



BENUTZERHANDBUCH

nCommand Lite v2.4

Manuelle Version: V.3



Inhalt

Kapitel 1	Einführung	4
Abschnitt 1.1 -	Zweck	4
Abschnitt 1.2 -	Glossar	4
Abschnitt 1.3 -	Beschreibung	5
1.3.1.	Verwendungszweck	6
1.3.2.	Indikationen für die Verwendung	6
1.3.3.	Vorgesehene Patientenpopulation	6
1.3.4.	Anwendungsumgebung	6
1.3.5.	Kontraindikationen	6
1.3.6.	Plattformfähigkeiten	6
1.3.7.	Klinischer Nutzen	7
1.3.8.	Vorgesehene Benutzer	7
1.3.9.	Betriebsumgebung	8
1.3.10.	Umgebung der Einrichtung	8
1.3.11.	Mindestanforderungen	10
1.3.12.	Symbole	11
1.3.13.	Lebensdauer	12
1.3.14.	Aktualisierung/Upgrade	12
Kapitel 2	Liste der allgemeinen Warnhinweise und Vorsichtsmaßnahmen	13
Kapitel 3	Plattformnutzung am jeweiligen Standort	16
Abschnitt 3.1 -	Zugang und Verwendung von nCommand Lite	16
Abschnitt 3.2 -	Erstmaliger Zugriff auf die Plattform	16
3.2.1.	Anmeldung über nCommand Lite	17
3.2.2.	Anmeldung über einen External IdP	18
Abschnitt 3.3 -	Passwortverwaltung	20
Abschnitt 3.4 -	Zugriff mit dem Profil des Technologen vor Ort	23
Abschnitt 3.5 -	Zugriff mit Remote-Technologenprofil	25
3.5.1.	Zugriffsmodus	26
3.5.2.	Streaming-Leiste	29
3.5.3.	Multikamera	32
3.5.4.	Ein anderes Gerät öffnen	34
3.5.5.	Systemcheck	36

Abschnitt 3.6 - Chat	38
Abschnitt 3.7 - Beenden Ihrer Sitzung auf der Plattform	42
Abschnitt 3.8 - Betriebsschulung	44
Abschnitt 3.9 - Richtlinien zur Fehlerbehebung	45
Abschnitt 3.10 - Methoden zur Reinigung der Hardware	51
Kapitel 4 Cybersicherheit und Datenschutz	52
Abschnitt 4.1 - Sicherheits- und Datenschutzrisiken	52
Abschnitt 4.2 - Schutz personenbezogener Daten (Einhaltung von DSGVO / HIPAA)	52
Abschnitt 4.3 - Zugriffsverwaltung und Authentifizierung	53
Abschnitt 4.4 - Systemcheck-Zugriffskontrolle	53
Abschnitt 4.5 - Regionale Datentrennung und Logbuchaufbewahrung	54
Abschnitt 4.6 - Datensicherheit und -integrität	54
Abschnitt 4.7 - Reaktion auf Sicherheitsvorfälle	54
Kapitel 5 Servicekanäle	56
Kapitel 6 Rechtliche und regulatorische Informationen	57
Kapitel 7 Überarbeitungsverlauf	60
ANHANG I - Checkliste für den Wartungsbeginn	61

**VORSICHT**

Laut US-Bundesgesetz darf dieses Gerät nur von einem Arzt oder auf dessen Anordnung verkauft werden und muss von einem in dem Staat, in dem er praktiziert, zugelassenen Medizintechniker verwendet werden.

(für die Vereinigten Staaten von Amerika)

**VORSICHT**

In Brasilien ist diese Software von Anvisa ausschließlich zur Verwendung mit Magnetresonanztomographen (MRT) zugelassen. Eine andere Verwendung ist nicht gestattet.

(Für die Verwendung in Brasilien)

**VORSICHT**

Stellen Sie vor der Verwendung sicher, dass Sie die spezifischen Anforderungen Ihres Landes oder Ihrer Region kennen. Die Nichteinhaltung von Vorschriften kann zu Gesundheitsrisiken führen.

**VORSICHT**

Stellen Sie sicher, dass die Version dieses Benutzerhandbuchs mit der Version der verwendeten Plattform übereinstimmt. Die Verwendung einer nicht übereinstimmenden Version kann zu Fehlfunktionen oder Fehlinterpretationen von Funktionen führen.

Kapitel 1 Einführung

Abschnitt 1.1 - Zweck

Dieses Handbuch soll Technologen vor Ort und Remote-Technologen ein umfassendes Verständnis der spezifischen Funktionen des nCommand Lite Systems vermitteln. Dieses Dokument dient als Benutzerhandbuch und vermittelt präzise und praktische Informationen, die den Benutzer durch die Funktionen des Systems und die Fehlerbehebung führen. Durch Befolgung dieses Handbuchs können Benutzer nCommand Lite effizient verwenden, was zur Maximierung der Produktivität und Reduzierung der Abhängigkeit vom technischen Support beiträgt.

Abschnitt 1.2 - Glossar

**VORSICHT**

Dieses Etikett gilt für Bedingungen oder Maßnahmen, die eine potenzielle Gefahr darstellen. Sie können leichte Verletzungen oder Sachschäden verursachen, wenn Sie diese Anweisungen ignorieren.

**WARNUNG**

Dieses Etikett weist auf Bedingungen oder Maßnahmen hin, die zu einer bestimmten Gefahr führen. Sie können schwere Verletzungen oder erhebliche Sachschäden verursachen, wenn Sie diese Anweisungen ignorieren.

Nutzungsbedingungen der Plattform	Entsprechender Begriff
Bildgebungseinrichtung	Medizinische Einrichtung, Gerät, Mobile Geräte, Gesundheitseinrichtung, Gesundheitsgerät
Remote-Einrichtung	Ferncomputer, Remote-Ort, Remote-Büro, Remote-Standort, Command Center
Plattform	nCommand Lite Webanwendung
System	nCommand Lite mit allen Subsystemen
Gerät	Medizinischer Scanner, Scanner, Ausrüstung, Medizinisches Gerät, Bildgebungsgerät, Bildgebende Ausrüstung
Technologie vor Ort	Benutzer vor Ort, Technologie vor Ort, Medizinisches Fachpersonal vor Ort (Local Healthcare Professional oder LHP), Benutzer in der Einrichtung

Abschnitt 1.3 - Beschreibung

Das nCommand Lite System ist eine SaMD (Software as a Medical Device – Software als Medizinprodukt), die kundennah ist und Fernzugriff über eine Webanwendung zur Anzeige/Überprüfung von Bildern bietet sowie die Möglichkeit, dem patientennahen lizenzierten Technologen (Benutzer vor Ort), der die medizinischen Bildgebungsgeräte im Rahmen von Schulungen oder Verfahrensbeurteilungen bedient, aus der Ferne Echtzeitanweisungen für MRT-, CT- und PET/CT-Scanner zu geben.

Remote-Benutzer sind lizenzierte Technologen, die von einem Computer aus auf ein medizinisches Bildgebungsgerät zugreifen können, das die erforderlichen Mindestspezifikationen an jedem beliebigen Ort erfüllt, indem sie eine sichere Softwareverbindung verwenden, die Videos streamt und Tastatur- und Mauszugriff bietet. Dies ermöglicht Remote-Benutzern, Benutzer vor Ort zu unterstützen, ohne dass die Entfernung eine Einschränkung darstellt. Dieser Zugriff muss vom Benutzer vor Ort, der das System verwendet, gewährt werden und kann auch jederzeit vom Benutzer vor Ort widerrufen werden, sodass er jederzeit die vollständige Kontrolle über die Sitzung behalten kann. Außerdem wird jede Remote-Sitzung über sichere Anmeldedaten gesteuert, die vom Benutzer vor Ort verwaltet werden. Die Verbindungen zu einem Medizinprodukt sind auf jeweils eine gleichzeitige Remote-Sitzung beschränkt, um eine strenge Kontrolle darüber zu behalten, wer mit dem System aus der Ferne interagiert. Aus der Ferne überprüfte Bilder sind nicht für diagnostische Zwecke bestimmt.

Das nCommand Lite System besteht aus einer IT-Hardware- und softwarebasierten Installationslösung, die Mehrfachsitzungen unterstützt, so dass Remote-Technologen bei Bedarf auf mehrere medizinische Bildgebungsgeräte zugreifen können. Scanner, die mit dem nCommand Lite System kompatibel sind, entsprechen einem gängigen Protokoll, das das Scannen von Parametern und das Scannen aus der Ferne ermöglicht.

1.3.1. Verwendungszweck

Das nCommand Lite-System bietet Fernzugriff zum Anzeigen/Prüfen von Bildern sowie die Möglichkeit, dem lizenzierten Technologen, der den Scanner bedient, eine Echtzeit-Anleitung zu bieten. Diese Anleitung umfasst Schulung, Beurteilung des Verfahrens und Verwaltung der Scanparameter.

1.3.2. Indikationen für die Verwendung

Das nCommand Lite-System ermöglicht den Fernzugriff zum Anzeigen/Prüfen von Bildern sowie die Möglichkeit, dem lizenzierten Technologen, der einen kompatiblen MRT-, CT- oder PET/CT-Scanner bedient, eine Echtzeit-Anleitung zu bieten. Dieser Zugriff muss vom lizenzierten Technologen vor Ort gewährt werden, der das System bedient. Der Fernzugriff ist nur für Systeme verfügbar, die Remote-Konnektivität unterstützen. Aus der Ferne überprüfte Bilder sind nicht für diagnostische Zwecke bestimmt.

1.3.3. Vorgesehene Patientenpopulation

Für jeden Patienten, dem eine Bildgebung über ein angeschlossenes Bildgebungs-Medizinprodukt verordnet wurde.

1.3.4. Anwendungsumgebung

Bildgebende Einrichtungen, die Magnetresonanztomographie (MRT), Computertomographie (CT) und Positronen-Emissionstomographie – Computertomographie (PET/CT)-Untersuchungen durchführen, sowie Remote-Command-Center.

1.3.5. Kontraindikationen

Die Plattform darf nicht von Benutzern bedient werden, die keine zugelassenen Technologen sind und keine Schulung in der Verwendung von nCommand Lite erhalten haben.

1.3.6. Plattformfähigkeiten

- **Remote Scanning:** Zeigt den Bildschirm des medizinischen Bildgebungsgeräts in Echtzeit an, sodass ein lizenzierter Technologe aus der Ferne an einer Untersuchung teilnehmen kann.
- **Chat:** Ermöglicht die Kommunikation zwischen dem lizenzierten Remote-Technologen und dem lizenzierten Technologen vor Ort über Text- und Sprachnachrichten. Die Technologen vor Ort und Remote-Technologen können auch Sprach- und Videoanrufe tätigen und empfangen.
- **Multikamera:** Erleichtert die Fernüberwachung von Patienten und der medizinischen Einrichtung während des Eingriffs. Der Remote-Technologe kann auf die Ansicht der Kameras über die Registerkarten zugreifen, die zwischen allen Kamera-Registerkarten und den einzelnen Registerkarten unterteilt sind. Dieser Mechanismus repliziert die visuelle Kontrolle, die ein Angehöriger der Gesundheitsberufe haben würde, wenn er sich in der Nähe des Patienten befindet, und führt so zu einer zusätzlichen Sicherheitsebene.
- **Das Multisession-Remote-Scanning (Remote-Scannen mit mehreren Sitzungen)** ermöglicht es dem Remote-Technologen, nach Bedarf auf mehrere medizinische Bildgebungsgeräte zuzugreifen.
- **Zugriffsmodus:** Ermöglicht dem Remote-Technologen die Auswahl zwischen Ansichten oder die Steuerung des Geräts. Im Modus „Anzeigen“ können Remote-Technologen nur

sehen, was gerade gestreamt wird. Im Modus „Steuern“ hat er die Kontrolle über Maus und Tastatur.

- **Remote-Technologenzugriff verwalten:** Ermöglicht es dem Technologen vor Ort, den Remote-Technologenzugriff und seinen Zugriffsmodus (View (Anzeigen) oder Control (Steuern)) zu steuern. Um die Verbindung des Remote-Technologen zu ermöglichen, muss der Technologie vor Ort, der die Plattform verwendet, Zugriff gewähren, und dieser kann auch jederzeit vom Technologen vor Ort widerrufen werden, sodass dieser jederzeit die vollständige Kontrolle über die Sitzung behalten kann.
- **Streaming-Größe:** Der Remote-Technologie kann die Original-Streaming-Größe und die aktuelle Streaming-Größe in Pixeln sehen. Er wird auch benachrichtigt, wenn die aktuelle Streaming-Größe kleiner ist als die Originalgröße.
- **Maus- und Tastaturstatus:** Der Remote-Technologie hat Feedback darüber, ob Maus und Tastatur des medizinischen Bildgebungsgeräts korrekt funktionieren.
- **Sitzungsdetails:** Technologen vor Ort und Remote-Technologen können auf Details zur Sitzung zugreifen.

1.3.7. Klinischer Nutzen

nCommand Lite verbessert die diagnostische Bildgebung, indem es den Fernbetrieb von **MRT-, CT- und PET-CT-**Systemen ermöglicht und so eine gleichbleibende Bildqualität und Einhaltung von Protokollen gewährleistet. Es ermöglicht erfahrenen Technologen, Scans in Echtzeit zu überwachen und zu unterstützen, wodurch die Effizienz des Arbeitsablaufs optimiert und Fehler reduziert werden, die die diagnostische Genauigkeit beeinträchtigen könnten. Das System erleichtert die Zusammenarbeit zwischen den Technologen, verbessert die Konsistenz der Untersuchung und ermöglicht eine schnellere Entscheidungsfindung in komplexen Fällen. Durch die Möglichkeit für externe Fachkräfte, mehrere Einrichtungen zu unterstützen, erhöht **nCommand Lite** die **Verfügbarkeit, Vielfalt und Qualität** von bildgebenden Untersuchungen und stellt sicher, dass mehr Patienten Zugang zu fortschrittlicher Diagnostik haben und gleichzeitig die Ressourcen des Gesundheitswesens optimiert werden. Darüber hinaus trägt es dazu bei, Personalmangel zu mindern, indem es die Abhängigkeit von Spezialisten vor Ort reduziert und gleichzeitig die Einhaltung strenger regulatorischer und Datensicherheitsstandards aufrechterhält.

1.3.8. Vorgesehene Benutzer

- **Technologie vor Ort**
Der Technologie vor Ort ist der Benutzer in der Einrichtung, der für die persönliche Unterstützung und Anleitung von Patienten in der medizinischen Einrichtung verantwortlich ist. Er muss über die erforderlichen Kenntnisse verfügen, um Scanverfahren für ein bestimmtes Bildgebungssystem durchzuführen. Darüber hinaus steuert er den Zugriffsmodus des Remote-Technologen (Anzeigen oder Steuern), und der Remote-Zugriff muss vom Technologen vor Ort über die Plattform gewährt werden und kann jederzeit widerrufen werden.
- **Remote-Technologie**
Eine Fachkraft, die Vorgänge aus der Ferne durchführt und dabei Zugriff auf den Gerätecomputer hat und diesen kontrolliert. Ebenso wie der Technologie vor Ort muss auch der Remote-Technologie über die erforderlichen Kenntnisse verfügen, um Scanverfahren für ein bestimmtes Bildgebungssystem durchzuführen.

- **Support-/IT-Benutzer**

Für die Einrichtung der Plattform verantwortlicher Experte (nicht in diesem Benutzerhandbuch enthalten).

1.3.9. Betriebsumgebung

Die folgenden Spezifikationen beziehen sich auf die Umgebungsbedingungen des e-KVM-Computers.

- **Maximale Höhe (ohne Druckausgleich)**
 - Betrieb: Von 0 m (0 Fuß) bis 3048 m (10.000 Fuß)
 - Speicher: Von 0 m (0 Fuß) bis 12.192 m (40.000 Fuß)
- **Temperatur**
 - Betrieb: Von 10 °C (50 °F) bis 35 °C (95 °F)
 - Speicher: Von -10 °C (14 °F) bis 50 °C (122 °F)
- **Relative Luftfeuchtigkeit**
 - Betrieb: 20 %–80 % (nicht kondensierend)
 - Speicher: 10 %–90 % (nicht kondensierend)

1.3.10. Umgebung der Einrichtung

Die nCommand Lite-Plattform verfügt über zwei verschiedene Umgebungsstandorttypen:

- **Bildgebungseinrichtung:** Einrichtungen, die Untersuchungen mittels Magnetresonanztomographie (MRT), Computertomographie (CT) oder Positronen-Emissionstomographie – Computertomographie (PET/CT) durchführen.
- **Remote-Einrichtung:** Ein Ort, an dem Remote-Technologen aus der Ferne auf Geräte (MRT-, CT- oder PET/CT-Scanner) zugreifen und diese remote verwalten können. Dieser Ferncomputer kann in verschiedenen Umgebungen wie Büros, Command Centern, Remote-Standorten oder sogar sekundären Standorten innerhalb der Gesundheitseinrichtung eingesetzt werden. Der Ferncomputer kann sich an einem beliebigen Ort befinden, der dem Benutzer geeignete Bedingungen für die konzentrierte Tätigkeit und ein Mindestmaß an Konnektivität sowie Anforderungen an die Computerkonfiguration bietet.

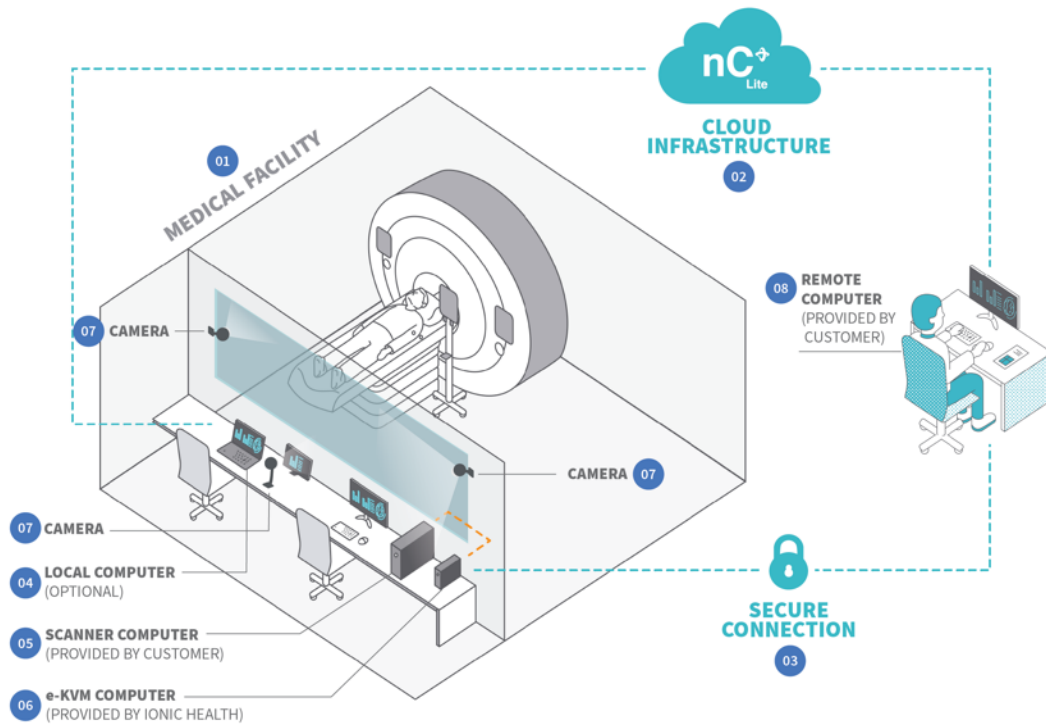


Abbildung 01: Übersicht über das Produkt und seine Verbindungen über eine sichere Verbindung (z. B. VPN).

- 01 – Medizinische Einrichtung; 02 – Cloud-Infrastruktur; 03 – Sichere Verbindung; 04 – Lokaler Computer (optional);
 05 – Scanner-Computer (bereitgestellt vom Kunden); 06 – e-KVM (bereitgestellt von IONIC Health);
 07 – Kamera; 08 – Remote-Computer (vom Kunden bereitgestellt)



WARNUNG!

Kompatibilität mit Remote-Scanning

IONIC Health (IH) validiert die Remote-Scanning-Funktionalität auf den aufgelisteten kompatiblen Geräten. IH führt eine vollständige Bewertung der Anforderungen an das IH-Remote-Scanning durch und testet das System während der Installation in der Zielumgebung. Dies gewährleistet Kompatibilität und ordnungsgemäße Leistung zu diesem Zeitpunkt für das Remote-Scanning. Diese Überprüfung bedeutet nicht, dass alle Herstelleranforderungen an das Gerät in dieser Konfiguration erfüllt werden. Jede Abweichung von den Herstelleranforderungen liegt in der Verantwortung des Endnutzers.

Änderungen am System oder an der Umgebung nach der Installation müssen an IH gemeldet werden, um die fortgesetzte Kompatibilität zu überprüfen. IH kann keine Garantie für die Leistung oder Verantwortung für Konfigurationen übernehmen, die von den während der Installation validierten abweichen.

1.3.11. Mindestanforderungen

- **Lokaler Computer**

Dieser Computer wird vom **Technologen vor Ort** verwendet, um den Fernzugriff auf das Gerät über nCommand Lite® zu autorisieren und zu unterstützen. Er ermöglicht auch die direkte Kommunikation mit dem **Remote-Technologen** über die Chat-Funktion auf der Plattform.

Die technischen Mindestanforderungen sind:

- Prozessor: AMD® A4-9120C oder höher, oder ähnlich
- Arbeitsspeicher: 4 GB oder höher
- Speicher: 128 GB SSD oder höher
- Peripheriegeräte: Mikrofon und Lautsprecher oder Headset und Webcam
- Monitor: 14" FHD (1920 x 1080) oder höher
- Betriebssystem: Chrome OS, Windows OS oder MAC OS
- Installationsort: Dieser Computer muss sich in der Nähe des Scannercomputers befinden
- IT-Routine: Erstellen Sie eine nCommand Lite-Verknüpfung auf dem Desktop jedes Benutzers
- Browser-Kompatibilität: Google Chrome oder Microsoft Edge.

