

UŽIVATELSKÁ PŘÍRUČKA

nCommand Lite v.4

Manuální verze: V.3



Obsah

Kapitola 1	Úvod	4
Oddíl 1.1 -	Účel	4
Oddíl 1.2 -	Slovník pojmů	4
Oddíl 1.3 -	Popis	5
1.3.1.	Zamýšlené použití	5
1.3.2.	Indikace použití	6
1.3.3.	Zamýšlená skupina pacientů	6
1.3.4.	Prostředí použití	6
1.3.5.	Kontraindikace	6
1.3.6.	Možnosti platformy	6
1.3.7.	Klinické přínosy	7
1.3.8.	Zamýšlení uživatelé	7
1.3.9.	Provozní prostředí	7
1.3.10.	Prostředí zařízení	8
1.3.11.	Minimální požadavky	9
1.3.12.	Symboly	10
1.3.13.	Životnost	11
1.3.14.	Upgrade / aktualizace	11
Kapitola 2	Seznam obecných varování a bezpečnostních opatření	12
Kapitola 3	Použití platformy v každé lokalitě	15
Oddíl 3.1 -	Přístup a používání systému nCommand Lite	15
Oddíl 3.2 -	První přihlášení k platformě	15
3.2.1.	Přihlášení přes nCommand Lite	15
3.2.2.	Přihlášení přes External IdP	17
Oddíl 3.3 -	Správa hesel	18
Oddíl 3.4 -	Přístup s profilem místního technika	21
Oddíl 3.5 -	Přístup s profilem vzdáleného technika	24
3.5.1.	Režim přístupu	25
3.5.2.	Panel přenosu	27
3.5.3.	Více kamer	29
3.5.4.	Otevřít další zařízení	31
3.5.5.	Kontrola systému	33
Oddíl 3.6 -	Chat	34

Oddíl 3.7 -	Ukončení relace na platformě.....	38
Oddíl 3.8 -	Provozní školení	40
Oddíl 3.9 -	Pokyny pro řešení problémů.....	41
Oddíl 3.10 –	Způsob čištění hardwaru	46
Kapitola 4	Kybernetická bezpečnost a ochrana osobních údajů	47
Oddíl 4.1 -	Rizika v oblasti bezpečnosti a ochrany osobních údajů	47
Oddíl 4.2 -	Ochrana osobních údajů (soulad s GDPR / HIPAA)	47
Oddíl 4.3 -	Správa přístupu a autentizace.....	48
Oddíl 4.4 -	Kontrola systému řízení přístupu.....	48
Oddíl 4.5 -	Regionální segregace údajů a uchovávání přístupových záznamů	49
Oddíl 4.6 -	Bezpečnost a integrita údajů	49
Oddíl 4.7 -	Reakce na bezpečnostní incidenty.....	49
Kapitola 5	Servisní kanály	51
Kapitola 6	Právní a regulační informace.....	52
Kapitola 7	Historie revizí.....	55
PŘÍLOHA I –	Kontrolní seznam pro zahájení služby	56

**UPOZORNĚNÍ**

Federální zákon stanovuje, že toto zařízení může být prodáváno pouze lékařem nebo na jeho předpis a smí jej používat pouze zdravotnický technik s licencií ve státě, kde vykonává svou praxi.

(pro Spojené státy americké)

**UPOZORNĚNÍ**

V Brazílii je tento software schválen společností Anvisa pro použití výhradně se zařízením pro magnetickou rezonanci (MRI). Jakékoli jiné použití není povoleno.

(pro použití v Brazílii)

**UPOZORNĚNÍ**

Před použitím se ujistěte, že jste se seznámili s konkrétními požadavky platnými ve vaší zemi nebo regionu. Nedodržení předpisů může vést ke zdravotním rizikům.

**UPOZORNĚNÍ**

Ujistěte se, že verze této uživatelské příručky odpovídá verzi používané platformy. Použití neodpovídající verze může vést k nesprávnému fungování nebo chybnému výkladu funkcí.

Kapitola 1 Úvod

Oddíl 1.1 - Účel

Tato příručka si klade za cíl poskytnout místním i vzdáleným technikům ucelený přehled o specifických funkcích systému nCommand Lite. Tento dokument slouží jako uživatelská příručka a nabízí stručné a praktické informace, které uživatele provádějí funkcemi systému i řešením problémů. Dodržováním této příručky budou uživatelé schopni efektivně využívat systém nCommand Lite, což jim pomůže zvýšit produktivitu a snížit závislost na technické podpoře.

Oddíl 1.2 - Slovník pojmů

**UPOZORNĚNÍ**

Tento štítek se vztahuje na podmínky nebo činnosti, které představují potenciální nebezpečí. Pokud tyto pokyny nebudete dodržovat, může dojít k lehkému zranění nebo k poškození majetku.

**VAROVÁNÍ**

Tento štítek označuje podmínky nebo činnosti, které mají za následek konkrétní nebezpečí. Pokud tyto pokyny nebudete dodržovat, způsobíte vážné zranění nebo značnou škodu na majetku.

Termín používaný na platformě	Odpovídající termín
Zobrazovací pracoviště	zdravotnické zařízení poskytující lékařskou péči, jednotka, mobilní jednotky, zdravotnické zařízení, zdravotnická jednotka
Vzdálené zařízení	Vzdálená pracovní stanice, Vzdálené místo, Vzdálená kancelář, Vzdálená lokalita, Příkazové centrum
Platforma	Webová aplikace nCommand Lite
Systém	Systém nCommand Lite se všemi „subsystémy“
Zařízení	lékařský skener, skener, vybavení, lékařské zařízení, zobrazovací zařízení, zobrazovací vybavení
Místní technik	lokální uživatel, lokální technik, lokální zdravotnický pracovník (LHP), uživatel na pracovišti

Oddíl 1.3 - Popis

Systém nCommand Lite je software jako lékařské zařízení (SaMD) určený pro koncového uživatele. Poskytuje vzdálený přístup přes webovou aplikaci pro prohlížení a hodnocení zobrazovacích snímků a zároveň umožňuje vzdáleně poskytovat reálnou asistenci technikovi s licenci, který se nachází u pacienta (místní uživatel) a obsluhuje lékařská zobrazovací zařízení, v rámci školení nebo hodnocení postupů, u zařízení MRI, CT a PET/CT.

Vzdálení uživatelé jsou licencovaní technici, kteří mají možnost přistupovat k lékařskému zobrazovacímu zařízení z počítače splňujícího minimální požadované specifikace, odkudkoli, prostřednictvím bezpečného softwarového připojení, které přenáší video a umožňuje ovládání zařízení přes klávesnici a myš. To umožňuje vzdáleným uživatelům asistovat místním uživatelům bez ohledu na vzdálenost. Tento přístup musí udělit místní uživatel pracující se systémem a může jej také kdykoli zrušit, čímž si po celou dobu zachovává plnou kontrolu nad relací. Každá vzdálená relace je navíc řízena prostřednictvím zabezpečených přihlašovacích údajů, které spravuje místní uživatel. Připojení k lékařskému zařízení je omezeno na jednu vzdálenou relaci v daný okamžik, aby byla zajištěna přísná kontrola nad tím, kdo se systémem na dálku pracuje. Snímky prohlížené na dálku nejsou určeny k diagnostickému použití.

Systém nCommand Lite se skládá z hardwarového a softwarového IT řešení, které podporuje více relací a umožňuje vzdáleným technikům podle potřeby přistupovat k více lékařským zobrazovacím zařízením. Skenery kompatibilní se systémem nCommand Lite využívají společný protokol, který umožňuje správu skenovacích parametrů a vzdálené skenování.

1.3.1. Zamýšlené použití

Systém nCommand Lite poskytuje vzdálený přístup k prohlížení a hodnocení snímků a zároveň umožňuje na dálku poskytovat licencovanému technikovi obsluhujícímu skener asistenci v reálném čase. Tato asistence zahrnuje školení, hodnocení postupů a správu skenovacích parametrů.

1.3.2. Indikace použití

Systém nCommand Lite umožňuje vzdálený přístup k prohlížení a hodnocení snímků a zároveň poskytuje možnost na dálku poskytovat licencovanému technikovi obsluhujícímu kompatibilní skener MRI, CT nebo PET/CT asistenci v reálném čase. Tento přístup musí udělit místní licencovaný technik, který systém obsluhuje. Vzdálený přístup je k dispozici pouze pro systémy podporující možnost vzdáleného připojení. Snímky prohlížené na dálku nejsou určeny k diagnostickým účelům.

1.3.3. Zamýšlená skupina pacientů

Pro každého pacienta, u kterého je předepsáno zobrazovací vyšetření pomocí připojeného lékařského zobrazovacího zařízení.

1.3.4. Prostředí použití

Zobrazovací pracoviště provádějící vyšetření magnetickou rezonancí (MRI), počítačovou tomografií (CT) a pozitronovou emisní tomografií – počítačovou tomografií (PET/CT) a vzdálená řídicí centra.

1.3.5. Kontraindikace

Platformu by neměli obsluhovat uživatelé, kteří nejsou licencovaní technici a kteří neabsolvovali školení pro používání systému nCommand Lite.

1.3.6. Možnosti platformy

- **Vzdálené skenování:** zobrazuje obrazovku lékařského zobrazovacího zařízení v reálném čase, což umožňuje vzdálenému licencovanému technikovi sledovat vyšetření.
- **Chat:** umožňuje komunikaci mezi vzdáleným a místním licencovaným technikem prostřednictvím textových a hlasových zpráv. Místní i vzdálení technici mohou rovněž uskutečňovat a přijímat hlasové a videohovory.
- **Více kamer:** umožňuje vzdálené sledování pacientů a lékařského zařízení během vyšetření. Vzdálený technik může přistupovat k obrazům z kamer prostřednictvím záložek, které jsou rozděleny na záložky všech kamer a jednotlivé kamery. Tento mechanismus napodobuje vizuální dohled, jaký by měl zdravotnický odborník, kdyby byl přímo u pacienta, čímž zvyšuje úroveň bezpečnosti.
- **Více relací vzdáleného skenování** umožňuje vzdálenému technikovi podle potřeby přistupovat k více lékařským zobrazovacím zařízením.
- **Režim přístupu:** umožňuje vzdálenému technikovi volit mezi zobrazením snímků nebo ovládáním zařízení. V režimu Zobrazit mohou vzdálení technici sledovat pouze přenášený obraz. V režimu Ovládat mají k dispozici ovládání myši a klávesnice.
- **Správa přístupu vzdáleného technika:** umožňuje místnímu technikovi řídit přístup vzdáleného technika a jeho režim přístupu (Zobrazit nebo Ovládat) Pro povolení připojení vzdáleného technika musí místní technik pracující s platformou udělit přístup, který může kdykoli také zrušit, čímž si po celou dobu zachovává plnou kontrolu nad relací.
- **Velikost přenosu:** vzdálený technik může vidět původní velikost přenosu i aktuální velikost přenosu v pixelech. Je rovněž upozorněn, pokud je aktuální velikost přenosu menší než původní.
- **Stav myši a klávesnice:** vzdálený technik získává zpětnou vazbu o tom, zda myš a klávesnice lékařského zobrazovacího zařízení fungují správně.

- **Podrobnosti o relaci:** místní i vzdálení technici mají přístup k informacím o relaci.

1.3.7. Klinické přínosy

Systém nCommand Lite zlepšuje diagnostické zobrazování tím, že umožňuje vzdálené ovládání systémů **MRI, CT a PET/CT**, čímž zajišťuje konzistentní kvalitu snímků a dodržování protokolů. Umožňuje zkušeným technikům sledovat a asistovat při vyšetřeních v reálném čase, čímž optimalizuje efektivitu pracovního postupu a snižuje riziko chyb, které by mohly ovlivnit přesnost diagnostiky. Systém usnadňuje spolupráci mezi techniky, zlepšuje konzistenci vyšetření a umožňuje rychlejší rozhodování v komplikovaných případech. Díky možnosti vzdálené podpory více zařízeními zvyšuje **systém nCommand Lite dostupnost, rozmanitost a kvalitu** zobrazovacích vyšetření, čímž zajišťuje, že více pacientů má přístup k pokročilé diagnostice, a zároveň optimalizuje využití zdravotnických zdrojů. Kromě toho pomáhá zmírnit nedostatek personálu tím, že snižuje závislost na lokálních odbornících, a přitom zachovává dodržování přísných regulačních a bezpečnostních standardů pro data.

1.3.8. Zamýšlení uživatelé

- **Místní technik**

Místní technik je uživatel na místě, který je zodpovědný za osobní asistenci a vedení pacientů na zdravotnickém zařízení. Musí mít potřebné znalosti k provádění skenovacích postupů na daném lékařském zobrazovacím zařízení. Kromě toho řídí režim přístupu vzdáleného technika (Zobrazit nebo Ovládat), přičemž vzdálený přístup musí být udělen místním technikem prostřednictvím platformy a jej lze kdykoli zrušit.

- **Vzdálený technik**

Odborník, který provádí činnosti na dálku a má přístup k počítači zařízení a jeho ovládání. Stejně jako místní technik musí mít i vzdálený technik potřebné znalosti k provádění skenovacích postupů na daném lékařském zobrazovacím zařízení.

- **Uživatel podpory/IT**

Odborník odpovědný za nastavení platformy (není součástí této uživatelské příručky).

1.3.9. Provozní prostředí

Následující specifikace se vztahují na požadavky na prostředí počítače e-KVM.

- **Maximální nadmořská výška (bez přetlakování)**

- Provoz: Od 0 m (0 stop) do 3048 m (10 000 stop)
- Skladování: Od 0 m (0 stop) do 12192 m (40 000 stop)

- **Teplota**

- Provoz: 10 °C (50 °F) až 35 °C (95 °F)
- Skladování: -10 °C (14 °F) až 50 °C (122 °F)

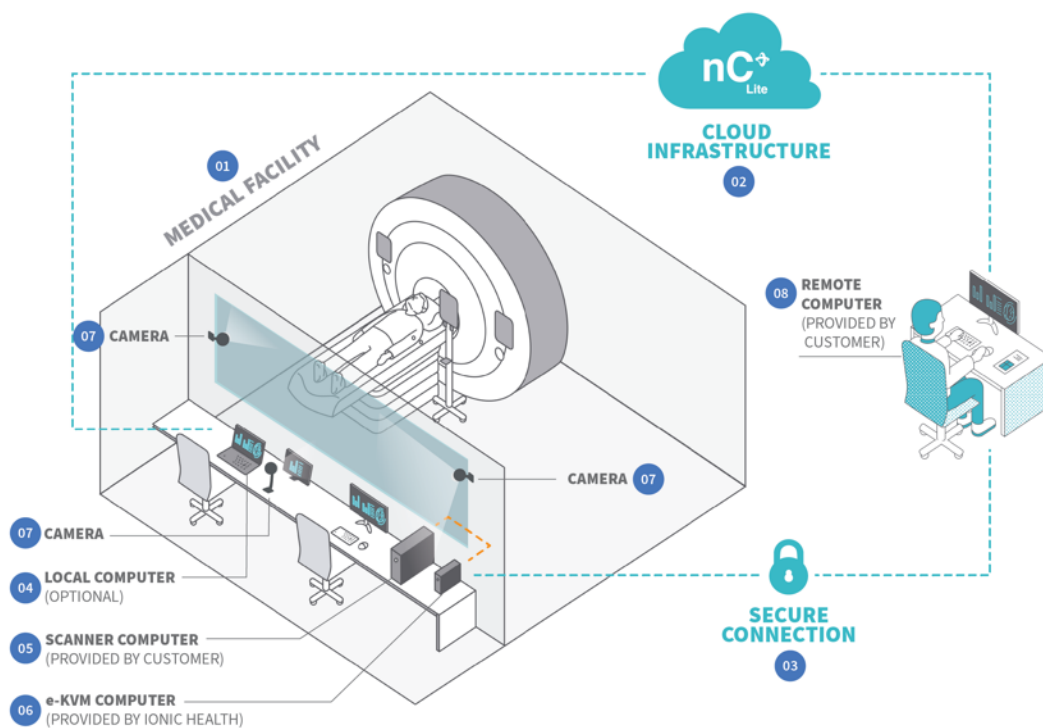
- **Relativní vlhkost**

- Provoz: 20 % až 80 % (bez kondenzace)
- Skladování: 10 % až 90 % (bez kondenzace)

1.3.10. Prostředí zařízení

Platforma nCommand Lite má dva různé typy prostředí:

- **Zobrazovací pracoviště:** Pracoviště provádějící vyšetření magnetickou rezonancí (MRI), počítačovou tomografií (CT) nebo pozitronovou emisní tomografií – počítačovou tomografií (PET/CT).
- **Vzdálené pracoviště:** Místo, kde vzdálení technici mohou přistupovat k zařízením a spravovat je na dálku (skenery MRI, CT nebo PET/CT). Tato stanice může být používána v různých prostředích, například v kancelářích, řídicích centrech, vzdálených lokalitách nebo dokonce na sekundárních pracovištích v rámci zdravotnického zařízení. Vzdálená stanice může být umístěna v jakémkoli prostoru, který uživatel poskytuje vhodné podmínky pro soustředění a splňuje minimální požadavky na připojení a konfiguraci počítače.



Obrázek 01: Přehled produktu a jeho propojení prostřednictvím zabezpečeného připojení (např. VPN).

01 – Lékařské zařízení; 02 – Cloudová infrastruktura; 03 – Zabezpečené připojení; 04 – Místní počítač (volitelné); 05 – Skener (poskytnutý zákazníkem); 06 – e-KVM (poskytnutý společností IONIC Health); 07 – Fotoaparát; 08 - Vzdálený počítač (poskytnutý zákazníkem)

**VAROVÁNÍ!****Kompatibilita vzdáleného skenování**

Společnost IONIC Health (IH) ověřuje funkčnost vzdáleného skenování na uvedených kompatibilních zařízeních. IH provádí kompletní hodnocení požadavků na vzdálené skenování a během instalace testuje systém v cílovém prostředí. Tím se zajišťuje kompatibilita a správná funkčnost systému pro vzdálené skenování v daném okamžiku. Toto ověření neznamená, že jsou v této konfiguraci splněny všechny požadavky výrobce původního zařízení (OEM). Za jakékoli odchylky od požadavků výrobce původního zařízení (OEM) odpovídá koncový uživatel.

Jakékoli úpravy systému nebo prostředí po instalaci musí být nahlášeny IH, aby byla ověřena pokračující kompatibilita. IH nemůže zaručit funkčnost ani převzít odpovědnost za konfigurace odlišné od těch, které byly ověřeny během instalace.

1.3.11. Minimální požadavky

- **Místní počítač**

Tento počítač používá **místní technik** k udělení a podpoře vzdáleného přístupu k zařízení prostřednictvím systému nCommand Lite®. Umožňuje také přímou komunikaci se **vzdáleným technikem** prostřednictvím chatovací funkce na platformě.

