



MANUAL DO USUÁRIO

nCommand Lite v2.4

Versão Manual: V.3



Conteúdo

Capítulo 1	Introdução.....	4
Sessão 1.1 -	Finalidade	4
Sessão 1.2 -	Glossário	4
Sessão 1.3 -	Descrição	5
1.3.1.	Utilização pretendido	5
1.3.2.	Indicações de utilização	6
1.3.3.	População de pacientes pretendida	6
1.3.4.	Ambiente de utilização	6
1.3.5.	Contraindicações	6
1.3.6.	Capacidades da Plataforma	6
1.3.7.	Benefícios Clínicos	7
1.3.8.	Usuários previstos	7
1.3.9.	Ambiente operacional	7
1.3.10.	Ambiente da instalação.....	8
1.3.11.	Requisitos mínimos.....	9
1.3.12.	Símbolos	10
1.3.13.	Vida útil	11
1.3.14.	Atualizações/melhorias (Upgrades).....	11
Capítulo 2	Lista de Avisos e Precauções Gerais.....	12
Capítulo 3	Utilização da plataforma em cada localidade	14
Sessão 3.1 -	Acesso e uso do nCommand Lite	14
Sessão 3.2 -	Primeiro acesso à plataforma.....	14
3.2.1.	Login via nCommand Lite	15
3.2.2.	Login via IdP Externo	16
Sessão 3.3 -	Gerenciamento de senhas	17
Sessão 3.4 -	Acesso com perfil de técnico local	20
Sessão 3.5 -	Acesso com perfil de técnico remoto	23
3.5.1.	Modo de Acesso	24
3.5.2.	Barra de Streaming	27
3.5.3.	Multi-câmera	30
3.5.4.	Abrir Outro Equipamento.....	32
3.5.5.	System Check	34
Sessão 3.6 -	Chat.....	35
Sessão 3.7 -	Encerrando sessão na plataforma	38
Sessão 3.8 -	Treinamento Operacional.....	40
Sessão 3.9 -	Diretrizes de Solução de Problemas	41

Sessão 3.10 - Métodos de Limpeza do Hardware	46
Capítulo 4 Cibersegurança e Privacidade	47
Sessão 4.1 - Riscos de Segurança e Privacidade	47
Sessão 4.2 - Proteção de Dados Pessoais (Conformidade com GDPR / HIPAA)	47
Sessão 4.3 - Gerenciamento de Acesso e Autenticação	48
Sessão 4.4 - Controle de Acesso à Verificação do Sistema	48
Sessão 4.5 - Segregação Regional de Dados e Retenção de Registros	49
Sessão 4.6 - Segurança e Integridade de Dados	49
Sessão 4.7 - Resposta a Incidentes de Segurança	49
Capítulo 5 Canais de Atendimento	50
Capítulo 6 Informações Legais e Regulatórias	51
Capítulo 7 Histórico de Revisões	54
APÊNDICE - Lista de Verificação para Início de Utilização	55

**ATENÇÃO**

A lei federal restringe a venda desse dispositivo a um médico ou por ordem deste, e usado por um técnico médico licenciado no estado em que exerce a profissão.

(para os Estados Unidos da América)

**ATENÇÃO**

No Brasil, esse software é autorizado pela Anvisa para uso exclusivo em aparelhos de Ressonância Magnética (RM). Qualquer outro uso não é permitido.

(para uso no Brasil)

**ATENÇÃO**

Antes de usar, informe-se sobre os requisitos específicos do seu país ou região. O descumprimento das normas pode resultar em riscos à saúde.

**ATENÇÃO**

Certifique-se de que a versão deste manual do usuário corresponde à versão da plataforma em uso. O uso de uma versão incompatível pode resultar em operação incorreta ou interpretação errônea dos recursos.

Capítulo 1 Introdução

Sessão 1.1 - Finalidade

O objetivo deste manual é fornecer aos técnicos locais e remotos uma compreensão abrangente das funcionalidades específicas do sistema nCommand Lite. Funcionando como um Manual do Usuário, este documento fornece informações concisas e práticas, orientando os usuários através das funcionalidades e resolução de problemas do sistema.

Seguindo este manual, os usuários poderão utilizar o nCommand Lite de forma eficiente, ajudando a maximizar a produtividade e reduzir a dependência do suporte técnico.

Sessão 1.2 - Glossário

**ATENÇÃO**

Este símbolo aplica-se a condições ou ações que podem representar um risco potencial. Pode causar ferimentos leves ou danos materiais se ignorar essas instruções.

**AVISO**

Este símbolo identifica condições ou ações que resultam em um perigo específico. Poderá causar ferimentos graves ou danos materiais significativos se ignorar estas instruções.

Termo da Plataforma	Termo Correspondente
Unidade Médica	Estabelecimento médico, Unidade, Unidade médica móvel, Estabelecimento de saúde, Unidade de saúde, Clínica, Hospital
Estação de Trabalho remota	Estação Remota, Escritório remoto, Centro de comando (<i>Command Center</i>), Sala Remota
Plataforma	Aplicação web nCommand Lite
Sistema	nCommand Lite com todos os subsistemas/acessórios (e-KVM, câmera)
Equipamento	Scanner médico, Dispositivo médico, Dispositivo de imagem, Equipamento de imagem médica, dispositivo médico
Técnico local	Operador local, Equipe Local, Apoio Local, Usuário Local

Sessão 1.3 - Descrição

O sistema nCommand Lite é um SaMD (Software como Dispositivo Médico) que fornece ao cliente acesso remoto por meio de uma aplicação Web para visualização/revisão de imagens, bem como a capacidade de fornecer orientação remota em tempo real ao técnico habilitado próximo ao paciente (usuário local) que opera os equipamentos médicos de imagem no contexto de treinamento ou avaliação de procedimentos, para equipamentos de RM, TC e PET/CT.

Os usuários remotos são técnicos habilitados que podem acessar um equipamento de imagem médica a partir de um computador que atenda às especificações mínimas exigidas em qualquer lugar, utilizando uma conexão de software segura que transmite vídeo e fornece acesso ao teclado e ao mouse. Isso permite que usuários remotos auxiliem usuários locais sem que a distância seja uma limitação. Este acesso deve ser concedido pelo usuário local que utiliza o sistema e também pode ser revogado a qualquer momento, pelo usuário local, permitindo-lhe manter o controle total da sessão em todos os momentos. Além disso, cada sessão remota é controlada por meio de uma credencial segura gerenciada pelo usuário local. As conexões a um equipamento médico estão limitadas a uma sessão remota por vez, para manter um controle rigoroso sobre quem interage remotamente com o sistema. As imagens revistas remotamente não se destinam a utilização em diagnóstico.

O sistema nCommand Lite consiste numa solução de instalação baseada em hardware e software de TI que suporta múltiplas sessões, permitindo aos técnicos remotos acessar vários equipamentos de imagem médica, conforme necessário. Os equipamentos compatíveis com o sistema nCommand Lite seguem um protocolo comum, permitindo a gestão de parâmetros e a operação remota.

1.3.1. Utilização pretendido

O sistema nCommand Lite fornece acesso remoto para visualização/revisão de imagens, bem como a capacidade de fornecer orientação remota em tempo real ao técnico habilitado que utiliza o equipamento. Essas orientações incluem treinamento, avaliação de procedimentos e gerenciamento de parâmetros de varredura.

1.3.2. Indicações de utilização

O sistema nCommand Lite permite o acesso remoto para visualização/revisão de imagens, bem como a capacidade de fornecer orientação remota em tempo real ao técnico habilitado que utiliza um equipamento de RM, TC ou PET/CT compatível. Este acesso deve ser concedido pelo técnico local habilitado que está utilizando o sistema. O acesso remoto está disponível apenas para sistemas compatíveis com a funcionalidade de conectividade remota. As imagens analisadas remotamente não se destinam ao uso diagnóstico.

1.3.3. População de pacientes pretendida

Qualquer paciente com prescrição para realizar exames de imagem por meio de um equipamento de imagem médica conectado.

1.3.4. Ambiente de utilização

Instalações de imagem que realizam exames de Ressonância Magnética (RM), Tomografia Computadorizada (TC) e Tomografia por Emissão de Pósitrons – Tomografia Computadorizada (PET/CT) e Centros de Comando remotos.

1.3.5. Contraindicações

A plataforma não deve ser utilizada por usuários que não sejam técnicos habilitados e que não tenham recebido formação na utilização do nCommand Lite.

1.3.6. Capacidades da Plataforma

- **Operação remota:** exibe a tela do equipamento médico de imagem em tempo real, permitindo que um técnico remoto autorizado assista a um exame.
- **Chat:** permite a comunicação entre os técnicos habilitados remotos e locais através de mensagens de texto e voz. Os técnicos locais e remotos também podem fazer e receber chamadas de voz e vídeo.
- **Multicâmera:** facilita a observação remota dos pacientes e das unidades médicas durante o procedimento. O técnico remoto pode ver as câmeras através das abas que estão divididas entre todas as câmeras e as abas individuais. Este mecanismo replica a supervisão visual que um profissional de saúde teria se estivesse próximo ao paciente, introduzindo assim uma camada adicional de segurança.
- **Multi-sessão para acesso remoto** permite que o técnico remoto acesse vários equipamentos médicos de imagem, conforme necessário.
- **Modo de acesso:** permite ao técnico remoto escolher entre visualizar ou controlar o equipamento. No modo de Visualização, os técnicos remotos só podem ver o que está sendo transmitido. No modo de Controle, ele tem controle sobre o mouse e o teclado.
- **Gerenciar o acesso do técnico remoto:** permite que o técnico local controle o acesso do técnico remoto e seu modo de acesso (Visualização ou Controle). Para permitir a conexão do técnico remoto, o acesso deve ser concedido pelo técnico local que estiver usando a plataforma e também pode ser revogado a qualquer momento pelo técnico local, permitindo que ele mantenha o controle total da sessão o tempo todo.
- **Resolução do streaming:** o técnico remoto pode ver a resolução original e a resolução atual do streaming em pixels. Ele também é notificado quando a resolução do streaming atual é menor do que o original.
- **Estado do mouse e do teclado:** o técnico remoto recebe feedback se o mouse e o teclado do equipamento médico de imagem estão funcionando corretamente.

- **Detalhes da sessão:** os técnicos locais e remotos podem acessar detalhes sobre a sessão.

1.3.7. Benefícios Clínicos

O **nCommand Lite** aprimora o diagnóstico por imagem ao permitir a operação remota de sistemas de **RM, TC e PET-CT**, garantindo a qualidade consistente da imagem e a adesão aos protocolos. Ele permite que técnicos experientes supervisionem e auxiliem nos exames em tempo real, otimizando a eficiência do fluxo de trabalho e reduzindo erros que poderiam afetar a precisão do diagnóstico. O sistema facilita a colaboração entre os técnicos, melhorando a consistência dos exames e permitindo uma tomada de decisão mais rápida em casos complexos. Ao permitir que os profissionais remotos ofereçam suporte a várias instalações, o **nCommand Lite** aumenta a **disponibilidade, variedade e qualidade** dos exames de imagem, garantindo que mais pacientes tenham acesso a diagnósticos avançados e, ao mesmo tempo, otimizando os recursos do setor de saúde. Além disso, ajuda a atenuar a escassez de pessoal, reduzindo a dependência de especialistas no local, tudo isso mantendo a conformidade com rigorosos padrões regulatórios e de segurança de dados.

1.3.8. Usuários previstos

- **Técnico Local**

O técnico local é o usuário no local responsável por auxiliar e orientar os pacientes presencialmente na unidade médica. Deve possuir o conhecimento necessário para realizar procedimentos de imagens para um determinado equipamento. Além disso, controla o modo de acesso do técnico remoto (Visualização ou Controle) que deve ser concedido pelo técnico local por meio da plataforma e pode ser revogado a qualquer momento.

- **Técnico remoto**

Um profissional que realiza procedimentos remotamente, com acesso e controle do computador do equipamento. Assim como o técnico local, o técnico remoto também deve ter o conhecimento necessário para executar os procedimentos de varredura de um determinado equipamento médico de imagem.

- **Suporte/Usuário de TI**

Profissional responsável pela configuração da plataforma (não incluído neste Manual do Usuário).

1.3.9. Ambiente operacional

As especificações a seguir referem-se aos requisitos ambientais do computador e-KVM.

- **Altitude máxima (sem pressurização)**

- Operação: De 0 m (0 pés) a 3048 m (10.000 pés)
- Armazenamento: De 0 m (0 pés) a 12.192 m (40.000 pés)

- **Temperatura**

- Operação: De 10°C (50°F) a 35°C (95°F)
- Armazenamento: De -10°C (14°F) a 50°C (122°F)

- **Umidade relativa**
 - Operação: 20%-80% (não condensante)
 - Armazenamento: 10%-90% (não condensante)

1.3.10. Ambiente da instalação

A plataforma nCommand Lite possui dois tipos diferentes de localização de ambiente:

- **Unidade Médica:** Instalações que realizam exames de Ressonância Magnética (RM), Tomografia Computadorizada (TC) ou Tomografia por Emissão de Pósitrons - Tomografia Computadorizada (PET/CT).
- **Estação de Trabalho Remota:** Local onde técnicos remotos podem acessar e gerir remotamente equipamentos médicos de imagem (RM, TC ou PET/CT). Esta estação de trabalho pode ser utilizada em vários ambientes, tais como escritórios, centros de comando (*Command Centers*), locais remotos ou mesmo locais secundários dentro das instalações de saúde. A estação de trabalho remota pode estar situada em qualquer espaço que ofereça ao usuário condições adequadas para concentração e conectividade mínima, bem como requisitos de configuração do computador.

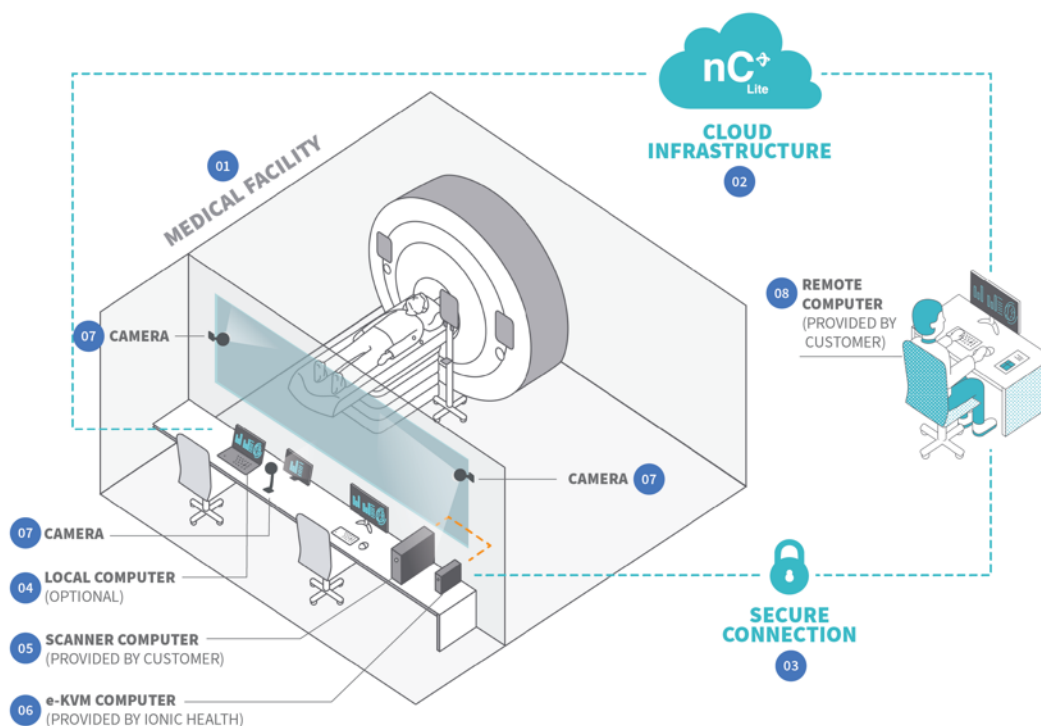


Figura 01: Visão geral do produto e das suas conexões através de uma conexão segura (por exemplo, VPN).

01 – Unidade médica; 02 – Infraestrutura em nuvem; 03 – Conexão segura; 04 – Computador local (opcional); 05 – Computador do equipamento médico (fornecido pelo cliente); 06 – e-KVM (fornecido pela IONIC Health); 07 – Câmera; 08 - Computador remoto (fornecido pelo cliente)

**AVISO!****Compatibilidade com varredura remota**

A IONIC Health (IH) valida a funcionalidade de digitalização remota nos dispositivos compatíveis listados. A IH realiza uma avaliação completa dos requisitos de digitalização remota da IH e testa o sistema no ambiente de destino durante a instalação. Isso garante compatibilidade e desempenho adequado naquele momento para a digitalização remota. Esta verificação não implica que todos os requisitos do dispositivo OEM (Original Equipment Manufacturer) sejam atendidos nesta configuração. Qualquer desvio dos requisitos OEM é responsabilidade do usuário final.

As modificações no sistema ou ambiente após a instalação devem ser comunicadas à IH para verificar a compatibilidade contínua. A IH não pode garantir o desempenho nem assumir responsabilidade por configurações diferentes das validadas durante a instalação.

1.3.11. Requisitos mínimos

- **Computador local**

Este computador é usado pelo **técnico local** para autorizar e possibilitar o acesso remoto do equipamento via nCommand Lite®. Também permite comunicação direta com o **técnico remoto** via recurso de chat na plataforma.

As especificações técnicas mínimas exigidas são:

- Processador: AMD® A4-9120C ou superior, ou similar
- Memória: 4GB ou mais
- Armazenamento: SSD de 128 GB ou superior
- Periféricos: microfone e alto-falante, ou headset e webcam
- Monitor: 14" FHD (1920 x 1080) ou superior
- Sistema operacional: Chrome OS, Windows OS ou MAC OS
- Local de instalação: este computador deve estar próximo ao computador do equipamento de imagem
- Rotina de TI: Criar atalho nCommand Lite na área de trabalho de cada usuário
- Compatibilidade do navegador: Google Chrome ou Microsoft Edge.

