cache, chiudere il browser e infine accedere nuovamente.
Caratteristiche malfunzionanti	Prima di provare altre procedure di risoluzione dei problemi, svuotare la cache del browser (cercare le istruzioni per il proprio browser attuale) dopo aver effettuato l'accesso, quindi chiudere e riaprire il browser, accedere nuovamente alla piattaforma e riprovare l'azione.
Aggiornamento	Dopo aver aggiornato la piattaforma, svuotare la cache del browser (fare riferimento alle istruzioni del proprio browser) prima di accedere alla nuova versione.
AUDIO	
Assenza di suono	Assicurarsi che il volume del microfono e dell'altoparlante dell'unità (struttura medica) siano regolati su livelli adeguati. Verificare se il browser dispone dell'autorizzazione all'uso di audio e microfono. Verificare che le cuffie siano collegate e funzionino correttamente.
Latenza del suono	Verificare i collegamenti elettrici e di rete dell'apparecchiatura. Aggiornare la pagina del browser premendo Ctrl+F5 e accedere nuovamente. Se il problema persiste, provare a effettuare la disconnessione dalla piattaforma, svuotare la cache, chiudere il browser e infine accedere nuovamente.

CHAT	
Mancata visualizzazione della chat	Assicurarsi che il browser non sia ridotto a icona. In caso contrario, aprire la chat dopo aver effettuato l'accesso alla piattaforma nCommand. Verificare che l'unità (struttura sanitaria) sia stata selezionata e che l'utente sia autorizzato ad abilitare la comunicazione tramite chat. Assicurarsi che le autorizzazioni relative ad audio e microfono del browser siano accettate. Verificare i collegamenti dei cavi, che potrebbero essere scollegati. Aggiornare la pagina del browser premendo Ctrl+F5 ed effettuare nuovamente la connessione alla piattaforma. Verificare se la chat del sito è aperta in più di una scheda. In questo caso, chiudere la scheda che non viene utilizzata.
Ritardo della chat	Aggiornare la pagina del browser premendo Ctrl+F5 ed effettuare nuovamente la connessione alla piattaforma. Se il problema persiste, provare a effettuare la disconnessione dalla piattaforma, svuotare la cache, chiudere il browser e infine accedere nuovamente. Verificare i collegamenti dei cavi, che potrebbero essere scollegati.
Problemi durante l'invio di messaggi audio	Verificare le autorizzazioni del browser per audio e microfono e assicurarsi che sia il microfono sia i dispositivi audio siano collegati al computer. Se è necessario modificare le autorizzazioni del browser, premere Ctrl+F5 per chiedere al browser di riconoscere le

	modifiche in seguito al ricaricamento della pagina.
Mancato avvio della chiamata vocale	Verificare la connessione a Internet e controllare se è comparsa una notifica che spiega il motivo per cui la chiamata non è stata avviata. Assicurarsi di disporre di un dispositivo audio connesso e che le autorizzazioni per audio e microfono siano consentite nel browser. Se il problema persiste, aggiorna la pagina con Ctrl+F5 per riprovare.
Utente non trovato nella chat	Se non è possibile individuare un utente nella chat, fare clic sulla scheda "Others" (Altri) per assicurarsi che non sia elencato lì. Gli utenti associati ad altri contratti vengono visualizzati separatamente nell'elenco dei contatti. Se l'utente non figura nell'elenco dei contatti dopo che è stato selezionato il dispositivo, premere Ctrl+F5 per aggiornare la schermata e selezionare nuovamente. Assicurarsi di disporre di una connessione a Internet.
RICHIESTA DI ACCESSO AL DISPOSITIVO	
La piattaforma non ha riconosciuto che il tecnico in locale è connesso	Selezionare l'opzione "Others" (Altri) per verificare se l'utente in locale è connesso. Se l'utente è effettivamente connesso ma continua a comparire il messaggio in cui si comunica che l'utente in locale non è connesso allo scanner, aggiornare la schermata premendo Ctrl+F5 e chiedere all'utente in locale di ripetere la stessa procedura. Selezionare quindi nuovamente il dispositivo e chiedere di selezionare ancora una volta il dispositivo anche all'utente in locale. Se il problema persiste, contattare l'assistenza per verificare la rete.
Mancato invio della richiesta di accesso	Aggiornare la pagina premendo Ctrl+F5 e verificare tramite chat con l'utente in locale che la richiesta di accesso sia stata ricevuta. Se il problema persiste, contattare l'assistenza per ricevere ulteriore assistenza.
DISPOSITIVO DI STREAMING (COMPUTER e-KVM)	
Mancato funzionamento del dispositivo di streaming (COMPUTER e-KVM)	Fare clic sul pulsante "Reload streaming" (Ricarica streaming) sulla piattaforma.

