



MANUEL DE L'UTILISATEUR

nCommand Lite v2.4

Version du manuel : V.3



Table des matières

Chapitre 1 Introduction.....	4
Section 1.1 - Objectif.....	4
Section 1.2 - Glossaire	4
Section 1.3 - Description	5
1.3.1. Utilisation prévue	5
1.3.2. Indications d'utilisation.....	6
1.3.3. Population de patients visée.....	6
1.3.4. Environnement d'utilisation.....	6
1.3.5. Contre-indications.....	6
1.3.6. Fonctionnalités de la plateforme.....	6
1.3.7. Avantages cliniques.....	7
1.3.8. Utilisateurs prévus	7
1.3.9. Environnement de fonctionnement.....	7
1.3.10. Environnement de l'établissement.....	8
1.3.11. Exigences minimales	10
1.3.12. Symboles.....	11
1.3.13. Durée de vie	12
1.3.14. Mise à niveau / Mise à jour	12
Chapitre 2 Liste des avertissements et précautions d'ordre général	13
Chapitre 3 Utilisation de la plateforme selon l'emplacement	16
Section 3.1 - Accès et utilisation de nCommand Lite	16
Section 3.2 - Accès à la plateforme pour la première fois.....	16
3.2.1. Connectez-vous via nCommand Lite	17
3.2.2. Connexion via un fournisseur d'identité externe	18
Section 3.3 - Gestion des mots de passe.....	20
Section 3.4 - Accès avec profil d'opérateur local	22
Section 3.5 - Accès avec profil d'opérateur à distance	25
3.5.1. Mode d'accès	26
3.5.2. Barre de streaming	29
3.5.3. Multi-caméras	32
3.5.4. Open Another Device (Ouvrir un autre appareil)	34
3.5.5. Vérification du système	36
Section 3.6 - Chat.....	37

Section 3.7 - Mettre fin à votre session sur la plateforme	41
Section 3.8 - Formation opérationnelle	43
Section 3.9 - Directives de dépannage	44
Section 3.10 - Méthodes de nettoyage du matériel	49
Chapitre 4 Cybersécurité et confidentialité	50
Section 4.1 - Risques liés à la sécurité et à la confidentialité.....	50
Section 4.2 - Protection des données personnelles (conformité RGPD / HIPAA).....	50
Section 4.3 - Gestion des accès et authentification	51
Section 4.4 - Commande d'accès à la vérification système	51
Section 4.5 - Ségrégation régionale des données et conservation des journaux	52
Section 4.6 - Sécurité et intégrité des données.....	52
Section 4.7 - Réponse aux incidents de sécurité	52
Chapitre 5 Canaux de service.....	54
Chapitre 6 Informations juridiques et réglementaires	55
Chapitre 7 Historique des révisions	58
ANNEXE I - Liste de contrôle pour le début de l'entretien	59

**MISE EN GARDE**

En vertu de la loi fédérale, cet appareil ne peut être vendu que par un médecin ou sur ordonnance médicale et utilisé par un opérateur médical agréé dans l'État où il/elle exerce.

(pour les États-Unis d'Amérique)

**MISE EN GARDE**

Au Brésil, ce logiciel est autorisé par Anvisa pour une utilisation exclusivement avec un appareil d'imagerie par résonance magnétique (IRM). Toute autre utilisation est interdite.

(pour une utilisation au Brésil)

**MISE EN GARDE**

Avant toute utilisation, assurez-vous de connaître les exigences spécifiques de votre pays ou région. Le non-respect des réglementations peut entraîner des risques pour la santé.

**MISE EN GARDE**

Assurez-vous que la version de ce manuel d'utilisation correspond à la version de la plateforme utilisée. L'utilisation d'une version inadaptée peut entraîner un fonctionnement incorrect ou une mauvaise interprétation des fonctionnalités.

Chapitre 1 Introduction

Section 1.1 - Objectif

Ce manuel vise à fournir aux opérateurs locaux et à distance une compréhension complète des fonctionnalités spécifiques du système nCommand Lite. À titre de manuel de l'utilisateur, ce document fournit des informations concises et pratiques, guidant les utilisateurs à travers les fonctionnalités du système et le dépannage. En suivant ce manuel, les utilisateurs pourront utiliser nCommand Lite efficacement, ce qui contribue à optimiser la productivité et à réduire la dépendance à l'assistance technique.

Section 1.2 - Glossaire

**MISE EN GARDE**

Cette étiquette s'applique aux conditions ou actions présentant un danger potentiel. Vous pouvez provoquer des blessures légères ou des dommages matériels si vous ignorez ces instructions.

**AVERTISSEMENT**

Cette étiquette identifie les conditions ou les actions qui entraînent un danger spécifique. Si vous ignorez ces instructions, vous risquez de provoquer des blessures corporelles graves ou des dommages matériels importants.

Terme utilisé sur la plateforme	Terme correspondant
Installation d'imagerie	Établissement médical, unité, unités mobiles, établissement de santé, unité de soins de santé
Établissement distant	Poste de travail distant, Lieu distant, Bureau distant, Emplacement éloigné, Centre de commande
Plateforme	Application Web nCommand Lite
Système	nCommand Lite avec tous les sous-systèmes
Appareil	Scanner médical, Scanner, Équipement, Dispositif médical, Appareil d'imagerie, Équipement d'imagerie
Opérateur local	Utilisateur local, Technicien local, Professionnel de santé local (LHP), Utilisateur sur site

Section 1.3 - Description

Le système nCommand Lite est un SaMD (logiciel en tant que dispositif médical) destiné au client et offrant un accès à distance via une application web pour visualiser/réviser des images, ainsi que la possibilité de fournir à distance des instructions en temps réel à l'opérateur agréé (utilisateur local) se trouvant à proximité du patient et utilisant les appareils d'imagerie médicale dans le cadre de la formation ou de l'évaluation des procédures, pour les scanners IRM, de tomodensitométrie ou de TEP/TDM.

Les utilisateurs à distance sont des opérateurs agréés, qui peuvent accéder, partout, à un appareil médical d'imagerie à partir d'un ordinateur qui répond aux spécifications minimales requises, en utilisant une connexion logicielle sécurisée qui diffuse la vidéo et fournit un accès au clavier et à la souris. Cela permet aux utilisateurs à distance d'aider les utilisateurs locaux sans que la distance soit un inconvénient. Cet accès doit être accordé par l'utilisateur local utilisant le système, et il peut également être révoqué à tout moment par l'utilisateur local, ce qui lui permet de garder le contrôle total de la session à tout moment. De plus, chaque session à distance est contrôlée par le biais d'un identifiant sécurisé géré par l'utilisateur local. Les connexions à un appareil médical sont limitées à une session à distance à la fois pour garder un contrôle strict sur les personnes qui interagissent à distance avec le système. Les images examinées à distance ne sont pas destinées à des fins diagnostiques.

Le système nCommand Lite se compose d'une solution d'installation informatique basée sur le matériel et le logiciel, qui prend en charge plusieurs sessions, permettant aux opérateurs à distance d'accéder à plusieurs appareils d'imagerie médicale selon les besoins. Les scanners compatibles avec le système nCommand Lite sont conformes à un protocole commun, permettant la gestion des paramètres d'analyse et l'analyse à distance.

1.3.1. Utilisation prévue

Le système nCommand Lite offre un accès à distance pour la visualisation/l'analyse d'images, ainsi que la possibilité de fournir à distance des instructions en temps réel à l'opérateur agréé

qui utilise le scanner. Ces orientations comprennent la formation, l'évaluation de la procédure et la gestion des paramètres d'analyse.

1.3.2. Indications d'utilisation

Le système nCommand Lite permet l'accès à distance pour visualiser/examiner des images, ainsi que la possibilité de fournir à distance des instructions en temps réel à l'opérateur agréé utilisant un scanner IRM, de tomodensitométrie ou de TEP/TDM compatible. Cet accès doit être accordé par l'opérateur local agréé qui utilise le système. L'accès à distance n'est disponible que pour les systèmes prenant en charge la fonctionnalité de connectivité à distance. Les images examinées à distance ne sont pas destinées à des fins diagnostiques.

1.3.3. Population de patients visée

Pour tout patient à qui l'on a prescrit des examens d'imagerie via un appareil d'imagerie médicale connecté.

1.3.4. Environnement d'utilisation

Les centres d'imagerie qui effectuent des examens d'imagerie par résonance magnétique (IRM), de tomodensitométrie (TDM) et de tomographie par émission de positons/tomodensitométrie (TEP/TDM) ainsi que les centres de commande à distance.

1.3.5. Contre-indications

La plateforme ne doit pas être utilisée par des utilisateurs qui ne sont pas des opérateurs agréés et qui n'ont pas reçu de formation sur l'utilisation de nCommand Lite.

1.3.6. Fonctionnalités de la plateforme

- **Analyse à distance** : affiche l'écran de l'appareil d'imagerie médicale en temps réel, permettant à un opérateur à distance agréé d'assister à un examen.
- **Chat** : permet la communication entre les opérateurs à distance et les opérateurs locaux agréés par le biais de messages texte et vocaux. Les opérateurs locaux et à distance peuvent également passer et recevoir des appels vocaux et vidéo.
- **Multi-caméras** : facilite l'observation à distance des patients et de l'établissement médical pendant la procédure. L'opérateur à distance peut accéder à la visualisation des caméras par le biais des onglets qui sont divisés entre tous les onglets de la caméra et les différents onglets. Ce mécanisme reproduit la surveillance visuelle qu'un professionnel de santé assurerait s'il se trouvait à proximité du patient, introduisant ainsi une couche de sécurité accrue.
- **L'analyse à distance multisession** : permet à l'opérateur à distance d'accéder à plusieurs appareils d'imagerie médicale selon les besoins.
- **Access Mode (Mode d'accès)** : permet à l'opérateur à distance de choisir entre les affichages ou de commander l'appareil. En mode Afficher, les opérateurs à distance ne peuvent visualiser que ce qui est en cours de diffusion. En mode Commande, l'opérateur a le contrôle de la souris et du clavier.
- **Gérer l'accès de l'opérateur à distance** : permet à l'opérateur local de contrôler l'accès de l'opérateur à distance et son mode d'accès (View [Afficher] ou Control [Commande]). Pour permettre la connexion de l'opérateur à distance, l'accès doit être accordé par l'opérateur local à l'aide de la plateforme, et il peut également être révoqué à tout moment.

par l'opérateur local, ce qui permet à celui-ci de garder le contrôle total de la session à tout moment.

- **Taille du streaming** : l'opérateur à distance peut voir la taille d'origine du streaming et la taille actuelle du streaming en pixels. Il est également notifié lorsque la taille actuelle du streaming est inférieure à la taille d'origine.
- **État de la souris et du clavier** : l'opérateur à distance reçoit un feedback sur le bon fonctionnement de la souris et du clavier de l'appareil d'imagerie médicale.
- **Détails de la session** : les opérateurs locaux et à distance peuvent accéder aux détails de la session.

1.3.7. Avantages cliniques

nCommand Lite améliore l'imagerie diagnostique en permettant la commande à distance des systèmes **IRM, TDM et TEP-TDM**, garantissant une qualité d'imagerie constante et le respect des protocoles. Il permet aux opérateurs expérimentés de surveiller et d'aider aux analyses en temps réel, d'optimiser l'efficacité du flux de travail et de réduire les erreurs susceptibles d'affecter la précision du diagnostic. Le système facilite la collaboration entre les opérateurs, améliorant la cohérence des examens et permettant une prise de décision plus rapide dans les cas complexes. En permettant aux professionnels à distance de prendre en charge plusieurs établissements, **nCommand Lite** augmente **la disponibilité, la variété et la qualité** des examens d'imagerie, garantissant ainsi que plus de patients ont accès à des diagnostics avancés tout en optimisant les ressources en soins de santé. De plus, il contribue à atténuer les pénuries de personnel en réduisant la dépendance aux spécialistes sur site, tout en assurant la conformité aux normes réglementaires et de sécurité des données strictes.

1.3.8. Utilisateurs prévus

- **Opérateur local**
L'opérateur local est l'utilisateur sur site chargé d'aider et d'orienter les patients en personne dans l'établissement médical. Il doit disposer de connaissances nécessaires pour effectuer les procédures d'analyse avec un appareil d'imagerie donné. De plus, il contrôle le mode d'accès de l'opérateur à distance (View [Afficher] ou Control [Commande]) et l'accès à distance doit être accordé par l'opérateur local via la plateforme et peut être révoqué à tout moment.
- **Opérateur à distance**
Professionnel qui effectue des opérations à distance, en accédant à l'ordinateur de l'appareil et en le contrôlant. Comme l'opérateur local, l'opérateur à distance doit également disposer de connaissances nécessaires pour effectuer les procédures d'analyse avec un appareil d'imagerie donné.
- **Utilisateur du service d'assistance/informatique**
Professionnel responsable de la configuration de la plateforme (non inclus dans ce manuel de l'utilisateur).

1.3.9. Environnement de fonctionnement

Les spécifications suivantes se rapportent aux exigences environnementales de l'ordinateur e-KVM.

- **Altitude maximale (sans pressurisation)**
 - En fonctionnement : de 0 m (0 pi) à 3 048 m (10 000 pi)
 - Stockage : de 0 m (0 pi) à 12 192 m (40 000 pi)
- **Température**
 - En fonctionnement : de 10 °C (50 °F) à 35 °C (95 °F)
 - Stockage : de -10 °C (14 °F) à 50 °C (122 °F)
- **Humidité relative**
 - En fonctionnement : 20 % à 80 % (sans condensation)
 - Stockage : 10 % à 90 % (sans condensation)

1.3.10. Environnement de l'établissement

La plateforme nCommand Lite possède deux types d'emplacements d'environnement différents :

- **Centre d'imagerie** : Établissements qui effectuent des examens d'imagerie par résonance magnétique (IRM), de tomodensitométrie (TDM) ou de tomographie par émission de positons/tomodensitométrie (TEP/TDM).
- **Établissement à distance** : Un endroit où les technologues à distance peuvent accéder aux équipements et les gérer à distance (scanners IRM, TDM ou TEP/TDM). Ce poste de travail peut être utilisé dans divers environnements tels que des bureaux, des centres de commande, des sites distants ou même des emplacements secondaires au sein de l'établissement de santé. Le poste de travail distant peut être installé dans tout espace offrant à l'utilisateur des conditions appropriées pour la concentration, ainsi que les exigences minimales en matière de connectivité et de configuration informatique.

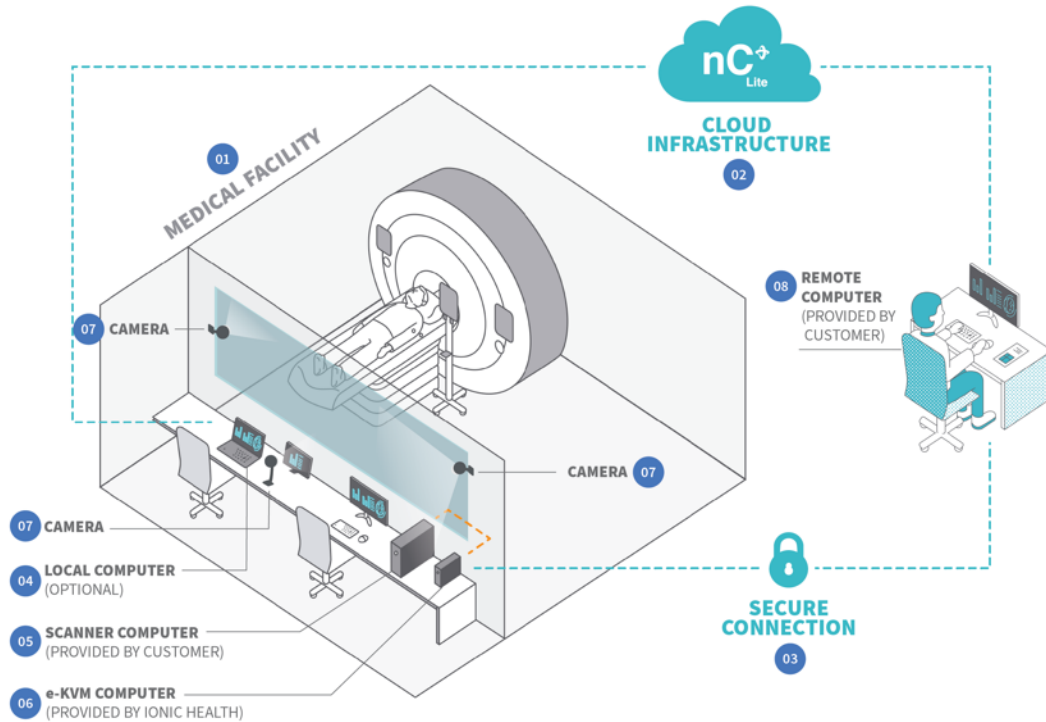


Figure 01 : Présentation du produit et de ses connexions par le biais d'une connexion sécurisée (p. ex. VPN).

01 – Établissement médical ; 02 – Infrastructure cloud ; 03 – Connexion sécurisée ; 04 – Ordinateur local (optionnel) ; 05 – Ordinateur du scanner (fourni par le Client) ; 06 – e-KVM (fourni par IONIC Health) ; 07 – Caméra ; 08 - Ordinateur distant (fourni par le client)



AVERTISSEMENT !

Compatibilité avec la numérisation à distance

IONIC Health (IH) valide la fonctionnalité de numérisation à distance sur les appareils compatibles répertoriés. IH effectue une évaluation complète des exigences de numérisation à distance d'IH et teste le système dans l'environnement cible lors de l'installation. Cela garantit la compatibilité et les performances appropriées à ce moment-là pour la numérisation à distance. Cette vérification n'implique pas que toutes les exigences du dispositif OEM (Original Equipment Manufacturer) sont satisfaites dans cette configuration. Tout écart par rapport aux exigences OEM est de la responsabilité de l'utilisateur final.

Les modifications apportées au système ou à l'environnement après l'installation doivent être signalées à IH pour vérifier la compatibilité continue. IH ne peut garantir les performances ni assumer la responsabilité de configurations différentes de celles validées lors de l'installation.

1.3.11. Exigences minimales

- **Ordinateur local**

Cet ordinateur est utilisé par l'**opérateur local** pour autoriser et prendre en charge l'accès à distance de l'appareil via nCommand Lite®. Il permet également une communication directe avec l'**opérateur à distance** via la fonction chat de la plateforme.

Les spécifications techniques minimales requises sont les suivantes :

- Processeur : AMD® A4-9120C ou supérieur, ou similaire
- Mémoire : 4 Go ou plus
- Stockage : SSD 128 Go ou plus
- Périphériques : microphone et haut-parleur, ou casque et webcam
- Moniteur : FHD 14" (1920 x 1080) ou supérieur
- Système d'exploitation : Chrome OS, Windows OS ou MAC OS
- Site d'installation : cet ordinateur doit se trouver à proximité de l'ordinateur du scanner
- Routine informatique : Créez un raccourci nCommand Lite sur le bureau de chaque utilisateur
- Compatibilité avec les navigateurs : Google Chrome ou Microsoft Edge.

- **Poste de travail à distance**

Ce poste est utilisé par l'**opérateur à distance** pour accéder à l'appareil et le contrôler via nCommand Lite®. Le poste de travail distant doit établir une connexion sécurisée avec l'ordinateur e-KVM (fournie par IONIC HEALTH®).

Le client est responsable de la mise à disposition de l'ordinateur distant et choisira l'un des deux scénarios suivants : soit un fonctionnement 24 heures sur 24, 7 jours sur 7, soit un fonctionnement pendant les heures ouvrables.