Minimální požadované technické specifikace jsou:

- Procesor: AMD® A4-9120C nebo vyšší, nebo podobný
- Paměť: 4 GB nebo více
- Úložiště: 128 GB SSD nebo vyšší
- Periferní zařízení: mikrofon a reproduktor, nebo náhlavní souprava a webkamera
- Monitor: 14" displej s rozlišením FHD (1920 x 1080) nebo vyšší
- Operační systém: Chrome OS, Windows OS nebo MAC OS
- Místo instalace: tento počítač musí být v blízkosti počítače skeneru
- IT rutinní úkony: Vytvořit zástupce nCommand Lite na ploše každého uživatele
- Kompatibilita s prohlížečem: Google Chrome nebo Microsoft Edge.

- **Vzdálená stanice**

Tato stanice slouží **vzdálenému technikovi** k přístupu a ovládání zařízení prostřednictvím systému nCommand Lite®. Vzdálená stanice musí navázat zabezpečené připojení k počítači e-KVM (poskytnutému společností IONIC HEALTH®).

Zákazník je odpovědný za zajištění vzdáleného počítače a rozhodne se pro jeden ze dvou scénářů: první je provoz 24/7 a druhý provoz během pracovní doby.

Pro každý scénář naleznete níže příslušné specifikace pro výběr modelů počítačů:

Scénář 1 (provoz 24/7) – Musí splňovat následující specifikace:

- Intel Xeon W-2223 (4 jádra, 8 vláken, 8,25 MB cache, 3,90 GHz Turbo) nebo vyšší.
- RAM: 16 GB nebo více.

- Grafika: NVIDIA RTX A2000 6GB nebo vyšší, nebo podobné.
- Úložiště: 128 GB SSD nebo vyšší.
- Operační systém: Windows 11 Pro 64B nebo vyšší.
- Minimální požadavky na monitor: Velikost 27", poměr stran 16:9, rozlišení 4k.
- Náhlavní souprava: BLACKWIRE 3200 nebo podobný.
- Kompatibilita prohlížeče: Google Chrome nebo Microsoft Edge.

Scénář 2 (provoz v pracovní době) – Musí splňovat následující specifikace:

- Intel® Core™ i7-12700k vPro® nebo vyšší.
- RAM: 16 GB nebo více.
- Grafika: NVIDIA T400 GB nebo vyšší, nebo podobné.
- Úložiště: 128 GB SSD nebo vyšší.
- Operační systém: Windows 11 Pro 64B nebo vyšší.
- Minimální požadavky na monitor: Velikost 27", poměr stran 16:9, rozlišení 4k.
- Náhlavní souprava: BLACKWIRE 3200 nebo podobný.
- Kompatibilita s prohlížečem: Google Chrome nebo Microsoft Edge.



VAROVÁNÍ!

Nesplnění vhodného nastavení a minimálních požadavků může vést ke snížené kvalitě nebo selhání komunikace mezi uživateli.

• Konfigurace sítě (minimální požadavky)

Pro navázání relace mezi vzdáleným uživatelem a počítačem e-KVM musí být zajištěna síťová komunikace mezi oběma zařízeními. Systém nCommand Lite využívá peer-to-peer (P2P) k navázání spojení mezi místním uživatelem, vzdáleným uživatelem a počítačem e-KVM. Existují tři kompatibilní scénáře:

- **Scénář 1** – firemní síť používající jeden z následujících protokolů: LAN, LAN-to-LAN, MPLS nebo VPN;
- **Scénář 2** – firemní síť, která využívá důvěryhodnou WAN (externí síť) a nepoužívá žádný z následujících protokolů: LAN, LAN-to-LAN, MPLS nebo VPN;
- **Scénář 3** – veřejná síť na straně vzdáleného počítače (vzdálený uživatel).

Konfigurace pro každý scénář jsou podrobně popsány v technické dokumentaci.

1.3.12. Symboly

Symbol	Popis	Odkaz
	Výrobce	ISO 15223-1, ISO 7000-3082
	Datum výroby	ISO 15223-1, ISO 7000-2497
	Symbol označuje, že tento produkt je zdravotnický prostředek	ISO 15223-1
	Jedinečný identifikátor zařízení	ISO 15223-1

	Referenční model	ISO 15223-1, ISO 7000-2493
	Dovozce	ISO 15223-1, ISO 7000-3725
	Nahlédněte do uživatelské příručky	ISO 15223-1, ISO 7000-1641
	Distributor	ISO 15223-1, ISO 7000-3724
	Upozornění	ISO 15223-1, ISO 7000-0434A
	Varování	ISO 7010-W001
	Sériové číslo <i>(nebo verze softwaru)</i>	ISO 15223-1, ISO 7000-2498
	Zplnomocněný zástupce v Evropském společenství	ISO 15223-1
	Švýcarský zplnomocněný zástupce (CH-REP)	ISO 15223-1
	CE – označení shody s evropskými předpisy; 2803 – označení oznámeného subjektu	Nařízení EU 2017/745

1.3.13. Životnost

Předpokládaná životnost produktu je 5 let, s přihlédnutím k životnosti komponent, z nichž je produkt složen. Toto komplexní hodnocení zajišťuje, že životnost každé klíčové komponenty odpovídá celkové předpokládané životnosti produktu, čímž je garantována konzistentní funkčnost a spolehlivost po celou dobu jeho určeného používání.

1.3.14. Upgrade / aktualizace

Společnost IONIC Health bude systém nCommand Lite aktualizovat v rámci plánované údržby nebo při vydávání aktualizací. Tyto aktualizace jsou navrženy tak, aby zajišťovaly pokračující výkon a spolehlivost, aniž by narušily aktuálně použitou verzi u zákazníků. V závislosti na typu aktualizace může být produkt aktualizován na dálku, nebo může být vyžadována návštěva servisního technika na místě.

Kapitola 2 Seznam obecných varování a bezpečnostních opatření



VAROVÁNÍ!

Před použitím systému nCommand Lite si prosím přečtete všechna níže uvedená varování.



UPOZORNĚNÍ

Systém nCommand Lite nelze opravovat ani provádět jeho údržbu během používání k ovládání zařízení MRI, CT nebo PET/CT za přítomnosti pacienta.

- Věnujte zvýšenou pozornost všem upozorněním systému, protože jsou zásadní pro bezpečný provoz.
- Při všech činnostech upřednostňujte bezpečnost a soustředění.
- Federální zákon stanovuje, že toto zařízení může být prodáváno pouze lékařem nebo na jeho předpis, a smí jej používat pouze zdravotnický technik s licenci ve státě, kde vykonává svou praxi.
- Systém nCommand Lite smí používat pouze technici, kteří absolvovali školení pro práci s platformou.
- Tento systém používejte pouze s kompatibilními webovými prohlížeči. Podporované prohlížeče jsou Google Chrome a Microsoft Edge.
- V případě nouzové situace musí na zobrazovacím pracovišti zůstat školený licencovaný technik, aby provedl vyšetření MRI, CT nebo PET/CT bez použití systému nCommand Lite.
- Současný přístup k více zařízením vyžaduje vysokou míru soustředění a komunikace s místními týmy.
- Vyhněte se současnému přístupu k zařízením se stejným uspořádáním nebo k vyšetřením stejné anatomické oblasti.
- Můžete zobrazovat více obrazovek, ale ovládání je možné pouze u jednoho zařízení současně.
- Při připojení k zařízení vždy zahajte chat pro zajištění jasné komunikace.
- Upozornění na hovory se zobrazují na obrazovce příslušného zařízení; současně může být aktivní pouze jeden hovor.
- Ověřte videokomunikaci při přístupu k aplikaci (před zahájením pracovní relace), abyste zkontrolovali případné selhání připojení videovýstupu u zařízení MRI, CT nebo PET/CT nebo u jakéhokoli zařízení souvisejícího s přenosem videa.
- Zařízení by nemělo být připojováno do zásuvky a/nebo do nepřerušitelného a stabilizovaného zdroje napájení prostřednictvím prodlužovacích kabelů nebo „zásuvkových lišt“.
- V případě poruchy videa zkontrolujte připojení videa mezi systémem zařízení a počítačem e-KVM.
- Pokud je aplikace při vzdáleném přístupu pomalá, obnovte stránku pomocí příkazu Ctrl+F5 v prohlížeči počítače vzdáleného technika. Pokud problém přetrvává, obraťte se na technickou podporu.
- Při každém obnovení stránky v prohlížeči se připojení k zařízení přeruší a je nutné znovu provést proces udělení přístupu.
- Nepřihlašujte se pomocí jiného prohlížeče, pokud jste již přihlášení.

- Zobrazovací pracoviště zákazníka musí mít záložní internetové připojení od jiného poskytovatele než je hlavní poskytovatel, aby bylo možné okamžitě přejít na záložní spojení v případě ztráty komunikace se systémem/platformou.
- V případě ztráty komunikace nebo zpomalení myši proveďte na stránce používané v prohlížeči „resynchronizaci myši“.
- Ujistěte se, že počítače používané pro ovládání systému nCommand Lite, jak na zobrazovacím pracovišti, tak v řídicím centru, splňují minimální požadavky; jinak může dojít ke snížení výkonu aplikace.
- Pro přenos platformy by měla být na hlavním i záložním připojení aplikována QoS (Quality of Service) a výkon připojení by měl být průběžně monitorován.
- Před použitím zkontrolujte úroveň hlasitosti reproduktorů a mikrofonu, stejně jako oprávnění pro přístup k zvuku a mikrofonu v prohlížeči.
- Před použitím zkontrolujte funkčnost klávesnice a myši; pokud jsou pomalé nebo nesynchronní, aktivujte tlačítko „resynchronizace myši“. Zkontrolujte, zda je počítač e-KVM připojen a zapnutý.
- Ujistěte se, že rozložení klávesnice ve vzdálené lokalitě odpovídá rozložení klávesnice na zobrazovacím pracovišti.
- Pokud je nutné změnit místo, kde je platforma používána, musí zákazník kontaktovat technickou podporu pro provedení nové instalace. Nepřeinstalovávejte systém, aniž byste kontaktovali technickou podporu.
- Před zahájením procesu vzdáleného přístupu k zařízení MRI, CT nebo PET/CT je důležité, aby týmy techniků zkontrolovaly všechny položky nezbytné pro správný chod platformy, aby nedošlo k omezení průběhu vyšetření. Tyto položky jsou uvedeny v dokumentu „Kontrolní seznam před zahájením služby“.
- Konfigurace firewallu na zobrazovacím pracovišti musí být kontrolována měsíčně s IT týmem, přičemž je nutné ověřit, že nedochází k žádným problémům s povolením firewallu, které by mohly ohrozit používání systému nCommand Lite.
- Jakákoli odchylka zaznamenaná při používání aplikace musí být okamžitě nahlášena podpůrnému týmu před zahájením přístupu, nebo musí být přístup přerušen, pokud již byl zahájen.
- Aplikaci by měli obsluhovat pouze licencovaní technici, kteří absolvovali školení pro používání systému nCommand Lite.
- Vzdálený přístup prostřednictvím platformy nenahrazuje ani nekonkuruje žádnému jinému provoznímu postupu pro zařízení MRI, CT nebo PET/CT, který stanovuje výrobce lékařského zařízení nebo protokoly a postupy zdravotnického zařízení.
- Vyvarujte se ohýbání nebo natahování hardwarových kabelů.
- V případě problémů s hlasovou nebo chatovou komunikací použijte funkci telefonního hovoru k navázání spojení mezi místním technikem na zobrazovacím pracovišti a vzdáleným technikem v řídicím centru. Řiďte se pokyny uvedenými v části „Pokyny v případě poruchy“ a v případě potřeby kontaktujte technickou podporu pro provedení opravy.
- Pokud je nutné vyměnit počítač nebo jiné zařízení, které přímo ovlivňuje instalaci systému nCommand Lite, kontaktujte technickou podporu, aby byla zajištěna kontinuita provozu systému.
- Současně může k zařízení MRI, CT nebo PET/CT přistupovat na dálku pouze jedna osoba.
- Nedotýkejte se žádných fyzických video kabelů, pokud je počítač zařízení a systém nCommand Lite zapnutý.
- Při přístupu k dalšímu zařízení se otevře nová záložka. Tuto záložku přetáhněte na druhý monitor, protože systém je navržen tak, aby pro každé zařízení byla použita samostatná obrazovka.

- Jakákoli závažná událost související s používáním tohoto zařízení by měla být nahlášena jak výrobcí, tak zdravotnímu úřadu/příslušnému orgánu ve státě, kde je zařízení instalováno (*podrobnosti viz kapitola Servisní kanály*).

Kapitola 3 Použití platformy v každé lokalitě

Oddíl 3.1 - Přístup a používání systému nCommand Lite



VAROVÁNÍ!

V případě jakýchkoli problémů kontaktujte technickou podporu, která vám poskytne pomoc.



VAROVÁNÍ!

Zkontrolujte rozložení klávesnice a ujistěte se, že je totožné na obou místech (pracoviště a vzdálené pracoviště). Různá rozložení klávesnice mohou ztížit práci uživatele.

Tato kapitola poskytuje vše, co potřebujete vědět, abyste získali přístup k platformě nCommand Lite a mohli ji začít používat. Naleznete zde jednoduché, krok za krokem vedené pokyny, jak se přihlásit, orientovat v rozhraní a porozumět hlavním funkcím. Ať už pracujete na místě, nebo na vzdáleném pracovišti, tato příručka vám pomůže začít rychle a s jistotou.

Změna jazyka - Systém je ve výchozím nastavení nastaven na angličtinu, ale jazyk si můžete snadno změnit podle svých preferencí. Na přihlašovací obrazovce klikněte v pravém horním rohu na položku, kde je uvedeno „English (en-US)“. Otevře se rozevírací seznam dostupných jazyků, ze kterého si můžete vybrat.

Po přihlášení můžete jazyk změnit také kliknutím na aktuálně zvolený jazyk vpravo na horní liště. Otevře se rozevírací seznam dostupných jazyků, ze kterého si můžete vybrat.

Upozorňujeme, že pokud změníte jazyk během připojení k zařízení, aktuální spojení bude automaticky ukončeno a bude nutné se znovu připojit.

Při přístupu k platformě si můžete na přihlašovací obrazovce zvolit preferovaný jazyk. Některé zprávy zobrazované během přihlašování se však mohou objevit v jazyce nastaveném ve vašem webovém prohlížeči, a to bez ohledu na jazyk zvolený na platformě. Aby bylo používání platformy jednodušší, doporučujeme nastavit jazyk prohlížeče stejný jako jazyk platformy.

Oddíl 3.2 - První přihlášení k platformě

Přihlášení do platformy lze provést dvěma způsoby: přes nCommand Lite nebo přes externí poskytovatele identity (External IdP). Uživatel se může přihlásit pomocí jednoho z předem nastavených způsobů. Pokud je nastavený způsob přihlášení přes externího poskytovatele identity (External IdP), metoda nCommand Lite nebude fungovat, a naopak. Pro přihlášení přes External IdP přejděte přímo na **podkapitolu 3.2.2**.

3.2.1. Přihlášení přes nCommand Lite

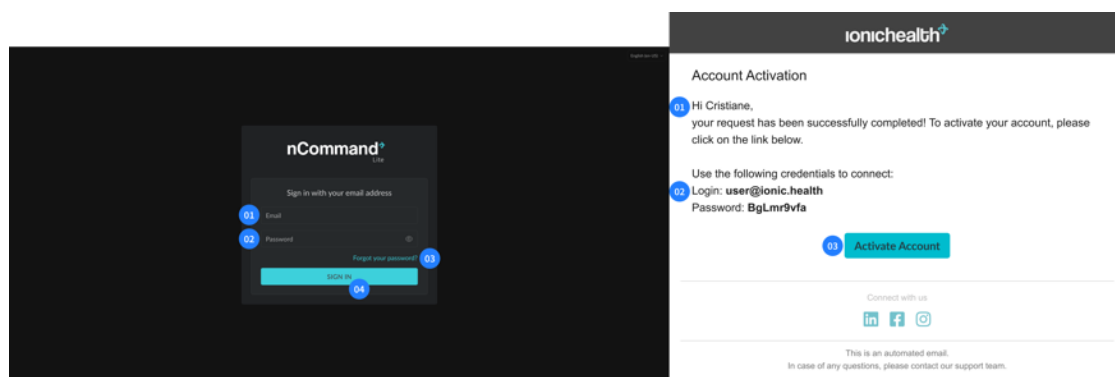
Poznámka: Tato část se nevztahuje na uživatele, kteří se přihlašují přes externího poskytovatele identity (External IdP).

Zapněte počítač a poklepejte na ikonu zástupce nCommand Lite, která se obvykle nachází na ploše. Platformu můžete také otevřít přímo zadáním URL do prohlížeče.

První přístup je zásadní krok pro bezpečné a efektivní používání platformy. Toto byste měli vědět:

1 - Uvítací e-mail: Obdržíte e-mail s přihlašovacími údaji, včetně vaší osobní e-mailové adresy, dočasného hesla a přímého odkazu na klientskou platformu. Tento e-mail je nezbytný pro zahájení práce na platformě nCommand Lite.

2 - Vytvoření hesla: Po otevření odkazu budete muset zadat svou registrovanou e-mailovou adresu a heslo, které jste obdrželi v uvítacím e-mailu. Po kliknutí na „Přihlásit se“ budete přesměrováni na stránku pro vytvoření nového hesla. Musíte zadat staré heslo, nové heslo a potvrzení nového hesla. Heslo musí být silné a bezpečné, obsahovat alespoň 3 z následujících položek: malé písmeno, velké písmeno, číslici a symbol, a mít minimálně 8 znaků. Po kliknutí na „Pokračovat“ budete přesměrováni na stránku, kde znovu potvrdíte svou e-mailovou adresu. Po kliknutí na „Pokračovat“ budete nyní přesměrováni na domovskou obrazovku, která je přizpůsobena vašemu konkrétnímu uživatelskému profilu.