- **Estação de trabalho remota**

Essa estação é usada pelo **técnico remoto** para acessar e controlar o equipamento via nCommand Lite®. A estação de trabalho remota deve estabelecer uma ligação segura ao computador e-KVM (fornecido pela IONIC HEALTH®).

O cliente é responsável por fornecer o computador remoto e decidirá entre duas opções: a primeira é uma operação 24x7, e a segunda é uma operação em horário comercial.

A seguir, apresentamos as especificações adequadas para a escolha dos modelos de computador para cada cenário:

Cenário 1 (Operação 24x7) - Deve atender às seguintes especificações:

- Intel Xeon W-2223 (4 cores, 8 threads, 8,25 MB de cache, 3,90 GHz Turbo) ou superior.
- RAM: 16GB ou mais.
- Gráficos: NVIDIA RTX A2000 6GB ou superior, ou similar.
- Armazenamento: 128 GB SSD ou superior.
- Sistema operacional: Windows 11 Pro 64B ou superior.
- Requisitos mínimos para o monitor: Tamanho 27", Proporção 16:9, Resolução 4k.
- Fone de ouvido: BLACKWIRE 3200 ou similar.
- Compatibilidade do navegador: Google Chrome ou Microsoft Edge.

Cenário 2 (operação em horário comercial) - Deve atender às seguintes especificações:

- Intel® Core™ i7-12700k vPro® ou superior.
- RAM: 16GB ou mais.
- Gráficos: NVIDIA T400 GB ou superior, ou similar.
- Armazenamento: 128 GB SSD ou superior.
- Sistema operacional: Windows 11 Pro 64B ou superior.
- Requisitos mínimos para o monitor: Tamanho 27", Proporção 16:9, Resolução 4k.
- Fone de ouvido: BLACKWIRE 3200 ou similar.
- Compatibilidade do navegador: Google Chrome ou Microsoft Edge.



AVISO!

O não atendimento aos requisitos mínimos e à configuração adequada pode resultar em uma comunicação interrompida ou prejudicada entre os usuários.

● **Configurações de rede (requisitos mínimos)**

Para estabelecer a sessão entre o usuário remoto e o computador e-KVM, é necessário garantir a comunicação de rede entre os dois dispositivos. O sistema nCommand Lite utiliza peer-to-peer (P2P) para estabelecer a ligação entre o usuário local, o usuário remoto e o computador e-KVM. Existem três cenários compatíveis:

- **Scenario 1** – Rede corporativa que utiliza um dos seguintes protocolos: LAN, LAN-to-LAN, MPLS ou VPN;
- **Cenário 2** – Rede corporativa que utiliza WAN (rede externa) confiável e não utiliza nenhum dos seguintes protocolos: LAN, LAN-to-LAN, MPLS ou VPN;
- **Cenário 3** – Rede pública no lado do computador remoto (usuário remoto).

As configurações de cada cenário estão detalhadas na documentação técnica.

1.3.12. Símbolos

Símbolo	Descrição	Referência
	Fabricante	ISO 15223-1, ISO 7000-3082
	Data de fabricação	ISO 15223-1, ISO 7000-2497

	Este símbolo indica que o produto é um dispositivo médico	ISO 15223-1
	Identificador Único de Dispositivo	ISO 15223-1
	Referência do modelo	ISO 15223-1, ISO 7000-2493
	Importador	ISO 15223-1, ISO 7000-3725
	Consulte o Manual do Usuário	ISO 15223-1, ISO 7000-1641
	Distribuidor	ISO 15223-1, ISO 7000-3724
	Atenção	ISO 15223-1, ISO 7000-0434A
	Aviso	ISO 7010-W001
	Número de série <i>(ou versão do software)</i>	ISO 15223-1, ISO 7000-2498
	Representante Autorizado na Comunidade Europeia	ISO 15223-1
	Representante autorizado suíço (CH-REP)	ISO 15223-1
	CE - Marcação de Conformidade Europeia; 2803 – Designação de Corpo Notificado	Regulamento da UE 2017/745

1.3.13. Vida útil

A vida útil esperada do produto é de 5 anos, considerando a vida útil dos componentes. Essa avaliação abrangente garante que a vida útil de cada componente crítico esteja alinhada com a vida útil geral, garantindo desempenho e confiabilidade consistentes durante toda a duração prevista do produto.

1.3.14. Atualizações/melhorias (Upgrades)

A IONIC Health atualizará o sistema nCommand Lite como parte da manutenção programada ou das versões de atualização. Essas atualizações foram projetadas para garantir desempenho e confiabilidade contínuos sem interromper a versão atualmente implementada nas instalações do cliente. Dependendo do tipo de atualização, o produto poderá ser atualizado remotamente ou poderá exigir a visita presencial de um engenheiro de campo.

Capítulo 2 Lista de Avisos e Precauções Gerais



AVISO!

Leia todos os avisos abaixo antes de utilizar o sistema nCommand Lite.



ATENÇÃO

O sistema nCommand Lite não pode passar por reparos ou manutenção enquanto estiver sendo utilizado para controlar um equipamento de RM, TC ou PET-CT na presença de um paciente.

- Preste muita atenção a todos os alertas do sistema, pois eles são cruciais para operações seguras.
- Priorize a segurança e a atenção durante todas as operações.
- A lei federal restringe a venda deste dispositivo a um médico ou por ordem deste, conforme usado por técnicos médicos habilitados no estado em que ele pratica.
- O sistema nCommand Lite deve ser utilizado apenas por técnicos que tenham recebido treinamento no uso da plataforma.
- Use esse sistema somente com navegadores da Web compatíveis. Os navegadores compatíveis são o Google Chrome e o Microsoft Edge.
- Em caso de contingência, um técnico treinado e habilitado deve permanecer na unidade médica para realizar a operação de RM, TC ou PET/CT sem o nCommand Lite.
- O acesso a vários equipamentos simultaneamente exige foco intenso e comunicação com as equipes locais.
- Evite acessar equipamentos com layouts idênticos ou exames da mesma região anatômica simultaneamente.
- É possível visualizar várias telas, mas o controle é limitado a um equipamento de cada vez.
- Sempre inicie o chat quando estiver conectado a um equipamento para uma comunicação mais clara.
- Os alertas de chamada aparecem na tela do equipamento associado; apenas uma chamada pode estar ativa por vez.
- Teste a comunicação por vídeo ao acessar à aplicação (antes do início de uma sessão de trabalho) para verificar se há alguma falha na conexão de saída de vídeo dos equipamentos de RM, TC ou PET/CT, ou de qualquer equipamento relacionado a transmissão de vídeo.
- O dispositivo não deve ser conectado à tomada e/ou a uma fonte de alimentação ininterrupta e estabilizada por meio de extensões ou régua de energia.
- Se ocorrerem falhas de vídeo, verifique a ligação de vídeo entre o sistema do equipamento e o computador e-KVM.
- Se o acesso remoto da aplicação estiver lento, atualize a página com os comandos Ctrl+F5 no navegador do computador do técnico remoto. Se o problema persistir, contate o suporte técnico.
- Sempre que a página do navegador for atualizada, a conexão ao equipamento é interrompida, exigindo que o processo de aprovação seja realizado novamente.
- Não inicie sessão utilizando um navegador diferente quando já estiver com a sessão iniciada.
- A unidade médica deve ter uma conexão de internet redundante com um fornecedor diferente do principal, para que seja possível fazer uma mudança imediata em caso de perda de comunicação do sistema/plataforma.

- Em caso de perda de comunicação ou lentidão do mouse, execute a “ressincronização do mouse” na página utilizada no navegador.
- Certifique-se de que os computadores utilizados para o controle do sistema nCommand Lite, tanto na unidade médica quanto na estação remota, atendam aos requisitos mínimos; caso contrário, poderá haver perda de desempenho da aplicação.
- A QoS (Qualidade de Serviço) deve ser aplicada ao link principal e ao link redundante para transmissão da plataforma, e o desempenho do link deve ser monitorizado.
- Antes de usar, verifique os níveis de volume do áudio e do microfone, bem como as permissões de áudio e microfone no navegador da web.
- Antes de usar, verifique o funcionamento do teclado e do mouse; se eles estiverem lentos ou fora de sincronia, ative o botão “mouse resync”. Verifique se o computador e-KVM está conectado e ligado.
- Certifique-se de que o layout do teclado na estação remota seja idêntico ao layout do teclado na unidade.
- Se for necessário mudar o local onde a plataforma é usada, o cliente deve ligar para o suporte técnico para fazer uma nova instalação. Não reinstale sem entrar em contato com o suporte técnico.
- Antes de iniciar o processo de acesso remoto ao aparelho de RM, TC ou PET/CT, é importante que as equipes de técnicos verifiquem todos os itens necessários para o bom desempenho da plataforma, de modo a não prejudicar o exame. Esses itens estão listados no documento “Lista de Verificação de Início de Utilização”.
- A configuração do firewall da unidade médica deve ser verificada mensalmente com a equipe de TI, confirmando que não há problemas com a liberação do firewall que possam comprometer o uso do nCommand Lite.
- Qualquer anomalia observada no uso da aplicação deve ser imediatamente notificada à equipe de suporte antes de iniciar o acesso ou abortá-lo, caso já tenha sido iniciado.
- Somente técnicos habilitados e treinados no uso do nCommand Lite devem utilizar o sistema.
- O acesso remoto por meio da plataforma não substitui nem compete com qualquer outro procedimento operacional de RM, TC ou PET/CT estabelecido pelo fabricante do equipamento médico e/ou pelos protocolos e procedimentos da unidade médica.
- Evite dobrar ou esticar os cabos do hardware.
- Se ocorrerem problemas com a comunicação por voz ou chat, faça uma chamada telefônica para estabelecer comunicação entre o técnico local na unidade médica e o técnico remoto. Siga as instruções descritas na seção “Orientações em caso de falha” e, se necessário, entre em contato com o suporte técnico para realizar o reparo.
- Se for necessário substituir um computador ou qualquer outro equipamento que influencie diretamente a instalação do nCommand Lite, acione o suporte técnico, garantindo a preservação da operação do sistema.
- Apenas uma pessoa por vez pode acessar remotamente o equipamento de RM, TC ou PET/CT.
- Não toque em nenhum cabo de vídeo físico enquanto o computador do equipamento e o sistema nCommand Lite estiverem ligados.
- Ao acessar um equipamento adicional, uma nova guia será aberta. Arraste essa guia para um segundo monitor, pois o sistema foi projetado para ser usado com uma tela separada para cada equipamento.
- Qualquer incidente grave relacionado ao uso deste dispositivo deve ser relatado ao fabricante e à autoridade de saúde/autoridade competente onde o dispositivo está instalado (*consulte mais detalhes no capítulo Canais de Atendimento*).

Capítulo 3 Utilização da plataforma em cada localidade

Sessão 3.1 - Acesso e uso do nCommand Lite

**AVISO!**

Em caso de problemas, entre em contato com o suporte técnico para obter assistência.

**AVISO!**

Verifique o layout do teclado e certifique-se de que ele seja idêntico em ambos os locais (unidade médica e estação remota). Layouts de teclado diferentes podem prejudicar a experiência do usuário.

Este capítulo fornece tudo o que você precisa saber para acessar e começar a usar a plataforma nCommand Lite. Você encontrará instruções simples e passo a passo para fazer login, navegar pela interface e entender os principais recursos. Este guia o ajudará a começar a trabalhar no local ou remotamente, com rapidez e confiança.

Alteração do idioma - O sistema é predefinido para o inglês por padrão, mas o idioma pode ser alterado facilmente de acordo com sua preferência. Na tela de login, clique no canto superior direito, onde é exibido “English (en-US)”. Isso abrirá uma lista suspensa de idiomas disponíveis para selecionar.

Após fazer o login, também é possível alterar o idioma clicando no idioma selecionado no momento, no lado direito da barra superior. Isso abrirá uma lista suspensa de idiomas disponíveis para escolher.

Observe que, se o idioma for alterado enquanto estiver conectado a um equipamento, a conexão atual será automaticamente encerrada e você precisará se reconectar.

Ao acessar a plataforma, é possível escolher o idioma de sua preferência na tela de login. No entanto, algumas mensagens exibidas durante o processo de login podem aparecer no idioma definido em seu navegador da Web, independentemente do idioma selecionado na plataforma. Para uma experiência consistente, recomendamos alinhar as configurações de idioma do navegador com o idioma preferido da plataforma.

Sessão 3.2 - Primeiro acesso à plataforma

O processo de login na plataforma pode ocorrer de duas maneiras: por meio do nCommand Lite ou de um provedor de identidade externo (External IdP). O usuário pode fazer login usando um dos métodos pré-configurados. Se o método configurado for o Provedor de Identidade Externo (IdP Externo), o método nCommand Lite não funcionará, e vice-versa. Para fazer login via External IdP, vá diretamente para **sub-item 3.2.2**.

3.2.1. Login via nCommand Lite

Nota: Esta seção não se aplica a usuários que fazem login por meio de um provedor de identidade externo (External IdP).

Ligue o computador e clique duas vezes no ícone de atalho do nCommand Lite, que geralmente se encontra na área de trabalho. Você também pode acessar o URL diretamente no navegador.

O primeiro acesso é uma etapa crucial para começar a usar a plataforma com segurança e eficiência. Veja os principais pontos a serem considerados:

1 - E-mail de boas-vindas: Você receberá um e-mail com seus dados para login, incluindo seu e-mail pessoal associado, uma senha temporária e um link direto para a plataforma. Este e-mail é fundamental para iniciar sua jornada no nCommand Lite.

2 - Criação de senha: Ao acessar o link, você precisará inserir seu e-mail associado e a senha recebida no e-mail de boas-vindas. Ao clicar em “Sign in” (Entrar), você será direcionado a uma página para criar uma nova senha. Você precisa inserir a senha antiga, a nova senha e a confirmação da nova senha. Ela deve ser forte e seguro, incluindo pelo menos 3 itens dos seguintes: uma letra minúscula, uma letra maiúscula, um número e um símbolo, e ter pelo menos 8 caracteres. Ao clicar em “Continue”, você será redirecionado para uma página para confirmar seu e-mail novamente. Ao clicar em “Continue”, você será redirecionado para a tela inicial, que é personalizada de acordo com o seu perfil de usuário específico.

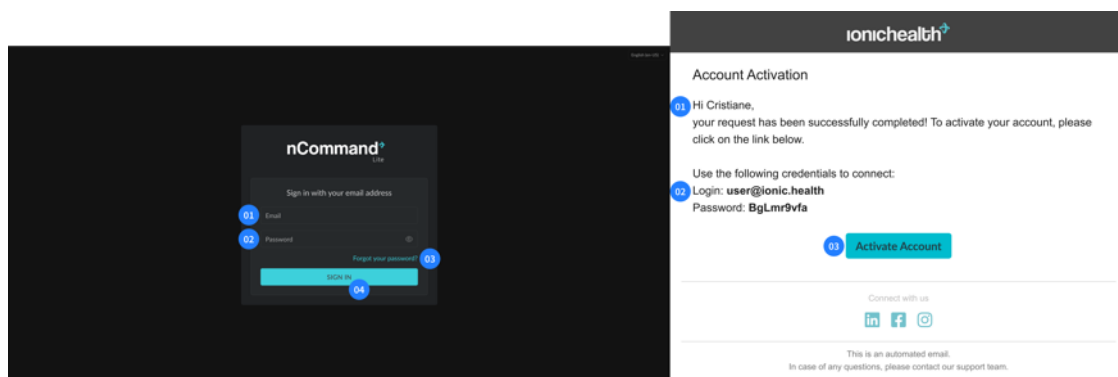


Figura 02: Primeiro acesso

Esquerda - Página de login: 01 – E-mail; 02 – Senha; 03 – “Forgot your password?” (Esqueceu sua senha?); 04 – Botão Sign In (Entrar)

Direita - Email de boas-vindas: 01 – Texto do e-mail de ativação de conta; 02 – Credenciais de login; 03 – Botão Ativar Conta

Esse procedimento inicial foi desenvolvido para garantir a máxima segurança para sua conta desde o início. A partir do seu segundo acesso, o processo será simplificado, mas igualmente seguro, com um código de autenticação de dois fatores enviado ao seu e-mail associado a cada login para garantir a segurança contínua da sua conta.

Depois de fazer login no nCommand Lite, o sistema o direcionará automaticamente para a tela inicial, que é personalizada de acordo com o seu perfil de usuário específico. Seja para um técnico local ou o técnico remoto, a interface foi projetada para atender às necessidades e aos níveis de acesso relevantes de cada função. Esse design intuitivo garante que você tenha todas

as ferramentas e informações necessárias para uma experiência de usuário eficaz e eficiente desde o momento do login.

Nota: Quando o método de login é configurado como nCommand Lite, o login sempre deve ser feito por meio dessa opção. Mesmo que um botão IdP externo apareça na tela de login, ele não funcionará para esses usuários. Cada conta de usuário é registrada na plataforma com um método de autenticação específico: credenciais do nCommand Lite ou um serviço de IdP externo. Se um usuário tentar fazer login usando um método de autenticação diferente daquele atribuído à sua conta, o sistema exibirá uma mensagem de erro informando que a conta não está autorizada para esse tipo de autenticação.

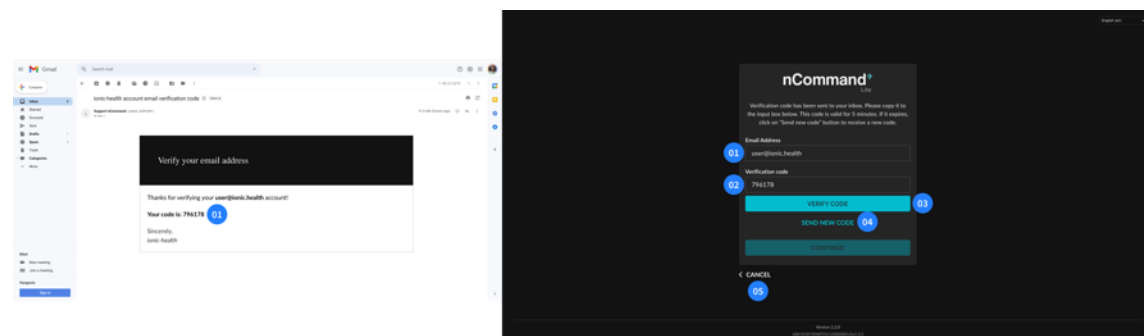


Figura 03: Autenticação de dois fatores (2-FA)

Esquerda – E-mail: 01 – 2-FA Código

Direita - Página de autenticação de dois fatores: 01 – E-mail; 02 – Código de verificação; 03 – Código de verificação botão confirmar; 04 – Enviar novo código; 05 – Cancelar

3.2.2. Login via IdP Externo

Em alguns casos, os usuários podem fazer login na plataforma por meio de um IdP (External Identity Provider, provedor de identidade externo), o que lhes permite usar o serviço de autenticação existente da organização, um mecanismo também conhecido como SSO (Single Sign On, logon único). Por esse método, o usuário pré-registrado não receberá um e-mail de boas-vindas. O serviço de TI local deve verificar a compatibilidade, configurar o método e informar ao usuário qual e-mail (IdP externo) deve ser usado.