- **Ferncomputer**

Dieser Computer wird vom **Remote-Technologen** verwendet, um über nCommand Lite® auf das Gerät zuzugreifen und es zu steuern. Der Ferncomputer muss eine sichere Verbindung zum e-KVM-Computer (von IONIC HEALTH® bereitgestellt) herstellen.

Der Kunde ist für die Bereitstellung des Ferncomputers verantwortlich und kann sich für eines von zwei Szenarien entscheiden: Das erste ist ein 24/7-Betrieb, das zweite ein Betrieb während der Geschäftszeiten.

Für jedes Szenario finden Sie im Folgenden die richtigen Spezifikationen für die Auswahl der Computermodelle:

Szenario 1 (Betrieb rund um die Uhr) – Muss die folgenden Spezifikationen erfüllen:

- Intel Xeon W-2223 (4 Cores, 8 Threads, 8,25 MB Cache, 3,90 GHz Turbo) oder höher.
- RAM: 16 GB oder höher.
- Graphik: NVIDIA RTX A2000 6 GB oder höher, oder ähnlich.
- Speicher: 128 GB SSD oder höher.
- Betriebssystem: Windows 11 Pro 64B oder höher.
- Mindestanforderungen an den Monitor: Größe 27 Zoll, Seitenverhältnis 16:9, Auflösung 4k.
- Headset: BLACKWIRE 3200 oder ähnlich.
- Browser-Kompatibilität: Google Chrome oder Microsoft Edge.

Szenario 2 (Betrieb während der Geschäftszeiten) – Muss die folgenden Spezifikationen erfüllen:

- Intel® Core™ i7-12700k vPro® oder höher.
- RAM: 16 GB oder höher.

- Graphik: NVIDIA T400 GB oder höher, oder ähnlich.
- Speicher: 128 GB SSD oder höher.
- Betriebssystem: Windows 11 Pro 64B oder höher.
- Mindestanforderungen an den Monitor: Größe 27 Zoll, Seitenverhältnis 16:9, Auflösung 4k.
- Headset: BLACKWIRE 3200 oder ähnlich.
- Browser-Kompatibilität: Google Chrome oder Microsoft Edge.

**WARNUNG!**

Die Nichteinhaltung der entsprechenden Einrichtung und Mindestanforderungen kann zu einer beeinträchtigten oder fehlgeschlagenen Kommunikation zwischen Benutzern führen.

- **Netzwerkkonfigurationen (Mindestanforderungen)**

Um die Sitzung zwischen dem Remote-Benutzer und dem e-KVM-Computer herzustellen, muss die Netzwerkkommunikation zwischen den beiden Geräten gewährleistet sein. Das nCommand Lite-System verwendet Peer-zu-Peer (P2P), um eine Verbindung zwischen lokalem Benutzer, Fernbenutzer und e-KVM-Computer herzustellen. Es gibt drei kompatible Szenarien:

- **Szenario 1** – Unternehmensnetzwerk, das eines der folgenden Protokolle verwendet: LAN, LAN-zu-LAN, MPLS oder VPN;
- **Szenario 2** – Unternehmensnetzwerk, das ein vertrauenswürdigen WAN (externes Netzwerk) verwendet und keines der folgenden Protokolle verwendet: LAN, LAN-zu-LAN, MPLS oder VPN;
- **Szenario 3** – Öffentliches Netzwerk auf der Seite des Ferncomputers (Remote-Benutzer).

Die Konfigurationen für jedes Szenario sind in der technischen Dokumentation detailliert beschrieben.

1.3.12. Symbole

Symbol	Beschreibung	Referenz
	Hersteller	ISO 15223-1, ISO 7000-3082
	Herstellungsdatum	ISO 15223-1, ISO 7000-2497
	Das Symbol bedeutet, dass es sich bei diesem Produkt um ein Medizinprodukt handelt	ISO 15223-1
	Eindeutige Produktkennung	ISO 15223-1
	Modellreferenz	ISO 15223-1, ISO 7000-2493

	Importeur	ISO 15223-1, ISO 7000-3725
	Benutzerhandbuch hinzuziehen	ISO 15223-1, ISO 7000-1641
	Händler	ISO 15223-1, ISO 7000-3724
	Vorsicht	ISO 15223-1, ISO 7000-0434A
	Warnung	ISO 7010-W001
	Seriennummer (oder Softwareversion)	ISO 15223-1, ISO 7000-2498
	Bevollmächtigter Vertreter in der Europäischen Gemeinschaft	ISO 15223-1
	Bevollmächtigter Vertreter in der Schweiz (CH-REP)	ISO 15223-1
	CE – Europäische Konformitätskennzeichnung; 2803 – Bezeichnung der benannten Stelle	EU-Verordnung 2017/745

1.3.13. Lebensdauer

Die erwartete Lebensdauer des Produkts beträgt 5 Jahre, unter Berücksichtigung der Nutzungsdauer der Komponenten, aus denen das Produkt besteht. Diese umfassende Bewertung stellt sicher, dass die Lebensdauer jeder kritischen Komponente mit der gesamten Lebensdauer übereinstimmt, und gewährleistet eine gleichbleibende Leistung und Zuverlässigkeit während der gesamten vorgesehenen Produktlebensdauer.

1.3.14. Aktualisierung/Upgrade

IONIC Health aktualisiert das nCommand Lite-System im Rahmen geplanter Wartungs- oder Upgrade-Versionen. Diese Updates sollen die kontinuierliche Leistung und Zuverlässigkeit gewährleisten, ohne die derzeit bei den Kunden eingesetzte Version zu beeinträchtigen. Je nach Art des Updates kann das Produkt per Fernzugriff aktualisiert werden oder ein Vor-Ort-Besuch eines Außendiensttechnikers erforderlich sein.

Kapitel 2 Liste der allgemeinen Warnhinweise und Vorsichtsmaßnahmen



WARNUNG!

Bitte lesen Sie alle nachstehenden Warnhinweise, bevor Sie das nCommand Lite-System verwenden.



VORSICHT

Das nCommand Lite System kann nicht repariert oder gewartet werden, während es zur Steuerung eines MRT-, CT- oder PET-CT-Geräts in Anwesenheit eines Patienten verwendet wird.

- Achten Sie genau auf alle Systemwarnungen, da diese für einen sicheren Betrieb von entscheidender Bedeutung sind.
- Sicherheit und Aufmerksamkeit haben bei allen Einsätzen oberste Priorität.
- Ein US-Bundesgesetz beschränkt den Verkauf dieses Geräts auf den Verkauf durch oder auf Anordnung eines Arztes, wie er von medizinischen Technologen verwendet wird, die in dem Staat zugelassen sind, in dem er/sie praktiziert.
- Das nCommand Lite System darf nur von Technolgen verwendet werden, die in der Verwendung der Plattform geschult wurden.
- Verwenden Sie dieses System nur mit kompatiblen Webbrowsern. Unterstützte Browser sind Google Chrome und Microsoft Edge.
- Im Notfall muss ein geschulter, lizenzierter Technologe in der Bildgebungseinrichtung bleiben, um die MRT-, CT- oder PET/CT-Operation ohne nCommand Lite durchzuführen.
- Der gleichzeitige Zugriff auf mehrere Geräte erfordert höchste Konzentration und Kommunikation mit den Teams vor Ort.
- Vermeiden Sie den gleichzeitigen Zugriff auf Geräte mit identischen Layouts oder gleichzeitige Untersuchungen derselben anatomischen Region.
- Sie können mehrere Bildschirme anzeigen, die Steuerung ist jedoch auf jeweils ein Gerät beschränkt.
- Starten Sie immer einen Chat, wenn Sie mit einem Gerät verbunden sind, um eine klare Kommunikation zu gewährleisten.
- Auf dem zugehörigen Gerätebildschirm werden Anrufwarnungen angezeigt; es kann jeweils nur ein Anruf aktiv sein.
- Testen Sie die Videokommunikation beim Zugriff auf die Anwendung (vor Beginn einer Arbeitssitzung), um zu prüfen, ob der Videoausgangsanschluss der MRT-, CT- oder PET/CT-Geräte oder eines anderen Geräts das mit dem Videostreaming verbunden ist, gestört ist.
- Das Gerät darf nicht über Verlängerungskabel oder „Steckerleisten“ an die Steckdose und/oder das unterbrechungsfreie und stabilisierte Netzteil angeschlossen werden.
- Wenn Videofehler auftreten, überprüfen Sie die Videoverbindung zwischen dem Gerätesystem und dem e-KVM-Computer.
- Wenn die Anwendung im Fernzugriff nur langsam verfügbar ist, aktualisieren Sie die Seite mit den Befehlen Strg+F5 im Browser des Remote-Technologen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

- Wenn die Browserseite aktualisiert wird, wird die Verbindung zum Gerät unterbrochen, sodass der Genehmigungsprozess erneut durchgeführt werden muss.
- Melden Sie sich nicht mit einem anderen Browser an, wenn Sie bereits angemeldet sind.
- Die Bildgebungseinrichtung des Kunden muss über eine redundante Internetverbindung mit einem anderen Anbieter als der Hauptanbieter verfügen, um im Falle eines Verlusts der System-/Plattformkommunikation sofort Änderungen vornehmen zu können.
- Führen Sie im Falle eines Kommunikationsverlusts oder einer Verlangsamung der Maus auf der im Browser verwendeten Seite eine „erneute Maussynchronisation“ durch.
- Stellen Sie sicher, dass die für die Steuerung des nCommand Lite Systems verwendeten Computer sowohl in der Bildgebungseinrichtung als auch im Command Center die Mindestanforderungen erfüllen; andernfalls kann es zu einem Verlust der Anwendungsleistung kommen.
- QoS (Quality of Service – Service-Qualität) sollte auf den Hauptlink und den redundanten Link für die Übertragung der Plattform angewendet und die Leistung des Links überwacht werden.
- Überprüfen Sie vor der Verwendung die Lautstärke von Audio und Mikrofon sowie die Audio- und Mikrofonberechtigung im Webbrowser.
- Überprüfen Sie vor der Verwendung die Funktion von Tastatur und Maus. Wenn sie langsam oder nicht synchronisiert sind, aktivieren Sie die Schaltfläche „mouse resync“ (Maus neu synchronisieren). Überprüfen Sie, ob der e-KVM-Computer angeschlossen und eingeschaltet ist.
- Stellen Sie sicher, dass das Tastaturlayout an der Remote-Einrichtung mit dem Tastaturlayout an der Bildgebungseinrichtung identisch ist.
- Wenn der Ort, an dem die Plattform verwendet wird, geändert werden muss, muss der Kunde den technischen Support anrufen, um eine Neuinstallation vorzunehmen. Nicht erneut installieren, ohne den technischen Support zu kontaktieren.
- Vor Beginn des Fernzugriffs auf das MRT-, CT- oder PET/CT-Gerät ist es wichtig, dass die Teams der Technolgen alle für die ordnungsgemäße Leistung der Plattform erforderlichen Elemente überprüfen, um die Untersuchung nicht zu behindern. Diese Punkte sind in dem Dokument „Checkliste für den Servicestart“ aufgeführt.
- Die Firewall-Konfiguration der Bildgebungseinrichtung muss monatlich mit dem IT-Team überprüft werden und sicherstellen, dass keine Probleme mit der Firewall-Version vorliegen, die die Verwendung von nCommand Lite beeinträchtigen könnten.
- Jede Anomalie, die bei der Nutzung der Anwendung beobachtet wird, muss dem Support-Team sofort gemeldet werden, bevor der Zugriff gestartet oder abgebrochen wird, wenn er bereits begonnen hat.
- Die Anwendung darf nur von zugelassenen Technolgen bedient werden, die in der Verwendung des nCommand Lite geschult sind.
- Der Fernzugriff über die Plattform ersetzt oder konkurriert nicht mit anderen Betriebsverfahren für den MRT-, CT- oder PET/CT-Betrieb, die vom Hersteller des Medizinprodukts und den Protokollen und Verfahren der Pflegeeinrichtung festgelegt wurden.
- Biegen oder Dehnen der Hardwarekabel vermeiden.
- Wenn Probleme mit der Sprach- oder Chat-Kommunikation auftreten, verwenden Sie die Anruffunktion, um die Kommunikation zwischen dem Technolgen vor Ort an der Bildgebungseinrichtung und dem Remote-Technologen am Command Center herzustellen. Befolgen Sie die Anweisungen im Abschnitt „Richtlinien im Fehlerfall“ und wenden Sie sich bei Bedarf an den technischen Support, um die Reparatur durchzuführen.

- Wenn ein Computer oder ein anderes Gerät ausgetauscht werden muss, das die Installation von nCommand Lite direkt beeinflusst, aktivieren Sie den technischen Support und gewährleisten so den Erhalt des Systembetriebs.
- Es kann jeweils nur eine Person aus der Ferne auf das MRT-, CT- oder PET/CT-Gerät zugreifen.
- Berühren Sie keine physischen Videokabel, während der Gerätecomputer und das nCommand Lite System eingeschaltet sind.
- Beim Zugriff auf ein zusätzliches Gerät öffnet sich eine neue Registerkarte. Ziehen Sie diese Registerkarte auf einen zweiten Monitor, da das System für die Verwendung mit einem separaten Bildschirm für jedes Gerät vorgesehen ist.
- Jeder schwerwiegende Vorfall im Zusammenhang mit der Verwendung dieses Geräts sollte sowohl dem Hersteller als auch der Gesundheitsbehörde/zuständigen Behörde, bei der das Gerät installiert ist, gemeldet werden (*weitere Einzelheiten finden Sie im Kapitel Servicekanäle*).

Kapitel 3 Plattformnutzung am jeweiligen Standort

Abschnitt 3.1 - Zugang und Verwendung von nCommand Lite

**WARNUNG!**

Wenden Sie sich bei Problemen bitte an den technischen Support.

**WARNUNG!**

Überprüfen Sie das Tastaturlayout und stellen Sie sicher, dass es an beiden Orten identisch ist (medizinische Einrichtung und Remote-Einrichtung). Verschiedene Tastaturlayouts können die Benutzererfahrung beeinträchtigen.

In diesem Kapitel finden Sie alles, was Sie wissen müssen, um auf die nCommand Lite-Plattform zuzugreifen und sie zu verwenden. Hier finden Sie klare Schritt-für-Schritt-Anleitungen, um sich anzumelden, in der Benutzeroberfläche zu navigieren und die Hauptfunktionen zu verstehen. Mithilfe dieses Leitfadens können Sie schnell und sicher mit der Arbeit beginnen, unabhängig davon, ob Sie vor Ort oder aus der Ferne arbeiten.

Ändern der Sprache – Das System ist standardmäßig auf Englisch voreingestellt, aber Sie können die Sprache ganz einfach entsprechend Ihren Präferenzen ändern. Klicken Sie auf dem Anmeldebildschirm auf die obere rechte Ecke, in der „English (en-US)“ (Englisch (en-US)) angezeigt wird. Dadurch wird eine Dropdown-Liste mit verfügbaren Sprachen geöffnet, aus der Sie auswählen können.

Nach dem Anmelden können Sie auch die Sprache ändern, indem Sie auf die aktuell ausgewählte Sprache auf der rechten Seite der oberen Leiste klicken. Dadurch wird eine Dropdown-Liste mit verfügbaren Sprachen geöffnet, aus der Sie auswählen können.

Bitte beachten Sie, dass die aktuelle Verbindung automatisch beendet wird, wenn Sie die Sprache ändern, während Sie mit einem Gerät verbunden sind, und Sie eine erneute Verbindung herstellen müssen.

Beim Zugriff auf die Plattform können Sie auf dem Anmeldebildschirm Ihre bevorzugte Sprache auswählen. Einige Meldungen, die während des Anmeldevorgangs angezeigt werden, können jedoch in der Sprache angezeigt werden, die in Ihrem Webbrowser eingestellt ist, unabhängig von der auf der Plattform ausgewählten Sprache. Für ein einheitliches Erlebnis empfehlen wir Ihnen, die Spracheinstellungen Ihres Browsers mit der von Ihnen bevorzugten Plattformsprache abzustimmen.

Abschnitt 3.2 - Erstmaliger Zugriff auf die Plattform

Der Anmeldevorgang auf der Plattform kann auf zwei Arten erfolgen: über nCommand Lite oder über einen External Identity Provider (External IdP). Der Benutzer kann sich mit einer der

vorkonfigurierten Methoden anmelden. Wenn es sich bei der konfigurierten Methode um den externen Identitätsanbieter (External IdP) handelt, funktioniert die nCommand Lite-Methode nicht; dies gilt auch im umgekehrten Fall. Um sich über den External IdP anzumelden, gehen Sie direkt zum **Unterabschnitt 3.2.2**.

3.2.1. Anmeldung über nCommand Lite

Hinweis: Dieser Abschnitt gilt nicht für Benutzer, die sich über einen External Identity Provider (External IdP) anmelden.

Schalten Sie den Computer ein und doppelklicken Sie auf das Verknüpfungssymbol nCommand Lite, das sich normalerweise auf dem Desktop befindet. Sie können auch direkt im Browser auf die URL zugreifen.

Ihr erster Zugriff ist ein entscheidender Schritt, um mit der sicheren und effizienten Nutzung der Plattform zu beginnen. Hier ist, was Sie wissen müssen:

1 – Willkommens-E-Mail: Sie erhalten eine E-Mail mit Ihren Anmeldedaten, einschließlich Ihrer zugehörigen persönlichen E-Mail, einem temporären Passwort und einem direkten Link zur Client-Plattform. Diese E-Mail ist entscheidend, um mit der Verwendung von nCommand Lite zu beginnen.

2 – Passwörterstellung: Wenn Sie auf den Link zugreifen, müssen Sie Ihre zugehörige E-Mail-Adresse und das in der Willkommens-E-Mail erhaltene Passwort eingeben. Wenn Sie auf „Sign in“ (Anmelden) klicken, gelangen Sie zu einer Seite, auf der Sie ein neues Passwort erstellen können. Sie müssen das alte Passwort, das neue Passwort und die Bestätigung des neuen Passworts eingeben. Dieses muss stark und sicher sein, und mindestens 3 der folgenden Elemente enthalten: ein Kleinbuchstabe, ein Großbuchstabe, eine Zahl und ein Symbol, und es muss mindestens 8 Zeichen lang sein. Wenn Sie auf „Continue“ (Weiter) klicken, werden Sie zu einer Seite weitergeleitet, um Ihre E-Mail erneut zu bestätigen. Wenn Sie auf „Continue“ (Weiter) klicken, werden Sie nun zum Startbildschirm weitergeleitet, der an Ihr spezifisches Benutzerprofil angepasst wird.

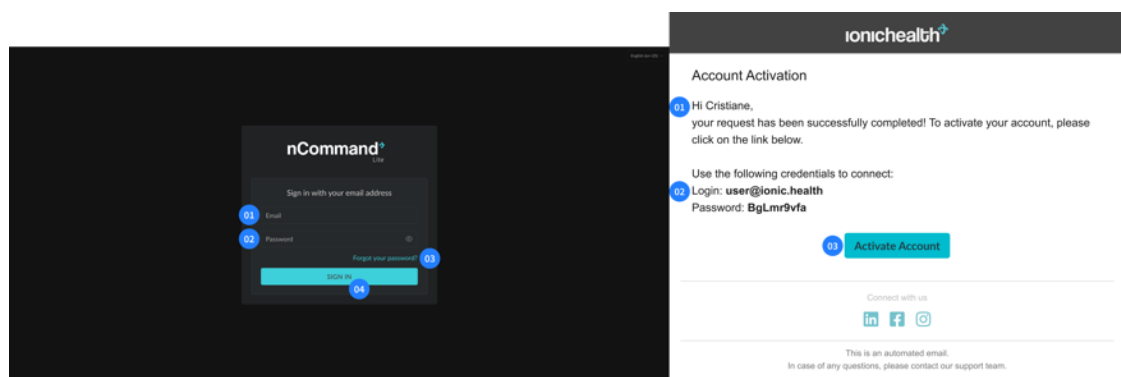


Abbildung 02: Erster Zugriff

Links – Anmeldeseite: 01 – Email Address (E-Mail-Adresse); 02 – Password (Kennwort); 03 – „Forgot your password?“ (Kennwort vergessen?); 04 – Schaltfläche Sign In (Anmelden)

Rechts – Willkommens-E-Mail: 01 – E-Mail-Text zur Kontoaktivierung; 02 – Anmeldedaten; 03 – Schaltfläche Active Account (Konto aktiv)

Dieses Einleitungsverfahren soll von Anfang an maximale Sicherheit für Ihr Konto gewährleisten. Ab Ihrem zweiten Zugriff wird der Prozess rationalisiert, bleibt aber ebenso sicher, wobei bei jeder Anmeldung ein Zwei-Faktor-Authentifizierungscode an Ihre zugehörige E-Mail gesendet wird, um die anhaltende Sicherheit Ihres Kontos zu gewährleisten.

Nach der Anmeldung bei nCommand Lite führt Sie das System automatisch zum Startbildschirm, der entsprechend Ihrem spezifischen Benutzerprofil angepasst wird. Unabhängig davon, ob Sie ein Technologie vor Ort oder ein Remote-Technologie sind, die Benutzeroberfläche ist so konzipiert, dass sie den Anforderungen und dem Zugang Ihrer Rolle entspricht. Dieses intuitive Design stellt sicher, dass Sie über alle Tools und Informationen verfügen, die Sie für eine effektive und effiziente Benutzererfahrung benötigen, sobald Sie sich anmelden.