Obrázek 02: První přístup

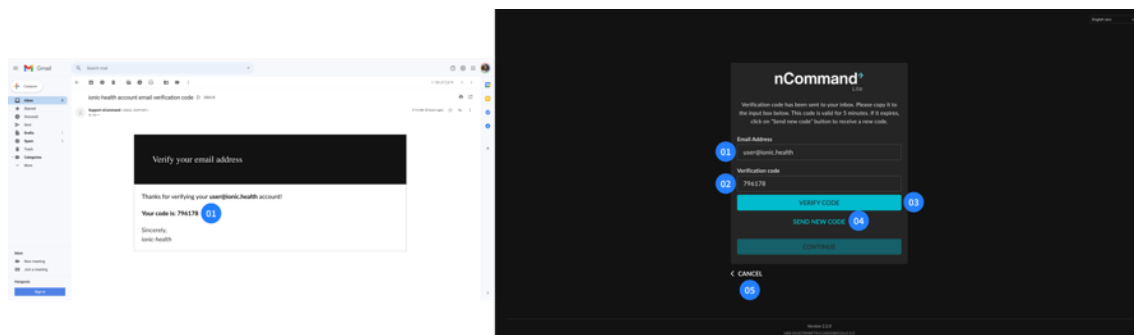
Vlevo – Přihlašovací stránka: 01– E-mailová adresa; 02 – Heslo; 03 – "Zapomněli jste heslo?"; 04 – Tlačítko přihlásit
Vpravo – Uvítací e-mail: 01 – Text e-mailu pro aktivaci účtu; 02 – Přihlašovací údaje; 03 – Tlačítko Aktivní účet

Tento úvodní postup je navržen tak, aby od začátku zajistil maximální bezpečnost vašeho účtu. Od druhého přihlášení bude proces zjednodušen, ale stejně bezpečný – při každém přihlášení vám bude na registrovaný e-mail zaslán kód pro dvoufaktorové ověření, který zajistí neustálou bezpečnost vašeho účtu.

Po přihlášení do nCommand Lite vás systém automaticky přesměruje na domovskou obrazovku, která je přizpůsobena vašemu konkrétnímu uživatelskému profilu. Ať už jste místní nebo vzdálený technik, rozhraní je navrženo tak, aby vyhovovalo potřebám a přístupovým právům vaší role. Tento intuitivní design zajišťuje, že od okamžiku přihlášení budete mít k dispozici všechny nástroje a informace potřebné pro efektivní a snadné používání.

Poznámka: Pokud je způsob přihlášení nastaven na nCommand Lite, musí být přihlášení vždy provedeno touto možností. I když se na přihlašovací obrazovce zobrazí tlačítko pro externího poskytovatele identity (External IdP), pro tyto uživatele nebude funkční. Každý uživatelský účet je na platformě registrován s konkrétní metodou ověření - buď přihlašovacími údaji nCommand Lite nebo službou Externího poskytovatele identity. Pokud se uživatel pokusí

přihlásit jiným způsobem, než který je přiřazen k jeho účtu, systém zobrazí chybovou zprávu, že účet není autorizován pro tento typ ověření.



Obrázek 03: Dvoufaktorové ověření (2-FA)

Vlevo – E-mail: 01 – 2-FA Kód

Vpravo – Stránka dvoufaktorového ověření: 01 – E-mailová adresa; 02 – Ověřovací kód; 03 – Potvrdit tlačítko ověřovacího kódu; 04 – Odeslat nový kód; 05 – Zrušit

3.2.2. Přihlášení přes External IdP

V některých případech se mohou uživatelé přihlásit na platformu přes externího poskytovatele identity (External IdP), který jim umožňuje využít stávající autentizační službu jejich organizace, mechanismus také známý jako Single Sign-On (SSO). Tímto způsobem předem registrovaný uživatel neobdrží uvítací e-mail. Místní IT oddělení musí zkontrolovat kompatibilitu, nastavit způsob přihlášení a informovat uživatele, který e-mail (External IdP) má být použit.

Když je tato možnost dostupná, musí se uživatel vždy přihlásit pomocí externího poskytovatele identity (External IdP) (např. Amazon Cognito, Microsoft Entra ID, Microsoft AD B2C). Metoda přihlášení přes nCommand Lite nebude pro uživatele External IdP dostupná.

Pro přihlášení pomocí External IdP klikněte na tlačítko s názvem IdP a řiďte se pokyny poskytovanými externím autentizátorem. Pokud má vaše instituce integrováno více než jedno External IdP, ujistěte se, že potvrzujete poskytovatele, u kterého jste registrováni. Uvedení jiných poskytovatelů nebude fungovat. Pokud máte jakékoli dotazy nebo narazíte na problémy, obraťte se na své lokální IT oddělení.

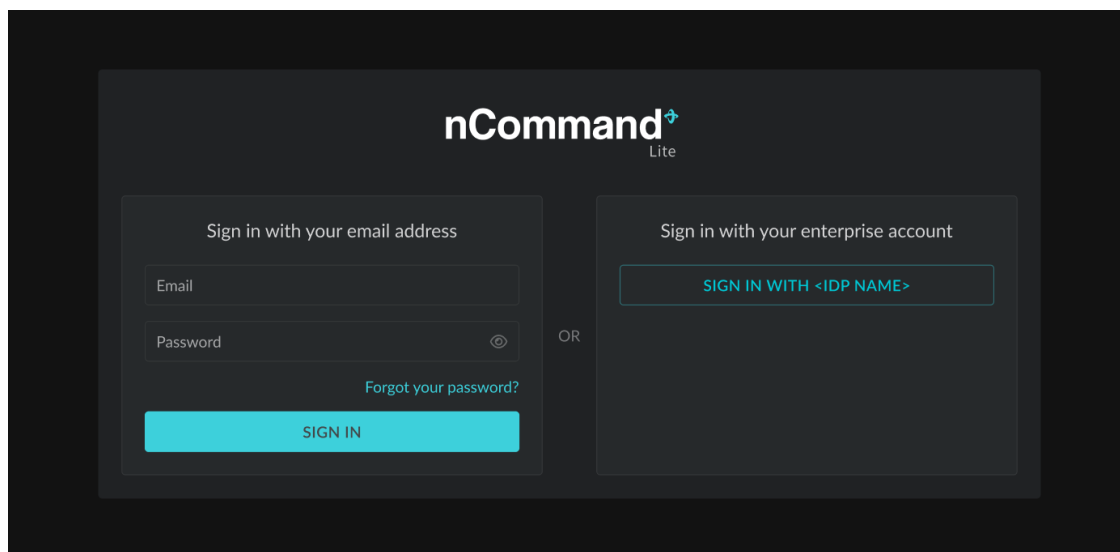
V případech, kdy uživatelé sdílí stejný počítač a používají Single Sign-On (SSO), se doporučuje, aby každý uživatel při přihlášení přes External IdP (je-li tato možnost k dispozici) zvolil možnost „zůstat přihlášen“ nikoli, nebo aby se po odhlášení z nCommand Lite odhlásil i z externího poskytovatele.

U této možnosti přihlášení je celý proces přihlášení a odhlášení – včetně vytváření a vypršení hesla, vícefaktorového ověřování (MFA) a zablokování účtu – plně spravován IT oddělením klienta, které nakonfigurovalo External IdP.

Při přihlašování přes External IdP musí být funkce „Zapomněli jste heslo“ a „Změnit heslo“ prováděny podle postupu External IdP.

Poznámka: Na přihlašovací obrazovce se i nadále zobrazí možnost „Zapomněli jste heslo“, ale pro tyto uživatele nebude funkční. Může vás nasměrovat na další kroky procesu, ale proces nebude dokončen. Pokud potřebujete obnovit heslo, řiďte se pokyny svého External IdP.

Důležité: I při použití External IdP musí být uživatel předem registrován na platformě nCommand Lite, aby získal přístup.



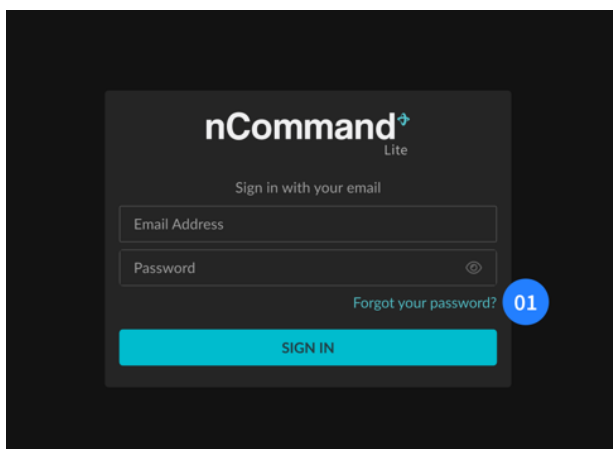
Obrázek 04: Ukázka přihlašovací obrazovky přes External IdP

Oddíl 3.3 - Správa hesel

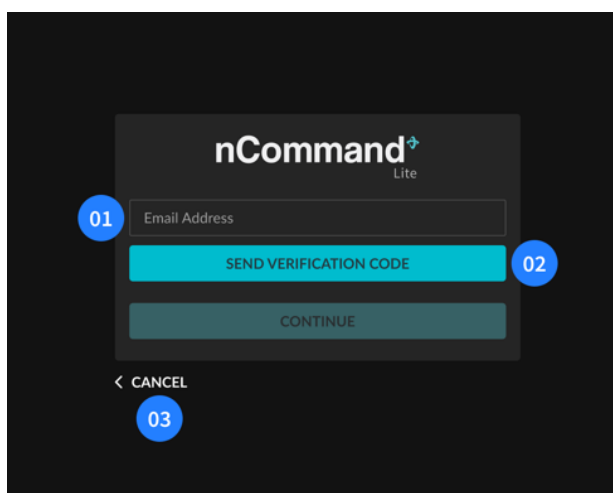
Po prvním přístupu k platformě si uživatel může změnit své heslo nebo, pokud ho zapomněl, nastavit nové heslo.

Poznámka: Při přihlašování přes External IdP musí být funkce **Zapomněli jste heslo** a **Změnit heslo** prováděny podle postupu External IdP.

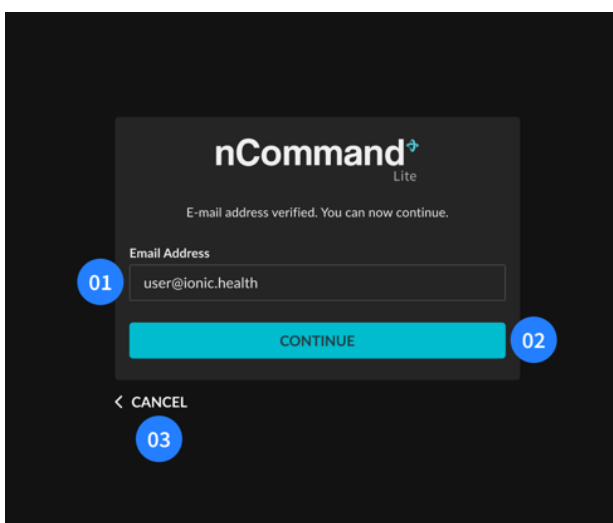
- **Obnovit heslo:** Umožňuje uživatelům obnovit přístup k účtu v případě, že zapomenou své heslo. Jednoduše klikněte na odkaz „Zapomněli jste heslo?“ na přihlašovací stránce, zadejte svou registrovanou e-mailovou adresu a odešlete údaje. Systém vám následně pošle e-mail s ověřovacím kódem. Po zadání kódu a kliknutí na „Ověřit kód“ budou uživatelé vyzváni k potvrzení registrované e-mailové adresy. Po kliknutí na „Pokračovat“ jsou uživatelé přesměrováni na stránku, kde mohou zadat nové heslo a jeho potvrzení. Pokud nové heslo splňuje požadavky systému, uživatelé jej mohou úspěšně zaregistrovat a následně se přihlásit s aktualizovanými přihlašovacími údaji.



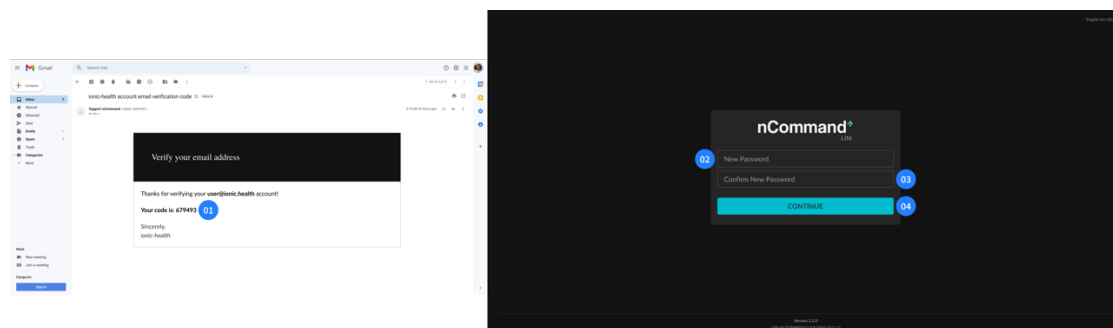
Obrázek 05: Odkaz na stránku pro resetování hesla
01 – Zapomněli jste heslo?



Obrázek 06: Stránka pro obnovu hesla
01 – E-mailová adresa; 02 – Odeslat ověřovací kód; 03 – Zrušit

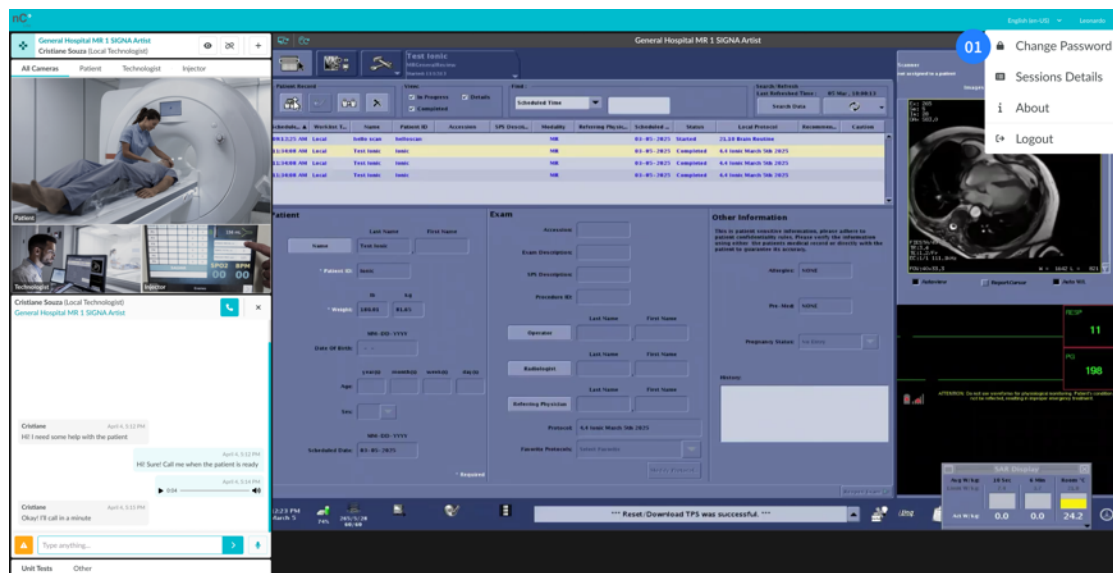


Obrázek 07: E-mailové potvrzení
01 – E-mailová adresa; 02 – Tlačítko Pokračovat; 03 – Zrušit

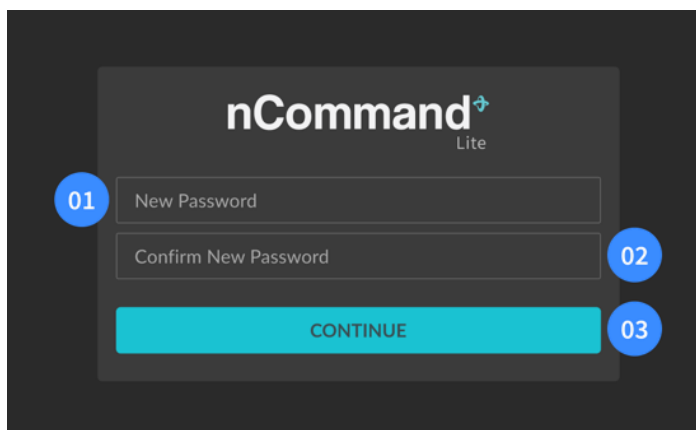


Obrázek 08: E-mail s kódem pro registraci nového hesla (vlevo) – 01 – 2-FA kód
Stránka Změna hesla (vpravo) – 02 – Nové heslo; 03 – Potvrdit nové heslo; 04 – Tlačítko Pokračovat

- Změnit heslo:** Umožňuje uživatelům změnit heslo podle stanovených kritérií – musí obsahovat alespoň tři z následujících prvků: malé písmeno, velké písmeno, číslici a symbol, a mít délku minimálně 8 znaků. Systém ověřuje, zda nové heslo splňuje tato kritéria, a pokud ne, upozorní uživatele zprávou. Kromě toho musí uživatelé nové heslo potvrdit, aby se předešlo chybám při zadávání. Pro změnu hesla musí uživatel po přihlášení kliknout na ikonu v pravém horním rohu a zvolit možnost „Změnit heslo“. Bude odhlášen z platformy a přesměrován na stránku pro potvrzení přiřazeného e-mailu. Systém vám následně pošle e-mail s ověřovacím kódem. Po vyplnění kódu a kliknutí na „Ověřit kód“ jsou uživatelé přesměrováni na obrazovku, kde mohou zadat nové heslo.



Obrázek 09: Položka rozbalovací nabídky pro změnu hesla
01 – Změna hesla



Obrázek 10: Stránka pro změnu hesla
 01 – Nové heslo; 02 – Potvrdit nové heslo; 03 – Tlačítko Pokračovat

Oddíl 3.4 - Přístup s profilem místního technika



VAROVÁNÍ!

Před použitím platformy kontaktujte vzdáleného technika telefonicky.



VAROVÁNÍ!

Aby nedošlo k přehřátí, neumísťujte žádné předměty před chladič e-KVM počítače, a abyste předešli poškození, nepokládejte na něj žádné předměty.



VAROVÁNÍ!

Během vzdálených sezení je místní technik zodpovědný za dodržování a prosazování místních bezpečnostních pravidel pro každý typ vyšetření a jeho specifické požadavky. Vždy zůstaňte přítomni v řídicí místnosti a/nebo vyšetřovací místnosti, aby byla zajištěna bezpečnost pacienta i zapojených odborníků.



VAROVÁNÍ!

Pohyby stolu během sezení smí provádět pouze místní technik, a to pouze na pokyn systému. Před odchodem z operačního sálu musí místní technik vždy odebrat přístup vzdálenému technikovi.



VAROVÁNÍ!