Pour chaque scénario, vous trouverez ci-dessous les spécifications appropriées pour choisir les modèles d'ordinateurs :

Scénario 1 (fonctionnement 24 h/24, 7 J/7) - Doit répondre aux spécifications suivantes :

- Intel Xeon W-2223 (4 cœurs, 8 threads, 8,25 Mo de mémoire cache, 3,90 GHz Turbo) ou supérieur.
- RAM : 16 Go ou plus.
- Carte graphique : NVIDIA RTX A2000 6GB ou supérieur, ou similaire.
- Stockage : SSD 128 Go ou plus.
- Système d'exploitation : Windows 11 Professionnel 64 bits ou supérieur.
- Configuration minimale requise pour le moniteur : Taille 27", rapport d'aspect 16:9, résolution 4k.
- Casque : BLACKWIRE 3200 ou similaire.
- Compatibilité avec les navigateurs : Google Chrome ou Microsoft Edge.

Scénario 2 (fonctionnement pendant les heures ouvrables) - Doit répondre aux spécifications suivantes :

- Intel® Core™ i7-12700k vPro® ou supérieur.
- RAM : 16 Go ou plus.
- Carte graphique : NVIDIA T400 GB ou supérieur, ou similaire.
- Stockage : SSD 128 Go ou plus.

- Système d'exploitation : Windows 11 Professionnel 64 bits ou supérieur.
- Configuration minimale requise pour le moniteur : Taille 27", rapport d'aspect 16:9, résolution 4k.
- Casque : BLACKWIRE 3200 ou similaire.
- Compatibilité avec les navigateurs : Google Chrome ou Microsoft Edge.

**AVERTISSEMENT !**

Le non-respect des conditions d'installation appropriées et des exigences minimales peut entraîner une dégradation ou une interruption de communication entre les utilisateurs.

- **Configurations réseau (exigences minimales)**

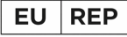
Pour établir la session entre l'utilisateur distant et l'ordinateur e-KVM, la communication réseau entre les deux périphériques doit être assurée. Le système nCommand Lite utilise le peer-to-peer (P2P) pour établir la connexion entre l'utilisateur local, l'utilisateur distant et l'ordinateur e-KVM. Il existe trois scénarios compatibles :

- **Scénario 1** – Réseau d'entreprise qui utilise l'un des protocoles suivants : LAN, LAN-to-LAN, MPLS ou VPN ;
- **Scénario 2** – Réseau d'entreprise qui utilise un réseau étendu (WAN) de confiance (réseau externe) et n'utilise aucun des protocoles suivants : LAN, LAN-to-LAN, MPLS ou VPN ;
- **Scénario 3** – Réseau public du côté de l'ordinateur distant (utilisateur distant).

Les configurations pour chaque scénario sont détaillées dans la documentation technique.

1.3.12. Symboles

Symbole	Description	Référence
	Fabricant	ISO 15223-1, ISO 7000-3082
	Date de fabrication	ISO 15223-1, ISO 7000-2497
	Le symbole indique que ce produit est un appareil médical	ISO 15223-1
	Identifiant unique du dispositif	ISO 15223-1
	Référence du modèle	ISO 15223-1, ISO 7000-2493
	Importateur	ISO 15223-1, ISO 7000-3725
	Consulter le manuel de l'utilisateur	ISO 15223-1, ISO 7000-1641

	Distributeur	ISO 15223-1, ISO 7000-3724
	Mise en garde	ISO 15223-1, ISO 7000-0434A
	Avertissement	ISO 7010-W001
	Numéro de série (ou version logicielle)	ISO 15223-1, ISO 7000-2498
	Représentant autorisé dans la Communauté européenne	ISO 15223-1
	Représentant autorisé en Suisse (CH-REP)	ISO 15223-1
	CE - Marquage de conformité européenne ; 2803 – Désignation de l'organisme notifié	Règlement UE 2017/745

1.3.13. Durée de vie

La durée de vie prévue du produit est de 5 ans, compte tenu de la durée de vie utile des composants qui composent le produit. Cette évaluation complète garantit que la durée de vie de chaque composant critique est alignée sur la durée de vie globale, assurant ainsi des performances et une fiabilité constantes pendant toute la durée prévue du produit.

1.3.14. Mise à niveau / Mise à jour

IONIC Health mettra à jour le système nCommand Lite dans le cadre d'une maintenance planifiée ou de mises à jour. Ces mises à jour sont conçues pour garantir la continuité des performances et de la fiabilité sans perturber la version actuellement déployée sur les sites des clients. Selon la nature de la mise à jour, le produit peut être mis à niveau à distance ou nécessiter la visite d'un ingénieur sur site.

Chapitre 2 Liste des avertissements et précautions d'ordre général



AVERTISSEMENT !

Veuillez lire tous les avertissements ci-dessous avant d'utiliser le système nCommand Lite.



MISE EN GARDE

Le système nCommand Lite ne peut pas faire l'objet d'une réparation ou d'un entretien lorsqu'il est utilisé pour contrôler un équipement d'IRM, de tomodensitométrie ou de TEP-TDM en présence d'un patient.

- Faites particulièrement attention à toutes les alertes du système, car elles sont essentielles à la sécurité des opérations.
- Donnez la priorité à la sécurité et à l'attention pendant toutes les opérations.
- En vertu de la loi fédérale, cet appareil ne peut être vendu que par un médecin ou sur ordonnance médicale et utilisé par des opérateurs médicaux agréés dans l'État où ils/elles exercent.
- Le système nCommand Lite ne doit être utilisé que par des opérateurs ayant reçu une formation sur l'utilisation de la plateforme.
- Utilisez ce système uniquement avec des navigateurs Web compatibles. Les navigateurs pris en charge sont Google Chrome et Microsoft Edge.
- En cas d'urgence, un opérateur formé et agréé doit rester dans l'établissement d'imagerie pour effectuer l'opération d'IRM, de TDM ou de TEP/TDM sans le système nCommand Lite.
- L'accès simultané à plusieurs appareils exige une concentration intense et une communication avec les équipes locales.
- Evitez d'accéder à des appareils dont la disposition est identique ou d'examiner la même région anatomique en même temps.
- Vous pouvez visualiser plusieurs écrans, mais la commande est limitée à un seul appareil à la fois.
- Lancez toujours un chat lorsque vous êtes connecté à un appareil pour une communication claire.
- Les alertes d'appel apparaissent sur l'écran de l'appareil associé ; un seul appel peut être actif à la fois.
- Testez la communication vidéo lorsque vous accédez à l'application (avant le début d'une session de travail) pour vérifier s'il y a une défaillance dans la connexion de sortie vidéo des appareils IRM, TDM, TEP/TDM ou de tout autre appareil lié au streaming vidéo.
- L'appareil ne doit pas être branché sur la prise et/ou sur l'alimentation électrique sans coupure et stabilisée par le biais de rallonges ou de « barres multiprises ».
- En cas de défaillance vidéo, vérifiez la connexion vidéo entre le système de l'appareil et l'ordinateur e-KVM.
- Si l'application est lente en accès à distance, actualisez la page avec les commandes Ctrl+F5 dans le navigateur de l'ordinateur de l'opérateur à distance. Si le problème persiste, contactez l'assistance technique.
- Chaque fois que la page du navigateur est actualisée, la connexion à l'appareil est interrompue, ce qui rend nécessaire la répétition du processus d'approbation.

- Ne vous connectez pas en utilisant un navigateur différent lorsque vous êtes déjà connecté.
- L'établissement d'imagerie du client doit disposer d'une liaison Internet redondante avec un fournisseur différent du fournisseur principal pour un changement immédiat de liaison en cas de perte de communication du système/de la plateforme.
- En cas de perte de communication ou de ralentissement de la souris, effectuez une « resynchronisation de la souris » sur la page utilisée dans le navigateur.
- Assurez-vous que les ordinateurs utilisés pour le contrôle du système nCommand Lite, à la fois dans l'établissement d'imagerie et dans le centre de commande, répondent aux exigences minimales ; sinon, l'application peut connaître une perte de performances.
- La qualité de service (QoS) doit être appliquée à la liaison principale et à la liaison redondante pour la transmission de la plateforme, et les performances de la liaison doivent être surveillées.
- Avant toute utilisation, vérifiez les niveaux de volume audio et du microphone, ainsi que les autorisations audio et d'accès au microphone dans le navigateur Web.
- Avant toute utilisation, vérifiez le fonctionnement du clavier et de la souris ; s'ils sont lents ou désynchronisés, activez le bouton « Mouse resync » (Resynchronisation de la souris). Vérifiez que l'ordinateur e-KVM est connecté et mis en marche.
- Assurez-vous que la disposition du clavier de l'établissement distant est identique à celle du site d'imagerie.
- S'il est nécessaire de changer l'endroit où la plateforme est utilisée, le client doit appeler l'assistance technique pour qu'elle effectue une nouvelle installation. Ne procédez pas à une réinstallation sans avoir contacté l'assistance technique.
- Avant de commencer le processus d'accès à distance de l'appareil IRM, TDM ou TEP/TDM, il est important que les équipes des opérateurs vérifient tous les éléments requis pour assurer le bon fonctionnement de la plateforme, afin de ne pas compromettre l'examen. Ces éléments sont répertoriés dans le document « Liste de contrôle pour le début de l'entretien ».
- La configuration du pare-feu de l'établissement d'imagerie doit être vérifiée tous les mois par l'équipe informatique, qui doit s'assurer que la version du pare-feu ne présente aucun problème pouvant compromettre l'utilisation de nCommand Lite.
- Toute anomalie constatée lors de l'utilisation de l'application doit être immédiatement signalée à l'équipe d'assistance avant de démarrer l'accès ou, si celui-ci a déjà été initié, en l'interrompant.
- L'application ne doit être utilisée que par des opérateurs agréés formés à l'utilisation de nCommand Lite.
- L'accès à distance via la plateforme ne remplace pas et n'est pas en concurrence avec toute autre procédure d'utilisation pour une intervention d'IRM, de TDM ou de TEP/TDM établie par le fabricant de l'appareil médical et les protocoles et procédures de l'établissement de soins.
- Évitez de plier ou d'étirer les câbles matériels.
- En cas de problème de communication vocale ou par chat, utilisez la fonction d'appel téléphonique pour établir la communication entre l'opérateur local de l'établissement d'imagerie et l'opérateur à distance du centre de commande. Suivez les instructions décrites dans la section « Directives en cas de défaillance » et, si nécessaire, contactez l'assistance technique pour qu'elle effectue la réparation.
- S'il est nécessaire de remplacer un ordinateur ou tout autre équipement qui influence directement l'installation de nCommand Lite, activez l'assistance technique, ce qui garantit la préservation du fonctionnement du système.
- Une seule personne à la fois peut accéder à distance à l'appareil IRM, TDM ou TEP/TDM.
- Ne manipulez aucune des connexions vidéo lorsque l'ordinateur de l'équipement et le système nCommand Lite sont sous tension.

- Lorsque vous accédez à un appareil supplémentaire, un nouvel onglet s'ouvre. Faites glisser cet onglet vers un deuxième moniteur, car le système est conçu pour être utilisé avec un écran distinct pour chaque appareil.
- Tout incident grave lié à l'utilisation de ce appareil doit être signalé à la fois au fabricant et à l'autorité sanitaire / autorité compétente du pays dans lequel le dispositif est installé (*voir plus de détails dans le chapitre Canaux de service*).

Chapitre 3 Utilisation de la plateforme selon l'emplacement

Section 3.1 - Accès et utilisation de nCommand Lite

**AVERTISSEMENT !**

En cas de problème, contactez l'assistance technique pour obtenir de l'aide.

**AVERTISSEMENT !**

Vérifiez la disposition du clavier et assurez-vous qu'elle est identique aux deux emplacements (établissement médical et établissement distant). Des configurations de clavier différentes peuvent compromettre l'expérience de l'utilisateur.

Ce chapitre fournit tout ce que vous devez savoir pour accéder à la plateforme nCommand Lite et commencer à l'utiliser. Vous trouverez des instructions simples, étape par étape, pour vous connecter, naviguer dans l'interface et comprendre les principales fonctionnalités. Que vous travailliez sur site ou à distance, ce guide vous aidera à démarrer rapidement et en toute confiance.

Modification de la langue : le système est préreglé sur l'anglais par défaut, mais vous pouvez facilement modifier la langue en fonction de vos préférences. Sur l'écran de connexion, cliquez sur le coin supérieur droit où « English (en-US) » (Anglais [en-US]) s'affiche. Cette action ouvrira une liste déroulante de langues disponibles à partir de laquelle vous pourrez sélectionner une langue.

Une fois connecté, vous pouvez également modifier la langue en cliquant sur la langue actuellement sélectionnée à droite de la barre supérieure. Cette action ouvrira une liste déroulante de langues disponibles à partir de laquelle vous ferez votre choix.

Veuillez noter que si vous modifiez la langue lorsque vous êtes connecté à un appareil, la connexion en cours sera automatiquement interrompue et vous devrez vous reconnecter.

Lorsque vous accédez à la plateforme, vous pouvez choisir votre langue préférée sur l'écran de connexion. Cependant, certains messages affichés lors du processus de connexion peuvent apparaître dans la langue définie dans votre navigateur Web, quelle que soit la langue sélectionnée sur la plateforme. Pour une expérience cohérente, nous vous recommandons d'aligner les paramètres de langue de votre navigateur sur la langue de votre plateforme préférée.

Section 3.2 - Accès à la plateforme pour la première fois

Le processus de connexion sur la plateforme peut se faire de deux manières : via nCommand Lite ou via un fournisseur d'identité externe (External IdP). L'utilisateur peut se connecter à l'aide de l'une des méthodes préconfigurées. Si la méthode configurée est le fournisseur d'identité

externe (External IdP), la méthode nCommand Lite ne fonctionnera pas, et vice versa. Pour vous connecter via un fournisseur d'identité externe, rendez-vous directement sur **sous-élément 3.2.2.**

3.2.1. Connectez-vous via nCommand Lite

Remarque : Cette section ne s'applique pas aux utilisateurs qui se connectent via un fournisseur d'identité externe (IdP externe).

Mettez l'ordinateur en marche et double-cliquez sur l'icône de raccourci nCommand Lite qui se trouve généralement sur le bureau. Vous pouvez également accéder à l'URL directement dans le navigateur.

Votre premier accès est une étape cruciale pour commencer à utiliser la plateforme de manière sûre et efficace. Voici ce que vous devez savoir :

1 - E-mail de bienvenue : Vous recevrez un e-mail avec vos identifiants de connexion, y compris votre adresse e-mail personnelle associée, un mot de passe temporaire et un lien direct vers la plateforme client. Cette adresse e-mail est essentielle pour commencer votre expérience sur nCommand Lite

2 - Création du mot de passe : Après avoir accédé au lien, vous devrez saisir votre adresse e-mail associée et le mot de passe reçus dans l'e-mail de bienvenue. En cliquant sur « Sign in » (Connexion), vous serez dirigé vers une page pour créer un nouveau mot de passe. Vous devez saisir l'ancien mot de passe, le nouveau mot de passe et la confirmation du nouveau mot de passe. Il doit être fort et sécurisé, comportant au moins 3 éléments parmi ce qui suit : une lettre minuscule, une lettre majuscule, un chiffre et un symbole, et avoir une longueur d'au moins 8 caractères. En cliquant sur « Continue » (Continuer), vous serez redirigé vers une page pour confirmer à nouveau votre adresse e-mail. En cliquant sur « Continue » (Continuer), vous serez redirigé vers l'écran d'accueil, qui est personnalisé en fonction de votre profil d'utilisateur spécifique.

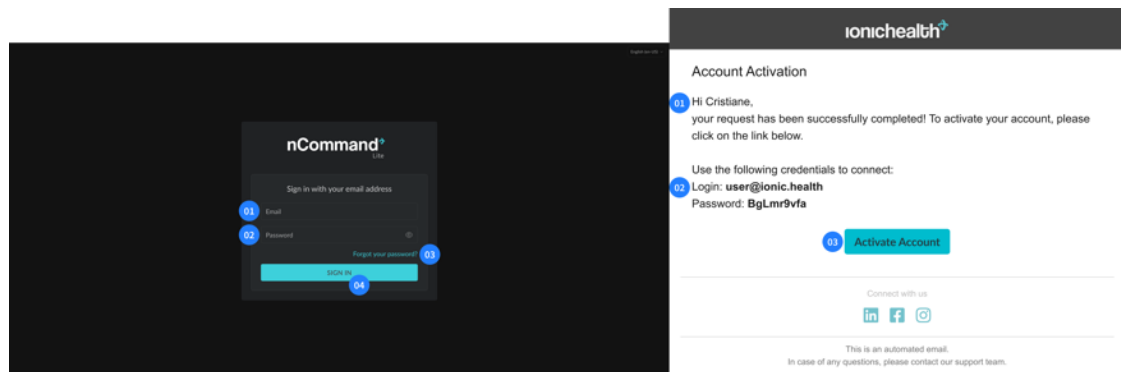


Figure 02 : Premier Accès

Gauche - Page de connexion : 01 – Email Address (Adresse e-mail) ; 02 – Password (Mot de passe) ; 03 – “Forgot your password?” (Mot de passe oublié ?) ; 04 – Bouton Sign In (Se Connecter)

Droite - E-mail de bienvenue : 01 – Texte de l'e-mail d'activation du compte ; 02 – Identifiants de connexion ; 03 – Bouton Activate Account (Activer le compte)

Cette procédure initiale est conçue pour garantir une sécurité maximale de votre compte dès le début. À partir de votre deuxième accès, le processus sera simplifié, mais tout aussi sécurisé, avec un code d'authentification à deux facteurs envoyé à votre adresse e-mail associée à chaque connexion afin de garantir la sécurité continue de votre compte.

Une fois connecté à nCommand Lite, le système vous dirigera automatiquement vers l'écran d'accueil, qui est personnalisé en fonction de votre profil d'utilisateur spécifique. Que vous soyez un opérateur local ou un opérateur à distance, l'interface est conçue pour répondre aux besoins d'accès pertinents pour votre rôle. Grâce à cette conception intuitive, vous disposez de tous les outils et informations nécessaires pour une expérience utilisateur efficace et efficiente dès votre connexion.

Remarque : Lorsque la méthode de connexion est configurée sur nCommand Lite, la connexion doit toujours être réalisée via cette option. Même si un bouton IdP externe apparaît sur l'écran de connexion, il ne fonctionnera pas pour ces utilisateurs. Chaque compte utilisateur est enregistré sur la plateforme avec une méthode d'authentification spécifique — soit des identifiants nCommand Lite, soit un service IdP externe. Si un utilisateur tente de se connecter en utilisant une méthode différente de celle attribuée à son compte, le système affichera un message d'erreur indiquant que le compte n'est pas autorisé pour ce type d'authentification.