Hinweis: Wenn die Anmeldemethode als nCommand Lite konfiguriert ist, muss die Anmeldung immer über diese Option erfolgen. Selbst wenn die Schaltfläche „External IdP“ auf dem Anmeldebildschirm angezeigt wird, funktioniert sie für diese Benutzer nicht. Jedes Benutzerkonto ist auf der Plattform mit einer bestimmten Authentifizierungsmethode registriert – entweder Zugangsdaten von nCommand Lite oder einem External IdP-Dienst. Wenn ein Benutzer versucht, sich mit einer anderen Methode als der seinem Konto zugewiesenen Methode anzumelden, zeigt das System eine Fehlermeldung an, die darauf hinweist, dass das Konto für diesen Authentifizierungstyp nicht autorisiert ist.

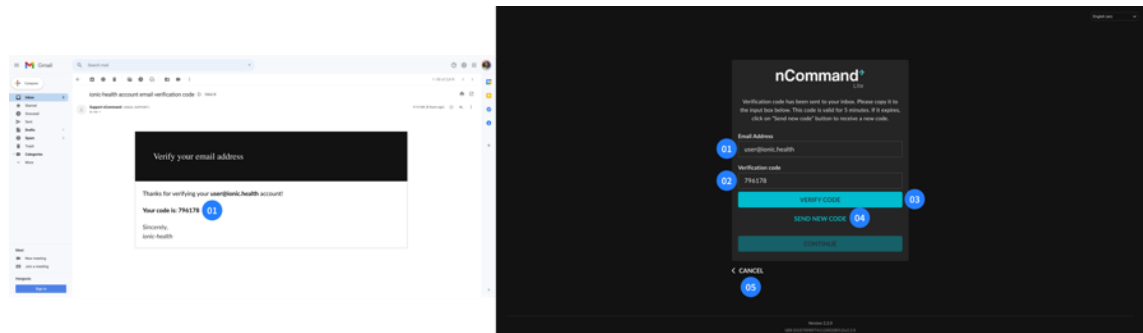


Abbildung 03: Zwei-Faktor-Authentifizierung (2-FA)

Links – E-Mail: 01 – 2-FA-Code

Rechts – Zwei-Faktor-Authentifizierungsseite: 01 – E-Mail-Adresse; 02 – Prüfcode;
03 – Bestätigungscode-Schaltfläche bestätigen; 04 – Neuen Code senden; 05 – Abbrechen

3.2.2. Anmeldung über einen External IdP

In einigen Fällen können sich Benutzer über einen External Identity Provider (IdP) bei der Plattform anmelden. Dadurch können sie den bestehenden Authentifizierungsdienst ihrer Einrichtung nutzen, ein Mechanismus, der auch als Single Sign On (SSO) bekannt ist. Auf diese Weise erhält der vorregistrierte Benutzer keine Willkommens-E-Mail. Der IT-Service vor Ort muss die Kompatibilität prüfen, die Methode konfigurieren und den Benutzer darüber informieren, welche E-Mail (External IdP) verwendet werden soll.

Wenn diese Option verfügbar ist, muss sich der Benutzer immer mit dem External IdP anmelden (z. B. Amazon Cognito, Microsoft Entra ID, Microsoft AD B2C). Die Anmeldemethode über nCommand Lite ist für External IdP-Benutzer nicht verfügbar.

Um sich mit dem External IdP anzumelden, klicken Sie auf die Schaltfläche mit dem IdP-Namen und folgen Sie den Anweisungen des externen Authentifikators. Wenn Ihre Einrichtung mehr als einen External IdP integriert hat, vergewissern Sie sich, bei welchem Anbieter Sie registriert sind. Andere Anbieter funktionieren nicht. Bei Fragen oder Schwierigkeiten wenden Sie sich bitte an Ihren IT-Service vor Ort.

In Szenarien, in denen Benutzer denselben Rechner nutzen und Single Sign-On (SSO) verwenden, wird empfohlen, dass jeder Benutzer bei der Anmeldung bei einem External IdP (falls verfügbar) die Option „nicht angemeldet bleiben“ auswählt oder sich nach der Abmeldung von nCommand Lite bei dem externen Anbieter abmeldet.

Bei dieser Anmeldeoption wird der gesamte An- und Abmeldeprozess – einschließlich Richtlinien zur Erstellung und zum Ablauf von Passwörtern, Multi-Faktor-Authentifizierung (MFA) und Kontosperrungen – vollständig vom IT-Team des Kunden verwaltet, das den External IdP konfiguriert hat.

Bei der Anmeldung über einen External IdP müssen die Funktionen „Passwort vergessen“ und „Passwort ändern“ gemäß dem Prozess des External IdP ausgeführt werden.

Hinweis: Die Option „Passwort vergessen“ wird weiterhin auf dem Anmeldebildschirm angezeigt, ist jedoch für diese Benutzer nicht funktionsfähig. Sie kann zu den nächsten Schritten des Prozesses führen, wird ihn aber nicht abschließen. Wenn Sie Ihr Passwort wiederherstellen müssen, befolgen Sie die Anweisungen Ihres External IdP.

Wichtig: Auch wenn ein External IdP verwendet wird, muss der Benutzer auf der nCommand Lite-Plattform vorregistriert sein, um Zugriff zu erhalten.

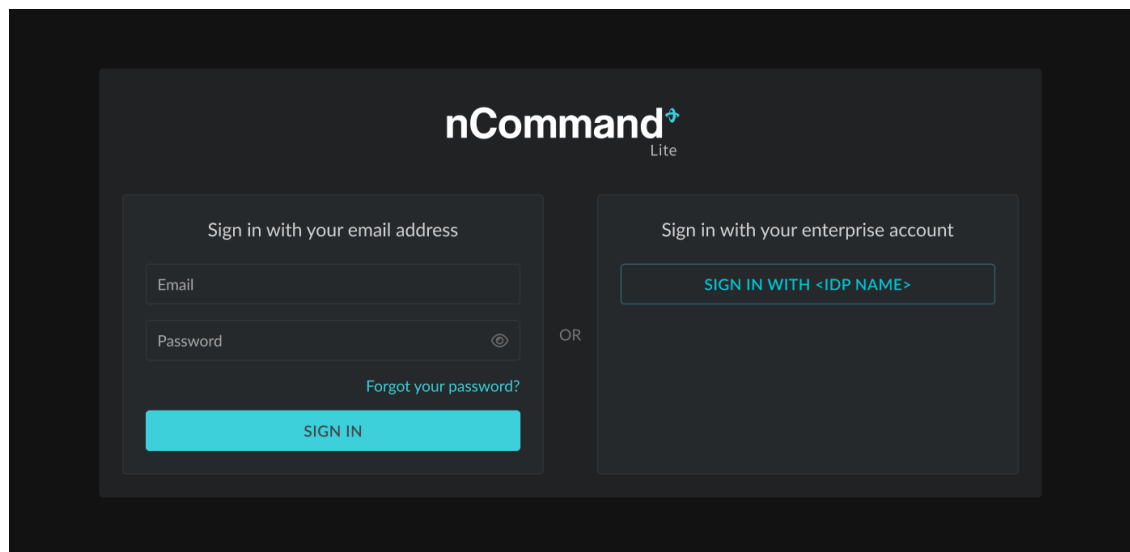


Abbildung 04: Anmeldebildschirm über External IdP (Beispiel)

Abschnitt 3.3 - Passwortverwaltung

Nach dem ersten Zugriff auf die Plattform können Benutzer ihr Passwort ändern oder, falls es vergessen wurde, ein neues Passwort festlegen.

Hinweis: Bei der Anmeldung über einen External IdP müssen die Funktionen **Passwort vergessen** und **Passwort ändern** gemäß dem Prozess des External IdP ausgeführt werden.

- **Passwort wiederherstellen:** Ermöglicht Benutzern die Wiederherstellung des Kontozugriffs, falls sie ihr Passwort vergessen haben. Klicken Sie einfach auf den Link „Forgot your password?“ (Kennwort vergessen?) auf der Anmeldeseite, geben Sie die zugehörige E-Mail-Adresse ein und übermitteln Sie die Informationen. Das System sendet dann eine E-Mail mit einem Verifizierungscode. Wenn der Code eingegeben und auf „Verify code“ (Code überprüfen) geklickt wird, werden die Benutzer aufgefordert, die zugehörige E-Mail zu bestätigen. Durch Klicken auf „Continue“ (Weiter) werden Benutzer zu einer Seite weitergeleitet, auf der sie ein neues Passwort eingeben und das neue Passwort bestätigen können. Wenn das neue Passwort die Systemanforderungen erfüllt, können Benutzer es erfolgreich registrieren und sich anschließend mit den aktualisierten Anmeldeinformationen anmelden.

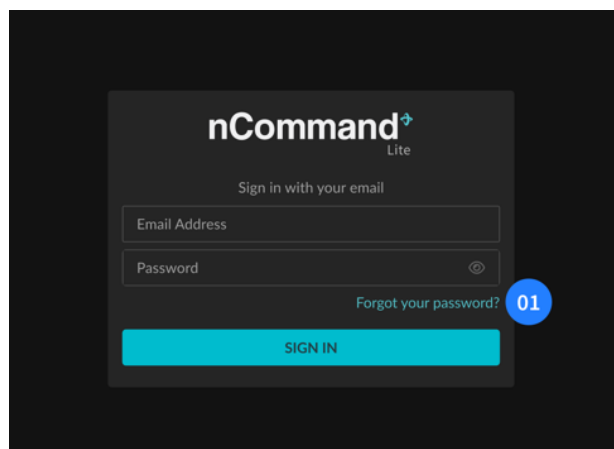


Abbildung 05: Link zur Passwort-Zurücksetzungsseite
01 – Forgot your password? (Kennwort vergessen?)

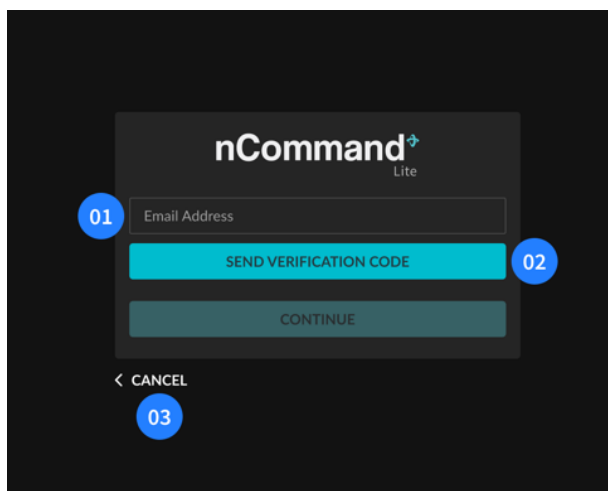


Abbildung 06: Passwort-Zurücksetzungsseite

01 – E-mail Address (E-Mail-Adresse); 02 – Send Verification Code (Prüfcode senden); 03 – Cancel (Abbrechen)

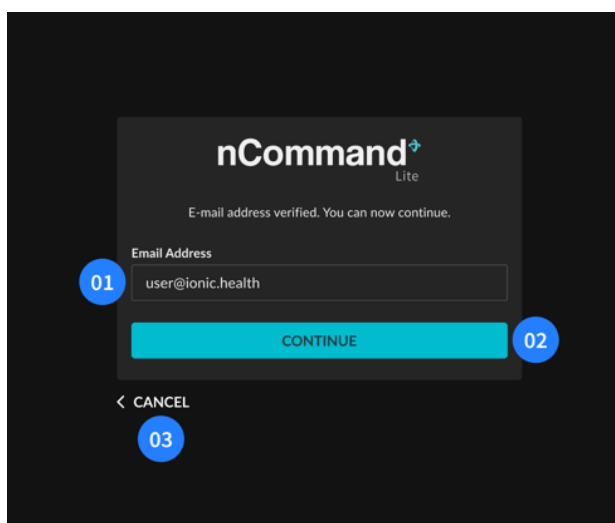


Abbildung 07: E-Mail-Bestätigung

01 – E-mail Address (E-Mail-Adresse); 02 – Schaltfläche Continue (Weiter); 03 – Cancel (Abbrechen)

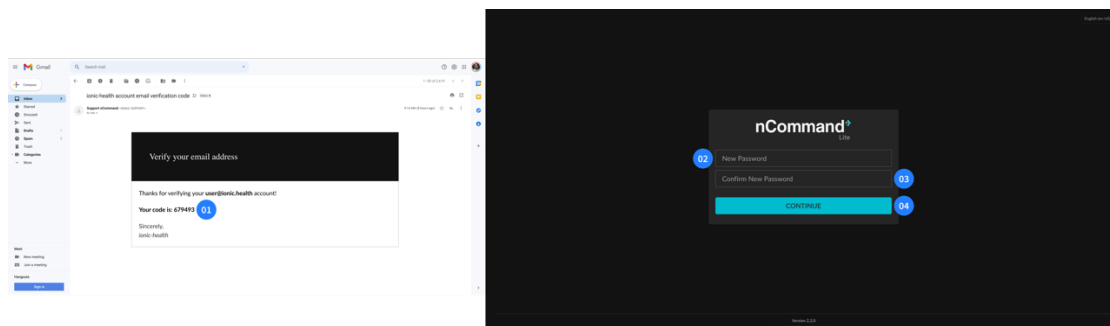


Abbildung 08: E-Mail mit Code zur Registrierung des neuen Passworts (links) – 01 – 2-FA Code Seite Change Password (Passwort ändern) (rechts) – 02 – New Password (Neues Passwort); 03 – Confirm New Password (Neues Passwort bestätigen); 04 – Schaltfläche Continue (Weiter)

- Passwort ändern:** Ermöglicht es Benutzern, ihr Passwort zu aktualisieren, unter Einhaltung bestimmter Kriterien, darunter mindestens 3 der folgenden Punkte: ein Kleinbuchstabe, ein Großbuchstabe, eine Zahl und ein Symbol, und eine Mindestlänge von 8 Zeichen. Das System prüft, ob das neue Passwort diese Kriterien erfüllt, und fordert den Benutzer mit einer Meldung dazu auf, wenn dies nicht der Fall ist. Darüber hinaus müssen Benutzer das neue Passwort bestätigen, um Eingabefehler zu vermeiden. Um das Passwort zu ändern, muss der Benutzer nach dem Anmeldevorgang auf das Symbol in der oberen rechten Ecke klicken und das Menü „Change Password“ (Passwort ändern) auswählen. Er wird von der Plattform getrennt und zu einer Seite weitergeleitet, um dort die zugehörige E-Mail zu bestätigen. Das System sendet dann eine E-Mail mit einem Verifizierungscode. Wenn der Code eingegeben und auf „Verify code“ (Code überprüfen) geklickt wird, werden die Benutzer zu einem Bildschirm weitergeleitet, auf dem sie ein neues Passwort eingeben können.

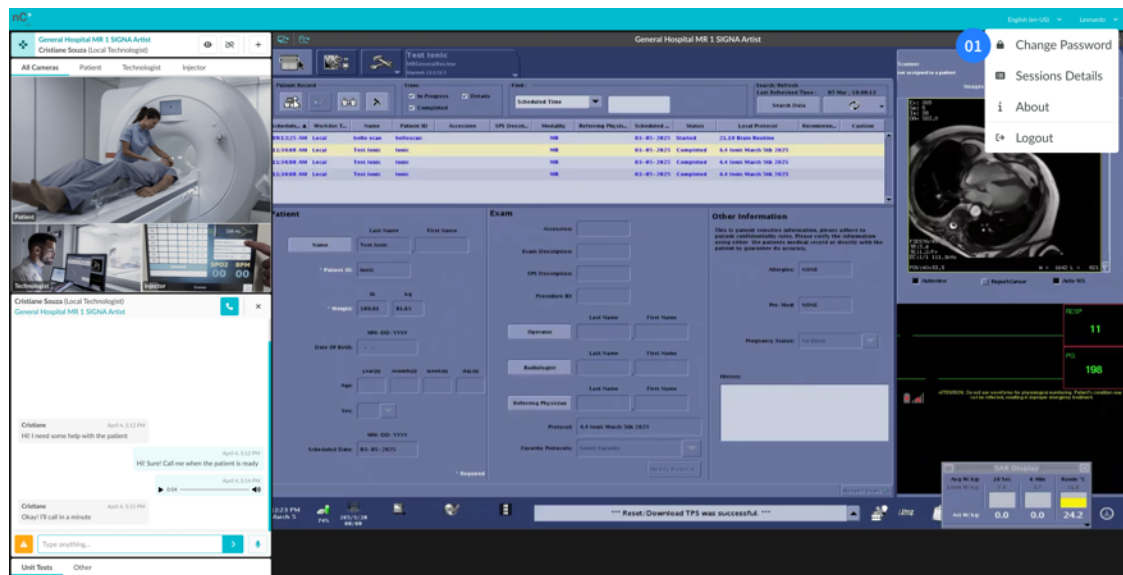


Abbildung 09: Passwort ändern Dropdown-Menüpunkt
01 – Passwort ändern

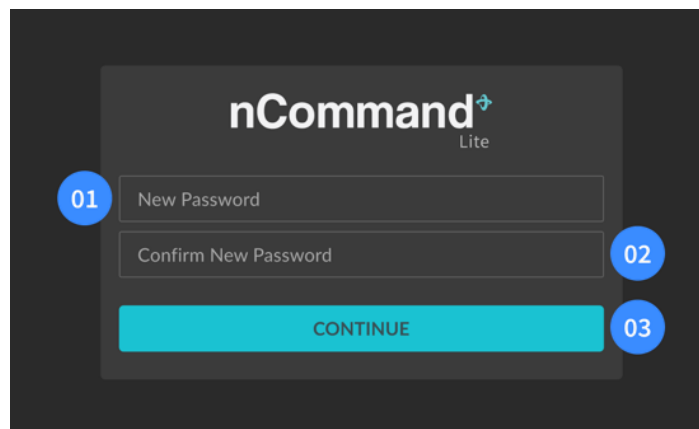


Abbildung 10: Seite Passwort ändern
01 – New Password (Neues Passwort); 02 – Confirm New Password (Neues Passwort bestätigen); 03 – Schaltfläche Continue (Weiter)

Abschnitt 3.4 - Zugriff mit dem Profil des Technologen vor Ort



WARNUNG!

Wenden Sie sich vor der Verwendung der Plattform telefonisch an den Remote-Technologen.



WARNUNG!

Um eine Überhitzung zu vermeiden, stellen Sie bitte keine Gegenstände vor den Lüftungsschlitz des e-KVM-Computers und stellen Sie keine Gegenstände darauf, um Schäden zu vermeiden.



WARNUNG!

Während Remote-Sitzungen ist der Technologe vor Ort für die Verwaltung und Durchsetzung lokaler Sicherheitsregeln für jede Art von Untersuchung und ihre spezifischen Anforderungen verantwortlich. Stets im Kontrollraum und/oder Untersuchungsraum bleiben, um die Sicherheit sowohl des Patienten als auch der beteiligten Fachkräfte zu gewährleisten.



WARNUNG!

Tischbewegungen während der Sitzung dürfen nur vom Technologen vor Ort durchgeführt werden, wenn dies vom System gefordert wird. Vor Verlassen des Operationssaals sollte der Technologe vor Ort immer den Zugriff des Remote-Technologen widerrufen.



WARNUNG!

Nur der Technologe vor Ort darf den Tisch bewegen, um den Patienten im Gerät zu positionieren und den Patienten sicher zu lösen. Vor Verlassen des Operationssaals sollte der Technologe vor Ort immer den Zugriff des Remote-Benutzers widerrufen.

Nachdem Sie sich bei der Plattform angemeldet haben, wählen Sie das gewünschte Gerät im Feld Device Selection (Geräteauswahl) aus. Sie sind für dieses Gerät verantwortlich, sodass Sie die Anfrage des Remote-Technologen für den Zugriff auf das Gerät überprüfen können. Wenn ein Remote-Technologe auf das Gerät zugreifen möchte, wird ein Popup-Fenster angezeigt, in dem Sie alle angezeigten Informationen überprüfen können, bevor Sie den Zugriff gewähren oder ablehnen. Achten Sie auf eine eingehende Anfrage eines Remote-Technologen. Es ist äußerst wichtig, jedes Detail sorgfältig zu überprüfen. In Fällen, in denen die bereitgestellten Informationen nicht erkannt werden, darf kein Zugriff gewährt werden.

Der Remote-Technologe kann mit einem von zwei Zugriffsmodi auf das Gerät zugreifen: **Steuerung** oder **Anzeigen**:

- **Modus „Steuern“** – ermöglicht dem Remote-Technologen, Maus und Tastatur zu steuern sowie das Streaming des Geräts anzuzeigen. Der Technologe vor Ort verliert jedoch nicht die Kontrolle über die lokale Maus und Tastatur und kann die Steuerung jederzeit übernehmen.
- **Anzeigen** – ermöglicht es dem Remote-Technologen, nur den Bildschirm des Geräts zu sehen und den Chat für die Kommunikation zu nutzen

Nach Auswahl des Geräts hat der Benutzer Zugriff auf die Chat-Funktion, die die Kommunikation über Text, Audionachrichten, Sprach- und Videoanrufe mit den anderen Benutzern ermöglicht.