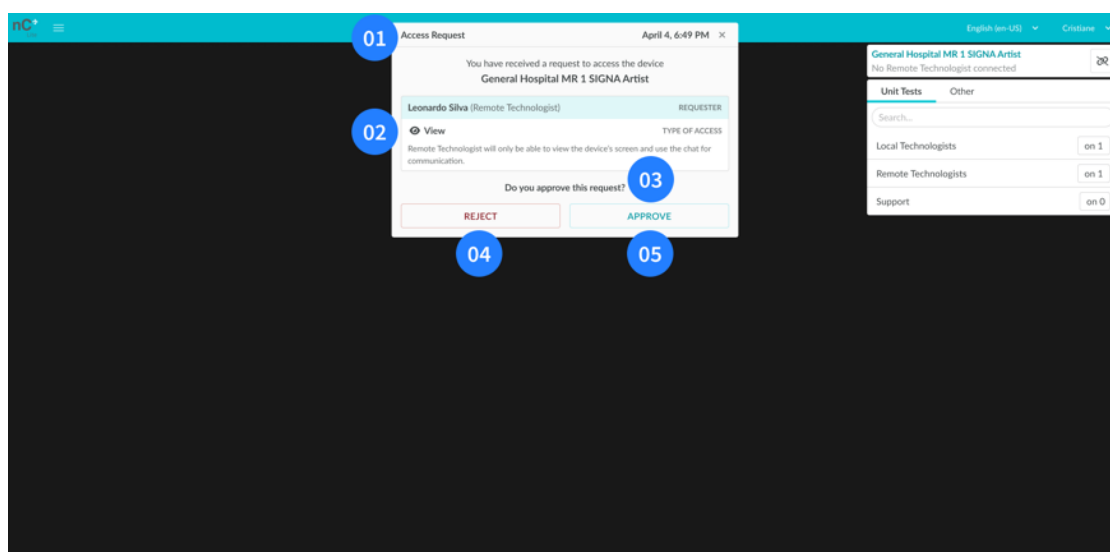
K přesunutí stolu za účelem umístění pacienta do zařízení a k jeho bezpečnému uvolnění je oprávněn pouze místní technik. Před odchodem z operačního sálu musí místní technik vždy odebrat přístup vzdálenému uživateli.

Po přihlášení do platformy vyberte požadované zařízení v poli Výběr zařízení. Za toto zařízení budete nést odpovědnost vy, takže můžete zkontrolovat žádost vzdáleného technika o přístup k zařízení. Když bude chtít vzdálený technik získat přístup k zařízení, zobrazí se vyskakovací okno, ve kterém můžete před udělením nebo zamítnutím přístupu zkontrolovat všechny uvedené informace. Buďte ve střehu ohledně příchozí žádosti od vzdáleného technika. Je nesmírně důležité pečlivě zkontrolovat každý detail. V případech, kdy poskytnuté informace nejsou rozpoznány, nepovolujte přístup.

Vzdálený technik může k zařízení přistupovat jedním ze dvou režimů přístupu: **Ovládat** nebo **Zobrazit**:

- **Režim Ovládat** – umožňuje vzdálenému technikovi ovládat myš a klávesnici a zároveň sledovat přenos ze zařízení. Místní technik však neztrácí kontrolu nad místní myší a klávesnicí a může kdykoli převzít řízení.
- **Režim Zobrazit** – umožňuje vzdálenému technikovi pouze sledovat obrazovku zařízení a používat chat pro komunikaci.

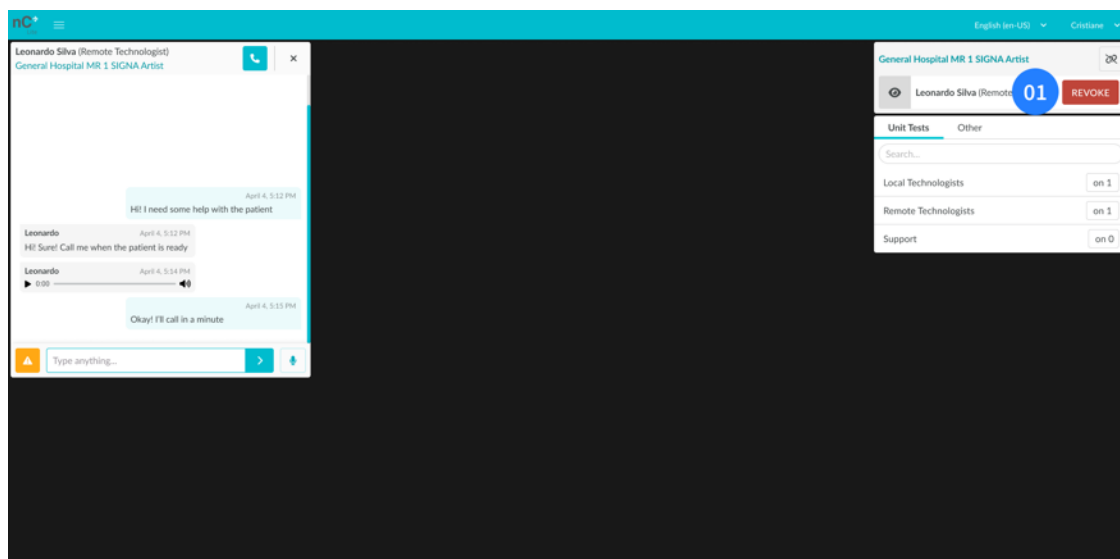
Po výběru zařízení má uživatel přístup k funkci chatu, která umožňuje komunikaci prostřednictvím textových zpráv, zvukových zpráv, hlasového hovoru a videohovoru s ostatními uživateli.



Obrázek 11: Hlavní obrazovka místního technika s upozorněním na žádost o přístup

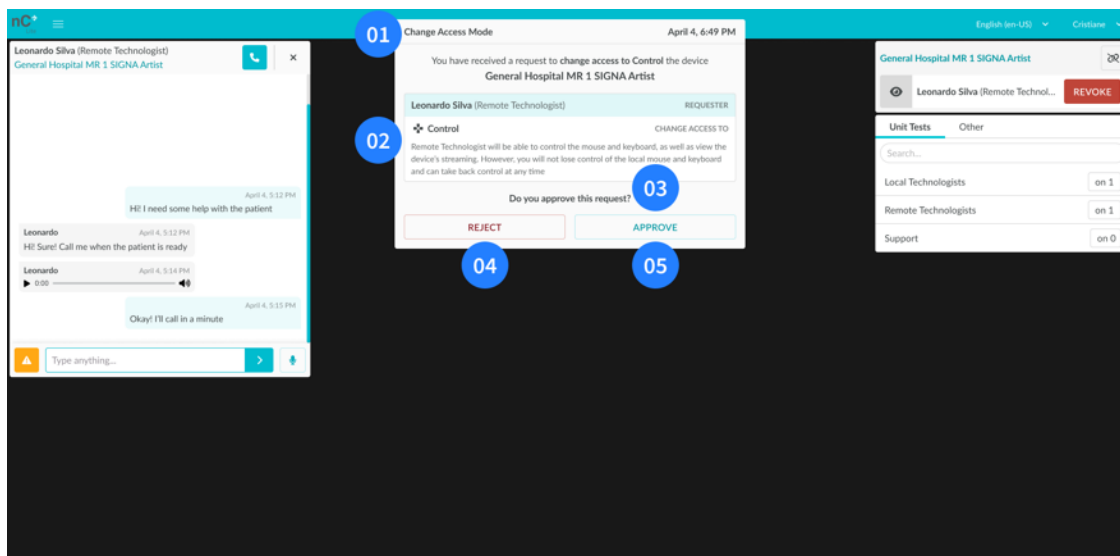
01 – Název (Žádost o přístup); **02** – Jméno žadatele, role a popis typu přístupu;
03 – Výzva: „Schvalujete tuto žádost?“; **04** – Tlačítko Zamítnout; **05** – Tlačítko Schválit

Po schválení může místní technik kdykoli odebrat přístup vzdálenému technikovi jednoduchým kliknutím na tlačítko ODEBRAT.



Obrázek 12: Hlavní obrazovka místního technika při připojení k zařízení
01 – Tlačítko Odebrat

Během vzdálené relace může vzdálený technik požádat o změnu režimu přístupu. Na obrazovce se zobrazí vyskakovací okno s žádostí. Můžete ji schválit nebo zamítnout. Mějte na paměti oprávnění, která každý režim přístupu vzdálenému technikovi umožňuje.



Obrázek 13: Hlavní obrazovka místního technika s požadavkem na změnu režimu přístupu
01 – Název (Změnit režim přístupu); 02 – Jméno žadatele, role a popis typu přístupu;
03 – Výzva: „Schvalujete tuto žádost?“; 04 – Tlačítko Zamítnout; 05 – Tlačítko Schválit



VAROVÁNÍ!

V případě ztráty připojení na místním počítači má vzdálený technik stále přístup k zařízení. **Okamžitě** kontaktujte vzdáleného technika a požádejte ho o **odpojení NEBO** se přihlaste na jiný počítač a **odeberte přístup** vzdáleného technika NEBO **stiskněte tlačítko napájení** a vypnete počítač e-KVM.

**VAROVÁNÍ!****V případě údržby skeneru:**

Než servisní inženýr zahájí jakékoli zásahy (na zařízení nebo v řídicí místnosti), informujte vzdáleného technika a odeberte jeho přístup kliknutím na tlačítko ODEBRAT PŘÍSTUP. Poté se odhlaste z platformy nCommand Lite.

Pokud není připojen žádný vzdálený technik, odhlaste se z platformy nCommand Lite před zahájením údržby.

Oddíl 3.5 - Přístup s profilem vzdáleného technika**VAROVÁNÍ!**

Uživatelské jméno a root heslo počítače zařízení: obě musí mít k dispozici místní hostitel, který přivítá instalační tým.

**VAROVÁNÍ!**

Pohyby stolu během sezení smí provádět pouze místní technik, a to pouze na pokyn systému. Před odchodem z operačního sálu musí místní technik vždy odebrat přístup vzdálenému technikovi.

**VAROVÁNÍ!**

K přesunutí stolu za účelem umístění pacienta do zařízení a k jeho bezpečnému uvolnění je oprávněn pouze místní technik. Před odchodem z operačního sálu musí místní technik vždy odebrat přístup vzdálenému uživateli.

**VAROVÁNÍ!**

Vždy sledujte situaci v místnosti prostřednictvím videokamery a před zahájením jakýchkoli činností zajistěte komunikaci s místním technikem.

**VAROVÁNÍ!**

V případě ztráty připojení na místním počítači okamžitě kontaktujte místního technika a odpojte se.

**VAROVÁNÍ!****V případě údržby skeneru:**

Po upozornění na zahájení údržby zařízení se ujistěte, že místní technik odebral přístup, a odhlaste se z platformy nCommand Lite. Pokud přístup nebyl odebrán, odhlaste se z platformy nCommand Lite a okamžitě kontaktujte místního technika, abyste jej informovali.

**VAROVÁNÍ!**

Pro vzdálené ovládání myši a klávesnice musí být zvolen režim přístupu Ovládat v režimu Zobrazit může vzdálený technik pouze sledovat přenos a lokální kamery.

**VAROVÁNÍ!**

Pokud odpověď na vaši žádost trvá déle, než je obvyklé, kontaktujte místního technika prostřednictvím chatu nebo telefonu.

Pracoviště vzdáleného technika zahrnuje vybavení, jako je počítač, monitory (obvykle tři), myš, klávesnice a náhlavní souprava.

V rámci klinického pracovního procesu mají místní technici přímý kontakt s pacientem. Odpovídají za interakci s pacientem, jeho polohování a zajištění bezpečnosti a dodržování protokolů během vyšetření MRI, CT nebo PET/CT v souladu s interními a regulačními normami.

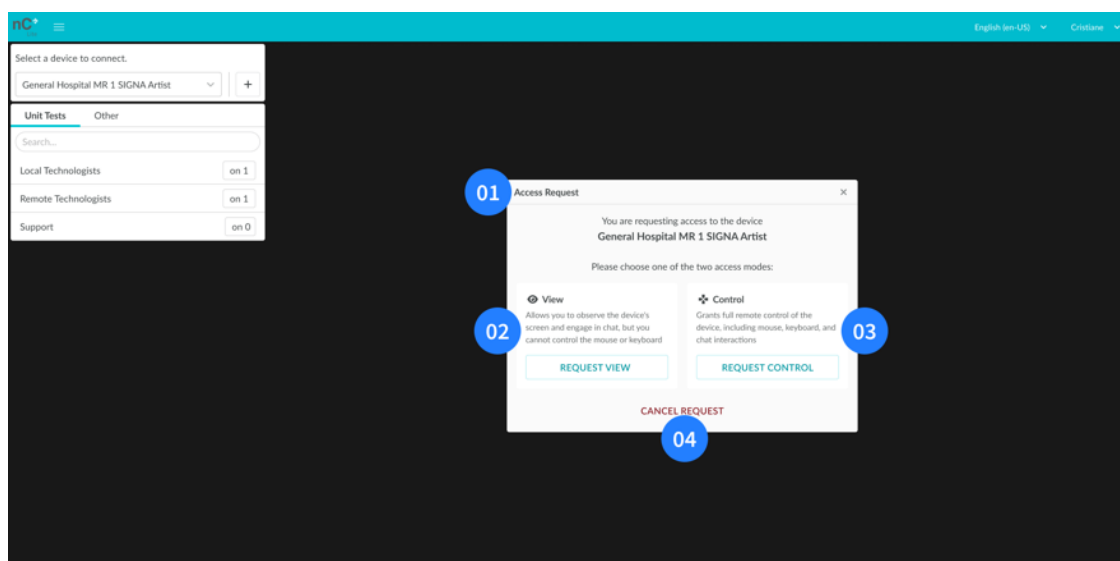
3.5.1. Režim přístupu

Po přihlášení do platformy vyberte v poli Výběr zařízení to zařízení, ke kterému se chcete připojit. Otevře se vyskakovací okno, ve kterém vyberte režim přístupu **Ovládat** nebo **Zobrazit**:

- **Režim Ovládat** – v tomto režimu je kromě sledování obrazovky povoleno také ovládání myši a klávesnice. Místní odborníci si zachovávají plný přístup k místní myši a klávesnici a mohou kdykoli převzít kontrolu.
- **Režim Zobrazit** – je možné pouze sledovat obrazovku zařízení a používat chat pro komunikaci.

Po výběru režimu přístupu se zobrazí pole Čeká na schválení, které signalizuje, že je potřeba schválení od připojeného místního technika pro pokračování. Tento místní technik má plnou pravomoc schvalovat nebo zamítat přístup a v případě potřeby kdykoli odebrat přístup. Toto opatření je nezbytné pro zajištění přísné kontroly a udržení bezpečnosti při používání zařízení.

Po výběru zařízení má uživatel přístup k funkci chatu, která umožňuje komunikaci s ostatními uživateli prostřednictvím textových zpráv, zvukových zpráv, hlasového hovoru a videohovoru. Pro přístup k chatu není potřeba schválení uživatele.



Obrázek 14: Dialogové okno žádosti o přístup pro vzdáleného technika

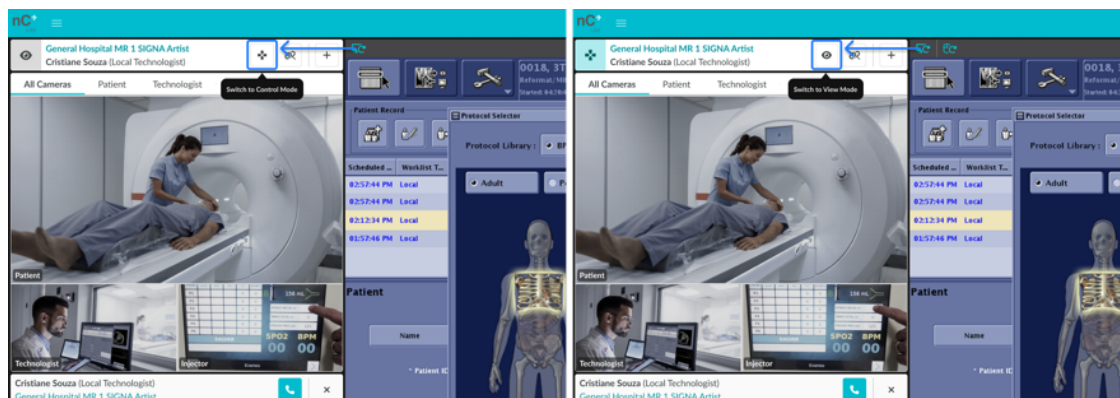
01 – Název (Žádost o přístup); **02** – Popis režimu Zobrazit a tlačítko Požádat o zobrazení; **03** – Popis režimu Ovládat a tlačítko Požádat o ovládání; **04** – Zrušit žádost

Jakmile místní technik schválí přístup k zařízení, rozhraní vzdáleného technika se aktualizuje a zobrazí živý přenos ze zařízení a jeho přidružených kamer. Pokud je vybraný režim přístupu Ovládat, bude aktivována možnost vzdáleného ovládání zařízení.

Tento postup zajišťuje efektivní a bezpečnou interakci, umožňující bezpečné vzdálené používání zařízení, aniž by byla ohrožena jeho integrita nebo bezpečnost pacienta.

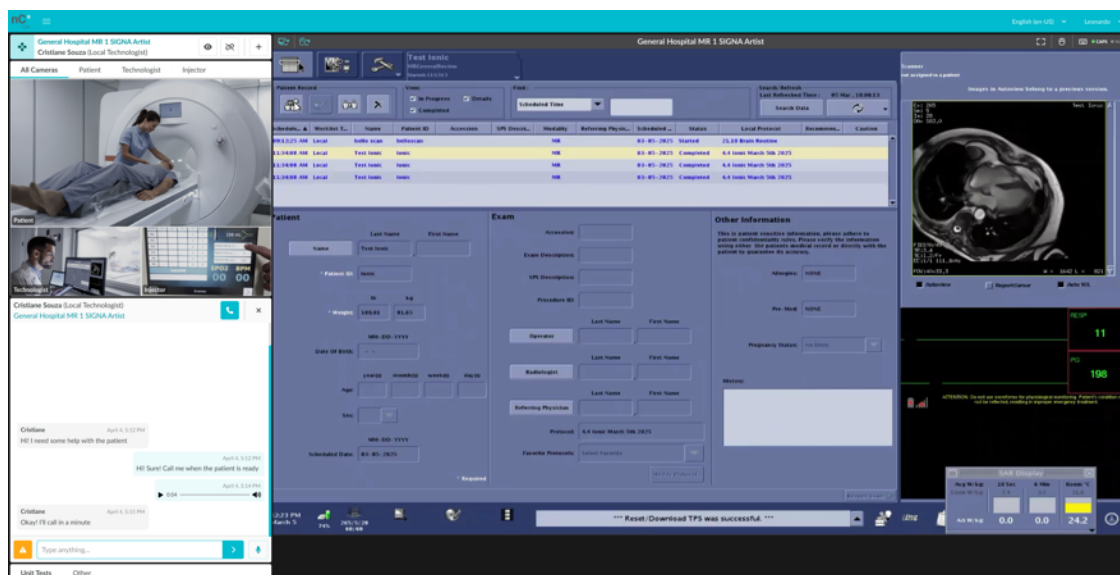
Chcete-li během vzdálené relace požádat o změnu režimu přístupu, klikněte na příslušnou ikonu. Místní technik může žádost schválit nebo zamítnout:

- **Schválit** – přenos se znovu načte, ale obsah chatu nebude ztracen. Pokud máte hlasový hovor nebo videohovor, relace skončí a bude ji muset znovu spustit jeden z uživatelů.
- **Zamítnout** – zobrazí se vyskakovací okno informující o zamítnutí místním technikem a aktuální přístup zůstane aktivní



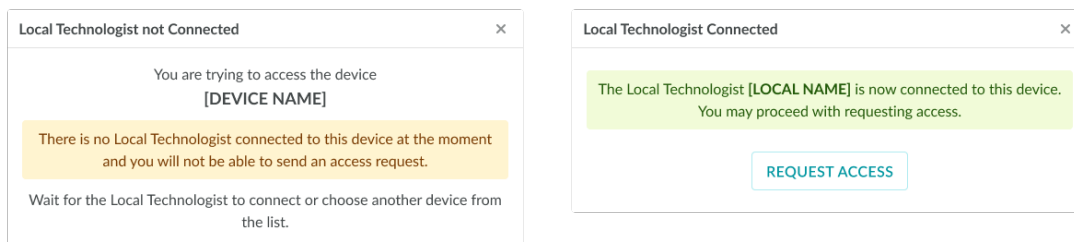
Obrázek 15: Změnit režim přístupu

Vlevo – Přepnout na ikonu a nápovědu v režimu Ovládat / **Vpravo** – Přepnout na ikonu a nápovědu v režimu Zobrazit



Obrázek 16: Hlavní obrazovka vzdáleného technika při připojení k zařízení

Když vzdálený technik žádá o přístup a k zařízení není připojen žádný místní technik, platforma zobrazí varovné vyskakovací okno. Jakmile se místní technik připojí, platforma informuje vzdáleného technika, že může znovu požádat o přístup.