	Assicurarsi che il gruppo di continuità (struttura sanitaria) e/o il dispositivo di streaming siano collegati e accesi correttamente. Spegnere il dispositivo di streaming e tutte le altre apparecchiature, e riaccenderli. Aggiornare la piattaforma.
Lentezza del dispositivo di streaming	Fare clic sul pulsante "Reload streaming" (Ricarica streaming) sulla piattaforma. Aggiornare la pagina con Ctrl+F5 ed effettuare nuovamente il collegamento alla piattaforma. Verificare la qualità della connessione di rete. Per convalidare lo stato della rete, è possibile eseguire un "ping test" sul dispositivo per verificare la perdita di pacchetti. In caso di problemi con Internet, la piattaforma potrebbe non funzionare come previsto. Aggiornare la pagina web e richiedere nuovamente l'accesso all'utente in locale.
Perdita dell'uscita video	Potrebbe accadere che una scarica elettrostatica causi la perdita dell'immagine. Dopo un riavvio del sistema, la comunicazione e lo streaming video devono essere ristabiliti automaticamente.

Sezione 3.10 - Metodi di pulizia dei componenti hardware

- Prima di avviare il processo di pulizia, assicurarsi che tutte le apparecchiature siano scollegate dalla presa elettrica.
- Non utilizzare prodotti abrasivi.
- Non immergere le apparecchiature o le periferiche in alcun tipo di liquido.
- Smaltire i detergenti conformemente alle normative per lo smaltimento dei rifiuti pericolosi.
- Si sconsiglia l'uso di disinfettanti spray, poiché il vapore potrebbe penetrare nelle apparecchiature e causare cortocircuiti o corrosioni.
- Questo prodotto non è sterile

Capitolo 4 Sicurezza informatica e riservatezza

Sezione 4.1 - Rischi per la sicurezza e la privacy

Il sistema **nCommand Lite System** implementa svariate misure tecniche e organizzative al fine di proteggere le informazioni elaborate.

Il sistema è certificato secondo gli standard ISO/IEC 27001 e ISO/IEC 27701 e segue un approccio basato sulla privacy fin dalla progettazione. Supporta la conformità alle leggi sulla protezione dei dati sanitari e alle normative sulla sicurezza informatica applicabili nell'UE, negli Stati Uniti, nel Regno Unito, in Svizzera, in Brasile, negli Emirati Arabi Uniti, in Arabia Saudita, in Australia e in Nuova Zelanda.

Tuttavia, gli utenti devono adottare buone pratiche per evitare un'esposizione non necessaria dei dati sensibili.

- Evitare la condivisione di dati personali o sensibili, tranne quando è strettamente necessario.
- Assicurarci che tutte le comunicazioni e gli accessi ai sistemi avvengano in ambienti protetti.
- Se si sospetta un'attività fraudolenta, notificare immediatamente il team responsabile.

Sezione 4.2 - Protezione dei dati personali (conformità GDPR / HIPAA)

Il sistema **nCommand Lite** è conforme a tutte le leggi e normative applicabili in materia di privacy e protezione dei dati nelle regioni in cui opera, inclusi, a titolo esemplificativo ma non esaustivo, i requisiti GDPR, HIPAA, LGPD e ISO/IEC. Tutte le attività di elaborazione dei dati sono svolte sotto i ruoli "**Processor**" e "**Sub-Processor**" come definiti dal GDPR, con una rigida segregazione regionale dei dati per garantire la conformità e prevenire trasferimenti di dati transfrontalieri non autorizzati

Quali dati vengono raccolti?