Quando essa opção está disponível, o usuário deve sempre fazer login usando o IdP externo (por exemplo, Amazon Cognito, Microsoft Entra ID, Microsoft AD B2C). O método de login via nCommand Lite não estará disponível para usuários de IdP Externo.

Para fazer login usando o IdP Externo, clique no botão com o nome do IdP e siga as instruções fornecidas pelo autenticador externo. Se a sua instituição utilizar mais de um IdP externo integrado, certifique-se e confirme em qual provedor você está registrado. Outros provedores não funcionarão. Em caso de dúvidas ou dificuldades, entre em contato com o serviço de TI local.

Em cenários em que os usuários compartilham a mesma máquina e usam Single Sign-On (SSO), recomenda-se que cada usuário selecione a opção “não permanecer conectado” durante o login do IdP externo (se disponível) ou saia do provedor externo após sair do nCommand Lite.

Para essa opção de login, o processo completo de login e logout, incluindo políticas de criação e expiração de senhas, autenticação multifator (MFA) e bloqueios de contas, é gerenciado inteiramente pela equipe de TI do cliente que configurou o IdP externo.

Ao fazer login via IdP Externo, as funções “Forgot Password” (Esqueci a senha) e “Change Password” (Alterar senha) devem ser executadas de acordo com o processo do IdP externo.

Nota: A opção “Forgot Password” (Esqueci a senha) ainda aparecerá na tela de login, mas não funcionará para esses usuários. Essa opção pode direcionar o usuário para as próximas etapas do processo, mas não o concluirá. Para recuperar a senha, siga as instruções do IDP externo.

Importante: Mesmo ao usar um IdP Externo, o usuário deve estar pré-cadastrado na plataforma nCommand Lite para obter acesso.

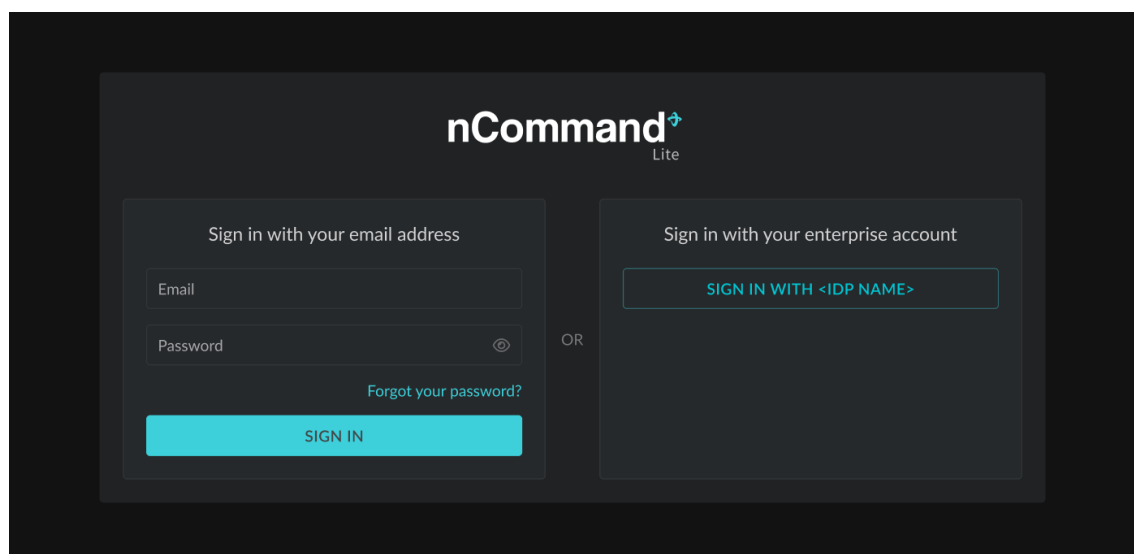


Figura 04: Tela de login via IdP Externo (Exemplo)

Sessão 3.3 - Gerenciamento de senhas

Após acessar a plataforma pela primeira vez, os usuários podem alterar sua senha ou, se esquecer a mesma, definir uma nova senha.

Nota: Ao fazer login via IdP Externo, as funções “Forgot Password” (Esqueci a senha) e “Change Password” (Alterar senha) devem ser executadas de acordo com o processo do IdP externo.

- **Recuperar senha:** Permite que os usuários recuperem o acesso à conta em caso de esquecimento da senha. Basta clicar no link “Forgot your password?” (Esqueceu sua senha?) na página de login, digitar o e-mail associado e enviar as informações. O sistema enviará um e-mail contendo um código de verificação. Ao preencher o código e clicar em “Verify code” (Verificar código), os usuários serão solicitados a confirmar o e-mail associado. Ao clicar em “Continue” (Continuar), os usuários são direcionados a uma página na qual podem inserir uma

nova senha e confirma-la. Se a nova senha atender aos requisitos do sistema, os usuários poderão registrá-la com sucesso e, posteriormente, fazer login com as credenciais atualizadas.

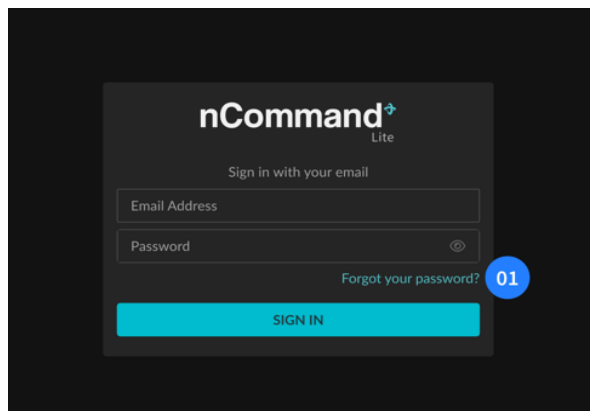


Figura 05: Link para a página de redefinição de senha
01 – Esqueceu sua senha?

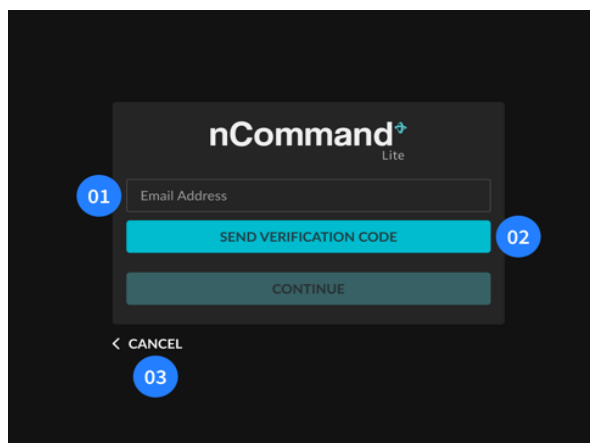


Figura 06: Página de redefinição de senha
01 – E-mail; 02 – Enviar código de verificação; 03 – Cancelar

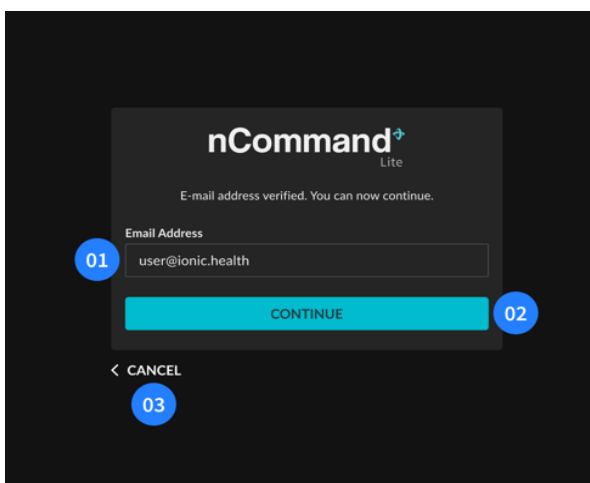
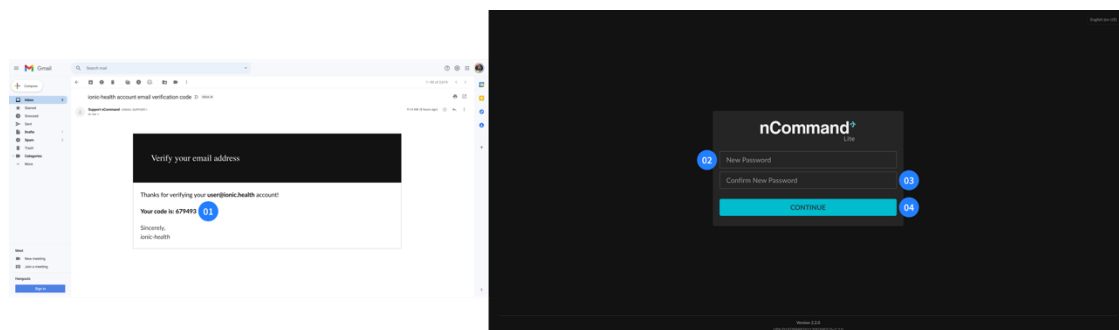
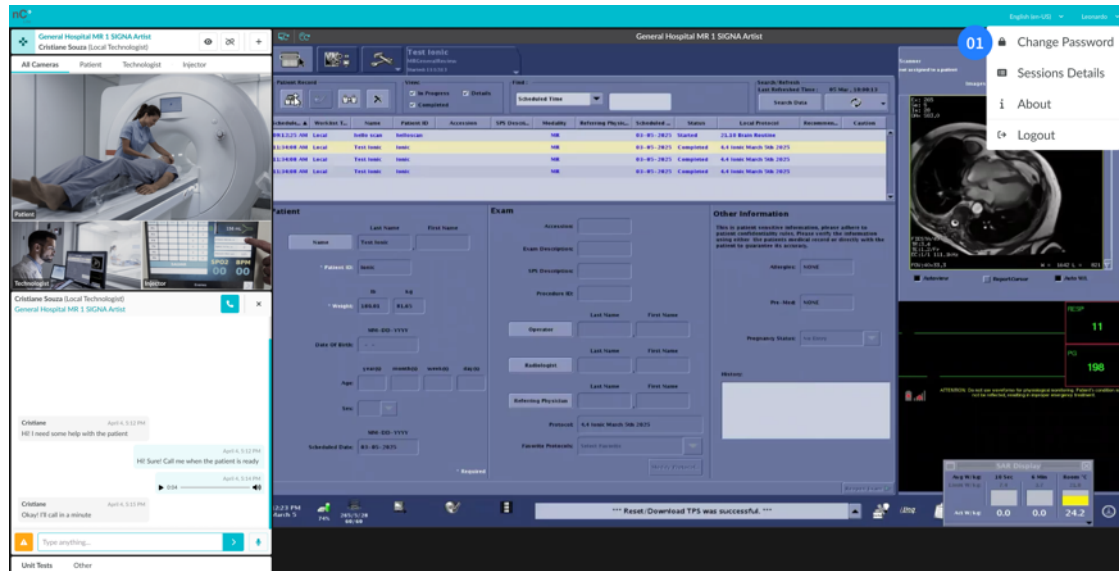


Figura 07: Confirmação por e-mail
01 – E-mail; 02 – Botão continuar; 03 – Cancelar



**Figura 08: E-mail com código para cadastrar nova senha (esquerda) - 01 – 2-Código de FA
Página Alterar senha (direita) - 02 – Nova senha; 03 – Confirmar nova senha; 04 – Botão Continuar**

- Alterar senha:** Permite que os usuários atualizem suas senhas obedecendo a critérios específicos, incluindo pelo menos 3 itens dos seguintes: uma letra minúscula, uma letra maiúscula, um número e um símbolo, e ter pelo menos 8 caracteres. O sistema verifica se a nova senha atende a esses critérios e avisa o usuário com uma mensagem caso contrário. Além disso, os usuários precisam confirmar a nova senha para evitar erros de entrada. Para alterar a senha, o usuário, após o processo de login, precisa clicar no ícone do canto superior direito e escolher o menu “Change Password” (Alterar senha). Ele(a) será desconectado(a) da plataforma e direcionado(a) a uma página para confirmar o e-mail associado. O sistema enviará um e-mail contendo um código de verificação. Ao preencher o código e clicar em “Verify code” (Verificar código), os usuários são redirecionados para uma tela onde podem inserir uma nova senha.



**Figura 09: Item do menu de alteração de senha
01 – Alterar senha**

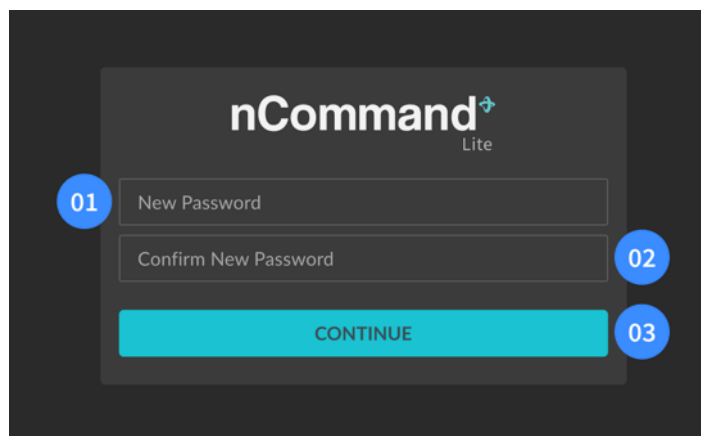


Figura 10: Página de alteração de senha
01 – Nova senha; 02 – Confirmar nova senha; 03 – Botão continuar

Sessão 3.4 - Acesso com perfil de técnico local



AVISO!

Antes de usar a plataforma, entre em contato com o técnico remoto por telefone.



AVISO!

Para evitar o superaquecimento, não coloque nenhum objeto na frente do resfriador de ar do computador e-KVM e, para evitar danos, não coloque nenhum objeto em cima dele.



AVISO!

Durante as sessões remotas, o técnico local é responsável por gerenciar e aplicar as regras de segurança locais para cada tipo de exame e seus requisitos específicos. Permaneça sempre presente na sala de controle e/ou na sala de exames para garantir a segurança do paciente e dos profissionais envolvidos.



AVISO!

Os movimentos da mesa durante a sessão só devem ser realizados pelo técnico local quando solicitados pelo sistema. Antes de sair da sala de operação, o técnico local deve sempre revogar o acesso do técnico remoto.



AVISO!

Somente o técnico local tem permissão para mover a mesa para posicionar o paciente dentro do equipamento e liberá-lo com segurança. Antes de sair da sala de operação, o técnico local deve sempre revogar o acesso do usuário remoto.

Depois de fazer login na plataforma, selecione o equipamento desejado na caixa Device Selection (Seleção de Equipamento). Você será responsável por esse equipamento, portanto, poderá analisar a solicitação do técnico remoto para acessar o equipamento. Quando um técnico remoto quiser acessar o equipamento, uma janela pop-up será exibida, permitindo que analise todas as informações apresentadas antes de conceder ou negar o acesso. Fique atento a uma solicitação enviada por um técnico remoto. É extremamente importante verificar cada

detalhe com muita atenção. Nos casos em que as informações fornecidas não forem reconhecidas, não conceda acesso.

O técnico remoto pode acessar o equipamento usando um dos dois modos de acesso: **Controle** ou **Visualização**:

- **Modo de Controle** - permite que o técnico remoto controle o mouse e o teclado, além de visualizar a tela do equipamento. No entanto, o técnico local não perde o controle do mouse e teclado locais e pode assumir o controle a qualquer momento.
- **Modo Visualização** - permite que o técnico remoto visualize apenas a tela do equipamento e use o chat para comunicação

Após selecionar o equipamento, o usuário tem acesso à função de chat, permitindo a comunicação por meio de texto, mensagens de áudio, voz e chamada de vídeo com outros usuários.



Figura 11: Tela principal do técnico local com Notificação de Solicitação de Acesso
01 – Título (Solicitação de Acesso); **02** - Nome e Função do Solicitante e Descrição do Tipo de Acesso;
03 – Prompt: “Você aprova este pedido?”; **04** – Botão Rejeitar; **05** – Botão Aprovar

Após a aprovação, o técnico local pode revogar o acesso do técnico remoto a qualquer momento, bastando clicar no botão REVOKE (Revogar).

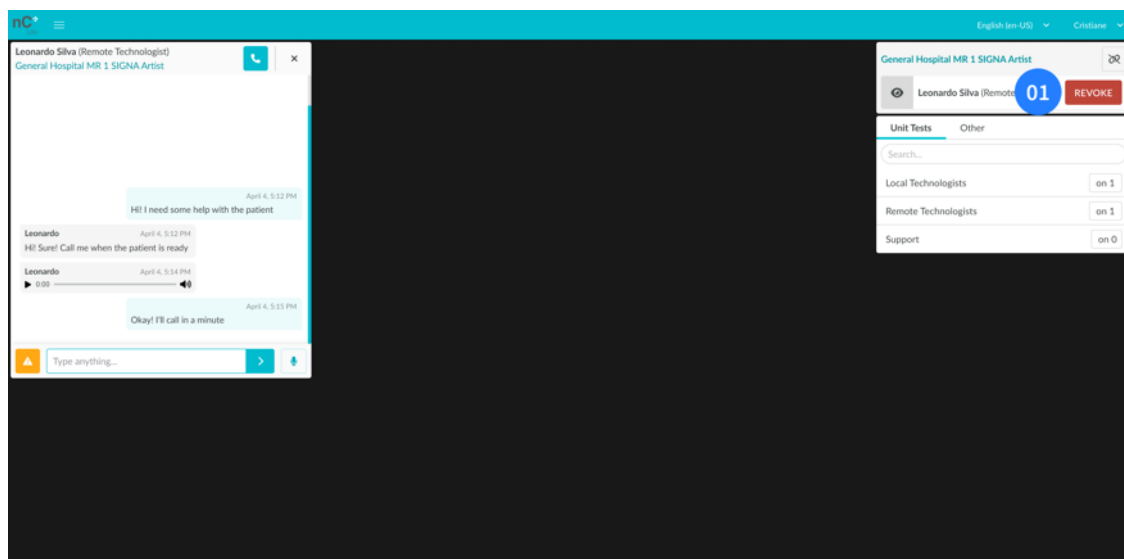


Figura 12: Tela principal do técnico local quando conectado a um dispositivo
01 – Botão Revogar

Durante a sessão remota, o técnico remoto pode solicitar uma alteração do modo de acesso. Um pop-up de solicitação será exibido na tela. Você pode aprovar ou rejeitar o pop-up. Esteja ciente das prerrogativas que cada modo de acesso permite ao técnico remoto.