Obrázek 17: Upozornění vzdáleného technika ohledně stavu připojení místního technika

Vlevo – Oznámení informující, že byl proveden pokus o přístup k zařízení, ale v současnosti není připojen žádný místní technik.

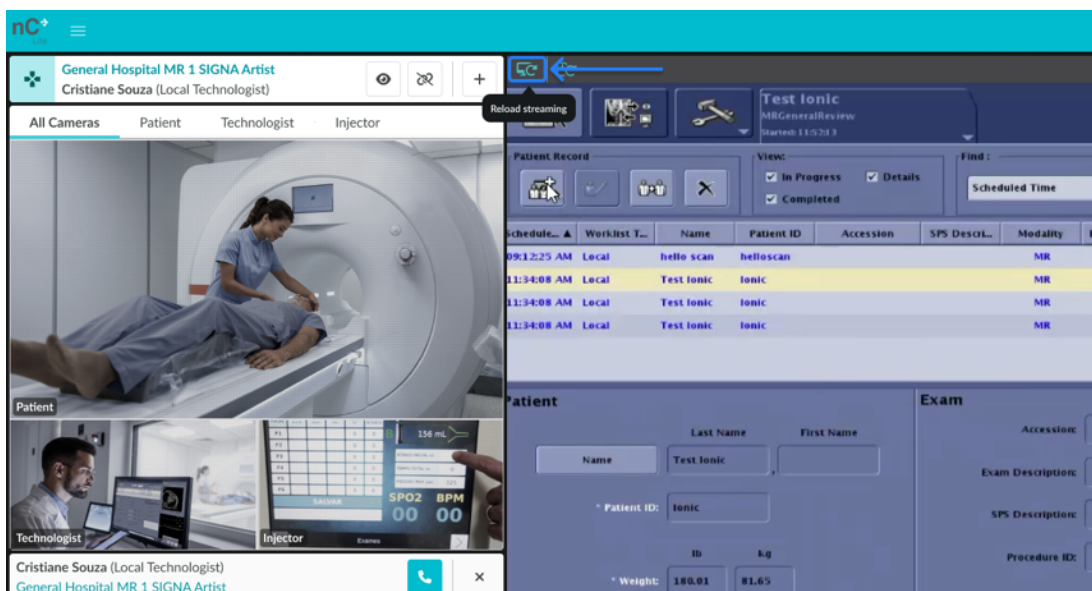
Vpravo – Oznámení potvrzující, že místní technik se připojil k zařízení poté, co předtím nebyl připojen.

3.5.2. Panel přenosu

Panel přenosu zobrazuje klíčové informace a ovládací prvky související s přenosovou relací zařízení. Obsahuje tlačítka Znovu načíst přenos a Resynchronizace myši, název zařízení, rozlišení obrazovky a aktuální stav myši a klávesnice vzdáleného počítače.

1 – Znovu načíst přenos

Tato funkce umožňuje vzdáleným technikům obnovit přístup k zařízením v případě výpadku připojení nebo zpomalení výkonu. Pokud na počítači zařízení dojde k výpadku připojení nebo zpoždění obrazu, můžete kliknout na ikonu Znovu načíst přenos umístěnou v panelu přenosu. Tím platforma naváže nové připojení k počítači zařízení a zároveň znovu načte systémové kamery.

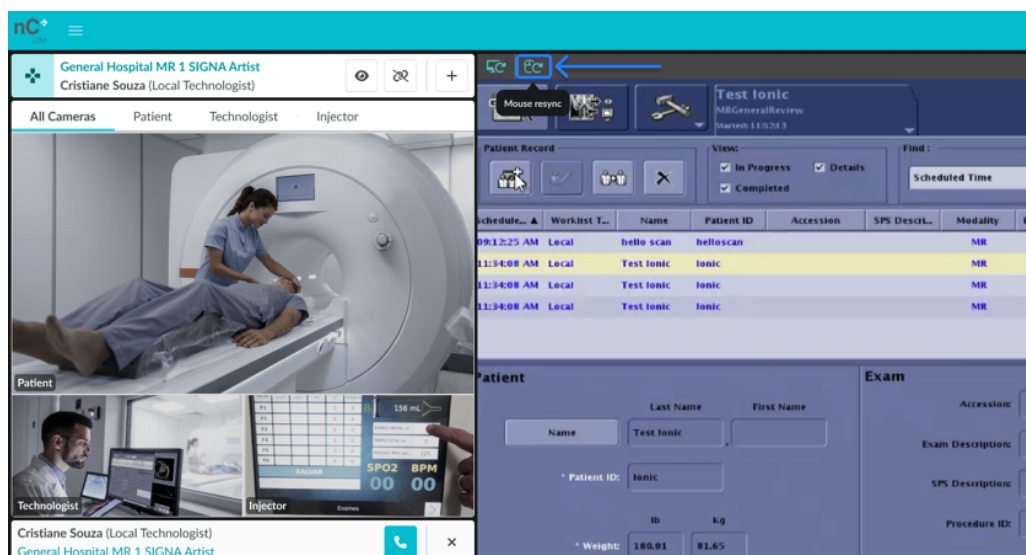


Obrázek 18: Tlačítko Znovu načíst přenos

2 – Resynchronizace myši

V případě zpomalení nebo nesouladu myši klikněte na tlačítko Resynchronizace myši umístěné na panelu nad oknem přenosu, aby se myš zařízení znovu synchronizovala s počítačem e-KVM.

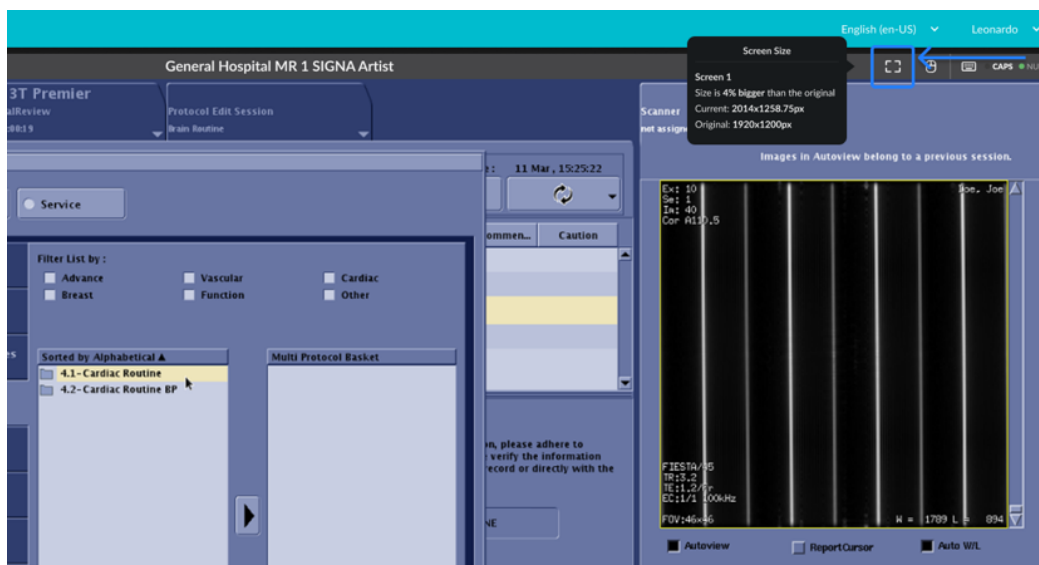
Alternativou je přesunout ukazatel myši mimo oblast přenosu a poté ho vrátit zpět, systém automaticky znovu synchronizuje myš bez nutnosti dalších akcí. Můžete také kliknout a uvolnit kolečko myši (pokud je k dispozici), aby se automaticky spustila synchronizace. Tato metoda však nemusí fungovat na zařízeních se dvěma nebo více obrazovkami, pokud jsou místní a vzdálené ukazatele myši na různých obrazovkách.



Obrázek 19: Tlačítko Resynchronizace myši

3 – Zobrazení přenosu

Tato funkce poskytuje vzdálenému technikovi informace o původním rozlišení přenosu (ze zařízení) a aktuálním rozlišení v pixelech, které se zobrazuje na vzdálené pracovní stanici.



Obrázek 20: Informační nástroj pro přenos

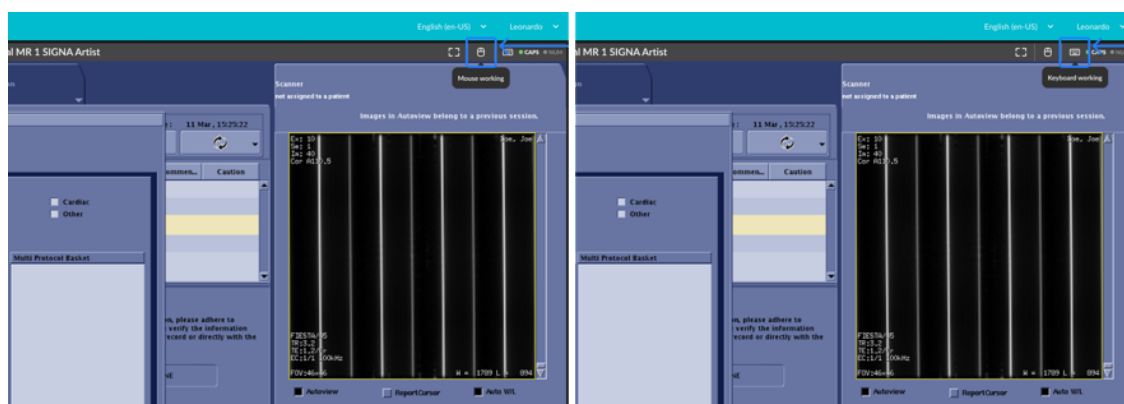
4 – Stav myši a klávesnice

Tato funkce informuje vzdáleného technika o tom, zda myš a klávesnice fungují správně. Společně se stavem klávesnice může uživatel vidět, zda jsou na počítači zařízení aktivní

klávesy **Caps Lock** a **Num Lock**. Tato funkce však závisí na tom, zda počítač zařízení poskytuje tyto informace; v případech, kdy systém zařízení tyto údaje neposkytuje, nebude stav kláves **Caps Lock** a **Num Lock** zobrazen. Stav myši i klávesnice se zobrazují pouze tehdy, pokud má uživatel přístup typu Ovládat.

Při připojení k zařízení může nesoulad mezi indikátory **Caps Lock** a **Num Lock** na vzdáleném počítači a na zařízení vést k nekonzistentnímu chování při psaní. Pokud se indikátory na zařízení zobrazují jako aktivní, ale na vzdáleném počítači ve skutečnosti nejsou, může uživatel psát na zařízení velká písmena, zatímco v chatu se zobrazí malá písmena, nebo naopak. Podobně, pokud je **Caps Lock** aktivní na vzdáleném počítači, ale na zařízení vypnutý, nastane stejný problém obráceně.

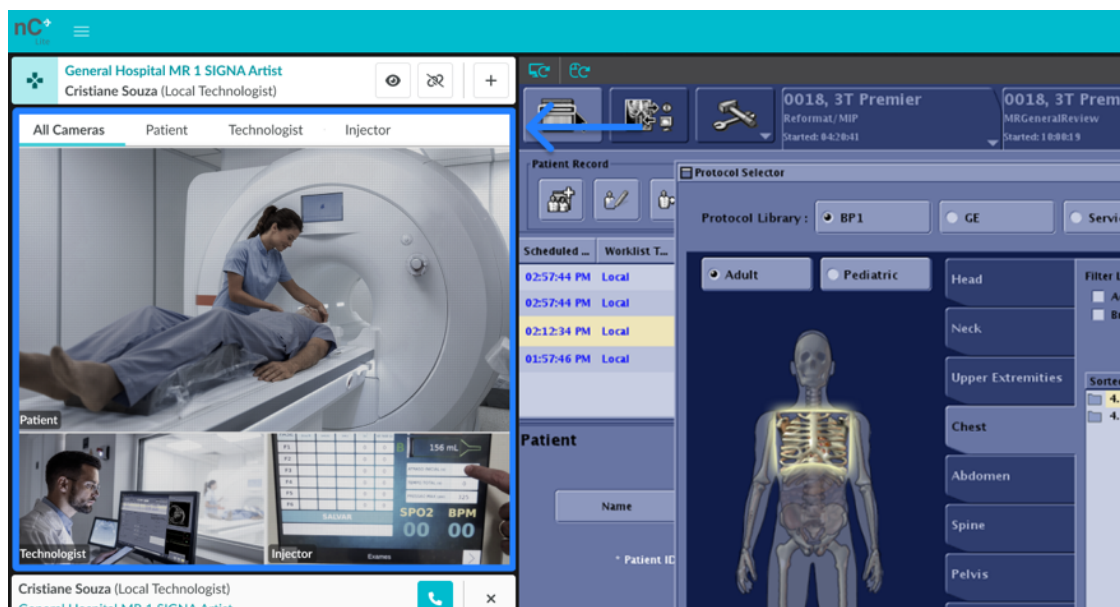
Aby se tomuto problému předešlo, ujistěte se, že klávesy **Caps Lock** a **Num Lock** jsou před přihlášením k zařízení buď obě aktivní, nebo obě deaktivované. V případě nesouladu by se měl uživatel od zařízení odpojit, upravit stav kláves na vzdáleném počítači a poté se znovu připojit.



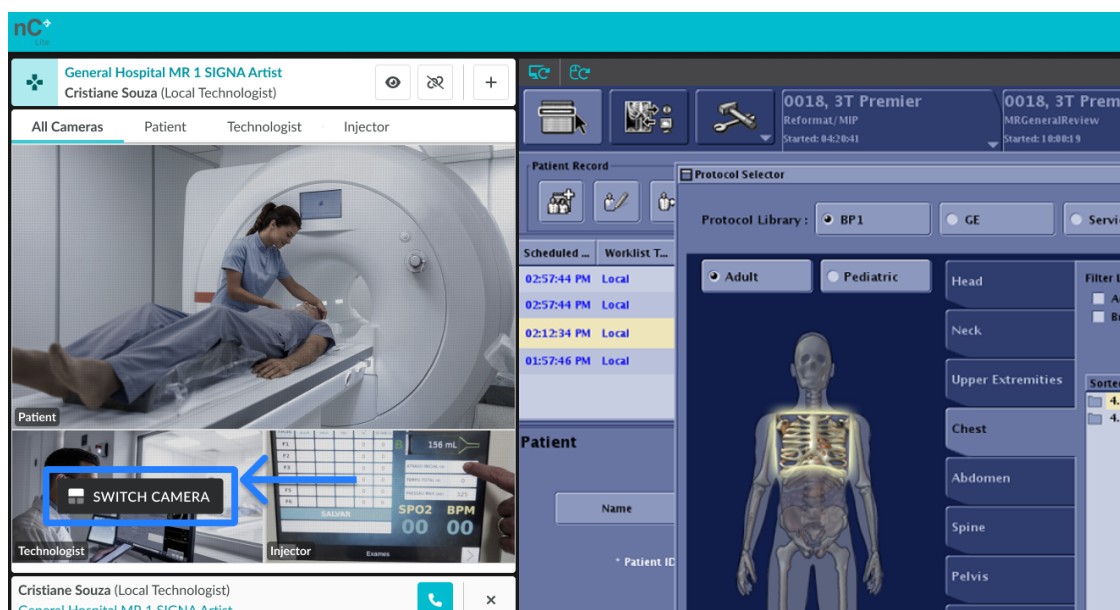
Obrázek 21: Panel přenosu
Vlevo – Informace o stavu myši
Vpravo – Informace o stavu klávesnice

3.5.3. Více kamer

Tato funkce umožňuje vzdálenému technikovi současně sledovat více kamer. Pokud je k dispozici více než jedna kamera, je možné zobrazit vždy pouze jednu a mezi nimi přepínat kliknutím na nabídku s příslušným názvem každé kamery. Po výběru možnosti VŠECHNY KAMERY se v zobrazení objeví všechny dostupné kamery, přičemž jedna z nich bude zvýrazněna. Chcete-li přepnout zvýrazněnou kameru, stačí umístit kurzor myši na jednu z kamer v menším zobrazení a kliknout na PŘEPNOUT KAMERU.