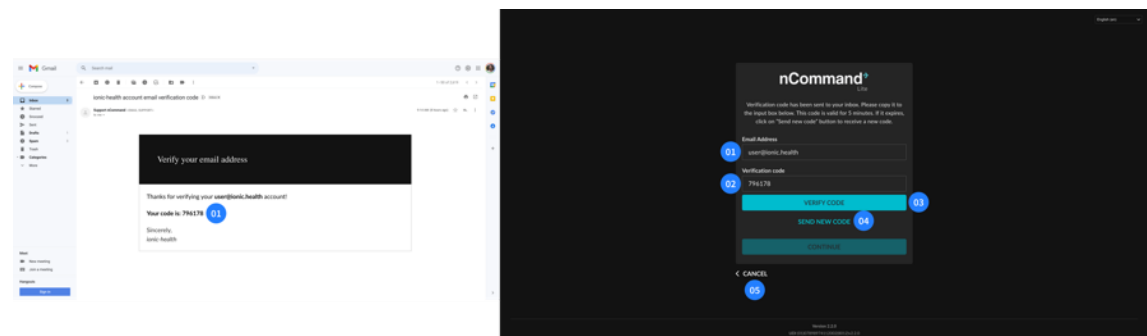


Figure 03 : Authentification à deux facteurs (2-FA)

Gauche – E-mail : 01 – Code d'authentification à deux facteurs

Droite - Page d'authentification à deux facteurs : 01 – E-mail Address (Adresse e-mail) ; 02 – Verification Code (Code de vérification) ;

03 – Bouton Confirmer le code de vérification ; 04 – Envoyer un nouveau code ; 05 – Annuler

3.2.2. Connexion via un fournisseur d'identité externe

Dans certains cas, les utilisateurs peuvent se connecter à la plateforme par le biais d'un fournisseur d'identité externe (IdP), ce qui leur permet d'utiliser le service d'authentification existant de leur organisation, un mécanisme également connu sous le nom d'authentification unique (SSO). Par cette méthode, l'utilisateur pré-inscrit ne recevra pas d'e-mail de bienvenue. Le service informatique local doit vérifier la compatibilité, configurer la méthode et informer l'utilisateur de l'adresse e-mail (External IdP) à utiliser.

Lorsque cette option est disponible, l'utilisateur doit toujours se connecter à l'aide du fournisseur d'identité externe (par exemple, Amazon Cognito, Microsoft Entra ID, Microsoft AD B2C). La méthode de connexion via nCommand Lite ne sera pas disponible pour les utilisateurs d'IdP externes.

Pour vous connecter à l'aide de l'IdP externe, cliquez sur le bouton avec le nom de l'IdP et suivez les instructions fournies par l'authentificateur externe. Si votre établissement dispose de plusieurs fournisseurs d'identité externes intégrés, assurez-vous de confirmer auprès de quel fournisseur vous êtes inscrit. Les autres fournisseurs ne fonctionneront pas. Si vous avez des questions ou rencontrez des difficultés, contactez votre service informatique local.

Dans les scénarios où les utilisateurs partagent la même machine et utilisent l'authentification unique (SSO), il est recommandé que chaque utilisateur sélectionne l'option « Ne pas rester connecté » lors de la connexion au fournisseur d'identité externe (le cas échéant) ou se déconnecte du fournisseur externe après s'être déconnecté de nCommand Lite.

Pour cette option de connexion, l'ensemble du processus de connexion et de déconnexion – y compris les stratégies de création et d'expiration de mot de passe, l'authentification multifacteur (MFA) et les verrouillages de compte – est entièrement géré par l'équipe informatique du client qui a configuré le fournisseur d'identité externe.

Lors de la connexion via un fournisseur d'identité externe, les fonctions « Mot de passe oublié » et « Changer de mot de passe » doivent être exécutées conformément au processus de l'IdP externe.

Remarque : L'option « Mot de passe oublié » apparaîtra toujours sur l'écran de connexion, mais ne sera pas fonctionnelle pour ces utilisateurs. Elle peut les diriger vers les prochaines étapes du processus, mais ne le terminera pas. Si vous avez besoin de récupérer votre mot de passe, suivez les instructions de votre fournisseur d'identité externe.

Important : Même lors de l'utilisation d'un fournisseur d'identité externe, l'utilisateur doit être pré-enregistré dans la plateforme nCommand Lite pour y accéder.

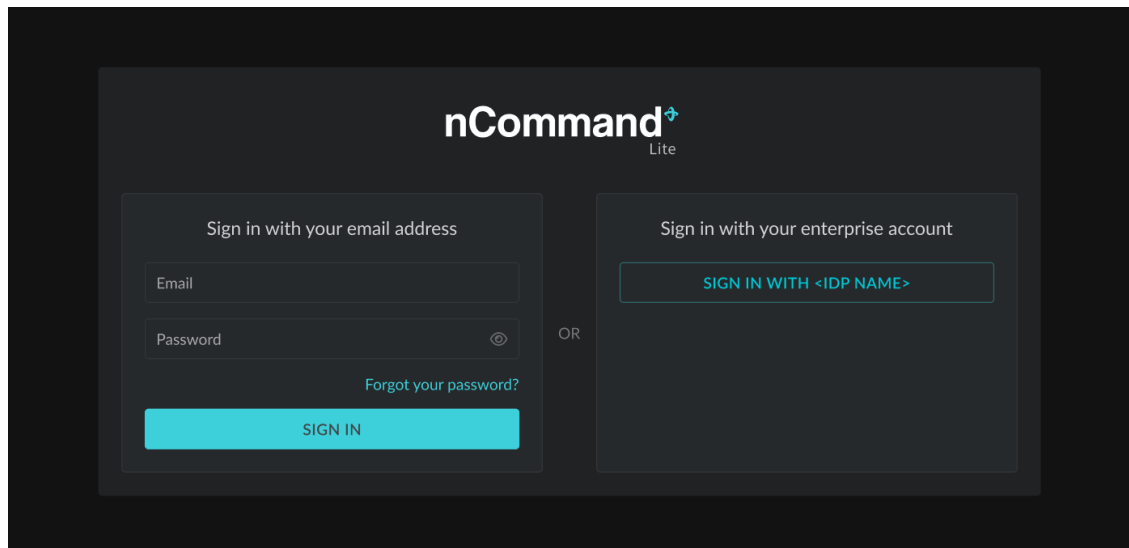


Figure 04 : Écran de connexion via un fournisseur d'identité externe (exemple)

Section 3.3 - Gestion des mots de passe

Après avoir accédé à la plateforme pour la première fois, les utilisateurs peuvent modifier leur mot de passe ou, en cas d'oubli, définir un nouveau mot de passe.

Remarque : Lors de la connexion via un fournisseur d'identité externe, les fonctions **Mot de passe oublié** et **Modifier le mot de passe** doivent être effectuées conformément au processus du fournisseur d'identité externe.

- **Récupérer le mot de passe :** Permet aux utilisateurs de récupérer l'accès à leur compte en cas d'oubli de leur mot de passe. Cliquez simplement sur le lien « Forgot your password? » (Vous avez oublié votre mot de passe?) sur la page de connexion, saisissez l'adresse e-mail associée et soumettez les informations. Le système enverra ensuite un e-mail contenant un code de vérification. Lors de la saisie du code et du clic sur « Verify code » (Vérifier le code), les utilisateurs seront invités à confirmer l'adresse e-mail associée. En cliquant sur « Continue » (Continuer), les utilisateurs sont dirigés vers une page où ils peuvent saisir un nouveau mot de passe et confirmer le nouveau mot de passe. Si le nouveau mot de passe répond aux exigences du système, les utilisateurs peuvent l'enregistrer avec succès et se connecter ultérieurement avec les identifiants mis à jour.

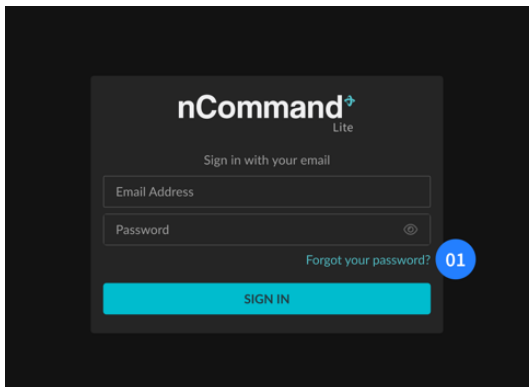


Figure 05 : Lien vers la page de réinitialisation du mot de passe
01 – Forgot your password? (Mot de passe oublié ?)

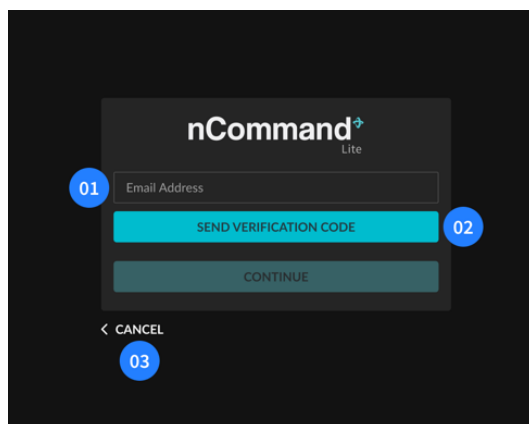


Figure 06 : Page de réinitialisation du mot de passe
01 – E-mail Address (Adresse e-mail) ; 02 – Send Verification Code (Envoyer le code de vérification) ; 03 – Cancel (Annuler)

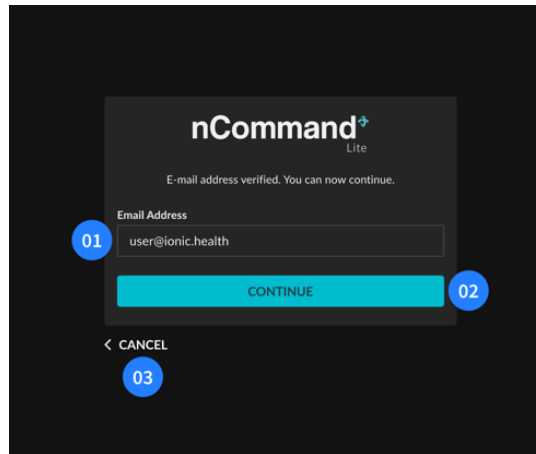


Figure 07 : Confirmation par e-mail

01 – E-mail Address (Adresse e-mail) ; 02 – Bouton Continue (Continuer) ; 03 – Cancel (Annuler)

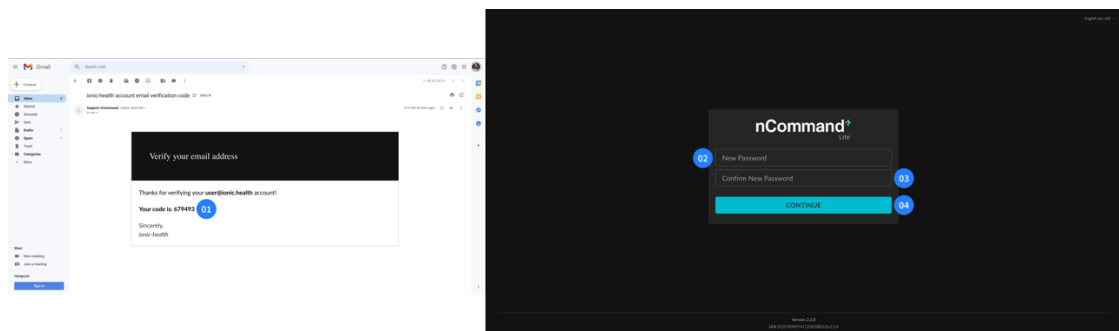


Figure 08 : Email contenant le code pour enregistrer un nouveau mot de passe (gauche) - 01 – 2-Code d'authentification à deux facteurs

Page Modifier le mot de passe (droite) - 02 – Nouveau mot de passe ; 03 – Confirmer le nouveau mot de passe ; 04 – Bouton Continuer

- Changer le mot de passe :** Permet aux utilisateurs de mettre à jour leur mot de passe en respectant des critères spécifiques, notamment au moins 3 éléments parmi ce qui suit : une lettre minuscule, une lettre majuscule, un chiffre et un symbole, et avoir une longueur d'au moins 8 caractères. Le système vérifie si le nouveau mot de passe répond à ces critères et informe l'utilisateur par un message si ce n'est pas le cas. De plus, les utilisateurs doivent confirmer le nouveau mot de passe pour éviter les erreurs de saisie. Pour changer le mot de passe, l'utilisateur, après le processus de connexion, doit cliquer sur l'icône en haut à droite et choisir le menu « Change Password » (Modifier le mot de passe). Il sera déconnecté de la plateforme et dirigé vers une page pour confirmer l'adresse e-mail associée. Le système enverra ensuite un e-mail contenant un code de vérification. Lors de la saisie du code et du clic sur « Verify code » (Vérifier le code), les utilisateurs sont redirigés vers un écran où ils peuvent saisir un nouveau mot de passe.

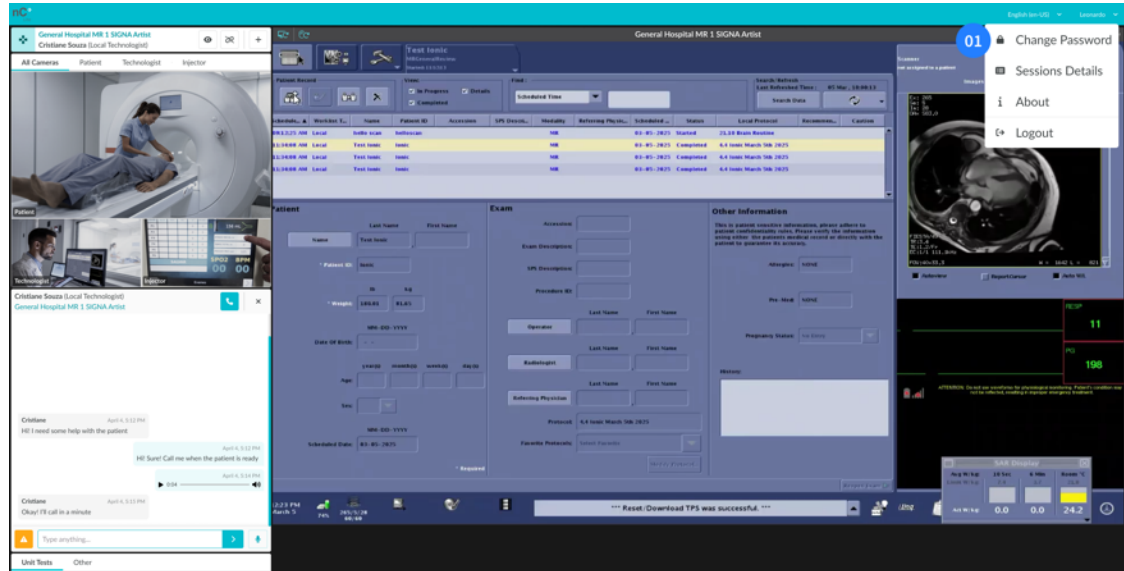


Figure 09 : Élément du menu déroulant « Modifier le mot de passe »
01 – Modifier le mot de passe

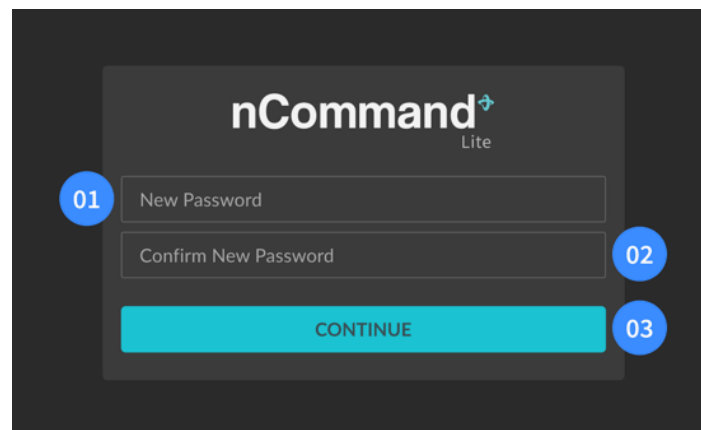


Figure 10 : Page de modification du mot de passe
01 – New Password (Nouveau mot de passe) ; 02 – Confirm New Password (Confirmer le nouveau mot de passe) ; 03 – Bouton Continue (Continuer)

Section 3.4 - Accès avec profil d'opérateur local



AVERTISSEMENT !

Avant d'utiliser la plateforme, contactez l'opérateur à distance par téléphone.



AVERTISSEMENT !

Pour éviter toute surchauffe, ne placez aucun objet devant le refroidisseur à air de l'ordinateur e-KVM et, pour éviter tout dommage, ne placez aucun objet au-dessus du refroidisseur à air.

**AVERTISSEMENT !**

Pendant les sessions à distance, l'opérateur local est responsable de la gestion et de l'application des règles de sécurité locales pour chaque type d'examen et ses exigences spécifiques. Restez toujours présent dans la salle de commande et/ou la salle d'examen afin d'assurer la sécurité du patient et des professionnels impliqués.

**AVERTISSEMENT !**

Les mouvements de la table pendant la session ne doivent être effectués par l'opérateur local que sur demande du système. Avant de quitter la salle d'opération, l'opérateur local doit toujours révoquer l'accès de l'opérateur à distance.

**AVERTISSEMENT !**

Seul l'opérateur local est autorisé à déplacer la table pour positionner le patient à l'intérieur de l'appareil et faire sortir le patient en toute sécurité. Avant de quitter la salle d'opération, l'opérateur local doit toujours révoquer l'accès de l'utilisateur à distance.

Après vous être connecté à la plateforme, sélectionnez l'appareil souhaité dans la boîte de dialogue Device Selection (Sélection de l'appareil). Vous serez responsable de cet appareil, afin de pouvoir examiner la demande de l'opérateur à distance d'accéder à l'appareil. Lorsqu'un opérateur à distance souhaite accéder à l'appareil, une fenêtre contextuelle s'affiche, vous permettant d'examiner toutes les informations présentées avant d'accorder ou de refuser l'accès. Restez attentif à toute demande entrante d'un opérateur à distance. Il est primordial de vérifier attentivement chaque détail. Dans les cas où les informations fournies ne sont pas reconnues, n'accordez pas l'accès.

L'opérateur à distance peut accéder à l'appareil en utilisant l'un des deux modes d'accès : **Commande** ou **Afficher** :

- **Mode Control (Mode Commande)** - permet à l'opérateur à distance de commander la souris et le clavier, ainsi que de visualiser le streaming de l'appareil. Cependant, l'opérateur local ne perd pas la commande de la souris et du clavier locaux et peut reprendre la commande à tout moment.
- **Mode View (Mode Afficher)** - permet à l'opérateur à distance de seulement visualiser l'écran de l'appareil et d'utiliser le chat pour la communication

Après avoir sélectionné l'appareil, l'utilisateur a accès à la fonction de chat, permettant de communiquer par texte, messages audio, appels vocaux et vidéo avec les autres utilisateurs.

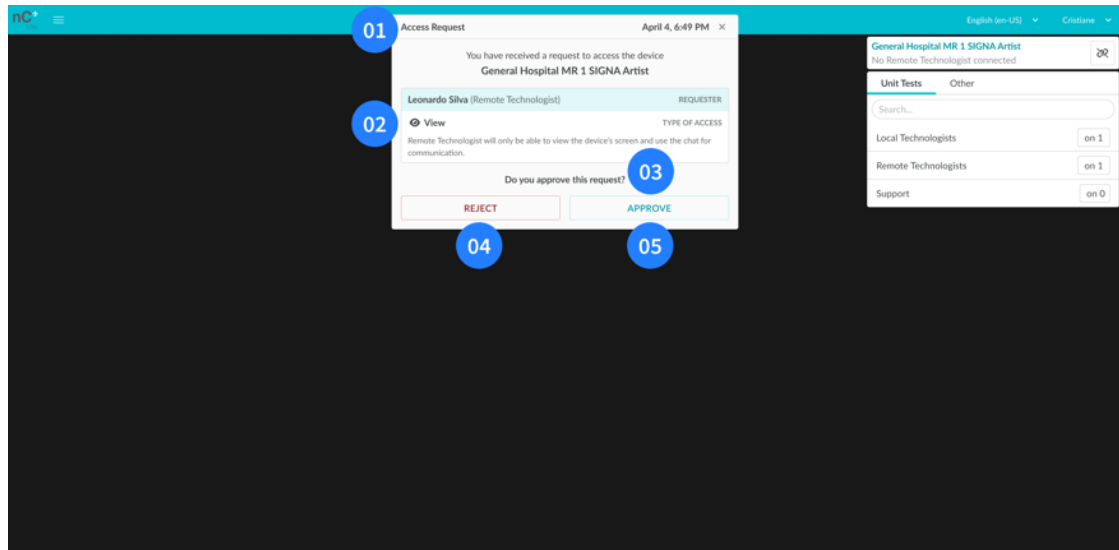


Figure 11 : Écran principal de l'Opérateur local avec notification de demande d'accès
01 – Titre (Demande d'accès) ; 02 – Nom du demandeur, rôle et description du type d'accès ;
03 – Invite : « Do you approve this request? » (Approuvez-vous cette demande ?) ; 04 – Bouton Reject (Rejeter) ; 05 – Bouton Approve (Approuver)

Après approbation, l'opérateur local peut révoquer l'accès de l'opérateur à distance à tout moment en cliquant simplement sur le bouton REVOKE (RÉVOQUER).