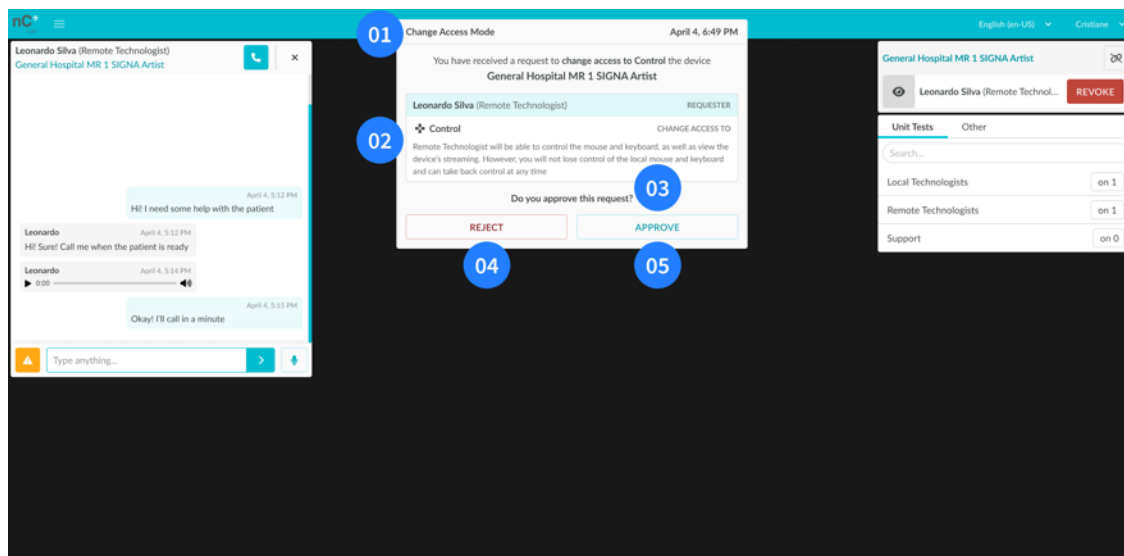


Figura 13: Tela principal do técnico local com Solicitação para Alterar o Modo de Acesso
01 – Título (Alterar o Modo de Acesso); 02 - Nome e Função do Solicitante e Descrição do Tipo de Acesso;
03 – Prompt: “Você aprova esta solicitação?”; 04 – Botão Rejeitar; 05 – Botão Aprovar

**AVISO!**

Em caso de perda de conexão no computador local, o técnico remoto ainda tem acesso ao equipamento. Entre em contato **imediatamente** com o técnico remoto e peça para ele(a) se **desconectar** OU faça login em outro computador e **revogue o acesso** do técnico remoto OU **pressione o botão de energia** para desligar o computador e-KVM.

**AVISO!****Em caso de Manutenção do Scanner:**

Antes de o Engenheiro de Campo iniciar qualquer procedimento (no equipamento ou na sala de controle), informe o técnico remoto e revogue o acesso clicando no botão “REVOKE ACCESS” (Revogar acesso). Em seguida, faça logoff da plataforma nCommand Lite.

Se nenhum técnico remoto estiver conectado, faça logoff da plataforma nCommand Lite antes de iniciar a manutenção.

Sessão 3.5 - Acesso com perfil de técnico remoto

**AVISO!**

Usuário do computador do equipamento e senha de root: ambos devem ser mantidos pelo host no local que receberá a equipe de instalação.

**AVISO!**

Os movimentos da mesa durante a sessão só devem ser realizados pelo técnico local quando solicitados pelo sistema. Antes de sair da sala de operação, o técnico local deve sempre revogar o acesso do técnico remoto.

**AVISO!**

Somente o técnico local tem permissão para mover a mesa para posicionar o paciente dentro do equipamento e liberá-lo com segurança. Antes de sair da sala de operação, o técnico local deve sempre revogar o acesso do usuário remoto.

**AVISO!**

Esteja sempre atento à sala por meio da câmera de vídeo e comunique-se com o técnico local antes de realizar qualquer atividade.

**AVISO!**

Em caso de perda de conexão no computador local, entre em contato com o técnico local imediatamente e desconecte-o.

**AVISO!****Em caso de Manutenção do Scanner:**

Depois de ser notificado sobre o início da manutenção do equipamento, certifique-se de que o acesso tenha sido revogado pelo técnico local e faça logoff da plataforma nCommand Lite.

Se o acesso não tiver sido revogado, faça logoff da plataforma nCommand Lite e entre imediatamente em contato com o técnico local para notificá-lo.

**AVISO!**

Para controlar o mouse e o teclado remotamente, o modo de acesso selecionado deve ser Control (Controle); no modo View (Visualização), o técnico remoto só pode visualizar as câmeras locais e de streaming.

**AVISO!**

Se a resposta à sua solicitação demorar mais do que o esperado, entre em contato com o técnico local por chat ou telefone.

O local de trabalho do técnico remoto inclui equipamentos como um computador, monitores (geralmente três), um mouse, um teclado e um fone de ouvido.

No fluxo de trabalho clínico, *técnicos locais* têm contato direto com o paciente. Eles são responsáveis pela interação com o paciente, pelo posicionamento e por garantir a segurança e a conformidade com o protocolo durante os procedimentos de RM, TC ou PET/CT, de acordo com as normas institucionais e regulatórios.

3.5.1. Modo de Acesso

Depois de fazer login na plataforma, selecione o equipamento ao qual deseja se conectar na Caixa de Seleção de Equipamentos. Uma janela pop-up será aberta para escolher o modo de acesso entre **Controle** e **Visualização**:

- **Modo de Controle** – Nesse modo, o controle do mouse e do teclado é ativado, além da visualização da tela. Os profissionais locais mantêm acesso total ao mouse e ao teclado locais e podem retomar o controle a qualquer momento.
- **Modo Visualização** – Só é possível visualizar a tela do equipamento e usar o chat para comunicação.

Ao selecionar o modo de acesso, uma caixa de “Waiting for approval” (Aguardando aprovação) será exibida, indicando que a aprovação do técnico local conectado é necessária para prosseguir. Esse técnico local tem total autoridade para aprovar ou rejeitar o acesso e revogar o acesso a qualquer momento, se for considerado necessário. Essa medida é essencial para garantir um controle rigoroso e manter a segurança ao usar o equipamento.

Após selecionar o equipamento, o usuário tem acesso à função de chat, permitindo a comunicação por meio de texto, mensagens de áudio, voz e chamada de vídeo com outros usuários. O usuário não precisa ser aprovado para acessar o chat.

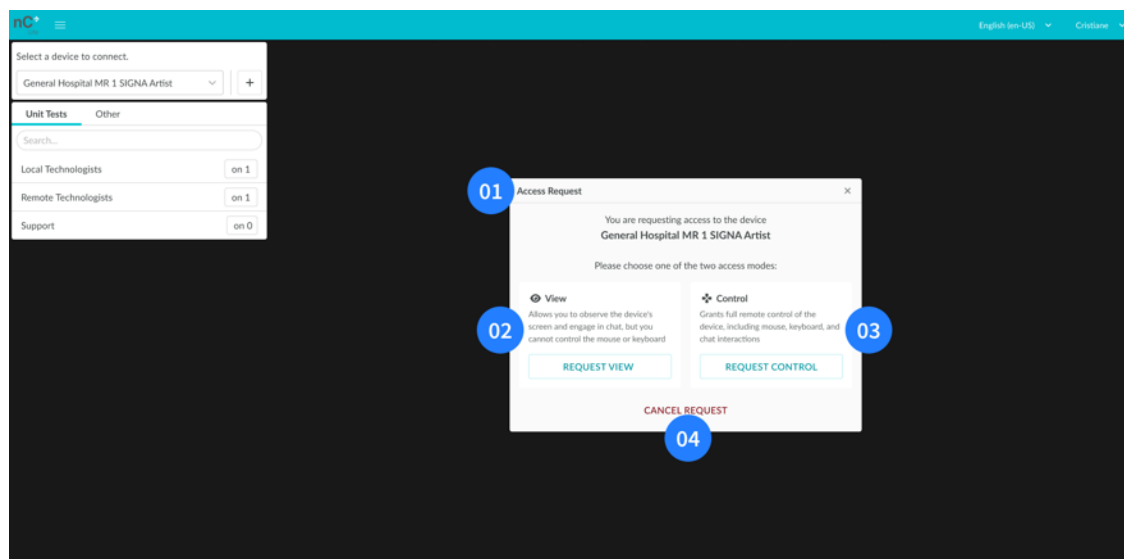


Figura 14: Diálogo de Solicitação de Acesso para técnico remoto

01 – Título (Solicitação de Acesso); **02** - Descrição do Modo de Visualização e botão Solicitar Visualização; **03** – Descrição do Modo de Controle e botão Solicitar Controle; **04** – Cancelar Solicitação

Depois que o acesso ao equipamento for autorizado pelo técnico local, a interface do técnico remoto será atualizada para a exibição ao vivo do equipamento e suas câmeras associadas. Se o modo de acesso escolhido for Controle, o recurso de operação remota do equipamento será ativado.

Esse processo garante uma interação eficaz e segura, permitindo o uso remoto seguro do equipamento sem comprometer sua integridade ou a segurança do paciente.

Para solicitar uma alteração no modo de acesso durante uma sessão remota, clique no ícone correspondente. O técnico local pode aceitar ou rejeitar a solicitação:

- **Aceitar** – o streaming vai recarregar, mas o conteúdo do chat não será perdido. Se você estiver em uma chamada de Voz e Vídeo, ela será encerrada e precisará ser reiniciada por um dos usuários.
- **Recusar** - um popup aparecerá notificando sobre a rejeição do técnico local e o acesso atual permanecerá ativo

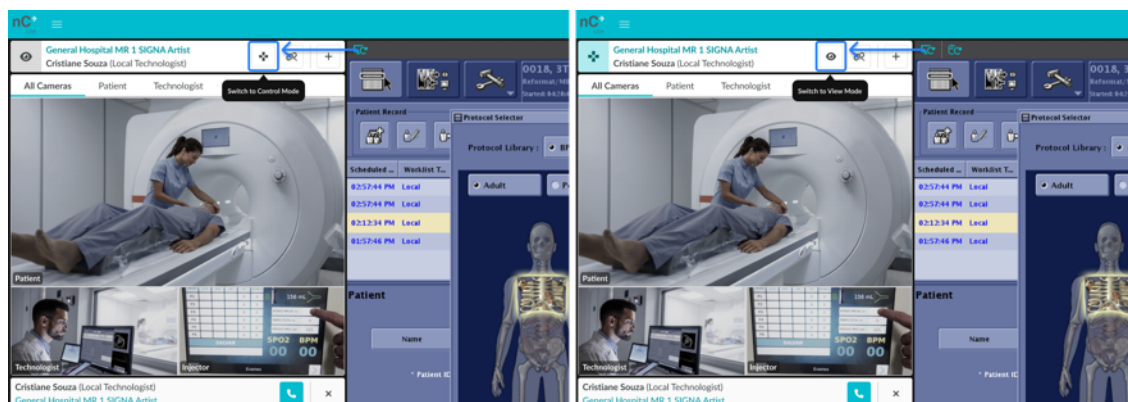


Figura 15: Alterar Modo de Acesso

Esquerda - Alternar para o Ícone e Dica do Modo de Controle / **Direita** - Alternar para o Ícone e Dica do Modo de Visualização

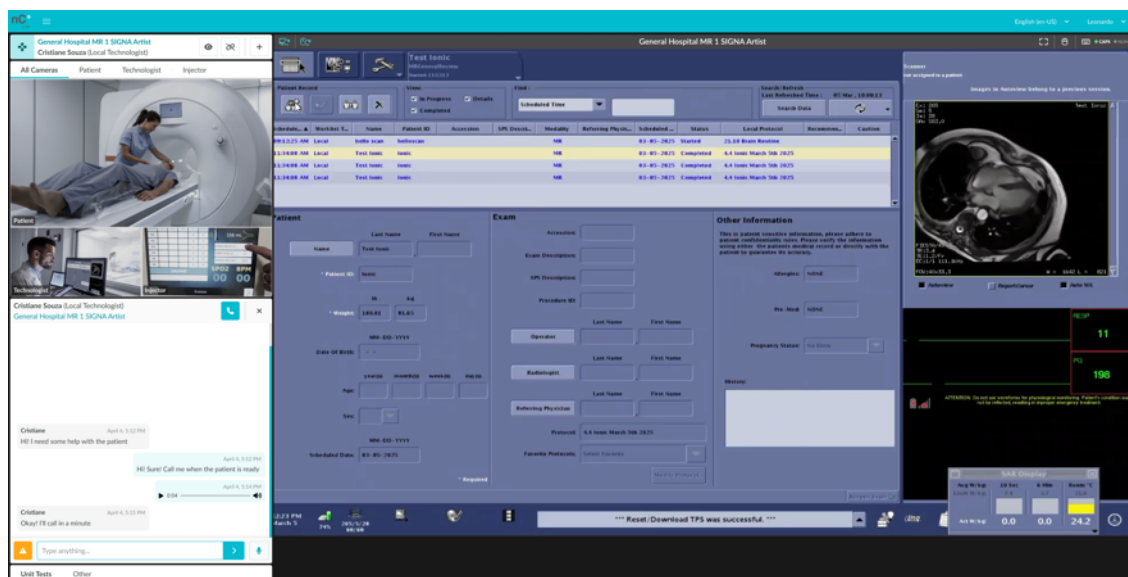


Figura 16: Tela principal do técnico remoto quando conectado a um equipamento

Quando o técnico remoto solicita acesso e não há um técnico local conectado ao equipamento, a plataforma exibe um aviso pop-up. Assim que o técnico local se conecta, a plataforma informa ao técnico remoto que ele pode solicitar acesso novamente.

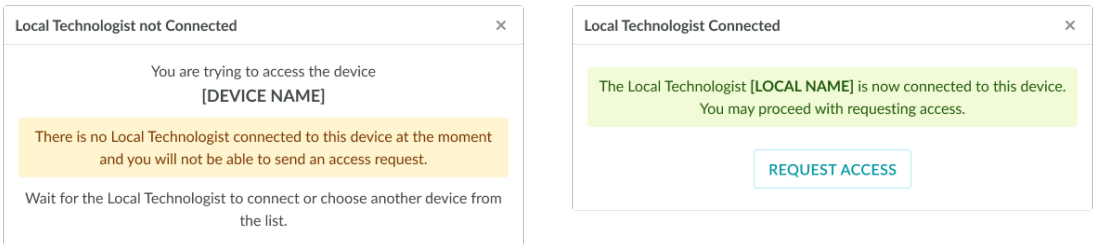


Figura 17: Alertas do técnico remoto sobre o status de conexão do técnico local
Esquerda - Notificação indicando que foi feita uma tentativa de acessar o equipamento, mas nenhum técnico local está conectado no momento.
Direita - Notificação confirmando que o técnico local se conectou ao equipamento.

3.5.2. Barra de Streaming

A Barra de Streaming exibe as principais informações e controles relacionados à sessão de streaming do equipamento. Ele inclui os botões “Reload Streaming” (Recarregar streaming) e “Mouse Resync” (Sincronizar mouse), o nome do equipamento, a resolução da tela e o status atual do mouse e do teclado do computador remoto.

1 - Recarregar Streaming

Esse recurso permite que os técnicos remotos recuperem o acesso aos equipamentos em caso de falha de conexão ou lentidão no desempenho. Se ocorrer algum tipo de desconexão ou atraso de tela no computador do equipamento, clique no ícone “Reload Streaming” (Recarregar streaming) localizado na barra de streaming. Isso fará com que a plataforma se reconecte ao computador do equipamento e recarregue as câmeras do sistema também.

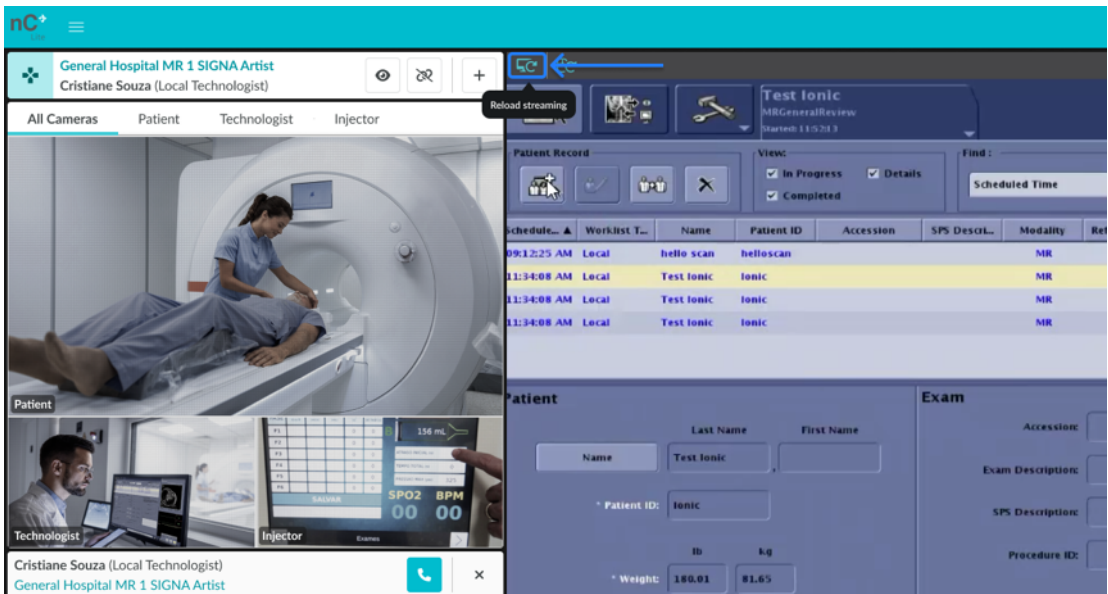


Figura 18: Botão de Recarregar Streaming

2 - Ressincronização do Mouse

Em caso de lentidão ou desalinhamento do mouse, clique no botão “Mouse Resync” (Ressincronizar mouse) localizado na barra acima da janela de streaming para sincronizar novamente o mouse do equipamento com o computador e-KVM.