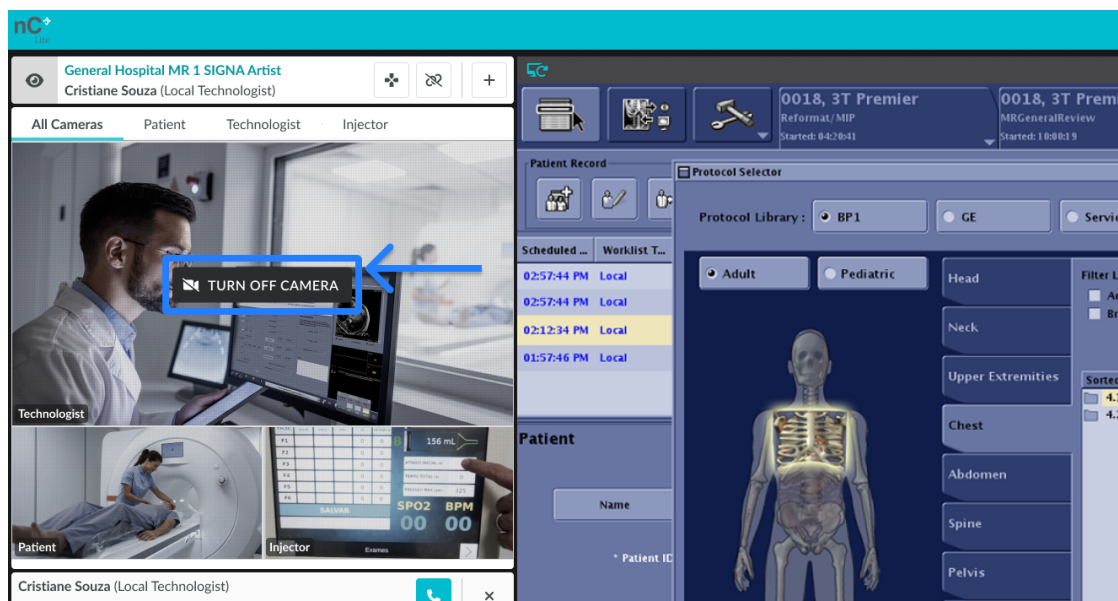
Obrázek 22: Zobrazení snímků z více kamer



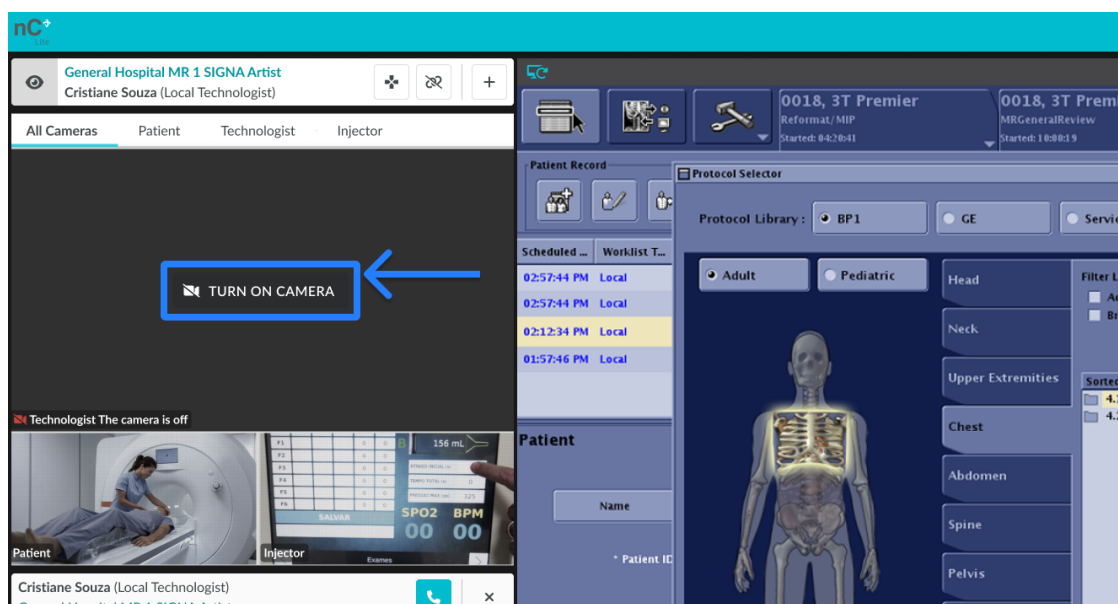
Obrázek 23: Tlačítko „PŘEPNOUT KAMERU“ při najetí myši

Během aktivní vzdálené relace, pokud má vzdálený technik přístup typu **Zobrazit**, je možné vypnout jednu nebo více kamer tak, že umístíte kurzor myši na vybranou kameru a kliknete na VYPNOUT KAMERU. Pro opětovné zobrazení kamery stačí postup zopakovat a kliknout na ZAPNOUT KAMERU.

POZNÁMKA: Možnost vypnout kamery je k dispozici pouze v režimu Zobrazit; v režimu Ovládat nelze kamery vypínat.



Obrazek 24: Tlačítko „VYPNOUT KAMERU“ při najetí myši v režimu Zobrazit pro více kamer



Obrazek 25: Tlačítko "ZAPNOUT KAMERU" při najetí myši v režimu Zobrazit pro více kamer

3.5.4. Otevřít další zařízení

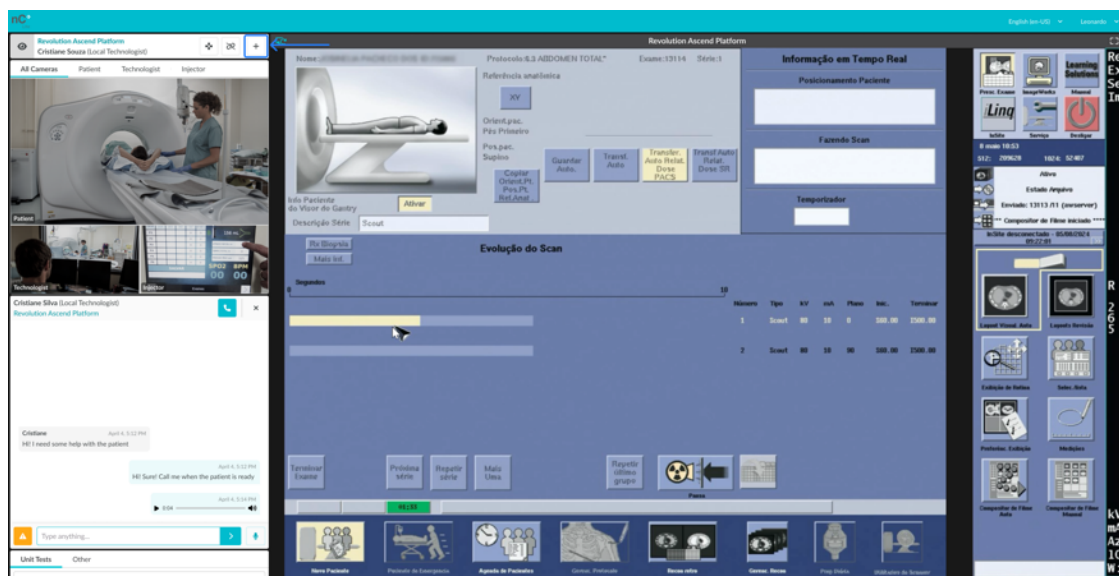
Umožňuje vzdálenému technikovi otevřít novou kartu prohlížeče s nCommand Lite, čímž si uživatel může vybrat nové zařízení a provádět více vzdálených vyšetření současně. Chcete-li otevřít nové zařízení pro přístup, stačí kliknout na tlačítko Otevřít další zařízení, přičemž se zobrazí upozornění, které umožní bezpečně provést tuto souběžnou operaci. Před otevřením tohoto nového okna si důkladně přečtete varování.

POZNÁMKA: Pro lepší zobrazení při současném přístupu se doporučuje po kliknutí na OTEVŘÍT DALŠÍ ZAŘÍZENÍ a potvrzení upozornění tlačítkem OK přetáhnout novou záložku na jiný dostupný monitor..

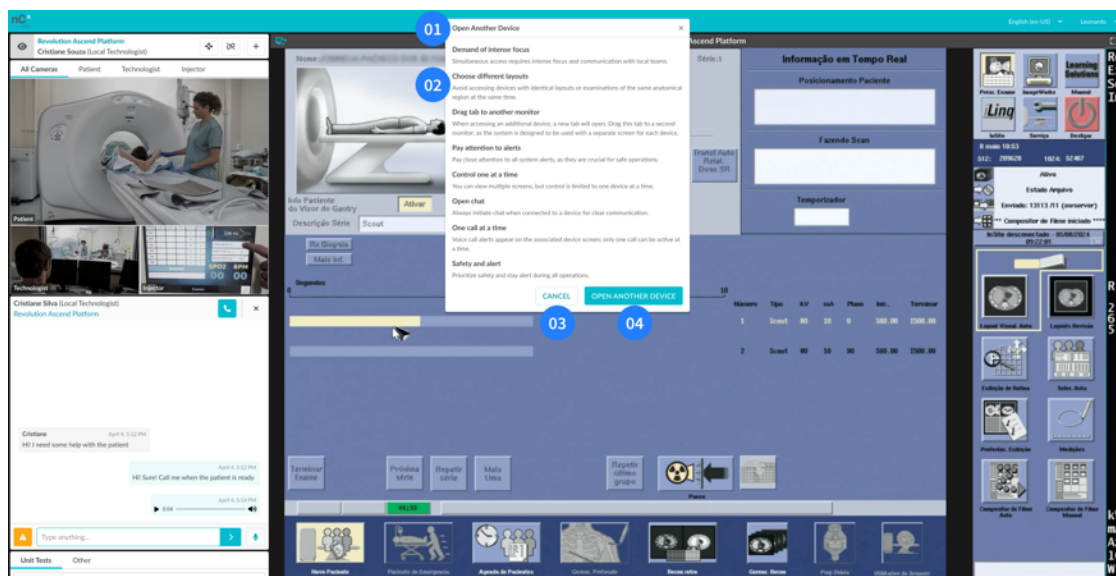
**VAROVÁNÍ!**

Bezpečnostní upozornění při současném přístupu k více skenerům

- **Požadavek na intenzivní soustředění:** Současný přístup vyžaduje intenzivní soustředění a komunikaci s lokálními týmy.
- **Vyberte si různé rozložení:** Vyhněte se současnému přístupu k zařízením se stejným uspořádáním nebo k vyšetřením stejné anatomické oblasti.
- **Přetáhněte záložku na jiný monitor:** Při přístupu k dalšímu zařízení se otevře nová záložka. Tuto záložku přetáhněte na druhý monitor, protože systém je koncipován tak, aby pro každé zařízení byla použita samostatná obrazovka.
- **Věnujte pozornost upozorněním:** Věnujte zvýšenou pozornost všem systémovým upozorněním, protože jsou klíčová pro bezpečný provoz.
- **Ovládejte jedno zařízení současně:** Můžete zobrazit více obrazovek, ale ovládat lze vždy pouze jedno zařízení současně.
- **Otevřete chat:** Při připojení k zařízení vždy zahajte chat, abyste zajistili jasnou komunikaci.
- **Jeden hovor současně:** Upozornění na hlasové hovory se zobrazují na obrazovce příslušného zařízení; současně může být aktivní pouze jeden hovor.
- **Bezpečnost a upozornění:** Při všech činnostech upřednostňujte bezpečnost a buďte ve střehu.



Obrázek 26: Tlačítko Otevřít další zařízení (+)



Obrázek 27: Varování před přístupem z více zařízení

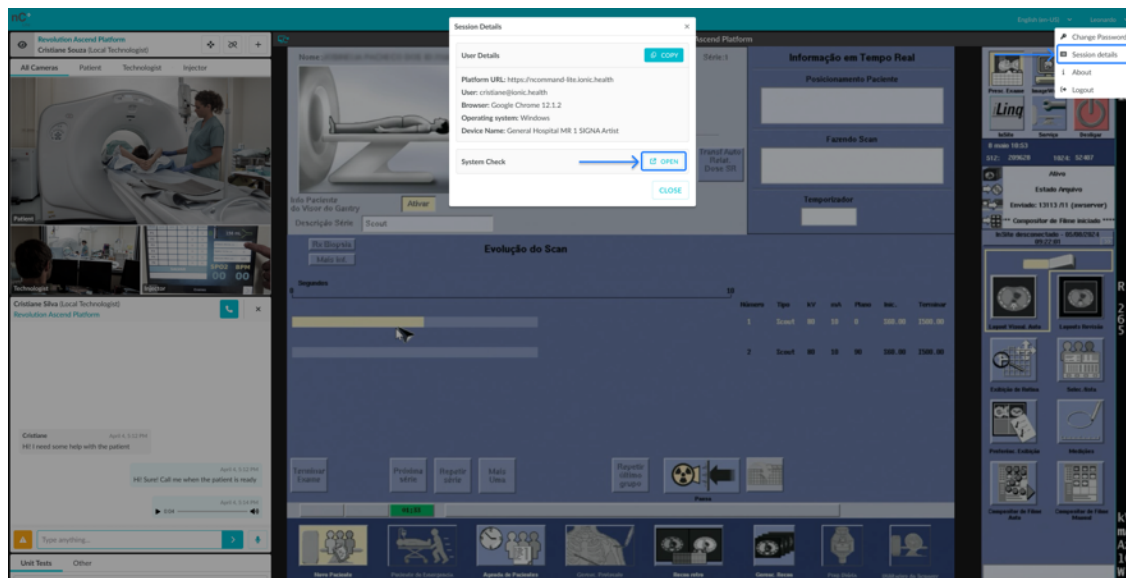
01 – Název (Otevřít další zařízení); **02** – Upozornění na bezpečnost provozu; **03** – Tlačítko Zrušit;
04 – Tlačítko Otevřít jiné zařízení

3.5.5. Kontrola systému

Funkce Kontrola systému pomáhá ověřit, zda současné zařízení, síť a internetové připojení splňují požadavky pro správné používání platformy nCommand Lite. Provádí rychlý automatický test, který kontroluje základní položky jako kvalitu internetu, přístup k požadovaným serverům a stabilitu připojení. Tento nástroj lze použít před zahájením relace, během instalace nebo pokud je podezření na problém s připojením. Pomáhá zajistit, že platforma bude fungovat podle očekávání, a pomáhá technickému týmu, pokud je potřeba řešit problémy.

Poznámka: Funkce Kontrola systému by měla být ideálně využívána s podporou nebo na žádost IT odborníka. Používání tohoto nástroje bez technického vedení může vést k nesprávnému výkladu výsledků.

Pro přístup k funkci Kontrola systému musí místní i vzdálený technik otevřít možnost Podrobnosti relace z rozbalovací nabídky, která je dostupná pod jejich uživatelským jménem v pravém horním rohu hlavní obrazovky. Poté klikněte na **Otevřít** vedle nástroje **Kontrola systému**. Jakmile se zobrazí stránka nástroje, klikněte na **Spustit test** pro zahájení ověřovacího procesu.

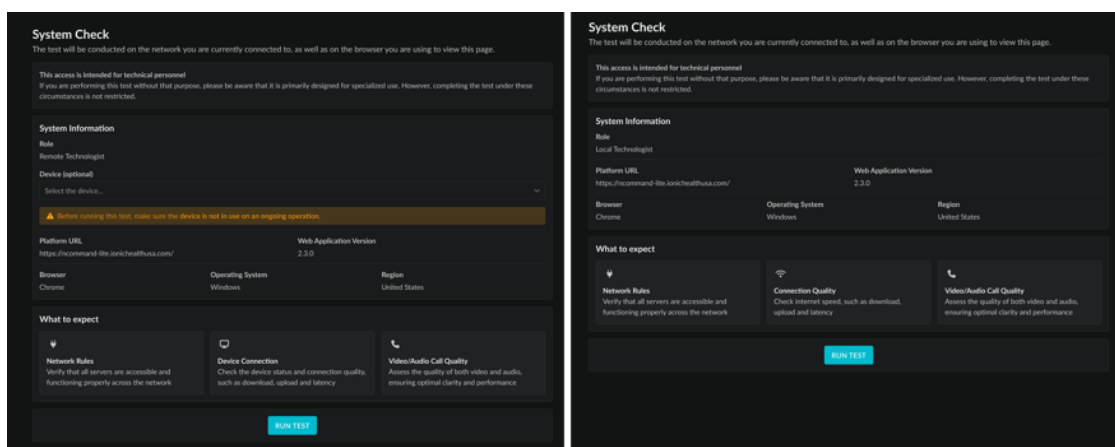


Obrázek 28: Přístup k funkci Kontrola systému

Při použití funkce vzdálený technik je možné na hlavní obrazovce nástroje vybrat zařízení, aby bylo zahrnuto do výsledků testu.

**VAROVÁNÍ!**

Před zahájením testu se ujistěte, že vybrané zařízení není aktuálně používáno.



Obrázek 29: Hlavní obrazovka Kontrola systému

Vlevo – Vzdálený technik / Vpravo – Místní technik

Po dokončení testu se na obrazovce zobrazí souhrn výsledků. IT odborníci mohou tyto informace zkontrolovat a identifikovat možné problémy ovlivňující výkon systému.

Oddíl 3.6 - Chat

Platforma nabízí chat a hovory v reálném čase s hlasovými a video funkcemi, které jsou určeny pro efektivní komunikaci mezi licencovanými technikými. Díky těmto funkcím mohou licencovaní technici vzájemně komunikovat o všech záležitostech týkajících se pracovního postupu relace.

**VAROVÁNÍ!**

V případě poruchy kontaktujte místního technika telefonicky.

Po připojení k zařízení budete mít okamžitý přístup k seznamu uživatelů chatu, který je uspořádán do dvou záložek. U zákazníků s více lokalitami může být každá pobočka nastavena jako samostatná smlouva. Po aktivaci jsou uživatelé seskupeni podle smlouvy, přičemž uživatelé z jiných smluv se zobrazují na záložce Ostatní.

Chcete-li zahájit konverzaci, poklepejte na jméno uživatele a otevřete rozhraní chatu, které podporuje jak textové zprávy, tak hlasové hovory. Ujistěte se, že vybraná relace odpovídá správnému zařízení. Platforma uživatele upozorní, pokud se síťové připojení zpomalí nebo bude nestabilní.

**VAROVÁNÍ!**

Před navázáním kontaktu ověřte název zařízení zobrazený pod jménem uživatele, protože někteří vzdálení technici mohou být připojeni k více zařízením.

Zde jsou nástroje dostupné pro komunikaci v rámci platformy:

1. **Hlasové hovory a videohovory:** Kliknutím na ikonu zahájíte hlasový hovor a videohovor až na 60 minut mezi vzdáleným a místním technikem. Připojení mezi uživateli se stejným profilem (Místní–Místní nebo Vzdálený–Vzdálený) není podporováno.

Když místní technik zahájí hovor, může vzdálený technik zvolit přijetí nebo zamítnutí hovoru. Naopak, když hovor zahájí vzdálený technik, spojení proběhne automaticky a místní technik je o tom informován – tato funkce slouží jako bezpečnostní mechanismus, který zajišťuje, že vzdálený technik může vždy komunikovat s osobou fyzicky přítomnou na pracovišti, jako by byl přítomen osobně.

Ve výchozím nastavení je mikrofon aktivní na začátku hovoru, zatímco kamera zůstává vypnutá. Každý technik může mikrofon a kameru kdykoli manuálně zapnout nebo vypnout.