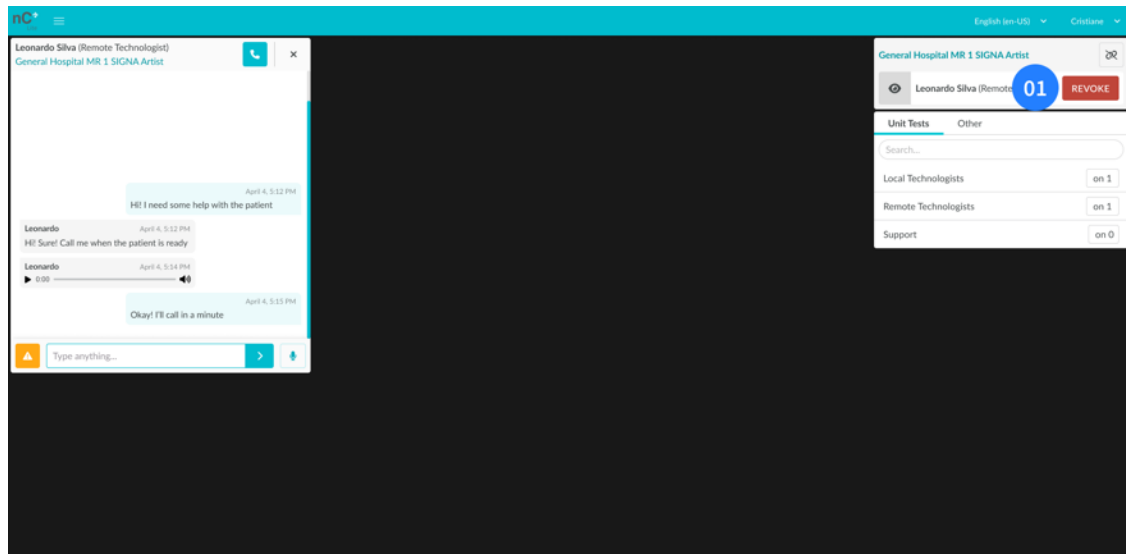


Figure 12 : Écran principal de l'Opérateur local lorsqu'il est connecté à un appareil
01 – Bouton Révoquer

Pendant la session à distance, l'opérateur à distance peut demander un changement de mode d'accès. Une fenêtre contextuelle de demande s'affichera à l'écran. Vous pouvez approuver ou rejeter la demande. Tenez compte des prérogatives que chaque mode d'accès donne à l'opérateur à distance.

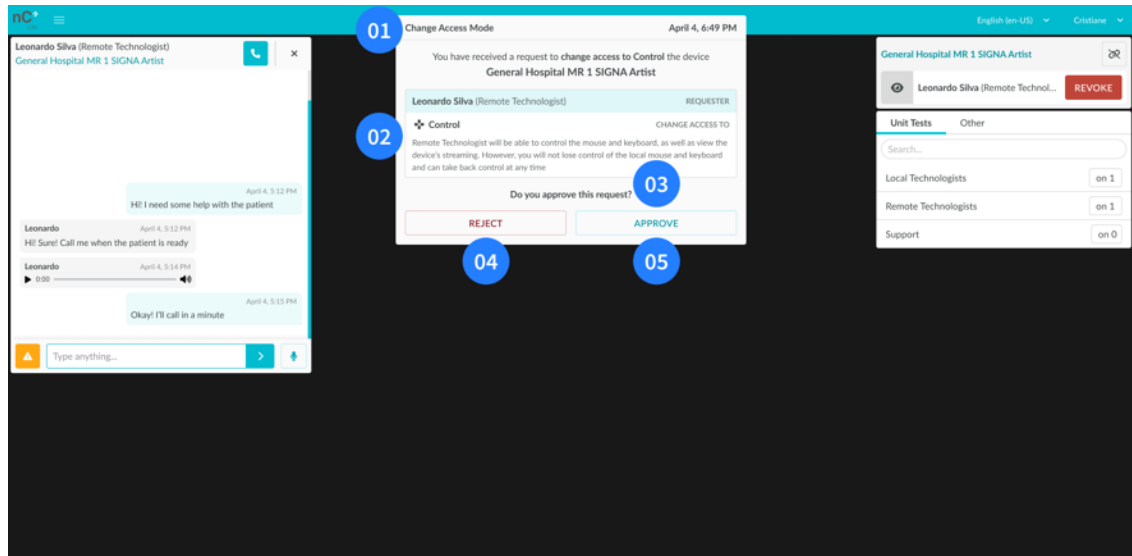


Figure 13 : Écran principal de l'Opérateur local avec demande de modification du mode d'accès

01 – Titre (Modifier le mode d'accès) ; **02** – Nom du demandeur, rôle et description du type d'accès ; **03** – Invite : "Do you approve this request?" (« Approuvez-vous cette demande ? ») ; **04** – Bouton Reject (Rejeter) ; **05** – Bouton Approve (Approuver)



AVERTISSEMENT !

En cas de perte de connexion au niveau de l'ordinateur local, l'opérateur à distance a toujours accès à l'appareil. Contactez **immédiatement** l'opérateur à distance et demandez-lui de se **déconnecter** OU de se connecter à un autre ordinateur et de **révoquer l'accès** de l'opérateur à distance OU d'**appuyer sur le bouton d'alimentation** pour éteindre l'ordinateur e-KVM.



AVERTISSEMENT !

En cas de maintenance du scanner :

Avant que l'ingénieur de terrain ne commence une procédure (que ce soit sur l'appareil ou dans la salle de commande), informez l'opérateur à distance et révoquez l'accès en cliquant sur le bouton « REVOKE ACCESS » (RÉVOQUER L'ACCÈS). Ensuite, déconnectez-vous de la plateforme nCommand Lite.

Si aucun opérateur à distance n'est connecté, déconnectez-vous de la plateforme nCommand Lite avant de commencer la maintenance.

Section 3.5 - Accès avec profil d'opérateur à distance



AVERTISSEMENT !

Mot de passe utilisateur et mot de passe root de l'ordinateur de l'appareil : les deux doivent être détenus par l'hôte sur site qui recevra l'équipe d'installation.



AVERTISSEMENT !

Les mouvements de la table pendant la session ne doivent être effectués par l'opérateur local que sur demande du système. Avant de quitter la salle d'opération, l'opérateur local doit toujours révoquer l'accès de l'opérateur à distance.

- | | | |
|---|------------------------|---|
|  | AVERTISSEMENT ! | Seul l'opérateur local est autorisé à déplacer la table pour positionner le patient à l'intérieur de l'appareil et faire sortir le patient en toute sécurité. Avant de quitter la salle d'opération, l'opérateur local doit toujours révoquer l'accès de l'utilisateur à distance. |
|  | AVERTISSEMENT ! | Surveillez toujours la pièce grâce à la caméra vidéo et assurez-vous de communiquer avec l'opérateur local avant d'effectuer toute activité. |
|  | AVERTISSEMENT ! | En cas de perte de connexion sur l'ordinateur local, contactez immédiatement l'opérateur local et déconnectez-vous. |
|  | AVERTISSEMENT ! | En cas de maintenance du scanner :
Après avoir été informé du début de la maintenance de l'appareil, assurez-vous que l'accès a été révoqué par l'opérateur local et déconnectez-vous de la plateforme nCommand Lite.
Si l'accès n'a pas été révoqué, déconnectez-vous de la plateforme nCommand Lite et contactez immédiatement l'opérateur local pour l'en informer. |
|  | AVERTISSEMENT ! | Pour contrôler la souris et le clavier à distance, le mode d'accès sélectionné doit être Control (Commande) ; en mode view (Afficher), l'opérateur à distance est uniquement autorisé à visualiser les flux vidéo et les caméras locales. |
|  | AVERTISSEMENT ! | Si la réponse à votre demande prend plus de temps que prévu, contactez l'opérateur local par chat ou téléphone. |

Le lieu de travail de l'opérateur à distance comprend un équipement tel qu'un ordinateur, des moniteurs (généralement trois), une souris, un clavier et un casque.

Dans le flux clinique, les techniciens locaux sont en contact direct avec le patient. Ils sont responsables de l'interaction avec les patients, du positionnement et de la sécurité ainsi que du respect des protocoles pendant les procédures d'IRM, de TDM ou de TEP/TDM, conformément aux normes institutionnelles et réglementaires.

3.5.1. Mode d'accès

Après vous être connecté à la plateforme, sélectionnez l'appareil auquel vous souhaitez vous connecter dans la boîte de dialogue Device Selection (Sélection de l'appareil). Une fenêtre contextuelle s'ouvrira pour choisir le mode d'accès entre **Control** (Commande) et **View** (Afficher) :

- **Mode Control (Mode Commande)** – Dans ce mode, le contrôle de la souris et du clavier est activé en plus de l'affichage à l'écran. Les professionnels locaux conservent un accès complet à la souris et au clavier locaux et peuvent reprendre le contrôle à tout moment.
- **Mode View (Mode Afficher)** – Il est seulement possible de visualiser l'écran de l'appareil et d'utiliser le chat pour la communication.

En sélectionnant le mode d'accès, une boîte « Waiting for approval » (En attente d'approbation) s'affichera, indiquant que l'approbation de l'opérateur local connecté est requise pour continuer.

Cet opérateur local est pleinement autorisé à approuver ou à rejeter l'accès et à révoquer l'accès à tout moment si cela est jugé nécessaire. Cette mesure est essentielle pour assurer un contrôle strict et maintenir la sécurité lors de l'utilisation de l'appareil.

Après avoir sélectionné l'appareil, l'utilisateur a accès à la fonction de chat, permettant la communication par texte, messages audio, appel vocal et vidéo avec les autres utilisateurs. L'utilisateur n'a pas besoin d'être approuvé pour accéder au chat.

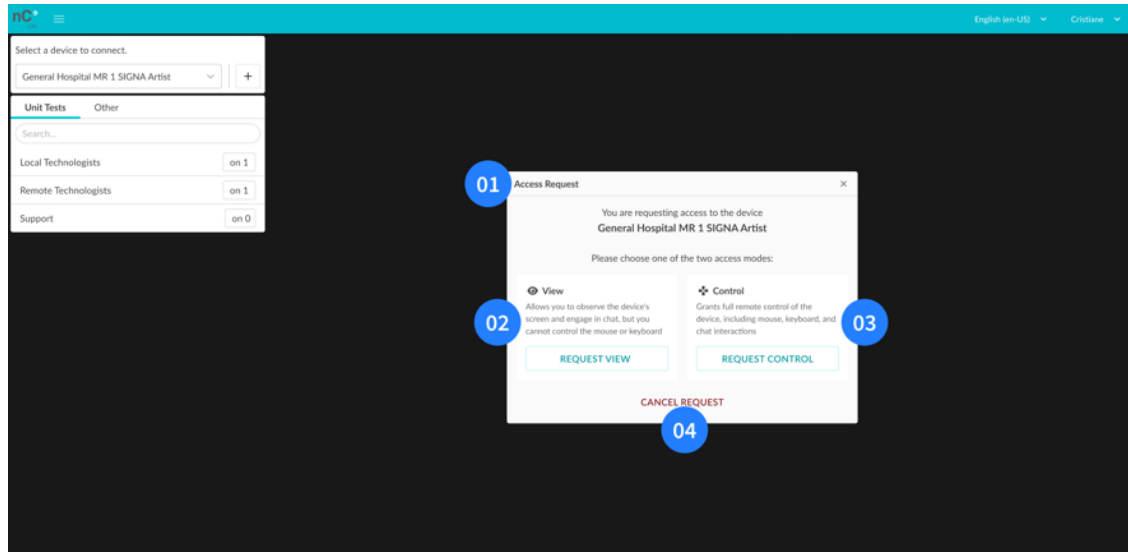


Figure 14 : Boîte de dialogue de demande d'accès pour Opérateur à distance

01 – Titre (Demande d'accès) ; **02** – Description du mode Visualisation et bouton Request View (Demander la visualisation) ; **03** – Description du mode Commande et bouton Request Control (Demander la commande) ; **04** – Cancel Request (Annuler la demande)

Une fois l'accès à l'appareil autorisé par l'opérateur local, l'interface de l'opérateur à distance sera mise à jour pour afficher le flux en direct de l'appareil et de ses caméras associées. Si le mode d'accès choisi est Control (Commande), la fonctionnalité de fonctionnement à distance de l'appareil sera activée.

Ce processus garantit une interaction efficace et sécurisée, permettant l'utilisation à distance en toute sécurité de l'appareil sans compromettre son intégrité ni la sécurité des patients.

Pour demander un changement du mode d'accès pendant une session à distance, cliquez sur l'icône correspondante. L'opérateur local peut accepter ou rejeter la demande :

- **Accepter** – le streaming se rechargera, mais le contenu du chat ne sera pas perdu. Si vous êtes sur un appel Voix & Vidéo, il se terminera et devra être redémarré par l'un des utilisateurs.
- **Refuser** - une fenêtre contextuelle apparaîtra pour vous informer du rejet du technologue local et l'accès actuel restera actif

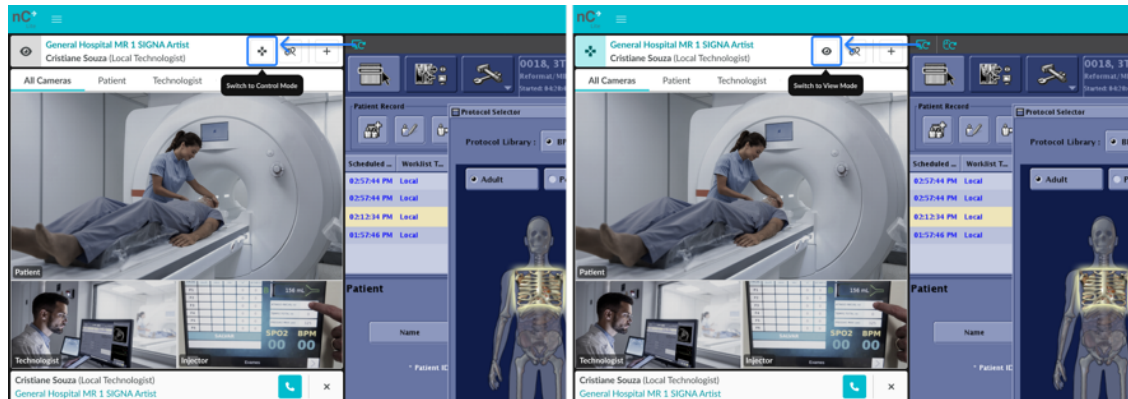


Figure 15 : Modifier le mode d'accès

Gauche - Icône et infobulle Passer en mode Commande / **Droite** - Icône et infobulle Passer en mode Afficher

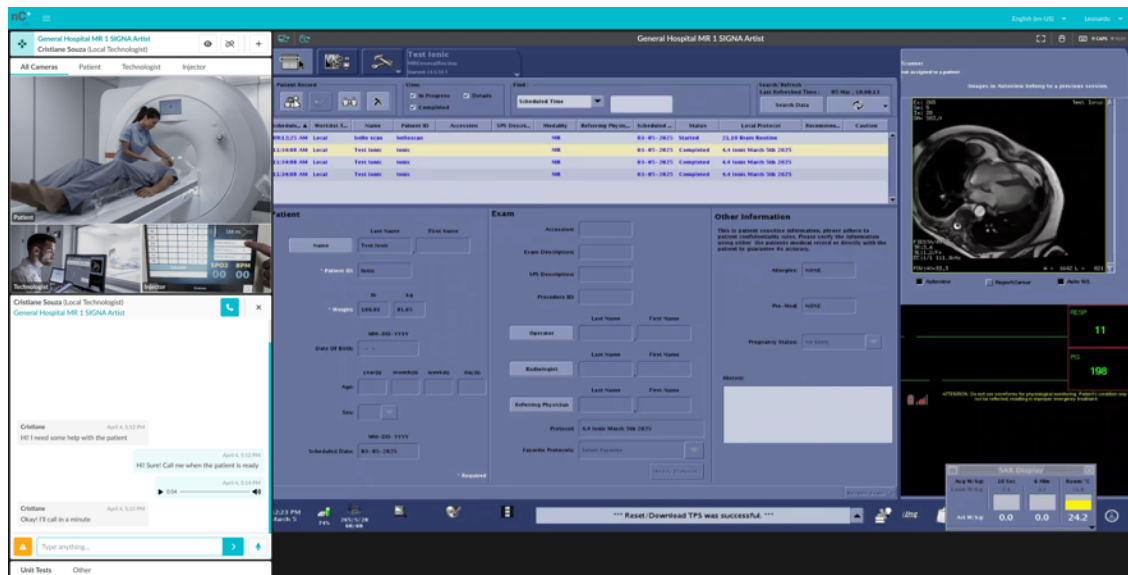


Figure 16 : Écran principal de l'Opérateur à distance lorsqu'il est connecté à un appareil

Lorsque l'opérateur à distance demande l'accès et qu'aucun opérateur local n'est connecté à l'appareil, la plateforme affiche un avertissement contextuel. Dès que l'opérateur local se connecte, la plateforme informe l'opérateur à distance qu'il peut demander à nouveau l'accès.

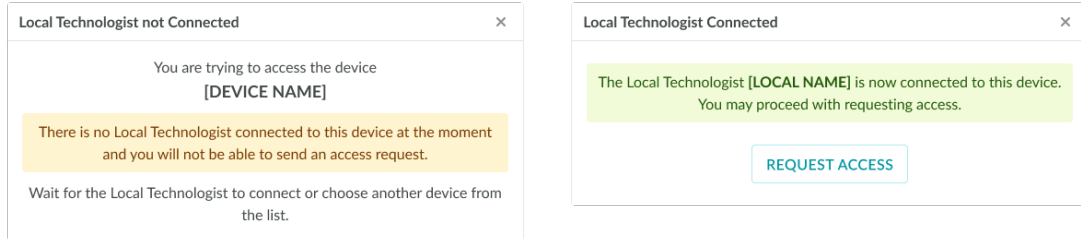


Figure 17 : Avertissements de l'Opérateur à distance concernant l'état de connexion de l'Opérateur local
Gauche - Notification indiquant qu'une tentative d'accès à l'appareil a été effectuée, mais qu'aucun Opérateur local n'est actuellement connecté.

Droite : Notification confirmant que l'Opérateur local s'est connecté à l'appareil après une absence de connexion antérieure.

3.5.2. Barre de streaming

La barre de streaming affiche des informations clés et des contrôles liés à la session de streaming de l'appareil. Il comprend les boutons « Reload Streaming » (Recharger le streaming) et « Mouse Resync » (Resynchroniser la souris), le nom de l'appareil, la résolution de l'écran et l'état actuel de la souris et du clavier de l'ordinateur distant.