Uma alternativa é mover o ponteiro do mouse para fora da área de streaming e, em seguida, trazê-lo de volta. O sistema ressincronizará automaticamente o mouse sem a necessidade de nenhuma ação adicional. Também é possível clicar e soltar o botão da roda de rolagem do mouse (quando disponível) para acionar a ressincronização automaticamente. No entanto, este método pode não funcionar em equipamentos com duas ou mais telas se os ponteiros do mouse local e remoto estiverem em telas diferentes.

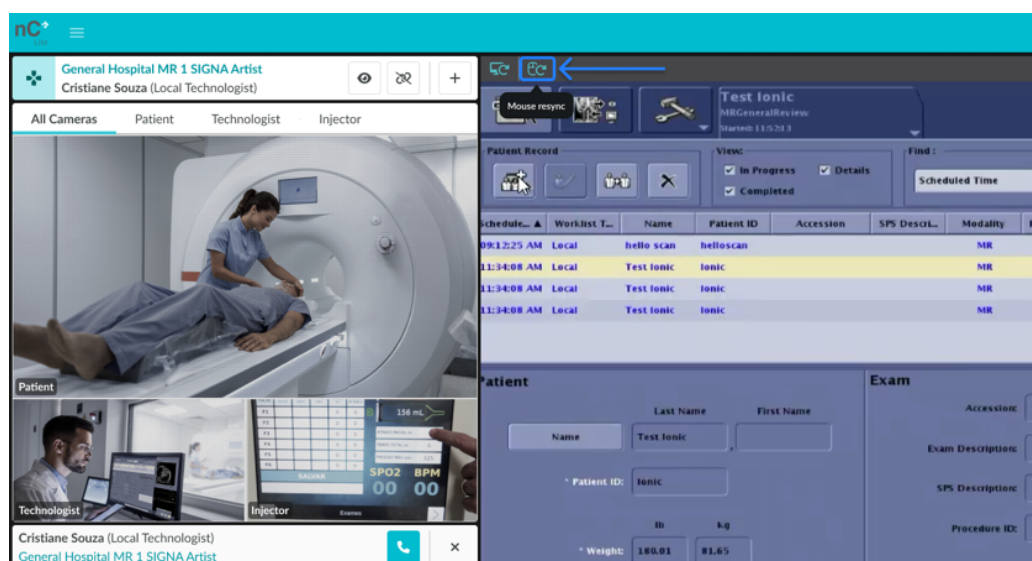


Figura 19: Botão de Ressincronização do Mouse

3 - Resolução do streaming

Esta funcionalidade fornece ao técnico remoto informações sobre a resolução original do streaming (do equipamento) e a resolução atual em pixels que está a ser exibida na estação de trabalho remota.

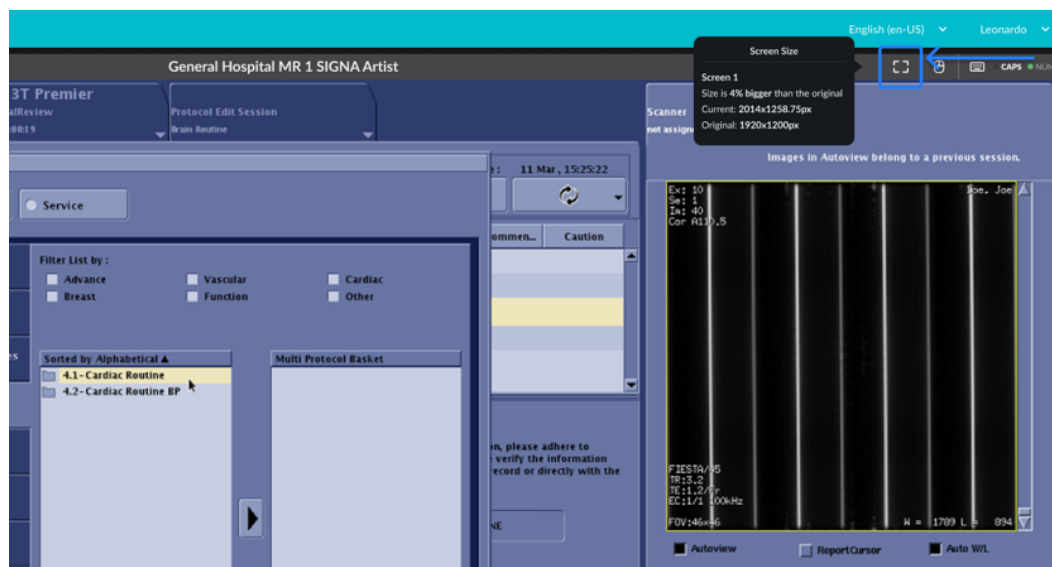


Figura 20: Dica de Informação em Streaming

4 - Estado (Status) do Mouse e Teclado

Esse recurso informa o técnico remoto sobre se o mouse e o teclado estão funcionando corretamente. Juntamente com o estado do teclado, o utilizador pode ver se as teclas **Caps Lock** e **Num Lock** do teclado do computador do equipamento estão ativadas ou desativadas. No entanto, esta funcionalidade depende do computador do equipamento fornecer essas informações; em cenários em que essas informações não são disponibilizadas pelo sistema do equipamento, o estado das teclas **Caps Lock** e **Num Lock** não será exibido. Os status do Mouse e do Teclado são mostrados somente quando o usuário tem o tipo de acesso Controle.

Ao se conectar a um equipamento, uma incompatibilidade entre os indicadores **Caps Lock** e **Num Lock** no computador remoto e no equipamento pode levar a um padrão inconsistente de digitação. Se os indicadores aparecerem ativados no equipamento, mas não estiverem realmente ativos no computador remoto, o usuário poderá digitar em letras maiúsculas no equipamento enquanto o texto aparece em letras minúsculas no chat, ou vice-versa. Da mesma forma, se o **Caps Lock** estiver ativado no computador remoto, mas desativado no equipamento, o mesmo problema ocorrerá ao contrário.

Para evitar esse problema, certifique-se de que **Caps Lock** e **Num Lock** estejam ambos ativados, ou ambos desativados antes de fazer login no equipamento. Se ocorrer uma incompatibilidade, o usuário deverá se desconectar do equipamento, ajustar o status da chave no computador remoto e, em seguida, reconectar-se.

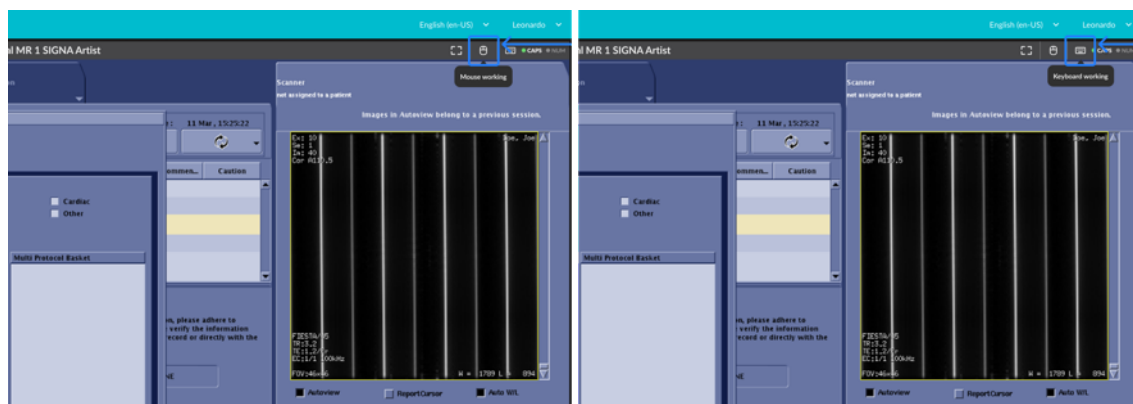


Figura 21: Barra de Streaming

Esquerda - Informações da Dica de Status do Mouse

Direita - Informações sobre o Status do Teclado sobre Dicas da Ferramenta

3.5.3. Multi-câmera

Esse recurso permite que o técnico remoto visualize várias câmeras ao mesmo tempo. Se mais de uma câmera estiver disponível, é possível visualizar apenas uma e alternar entre elas clicando no menu com o nome designado para cada câmera. Ao selecionar “ALL CAMERAS”, todas as câmeras disponíveis serão exibidas no quadro, com uma delas destacada. Para trocar a câmera destacada, basta passar o mouse sobre uma das câmeras no quadro menor e clicar em “SWITCH CAMERA”.

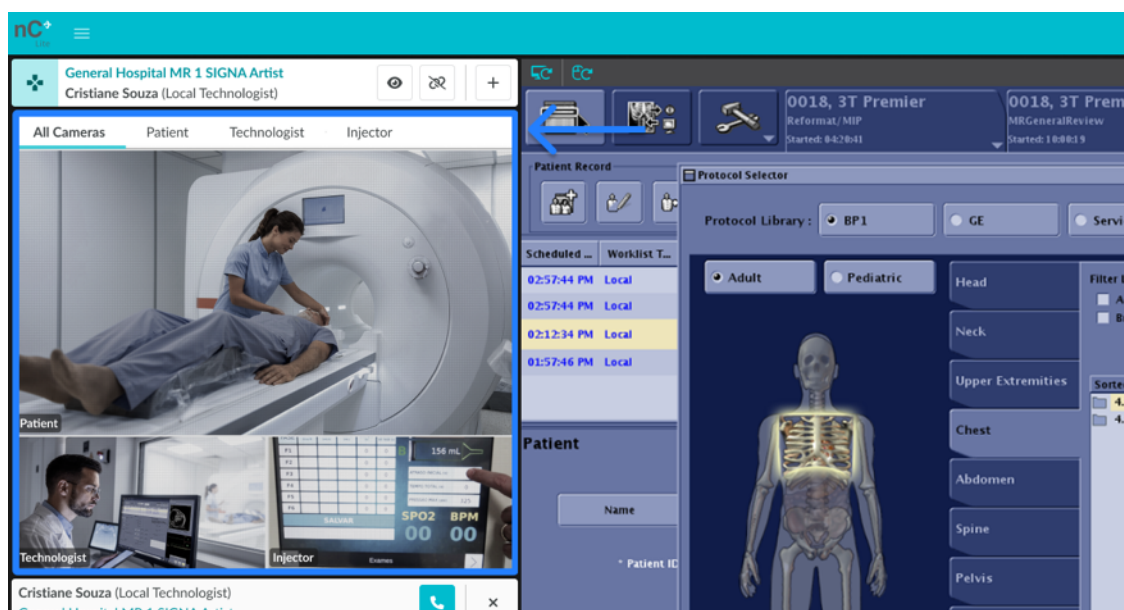


Figura 22: Visualização do Quadro Multi-câmera

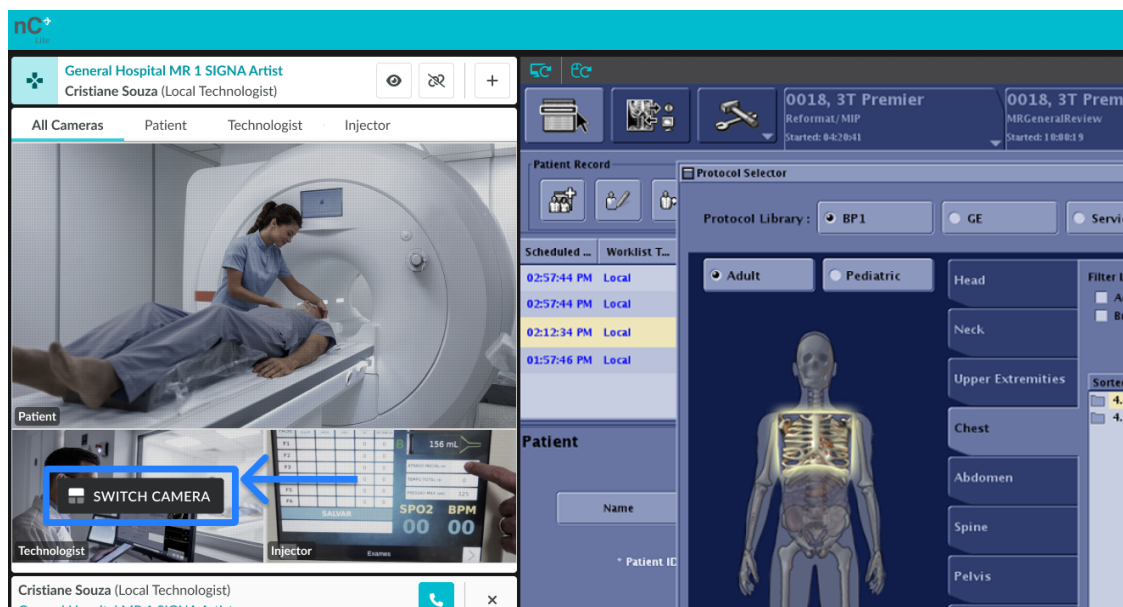


Figura 23: Botão Hover “SWITCH CAMERA” para Multi-câmera

Durante uma sessão remota ativa, se o técnico remoto estiver acessando como **Visualização**, há uma opção para desligar uma ou mais câmeras passando o mouse sobre a câmera escolhida e clicando em “TURN OFF CAMERA” (Desligar câmera). Para visualizar a câmera novamente, basta repetir o processo e clicar em “TURN ON CAMERA” (Ligar câmera).

OBS.: A opção de desligar as câmeras só está disponível no Modo de Visualização; no Modo de Controle, não é possível desligar as câmeras.

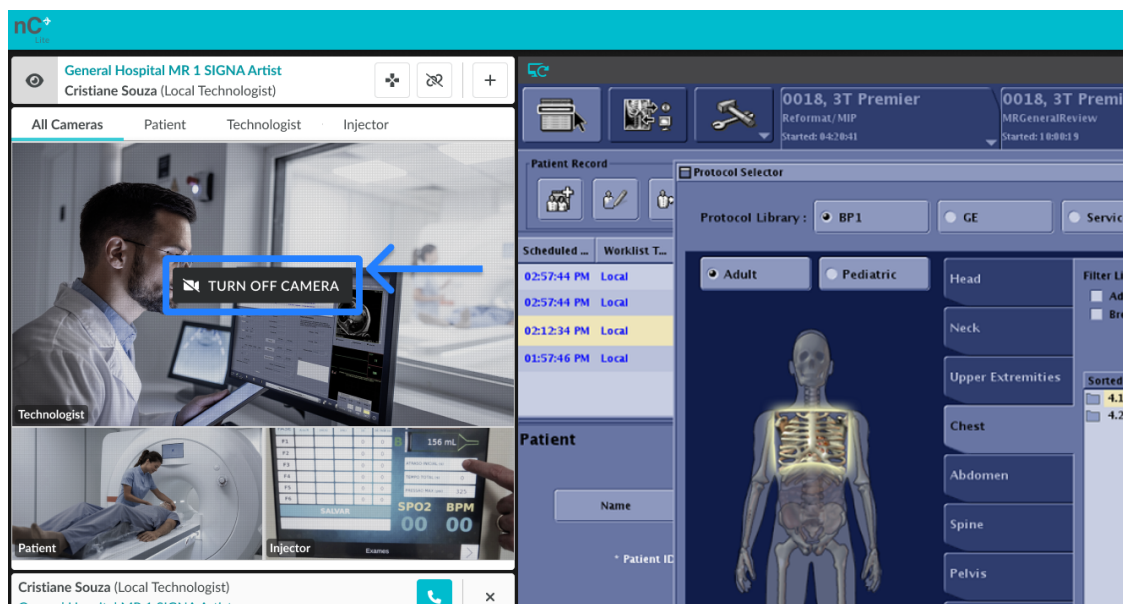


Figura 24: Botão Hover “TURN OFF CAMERA” (Desligar câmera) de várias câmeras no modo de visualização

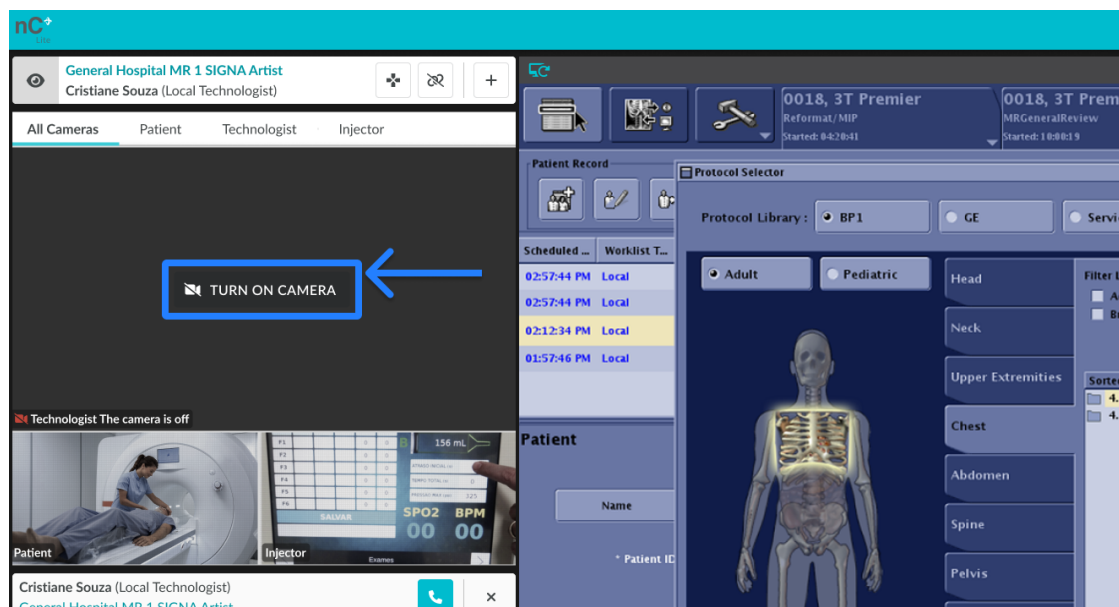


Figura 25: Botão Hover “TURN ON CAMERA” (Ligar câmera) de várias câmeras no modo de visualização

3.5.4. Abrir Outro Equipamento

Permite que o tecnólogo remoto abra uma nova guia do navegador do nCommand Lite, permitindo que o usuário selecione um novo equipamento para realizar mais de uma varredura remota simultaneamente. Para abrir um novo equipamento para acesso, basta clicar no botão “Open Another Device” (Abrir Outro Equipamento), e um aviso é exibido para que você possa fazer essa operação simultânea com segurança. Leia o aviso antes de acessar essa nova janela.