- **Utenti:** Nome, email e azienda (solo per autenticazione e gestione degli accessi).
- **Dati del paziente:** Solo trasmissione degli esami medici tramite streaming in tempo reale, senza conservazione dei dati

Come vengono utilizzati e protetti i dati?

- I dati servono solo a scopi di **autenticazione, controllo degli accessi e tracciabilità delle sessioni**.
- La trasmissione delle informazioni è protetta tramite la **crittografia AES-256 per la conservazione e TLS 1.3 per i dati in transito**.
- **L'accesso è limitato** e segue il **principio del privilegio minimo (RBAC)**.
- Crittografia end-to-end garantita per i flussi video P2P e di controllo tramite WebRTC.
- I provider di servizi cloud autorizzati (ad esempio Microsoft Azure) elaborano dati limitati nel rispetto di rigide garanzie contrattuali.

Agli utenti vengono concessi i diritti seguenti:

- **Accesso e correzione** delle informazioni personali.
- **Richiesta di eliminazione dei dati**, ove applicabile.

In caso di domande, inviare un'e-mail al responsabile della protezione dei dati di Ionic Health all'indirizzo privacy@ionic.health. Tutte le richieste vengono gestite entro 30 giorni, prorogabili ai sensi del GDPR.

Sezione 4.3 - Gestione degli accessi e autenticazione

Gli utenti sono responsabili della definizione dei **ruoli e delle autorizzazioni di accesso** per i loro team, assicurando revisioni periodiche e documentazione degli accessi autorizzati.

Buone pratiche e controlli

- Seguire il **principio del minimo privilegio (RBAC)**, assicurandosi che gli utenti dispongano solo dell'accesso necessario.
- **L'autenticazione a più fattori (MFA)** è obbligatoria per l'accesso amministrativo e consigliata per tutti gli utenti.
- Sono richieste **password complesse**, composte da almeno **8 caratteri, comprese lettere maiuscole e minuscole, numeri e simboli**.
- **Non condividere le credenziali**.
- Le autorizzazioni di accesso vengono monitorate e riviste periodicamente.

Monitoraggio: L'accesso, le modifiche delle autorizzazioni e le attività importanti sono documentati nei registri di sicurezza del sistema. I registri vengono conservati per un minimo di 7 anni, in conformità con HIPAA, GDPR e altre normative applicabili. Supportano l'audit interno, l'analisi forense e la rendicontazione normativa. I registri sono protetti da manomissioni e conservati in ambienti sicuri con controllo degli accessi.

Sezione 4.4 - Controllo degli accessi a System Check

La funzione System Check è accessibile esclusivamente tramite l'**applicazione Web nCommand Lite** e richiede credenziali valide per l'accesso. L'accesso è consentito esclusivamente ai ruoli autorizzati — *Tecnologo da remoto, Tecnologo locale, Amministratore, Supervisore dei ruoli e Utente di system Check*.

Il ruolo di *Utente System Check* è progettato con permessi limitati, consentendo l'accesso esclusivamente a funzionalità diagnostiche relative alla validazione di rete e alla verifica della connettività. In questo modo si garantisce che i dettagli della rete, le informazioni di whitelist e le metriche di sistema non vengano mai resi pubblici a persone non autorizzate.

Tutte le richieste di accesso vengono autenticate tramite Azure AD B2C, con autenticazione a più fattori (MFA) e criteri di accesso condizionale adattivi gestiti da Microsoft Entra ID. La complessità della password è conforme ai criteri di sicurezza dell'organizzazione e richiede almeno otto caratteri, tra lettere maiuscole e minuscole, numeri e simboli. Le password scadono ogni 90 giorni e le sessioni si disconnettono automaticamente dopo 24 ore di inattività, estendibile fino a 90 giorni con utilizzo continuo.