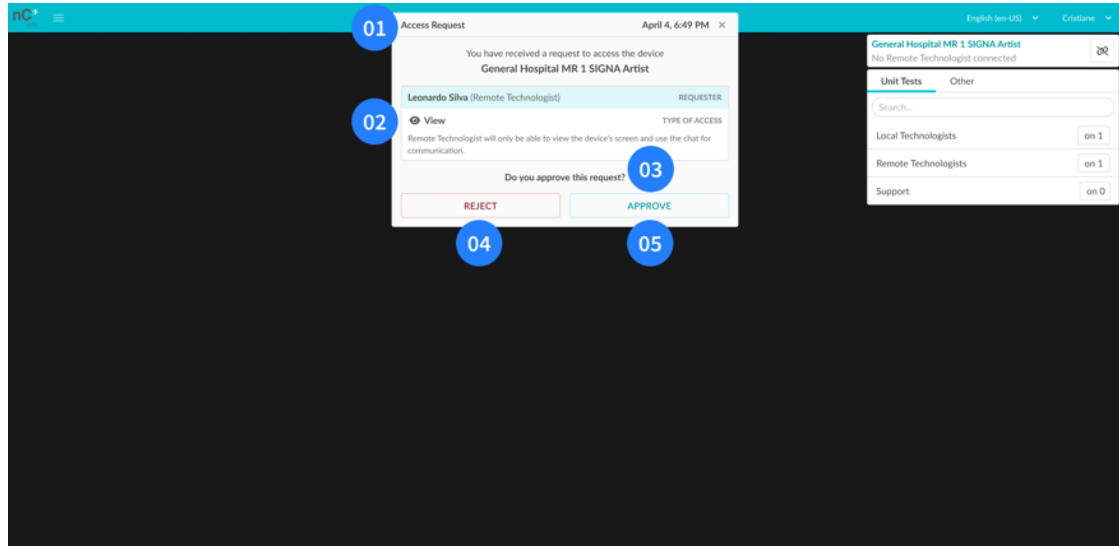


Abbildung 11: Hauptbildschirm des Technologen vor Ort mit Benachrichtigung über Zugriffsanfrage

- 01 – Titel Access Request (Zugriffsanfrage); 02 – Beschreibung des Anfragenden, sein Name, seine Rolle und der Zugriffstyp;
 03 – Eingabeaufforderung: „Do you approve. this request?“ (Genehmigen Sie diesen Antrag?); 04 – Schaltfläche Reject (Ablehnen); 05 – Schaltfläche Approve (Genehmigen)

Nach der Genehmigung kann der Technologie vor Ort den Zugriff des Remote-Technologen jederzeit widerrufen, indem er einfach auf die Taste REVOKE (WIDERRUFEN) klickt.

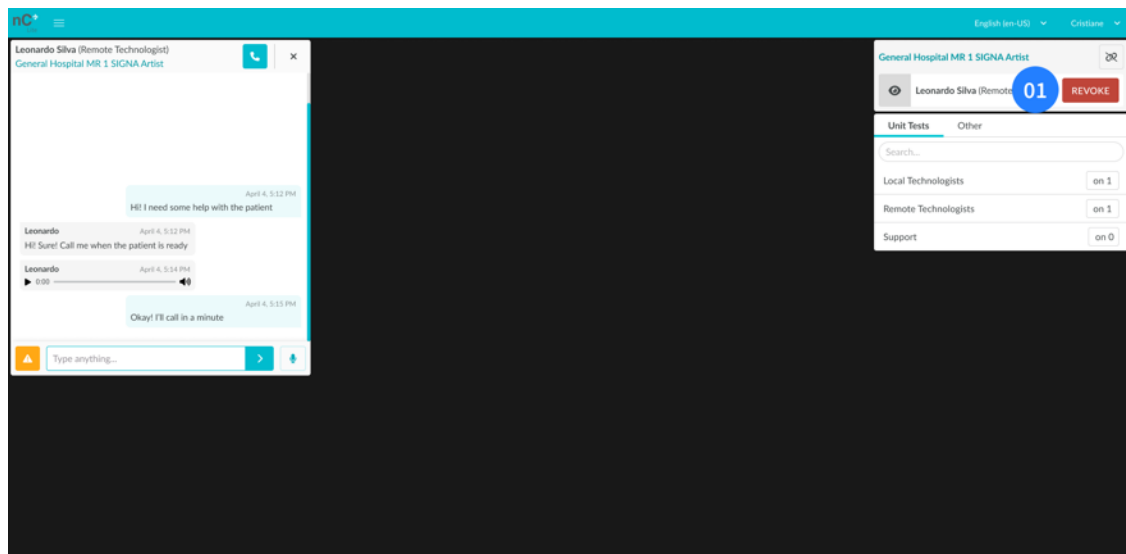


Abbildung 12: Hauptbildschirm des Technologen vor Ort bei Verbindung mit einem Gerät

- 01 – Taste Revoke (Widerrufen)

Während der Remote-Sitzung kann der Remote-Technologie einen Wechsel des Zugriffsmodus anfordern. Auf dem Bildschirm wird ein Popup-Fenster mit einer Anforderung angezeigt. Sie können sie genehmigen oder ablehnen. Beachten Sie die Vorrechte, die jeder Zugriffsmodus dem Remote-Technologen gewährt.

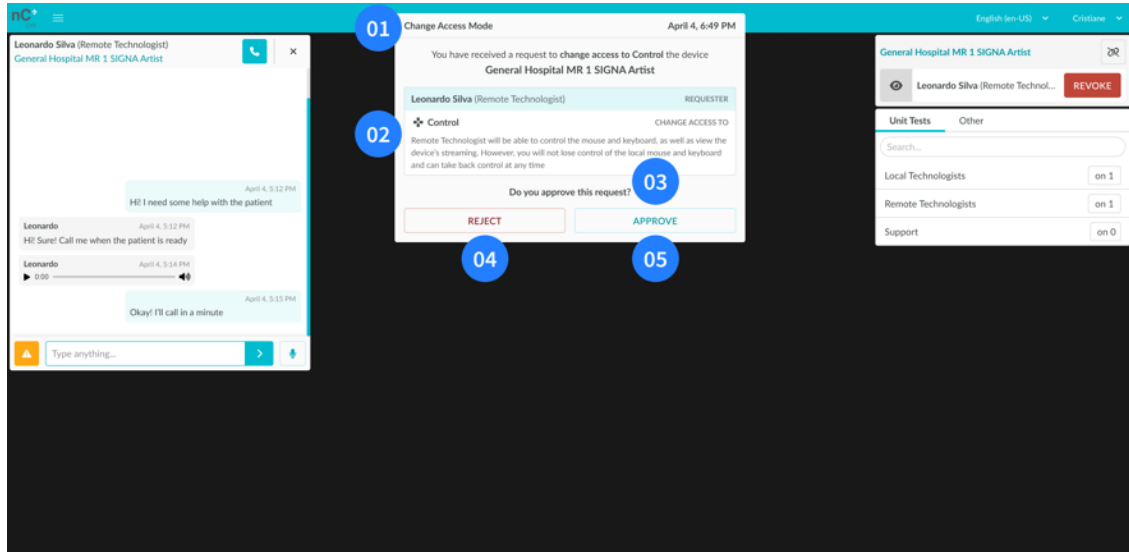


Abbildung 13: Hauptbildschirm des Technologen vor Ort mit Anforderung zur Änderung des Zugriffsmodus
 01 – Titel Change Access Mode (Zugriffsmodus ändern); 02 – Beschreibung des Anfragenden, sein Name, seine Rolle und der Zugriffstyp;

03 – Eingabeaufforderung: „Do you approve. this request?“ (Genehmigen Sie diesen Anfrage?); 04 – Schaltfläche Reject (Ablehnen); 05 – Schaltfläche Approve (Genehmigen)



WARNUNG!

Im Falle einer unterbrochenen Verbindung am lokalen Computer hat der Remote-Technologie weiterhin Zugriff auf das **Gerät**. Wenden Sie sich **sofort** an den Remote-Technologen und bitten Sie ihn, die Anmeldung zu **trennen** ODER sich bei einem anderen Computer anzumelden und **den Zugriff des Remote-Technologen zu widerrufen** ODER die **Ein/Aus-Taste zu drücken**, um den e-KVM-Computer herunterzufahren.



WARNUNG!

Im Falle einer Scannerwartung:

Bevor der Technologie vor Ort mit den Arbeiten beginnt (entweder am Gerät oder im Steuerraum), informieren Sie den Remote-Technologen und widerrufen Sie den Zugriff, indem Sie auf die Schaltfläche „ZUGRIFF WIDERRUFEN“ klicken. Melden Sie sich dann von der nCommand Lite-Plattform ab.

Wenn kein Remote-Technologie verbunden ist, melden Sie sich von der nCommand Lite-Plattform ab, bevor Sie mit der Wartung beginnen.

Abschnitt 3.5 - Zugriff mit Remote-Technologenprofil

**WARNUNG!**

Benutzer des Gerätecomputers und Root-Passwort: Beide müssen dem Host vor Ort, der das Installationsteam empfängt, zur Verfügung stehen.

**WARNUNG!**

Tischbewegungen während der Sitzung dürfen nur vom Technologen vor Ort durchgeführt werden, wenn dies vom System gefordert wird. Vor Verlassen des Operationssaals sollte der Technologe vor Ort immer den Zugriff des Remote-Technologen widerrufen.

**WARNUNG!**

Nur der Technologe vor Ort darf den Tisch bewegen, um den Patienten im Gerät zu positionieren und den Patienten sicher zu lösen. Vor Verlassen des Operationssaals sollte der Technologe vor Ort immer den Zugriff des Remote-Benutzers widerrufen.

**WARNUNG!**

Achten Sie stets durch die Videokamera auf den Raum und stellen Sie sicher, dass Sie vor jeglichen Aktivitäten mit dem Technologe vor Ort kommunizieren.

**WARNUNG!**

Sollte die Verbindung zum lokalen Computer unterbrochen werden, nehmen Sie umgehend Kontakt mit dem Technologen vor Ort auf und trennen Sie die Verbindung.

**WARNUNG!****Im Falle einer Scannerwartung:**

Stellen Sie nach der Benachrichtigung über den Beginn der Produktwartung sicher, dass der Technologe vor Ort den Zugriff widerrufen hat, und melden Sie sich von der nCommand Lite-Plattform ab.

Wenn der Zugriff nicht widerrufen wurde, melden Sie sich von der nCommand Lite-Plattform ab und wenden Sie sich umgehend an den Technologen vor Ort, um ihn zu benachrichtigen.

**WARNUNG!**

Zur Fernsteuerung von Maus und Tastatur muss der ausgewählte Zugriffsmodus Control (Steuern) sein; im Zugriffsmodus View (Anzeigen) darf der Remote-Technologe nur Streaming und lokale Kameras ansehen.

**WARNUNG!**

Wenn die Antwort auf Ihre Anfrage länger dauert als erwartet, wenden Sie sich per Chat oder Telefon an den Technologen vor Ort.

Der Arbeitsplatz des Remote-Technologen umfasst Geräte wie einen Computer, Monitore (normalerweise drei), eine Maus, eine Tastatur und ein Headset.

Im klinischen Arbeitsablauf haben *Technologen vor Ort* direkten Kontakt mit dem Patienten. Sie sind verantwortlich für die Patienteninteraktion, die Positionierung und die Gewährleistung der Sicherheit sowie der Protokolleinhaltung während MRT-, CT- oder PET/CT-Verfahren gemäß institutionellen und behördlichen Standards.

3.5.1. Zugriffsmodus

Wählen Sie nach dem Anmelden bei der Plattform in der Device Selection Box (dem Geräteauswahlfeld) das Gerät aus, mit dem Sie eine Verbindung herstellen möchten. Es öffnet sich ein Popup-Fenster, in dem Sie den Zugriffsmodus zwischen **Control** (Steuern) und **View** (Anzeigen) auswählen können:

- **Modus „Steuern“** – In diesem Modus ist die Maus- und Tastatursteuerung zusätzlich zur Bildschirmanzeige aktiviert. Das Fachpersonal vor Ort behält vollen Zugriff auf die lokale Maus und Tastatur und kann die Steuerung jederzeit wieder übernehmen.
- **Modus „Anzeigen“** – Es ist nur möglich, den Bildschirm des Geräts zu sehen und den Chat für die Kommunikation zu nutzen.

Wenn Sie den Zugriffsmodus auswählen, wird ein Feld mit der Meldung „Waiting for Approval“ (Warten auf Genehmigung) sichtbar, das anzeigt, dass die Genehmigung des verbundenen Technologen vor Ort erforderlich ist, um fortzufahren. Dieser Technologe vor Ort hat die volle Befugnis, den Zugriff jederzeit zu genehmigen oder abzulehnen und den Zugriff zu widerrufen, wenn dies als notwendig erachtet wird. Diese Maßnahme ist unerlässlich, um eine strenge Kontrolle zu gewährleisten und die Sicherheit bei der Verwendung des Produkts aufrechtzuerhalten.

Nach Auswahl des Geräts hat der Benutzer Zugriff auf die Chat-Funktion, die die Kommunikation über Text, Audionachrichten, Sprach- und Videoanrufe mit den anderen Benutzern ermöglicht. Der Benutzer muss für den Zugriff auf den Chat nicht zugelassen werden.

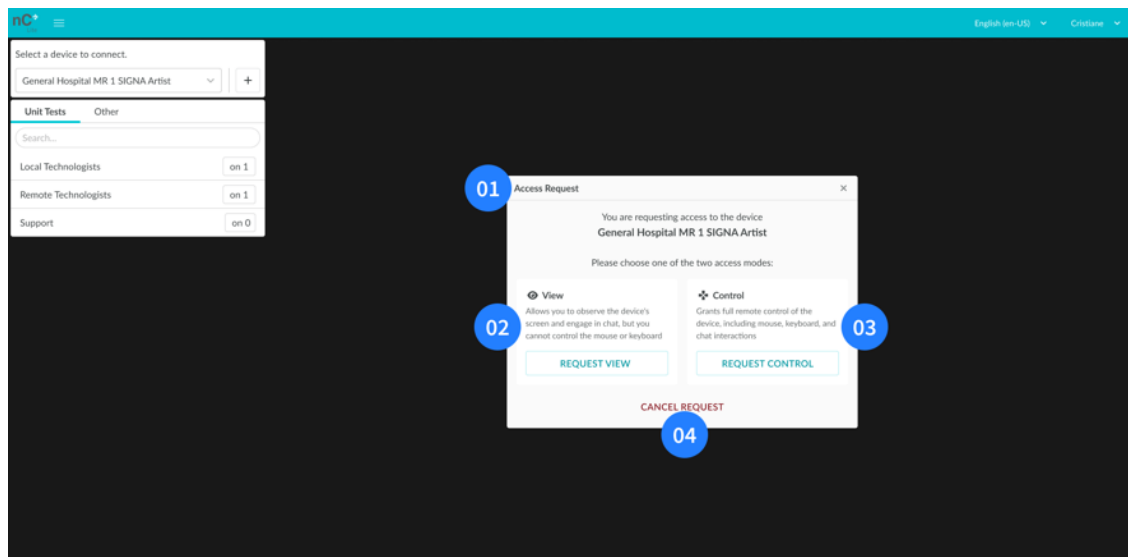


Abbildung 14: Zugriffsanfrage-Dialog für Remote-Technologen

01 – Titel Access Request (Zugriffsanfrage); **02** – Beschreibung des Ansichtsmodus und Schaltfläche Request View (Ansichtsanfrage); **03** – Beschreibung des Steuermodus und Schaltfläche Request Control (Steuerungsanfrage); **04** – Cancel Request (Anforderung abbrechen)

Sobald der Gerätezugriff vom Technologen vor Ort autorisiert wurde, wird die Benutzeroberfläche des Remote-Technologen aktualisiert, um den Live-Feed des Geräts und der zugehörigen Kameras anzuzeigen. Wenn der gewählte Zugriffsmodus Kontrolle ist, wird die Möglichkeit für den Fernbetrieb des Geräts aktiviert.

Dieser Prozess gewährleistet eine effektive und sichere Interaktion und ermöglicht die sichere Fernnutzung des Geräts, ohne dessen Funktionsfähigkeit oder die Sicherheit des Patienten zu gefährden.

Um eine Änderung des Zugriffsmodus während einer Remote-Sitzung anzufordern, klicken Sie auf das entsprechende Symbol. Der Technologie vor Ort kann die Anfrage annehmen oder ablehnen.

- **Accept (Akzeptieren)** – das Streaming wird neu geladen, aber der Chat-Inhalt geht nicht verloren. Wenn Sie sich in einem Sprach- und Videoanruf befinden, wird dieser beendet und muss von einem der Benutzer neu gestartet werden.
- **Decline (Ablehnen)** – es erscheint ein Popup-Fenster, das Sie über die Ablehnung des Technologen vor Ort informiert und der aktuelle Zugang bleibt aktiv.

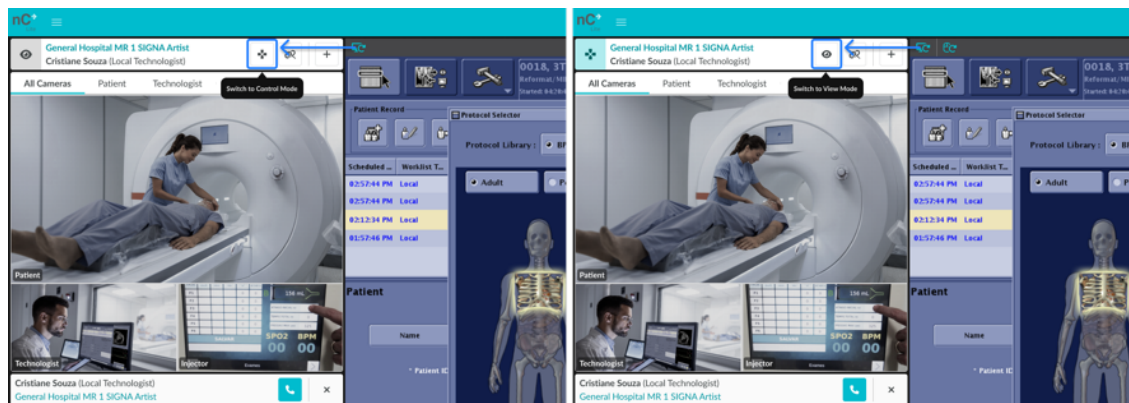


Abbildung 15: Zugriffsmodus ändern

Links – Symbol und Tooltip Switch to Control Mode (Zum Steuerungsmodus wechseln) / **Rechts** – Symbol und Tooltip Switch to View Mode (Zum Anzeigemodus wechseln)

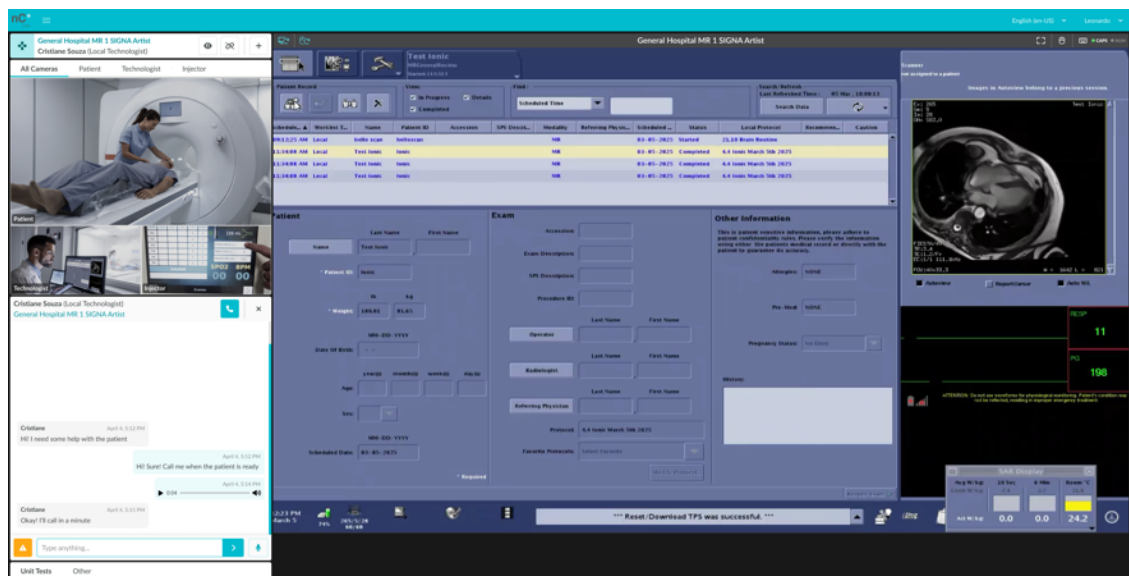


Abbildung 16: Hauptbildschirm des Remote-Technologen bei bestehender Verbindung zu einem Gerät

Wenn der Remote-Technologe Zugriff wünscht und kein Technologie vor Ort mit dem Gerät verbunden ist, zeigt die Plattform eine Popup-Warnung an. Sobald der Technologie vor Ort eine Verbindung herstellt, informiert die Plattform den Remote-Technologe darüber, dass er den Zugriff erneut anfordern kann.

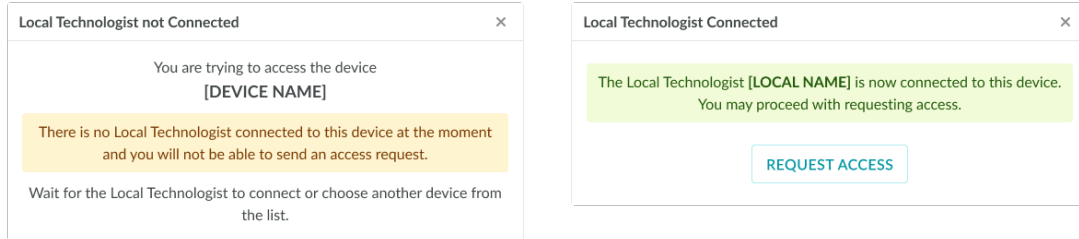


Abbildung 17: Warnhinweise des Remote-Technologen zum Verbindungsstatus des Technologen vor Ort
Links – Benachrichtigung, die angibt, dass ein Versuch unternommen wurde, auf das Gerät zuzugreifen, aber derzeit kein Technologie vor Ort verbunden ist.
Rechts – Benachrichtigung, die bestätigt, dass der Technologie vor Ort eine Verbindung zum Gerät hergestellt hat, nachdem er zuvor nicht verbunden war.