OBS.: Para uma melhor visualização durante o acesso simultâneo, recomenda-se que, após clicar em “OPEN ANOTHER DEVICE” (Abrir outro Equipamento) e clicar em “OK” nos avisos, arraste a nova guia para outro monitor disponível.



AVISO!

Aviso de Segurança para Acesso a Múltiplos Equipamentos

- **Exigência de foco intenso:** O acesso simultâneo exige foco e comunicação intensos com as equipes locais.
- **Escolha layouts diferentes:** Evite acessar equipamentos com layouts idênticos ou exames da mesma região anatômica ao mesmo tempo.
- **Arraste a aba para outro monitor:** Ao acessar um equipamento adicional, uma nova guia será aberta. Arraste essa guia para um segundo monitor, pois o sistema foi projetado para ser usado com uma tela separada para cada equipamento.
- **Preste atenção aos alertas:** Preste muita atenção a todos os alertas do sistema, pois eles são cruciais para operações seguras.
- **Controlar um de cada vez:** É possível visualizar várias telas, mas o controle é limitado a um equipamento por vez.
- **Abrir chat:** Sempre inicie o chat quando estiver conectado a um equipamento para uma comunicação clara.

- **Uma chamada por vez:** Os alertas de chamadas de voz aparecem na tela do equipamento associado; somente uma chamada pode estar ativa por vez.
- **Segurança e alerta:** Priorize a segurança e fique alerta durante todas as operações.

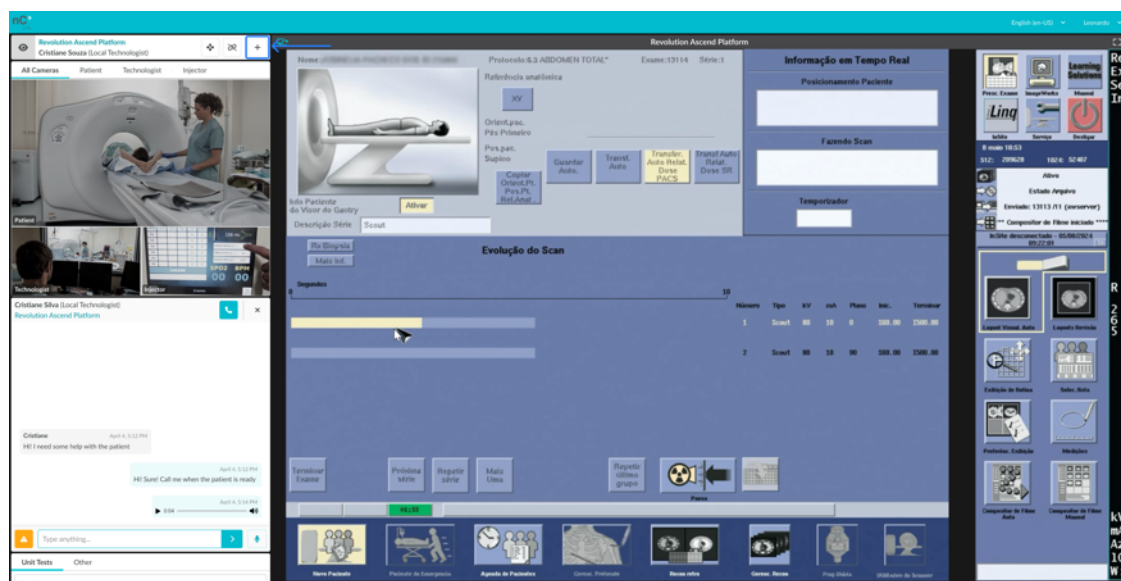


Figura 26: Botão para Abrir outro equipamento (+)

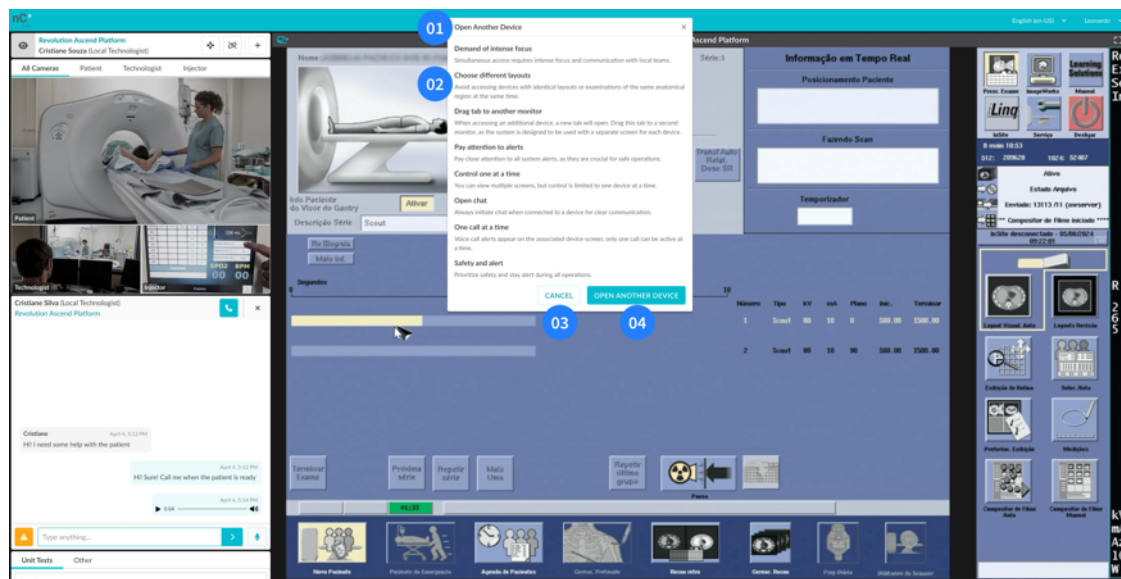


Figura 27: Avisos de Acesso a Múltiplos Equipamentos

- 01** – Título (Abrir outro Equipamento); **02** – Avisos de Segurança Operacional; **03** – Botão Cancelar; **04** – Botão para Abrir Outro Equipamento

3.5.5. System Check

O recurso System Check (Verificação do Sistema) ajuda a verificar se o equipamento atual, a rede e a conectividade com a Internet atendem aos requisitos para o uso adequado do nCommand Lite. Esse recurso realiza um teste automático rápido que verifica itens essenciais, como a qualidade da Internet, o acesso aos servidores necessários e a estabilidade da conexão. Essa ferramenta pode ser usada antes de iniciar uma sessão, durante a instalação ou quando houver suspeita de algum problema de conexão. Isso ajuda a garantir que a plataforma funcione conforme o esperado e auxilia a equipe técnica caso seja necessário solucionar problemas.

Nota: O System Check deve ser usado preferencialmente com o apoio ou mediante solicitação de um profissional de TI. A execução dessa ferramenta sem orientação técnica pode levar a uma interpretação errônea dos resultados.

Para acessar a Verificação do Sistema, os técnicos locais e remotos devem abrir a opção Session Details (Detalhes da sessão) no menu suspenso disponível sob seu nome de usuário, localizado no canto superior direito da tela principal. Depois, clique em **Open** (Abrir) ao lado da ferramenta System Check. Quando a página da ferramenta for exibida, clique em **Run Test** (Executar teste) para iniciar o processo de verificação.

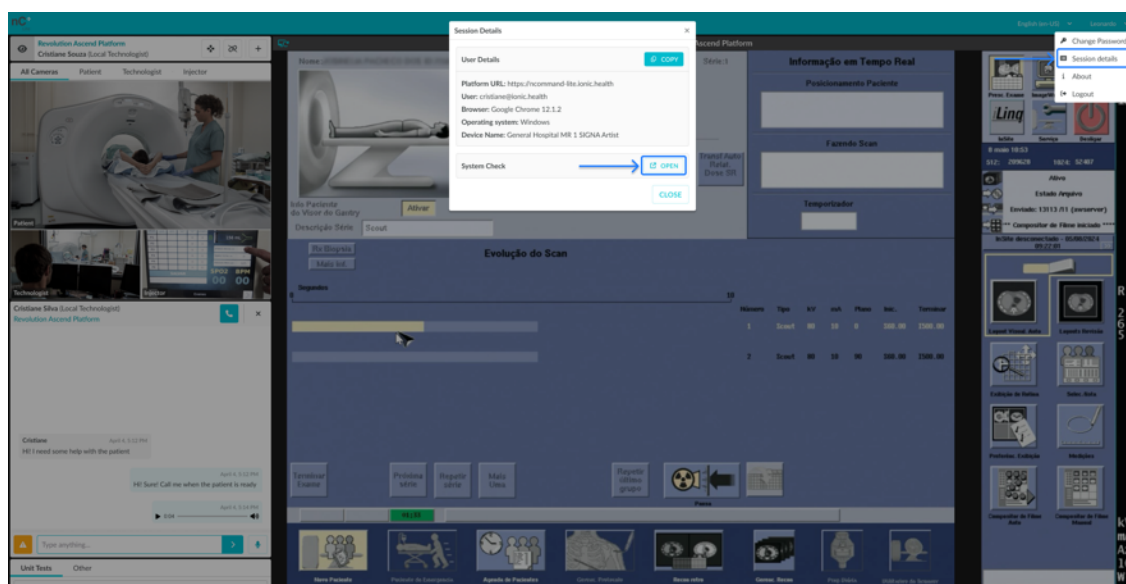


Figura 28: Como acessar o System Check

Ao usar como técnico remoto, é possível selecionar um equipamento na tela principal da ferramenta para que ele seja incluído nos resultados do teste.



AVISO!

Antes de iniciar o teste, certifique-se de que o equipamento selecionado não esteja em uso no momento.

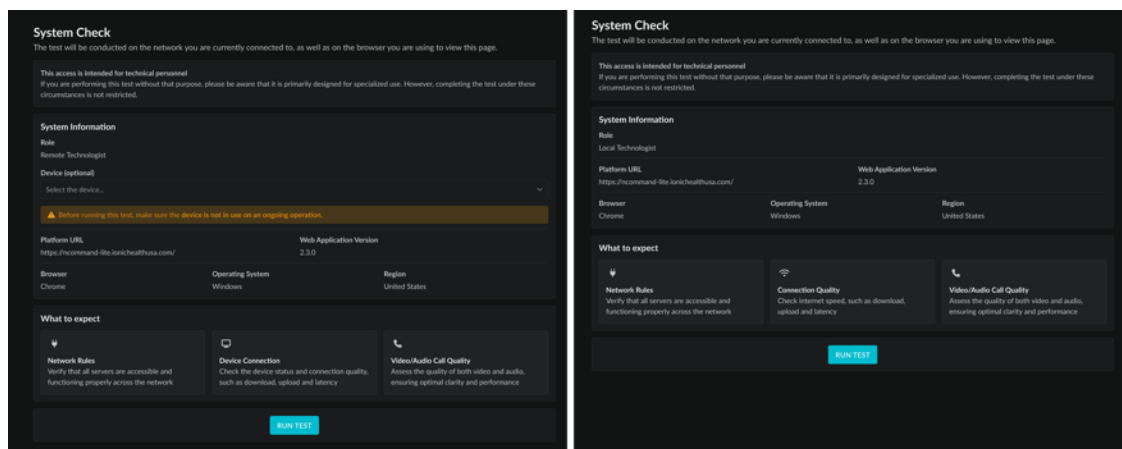


Figura 29: Tela principal do System Check
Esquerda - Técnico remoto / Direita - Técnico local

Após a conclusão do teste, um resumo dos resultados é exibido na tela. Os profissionais de TI podem analisar essas informações para identificar possíveis problemas que afetem o desempenho do sistema.

Sessão 3.6 - Chat

A plataforma oferece Chat e Chamada em tempo real com recursos de voz e vídeo, que são usados para a comunicação eficaz entre técnicos habilitados. Por meio desses recursos, os técnicos habilitados podem interagir sobre todos os assuntos relacionados ao fluxo de trabalho da sessão.



AVISO!

Em caso de falha, ligue para o técnico local por telefone.

Ao se conectar a um equipamento, você terá acesso imediato à lista de usuários do chat, organizada em duas guias. Para clientes com vários locais, cada filial pode ser configurada como um contrato separado. Quando ativado, os usuários são agrupados por contrato, com os usuários de outros contratos aparecendo na guia “Others” (Outros).

Para iniciar uma conversa, clique duas vezes no nome de um usuário para abrir a interface de chat, que suporta mensagens de texto e chamadas de voz. Verifique se a sessão selecionada corresponde ao equipamento correto. A plataforma notifica os usuários se a conexão de rede ficar lenta ou instável.



AVISO!

Antes de iniciar o contato, verifique o nome do equipamento mostrado abaixo do nome do usuário, pois alguns técnicos remotos podem estar conectados a vários equipamentos.

Veja a seguir as ferramentas disponíveis para comunicação na plataforma:

1. **Chamadas de Voz e Vídeo:** Clique no ícone para iniciar uma chamada de voz e vídeo de até 60 minutos entre um técnico remoto e um técnico local. Não há suporte para conexões entre usuários com o mesmo perfil (Local-Local ou Remoto-Remoto).

Quando um técnico local inicia uma chamada, o técnico remoto pode optar por aceitar ou recusar. Por outro lado, quando um técnico remoto inicia a chamada, ela é automaticamente conectada e o técnico local é notificado – isso funciona como um mecanismo de segurança para garantir que o técnico remoto possa sempre se comunicar com quem estiver fisicamente no local, como se estivesse lá pessoalmente.

Por padrão, o microfone fica ativo no início da chamada, enquanto a câmera permanece desligada. Cada técnico pode ativar ou desativar manualmente o microfone e a câmera a qualquer momento.

Para estabelecer uma chamada com sucesso, ambos os usuários devem ter um microfone e uma saída de áudio funcionando, com as permissões do navegador ativadas corretamente. Se algum desses componentes estiver faltando, o sistema notificará os dois usuários e a chamada não será concluída. Uma câmera é opcional – se ela não estiver disponível ou não for detectada, o sistema atualizará o ícone para refletir que não há suporte para vídeo.

Só é permitida uma chamada ativa por usuário. Se um usuário tentar iniciar uma nova chamada enquanto já estiver em uma, o sistema bloqueará a tentativa e exibirá uma notificação. Da mesma forma, se um usuário já estiver em uma chamada e receber outra chamada, o autor da chamada será informado de que o destinatário não está disponível no momento, e o usuário na chamada em andamento receberá um alerta indicando que alguém tentou entrar em contato com ele.

2. **Como encerrar Chats:** Quando um dos usuários fecha o chat clicando no botão Close (Fechar), uma mensagem automática é enviada ao outro usuário e a guia do chat é fechada. Isso garante que ambas as partes sejam informadas de que a conversa terminou. Quando a janela de chat for fechada, todas as mensagens desaparecem. Se você a reabrir durante a sessão, a conversa será reiniciada sem as mensagens anteriores.
3. **Mensagens de Texto:** Envie mensagens de texto no campo designado. Quando uma mensagem é enviada, é exibido um ícone com uma marca de seleção cinza e, quando a mensagem é recebida pelo destinatário, é exibido outro ícone com duas marcas de seleção azuis. Isso permite uma comunicação escrita segura, clara e concisa entre as duas partes.
4. **Chamar atenção:** Chame a atenção do outro usuário clicando no botão com um ponto de exclamação. Essa ação aplica um efeito de vibração visual à janela do outro usuário por alguns segundos e uma mensagem é enviada automaticamente, sinalizando urgência ou importância.
5. **Mensagens de Áudio:** Para enviar mensagens de áudio, clique no botão do microfone. Isso é usado quando você deseja transmitir uma mensagem de forma mais pessoal ou quando não é conveniente digitar.