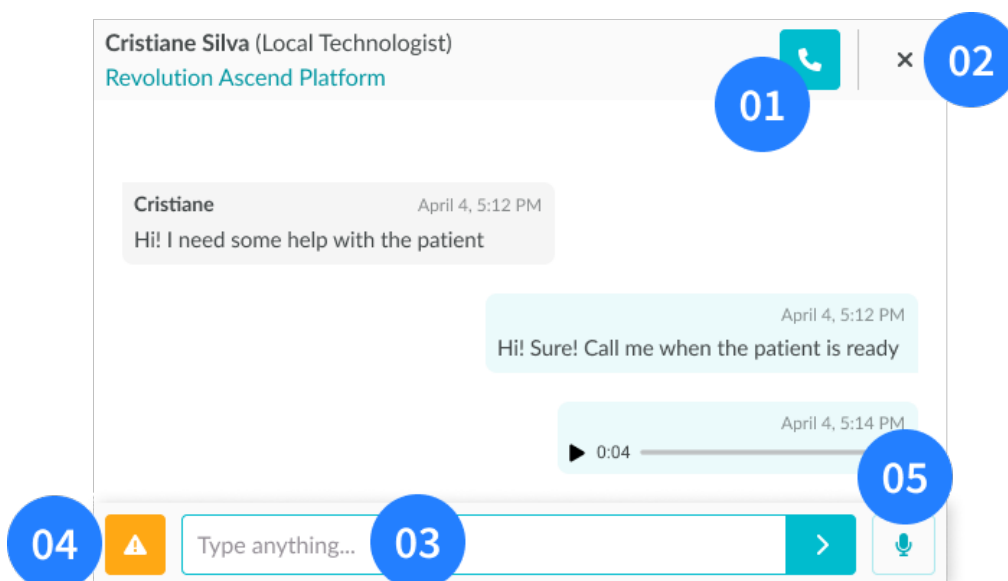
Pro úspěšné navázání hovoru musí mít oba uživatelé funkční mikrofon a zvukový výstup a musí být správně povolena oprávnění prohlížeče. Pokud některá z těchto součástí chybí, systém oba uživatele upozorní a hovor nebude uskutečněn. Kamera je volitelná – pokud není k dispozici nebo není detekována, systém aktualizuje ikonu tak, aby zobrazovala, že video není podporováno.

Každý uživatel může mít aktivní pouze jeden hovor. Pokud se technik pokusí zahájit nový hovor, zatímco je již v probíhajícím hovoru, systém tento pokus zablokuje a zobrazí upozornění. Podobně, pokud je uživatel již v hovoru a má další příchozí hovor, volající bude informován, že příjemce je momentálně nedostupný, a uživatel probíhajícího hovoru obdrží upozornění, že se někdo pokusil s ním spojit.

2. **Uzavírání chatu:** Když jeden z uživatelů zavře chat kliknutím na tlačítko Zavřít, automaticky se odešle zpráva druhému uživateli a záložka chatu se zavře. Tím je zajištěno, že obě strany jsou informovány o ukončení konverzace. Po zavření okna chatu všechny zprávy

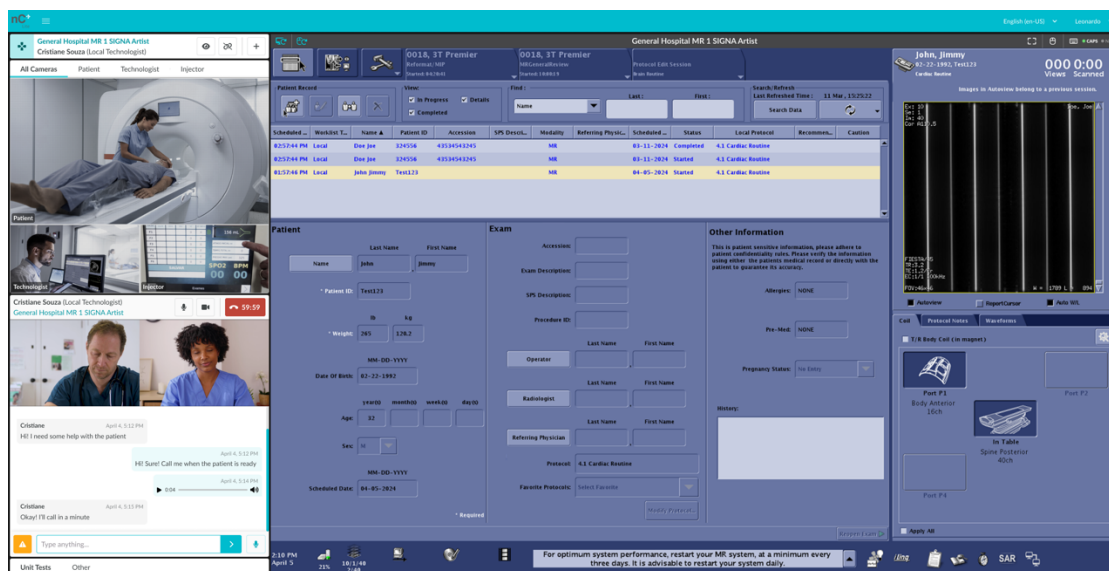
zmizí. Pokud jej během relace znovu otevřete, konverzace začne znovu bez předchozích zpráv.

3. **Textové zprávy:** Textové zprávy můžete odesílat ve vyhrazeném poli. Po odeslání zprávy se zobrazí ikona se šedou fajfkou a po doručení zprávy příjemci se zobrazí další ikona se dvěma modrými fajfkami. To umožňuje bezpečnou, jasnou a stručnou písemnou komunikaci mezi oběma stranami.
4. **Výzva k pozornosti:** Můžete upoutat pozornost druhého uživatele kliknutím na tlačítko s vykřičníkem. Tato akce způsobí, že se okno druhého uživatele na několik sekund vizuálně zatřese, a automaticky se odešle zpráva, která signalizuje naléhavost nebo důležitost.
5. **Zvukové zprávy:** Zvukové zprávy můžete odesílat kliknutím na tlačítko mikrofonu. Tento způsob se používá, když chcete sdělit zprávu osobněji nebo když není vhodné psát.

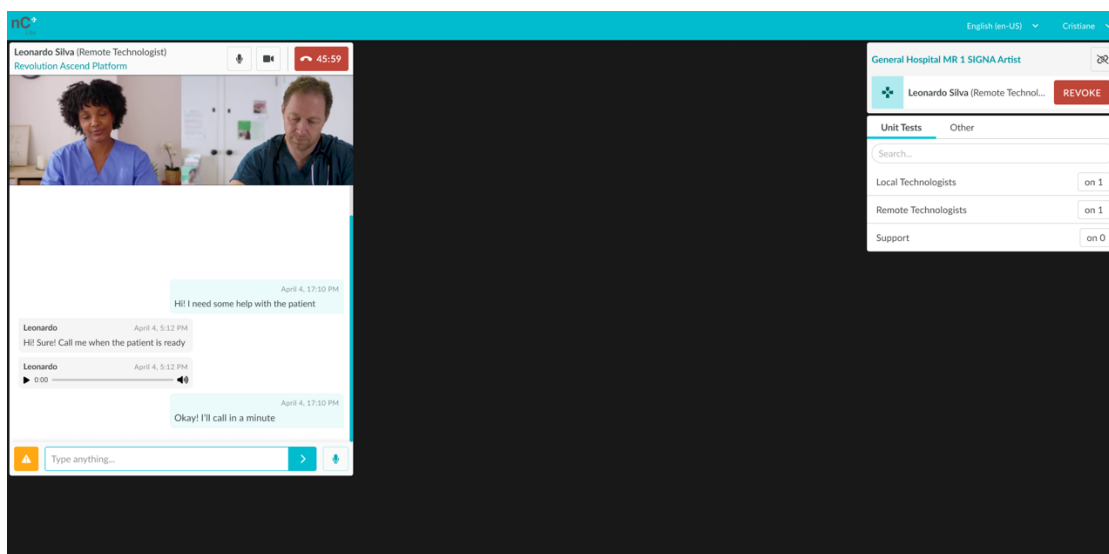


Obrázek 30: Zobrazení chatovacího okna

01 – Tlačítko hlasového hovoru a videohovoru; **02** – Tlačítko Zavřít chat; **03** – Textové pole zprávy;
04 – Tlačítko Výzva k pozornosti; **05** – Záznam Tlačítko zvukové zprávy



Obrázek 31: Hlavní obrazovka vzdáleného technika – Okno chatu (levý dolní roh)



Obrázek 32: Hlavní obrazovka místního technika – okno chatu

Problémy s připojením k internetu – Pokud některý z techniků zaznamená problémy se síťovým připojením, systém zobrazí zprávu a pokusí se o opětovné připojení. Pokud je připojení obnoveno, systém zobrazí zprávu **ONLINE** a vzdálená relace bude pokračovat běžným způsobem. Pokud se však po několika pokusech o opětovné připojení nepodaří připojení obnovit, systém ukončí aktivní relaci a technika upozorní, že byl odpojen kvůli problémům s internetem. Současně systém také upozorní druhého technika, že jeho protějšek byl odpojen kvůli problémům s internetem.

Oddíl 3.7 - Ukončení relace na platformě

Na konci služby se musí licencovaný technik odpojit od zařízení a odhlásit se z platformy.

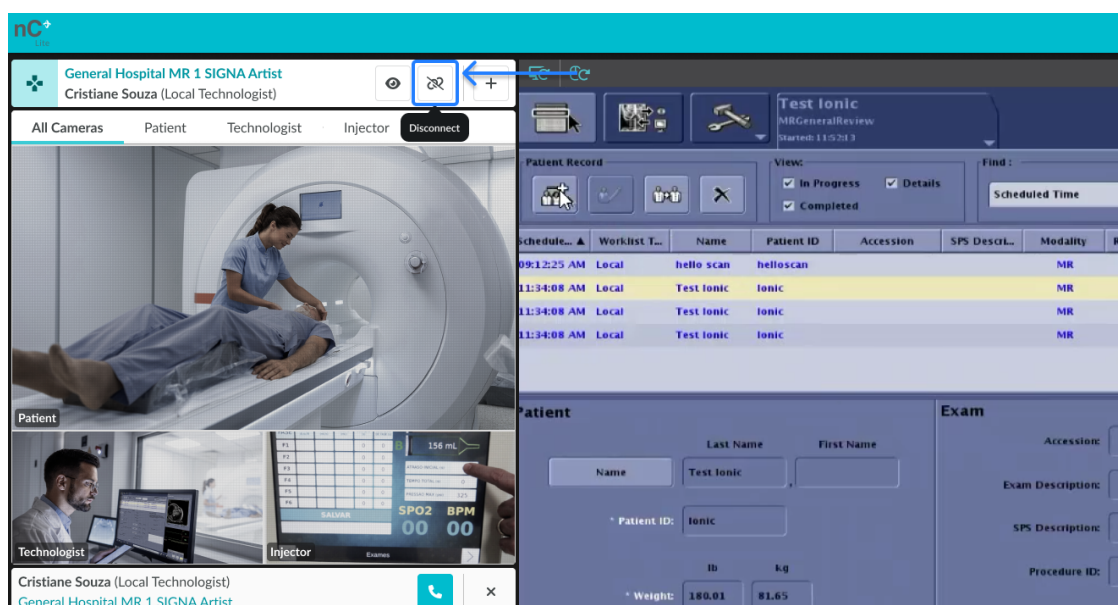


VAROVÁNÍ!

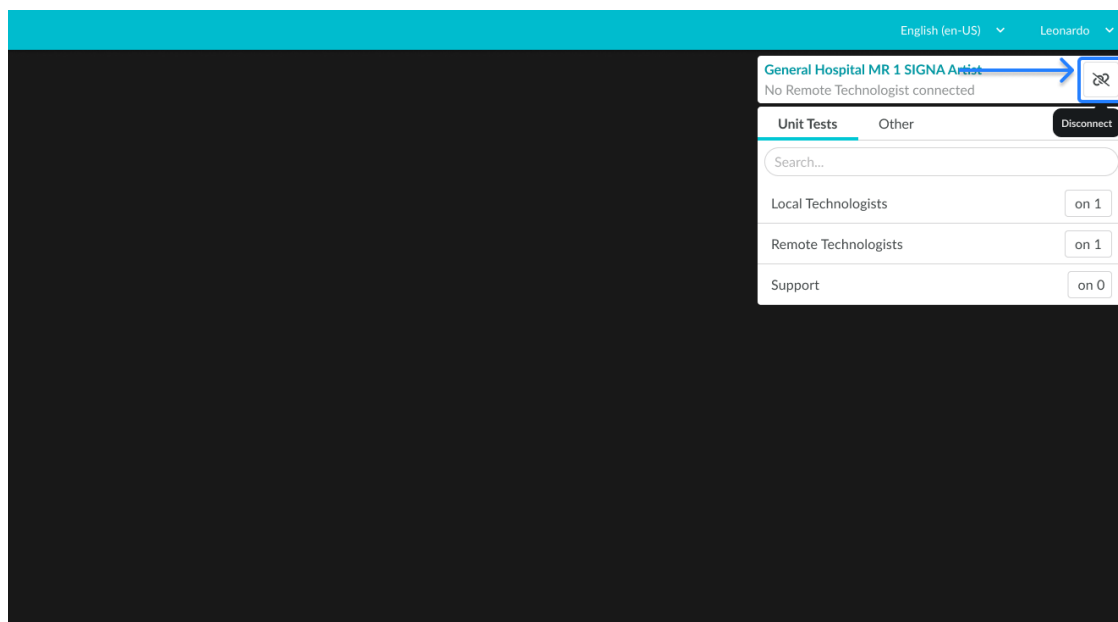
Licencovaní technici nesmí zapomenout se před koncem směny odhlásit z platformy.

Chcete-li se odpojit od zařízení, klikněte na ikonu Odpojit umístěnou v poli zařízení. Poznámka: Pokud pracujete jako místní technik, ujistěte se, že jste odebrali přístup všem vzdáleným technikům před odpojením zařízení.

Pro zajištění bezpečnosti obdržíte oznámení s potvrzením, zda se skutečně chcete odpojit od zařízení. Po potvrzení budete přesměrováni na úvodní obrazovku, aniž by bylo vybráno nějaké zařízení.



Obrázek 33: Tlačítko Odpojit – hlavní obrazovka vzdáleného technika



Obrázek 34: Tlačítko Odpojit – hlavní obrazovka místního technika

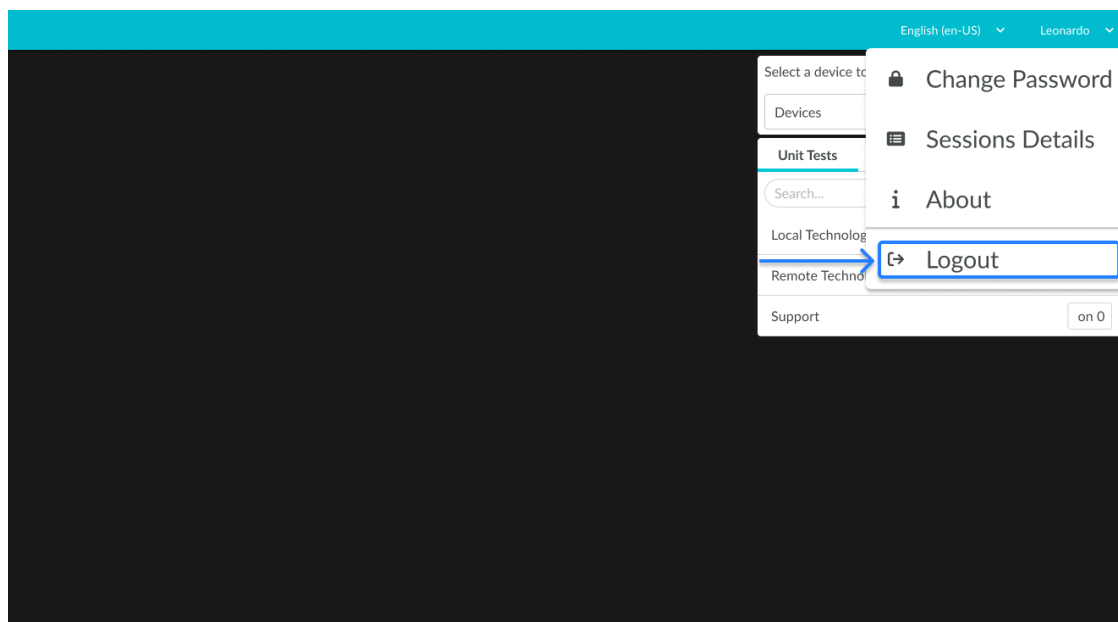


VAROVÁNÍ!

Před odhlášením se ujistěte, že jsou uzavřeny všechny další otevřené záložky.

Chcete-li ukončit relaci na platformě, klikněte na své uživatelské jméno v pravém horním rohu obrazovky a zvolte možnost Odhlásit se. Obdržíte oznámení s potvrzením, zda skutečně chcete opustit zdravotnické zařízení, ve kterém jste pracovali. Po potvrzení budete přesměrováni na přihlašovací stránku aplikace, čímž bezpečně ukončíte svou pracovní relaci.

Systém nCommand Lite nekontroluje relaci uživatele na externím poskytovateli identity (IdP) a proto nemůže provést odhlášení na úrovni IdP. V případech, kdy uživatelé sdílejí stejný počítač a používají jednotné přihlášení (SSO), se doporučuje, aby každý uživatel při přihlášení přes externího poskytovatele identity (IdP) zvolil možnost nezůstávat přihlášen (pokud je k dispozici) nebo se po odhlášení z nCommand Lite odhlásil také z IdP. Tím je zajištěno, že žádný další uživatel na stejném zařízení nemůže neúmyslně znovu použít aktivní relaci.



Obrázek 35: Položka nabídky pro odhlášení



VAROVÁNÍ!

Při použití externího poskytovatele identity na sdíleném nebo veřejném počítači se po odhlášení z platformy odhlaste také z poskytovatele identity. Pro další informace o postupu kontaktujte IT oddělení vaší organizace.

Oddíl 3.8 - Provozní školení

Účast ve školicím programu je povinná pro všechny uživatele systému nCommand Lite. Registrace uživatele na platformě je spravována týmem společnosti IONIC Health a je zahájena až po potvrzení, že uživatel úspěšně absolvoval požadované školení v LMS a je odborně způsobilý pro práci s platformou. Tento proces zajišťuje, že všichni uživatelé mají důkladné znalosti funkcí systému a jsou připraveni platformu používat efektivně a bezpečně. Pro zahájení procesu registrace ke školení kontaktujte svého obchodního zástupce.