Sezione 4.5 - Segregazione dei dati regionali e conservazione dei registri

La piattaforma **nCommand Lite** mantiene una rigorosa segregazione regionale dei dati per impedire trasferimenti transfrontalieri non autorizzati o non necessari. Gli ambienti sono isolati per regione, garantendo il rispetto delle normative vigenti.

Tutti i registri di accesso, i record delle attività e gli eventi di sicurezza vengono conservati per un minimo di sette (7) anni, in conformità con le normative applicabili in materia di protezione dei dati e di assistenza sanitaria. I registri vengono archiviati in ambienti sicuri, con accesso controllato e protetti da manomissioni. Queste informazioni supportano indagini forensi, audit di conformità e reporting normativo.

Sezione 4.6 - Sicurezza e integrità dei dati

Il sistema **nCommand Lite System** garantisce la riservatezza, l'integrità e la disponibilità dei dati tramite procedure di sicurezza standard del settore.

Gli utenti devono garantire la conformità con i protocolli di sicurezza, rivedere regolarmente le politiche di accesso e segnalare eventuali anomalie. Il sistema monitora costantemente le attività e gli amministratori devono applicare politiche di sicurezza per mantenere una difesa robusta contro le potenziali minacce.

Il sistema è protetto da un monitoraggio 24 ore su 24, 7 giorni su 7 tramite un Security Operations Center (SOC) dedicato con funzionalità SIEM per il rilevamento e la risposta alle minacce.

Sezione 4.7 - Risposta agli incidenti di sicurezza

Il sistema include un piano di risposta agli incidenti documentato, allineato con ISO 27035 e NIST CSF.

In caso di incidenti di sicurezza, come un accesso non autorizzato o un guasto di sistema, gli utenti devono seguire queste procedure:

Come identificare un incidente?

- **Accesso non autorizzato** rilevato nei registri delle attività.
- **Tentativi di accesso sospetti** o autenticazioni non riuscite ripetute.
- **Comportamento insolito del sistema**, come azioni impreviste o malfunzionamenti.

Come segnalare un incidente?

Registrare immediatamente l'evento tramite i canali di supporto disponibili (Capitolo 5).

Se viene confermata una violazione dei dati personali, IONIC, in qualità di sub-responsabile del trattamento, informerà GE in qualità di Responsabile del trattamento entro 48 ore, fornendo tutte le prove pertinenti, i dettagli sull'impatto e le misure di mitigazione. GE, a sua volta, è responsabile della notifica al Titolare del trattamento (il cliente) in conformità con i requisiti legali e contrattuali applicabili.

Capitolo 5 Canali di servizio

Per problemi tecnici, dubbi su una fase della procedura o ulteriori indicazioni, il nostro team sarà lieto di fornire l'assistenza necessaria. L'utente può contattarci telefonicamente, tramite e-mail o la piattaforma ITSM, in base allo strumento che ritiene più pratico. I nostri specialisti sono addestrati per offrire un'assistenza personalizzata, garantendo che ogni problema venga risolto in modo rapido ed efficiente.

Numeri di telefono

Stati Uniti	+1 (216) 2421223
Brasile	+55 12 3600 0181
Europa (Portogallo)	+351 (300) 528 410
Australia	+1 (216) 2421223
Nuova Zelanda	+1 (216) 2421223

Piattaforma ITSM

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

E-mail

helpdesk@ionic.health



AVVERTENZA!

Qualsiasi incidente grave correlato all'uso di questo dispositivo deve essere segnalato sia al fabbricante sia all'autorità sanitaria/autorità competente del luogo in cui è installato il dispositivo.

Per effettuare segnalazioni al fabbricante: contattare il rappresentante dell'assistenza della propria zona oppure scrivere un'e-mail all'indirizzo helpdesk@ionic.health
Fornire le seguenti informazioni:

- numero di versione del sistema, indicato nella schermata di accesso;
- data dell'incidente;
- descrizione dell'incidente, inclusi eventuali impatti/lesioni sul paziente o sull'utente;
- dati personali e di contatto (struttura, indirizzo, nome, titolo e numero di telefono).