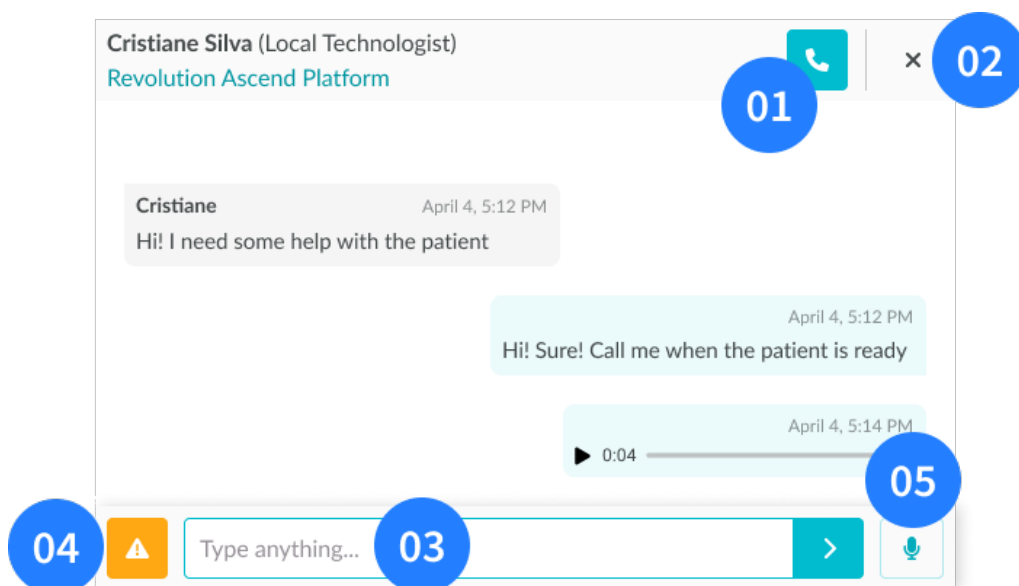


Figura 30: Visualização da Janela de Chat

01 – Botão de Chamada de Voz e Vídeo; **02** - Botão Fechar o Chat; **03** – Caixa de Texto da Mensagem; **04** – Botão Chamar atenção; **05** – Botão Gravar Mensagem de Áudio

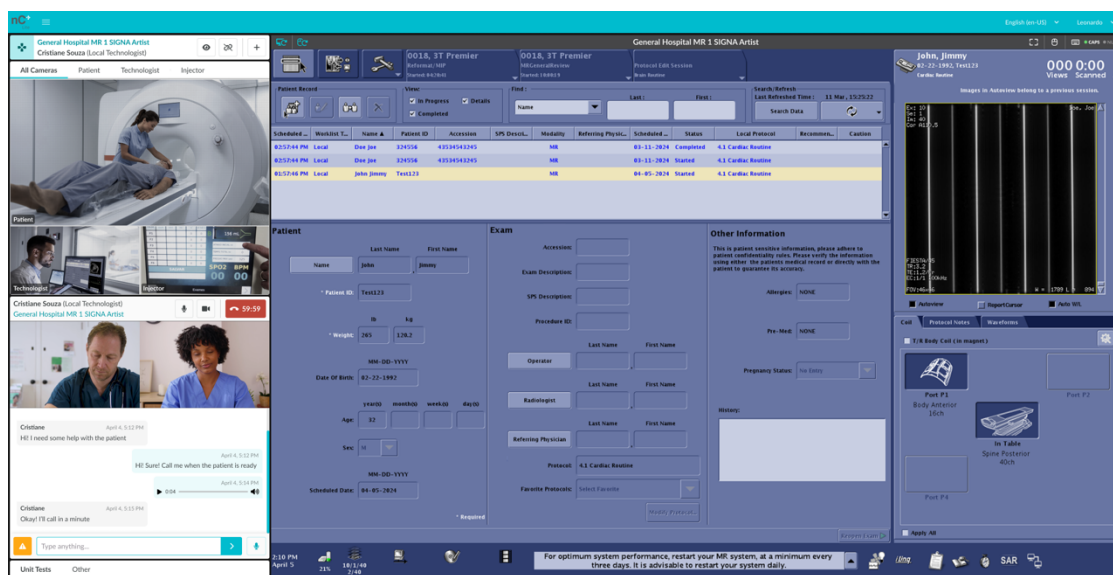


Figura 31: Tela principal do técnico remoto - janela de chat (canto inferior esquerdo)

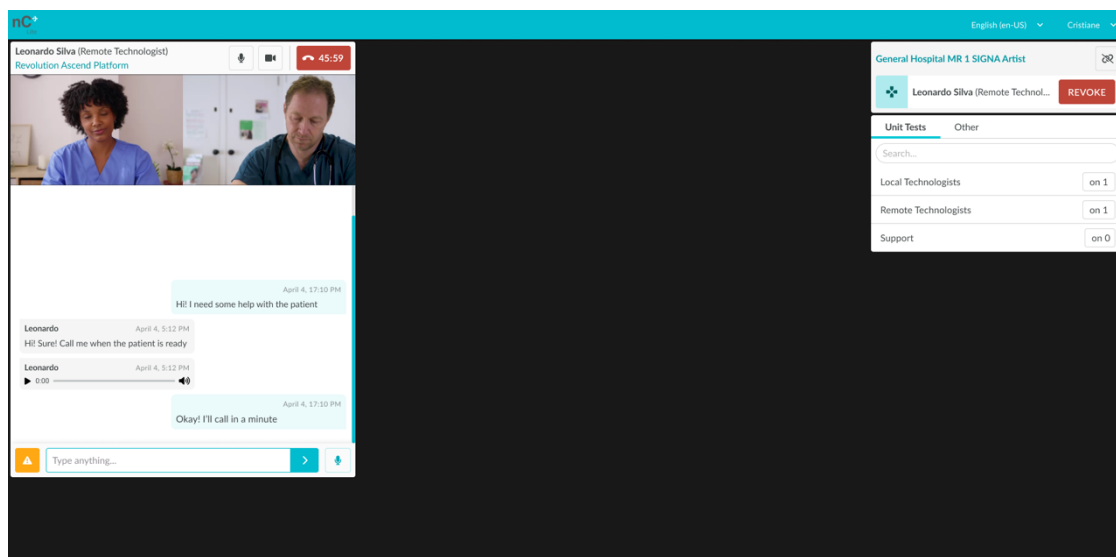


Figura 32: Tela principal do técnico local - janela de chat

Problemas de Conexão com a Internet - Quando um dos usuários apresenta problemas de conexão de rede, o sistema exibirá uma mensagem e tentará reconectar. Se a conexão for restaurada, o sistema mostrará uma mensagem **ONLINE** e a sessão remota continuará normalmente. No entanto, após várias tentativas de reconexão, se a conexão não for restabelecida, o sistema encerrará a sessão ativa e notificará o técnico de que ele foi desconectado devido a problemas na Internet. Ao mesmo tempo, ele também notificará o outro técnico de que sua contraparte foi desconectada devido a problemas de internet.

Sessão 3.7 - Encerrando sessão na plataforma

Ao final do expediente, o técnico deve se desconectar do equipamento e fazer logout da plataforma.



AVISO!

Os técnicos habilitados não devem se esquecer de fazer logout da plataforma antes do término do expediente.

Para se desconectar do equipamento, é necessário clicar no ícone de desconexão localizado na Caixa de Equipamento. Nota: Se estiver trabalhando como técnico local, certifique-se de ter revogado qualquer acesso de técnico remoto antes de se desconectar do equipamento.

Para garantir a segurança, você receberá uma notificação para confirmar que deseja se desconectar do equipamento. Após a confirmação, você será redirecionado para a tela inicial, sem nenhum equipamento selecionado.

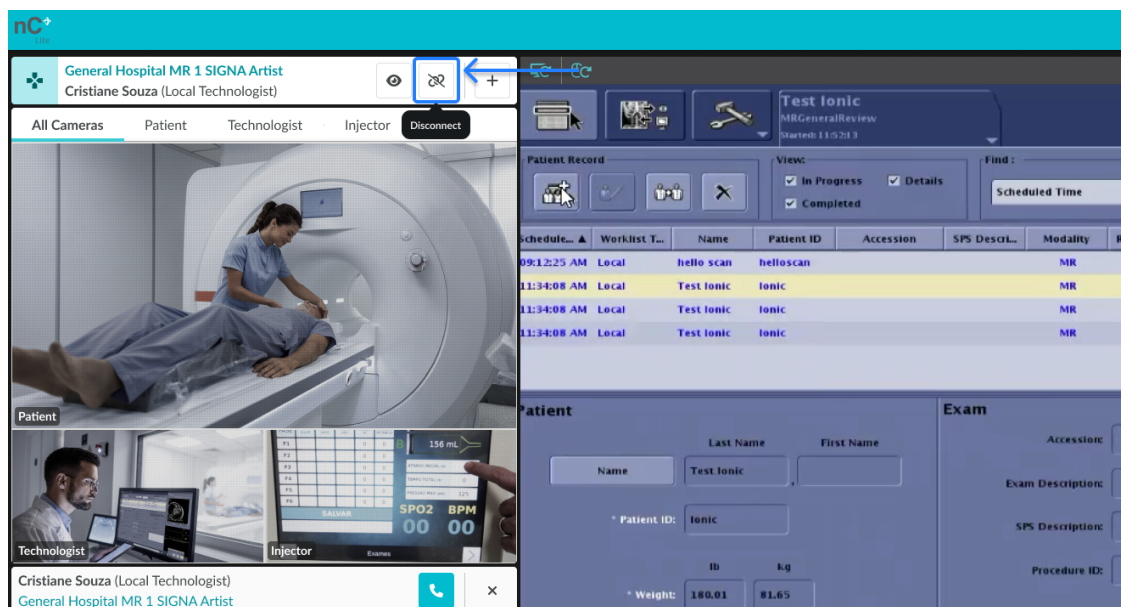


Figura 33: Botão Desconectar - Tela principal do técnico remoto

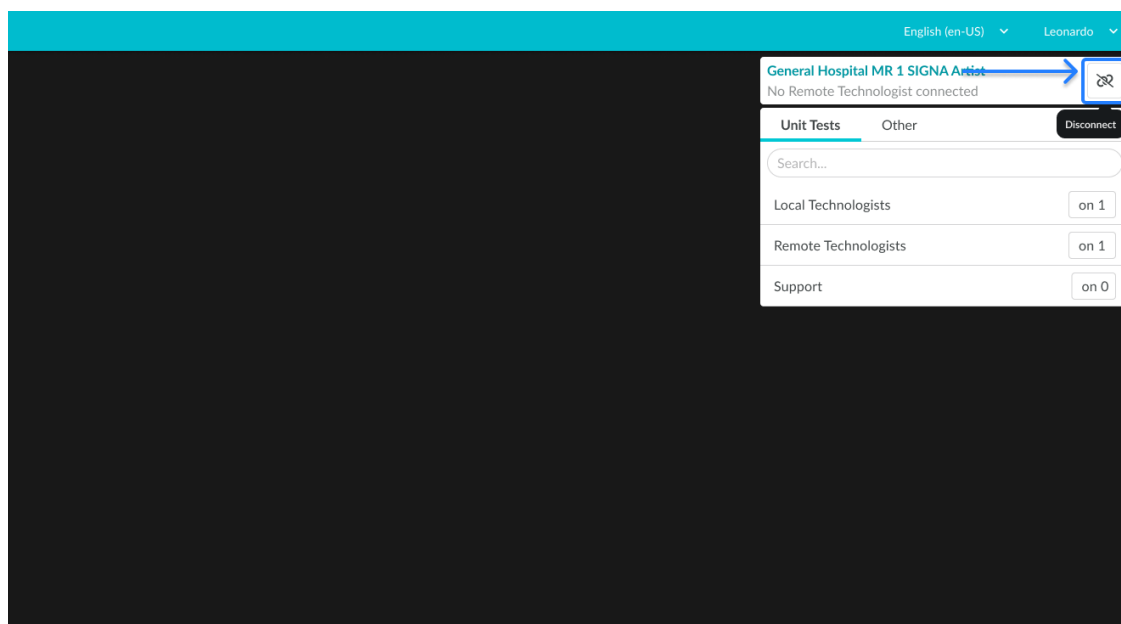


Figura 34: Botão Desconectar - Tela principal do técnico local



AVISO!

Antes de fazer o logout, certifique-se de que todas as guias adicionais que foram abertas estejam fechadas.

Para encerrar sua sessão na plataforma, clique no seu nome de usuário localizado no canto superior direito da tela e selecione a opção “Logout”. Você receberá uma notificação para confirmar que deseja deixar o centro médico onde estava trabalhando. Após a confirmação, você será redirecionado para a página de login da plataforma, concluindo assim sua jornada de trabalho com segurança.

O nCommand Lite não controla a sessão do usuário no IdP externo e, portanto, não pode executar um logout no nível do IdP. Em cenários em que os usuários compartilham a mesma máquina e usam Single Sign-On (SSO), recomenda-se que cada usuário selecione a opção “não permanecer conectado” durante o login do IdP externo (se disponível) ou saia do IdP após sair do nCommand Lite. Isso garante que nenhum usuário subsequente na mesma estação de trabalho possa reutilizar involuntariamente uma sessão ativa.

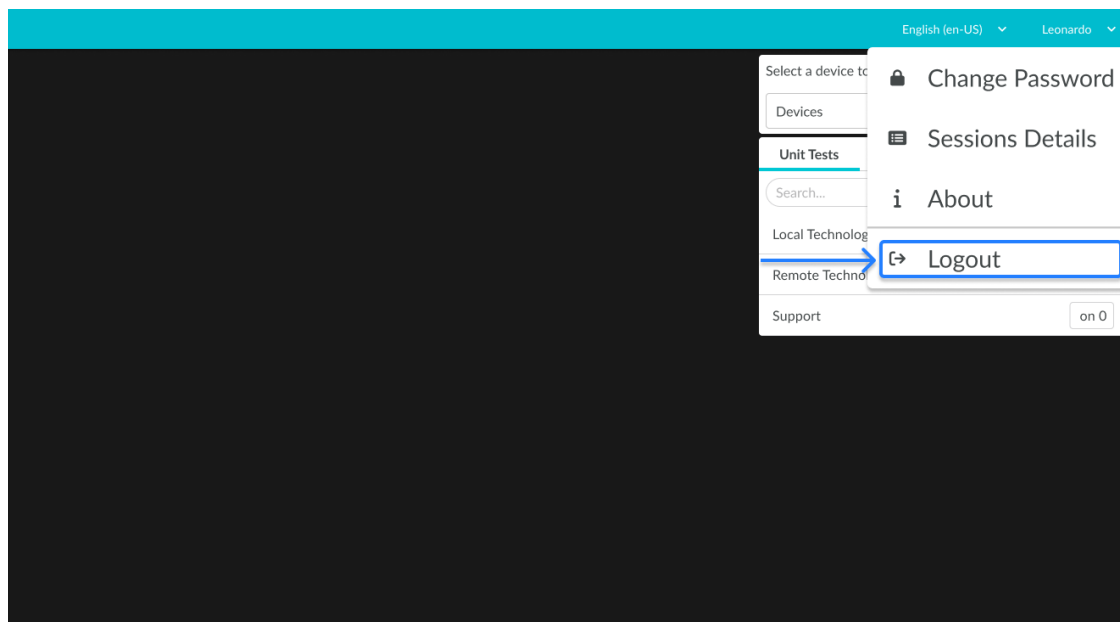


Figura 35: Item de Menu Suspenso de Logout



AVISO!

Ao usar um provedor de identidade externo em um computador compartilhado ou público, após fazer o logout da plataforma, faça também o logout do provedor de identidade. Para obter mais informações sobre como proceder, entre em contato com a equipe de suporte de TI da sua organização.

Sessão 3.8 - Treinamento Operacional

A participação no programa de treinamento é obrigatória para todos os usuários do sistema nCommand Lite. O registro do usuário na plataforma é gerenciado pela equipe da IONIC Health e só é iniciado após a confirmação de que o usuário concluiu com êxito o treinamento LMS necessário e está devidamente qualificado para operar a plataforma. Esse processo garante que todos os usuários tenham um entendimento completo das funcionalidades do sistema e estejam preparados para usar a plataforma de forma eficiente e segura. Entre em contato com o seu representante de vendas para iniciar o processo de inscrição no treinamento. [08]

Sessão 3.9 - Diretrizes de Solução de Problemas

USUÁRIO E SENHA	
Alteração de Senha	Confirme se os requisitos de senha foram atendidos; a senha deve ser forte e segura, incluindo pelo menos uma letra minúscula, uma letra maiúscula, um caractere especial e ter pelo menos 8 caracteres.
Esqueci Minha Senha	Confira sua caixa de entrada de e-mail: Certifique-se de que está usando o e-mail correto e que o e-mail de recuperação de senha não foi filtrado para sua pasta de spam ou lixo eletrônico. Tentar novamente: Espere alguns minutos e solicite outro e-mail de recuperação de senha clicando em “Dd you Forget your password?” (Você esqueceu sua senha?). Verifique a Conexão com a Internet: Certifique-se de estar conectado à internet.
E-mail de boas-vindas não recebido	Verifique se o e-mail está na sua pasta de spam. Se não estiver, entre em contato com um usuário administrador para garantir que o e-mail informado no seu cadastro está correto. Se não estiver correto, o administrador deverá atualizá-lo e reenviar o e-mail de boas-vindas.
Código de Autenticação de Dois Fatores Não Recebido	Clique em “Resend Code” (Reenviar Código) e verifique sua pasta de spam. Se não o receber, entre em contato com um usuário administrador para verificar se o e-mail cadastrado no Controle de Acesso está correto.
Tentativas de login superadas	Se o número permitido de tentativas de login for excedido, você deverá aguardar um período antes de tentar novamente.
PROVEDOR EXTERNO DE IDENTITY	
Problemas ao Acessar o Produto	Em caso de problemas de login durante o uso de um IdP (Provedor de Identidade) externo, observe que o processo de autenticação é gerenciado inteiramente pelo IdP e não pelo

	provedor do produto, ou seja, o IdP é o provedor do produto: Ionic Health. Dessa forma, o produto não pode ajudar com credenciais de conta, políticas de acesso, erros de autenticação ou bloqueio de conta. Nesses casos, entre em contato com a equipe de suporte de TI da sua organização, que poderá analisar a configuração do IdP e ajudar a resolver o problema.
Problemas de credenciais	Qualquer problema relacionado a credenciais (ex., senha esquecida, alteração de senha) deve ser resolvido diretamente com a equipe de suporte de TI da sua organização. A equipe de suporte de TI pode revisar a configuração do IdP e fornecer a assistência necessária.
Problemas com autenticador multifator (MFA)	Qualquer problema relacionado ao autenticador multifator (MFA) (ex., problemas de expiração do MFA, MFA não funcionando, login sem solicitar MFA) deve ser resolvido diretamente com a equipe de suporte de TI da sua organização. A equipe de suporte de TI pode revisar a configuração do IdP e fornecer a assistência necessária.
Credenciais que não funcionam na plataforma	Ao usar provedores de identidade externos (IdP), faça login no produto apenas usando o IdP. O uso das credenciais do IdP diretamente na página de login do produto resultará em falha no login.
MONITOR DE COMPUTADOR COM SCANNER	
Não liga	Verifique as conexões do monitor com o computador e a tomada elétrica. Podem ocorrer desconexões. Aperte o botão de energia do monitor novamente.
PLATAFORMA	
Inalcançável	Verifique a conexão de rede. Verificar se a plataforma foi iniciada e se o login ocorreu.
Latência da plataforma	Pressione Ctrl+F5 para atualizar a página. Verifique se o chat da unidade está aberto em mais de uma guia. Se for o caso, feche a guia que não estiver sendo usada.