1 - Reload Streaming (Recharger le streaming)

Cette fonction permet aux opérateurs à distance de retrouver l'accès aux appareils en cas de défaillance de la connexion ou de lenteur des performances. Si vous rencontrez un type de déconnexion ou de décalage d'écran sur l'ordinateur de l'appareil, vous pouvez cliquer sur l'icône « Reload Streaming » (Recharger le streaming) située dans la barre de streaming. Cela demandera à la plateforme de se reconnecter à l'ordinateur de l'appareil et de recharger également les caméras du système.

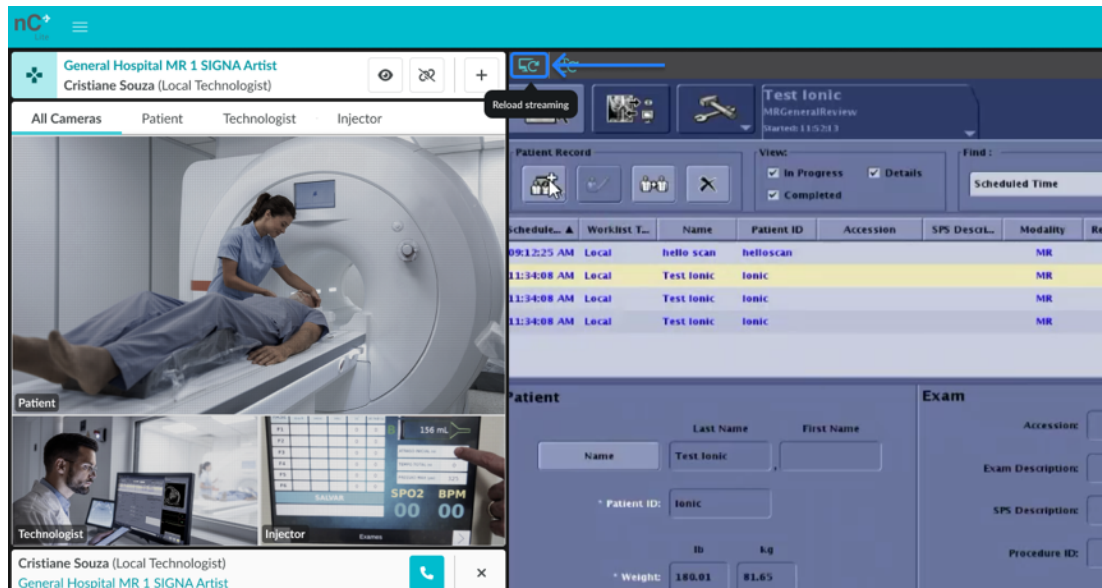


Figure 18 : Bouton Reload Streaming (Recharger le streaming)

2 - Mouse Resync (Resynchroniser la souris)

En cas de ralentissement ou de mauvais alignement de la souris, veuillez cliquer sur le bouton « Mouse Resync » (Resynchronisation de la souris) situé sur la barre au-dessus de la fenêtre de streaming pour resynchroniser la souris de l'appareil avec l'ordinateur e-KVM.

Une autre solution consiste à déplacer le pointeur de la souris hors de la zone de diffusion, puis à le ramener à l'intérieur ; le système resynchronisera automatiquement la souris sans aucune autre action nécessaire. Vous pouvez également cliquer et relâcher le bouton de la molette de la souris (lorsqu'il est disponible) pour déclencher la resynchronisation automatique. Toutefois, cette méthode peut ne pas fonctionner sur les appareils dotés de deux écrans ou plus si les pointeurs de souris locaux et distants se trouvent sur des écrans différents.

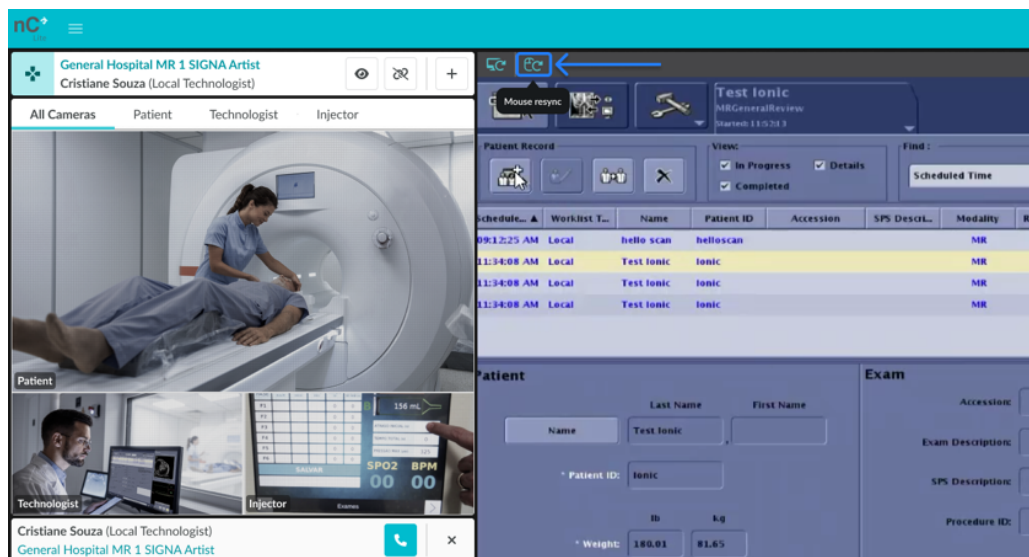


Figure 19 : Bouton Mouse Resync (Resynchronisation de la souris)

3 - Affichage du streaming

Cette fonctionnalité fournit au technicien distant des informations sur la résolution de diffusion en continu d'origine (à partir de l'appareil) et la résolution actuelle en pixels affichée sur le poste de travail distant.

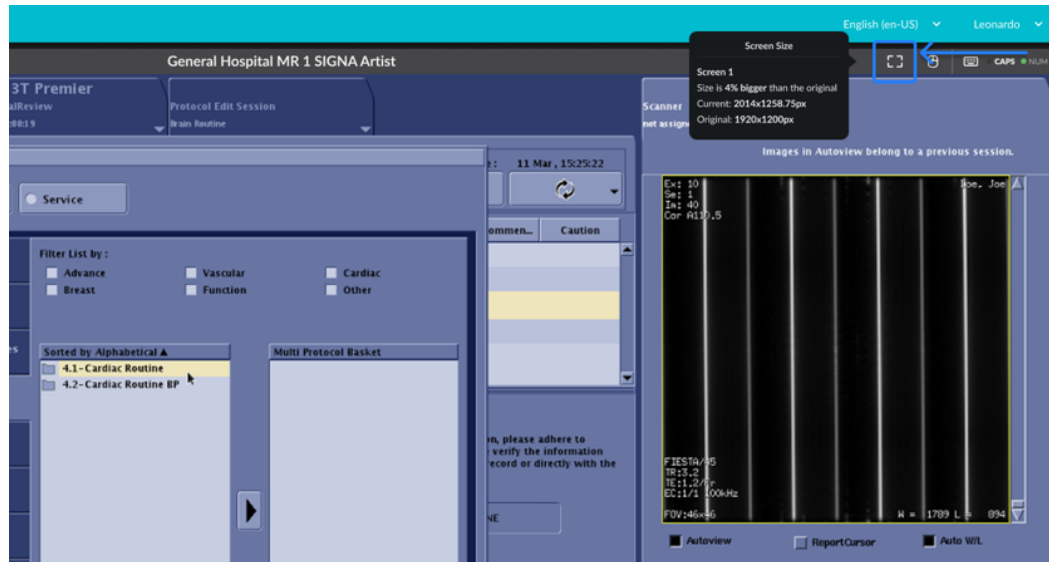


Figure 20 : Info-bulle d'information sur le streaming

4 - État de la souris et du clavier

Cette fonction informe l'opérateur à distance sur le fonctionnement correct ou non de la souris et du clavier. Avec l'état du clavier, l'utilisateur peut voir si les touches **Caps lock/Verr. Maj.** et **Num lock/Verr. Num.** du clavier de l'ordinateur de l'appareil sont activées ou désactivées. Cependant, cette fonctionnalité dépend de l'ordinateur de l'appareil qui fournit ces informations ; Dans les scénarios où ces informations ne sont pas mises à disposition par le système de l'appareil, l'état des touches **Caps Lock/Verr. Maj.** et **Num Lock/Verr. Num.** n'est pas affiché. Les états de la souris et du clavier ne sont affichés que lorsque l'utilisateur dispose d'un accès de type Control (Commande).

Lors de la connexion à un appareil, une incompatibilité entre les indicateurs **Caps Lock/Verr. Maj.** et **Num Lock/Verr. Num.** sur l'ordinateur distant et l'appareil peut entraîner un comportement de frappe incohérent. Si les indicateurs apparaissent activés sur l'appareil, mais ne sont pas réellement actifs sur l'ordinateur distant, l'utilisateur peut saisir des majuscules sur l'appareil tandis que du texte apparaît en minuscules dans le chat, ou inversement. De même, si la touche **Caps Lock/Verr. Maj.** est activée sur l'ordinateur distant, mais désactivée sur l'appareil, le même problème se produira dans le sens inverse.

Pour éviter ce problème, assurez-vous que les touches **Caps Lock/Verr. Maj.** et **Num Lock/Verr. Num.** sont toutes deux activées ou toutes deux désactivées avant de vous connecter à l'appareil. En cas de conflit, l'utilisateur doit se déconnecter de l'appareil, ajuster l'état de la touche sur l'ordinateur distant, puis se reconnecter.

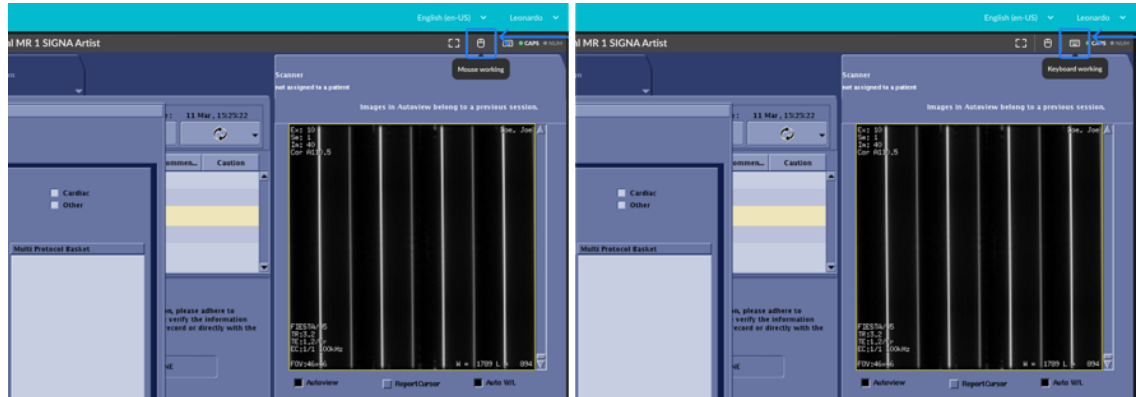


Figure 21 : Barre de streaming
Gauche - Informations sur l'infobulle d'état de la souris
Exact - Informations sur l'infobulle de statut du clavier

3.5.3. Multi-caméras

Cette fonction permet à l'opérateur à distance de visualiser simultanément plusieurs caméras. Si plusieurs caméras sont disponibles, il est possible de n'en afficher qu'une seule et de passer d'une caméra à l'autre en cliquant sur le menu portant le nom désigné pour chaque caméra. En sélectionnant « ALL CAMERAS » (TOUTES LES CAMÉRAS), toutes les caméras disponibles sont affichées dans le cadre, l'une d'entre elles étant mise en surbrillance. Pour changer la caméra en surbrillance, il suffit de passer la souris sur l'une des caméras dans le cadre plus petit et de cliquer sur « SWITCH CAMERA » (CHANGER DE CAMÉRA).

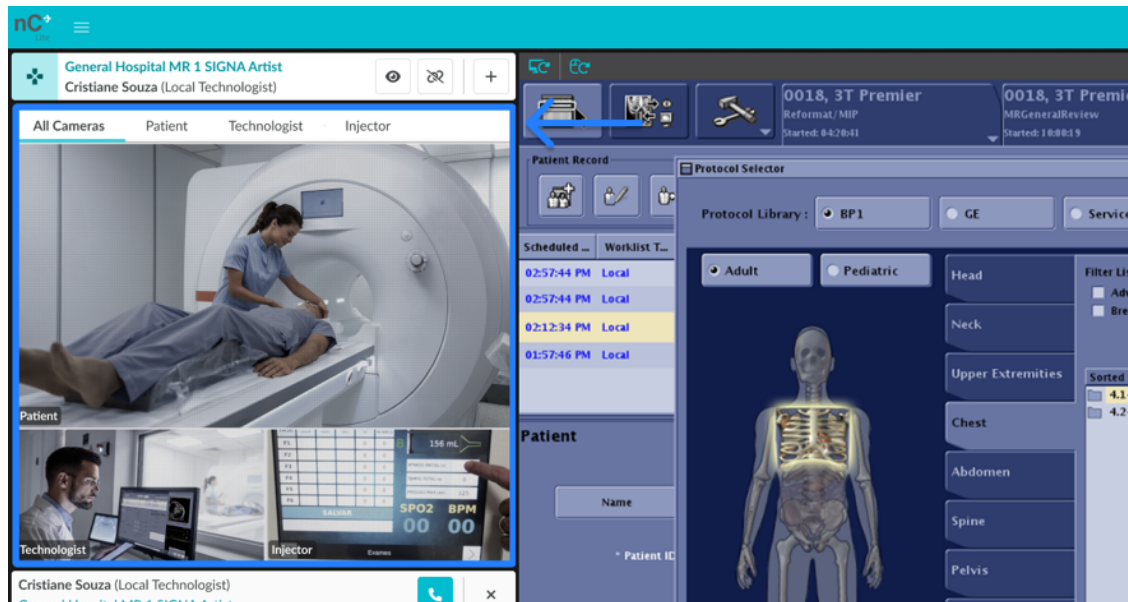


Figure 22 : Affichage multi-caméras

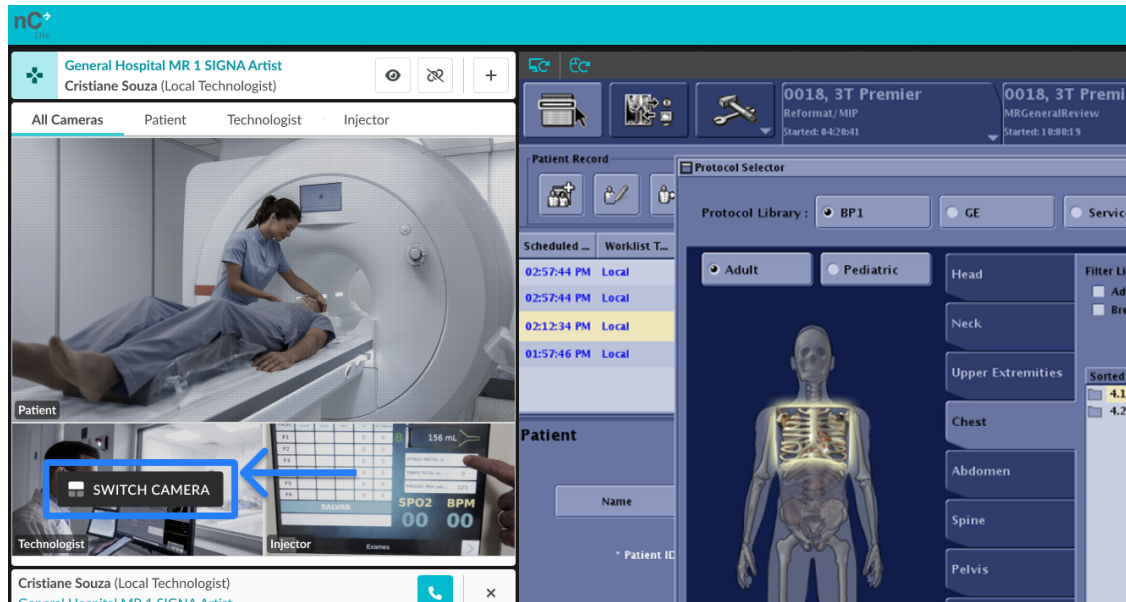


Figure 23 : Bouton de survol "SWITCH CAMERA" (Changer de caméra) (vue multi-caméras)

Au cours d'une session à distance active, si l'opérateur à distance obtient un accès pour le mode **Afficher**, il est possible de désactiver une ou plusieurs caméras en faisant passer la souris sur la caméra choisie et en cliquant sur « TURN OFF CAMERA » (ÉTEINDRE LA CAMÉRA). Pour visualiser à nouveau la caméra, il suffit de répéter le processus et de cliquer sur « TURN ON CAMERA » (ALLUMER LA CAMÉRA).

REMARQUE : L'option permettant de désactiver les caméras n'est disponible qu'en mode View (Afficher) ; en mode Control (Commande), il n'est pas possible de désactiver les caméras.

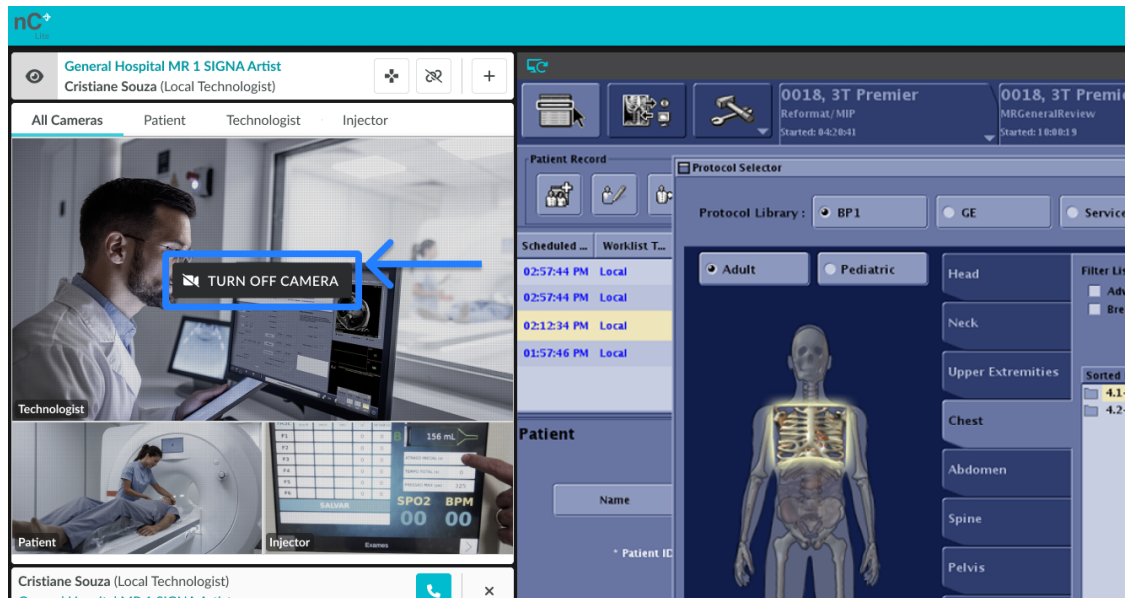


Figure 24 : Bouton de survol "TURN OFF CAMERA" (Désactiver la caméra) en mode affichage multi-caméras

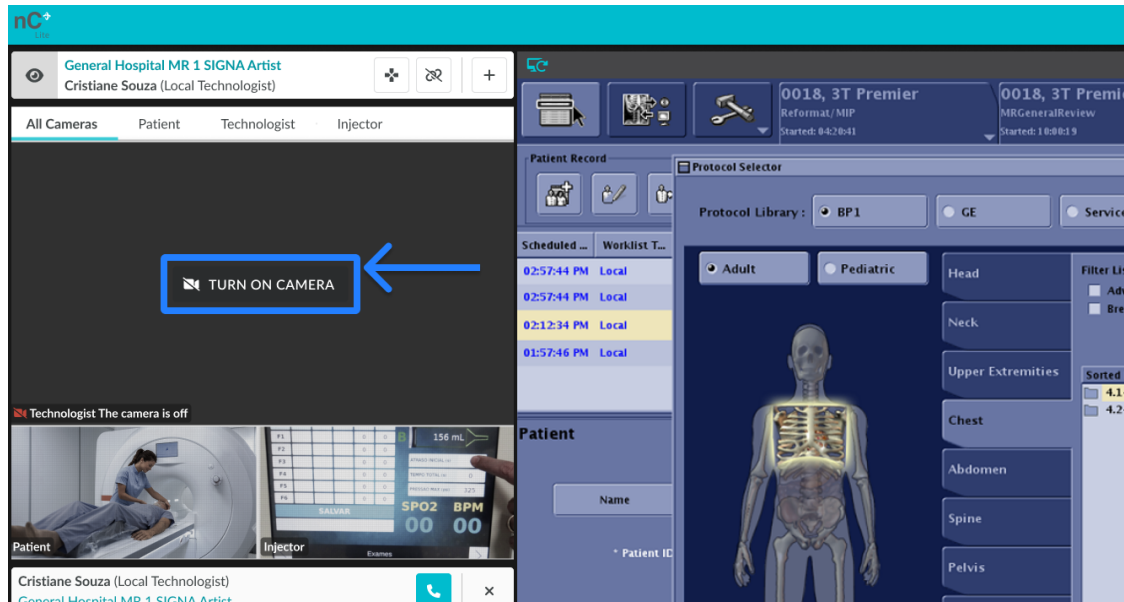


Figure 25 : Bouton de survol "TURN ON CAMERA" (Activer la caméra) en mode affichage multi-caméras

3.5.4. Open Another Device (Ouvrir un autre appareil)

Permet à l'opérateur à distance d'ouvrir un nouvel onglet du navigateur de nCommand Lite, ce qui permet à l'utilisateur de sélectionner un nouvel appareil pour effectuer plusieurs analyses à distance simultanément. Pour ouvrir un nouvel appareil auquel accéder, il suffit de cliquer sur le bouton « Open Another Device », et un avertissement est fourni afin que vous puissiez effectuer cette opération simultanée en toute sécurité. Vous devriez lire l'avertissement avant d'accéder à cette nouvelle fenêtre.