Capitolo 6 Informazioni legali e normative

Produttore



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
Brasile

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

Tecnico responsabile

Alexandre Seiji Fukuda Ribas
CREA-SP: 5071085437

ANVISA

82585300004

Importatore (USA)



nCommand Lite System

IONIC HEALTH USA INC.

11201 Cedar Avenue, STE 600
Cleveland, OH 44106
USA

+1 (216) 242 1223

Rappresentante UE / Importatore



nCommand Lite



Numero di identificazione dell'organismo
notificato: 2803

EUROPE IONIC HEALTH DIGITAL TECHNOLOGIES, LDA

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

+351 (300) 528 410

Rappresentante autorizzato in Svizzera (CH-REP) / Importatore**CH REP****REF**

nCommand Lite

FREYR LIFE SCIENCES GMBH

Bahnhofplatz
CH-6300 Zug
Svizzera

Persona Responsabile / Importatore Regno Unito**REF**

nCommand Lite

FREYR LIFE SCIENCES LTD

9 Greyfriars Road
Reading, Berkshire
RG1 1NU
Inghilterra, Regno Unito

Sponsor australiano**REF**

nCommand Lite

TAEVAS LIFE SCIENCES PTY LTD

46 Dora St
Blacktown NSW 2148
Australia

Sponsor neozelandese**REF**

nCommand Lite

TAEVAS LIFE SCIENCES LIMITED

Livello 3, 1 Margaret Street
Lower Hutt 5010
Nuova Zelanda

UDI-DI di base: 7898974112NCLITE2L

Richiesta di copia cartacea

Le copie cartacee del Manuale d'uso del sistema nCommand Lite saranno fornite su richiesta senza costi aggiuntivi. Per ottenere una copia cartacea del Manuale d'uso, contattare il rappresentante locale.

Data di fabbricazione

La data di rilascio del software è visualizzata nella pagina di accesso di nCommand Lite, nel formato MESE/ANNO.

Capitolo 7 Cronologia delle Revisioni

Revisione	Descrizione della modifica	Data
0	Versione aggiornata del manuale da 2.3 v1 a 2.4	25 novembre 2025
1	Etichette del Capitolo 6 aggiornate	04 dicembre 2025
2	Rimosso il requisito di un indirizzo IP statico dalla configurazione del computer locale nella sottosezione 1.3.11 Aggiornato il simbolo del Rappresentante autorizzato UE nella sottosezione 1.3.12 Nota rimossa dalla sottovoce 1.3.14 Aggiornato il contenuto nel Capitolo 2 Aggiornato il simbolo del Rappresentante autorizzato UE nel Capitolo 6	28 gennaio 2026
3	È stata revisionata la traduzione di «Tecnico responsabile» nel Capitolo 6.	9 febbraio 2026

APPENDICE I - Lista di controllo per l'avvio della manutenzione

1. Verifica delle connessioni elettriche e di rete

Assicurarsi che le connessioni elettriche e i punti di rete siano stabiliti correttamente sul computer e-KVM, sul computer dello scanner e sul computer in locale.

2. Verifica dello stato di alimentazione

Verificare che il gruppo di continuità e il computer e-KVM siano accesi e funzionino correttamente.

3. Accesso rapido alla piattaforma nC Lite:

Verificare la presenza del tasto di scelta rapida della piattaforma nC Lite sul desktop per un rapido accesso.

4. Accesso e connessione alla piattaforma nC Lite:

Aprire la piattaforma nCommand ed effettuare l'autenticazione per ottenere l'accesso completo e garantire la corretta funzionalità del sistema.

5. Configurazione dell'applicazione della chat:

Aprire l'applicazione della chat all'interno della piattaforma nC Lite in una sola scheda e non ridurla a icona per evitare interruzioni nella comunicazione.