3.5.2. Streaming-Leiste

Die Streaming-Leiste zeigt wichtige Informationen und Steuerungen zur Streaming-Sitzung des Geräts an. Sie enthält die Schaltflächen Reload Streaming (Streaming neu laden) und Mouse Resync (Maus neu synchronisieren), den Gerätenamen, die Bildschirmauflösung und den aktuellen Status von Maus und Tastatur des Remote-Computers.

1 – Streaming neu laden

Diese Funktion ermöglicht es Remote-Technologen, im Falle eines Verbindungsfehlers oder einer Leistungsbeeinträchtigung den Zugriff auf Geräte wiederherzustellen. Wenn Sie auf dem Computer Ihres Geräts eine Unterbrechung der Verbindung oder eine Verzögerung des Bildschirms feststellen, können Sie auf das Symbol „Reload Streaming“ (Streaming neu laden) klicken, das sich in der Streaming-Leiste befindet. Dadurch wird die Plattform aufgefordert, sich erneut mit dem Gerätecomputer zu verbinden und auch die Systemkameras neu zu laden.

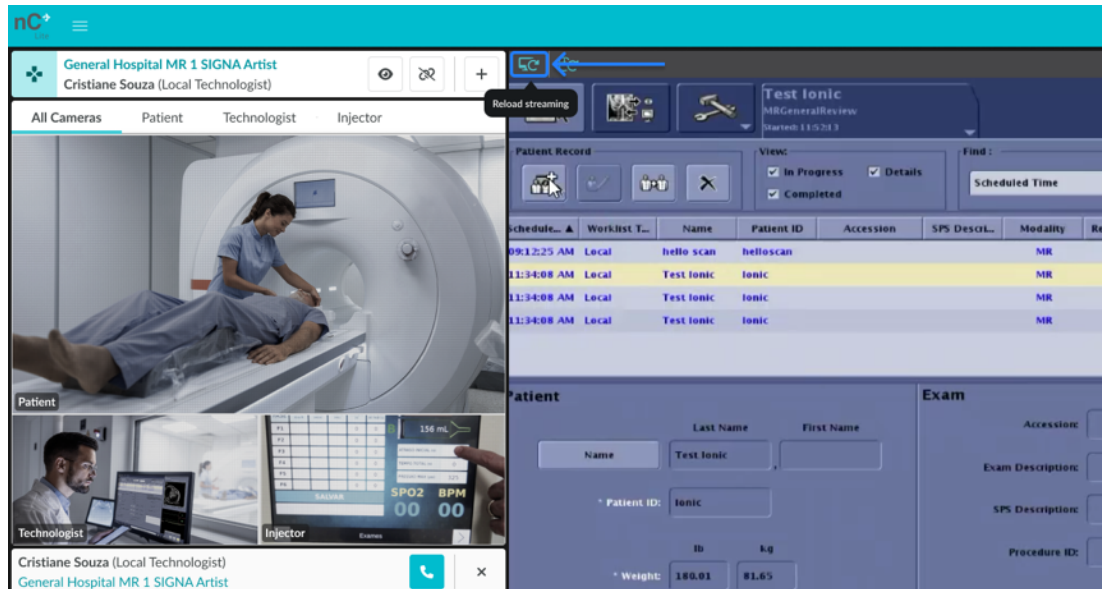


Abbildung 18: Schaltfläche Reload Streaming (Streaming neu laden)

2 – Maus-Resynchronisation

Wenn die Maus langsam oder falsch ausgerichtet ist, klicken Sie bitte auf die Schaltfläche „Mouse Resync“ (Maus-Resynchronisation) in der Leiste über dem Streaming-Fenster, um die Gerätemaus mit dem e-KVM-Computer neu zu synchronisieren.

Eine Alternative ist, den Mauszeiger außerhalb des Streaming-Bereichs zu bewegen und ihn dann wieder hereinzubringen; das System synchronisiert die Maus automatisch neu, ohne dass weitere Maßnahmen erforderlich sind. Sie können auch die Maus-Scrollrad-Taste (wenn verfügbar) anklicken und loslassen, um die Neusynchronisation automatisch auszulösen. Diese Methode funktioniert jedoch möglicherweise nicht auf Geräten mit zwei oder mehr Bildschirmen, wenn der lokale und der entfernte Mauszeiger auf unterschiedlichen Bildschirmen sind.

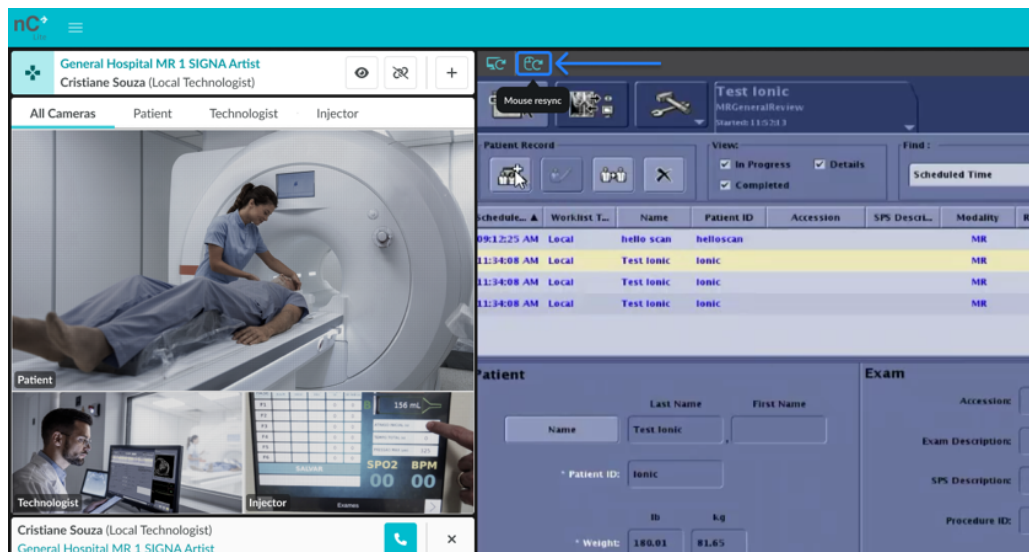


Abbildung 19: Schaltfläche Maus-Neusynchronisation

3 – Streaming-Anzeige

Mit dieser Funktion erhält der Remote-Technologe Informationen über die ursprüngliche Streamingauflösung (vom Gerät) und die aktuelle Auflösung in Pixeln, die auf dem Ferncomputer angezeigt werden.

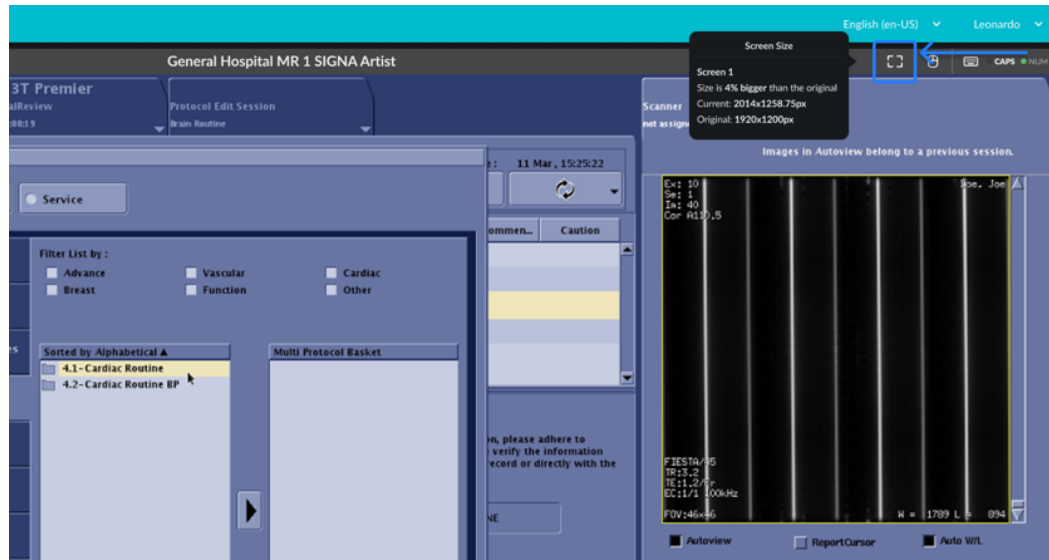


Abbildung 20: Tooltip für Streaming-Informationen

4 – Status von Maus und Tastatur

Diese Funktion informiert den Remote-Technologen darüber, ob Maus und Tastatur korrekt funktionieren. Zusammen mit dem Tastaturstatus kann der Benutzer sehen, ob die **Feststelltaste** und die **Num-Taste** auf dem Gerätecomputer ein- oder ausgeschaltet sind. Diese Funktion hängt jedoch vom Gerätecomputer ab, der diese Informationen bereitstellt. In Szenarien, in denen diese Informationen nicht vom Gerätesystem zur Verfügung gestellt werden, wird der Status der **Feststelltaste** und **Num-Taste** nicht angezeigt. Der Status der Maus und der Tastatur wird nur angezeigt, wenn der Benutzer über den Steuerzugriff verfügt.

Beim Anschließen an ein Gerät kann eine Diskrepanz zwischen den Anzeigen **Feststelltaste** und **Num-Taste** auf dem Remote-Computer und dem Gerät zu inkonsistentem Schreibverhalten führen. Wenn die Anzeigen auf dem Gerät aktiviert erscheinen, aber auf dem Remote-Computer nicht tatsächlich aktiv sind, kann der Benutzer Großbuchstaben auf dem Gerät eingeben, während Text in Kleinbuchstaben im Chat erscheint, oder umgekehrt. Ebenso tritt dasselbe Problem umgekehrt auf, wenn die **Feststelltaste** auf dem Remote-Computer aktiviert, aber auf dem Gerät deaktiviert ist.

Um dieses Problem zu vermeiden, stellen Sie sicher, dass sowohl **Feststelltaste** als auch **Num-Taste** aktiviert oder beide deaktiviert sind, bevor Sie sich am Gerät anmelden. Wenn eine Abweichung auftritt, sollte der Benutzer die Verbindung zum Gerät trennen, den Schlüsselstatus auf dem Remote-Computer anpassen und dann die Verbindung wieder herstellen.

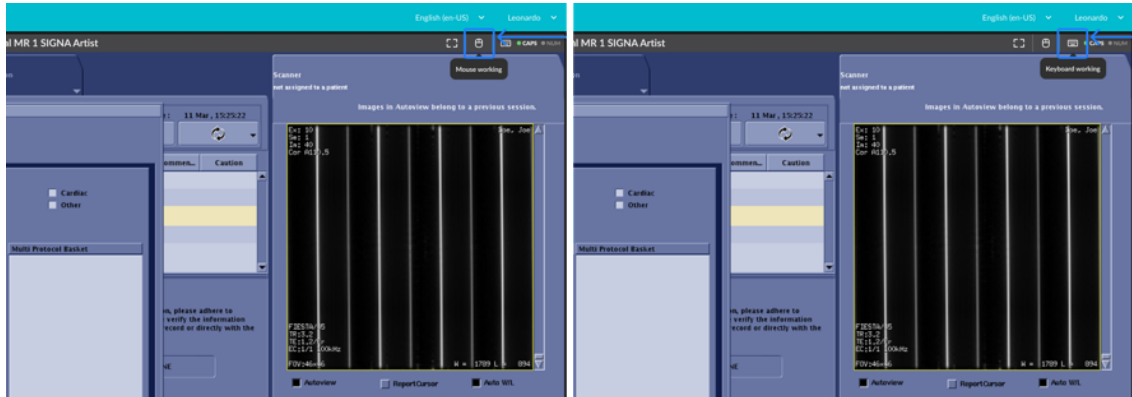


Abbildung 21: Streaming-Leiste
Links – Mausstatus-Tooltip-Informationen
Rechts – Tastaturstatus-Tooltip-Informationen

3.5.3. Multikamera

Diese Funktion ermöglicht es dem Remote-Technologen, mehrere Kameras gleichzeitig anzuzeigen. Wenn mehr als eine Kamera verfügbar ist, ist es möglich, dass Sie nur eine sehen und zwischen ihnen wechseln, indem Sie auf das Menü mit dem entsprechenden Namen für jede Kamera klicken. Durch Auswahl von „ALL CAMERAS“ (ALLE KAMERAS) werden alle verfügbaren Kameras im Rahmen angezeigt, wobei eine davon hervorgehoben ist. Um die hervorgehobene Kamera zu wechseln, bewegen Sie die Maus einfach über eine der Kameras im kleineren Rahmen und klicken Sie auf „SWITCH CAMERA“ (KAMERA WECHSELN).

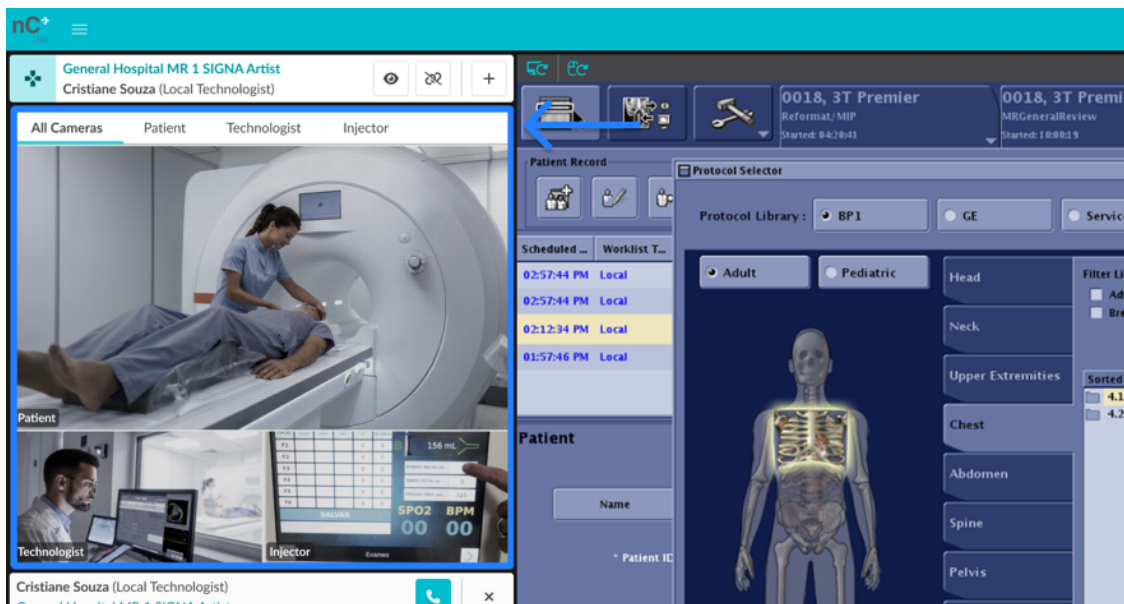


Abbildung 22: Multikamera-Rahmenansicht

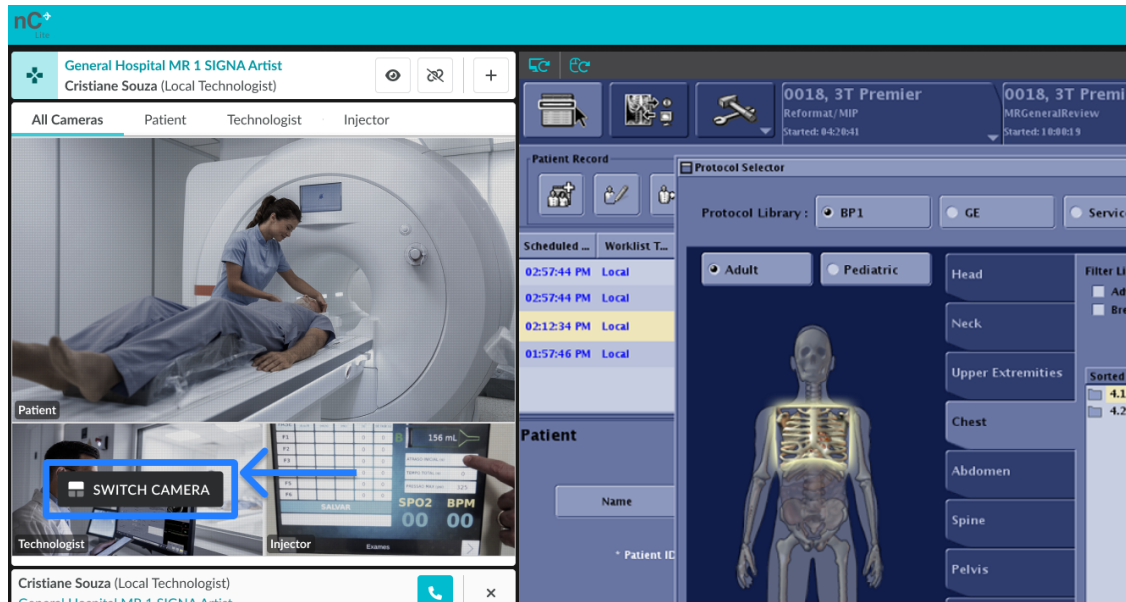


Abbildung 23: Multikamera-Schwebetaste „SWITCH CAMERA“ (KAMERA WECHSELN)

Wenn der Remote-Technologe während einer aktiven Remote-Sitzung auf **View (Anzeigen)** zugreift, besteht die Möglichkeit, eine oder mehrere Kameras auszuschalten, indem er die Maus über die ausgewählte Kamera bewegt und auf „TURN OFF CAMERA“ (KAMERA AUSSCHALTEN) klickt. Um die Kamera erneut anzuzeigen, wiederholen Sie einfach den Vorgang und klicken Sie auf „TURN ON CAMERA“ (KAMERA EINSCHALTEN).

HINWEIS: Die Möglichkeit, Kameras auszuschalten, ist nur im Zugriffsmodus View (Anzeigen) verfügbar; im Zugriffsmodus Control (Steuern) ist es nicht möglich, die Kameras auszuschalten.

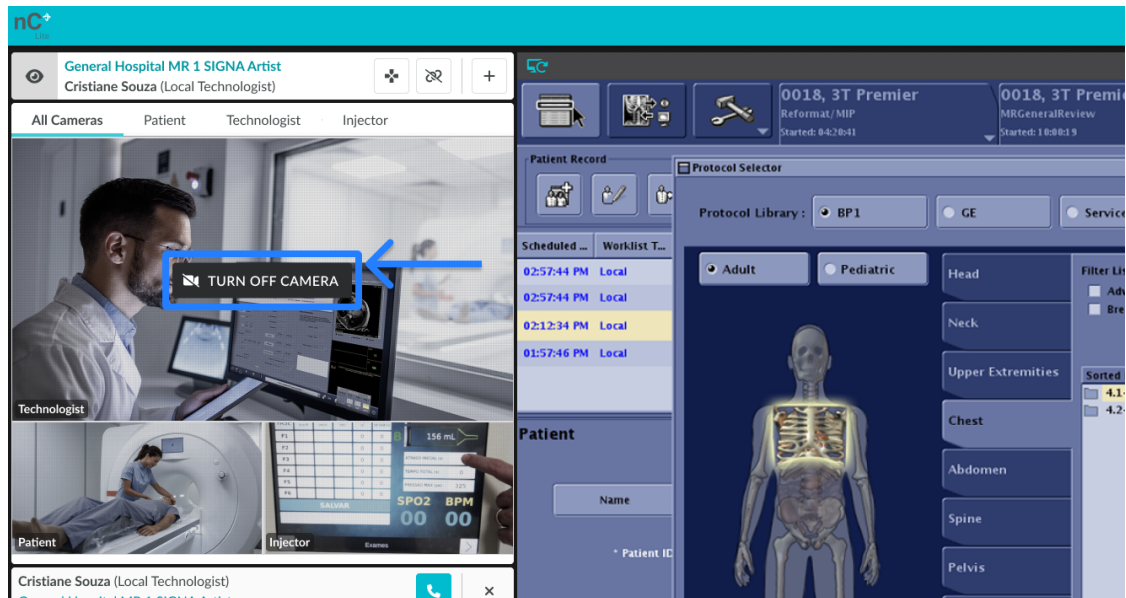


Abbildung 24: Multikamera-Schwebetaste „TURN OFF CAMERA“ (KAMERA AUSSCHALTEN) im Modus „Anzeigen“

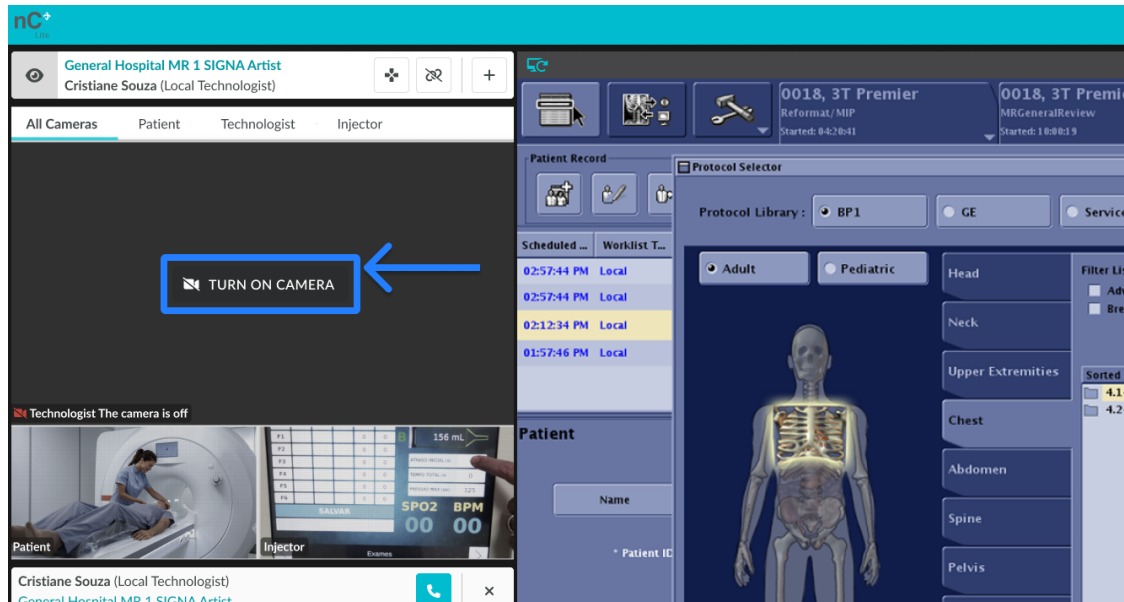


Abbildung 25: Multikamera-Schwebetaste „TURN ON CAMERA“ (KAMERA AUSSCHALTEN) im Modus „Anzeigen“

3.5.4. Ein anderes Gerät öffnen

Ermöglicht dem Remote-Technologen, eine neue Browser-Registerkarte von nCommand Lite zu öffnen, sodass der Benutzer ein neues Gerät auswählen kann, um mehr als einen Remote-Scan gleichzeitig durchzuführen. Um ein neues Gerät für den Zugriff zu öffnen, klicken Sie einfach auf die Schaltfläche Open another Device (Anderes Gerät öffnen). Eine Warnung wird angezeigt, damit Sie diesen gleichzeitigen Vorgang sicher durchführen können. Sie sollten die Warnung lesen, bevor Sie auf dieses neue Fenster zugreifen.