REMARQUE : Pour une meilleure visualisation lors d'un accès simultané, il est recommandé, après avoir cliqué sur "OPEN ANOTHER DEVICE" (OUVRIR UN AUTRE APPAREIL) et sur « OK » dans les avertissements, de faire glisser le nouvel onglet vers un autre écran disponible.



AVERTISSEMENT ! | Avertissement de sécurité – accès simultané à plusieurs scanners

- **Exigence d'une concentration intense :** L'accès simultané nécessite une concentration intense et une communication avec les équipes locales
- **Choisissez différentes mises en page :** Évitez d'accéder à des appareils dont la disposition est identique ou d'examiner la même région anatomique en même temps.
- **Glisser l'onglet vers un autre moniteur :** Lorsque vous accédez à un appareil supplémentaire, un nouvel onglet s'ouvre. Faites glisser cet onglet vers un deuxième moniteur, car le système est conçu pour être utilisé avec un écran distinct pour chaque appareil.
- **Faites attention aux alertes :** Faites particulièrement attention à toutes les alertes du système, car elles sont essentielles à la sécurité des opérations.
- **Contrôle un par un :** Vous pouvez visualiser plusieurs écrans, mais la commande est limitée à un seul appareil à la fois

- **Ouvrir le chat :** Lancez toujours le chat lorsque vous êtes connecté à un appareil pour une communication claire.
- **Un appel à la fois :** Les alertes d'appel vocal apparaissent sur l'écran de l'appareil associé ; un seul appel peut être actif à la fois.
- **Sécurité et alerte :** Accordez la priorité à la sécurité et restez vigilant pendant toutes les opérations.

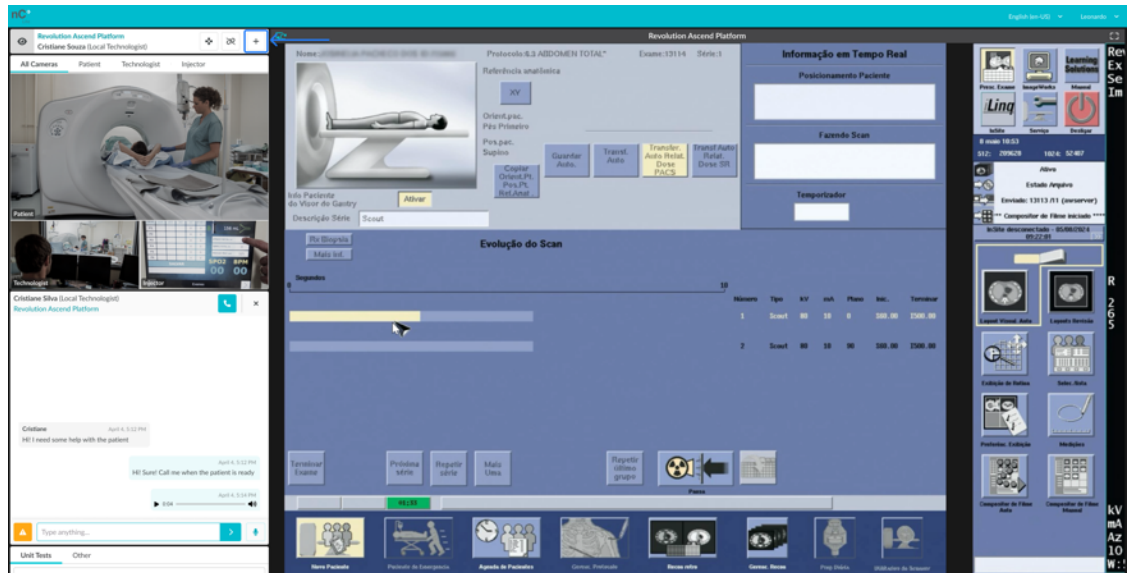


Figure 26 : Bouton Open Another Device (Ouvrir un autre appareil) (+)

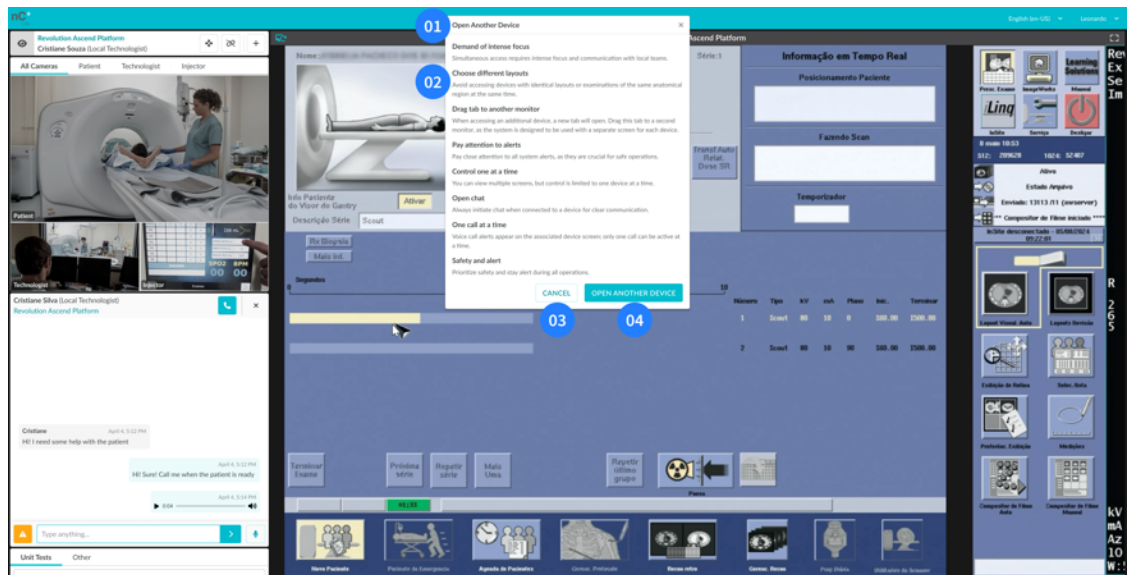


Figure 27 : Avertissements d'accès à plusieurs appareils

01 – Titre (Ouvrir un autre appareil) ; 02 – Avertissements de sécurité opérationnelle ; 03 – Bouton Cancel (Annuler) ; 04 – Bouton Open Another Device

3.5.5. Vérification du système

La fonction de vérification du système permet de vérifier que l'appareil, le réseau et la connectivité Internet actuels répondent aux exigences pour une utilisation correcte de nCommand Lite. Il effectue un test automatique rapide qui vérifie des éléments essentiels tels que la qualité d'Internet, l'accès aux serveurs requis et la stabilité de la connexion. Cet outil peut être utilisé avant le démarrage d'une session, lors de l'installation, ou lorsqu'un problème de connexion est suspecté. Cela permet de garantir que la plateforme fonctionnera comme prévu et d'aider l'équipe technique en cas de dépannage nécessaire.

Remarque : Il est préférable d'utiliser la vérification du système avec l'aide ou à la demande d'un professionnel de l'informatique. L'utilisation de cet outil sans assistance technique peut conduire à une mauvaise interprétation des résultats.

Pour accéder à la vérification du système, les opérateurs locaux et distants doivent ouvrir l'option Session Details (Détails de la session) à partir du menu déroulant disponible sous leur nom d'utilisateur, situé dans le coin supérieur droit de l'écran principal. Cliquez ensuite sur **Open (Ouvrir)** à côté de l'outil **System Check (Vérification du système)**. Une fois la page de l'outil affichée, cliquez sur **Run Test (Exécuter le test)** pour lancer le processus de vérification.

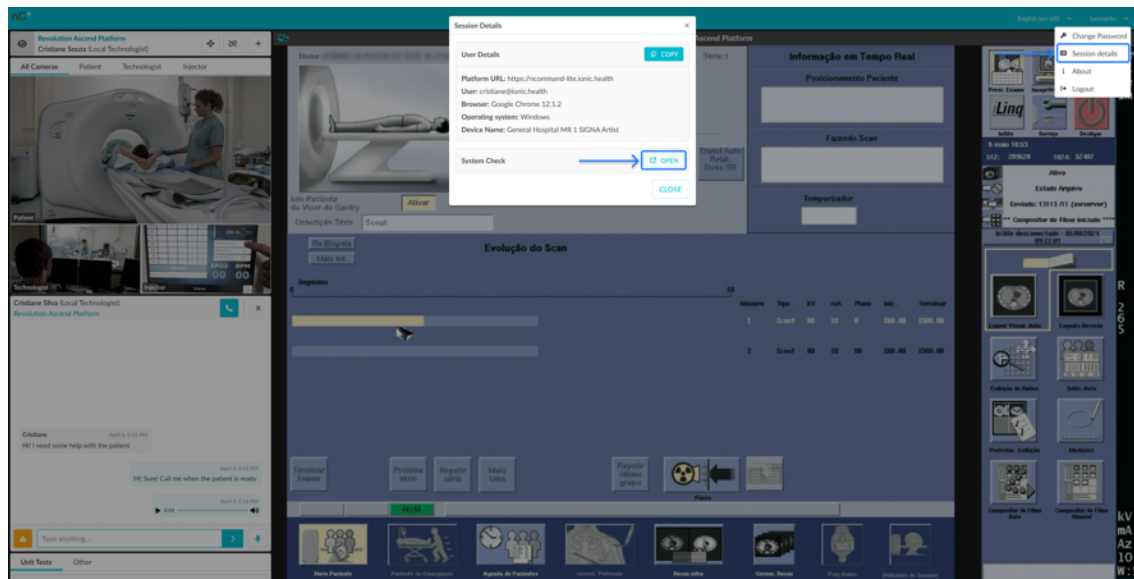


Figure 28 : Accès à la Vérification du système

Lors de l'utilisation de l'Opérateur à distance, il est possible de sélectionner un appareil sur l'écran principal de l'outil afin qu'il soit inclus dans les résultats du test.



AVERTISSEMENT !

Avant de commencer le test, assurez-vous que l'appareil sélectionné n'est pas en cours d'utilisation.

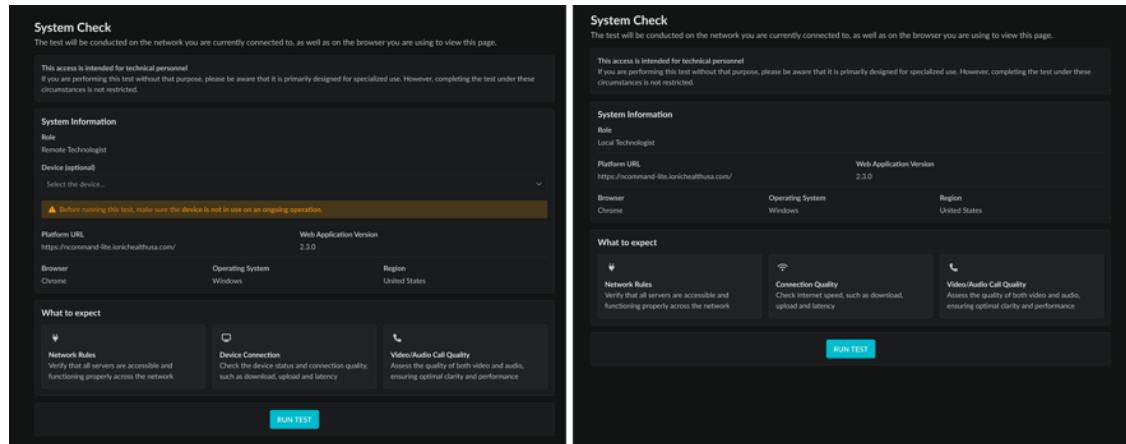


Figure 29 : Écran principal System Check (Vérification du système)
Gauche - Opérateur à distance / Droite - Opérateur local

Une fois le test terminé, un résumé des résultats s'affiche à l'écran. Les professionnels de l'informatique peuvent analyser ces informations pour identifier les problèmes potentiels affectant les performances du système.

Section 3.6 - Chat

La plateforme fournit une fonction de chat et d'appel en temps réel avec des fonctionnalités audio et vidéo, qui est utilisée pour une communication efficace entre les techniciens agréés. Grâce à ces fonctionnalités, les technologues agréés peuvent interagir sur toutes les questions liées au flux de travail de la session, en utilisant la communication vocale et textuelle directe.



AVERTISSEMENT !

En cas de défaillance, appelez l'opérateur local par téléphone.

Lors de la connexion à un appareil, vous aurez un accès immédiat à la liste des utilisateurs du chat, organisée en deux onglets. Pour les clients multisites, chaque succursale peut être configurée en tant que contrat distinct. Lorsque cette option est activée, les utilisateurs sont regroupés par contrat, les utilisateurs d'autres contrats apparaissant sous l'onglet « Others » (Autres).

Pour démarrer une conversation, double-cliquez sur le nom d'un utilisateur pour ouvrir l'interface de chat, qui prend en charge à la fois la messagerie texte et les appels vocaux. Assurez-vous que la session sélectionnée correspond au bon appareil. La plateforme avertit les utilisateurs si la connexion réseau devient lente ou instable.



AVERTISSEMENT !

Avant d'initier le contact, vérifiez le nom de l'appareil indiqué sous le nom de l'utilisateur, car certains technologues à distance peuvent être connectés à plusieurs appareils.

Voici les outils disponibles pour la communication sur la plateforme :

1. **Appels vocaux et vidéo** : Cliquez sur l'icône pour lancer un appel vocal et vidéo d'une durée maximale de 60 minutes entre une télécommande et un technicien local. Les connexions entre utilisateurs ayant le même profil (Local-Local ou Remote-Remote) ne sont pas prises en charge.

Lorsqu'un opérateur local initie un appel, l'opérateur à distance peut choisir d'accepter ou de refuser. À l'inverse, lorsqu'un technologue à distance lance l'appel, il est automatiquement connecté et le technologue local est averti — ces fonctions comme mécanisme de sécurité pour s'assurer que le technologue à distance peut toujours communiquer avec toute personne physiquement présente sur le site, comme s'il était là en personne.

Par défaut, le microphone est actif au début de l'appel, tandis que la caméra reste éteinte. Chaque technologue peut allumer ou éteindre manuellement son microphone et sa caméra à tout moment.

Pour établir un appel avec succès, les deux utilisateurs doivent disposer d'un microphone et d'une sortie audio fonctionnels, avec les autorisations du navigateur correctement activées. Si l'un de ces composants est manquant, le système en informera les deux utilisateurs et l'appel ne sera pas terminé. Une caméra est facultative : si elle n'est pas disponible ou non détectée, le système mettra à jour l'icône pour indiquer que la vidéo n'est pas prise en charge.

Un seul appel actif est autorisé par utilisateur. Si un technologue essaie de démarrer un nouvel appel alors qu'il est déjà en ligne, le système bloquera la tentative et affichera une notification. De même, si un utilisateur est déjà en communication et reçoit un autre appel entrant, l'appelant sera informé que le destinataire est actuellement indisponible, et l'utilisateur de l'appel en cours recevra une alerte indiquant que quelqu'un a tenté de le contacter.

2. **Fermeture des chats** : Lorsque l'un des utilisateurs ferme le chat en cliquant sur le bouton de fermeture, un message automatique est envoyé à l'autre utilisateur et l'onglet de chat se ferme. Cela garantit que les deux parties sont informées que la conversation est terminée. Lorsque la fenêtre de chat est fermée, tous les messages disparaissent. Si vous la rouvrez pendant la session, la conversation redémarre sans les messages précédents.
3. **Messages textes** : Envoyez des messages texte dans le champ désigné. Lorsqu'un message est envoyé, une icône avec une coche grise apparaît et, lorsque le message est reçu par le destinataire, une autre icône avec deux coches bleues s'affiche. Cela permet une communication écrite sûre, claire et concise entre les deux parties.
4. **Demander l'attention** : Attirez l'attention de l'autre utilisateur en cliquant sur le bouton présentant un point d'exclamation. Cette action applique un effet de vibration visuelle à la fenêtre de l'autre utilisateur pendant quelques secondes et un message est envoyé automatiquement, signalant l'urgence ou l'importance.
5. **Messages audio** : Envoyez des messages audio en cliquant sur le bouton du microphone. Cette fonction est utilisée lorsque vous souhaitez transmettre un message de façon plus personnelle ou lorsque la saisie n'est pas pratique.