	Se o problema persistir, tente fazer logout da plataforma, limpar o cache, fechar o navegador e, em seguida, fazer login novamente.
Recursos com problemas	Antes de tentar outros procedimentos de solução de problemas, limpe o cache do navegador (procure instruções em seu navegador atual) após o login, feche e reabra o navegador, faça login novamente na plataforma e tente novamente a ação.
Atualização	Depois que a plataforma for atualizada, limpe o cache do navegador (consulte as instruções do seu navegador) antes de fazer login na nova versão.
ÁUDIO	
Sem som	Certifique-se de que o volume do microfone e dos alto-falantes da unidade esteja ajustado para os níveis adequados. Verifique se o navegador tem permissão para usar o áudio e o microfone. Verifique se o fone de ouvido está conectado e funcionando corretamente.
Latência do som	Verifique as conexões elétricas e de rede do equipamento. Atualize a página do navegador pressionando Ctrl+F5 e faça login novamente. Se o problema persistir, tente fazer logout da plataforma, limpar o cache, fechar o navegador e, em seguida, fazer login novamente.
CHAT	
O chat não aparece	Certifique-se de que o navegador não esteja minimizado. Caso contrário, abra o chat após fazer login na plataforma nCommand Lite. Verifique se a unidade foi selecionada e o usuário está autorizado a habilitar a comunicação por chat.

	Certifique-se de que as permissões de áudio e microfone do seu navegador tenham sido aceitas. Verifique as conexões dos cabos, que podem estar desconectados. Atualize a página do navegador pressionando Ctrl+F5 e reconecte-se à plataforma. Verifique se o chat do site está aberto em mais de uma guia. Se for o caso, feche a guia que não estiver sendo usada.
Atraso no chat	Atualize a página do navegador pressionando Ctrl+F5 e reconecte-se à plataforma. Se o problema persistir, tente fazer logout da plataforma, limpar o cache, fechar o navegador e, em seguida, fazer login novamente. Verifique as conexões dos cabos, que podem estar desconectados.
Problemas ao enviar mensagens de áudio	Verifique as permissões do navegador para áudio e microfone e certifique-se de que o microfone e os dispositivos de áudio estejam conectados ao computador. Se as permissões do navegador precisarem ser ajustadas, pressione Ctrl+F5 para que o navegador reconheça as alterações ao atualizar a página.
Chamada de voz falhou ao iniciar	Verifique sua conexão com a Internet e veja se foi exibida alguma notificação explicando o motivo pelo qual a chamada não foi iniciada. Certifique-se de que você tenha um dispositivo de áudio conectado e que as permissões de áudio e microfone sejam permitidas no navegador. Se o problema persistir, atualize a página com Ctrl+F5 para tentar novamente.
Usuário não encontrado no chat	Se não conseguir localizar um usuário no chat, clique na aba "Others" (Outros)

	para garantir que ele não esteja listado lá. Os usuários associados a outros contratos aparecem separadamente na lista de contatos. Se o usuário não aparecer na lista de contatos após a seleção do equipamento, pressione Ctrl+F5 para atualizar a tela e selecione novamente. Verifique se você tem uma conexão com a internet.
SOLICITAR ACESSO AO EQUIPAMENTO	
A plataforma não reconheceu que o técnico local está conectado	Verifique a opção "Others" (Outros) para confirmar se o usuário local está conectado. Se o usuário estiver realmente conectado, mas você ainda estiver recebendo a mensagem de que o usuário local não está conectado ao scanner, atualize a tela pressionando Ctrl+F5 e peça ao usuário local para repetir a mesma instrução. Em seguida, selecione o equipamento novamente e peça ao usuário local para selecionar o dispositivo novamente também. Se o problema persistir, entre em contato com o suporte para verificar a rede.
A solicitação de acesso não está sendo enviada	Atualize a página pressionando Ctrl+F5 e confirme com o usuário local via chat se a solicitação de acesso está sendo recebida. Se o problema persistir, entre em contato com o suporte para obter mais assistência.
DISPOSITIVO DE STREAMING (COMPUTADOR E-KVM)	
Dispositivo de Streaming (COMPUTADOR E-KVM) não funcionando	Clique no botão "Reload streaming" (Recarregar streaming) na plataforma. Certifique-se de que a fonte de alimentação ininterrupta e estabilizada (unidade médica) e/ou dispositivo de streaming estejam devidamente conectados e ligados. Desligue o dispositivo de streaming e todos os outros equipamentos e ligue-os novamente. Atualize a plataforma.
Dispositivo de streaming lento	Clique no botão "Reload streaming" (Recarregar streaming) na plataforma. Atualize a página pressionando Ctrl+F5 e

	reconecte-se à plataforma. Verifique a qualidade da sua conexão de rede. Para validar o status da rede, é possível realizar um teste de ping no dispositivo para verificar se há perda de pacotes. Após problemas com a internet, a plataforma pode não funcionar como previsto. Atualize a página e solicite acesso ao usuário local novamente.
Perda de saída de vídeo	É admissível que uma descarga eletrostática cause perda de imagem. Após a reinicialização do sistema, a comunicação e o streaming de vídeo devem ser restabelecidos automaticamente.

Sessão 3.10 - Métodos de Limpeza do Hardware

- Antes de iniciar o processo de limpeza, certifique-se de que todo o equipamento esteja desconectado da rede elétrica.
- Não use produtos abrasivos.
- Não mergulhe nenhum equipamento ou periférico em nenhum tipo de líquido.
- Descarte os materiais de limpeza de acordo com as normas de descarte de resíduos perigosos.
- Não é recomendável usar desinfetante em spray, pois o vapor pode entrar no equipamento e causar curto-circuito ou corrosão.
- Este produto é não estéril

Capítulo 4 Cibersegurança e Privacidade

Sessão 4.1 - Riscos de Segurança e Privacidade

O Sistema **nCommand Lite** implementa múltiplas medidas técnicas e organizacionais para proteger as informações processadas.

O sistema foi certificado de acordo com as normas ISO/IEC 27001 e ISO/IEC 27701 e segue uma abordagem de privacidade desde a concepção. Oferece suporte à conformidade com as leis de proteção de dados de saúde e com as normas de segurança cibernética aplicáveis na UE, nos EUA, no Reino Unido, na Suíça, no Brasil, nos Emirados Árabes Unidos, na Arábia Saudita, na Austrália e na Nova Zelândia.

No entanto, os usuários devem adotar práticas recomendadas para evitar a exposição desnecessária de dados confidenciais.

- Evite compartilhar informações pessoais ou confidenciais, a menos que seja estritamente necessário.
- Garantir que as comunicações e o acesso ao sistema ocorram em ambientes seguros.
- Se suspeitar de alguma atividade maliciosa, notifique imediatamente a equipe responsável.

Sessão 4.2 - Proteção de Dados Pessoais (Conformidade com GDPR / HIPAA)

O sistema **nCommand Lite** está em conformidade com todas as leis e regulamentos de privacidade e proteção de dados aplicáveis nas regiões em que opera, incluindo, entre outros, os requisitos do GDPR, HIPAA, LGPD e ISO/IEC 27701. Todas as atividades de processamento de dados são executadas sob as funções de “**Processador**” e “**Subprocessador**”, conforme definido pelo GDPR, com rigorosa segregação de dados regionais para garantir a conformidade e evitar transferências de dados internacionais não autorizadas

Quais dados são recolhidos?

- **Usuários:** Name, email, and company (strictly for authentication and access management).
- **Dados do paciente:** Somente transmissões de exames médicos via streaming em tempo real, sem armazenamento de dados

Como os dados são usados e protegidos?

- Os dados são usados exclusivamente para **autenticação, controle de acesso e rastreabilidade da sessão**.
- A transmissão de informações é protegida por **criptografia AES-256 para armazenamento e TLS 1.3 para dados em trânsito**.
- **O acesso é restrito** e segue o princípio de **menor privilégio (RBAC)**.
- Criptografia de ponta a ponta garantida para vídeo P2P e fluxos de controle via WebRTC.
- Os provedores de cloud autorizados (por exemplo, Microsoft Azure) processam dados limitados sob estritas salvaguardas contratuais.

Os usuários têm os seguintes direitos:

- **Acesso e correção** de informações pessoais.
- **Solicite exclusão de dados**, conforme aplicável.

Se tiver alguma dúvida, envie um e-mail para privacy@ionic.health para entrar em contato com o DPO da Ionic Health. Todas as solicitações são tratadas dentro de 30 dias, prorrogáveis de acordo com o GDPR.

Sessão 4.3 - Gerenciamento de Acesso e Autenticação

Os usuários são responsáveis por definir **funções e permissões de acesso** para suas equipes, garantindo revisões periódicas e documentação do acesso concedido.

Melhores Práticas e Controles

- Siga o **princípio do menor privilégio (RBAC)**, garantindo que os usuários tenham apenas o acesso necessário.
- **Autenticação Multifator (MFA)** é obrigatória para acesso administrativo e recomendada para todos os usuários.
- **Senhas fortes** são necessárias, com pelo menos **8 caracteres, incluindo letras maiúsculas e minúsculas, números e símbolos**.
- **Não compartilhe credenciais**.
- As permissões de acesso são monitoradas e revisadas periodicamente.

Monitoramento: O acesso, as modificações de permissão e as atividades importantes são documentados nos registros de segurança do sistema. Os registros são retidos por um período mínimo de 7 anos, em alinhamento com a HIPAA, o GDPR e outras regulamentações aplicáveis. Eles apoiam a auditoria interna, a análise forense e os relatórios regulatórios. Os registros são protegidos contra adulteração e armazenados em ambientes seguros com controle de acesso.

Sessão 4.4 - Controle de Acesso à Verificação do Sistema

O recurso System Check é acessível exclusivamente pelo **nCommand Lite Web Application** e requer credenciais válidas para login. O acesso é limitado apenas a funções autorizadas — *Técnico Remoto, Técnico Local, Admin, Supervisor de Funções* e *Usuário do System Check*.

A função *Usuário do System Check* é projetada com permissões restritas, permitindo acesso exclusivamente a recursos de diagnóstico relacionados à validação de rede e verificação de conectividade. Isso garante que os detalhes da rede, as informações da lista de permissões e as métricas do sistema nunca sejam expostos a pessoas não autorizadas.

Todas as solicitações de acesso são autenticadas por meio do Azure AD B2C, com Autenticação Multifator (MFA) e políticas adaptativas de acesso condicional gerenciadas pelo Microsoft Entra ID. A complexidade da senha segue a política de segurança organizacional, exigindo pelo menos oito caracteres, incluindo letras maiúsculas e minúsculas, números e símbolos. As senhas expiram a cada 90 dias e as sessões se desconectam automaticamente após 24 horas de inatividade, podendo ser estendidas por até 90 dias com uso contínuo.

Sessão 4.5 - Segregação Regional de Dados e Retenção de Registros

A plataforma **nCommand Lite** mantém uma rigorosa segregação regional dos dados para evitar transferências internacionais não autorizadas ou desnecessárias. Os ambientes são isolados por região, garantindo a conformidade com os regulamentos aplicáveis.

Todos os logs de acesso, registros de atividades e eventos de segurança são retidos por um período mínimo de sete (7) anos, de acordo com as normas aplicáveis de proteção de dados e saúde. Os registros são armazenados em ambientes seguros, com acesso controlado e protegidos contra adulteração. Essas informações dão suporte a investigações forenses, auditorias de conformidade e relatórios regulamentares.

Sessão 4.6 - Segurança e Integridade de Dados

O Sistema **nCommand Lite** garante a confidencialidade, a integridade e a disponibilidade dos dados por meio de práticas de segurança padrão do setor.

Os usuários devem garantir a conformidade com os protocolos de segurança, revisar regularmente as políticas de acesso e relatar quaisquer anomalias. O sistema monitora continuamente as atividades, e os administradores devem aplicar políticas de segurança para manter uma defesa robusta contra possíveis ameaças.

O sistema é protegido por monitoramento 24 horas por dia, 7 dias por semana, por meio de um Centro de Operações de Segurança (SOC) dedicado, com recursos de SIEM para detecção e resposta a ameaças.

Sessão 4.7 - Resposta a Incidentes de Segurança

O sistema inclui um Plano de Resposta a Incidentes documentado, alinhado com a ISO 27035 e o NIST CSF.

Em caso de incidentes de segurança, como acesso não autorizado ou falhas no sistema, os usuários devem seguir estas etapas:

Como identificar um incidente?

- **Acesso não autorizado** detectado nos registros de atividade.
- **Tentativas de login suspeitas** ou falhas repetidas de autenticação.
- **Comportamento incomum do sistema**, como ações inesperadas ou falhas.

Como relatar um incidente?

Registre imediatamente o evento por meio dos canais de suporte disponíveis (Capítulo 5).

Se uma violação de dados pessoais for confirmada, a IONIC, atuando como subprocessadora, notificará a GE como Processadora em 48 horas, fornecendo todas as evidências relevantes, detalhes do impacto e medidas de mitigação. A GE, por sua vez, é responsável por notificar o Controlador (o cliente) conforme os requisitos legais e contratuais aplicáveis.

Capítulo 5 Canais de Atendimento

Se precisar de ajuda com um problema técnico, uma etapa não esclarecida do processo ou orientação adicional, nossa equipe está pronta para ajudar. Você pode entrar em contato conosco por telefone, e-mail ou pela plataforma ITSM, o que for mais conveniente para você. Nossos especialistas são treinados para oferecer assistência personalizada, garantindo que qualquer problema seja resolvido de forma rápida e eficiente.

Números de telefone

Estados Unidos	+1 (216) 2421223
Brasil	+55 12 3600 0181
Europa (Portugal)	+351 (300) 528 410
Austrália	+1 (216) 2421223
Nova Zelândia	+1 (216) 2421223

Plataforma ITSM

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

E-mail

helpdesk@ionic.saúde



AVISO!

Qualquer incidente grave relacionado ao uso desse dispositivo deve ser relatado ao fabricante e à autoridade sanitária/autoridade competente onde o dispositivo está instalado.

Para informar o fabricante: entre em contato com o representante de serviço local ou envie um relatório para: helpdesk@ionic.health

Forneça as seguintes informações:

- O número da versão do sistema, exibido na tela de login;
- Data do incidente;
- Descrição do incidente, incluindo qualquer impacto/lesão do paciente ou usuário;
- Suas informações de contato (unidade, endereço, nome de contato, cargo e telefone do local).

Capítulo 6 Informações Legais e Regulatórias

Fabricante



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
Brasil

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

Responsável Técnico

Alexandre Seiji Fukuda Ribas
CREA-SP: 5071085437

ANVISA

82585300004

Importador (EUA)



nCommand Lite System

IONIC HEALTH USA INC.

11201 Cedar Avenue, STE 600
Cleveland, OH 44106
USA

+1 (216) 242 1223

Representante / Importador da UE



nCommand Lite



Número de identificação do Corpo
Notificado: 2803

EUROPE IONIC HEALTH DIGITAL TECHNOLOGIES, LDA

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

+351 (300) 528 410

Representante Autorizado Suíço (CH-REP) / Importador**CH REP****REF**

nCommand Lite

FREYR LIFE SCIENCES GMBH

Bahnhofplatz
CH-6300 Zug
Suíça

Pessoa Responsável / Importadora do Reino Unido**REF**

nCommand Lite

FREYR LIFE SCIENCES LTD

9 Greyfriars Road
Reading, Berkshire
RG1 1NU
England, United Kingdom

Patrocinador Australiano**REF**

nCommand Lite

TAEVAS LIFE SCIENCES PTY LTD

46 Dora St
Blacktown NSW 2148
Australia

Patrocinador da Nova Zelândia**REF**

nCommand Lite

TAEVAS LIFE SCIENCES LIMITED

Level 3, 1 Margaret Street
Lower Hutt 5010
New Zealand

BASIC UDI-DI: 7898974112NCLITE2L**Solicitar cópia física**

Cópias físicas do Manual do Usuário nCommand Lite serão fornecidas mediante solicitação, sem custo adicional. Entre em contato com o seu representante local e solicite uma cópia impressa do Manual do Usuário.

Data de Fabricação

A data de lançamento do software é encontrada na página de login do nCommand Lite, no formato MÊS/ANO.

Capítulo 7 Histórico de Revisões

Revisão	Descrição da Mudança	Data
0	Versão manual atualizada da 2.3 v1 para a 2.4	25 de novembro de 2025
1	Etiquetas atualizadas do Capítulo 6	04 de dezembro de 2025
2	Removido o requisito de endereço IP estático da configuração do computador local na subseção 1.3.11 Atualização do símbolo do Representante Autorizado da UE na subseção 1.3.12 Nota removida do Subitem 1.3.14 Atualizado o conteúdo no Capítulo 2 Atualizado o símbolo do Representante Autorizado da UE no Capítulo 6	28 de janeiro de 2026
3	Revisada a tradução do termo Responsável Técnico no Capítulo 6	09 de fevereiro de 2026

APÊNDICE - Lista de Verificação para Início de Utilização

1. Verificar Conexões Elétricas e de Redes:

Certifique-se de que as conexões elétricas e os pontos de rede estejam devidamente estabelecidos no Computador e-KVM, Computador Scanner e Computador Local.

2. Verifique o Status de Energia:

Verifique se a fonte de alimentação ininterrupta e estabilizada e o computador e-KVM estão ligados e funcionando corretamente.

3. Acesso rápido à plataforma nC Lite:

Confirme a presença do atalho da plataforma nC Lite no desktop para acesso rápido.

4. Acesso e Login na Plataforma nC Lite:

Abra a plataforma nCommand e faça login para garantir acesso total e funcionalidade adequada.

5. Configuração do Aplicativo de Chat:

Abra o aplicativo de chat dentro da plataforma nC Lite em apenas uma aba e evite minimizá-lo para uma comunicação fluida.