HINWEIS: Für eine bessere Sicht während des gleichzeitigen Zugriffs wird empfohlen, die neue Registerkarte nach dem Klicken auf „OPEN ANOTHER DEVICE“ (ANDERES GERÄT ÖFFNEN) und dem Klicken auf „OK“ (OK) auf den Warnungen auf einen anderen verfügbaren Monitor zu ziehen.



WARNING!

Sicherheitswarnung für den Zugriff auf mehrere Geräte

- **Demand of intense focus (Forderung nach intensivem Fokus):** Ein gleichzeitiger Zugriff erfordert intensive Konzentration und Kommunikation mit den Teams vor Ort.
- **Choose different layouts (Andere Layouts auswählen):** Vermeiden Sie den gleichzeitigen Zugriff auf Geräte mit identischen Layouts oder gleichzeitige Untersuchungen derselben anatomischen Region.
- **Drag tab to another monitor (Registerkarte zu einem anderen Monitor ziehen):** Beim Zugriff auf ein zusätzliches Gerät öffnet sich eine neue Registerkarte. Ziehen Sie diese Registerkarte auf einen zweiten Monitor, da das System für die Verwendung mit einem separaten Bildschirm für jedes Gerät vorgesehen ist.

- **Pay attention to alerts (Achten Sie auf Warnungen):** Achten Sie genau auf alle Systemwarnungen, da diese für einen sicheren Betrieb von entscheidender Bedeutung sind.
- **Control one at a time (Eine nach der anderen kontrollieren):** Sie können mehrere Bildschirme anzeigen, die Steuerung ist jedoch auf jeweils ein Gerät beschränkt.
- **Open chat (Chat öffnen):** Starten Sie den Chat immer, wenn Sie mit einem Gerät verbunden sind, um eine klare Kommunikation zu gewährleisten.
- **One call at a time (Ein Anruf nach dem anderen):** Auf dem zugehörigen Gerätebildschirm werden Sprachanruf-Warnungen angezeigt; es kann jeweils nur ein Anruf aktiv sein.
- **Safety and alert (Sicherheit und Wachsamkeit):** Priorisieren Sie die Sicherheit und bleiben Sie während aller Vorgänge wachsam.

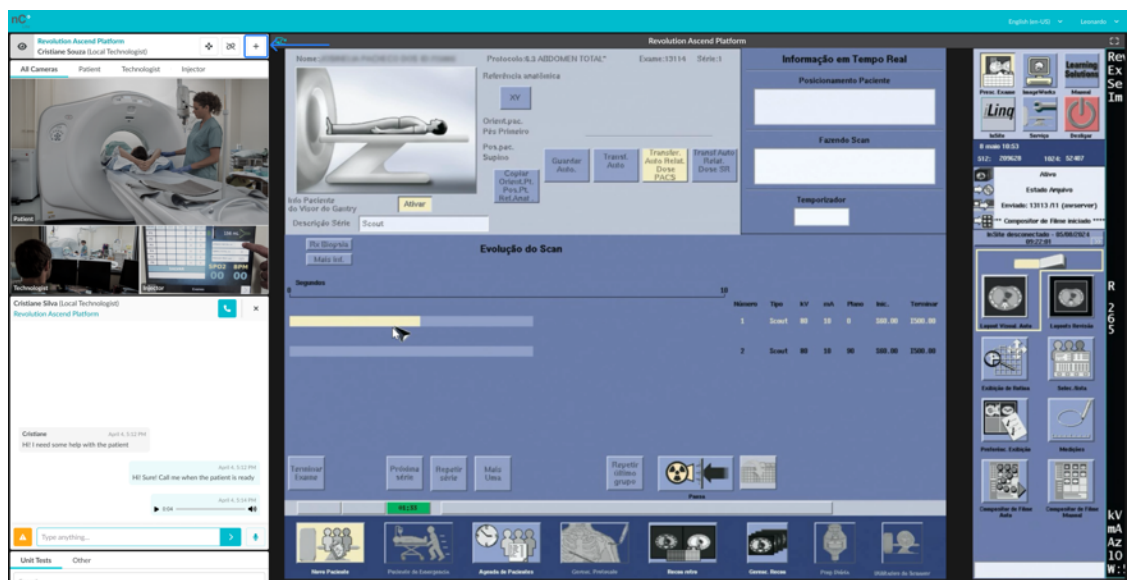


Abbildung 26: Schaltfläche Open Another Device (Ein anderes Gerät öffnen)(+)

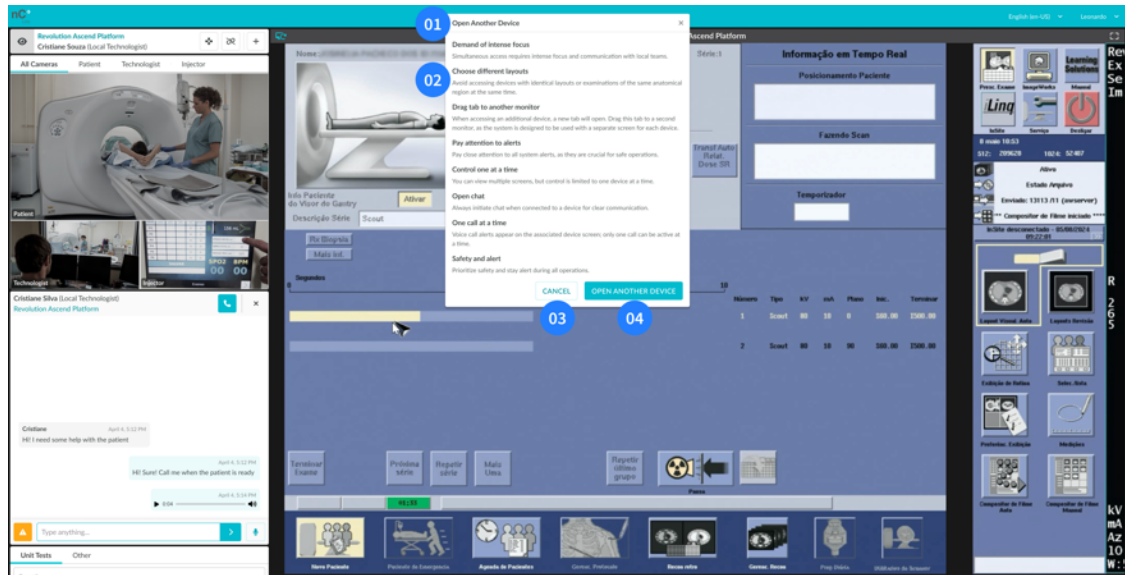


Abbildung 27: Warnungen zum Zugriff über mehrere Geräte

- 01** – Titel Open Another Device (Ein anderes Gerät öffnen); **02** – Warnhinweise zur Betriebssicherheit; **03** – Schaltfläche Cancel (Abbrechen);
04 – Schaltfläche Open Another Device (Anderes Gerät öffnen)

3.5.5. Systemcheck

Die Systemcheck-Funktion hilft zu überprüfen, ob das aktuelle Gerät, Netzwerk und die Internetverbindung den Anforderungen für die ordnungsgemäße Nutzung von nCommand Lite entsprechen. Sie führt einen schnellen automatischen Test durch, der wichtige Elemente wie Internetqualität, Zugang zu den benötigten Servern und die Verbindungsstabilität überprüft. Dieses Tool kann vor Beginn einer Sitzung, während der Installation oder bei Verdacht auf ein Verbindungsproblem verwendet werden. Es hilft sicherzustellen, dass die Plattform wie erwartet funktioniert, und unterstützt das Technologen-Team, falls Fehlerbehebung erforderlich ist.

Hinweis: Der Systemcheck sollte vorzugsweise mit dem Support oder auf Anfrage der IT verwendet werden. Das Ausführen dieses Tools ohne technische Anleitung kann zu einer Fehlinterpretation der Ergebnisse führen.

Um auf den Systemcheck zuzugreifen, müssen Remote-Technologen und Technologen vor Ort die Option Session Details (Sitzungsdetails) aus dem Dropdown-Menü auswählen, das unter ihrem Benutzernamen in der oberen rechten Ecke des Hauptbildschirms verfügbar ist. Klicken Sie dann auf **Open** (Öffnen) neben dem Tool **System Check**. Sobald die Tool-Seite angezeigt wird, klicken Sie auf **Run Test** (Test ausführen), um den Verifizierungsprozess zu starten.

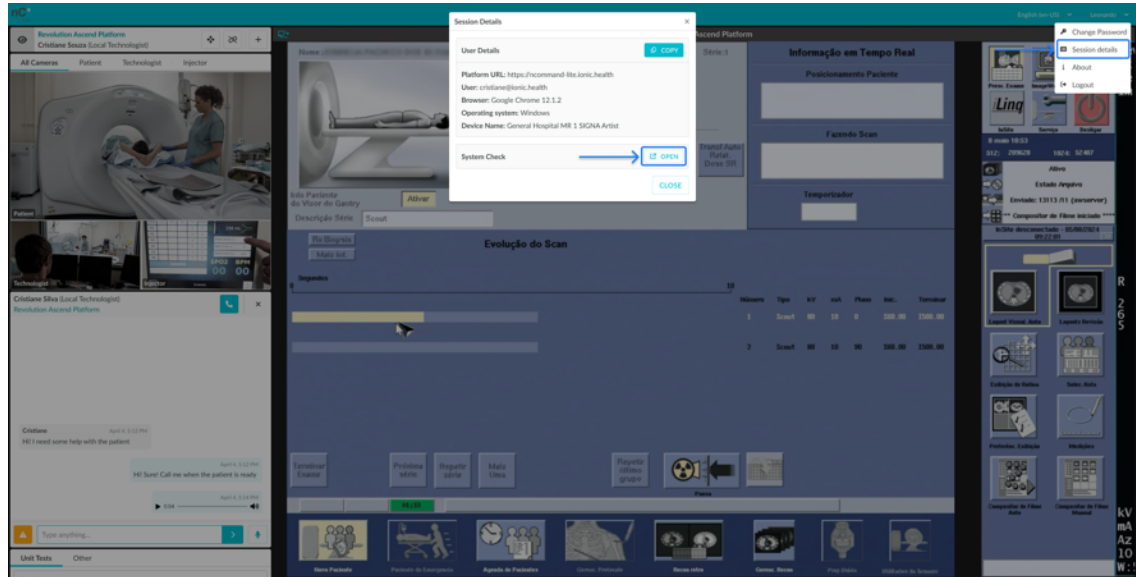


Abbildung 28: Zugriff auf den Systemcheck

Bei der Verwendung des Remote-Technologen ist es möglich, auf dem Hauptbildschirm des Tools ein Gerät auszuwählen, sodass dieses in die Testergebnisse einbezogen wird.

**WARNUNG!**

Bevor Sie den Test beginnen, vergewissern Sie sich, dass das ausgewählte Gerät derzeit nicht verwendet wird.

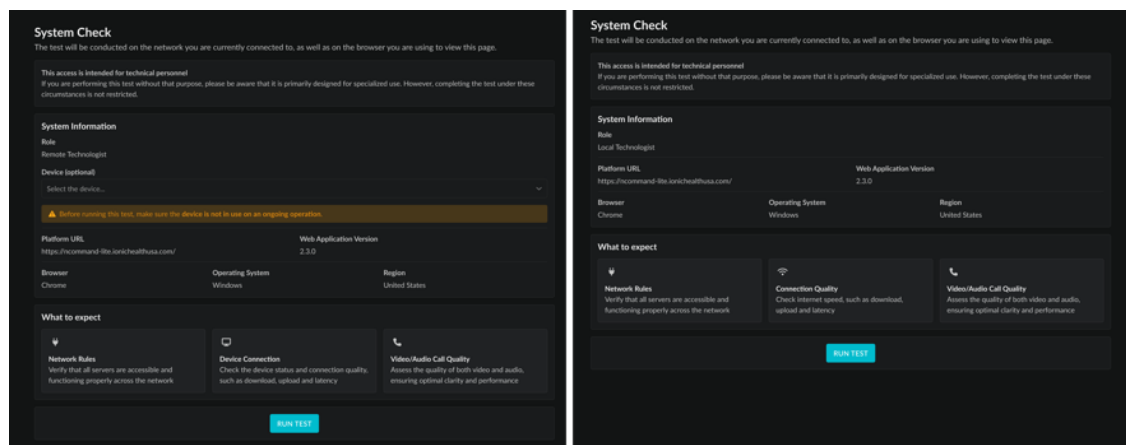


Abbildung 29: Systemcheck-Hauptbildschirm
Links – Remote-Technologie / Rechts – Technologie vor Ort

Nach Abschluss des Tests wird eine Zusammenfassung der Ergebnisse auf dem Bildschirm angezeigt. Die IT kann diese Informationen prüfen, um mögliche Probleme zu identifizieren, die die Systemleistung betreffen.

Abschnitt 3.6 - Chat

Die Plattform bietet einen Echtzeit-Chat und -Anruf mit Sprach- und Videofunktionen, der für eine effektive Kommunikation zwischen lizenzierten Technolgen verwendet wird. Durch diese Funktionen können die lizenzierten Technolgen in allen Belangen im Zusammenhang mit dem Arbeitsablauf der Sitzung miteinander kommunizieren.



WARNUNG!

Rufen Sie im Falle eines Fehlers den Technolgen vor Ort an.

Wenn Sie sich mit einem Gerät verbinden, haben Sie sofortigen Zugriff auf die Chat-Benutzerliste, die in zwei Registerkarten unterteilt ist. Für Kunden mit mehreren Standorten kann jede Filiale als separater Vertrag konfiguriert werden. Wenn diese Funktion aktiviert ist, werden die Benutzer nach Verträgen gruppiert, wobei Benutzer aus anderen Verträgen auf der Registerkarte „Andere“ erscheinen.

Um eine Konversation zu starten, doppelklicken Sie auf den Namen eines Benutzers, um die Chatoberfläche zu öffnen, die sowohl Textnachrichten als auch Sprachanrufe unterstützt. Achten Sie darauf, dass die ausgewählte Sitzung dem richtigen Gerät entspricht. Die Plattform benachrichtigt Benutzer, wenn die Netzwerkverbindung langsam oder instabil wird.



WARNUNG!

Bevor Sie den Kontakt aufnehmen, überprüfen Sie den Gerätenamen, der unter dem Namen des Benutzers angezeigt wird, da einige Remote-Technolgen möglicherweise mit mehreren Geräten verbunden sind.

Hier sind die Tools, die für die Kommunikation innerhalb der Plattform zur Verfügung stehen:

1. **Sprach- und Videoanrufe:** Klicken Sie auf das Symbol, um einen bis zu 60-minütigen Sprach- und Videoanruf zwischen einem Remote-Technologen und einem Technologen vor Ort zu initiieren. Verbindungen zwischen Benutzern mit demselben Profil (Vor Ort–Vor Ort oder Remote–Remote) werden nicht unterstützt.

Wenn ein Technologe vor Ort einen Anruf startet, kann der Remote-Technologe entscheiden, ob er annimmt oder ablehnt. Umgekehrt, wenn ein Remote-Technologe den Anruf initiiert, wird er automatisch verbunden und der Technologe vor Ort wird benachrichtigt. Dies fungiert als Sicherheitsmechanismus, um sicherzustellen, dass der Remote-Technologe immer mit denjenigen kommunizieren kann, die physisch am Standort anwesend sind, als ob sie persönlich anwesend wären.

Standardmäßig ist das Mikrofon zu Beginn des Anrufs aktiv, die Kamera bleibt jedoch ausgeschaltet. Jeder Technologe kann sein Mikrofon und seine Kamera jederzeit manuell ein- oder ausschalten.

Damit ein Anruf erfolgreich hergestellt werden kann, müssen beide Benutzer über ein funktionierendes Mikrofon und einen funktionierenden Audioausgang verfügen und die Browserberechtigungen müssen ordnungsgemäß aktiviert sein. Wenn eine dieser

Komponenten fehlt, benachrichtigt das System beide Benutzer und der Anruf wird nicht abgeschlossen. Eine Kamera ist optional. Wenn sie nicht verfügbar ist oder nicht erkannt wird, aktualisiert das System das Symbol, um anzuzeigen, dass Video nicht unterstützt wird.

Pro Benutzer ist nur ein aktiver Anruf zulässig. Wenn ein Technologe versucht, einen neuen Anruf zu starten, während er sich bereits in einem Anruf befindet, blockiert das System den Versuch und zeigt eine Benachrichtigung an. Wenn ein Benutzer bereits ein Gespräch führt und einen weiteren eingehenden Anruf erhält, wird der Anrufer darüber informiert, dass der Empfänger derzeit nicht erreichbar ist. Der Benutzer des laufenden Gesprächs wird darüber informiert, dass jemand versucht hat, ihn zu erreichen.

2. **Chats schließen:** Wenn einer der Benutzer den Chat durch Klicken auf die Schaltfläche Close (Schließen) schließt, wird eine automatische Nachricht an den anderen Benutzer gesendet und die Registerkarte Chat wird geschlossen. Dadurch wird sichergestellt, dass beide Parteien über das Ende des Gesprächs informiert werden. Wenn das Chat-Fenster geschlossen ist, werden alle Meldungen ausgeblendet. Wenn Sie es während der Sitzung erneut öffnen, wird das Gespräch ohne vorherige Nachrichten fortgesetzt.
3. **Textnachrichten:** Senden Sie Textnachrichten in dem dafür vorgesehenen Feld. Wenn eine Nachricht gesendet wird, wird ein Symbol mit einem grauen Häkchen angezeigt, und wenn die Nachricht beim Empfänger eingeht, wird ein anderes Symbol mit zwei blauen Häkchen angezeigt. Dies ermöglicht eine sichere, klare und prägnante schriftliche Kommunikation zwischen den beiden Parteien.
4. **Bitte um Aufmerksamkeit:** Wecken Sie die Aufmerksamkeit des anderen Benutzers, indem Sie auf die Schaltfläche mit dem Ausrufezeichen klicken. Diese Aktion bewirkt, dass das Fenster des anderen Benutzers für einige Sekunden mit einem visuellen Vibrationseffekt versehen wird und automatisch eine Nachricht gesendet wird, die auf Dringlichkeit oder Wichtigkeit hinweist.
5. **Sprachnachrichten:** Senden Sie Sprachnachrichten, indem Sie auf die Schaltfläche Mikrofon klicken. Dies wird verwendet, wenn Sie eine Nachricht persönlicher übermitteln möchten oder wenn das Tippen nicht praktisch ist.