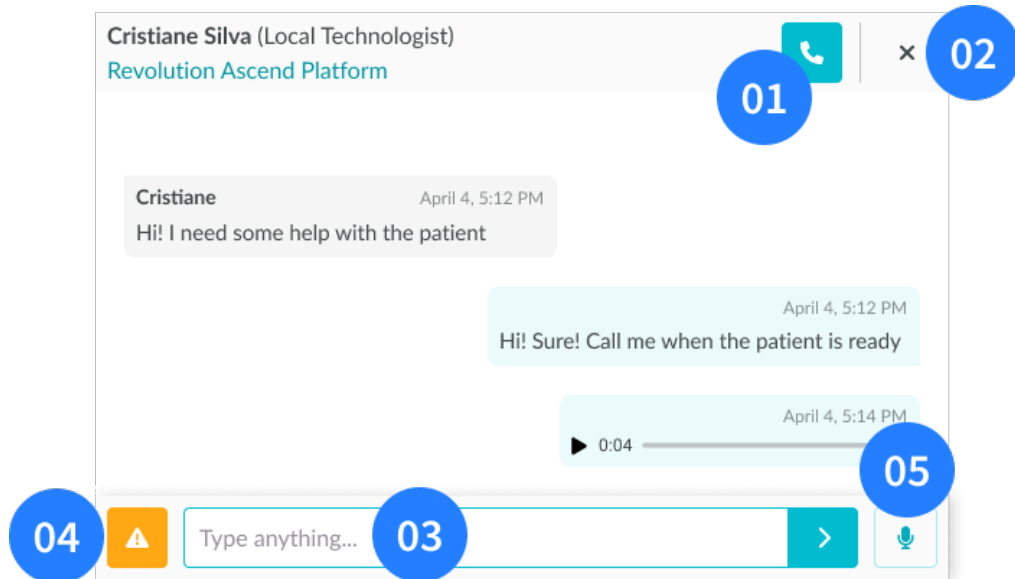


Figure 30 : Affichage de la fenêtre de chat

01 – Bouton d'appel vocal et vidéo ; 02 - Bouton Fermer le chat ; 03 – Zone de texte du message ;
04 – Bouton d'appel à l'attention ; 05 – Enregistrer Bouton de message audio

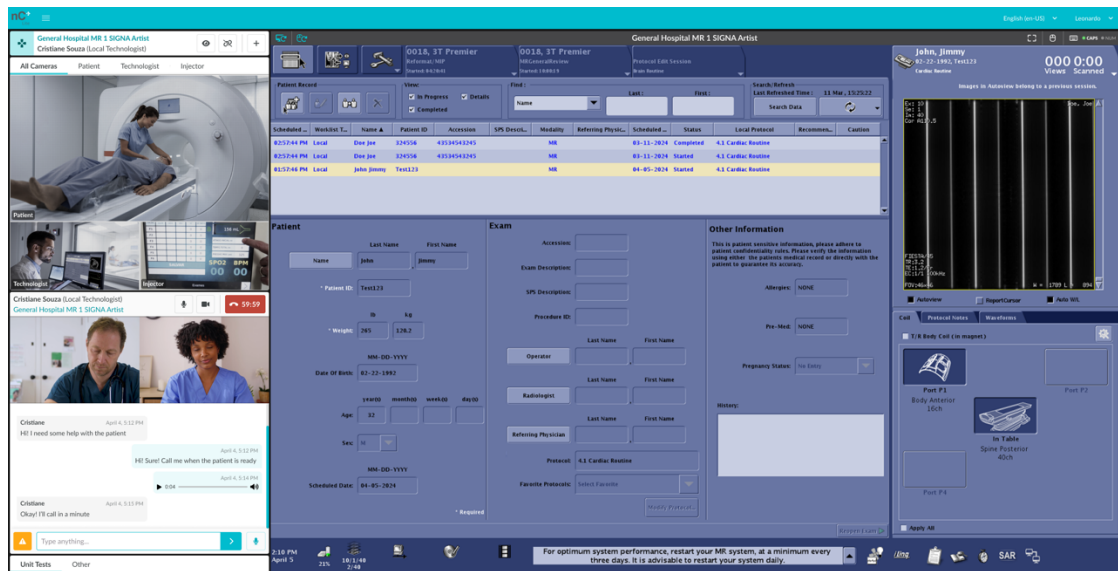


Figure 31 : Écran principal de l'Opérateur à distance – Fenêtre de chat (coin inférieur gauche)

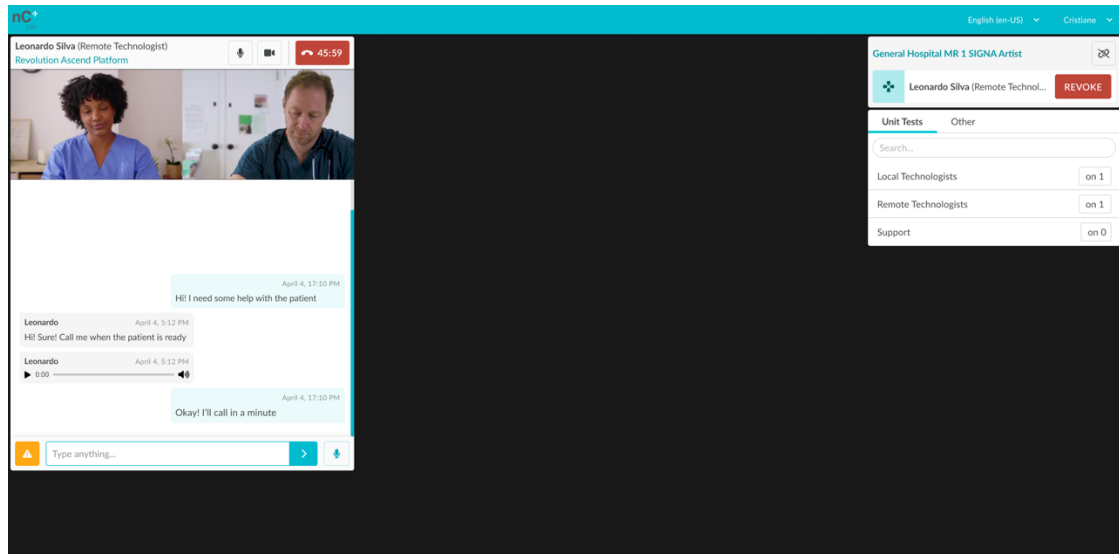


Figure 32 : Écran principal de l'Opérateur local – fenêtre de chat

Problèmes de connexion Internet : lorsque l'un des opérateurs rencontre des problèmes de connexion réseau, le système affiche un message et tente de se reconnecter. Si la connexion est rétablie, le système affiche un message **ONLINE (EN LIGNE)** et la session à distance se poursuit normalement. Cependant, après plusieurs tentatives de reconnexion, si la connexion n'est pas rétablie, le système mettra fin à la session active et notifiera l'opérateur qu'il a été déconnecté en raison de problèmes Internet. Dans le même temps, il informera également l'autre opérateur que son interlocuteur a été déconnecté en raison de problèmes de connexion Internet.

Section 3.7 - Mettre fin à votre session sur la plateforme

À la fin de son service, l'opérateur agréé doit se déconnecter de l'appareil et se déconnecter de la plateforme.



AVERTISSEMENT !

Les opérateurs agréés ne doivent pas oublier de se déconnecter de la plateforme avant la fin de leur service.

Pour vous déconnecter de l'appareil, vous devez cliquer sur l'icône de déconnexion située dans la boîte de dialogue de l'appareil. Note : Si vous travaillez en tant qu'opérateur local, assurez-vous d'avoir révoqué tout accès opérateur à distance avant de vous déconnecter de l'appareil.

Pour garantir la sécurité, vous recevrez une notification confirmant que vous souhaitez vous déconnecter de l'appareil. Après avoir confirmé, vous serez redirigé vers l'écran d'accueil, sans qu'aucun appareil ne soit sélectionné.

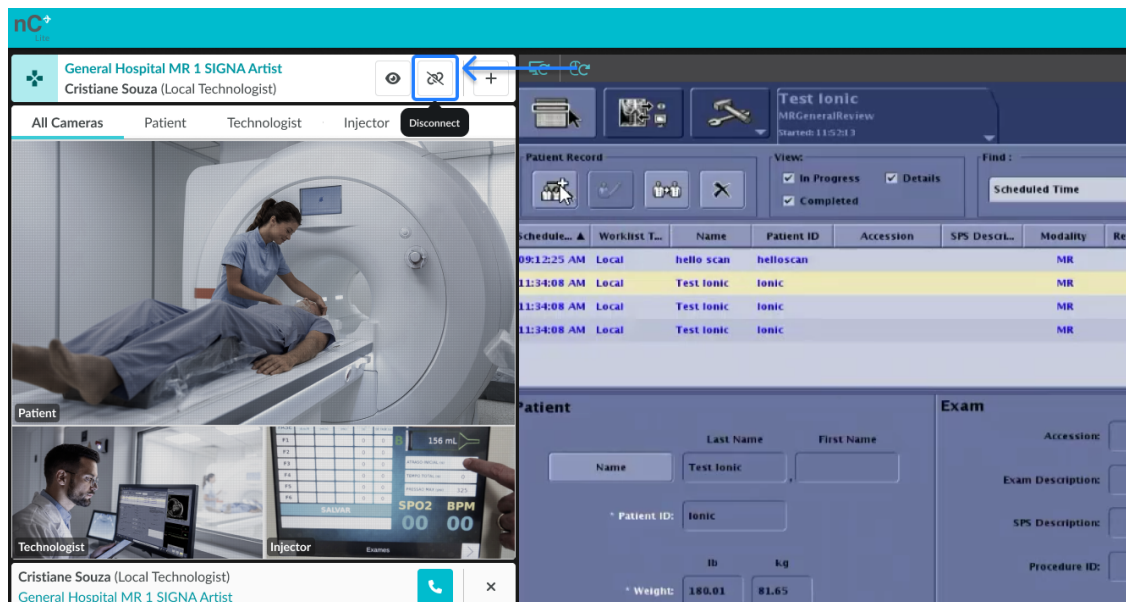


Figure 33 : Bouton Disconnect (Déconnexion) - écran principal de l'Opérateur à distance

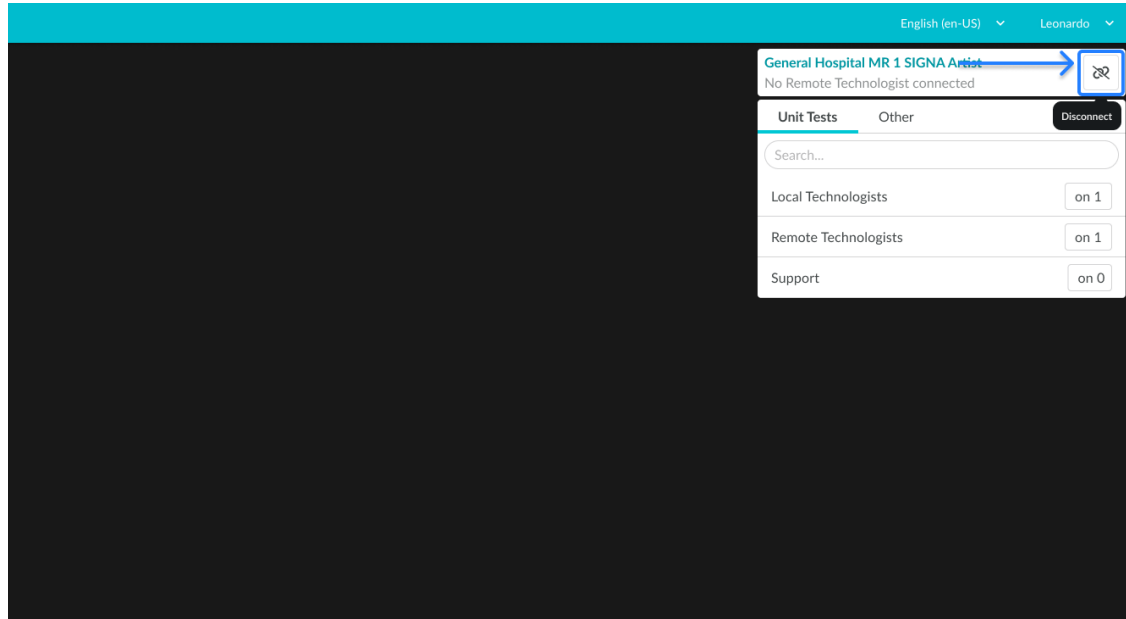


Figure 34 : Bouton Disconnect (Déconnexion) - écran principal de l'Opérateur local



AVERTISSEMENT !

Avant de vous déconnecter, assurez-vous que tous les onglets supplémentaires qui ont été ouverts sont fermés.

Pour mettre fin à votre session sur la plateforme, cliquez sur votre nom d'utilisateur situé dans le coin supérieur droit de l'écran et sélectionnez l'option « Logout » (Se déconnecter). Vous recevrez une notification confirmant que vous souhaitez quitter le centre médical où vous travailliez. Après confirmation, vous serez redirigé vers la page de connexion de l'application, ce qui conclura votre expérience de travail en toute sécurité.

nCommand Lite ne contrôle pas la session de l'utilisateur sur l'IdP externe et ne peut donc pas effectuer de déconnexion au niveau de l'IdP. Dans les scénarios où les utilisateurs partagent la même machine et utilisent l'authentification unique (SSO), il est recommandé que chaque utilisateur sélectionne l'option « Ne pas rester connecté » lors de la connexion au fournisseur d'identité externe (si disponible) ou se déconnecte du fournisseur d'identité après s'être déconnecté de nCommand Lite. Cela garantit qu'aucun utilisateur ultérieur sur le même appareil ne peut réutiliser involontairement une session active.

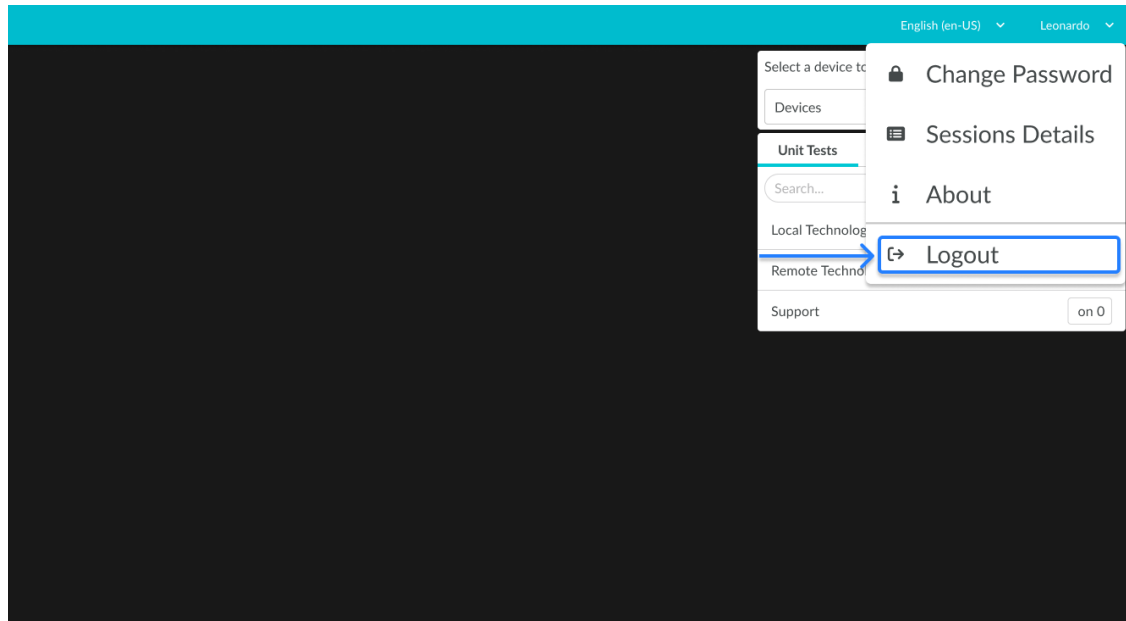


Figure 35 : Élément du menu déroulant de déconnexion



AVERTISSEMENT !

Lorsque vous utilisez un fournisseur d'identité externe sur un ordinateur partagé ou public, après vous être déconnecté de la plateforme, vous devez également vous déconnecter du fournisseur d'identité. Pour plus d'informations sur la procédure à suivre, contactez l'équipe de support informatique de votre organisation.

Section 3.8 - Formation opérationnelle

La participation au programme de formation est obligatoire pour tous les utilisateurs du système nCommand Lite. L'inscription des utilisateurs sur la plateforme est gérée par l'équipe IONIC Health et n'est lancée qu'après confirmation que l'utilisateur a réussi la formation LMS requise et est dûment qualifié pour utiliser la plateforme. Ce processus permet de s'assurer que tous les utilisateurs possèdent une compréhension approfondie des fonctionnalités du système et sont prêts à utiliser la plateforme de manière efficace et sûre. Pour lancer le processus d'inscription à la formation, veuillez contacter votre représentant commercial.

Section 3.9 - Directives de dépannage

UTILISATEUR ET MOT DE PASSE	
Modification du mot de passe	Vérifiez que les exigences de mot de passe ont été respectées : le mot de passe doit être fort et sécurisé, comportant au moins une lettre minuscule, une lettre majuscule, un caractère spécial et avoir une longueur d'au moins 8 caractères.
J'ai oublié mon mot de passe	Vérifiez votre boîte de réception : Assurez-vous d'utiliser la bonne adresse e-mail et que l'e-mail de récupération du mot de passe n'a pas été filtré dans votre dossier de spam ou de courrier indésirable. Réessayez : Attendez quelques minutes et demandez un autre e-mail de récupération du mot de passe en cliquant sur « Did you Forget your password? ». Vérifiez la connexion Internet : Assurez-vous d'être connecté à Internet.
E-mail de bienvenue non reçu	Vérifiez si l'e-mail se trouve dans votre dossier de spam. Si ce n'est pas le cas, contactez un utilisateur administrateur pour vous assurer que l'adresse e-mail fournie lors de votre inscription est correcte. Si ce n'est pas correct, l'administrateur doit la mettre à jour et renvoyer l'e-mail de bienvenue.
Code d'authentification à deux facteurs non reçu	Cliquez sur « Resend Code » (Renvoyer le code) et vérifiez votre dossier de spam. Si vous ne le recevez pas, veuillez contacter un administrateur pour vérifier si l'adresse e-mail enregistrée dans le contrôle d'accès est correcte.
Tentatives de connexion dépassées	Si vous dépassez le nombre autorisé de tentatives de connexion, vous devez attendre un certain temps avant de réessayer.
FOURNISSEUR D'IDENTITÉ EXTERNE	
Problèmes de connexion au produit	Si vous rencontrez des problèmes de connexion lors de l'utilisation d'un

	fournisseur d'identité (IdP) externe, veuillez noter que le processus d'authentification est entièrement géré par l'IdP et non par le fournisseur du produit, c'est-à-dire : Ionic Health. En tant que tel, le produit ne peut pas vous aider en ce qui concerne les informations d'identification du compte, les politiques d'accès, les erreurs d'authentification ou le verrouillage du compte. Dans ce cas, vous devez contacter l'équipe d'assistance informatique de votre organisation, qui peut examiner la configuration de l'IdP et vous aider à résoudre le problème.
Problèmes d'identifiants	Tout problème lié aux informations d'identification (<i>par exemple</i> , mot de passe oublié, changement de mot de passe) doit être résolu directement auprès de l'équipe de support informatique de votre organisation. Ils peuvent examiner la configuration de l'IdP et fournir l'assistance nécessaire.
Problèmes liés à l'authentification multifacteur (MFA)	Tout problème lié à l'authentification multifacteur (MFA) (<i>par exemple</i> , problèmes d'expiration de MFA, MFA ne fonctionne pas, connexion sans demander MFA) doit être résolu directement auprès de l'équipe de support informatique de votre organisation. Ils peuvent examiner la configuration de l'IdP et fournir l'assistance nécessaire.
Les identifiants ne fonctionnent pas sur la plateforme	Lorsque vous utilisez des fournisseurs d'identité externes (IdP), connectez-vous au produit uniquement à l'aide de l'IdP. L'utilisation des informations d'identification IdP directement sur la page de connexion du produit entraînera l'échec de la connexion.
MONITEUR DE L'ORDINATEUR DU SCANNER	
Ne s'allume pas	Vérifiez les connexions du moniteur à l'ordinateur et à la prise électrique. Des déconnexions peuvent se produire. Appuyez à nouveau sur le bouton d'alimentation du moniteur.
PLATEFORME	

Inaccessible	Vérifiez la connexion réseau. Vérifiez si la plateforme a démarré et si la connexion a eu lieu.
Latence de la plateforme	Actualisez la page en appuyant sur Ctrl+F5. Vérifiez si le chat de l'unité (établissement médical) est ouvert dans plusieurs onglets. Si c'est le cas, fermez l'onglet qui n'est pas utilisé. Si le problème persiste, essayez de vous déconnecter de la plateforme, de vider le cache, de fermer le navigateur, puis de vous reconnecter.
Fonctionnalités défaillantes	Avant d'essayer d'autres procédures de dépannage, effacez le cache du navigateur (recherchez des instructions sur votre navigateur actuel) après vous être connecté, puis fermez et rouvrez le navigateur, reconnectez-vous à la plateforme et réessayez l'action.
Mise à niveau	Une fois la plateforme mise à niveau, videz le cache de votre navigateur (reportez-vous aux instructions de votre navigateur) avant de vous connecter à la nouvelle version.
AUDIO	
Aucun son	Assurez-vous que les volumes du microphone et du haut-parleur de l'unité (établissement médical) sont réglés aux niveaux appropriés. Vérifiez si le navigateur est autorisé à utiliser la fonction audio et le microphone. Vérifiez si le casque est connecté et fonctionne correctement.
Latence sonore	Vérifiez les connexions électriques et réseau de l'équipement. Actualisez la page du navigateur en appuyant sur Ctrl+F5 et connectez-vous à nouveau. Si le problème persiste, essayez de vous déconnecter de la plateforme, de vider le cache, de fermer le navigateur, puis de vous reconnecter.

CHAT	
Le chat n'apparaît pas	Assurez-vous que le navigateur n'est pas réduit. Sinon, ouvrez le chat après vous être connecté à la plateforme nCommand Lite. Vérifiez que l'unité (établissement médical) a été sélectionnée et que l'utilisateur est autorisé à activer la communication par chat. Assurez-vous que les autorisations audio et microphone de votre navigateur sont acceptées. Vérifiez les connexions des câbles ; elles peuvent être déconnectées. Actualisez la page du navigateur en appuyant sur Ctrl+F5 et reconnectez-vous à la plateforme. Vérifiez si le chat du site est ouvert dans plusieurs onglets. Si c'est le cas, fermez l'onglet qui n'est pas utilisé.
Retard du chat	Actualisez la page du navigateur en appuyant sur Ctrl+F5 et reconnectez-vous à la plateforme. Si le problème persiste, essayez de vous déconnecter de la plateforme, de vider le cache, de fermer le navigateur, puis de vous reconnecter. Vérifiez les connexions des câbles ; elles peuvent être déconnectées.
Problèmes d'envoi de messages audio	Vérifiez les autorisations du navigateur pour la fonction audio et le microphone et assurez-vous que le microphone et les appareils audio sont connectés à l'ordinateur. Si les autorisations du navigateur doivent être ajustées, appuyez sur Ctrl+F5 pour amener le navigateur à reconnaître les modifications lors du rechargement de la page.

Échec de démarrage de l'appel vocal	Vérifiez votre connexion Internet et voyez si une notification expliquant la raison pour laquelle l'appel ne démarre pas s'est affichée. Assurez-vous qu'un appareil audio est connecté et que les autorisations audio et microphone sont autorisées dans le navigateur. Si le problème persiste, actualisez la page en appuyant sur Ctrl+F5 pour réessayer.
Utilisateur introuvable dans le chat	Si vous ne parvenez pas à localiser un utilisateur dans le chat, cliquez sur l'onglet « Others » (Autres) pour vous assurer qu'il n'y figure pas. Les utilisateurs associés à d'autres contrats apparaissent séparément dans la liste des contacts. Si votre utilisateur n'apparaît pas dans la liste des contacts après avoir sélectionné l'appareil, appuyez sur Ctrl+F5 pour actualiser l'écran et sélectionnez à nouveau l'appareil. Assurez-vous d'avoir une connexion Internet.
DEMANDER L'ACCÈS À L'APPAREIL	
La plateforme n'a pas remarqué que l'opérateur local était connecté	Cochez l'option « Others » (Autres) pour confirmer si l'utilisateur local est connecté. Si l'utilisateur est effectivement connecté, mais que vous recevez toujours le message indiquant que l'utilisateur local n'est pas connecté au scanner, actualisez l'écran en appuyant sur Ctrl+F5 et demandez à l'utilisateur local de répéter la même instruction. Ensuite, sélectionnez à nouveau l'appareil et demandez à l'utilisateur local de sélectionner à nouveau l'appareil. Si le problème persiste, contactez l'assistance pour faire vérifier le réseau.
La demande d'accès n'est pas envoyée	Actualisez la page en appuyant sur Ctrl+F5 et confirmez avec l'utilisateur local par chat si la demande d'accès est reçue. Si le problème persiste, veuillez contacter l'assistance pour obtenir de l'aide.
APPAREIL DE STREAMING (ORDINATEUR e-KVM)	
L'appareil de streaming (ORDINATEUR e-KVM) ne fonctionne pas	Cliquez sur le bouton « Reload streaming » (Recharger le streaming) sur la plateforme.

	Assurez-vous que l'alimentation électrique sans coupure et stabilisée (de l'établissement médical) et/ou l'appareil de streaming sont correctement connectés et sous tension. Éteignez l'appareil de streaming et tous les autres équipements et rallumez-les. Actualisez la plateforme.
Appareil de streaming lent	Cliquez sur le bouton « Reload streaming » (Recharger le streaming) sur la plateforme. Actualisez la page en appuyant sur Ctrl+F5 et reconnectez-vous à la plateforme. Vérifiez la qualité de votre connexion réseau. Pour confirmer l'état du réseau, il est possible d'effectuer un test ping sur l'appareil pour vérifier la perte de paquets. Après des problèmes Internet, la plateforme peut ne pas fonctionner comme prévu. Actualisez la page Web et demandez à nouveau l'accès à l'utilisateur local.
Perte de sortie vidéo	Il est admissible qu'une décharge électrostatique provoque une perte d'image. Après un redémarrage du système, la communication et le streaming vidéo devraient être rétablis automatiquement.

Section 3.10 - Méthodes de nettoyage du matériel

- Avant de commencer le processus de nettoyage, assurez-vous que tout l'équipement est débranché de la prise électrique.
- N'utilisez pas de produits abrasifs.
- N'immergez aucun équipement ou périphérique dans un liquide, quel qu'il soit.
- Éliminez les produits de nettoyage conformément aux réglementations relatives à l'élimination des déchets dangereux.
- Il n'est pas conseillé d'utiliser un désinfectant par pulvérisation, car de la vapeur pourrait pénétrer dans l'équipement et provoquer un court-circuit ou de la corrosion.
- Ce produit n'est pas stérile

Chapitre 4 Cybersécurité et confidentialité

Section 4.1 - Risques liés à la sécurité et à la confidentialité

Le **système nCommand Lite** met en œuvre diverses mesures techniques et organisationnelles pour protéger les informations traitées.

Le système a été certifié ISO/IEC 27001 et ISO/IEC 27701 et suit une approche de confidentialité dès la conception. Assure la conformité aux lois sur la protection des données de santé et aux réglementations en matière de cybersécurité applicables dans l'UE, aux États-Unis, au Royaume-Uni, en Suisse, au Brésil, aux Émirats arabes unis et en Arabie saoudite.

Toutefois, les utilisateurs doivent adopter les meilleures pratiques pour empêcher toute exposition inutile de données sensibles.

- Évitez de partager des informations personnelles ou sensibles si ce n'est pas strictement nécessaire.
- Veillez à ce que les communications et les accès au système aient lieu dans des environnements sécurisés.
- Si vous soupçonnez une activité malveillante, veuillez en informer immédiatement l'équipe responsable.

Section 4.2 - Protection des données personnelles (conformité RGPD / HIPAA)

Le **Système nCommand Lite** est conforme à toutes les lois et réglementations applicables en matière de confidentialité et de protection des données dans les régions où il opère, y compris, mais sans s'y limiter, les exigences du RGPD, de la loi HIPAA, de la LGPD et de la norme ISO/IEC 27701. Toutes les activités de traitement des données sont réalisées sous les rôles de « **sous-traitant** » et de « **sous-traitant ultérieur** » tels que définis par le RGPD, avec une stricte ségrégation régionale des données afin d'assurer la conformité et d'empêcher tout transfert transfrontalier non autorisé de données.

Quelles sont les données recueillies ?

- **Utilisateurs** : Nom, adresse e-mail, et nom de l'entreprise (uniquement pour l'authentification et la gestion des accès).
- **Données des patients** : Seuls les examens médicaux sont transmis en streaming en temps réel, sans stockage de données.

Comment les données sont-elles utilisées et protégées ?

- Les données sont utilisées uniquement à des fins **d'authentification, de contrôle d'accès, et de traçabilité des sessions**.
- La transmission des données est sécurisée par **chiffrement AES-256 pour le stockage** et par **TLS 1.3 pour les données en transit**.
- L'accès est restreint et suit le **principe du moindre privilège (RBAC)**.

- Cryptage de bout en bout assuré pour les flux vidéo P2P et de contrôle via WebRTC.
- Les fournisseurs de cloud autorisés (par exemple, Microsoft Azure) traitent des données limitées dans le cadre de garanties contractuelles strictes.

Les droits suivants sont octroyés aux utilisateurs :

- **Accès aux et correction** des informations personnelles.
- **Demande de suppression de données**, le cas échéant.

Pour toute question, veuillez communiquer avec le DPO (délégué à la protection des données) d'Ionic Health à l'adresse e-mail suivante : privacy@ionic.health. Toutes les demandes sont traitées dans un délai de 30 jours, prorogeable conformément au RGPD.

Section 4.3 - Gestion des accès et authentification

Les utilisateurs sont responsables de la définition des **rôles et permissions d'accès** pour leurs équipes, et sont tenus de régulièrement passer en revue et documenter les accès octroyés.

Meilleures pratiques et contrôles

- Pour garantir que les utilisateurs bénéficient uniquement du niveau d'accès nécessaire, suivez le **principe du moindre privilège (RBAC)**.
- L'**authentification multi-facteurs (MFA)** est obligatoire pour l'accès administratif et recommandée pour tous les utilisateurs.
- Des **mots de passe robustes** sont obligatoires, d'une longueur d'au moins **8 caractères et comportant des lettres minuscules et majuscules, des chiffres et des symboles**.
- **Ne pas partager les informations d'identification**.
- Les autorisations d'accès sont surveillées et révisées périodiquement.

Surveillance : Les accès, les modifications des permissions et les activités importantes sont consignés dans les journaux de sécurité du système. Les journaux sont conservés pendant au moins 7 ans, conformément à la HIPAA, au RGPD et à toute autre réglementation applicable. Ils soutiennent l'audit interne, l'analyse judiciaire et le reporting réglementaire. Les journaux sont protégés contre la falsification et stockés dans des environnements sécurisés avec contrôle d'accès.

Section 4.4 - Commande d'accès à la vérification système

La fonction de vérification du système est accessible exclusivement via l'**application Web nCommand Lite** et nécessite des identifiants valides pour la connexion. L'accès est strictement réservé aux rôles autorisés — *Opérateur à distance, Opérateur local, Administrateur, Superviseur de rôle et Utilisateur de vérification du système*.

Le rôle *Utilisateur de Vérification du système* est conçu avec des autorisations restreintes, permettant l'accès uniquement aux fonctionnalités de diagnostic liées à la validation du réseau et à la vérification de la connectivité. Cela garantit que les informations réseau, les données de liste blanche et les indicateurs système ne sont jamais accessibles à des personnes non autorisées.

Toutes les demandes d'accès sont authentifiées via Azure AD B2C, avec une authentification multifacteur (MFA) et des stratégies d'accès conditionnel adaptatives gérées par Microsoft Entra ID. La complexité des mots de passe est conforme à la politique de sécurité de l'organisation et exige au moins huit caractères, comprenant des lettres majuscules et minuscules, des chiffres et des symboles. Les mots de passe expirent tous les 90 jours et les sessions sont automatiquement déconnectées après 24 heures d'inactivité, une durée extensible jusqu'à 90 jours en cas d'utilisation continue.

Section 4.5 - Ségrégation régionale des données et conservation des journaux

La plateforme **nCommand Lite** maintient une stricte séparation régionale des données afin d'empêcher les transferts transfrontaliers non autorisés ou inutiles. Les environnements sont isolés par région, garantissant ainsi le respect des réglementations applicables.

Tous les journaux d'accès, les enregistrements d'activité et les événements de sécurité sont conservés pendant au moins sept (7) ans, conformément à la réglementation applicable en matière de protection des données et de soins de santé. Les journaux sont stockés dans des environnements sécurisés à accès contrôlé et protégés contre toute falsification. Ces informations servent de base aux enquêtes médico-légales, aux audits de conformité et aux rapports réglementaires.

Section 4.6 - Sécurité et intégrité des données

Le **système nCommand Lite** assure la confidentialité, l'intégrité et la disponibilité des données par le biais de pratiques de sécurité conformes aux normes sectorielles.

Les utilisateurs sont encouragés à assurer la conformité aux protocoles de sécurité, à régulièrement passer en revue les politiques d'accès, et à signaler toute anomalie. Le système surveille les activités en continu, et les administrateurs doivent appliquer les politiques de sécurité afin de maintenir une défense solide contre les menaces potentielles.

Le système est protégé par une surveillance 24h/24 et 7j/7 via un centre d'opérations de sécurité (SOC) dédié doté de capacités SIEM pour la détection et la réponse aux menaces.

Section 4.7 - Réponse aux incidents de sécurité

Le système comprend un plan de réponse aux incidents documenté, aligné sur ISO 27035 et NIST CSF.

En cas d'incident de sécurité, comme un accès non autorisé ou une défaillance système, les utilisateurs doivent suivre les étapes suivantes :

Comment reconnaître un incident ?

- **Accès non autorisé** détecté dans les journaux d'activité.
- **Tentatives de connexion suspectes** ou échecs d'authentification à répétition.

- **Comportement inhabituel du système**, par exemple des actions inattendues ou des dysfonctionnements.

Comment signaler un incident ?

Enregistrez immédiatement l'événement en utilisant les canaux d'assistance disponibles (Chapitre 5).

En cas de confirmation d'une violation de données personnelles, IONIC, agissant en tant que sous-traitant, notifiera GE en tant que responsable du traitement dans les 48 heures, en fournissant toutes les preuves pertinentes, les détails de l'impact et les mesures d'atténuation. GE, quant à elle, est responsable d'informer le contrôleur (le client) conformément aux exigences légales et contractuelles applicables.

Chapitre 5 Canaux de service

Que vous ayez besoin d'aide pour un problème technique, une étape peu claire du processus ou pour des conseils supplémentaires, notre équipe est prête à vous aider. Vous pouvez nous contacter par téléphone, e-mail ou par le biais de la plateforme ITSM, selon ce qui vous convient le mieux. Nos spécialistes sont formés pour offrir une aide personnalisée, en veillant à ce que tout problème soit résolu rapidement et efficacement.

Numéros de téléphone

États-Unis	+1 (216) 2421223
Brésil	+55 12 3600 0181
Europe (Portugal)	+351 (300) 528 410
Australie	+1 (216) 2421223
Nouvelle-Zélande	+1 (216) 2421223

Plateforme ITSM

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

E-mail

helpdesk@ionic.health



AVERTISSEMENT !

Tout incident grave lié à l'utilisation de ce dispositif doit être signalé à la fois au fabricant et à l'autorité sanitaire/compétente du lieu où l'appareil est installé.

Pour le signaler au fabricant : contactez votre représentant local du service après-vente ou adressez-vous à : helpdesk@ionic.health

Veillez fournir les informations suivantes :

- Le numéro de version du système, affiché à l'écran de connexion ;
- La date de l'incident ;
- La description de l'incident, y compris tout impact/blessure sur le patient ou l'utilisateur ;
- Vos coordonnées (établissement, adresse, nom de contact, titre et numéro de téléphone).

Chapitre 6 Informations juridiques et réglementaires

Fabricant



REF

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
Brésil

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

Technicien responsable

Alexandre Seiji Fukuda Ribas
CREA-SP : 5071085437

ANVISA

82585300004

Importateur (États-Unis)



REF

Système nCommand Lite

IONIC HEALTH USA INC.

11201 Cedar Avenue, STE 600
Cleveland, OH 44106
USA

+1 (216) 242 1223

Représentant/Importateur UE



EU REP

REF

nCommand Lite



Numéro d'identification de l'organisme
notifié : 2803

EUROPE IONIC HEALTH DIGITAL TECHNOLOGIES, LDA

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

+351 (300) 528 410

Représentant agréé suisse (CH-REP) / Importateur**CH REP****REF**

nCommand Lite

FREYR LIFE SCIENCES GMBH

Bahnhofplatz
CH-6300 Zug
Suisse

Personne responsable / Importateur au Royaume-Uni**REF**

nCommand Lite

FREYR LIFE SCIENCES LTD

9 Greyfriars Road
Reading, Berkshire
RG1 1NU
Angleterre, Royaume-Uni

Sponsor australien**REF**

nCommand Lite

TAEVAS LIFE SCIENCES PTY LTD

46 Dora St
Blacktown NSW 2148
Australie

Sponsor néo-zélandais**REF**

nCommand Lite

TAEVAS LIFE SCIENCES LIMITED

Niveau 3, 1 Margaret Street
Lower Hutt 5010
Nouvelle-Zélande

UDI-DI de base: 7898974112NCLITE2L

Demande d'une copie papier

Des copies papier du manuel de l'utilisateur nCommand Lite seront fournies sur demande, sans frais supplémentaires. Contactez votre représentant local et demandez une copie papier du manuel de l'utilisateur.

Date de fabrication

La date de sortie du logiciel se trouve sur la page de connexion de nCommand Lite, au format MOIS/ANNÉE.

Chapitre 7 Historique des révisions

Révision	Description des modifications	Date
0	Mise à jour manuelle de la version 2.3 v1 à la version 2.4	25 novembre 2025
1	Mise à jour des libellés du chapitre 6	04 décembre 2025
2	Suppression de l'exigence d'une adresse IP statique dans la configuration de l'ordinateur local (section 1.3.11). Mise à jour du symbole du représentant autorisé de l'UE dans la sous-section 1.3.12 Note supprimée du sous-élément 1.3.14 Mise à jour du contenu du chapitre 2 Mise à jour du symbole du représentant autorisé de l'UE au chapitre 6	28 janvier 2026
3	La traduction de « Technicien responsable » a été revue au chapitre 6.	9 février 2026

ANNEXE I - Liste de contrôle pour le début de l'entretien

1. Vérifier les connexions électriques et réseau :

Assurez-vous que les connexions électriques et les points de réseau sont correctement établis sur l'ordinateur e-KVM, l'ordinateur du scanner et l'ordinateur local.

2. Vérifier l'état de l'alimentation :

Vérifiez que l'alimentation électrique sans coupure et stabilisée et l'ordinateur e-KVM sont sous tension et fonctionnent correctement.

3. Accès rapide à la plateforme nC Lite :

Confirmez la présence du raccourci de la plateforme nC Lite sur le bureau pour un accès rapide.

4. Accès et connexion à la plateforme nC Lite :

Ouvrez la plateforme nCommand et connectez-vous pour garantir un accès complet et un fonctionnement correct.

5. Configuration de l'application de chat :

Ouvrez l'application de chat sur la plateforme nC Lite dans un seul onglet et évitez de le réduire, pour une communication fluide.