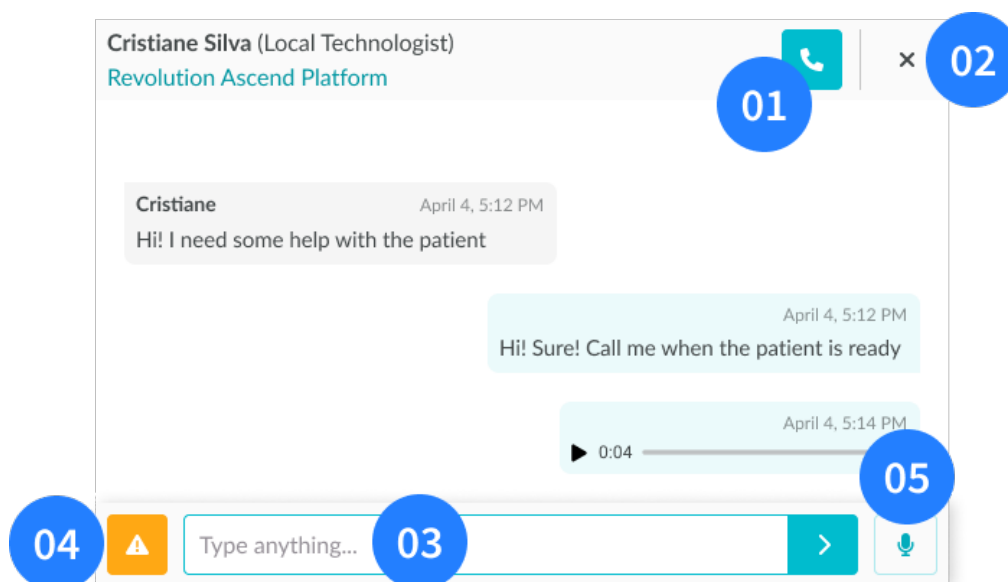


Abbildung 30: Chatfensteransicht

- 01 – Schaltfläche Voice and Video Call (Sprach- und Videoanruf); 02 – Schaltfläche Close Chat (Chat schließen); 03 – Textfeld für Nachrichten; 04 – Schaltfläche Call for attention (Aufmerksamkeit anfordern); 05 – Schaltfläche Record Audio Message (Sprachnachricht aufnehmen)

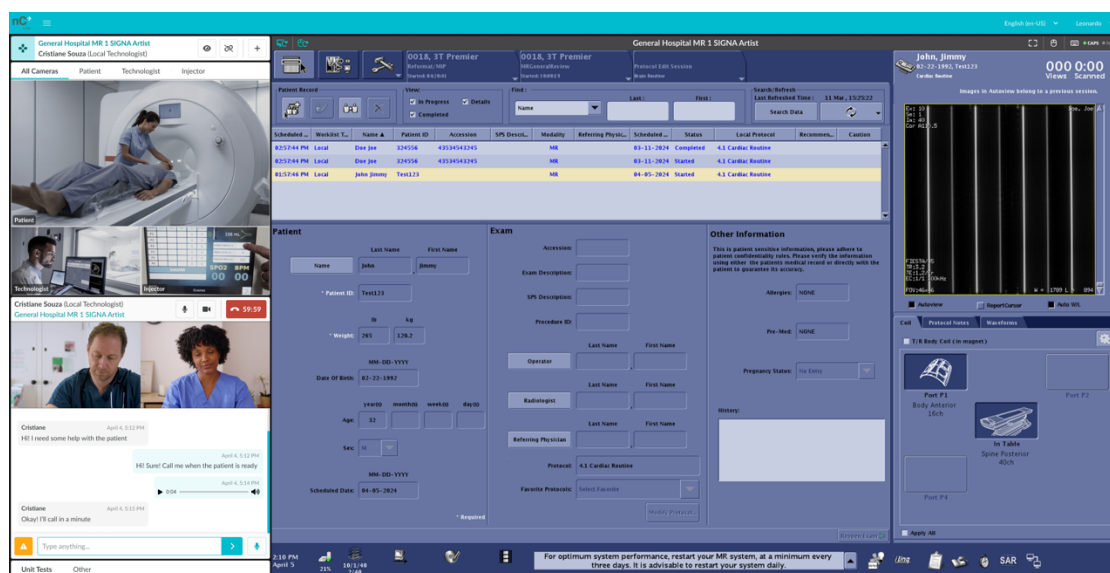


Abbildung 31: Hauptbildschirm des Remote-Technologen – Chatfenster (untere linke Ecke)

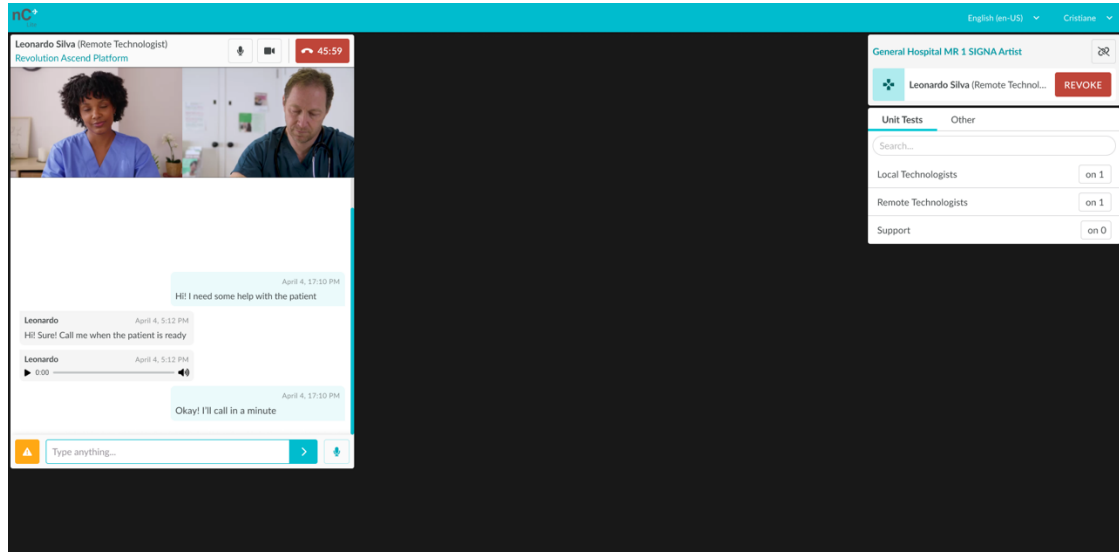


Abbildung 32: Hauptbildschirm des Technologen vor Ort – Chatfenster

Probleme mit der Internetverbindung – Wenn einer der Technologen Probleme mit der Netzwerkverbindung hat, zeigt das System eine Meldung an und versucht, die Verbindung wieder herzustellen. Wenn die Verbindung wiederhergestellt wird, zeigt das System eine **ONLINE**-Meldung an und die Remote-Sitzung wird wie gewohnt fortgesetzt. Wenn die Verbindung jedoch nach mehreren erneuten Verbindungsversuchen nicht wiederhergestellt wird, beendet das System die aktive Sitzung und informiert den Technologen darüber, dass sie aufgrund von Internetproblemen getrennt wurden. Gleichzeitig wird es den anderen Technologe darüber informieren, dass sein Gegenüber aufgrund von Internetproblemen getrennt wurde.

Abschnitt 3.7 - Beenden Ihrer Sitzung auf der Plattform

Am Ende seiner Arbeit muss der lizenzierte Technologie die Verbindung zum Gerät trennen und sich von der Plattform abmelden.



WARNUNG!

Die lizenzierten Technolgen dürfen nicht vergessen, sich vor Beendigung ihres Dienstes von der Plattform abzumelden.

Um die Verbindung zum Gerät zu trennen, müssen Sie auf das Symbol Trennen klicken, das sich in der Gerätebox befindet. Hinweis: Wenn Sie als Technologie vor Ort arbeiten, vergewissern Sie sich, dass Sie sämtliche Zugriffsrechte des Remote-Technologen widerrufen haben, bevor Sie die Verbindung zum Gerät trennen.

Zur Gewährleistung der Sicherheit erhalten Sie eine Benachrichtigung, um zu bestätigen, dass Sie die Verbindung zum Gerät trennen möchten. Nach der Bestätigung werden Sie zum Startbildschirm weitergeleitet, ohne dass ein Gerät ausgewählt wurde.

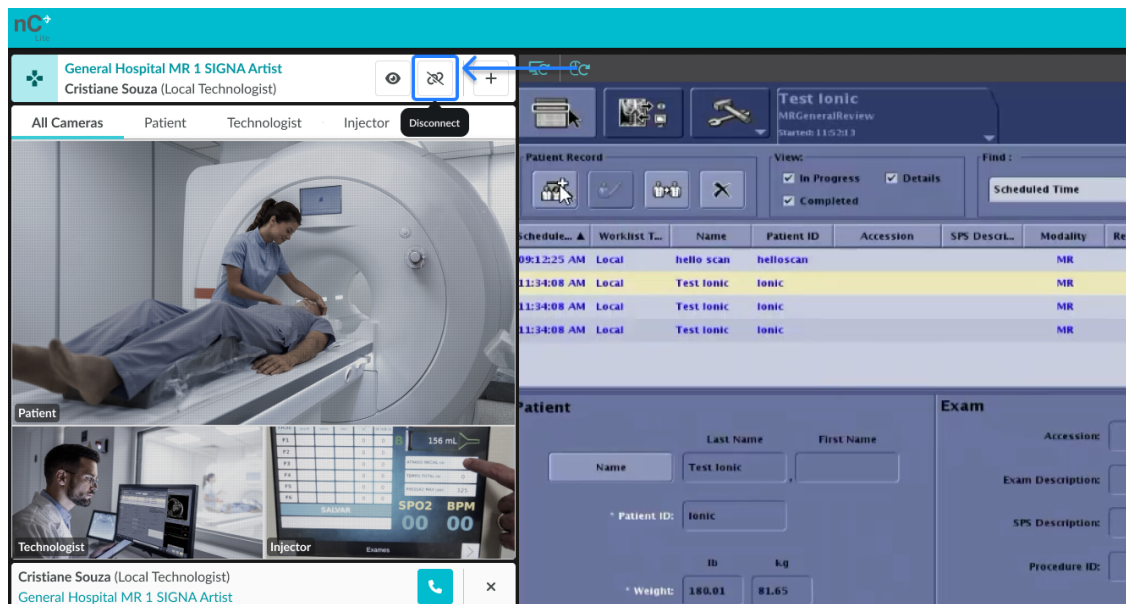


Abbildung 33: Schaltfläche Disconnect (Trennen) – Hauptbildschirm des Remote-Technologen

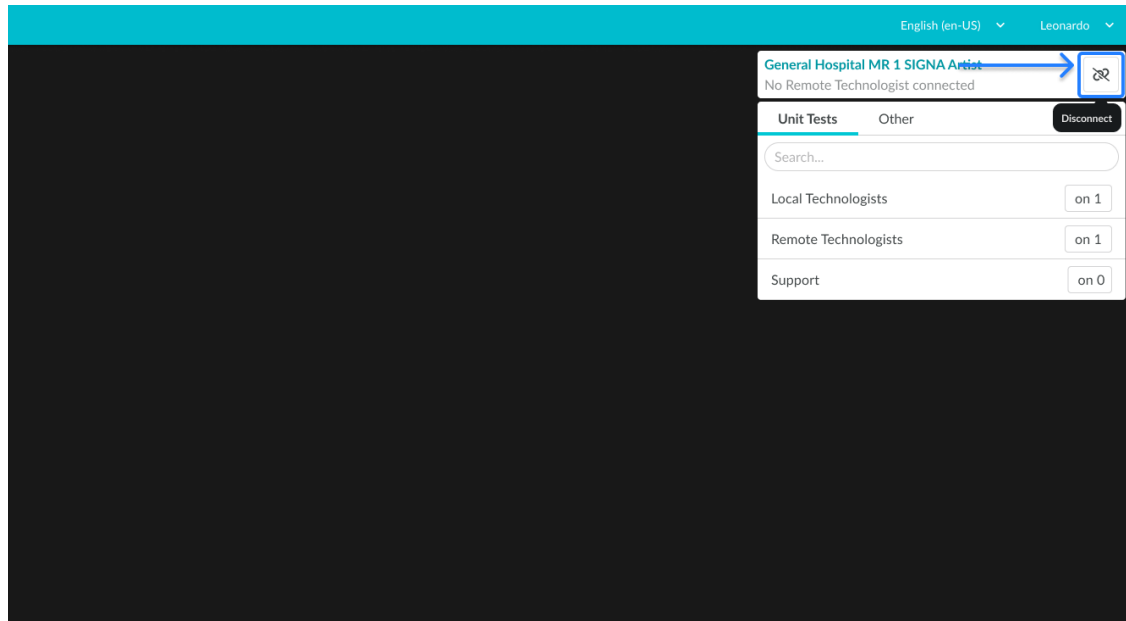


Abbildung 34: Schaltfläche Disconnect (Trennen) – Hauptbildschirm des Technologen vor Ort



WARNUNG!

Stellen Sie vor dem Abmelden sicher, dass alle weiteren geöffneten Registerkarten geschlossen sind.

Um Ihre Sitzung auf der Plattform zu beenden, klicken Sie auf Ihren Benutzernamen in der oberen rechten Ecke des Bildschirms und wählen Sie die Option „Logout“ (Abmelden). Sie erhalten eine Benachrichtigung, um zu bestätigen, dass Sie das medizinische Zentrum, in dem Sie gearbeitet haben, verlassen möchten. Nach der Bestätigung werden Sie zur Anmeldeseite der Anwendung weitergeleitet, um Ihre Arbeit sicher abzuschließen.

nCommand Lite steuert die Sitzung des Benutzers auf dem External IdP nicht und kann daher keine Abmeldung auf IdP-Ebene durchführen. In Szenarien, in denen Benutzer denselben Computer verwenden und Single Sign-On (SSO) nutzen, wird empfohlen, dass jeder Benutzer während der Anmeldung beim External IdP (falls verfügbar) die Option „Nicht angemeldet bleiben“ auswählt oder sich nach dem Abmelden von nCommand Lite vom IdP abmeldet. Dadurch wird sichergestellt, dass kein nachfolgender Benutzer auf demselben Gerät unbeabsichtigt eine aktive Sitzung wiederverwenden kann.

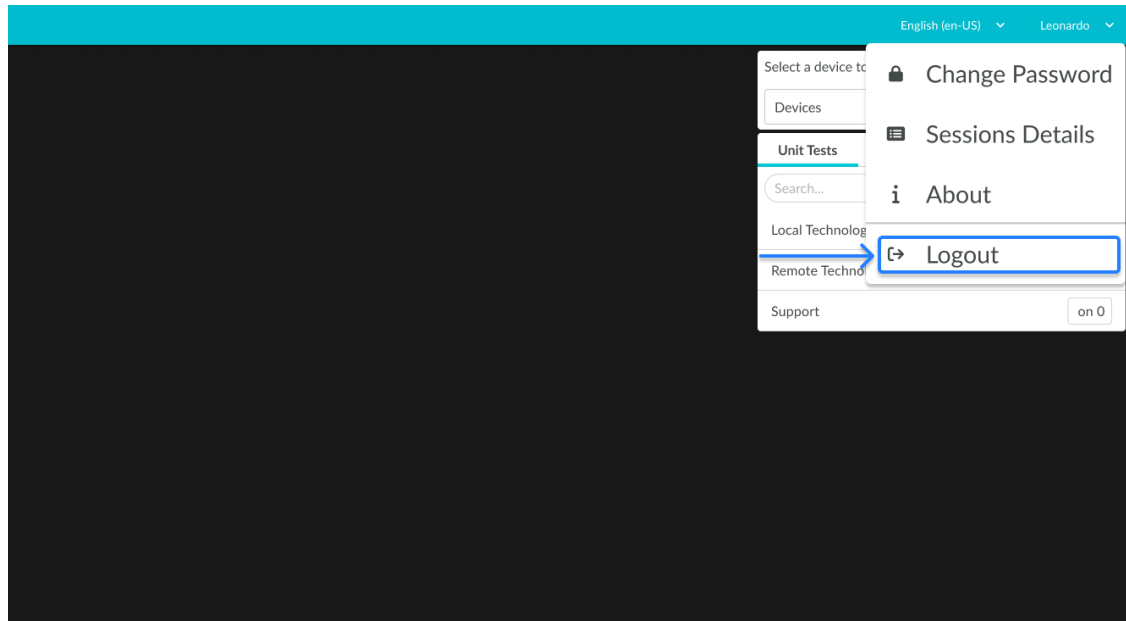


Abbildung 35: Abmelden Dropdown-Menüpunkt



WARNUNG!

Wenn Sie einen External Identity Provider auf einem gemeinsam genutzten oder öffentlichen Computer verwenden, melden Sie sich nach der Anmeldung bei der Plattform auch beim Identitätsanbieter ab. Weitere Informationen zum weiteren Vorgehen erhalten Sie vom IT-Supportteam Ihrer Einrichtung.

Abschnitt 3.8 - Betriebsschulung

Die Teilnahme am Schulungsprogramm ist für alle Benutzer des nCommand Lite Systems verpflichtend. Die Benutzerregistrierung auf der Plattform wird vom IONIC Health-Team verwaltet. Sie wird erst eingeleitet, nachdem bestätigt wurde, dass der Benutzer die erforderliche LMS-Schulung erfolgreich abgeschlossen hat und ordnungsgemäß für die Bedienung der Plattform qualifiziert ist. Mit diesem Prozess wird gewährleistet, dass alle Benutzer die Funktionen des Systems gründlich kennen und in der Lage sind, die Plattform effizient und sicher zu nutzen. Um den Anmeldeprozess für die Schulung zu starten, wenden Sie sich bitte an Ihren Vertriebsmitarbeiter.

Abschnitt 3.9 - Richtlinien zur Fehlerbehebung

BENUTZER UND PASSWORT	
Passwortänderung	Bestätigen Sie, dass die Passwortanforderungen erfüllt wurden, das Kennwort stark und sicher ist und mindestens einen Kleinbuchstaben, einen Großbuchstaben, ein Sonderzeichen enthält sowie mindestens 8 Zeichen lang ist.
Passwort vergessen	Überprüfen Sie Ihren E-Mail-Posteingang: Stellen Sie sicher, dass Sie die richtige E-Mail-Adresse verwenden und dass die E-Mail zur Passwortwiederherstellung nicht in Ihren Spam- oder Junk-Ordner gefiltert wurde. Versuchen Sie es erneut: Warten Sie einige Minuten und fordern Sie eine weitere E-Mail zur Passwortwiederherstellung an, indem Sie auf „Did you Forget your password?(Passwort vergessen?)“ klicken. Internetverbindung prüfen: Stellen Sie sicher, dass Sie mit dem Internet verbunden sind.
Willkommens-E-Mail nicht erhalten	Prüfen Sie, ob sich die E-Mail in Ihrem Spam-Ordner befindet. Wenn sie nicht vorhanden ist, wenden Sie sich an einen Admin-Benutzer, um sicherzustellen, dass die in Ihrer Registrierung angegebene E-Mail korrekt ist. Wenn sie nicht korrekt ist, sollte der Administrator sie aktualisieren und die Willkommens-E-Mail erneut senden.
Zwei-Faktor-Authentifizierungscode nicht erhalten	Klicken Sie auf „Resend Code“ (Code erneut senden) und überprüfen Sie Ihren Spam-Ordner. Wenn Sie ihn nicht erhalten, wenden Sie sich bitte an einen Admin-Benutzer, um zu überprüfen, ob die in der Zugriffskontrolle registrierte E-Mail korrekt ist.

Überschrittene Anmeldeversuche	Wenn Sie die zulässige Anzahl von Anmeldeversuchen überschreiten, müssen Sie eine Zeitlang warten, bevor Sie es erneut versuchen.
EXTERNAL IDENTITY PROVIDER	
Probleme beim Anmelden beim Produkt	Wenn Sie bei der Verwendung eines External Identity Providers (IdP) auf Anmeldeprobleme stoßen, beachten Sie bitte, dass der Authentifizierungsprozess vollständig vom IdP und nicht vom Produktanbieter verwaltet wird, d. h.: Ionic Health. Daher kann das Produkt nicht bei Kontoanmeldeinformationen, Zugriffsrichtlinien, Authentifizierungsfehlern oder Kontosperrungen helfen. In diesen Fällen sollten Sie sich an das IT-Supportteam Ihrer Einrichtung wenden, das die IdP-Konfiguration überprüfen und bei der Behebung des Problems helfen kann.
Probleme mit Anmeldeinformationen	Alle Probleme im Zusammenhang mit Anmeldeinformationen (z. B. vergessenes Kennwort, Kennwortänderung) müssen direkt mit dem IT-Supportteam Ihrer Einrichtung gelöst werden. Sie können die IdP-Konfiguration überprüfen und die erforderliche Unterstützung leisten.
Probleme mit dem Multi-Faktor-Authentifikator (MFA)	Alle Probleme im Zusammenhang mit dem Multi-Faktor-Authentifikator (MFA) (z. B., Probleme mit dem Ablauf von MFA, MFA funktioniert nicht, Anmeldung ohne Anforderung von MFA) müssen direkt mit dem IT-Supportteam Ihrer Einrichtung gelöst werden. Sie können die IdP-Konfiguration überprüfen und die erforderliche Unterstützung leisten.
Anmeldeinformationen funktionieren nicht auf der Plattform	Wenn Sie External Identity Provider (IdP) verwenden, melden Sie sich nur mit dem IdP beim Produkt an. Die Verwendung der IdP-Anmeldeinformationen direkt auf der Anmeldeseite des Produkts führt zu einem Fehler bei der Anmeldung.
SCANNER-COMPUTER-MONITOR	
Schaltet sich nicht ein	Überprüfen Sie die Verbindungen des Monitors zum Computer und zur

	Steckdose. Es kann zu einer Unterbrechung der Verbindung kommen. Drücken Sie die Ein/Aus-Taste des Monitors erneut.
PLATTFORM	
Nicht erreichbar	Überprüfen Sie die Netzwerkverbindung. Prüfen Sie, ob die Plattform gestartet wurde und ob die Anmeldung stattgefunden hat.
Plattform-Latenz	Aktualisieren Sie die Seite, indem Sie Strg+F5 drücken. Prüfen Sie, ob der Chat des Geräts (der medizinischen Einrichtung) in mehr als einer Registerkarte geöffnet ist. Wenn ja, schließen Sie die nicht verwendete Registerkarte. Wenn das Problem weiterhin besteht, versuchen Sie, sich von der Plattform abzumelden, den Cache zu löschen, den Browser zu schließen und sich dann erneut anzumelden.
Fehlerhafte Funktionen	Bevor Sie andere Verfahren zur Fehlerbehebung ausprobieren, leeren Sie nach der Anmeldung den Browser-Cache (suchen Sie nach entsprechenden Anweisungen für Ihren aktuellen Browser), schließen Sie den Browser, öffnen Sie ihn erneut, melden Sie sich wieder bei der Plattform an und versuchen Sie die Aktion erneut.
Aktualisieren	Nachdem die Plattform aktualisiert wurde, leeren Sie Ihren Browser-Cache (siehe Anweisungen für Ihren Browser), bevor Sie sich bei der neuen Version anmelden.
AUDIO	
Kein Ton	Stellen Sie sicher, dass die Mikrofon- und Lautsprecherlautstärken des Geräts (der medizinischen Einrichtung) auf die entsprechenden Pegel eingestellt sind. Prüfen Sie, ob der Browser über die Berechtigung zur Verwendung von Audio und Mikrofon verfügt.

	Überprüfen Sie, ob das Headset angeschlossen ist und ordnungsgemäß funktioniert.
Ton-Latenz	Überprüfen Sie die elektrischen Anschlüsse und Netzwerkverbindungen des Geräts. Aktualisieren Sie die Browserseite, indem Sie Strg+F5 drücken, und melden Sie sich erneut an. Wenn das Problem weiterhin besteht, versuchen Sie, sich von der Plattform abzumelden, den Cache zu löschen, den Browser zu schließen und sich dann erneut anzumelden.
CHAT	
Chat erscheint nicht	Stellen Sie sicher, dass der Browser nicht minimiert ist. Andernfalls öffnen Sie den Chat, nachdem Sie sich bei der nCommand Lite-Plattform angemeldet haben. Überprüfen Sie, ob die Einheit (die medizinische Einrichtung) ausgewählt wurde und der Benutzer berechtigt ist, die Chat-Kommunikation zu aktivieren. Stellen Sie sicher, dass die Audio- und Mikrofonberechtigungen Ihres Browsers akzeptiert werden. Überprüfen Sie die Kabelverbindungen, die möglicherweise getrennt sind. Aktualisieren Sie die Browserseite, indem Sie Strg+F5 drücken und die Verbindung zur Plattform wieder herstellen. Prüfen Sie, ob der Chat des Standorts in mehr als einer Registerkarte geöffnet ist. Wenn ja, schließen Sie die nicht verwendete Registerkarte.
Chat-Verzögerung	Aktualisieren Sie die Browserseite, indem Sie Strg+F5 drücken und die Verbindung zur Plattform wieder herstellen.

	Wenn das Problem weiterhin besteht, versuchen Sie, sich von der Plattform abzumelden, den Cache zu löschen, den Browser zu schließen und sich dann erneut anzumelden. Überprüfen Sie die Kabelverbindungen, die möglicherweise getrennt sind.
Problem beim Senden von Sprachnachrichten	Überprüfen Sie die Browser-Berechtigungen für Audio und Mikrofon und stellen Sie sicher, dass sowohl Mikrofon als auch Audiogeräte mit dem Computer verbunden sind. Wenn die Berechtigungen des Browsers geändert werden müssen, drücken Sie Strg+F5, um den Browser aufzufordern, die Änderungen beim erneuten Laden der Seite zu erkennen.
Sprachanruf konnte nicht gestartet werden	Überprüfen Sie Ihre Internetverbindung und prüfen Sie, ob eine Benachrichtigung angezeigt wurde, die den Grund für den nicht gestarteten Anruf erklärt. Stellen Sie sicher, dass ein Audiogerät angeschlossen ist und dass Audio- und Mikrofonberechtigungen im Browser zugelassen sind. Wenn das Problem weiterhin besteht, aktualisieren Sie die Seite mit Strg+F5, um es erneut zu versuchen.
Benutzer im Chat nicht gefunden	Wenn Sie einen Benutzer im Chat nicht finden können, klicken Sie auf die Registerkarte „Others“ (Sonstige), um sicherzustellen, dass er nicht dort aufgeführt ist. Benutzer, die mit anderen Verträgen verbunden sind, werden separat in der Kontaktliste aufgeführt. Wenn Ihr Benutzer nach der Auswahl des Geräts nicht in der Kontaktliste erscheint, drücken Sie Strg+F5, um den Bildschirm zu aktualisieren und erneut auszuwählen. Stellen Sie sicher, dass Sie eine Internetverbindung haben.
ZUGRIFF AUF DAS GERÄT BEANTRAGEN	
Plattform hat nicht erkannt, dass der Technologie vor Ort verbunden ist	Aktivieren Sie die Option „Others“ (Sonstige), um zu bestätigen, ob der Benutzer vor Ort verbunden ist. Wenn

	der Benutzer tatsächlich verbunden ist, aber Sie immer noch die Meldung erhalten, dass der Benutzer vor Ort nicht mit dem Scanner verbunden ist, aktualisieren Sie den Bildschirm, indem Sie Strg+F5 drücken, und bitten Sie den Benutzer vor Ort, die gleiche Anweisung zu wiederholen. Wählen Sie dann das Gerät erneut aus und bitten Sie den Benutzer vor Ort, das Gerät ebenfalls erneut auszuwählen. Wenn das Problem weiterhin besteht, wenden Sie sich an den Support, um das Netzwerk zu überprüfen.
Zugriffsanfrage wird nicht gesendet	Aktualisieren Sie die Seite, indem Sie Strg+F5 drücken, und bestätigen Sie mit dem Benutzer vor Ort per Chat, ob die Zugriffsanfrage empfangen wurde. Wenn das Problem weiterhin besteht, wenden Sie sich bitte an den Support, um weitere Unterstützung zu erhalten.
STREAMING-GERÄT (e-KVM COMPUTER)	
Streaming-Gerät (e-KVM COMPUTER) funktioniert nicht	Klicken Sie auf der Plattform auf die Schaltfläche Reload streaming (Streaming neu laden). Stellen Sie sicher, dass die unterbrechungsfreie und stabilisierte Stromversorgung (medizinische Einrichtung) und/oder das Streaming-Gerät korrekt angeschlossen und eingeschaltet sind. Schalten Sie das Streaming-Gerät und alle anderen Geräte aus und wieder ein. Aktualisieren Sie die Plattform.
Streaming-Gerät langsam	Klicken Sie auf der Plattform auf die Schaltfläche Reload streaming (Streaming neu laden). Aktualisieren Sie die Seite mit Strg+F5 und stellen Sie erneut eine Verbindung zur Plattform her. Überprüfen Sie die Qualität Ihrer Netzwerkverbindung.

	Um den Netzwerkstatus zu überprüfen, kann ein Ping-Test zum Gerät durchgeführt werden, um den Datenverlust zu ermitteln. Nach Internetproblemen funktioniert die Plattform möglicherweise nicht wie vorgesehen. Aktualisieren Sie die Webseite und fordern Sie erneut den Zugriff auf den Benutzer vor Ort an.
Verlust der Videoausgabe	Es ist durchaus möglich, dass eine elektrostatische Entladung zu einem Verlust des Bildes führt. Nach einem Neustart des Systems sollten die Kommunikation und das Videostreaming automatisch wiederhergestellt werden.

Abschnitt 3.10 - Methoden zur Reinigung der Hardware

- Vor Beginn des Reinigungsvorgangs sicherstellen, dass alle Geräte von der Steckdose getrennt sind.
- Keine scheuernden Produkte verwenden.
- Geräte oder Peripheriegeräte nicht in Flüssigkeiten jeglicher Art eintauchen.
- Entsorgen Sie Reinigungsmaterialien gemäß den Vorschriften für die Entsorgung von Sondermüll.
- Es ist nicht ratsam, Sprühdesinfektionsmittel zu verwenden, da Dämpfe in das Gerät eindringen und einen Kurzschluss oder Korrosion verursachen können.
- Dieses Produkt ist nicht steril.

Kapitel 4 Cybersicherheit und Datenschutz

Abschnitt 4.1 - Sicherheits- und Datenschutzrisiken

Das **nCommand Lite System** implementiert mehrere technische und organisatorische Maßnahmen zum Schutz der verarbeiteten Informationen.

Das System ist nach ISO/IEC 27001 und ISO/IEC 27701 zertifiziert und verfolgt einen Privacy-by-Design-Ansatz. Unterstützt die Einhaltung der Datenschutzgesetze im Gesundheitswesen sowie der Cybersicherheitsvorschriften, die in der EU, den USA, dem Vereinigten Königreich, der Schweiz, Brasilien, den Vereinigten Arabischen Emiraten, Saudi-Arabien, Australien und Neuseeland gelten.

Benutzer müssen jedoch bewährte Verfahren anwenden, um eine unnötige Offenlegung sensibler Daten zu verhindern.

- Geben Sie keine persönlichen oder sensiblen Informationen weiter, es sei denn, dies ist unbedingt erforderlich.
- Stellen Sie sicher, dass die Kommunikation und der Systemzugriff in sicheren Umgebungen erfolgen.
- Wenn Sie böswillige Aktivitäten vermuten, benachrichtigen Sie sofort das zuständige Team.

Abschnitt 4.2 - Schutz personenbezogener Daten (Einhaltung von DSGVO / HIPAA)

Das **nCommand Lite System** erfüllt alle geltende Datenschutzgesetze und -vorschriften in den Regionen, in denen es tätig ist, einschließlich, aber nicht beschränkt auf DSGVO, HIPAA, LGPD und ISO/IEC 27701-Anforderungen. Alle Datenverarbeitungstätigkeiten erfolgen in der Rolle des „**Auftragsverarbeiters**“ sowie des „**Unterauftragsverarbeiters**“ im Sinne der DSGVO, unter strikter regionaler Datentrennung, um die Einhaltung der gesetzlichen Vorgaben sicherzustellen und unzulässige grenzüberschreitende Datenübermittlungen zu verhindern.

Welche Daten werden erfasst?

- **Benutzer:** Name, E-Mail-Adresse und Unternehmen (ausschließlich für Authentifizierung und Zugriffsverwaltung).
- **Patientendaten:** Nur Übertragungen von medizinischen Untersuchungen per Streaming in Echtzeit, ohne Datenspeicherung

Wie werden Daten verwendet und geschützt?

- Die Daten werden ausschließlich für die **Authentifizierung, die Zugriffskontrolle und die Rückverfolgbarkeit von Sitzungen** verwendet.
- Die Informationsübertragung wird durch **AES-256-Verschlüsselung für die Speicherung** und **TLS 1.3 für Daten während der Übertragung** gesichert.

- **Der Zugriff ist eingeschränkt** und folgt dem **Prinzip der geringsten Privilegien (RBAC)**.
- Ende-zu-Ende-Verschlüsselung für P2P-Video- und Steuerungs-Streams über WebRTC sichergestellt.
- Autorisierte Cloud-Anbieter (z. B. Microsoft Azure) verarbeiten begrenzte Daten unter strengen vertraglichen Schutzmaßnahmen.

Den Benutzern werden folgende Rechte gewährt:

- **Zugang zu und Korrektur** von personenbezogenen Daten.
- **Antrag auf Datenlöschung**, wo zutreffend.

Wenn Sie Fragen haben, senden Sie eine E-Mail an privacy@ionic.health, um den Datenschutzbeauftragten von Ionic Health zu erreichen. Alle Anfragen werden innerhalb von 30 Tagen bearbeitet und können gemäß DSGVO verlängert werden.

Abschnitt 4.3 - Zugriffsverwaltung und Authentifizierung

Die Benutzer sind dafür verantwortlich, die **Zugriffsrollen und -berechtigungen** für ihre Teams festzulegen und sicherzustellen, dass die gewährten Zugriffsrechte regelmäßig überprüft und dokumentiert werden.

Best Practices und Kontrollen

- Folgen Sie dem **Prinzip der geringsten Privilegien (RBAC)**, um sicherzustellen, dass Benutzer nur über die erforderlichen Zugriffsrechte verfügen.
- **Die Multi-Faktor-Authentifizierung (MFA)** ist für den administrativen Zugriff obligatorisch und wird für alle Benutzer empfohlen.
- **Es sind sichere Passwörter** mit mindestens **8 Zeichen erforderlich, die Groß- und Kleinbuchstaben, Zahlen und Symbole enthalten**.
- **Geben Sie keine Anmeldeinformationen weiter.**
- Die Zugriffsberechtigungen werden regelmäßig überwacht und überprüft.

Überwachung: Zugriff, Änderungen von Berechtigungen und wichtige Aktivitäten werden in den Sicherheitsprotokollen des Systems dokumentiert. Protokolle werden in Übereinstimmung mit HIPAA, GDPR und anderen geltenden Vorschriften mindestens 6 Jahre lang aufbewahrt. Sie dienen der internen Auditierung, der forensischen Analyse und der aufsichtsrechtlichen Berichterstattung. Die Protokolle sind vor Manipulationen geschützt und werden in sicheren Umgebungen mit Zugriffskontrolle gespeichert.

Abschnitt 4.4 - Systemcheck-Zugriffskontrolle

Die Systemcheck-Funktion ist ausschließlich über die **nCommand Lite Web Application** zugänglich und erfordert gültige Zugangsdaten für die Anmeldung. Der Zugriff ist ausschließlich autorisierten Rollen vorbehalten – *Remote-Technologe*, *Technologe vor Ort*, *Admin*, *Rollenverantwortlicher* und *Systemcheckbenutzer*.

Die Rolle *Systemcheckbenutzer* ist mit eingeschränkten Berechtigungen konzipiert, die ausschließlich den Zugriff auf diagnostische Funktionen im Zusammenhang mit

Netzwerkvalidierung und Konnektivitätsverifikation ermöglichen. Dies stellt sicher, dass Netzwerkdetails, Whitelisting-Informationen und Systemmetriken niemals unbefugten Personen zugänglich gemacht werden.

Alle Zugriffsanfragen werden über Azure AD B2C authentifiziert, mit Multi-Faktor-Authentifizierung (MFA) und adaptiven Zugriffsrichtlinien, die von Microsoft Entra ID verwaltet werden. Die Passwortkomplexität richtet sich nach der unternehmensweiten Sicherheitsrichtlinie und erfordert mindestens acht Zeichen, darunter Groß- und Kleinbuchstaben, Zahlen sowie Symbole. Passwörter laufen alle 90 Tage ab, und Sitzungen melden sich nach 24 Stunden Inaktivität automatisch ab, was bei kontinuierlicher Nutzung bis zu 90 Tage verlängerbar ist

Abschnitt 4.5 - Regionale Datentrennung und Logbuchaufbewahrung

Die **nCommand Lite** -Plattform hält eine strikte regionale Datentrennung aufrecht, um unautorisierte oder unnötige grenzüberschreitende Übertragungen zu verhindern. Die Umgebungen sind pro Region isoliert, um die Einhaltung der geltenden Vorschriften sicherzustellen.

Alle Zugriffsprotokolle, Aktivitätsaufzeichnungen und Sicherheitsereignisse werden mindestens sieben (7) Jahre lang aufbewahrt, gemäß den geltenden Datenschutz- und Gesundheitsvorschriften. Protokolle werden in sicheren, zugriffskontrollierten Umgebungen gespeichert und sind vor Manipulationen geschützt. Diese Informationen unterstützen forensische Untersuchungen, Compliance-Audits und regulatorische Berichterstattung.

Abschnitt 4.6 - Datensicherheit und -integrität

Das **nCommand Lite System** gewährleistet die Vertraulichkeit, Integrität und Verfügbarkeit von Daten durch branchenübliche Sicherheitspraktiken.

Benutzer sollten die Einhaltung der Sicherheitsprotokolle sicherstellen, die Zugriffsrichtlinien regelmäßig überprüfen und jegliche Anomalien melden. Das System überwacht kontinuierlich die Aktivitäten, und Administratoren müssen Sicherheitsrichtlinien durchsetzen, um eine robuste Verteidigung gegen potenzielle Bedrohungen aufrechtzuerhalten.

Das System wird durch eine rund um die Uhr verfügbare Überwachung durch ein spezielles Security Operations Center (SOC) mit SIEM-Funktionen zur Erkennung von und Reaktion auf Bedrohungen geschützt.

Abschnitt 4.7 - Reaktion auf Sicherheitsvorfälle

Das System beinhaltet einen dokumentierten Plan zur Reaktion auf Sicherheitsvorfälle, der mit ISO 27035 und NIST CSF übereinstimmt.

Bei Sicherheitsvorfällen, wie z. B. unbefugtem Zugriff oder Systemausfällen, müssen Benutzer folgende Schritte befolgen:

Wie erkennt man einen Vorfall?

- **Nicht autorisierter Zugriff** in Aktivitätsprotokollen festgestellt.
- **Verdächtige Anmeldeversuche** oder wiederholte Authentifizierungsfehler.
- **Ungewöhnliches Systemverhalten**, wie unerwartete Aktionen oder Fehlfunktionen.

Wie meldet man einen Vorfall?

Melden Sie das Ereignis sofort über die verfügbaren Supportkanäle (Kapitel 5).

Wird eine Verletzung des Schutzes personenbezogener Daten bestätigt, wird IONIC in seiner Rolle als Unterauftragsverarbeiter GE als Auftragsverarbeiter innerhalb von 48 Stunden informieren und dabei alle relevanten Nachweise, Angaben zu den Auswirkungen sowie die ergriffenen oder geplanten Abhilfemaßnahmen bereitstellen. GE ist seinerseits dafür verantwortlich, den Verantwortlichen (den Kunden) gemäß den jeweils geltenden gesetzlichen und vertraglichen Anforderungen zu informieren.

Kapitel 5 Servicekanäle

Ob Sie Hilfe bei einem technischen Problem, einem unklaren Schritt im Prozess oder weitere Anleitung benötigen, unser Team steht Ihnen gerne zur Seite. Sie können uns per Telefon, E-Mail oder über die ITSM-Plattform kontaktieren, je nachdem, was für Sie am bequemsten ist. Unsere Spezialisten sind in der Bereitstellung personalisierter Unterstützung geschult und stellen sicher, dass jedes Problem schnell und effizient gelöst wird.

Telefonnummern

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

ITSM-Plattform

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

E-Mail

helpdesk@ionic.health



WARNUNG!

Jeglicher schwerwiegende Vorfall im Zusammenhang mit der Verwendung dieses Produkts sollte sowohl dem Hersteller als auch der Gesundheitsbehörde/zuständigen Behörde, in der das Produkt installiert ist, gemeldet werden.

Um dies dem Hersteller zu melden: wenden Sie sich entweder an Ihren lokalen Kundendienstvertreter oder melden Sie es an: helpdesk@ionic.health

Bitte geben Sie die folgenden Informationen an:

- Die Systemversionsnummer, die auf dem Anmeldebildschirm angezeigt wird;
- Datum des Vorfalls;
- Beschreibung des Vorfalls, einschließlich jeglicher Auswirkungen/Verletzungen bei Patienten oder Anwender;
- Ihre Kontaktinformationen (Einrichtung, Adresse, Kontaktnamen, Titel und Telefonnummer).

Kapitel 6 Rechtliche und regulatorische Informationen

Hersteller



nCommand Lite

IONIC HEALTH TECHNOLOGIES S.A.

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

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

Verantwortlicher Technologe

Alexandre Seiji Fukuda Ribas
CREA-SP: 5071085437

ANVISA

82585300004

Importeur (USA)



nCommand Lite System

IONIC HEALTH USA INC.

11201 Cedar Avenue, STE 600
Cleveland, OH 44106
USA

+1 (216) 242 1223

EU-Vertreter/Importeur



nCommand Lite



Kennnummer der Benannten Stelle: 2803

EUROPE IONIC HEALTH DIGITAL TECHNOLOGIES, LDA

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

+351 (300) 528 410

Schweizer Bevollmächtigter (CH-REP) / Importeur**CH REP****REF**

nCommand Lite

FREYR LIFE SCIENCES GMBH

Bahnhofplatz
CH-6300 Zug
Schweiz

UK-Verantwortlicher / Importeur**REF**

nCommand Lite

FREYR LIFE SCIENCES LTD

9 Greyfriars Road
Reading, Berkshire
RG1 1NU
England, Vereinigtes Königreich

Australischer Sponsor**REF**

nCommand Lite

TAEVAS LIFE SCIENCES PTY LTD

46 Dora St
Blacktown NSW 2148
Australien

Neuseeländischer Sponsor**REF**

nCommand Lite

TAEVAS LIFE SCIENCES LIMITED

Level 3, 1 Margaret Street
Lower Hutt 5010
Neuseeland

Basis-UDI-DI: 7898974112NCLITE2L

Anforderung einer Papierversion

Ausdrucke des nCommand Lite Benutzerhandbuchs werden auf Anfrage kostenlos zur Verfügung gestellt. Wenden Sie sich an Ihren örtlichen Vertreter und fordern Sie eine Papierversion des Benutzerhandbuchs an.

Herstellungsdatum

Das Datum der Softwarefreigabe ist auf der Anmeldeseite von nCommand Lite im Format MONAT/JAHR zu finden.

Kapitel 7 Überarbeitungsverlauf

Überarbeitung	Beschreibung der Änderung	Datum
0	Handbuchversion von 2.3 v1 auf 2.4 aktualisiert	25. November 2025
1	Beschriftungen in Kapitel 6 aktualisiert	04. Dezember 2025
2	Die Anforderung einer statischen IP-Adresse aus der lokalen Computerkonfiguration wurde in Unterabschnitt 1.3.11 entfernt Das Symbol des EU-Bevollmächtigten in Unterabschnitt 1.3.12 aktualisiert Hinweis aus Unterpunkt 1.3.14 entfernt Inhalt in Kapitel 2 aktualisiert Das Symbol des EU-Bevollmächtigten in Kapitel 6 aktualisiert	28. Januar 2026
3	Die Übersetzung von „Verantwortlicher Techniker“ in Kapitel 6 wurde überprüft.	09. Februar 2026

ANHANG I - Checkliste für den Wartungsbeginn

1. Elektrische Anschlüsse und Netzwerkverbindungen überprüfen:

Stellen Sie sicher, dass die elektrischen Anschlüsse und Netzwerkpunkte auf dem e-KVM-Computer, Scanner-Computer und dem lokalen Computer ordnungsgemäß eingerichtet sind.

2. Stromstatus überprüfen:

Sicherstellen, dass die unterbrechungsfreie und stabilisierte Stromversorgung und der e-KVM-Computer eingeschaltet sind und korrekt funktionieren.

3. Schnellzugriff auf die nC Lite-Plattform:

Bestätigen Sie, dass die Verknüpfung der nC Lite-Plattform auf dem Desktop vorhanden ist, damit Sie schnell darauf zugreifen können.

4. Zugriff auf und Anmeldung bei der nC Lite-Plattform:

Öffnen Sie die nCommand-Plattform und melden Sie sich an, um vollständigen Zugriff und ordnungsgemäße Funktionalität zu gewährleisten.

5. Einrichtung der Chat-Anwendung:

Öffnen Sie die Chat-Anwendung innerhalb der nC Lite-Plattform in nur einer Registerkarte und minimieren Sie sie nicht, um eine nahtlose Kommunikation zu gewährleisten.