Oddíl 3.9 - Pokyny pro řešení problémů

UŽIVATEL A HESLO	
Změna hesla	Ověřte, že byly splněny požadavky na heslo – heslo musí být silné a bezpečné, musí obsahovat alespoň jedno malé písmeno, jedno velké písmeno, jeden speciální znak a mít délku alespoň 8 znaků.
Zapomněl jsem heslo	Zkontrolujte svou e-mailovou schránku: Ujistěte se, že používáte správnou e-mailovou adresu, a zkontrolujte, zda e-mail pro obnovení hesla nebyl zařazen do složky nevyžádané pošty nebo spamu. Zkuste to znovu: Počkejte několik minut a poté si vyžádejte další e-mail pro obnovení hesla kliknutím na možnost „Zapomněli jste heslo?“. Zkontrolujte připojení k internetu: Ujistěte se, že jste připojeni k internetu.
Neobdržel jsem uvítací e-mail	Zkontrolujte, zda se e-mail nenachází ve složce nevyžádané pošty. Pokud tam není, obraťte se na administrátora a ověřte, zda je e-mail uvedený při registraci správný. Pokud není správný, administrátor by jej měl aktualizovat a znovu odeslat uvítací e-mail.
Neobdržel jsem kód pro dvoufaktorové ověření	Klikněte na „Znovu odeslat kód“ a zkontrolujte složku nevyžádané pošty. Pokud jej neobdržíte, obraťte se na administrátora a ověřte, zda je e-mail zaregistrovaný v Řízení přístupu správný.
Překročen počet pokusů o přihlášení	Pokud překročíte povolený počet pokusů o přihlášení, musíte před dalším pokusem vyčkat stanovenou dobu.
EXTERNÍ POSKYTOVATEL IDENTITY	
Problémy s přihlášením do produktu	Pokud narazíte na problémy s přihlášením při použití externího poskytovatele identity (IdP), mějte na paměti, že proces autentizace je plně spravován poskytovatelem IdP a nikoli poskytovatelem produktu, například:

	společností Ionic Health. Produkt tedy nemůže pomoci s přihlašovacími údaji, přístupovými pravidly, chybami autentizace ani s uzamčením účtu. V těchto případech byste se měli obrátit na IT oddělení vaší organizace, které může zkontrolovat konfiguraci IdP a pomoci problém vyřešit.
Problémy s přihlašovacími údaji	Veškeré problémy související s přihlašovacími údaji (<i>např.</i> zapomenuté heslo, změna hesla) musí být řešeny přímo s IT oddělením vaší organizace. Mohou zkontrolovat konfiguraci IdP a poskytnout potřebnou pomoc.
Problémy s vícefaktorovým ověřením (MFA)	Veškeré problémy související s vícefaktorovým ověřením (MFA) (<i>např.</i> problémy s vypršením platnosti MFA, nefunkční MFA, přihlášení bez vyžádání MFA) musí být řešeny přímo s IT oddělením vaší organizace. Mohou zkontrolovat konfiguraci IdP a poskytnout potřebnou pomoc.
Přihlašovací údaje nefungují na platformě	Při použití externích poskytovatelů identity (IdP) se přihlašujte do produktu výhradně přes IdP. Použití přihlašovacích údajů IdP přímo na přihlašovací stránce produktu povede k neúspěšnému přihlášení.
SKENER POČÍTAČOVÝ MONITOR	
Nezapíná se	Zkontrolujte připojení monitoru k počítači a k elektrické zásuvce. Může dojít k odpojení. Stiskněte znovu tlačítko napájení monitoru.
PLATFORMA	
Nedostupná	Zkontrolujte připojení k síti. Zkontrolujte, zda platforma byla spuštěna a zda bylo provedeno přihlášení.
Zpoždění platformy	Obnovte stránku stisknutím Ctrl+F5. Zkontrolujte, zda je chat jednotky (zdravotnické zařízení) otevřen ve více než jednom panelu. Pokud tomu tak je, zavřete panel, který se momentálně nepoužívá. Pokud problém přetrvává, zkuste se odhlásit z platformy, vymazat mezipaměť, zavřít prohlížeč a poté se znovu přihlásit.

Nefunkční funkce	Před vyzkoušením dalších postupů řešení problémů vymažte mezipaměť prohlížeče (návod najdete pro svůj aktuální prohlížeč) po přihlášení, poté prohlížeč zavřete a znovu otevřete, přihlaste se zpět na platformu a akci opakujte.
Aktualizace	Po aktualizaci platformy vymažte mezipaměť prohlížeče (návod najdete pro svůj prohlížeč) před přihlášením do nové verze.
AUDIO	
Žádný zvuk	Ujistěte se, že hlasitost mikrofonu a reproduktorů zařízení (zdravotnického zařízení) je nastavena na vhodnou úroveň. Zkontrolujte, zda má prohlížeč oprávnění používat zvuk a mikrofon. Zkontrolujte, zda je náhlavní souprava připojena a funguje správně.
Zpoždění zvuku	Zkontrolujte elektrická a síťová připojení zařízení. Obnovte stránku prohlížeče stisknutím Ctrl+F5 a znovu se přihlaste. Pokud problém přetrvává, zkuste se odhlásit z platformy, vymazat mezipaměť, zavřít prohlížeč a poté se znovu přihlásit.
CHAT	
Chat se nezobrazuje	Ujistěte se, že prohlížeč není minimalizován. V opačném případě otevřete chat po přihlášení do platformy nCommand Lite. Zkontrolujte, zda byla vybrána jednotka (zdravotnické zařízení) a zda má uživatel oprávnění pro aktivaci chatové komunikace. Ujistěte se, že prohlížeč má povolený přístup k zvuku a mikrofону. Zkontrolujte kabelové připojení, které

	může být odpojeno. Obnovte stránku prohlížeče stisknutím Ctrl+F5 a znovu se připojte k platformě. Zkontrolujte, zda je chat webu otevřen ve více než jedné záložce. Pokud tomu tak je, zavřete panel, který se momentálně nepoužívá.
Zpoždění chatu	Obnovte stránku prohlížeče stisknutím Ctrl+F5 a znovu se připojte k platformě. Pokud problém přetrvává, zkuste se odhlásit z platformy, vymazat mezipaměť, zavřít prohlížeč a poté se znovu přihlásit. Zkontrolujte kabelové připojení, které může být odpojeno.
Problémy s odesíláním zvukových zpráv	Zkontrolujte oprávnění prohlížeče pro zvuk a mikrofon a ujistěte se, že mikrofon i zvuková zařízení jsou připojena k počítači. Pokud je potřeba upravit oprávnění prohlížeče, stiskněte Ctrl+F5, aby prohlížeč po obnovení stránky změny rozpoznal.
Hlasový hovor se nepodařilo zahájit	Zkontrolujte své internetové připojení a ověřte, zda se nezobrazila nějaká oznámení vysvětlující důvod, proč se hovor nezahájil. Ujistěte se, že máte připojené zvukové zařízení a že prohlížeč má povolený přístup k zvuku a mikrofonu. Pokud problém přetrvává, obnovte stránku stisknutím Ctrl+F5 a zkuste to znovu.
Uživatel nebyl nalezen v chatu	Pokud nemůžete uživatele v chatu najít, klikněte na záložku „Ostatní“ a ověřte, zda se tam nenachází. Uživatelé spojení s jinými smlouvami se zobrazují samostatně v seznamu kontaktů. Pokud se váš uživatel po výběru zařízení nezobrazí v seznamu kontaktů, stiskněte Ctrl+F5 pro obnovení obrazovky a proveďte výběr znovu. Ujistěte se, že máte připojení k internetu.
ŽÁDOST O PŘÍSTUP K ZAŘÍZENÍ	
Platforma nerozpoznala, že místní technik je	Zkontrolujte v možnosti „Ostatní“, zda je

připojen	místní uživatel připojen. Pokud je uživatel skutečně připojen, ale stále se zobrazuje zpráva, že místní uživatel není připojen ke skeneru, obnovte obrazovku stisknutím Ctrl+F5 a požádejte místního uživatele, aby zopakoval stejný příkaz. Poté znovu vyberte zařízení a požádejte místního uživatele, aby také znovu vybral zařízení. Pokud problém přetrvává, obraťte se na podporu, aby zkontrolovala síť.
Žádost o přístup není odesílána	Obnovte stránku stisknutím Ctrl+F5 a ověřte s místním uživatelem prostřednictvím chatu, zda je žádost o přístup přijímána. Pokud problém přetrvává, obraťte se na podporu pro další pomoc.
VYSÍLACÍ ZAŘÍZENÍ (POČÍTAČ E-KVM)	
Vysílací zařízení (e-KVM COMPUTER) nefunguje	Klikněte na tlačítko „Obnovit vysílání“ na platformě. Ujistěte se, že nepřerušitelný a stabilizovaný zdroj napájení (zdravotnického zařízení) a/nebo vysílací zařízení jsou správně připojeny a zapnuty. Vypněte vysílací zařízení a veškeré další vybavení a poté je znovu zapněte. Obnovte platformu.
Vysílací zařízení je pomalé	Klikněte na tlačítko „Obnovit vysílání“ na platformě. Obnovte stránku stisknutím Ctrl+F5 a znovu se připojte k platformě. Zkontrolujte kvalitu síťového připojení. Pro ověření stavu sítě je možné provést ping test zařízení a zkontrolovat ztrátu paketů. Po problémech s internetovým připojením nemusí platforma fungovat podle očekávání. Obnovte webovou stránku a znovu požádejte o přístup pro místního uživatele.
Ztráta video výstupu	Je možné, že elektrostatický výboj způsobí ztrátu obrazu. Po restartu

	systemu by měla být komunikace a přenos videa automaticky obnoveny.
--	---

Oddíl 3.10 – Způsob čištění hardwaru

- Před zahájením čištění se ujistěte, že je veškeré vybavení odpojeno ze zásuvky.
- Nepoužívejte abrazivní přípravky.
- Neponořujte žádné zařízení ani periferní vybavení do žádného typu kapaliny.
- Likvidujte čisticí materiály v souladu s předpisy pro odstraňování nebezpečného odpadu.
- Nedoporučuje se používat rozprašovací dezinfekční prostředky, protože jejich výpary mohou proniknout do zařízení a způsobit zkrat nebo korozi.
- Tento produkt není sterilní

Kapitola 4 Kybernetická bezpečnost a ochrana osobních údajů

Oddíl 4.1 - Rizika v oblasti bezpečnosti a ochrany osobních údajů

Systém nCommand Lite zavádí více technických a organizačních opatření k ochraně zpracovávaných informací.

Systém je certifikován podle norem ISO/IEC 27001 a ISO/IEC 27701 a a uplatňuje přístup ochrany soukromí již při návrhu. Podporuje dodržování právních předpisů o ochraně zdravotnických dat a nařízení o kybernetické bezpečnosti platných v EU, USA, Velké Británii, Švýcarsku, Brazílii, Spojených arabských emirátech, Saúdské Arábii, Austrálii a na Novém Zélandu.

Uživatelé však musí dodržovat osvědčené postupy, aby předešli zbytečnému vystavení citlivých údajů.

- Vyvarujte se sdílení osobních nebo citlivých informací, pokud to není nezbytně nutné.
- Zajistěte, aby komunikace a přístup do systému probíhaly v bezpečném prostředí.
- Pokud máte podezření na jakoukoli škodlivou činnost, neprodleně informujte odpovědný tým.

Oddíl 4.2 - Ochrana osobních údajů (soulad s GDPR / HIPAA)

Systém **nCommand Lite** splňuje všechny platné zákony a předpisy o ochraně soukromí a ochraně údajů v regionech, kde působí, zejména včetně požadavků GDPR, HIPAA, LGPD a ISO/IEC 27701. Veškeré aktivity zpracování údajů probíhají v rolích „**Zpracovatel**“ a „**Další zpracovatel**“, jak je definováno v GDPR, s přísnou regionální segregací údajů, aby byla zajištěna shoda a zabránilo se neoprávněným přeshraničním přenosům údajů

Jaké údaje jsou shromažďovány?

- **Uživatelé:** Jméno, e-mail a společnost (pouze pro účely ověření a správy přístupu).
- **Údaje o pacientech:** Pouze přenosy lékařských vyšetření prostřednictvím vysílání v reálném čase, bez ukládání údajů.

Jak jsou údaje používány a chráněny?

- Údaje jsou používány výhradně pro **ověření identity, kontrolu přístupu a sledovatelnost relací**.
- Přenos informací je zabezpečen šifrováním **AES-256 pro ukládání údajů a protokolem TLS 1.3 pro údaje při přenosu**.
- **Přístup je omezen a řídí se principem nejmenších oprávnění (RBAC).**

- Úplné šifrování (end-to-end) je zajištěno pro P2P video a řídicí přenosy prostřednictvím WebRTC.
- Autorizovaní poskytovatelé cloudových služeb (např. Microsoft Azure) zpracovávají omezené údaje za přísných smluvních záruk.

Uživatelům jsou udělena tato práva:

- **Přístup k osobním údajům a jejich oprava.**
- **Žádost o vymazání údajů**, pokud je to relevantní.

Pokud máte jakékoli dotazy, zašlete e-mail na adresu privacy@ionic.health a obraťte se na pověřence pro ochranu osobních údajů (DPO) společnosti Ionic Health. Veškeré žádosti jsou vyřízeny do 30 dnů, s možností prodloužení dle GDPR.

Oddíl 4.3 - Správa přístupu a autentizace

Uživatelé odpovídají za definování **rolí a oprávnění přístupu** pro své týmy, zajištění pravidelných kontrol a dokumentace uděleného přístupu.

Osvědčené postupy a kontrolní opatření

- Říďte se **principem nejmenších oprávnění (RBAC)** a zajistěte, aby uživatelé měli pouze nezbytný přístup.
- **Vícefaktorová autentizace (MFA)** je povinná pro administrativní přístup a doporučena pro všechny uživatele.
- **Jsou vyžadována silná hesla**, která mají alespoň **8 znaků, včetně velkých písmen, malých písmen, číslic a symbolů**.
- **Nesdílejte s nikým své přihlašovací údaje.**
- Přístupová oprávnění jsou pravidelně monitorována a revidována.

Sledování: Přístup, změny oprávnění a důležité činnosti jsou zdokumentovány v protokolech zabezpečení systému. Protokoly se uchovávají po dobu nejméně 7 let v souladu s HIPAA, GDPR a dalšími platnými předpisy. Používají se k podpoře interního auditu, forenzní analýzy a regulačního výkaznictví. Protokoly jsou chráněny proti neoprávněné manipulaci a jsou uloženy v zabezpečeném prostředí s řízeným přístupem.

Oddíl 4.4 - Kontrola systému řízení přístupu

Funkce Kontrola systému je přístupná výhradně přes **webovou aplikaci nCommand Lite** a pro přihlášení vyžaduje platné přihlašovací údaje. Přístup je omezen pouze na oprávněné role — *Vzdálený technik, Místní technik, Administrátor, Role nadřízený a Uživatel kontroly systému*.

Role *Uživatel kontroly systému* je navržena s omezenými oprávněními, což umožňuje přístup pouze k diagnostickým funkcím souvisejícím s ověřováním sítě a ověřováním konektivity. To zajišťuje, že detaily sítě, informace o bílých seznamech a systémové metriky nikdy nebudou vystaveny neoprávněným osobám.

Všechny přístupové požadavky jsou ověřovány přes Azure AD B2C, s vícefaktorovým ověřením (MFA) a adaptivními politikami podmíněného přístupu spravovanými Microsoft Entra ID.

Složitost hesla odpovídá bezpečnostním zásadám společnosti a vyžaduje minimálně osm znaků, včetně velkých a malých písmen, čísel a symbolů. Hesla vyprší každých 90 dní a relace se automaticky odhlásí po 24 hodinách nečinnosti, což lze prodloužit až na 90 dní při nepřetržitém používání

Oddíl 4.5 - Regionální segregace údajů a uchovávání přístupových záznamů

Platforma **nCommand Lite** udržuje přísnou regionální segregaci údajů, aby zabránila neoprávněným nebo zbytečným přeshraničním přenosům. Prostředí jsou izolována podle regionů, což zajišťuje soulad s platnými předpisy.

Všechny přístupové záznamy, záznamy o aktivitách a bezpečnostní události jsou uchovávány minimálně sedm (7) let v souladu s platnými předpisy o ochraně osobních údajů a zdravotní péči. Přístupové záznamy jsou uchovávány v bezpečných, přístupově kontrolovaných prostředích a chráněny proti manipulaci. Tyto informace podporují forenzní vyšetřování, audity souladu s právními předpisy a regulační výkaznictví.

Oddíl 4.6 - Bezpečnost a integrita údajů

Systém **nCommand Lite** zajišťuje důvěrnost, integritu a dostupnost údajů prostřednictvím standardních bezpečnostních postupů.

Uživatelé musí zajistit soulad s bezpečnostními protokoly, pravidelně kontrolovat zásady přístupu a hlásit jakékoli nesrovnalosti. Systém nepřetržitě monitoruje aktivity a administrátoři musí prosazovat bezpečnostní zásady, aby udrželi účinnou obranu proti případným hrozbám.

Systém je chráněn nepřetržitým 24/7 monitorováním prostřednictvím specializovaného bezpečnostního operačního centra (SOC) s funkcemi SIEM pro detekci hrozeb a reakci na ně.

Oddíl 4.7 - Reakce na bezpečnostní incidenty

Systém zahrnuje zdokumentovaný plán reakce na incidenty, který je v souladu s normami ISO 27035 a NIST CSF.

V případě bezpečnostních incidentů, jako je neoprávněný přístup nebo selhání systému, musí uživatelé postupovat podle následujících pokynů:

Jak identifikovat incident?

- **Neoprávněný přístup** zjištěný v protokolech aktivit.
- **Podezřelé pokusy o přihlášení** nebo opakované selhání ověření.
- **Neobvyklé chování systému**, jako jsou neočekávané akce nebo poruchy.

Jak nahlásit incident?

Okamžitě zaznamenejte událost prostřednictvím dostupných kanálů podpory (kapitola 5).

Pokud je únik osobních údajů potvrzen, společnost IONIC jako další zpracovatel do 48 hodin informuje GE jako zpracovatele a poskytne všechny příslušné důkazy, detaily dopadu a opatření k nápravě. GE je naopak odpovědná za informování kontrolora (zákazníka) v souladu s platnými právními a smluvními požadavky.

Kapitola 5 Servisní kanály

Ať už potřebujete pomoc s technickým problémem, nejasným krokem v procesu nebo dalšími pokyny, náš tým je připraven vám pomoci. Můžete nás kontaktovat telefonicky, e-mailem nebo prostřednictvím platformy ITSM, podle toho, co vám více vyhovuje. Naši odborníci jsou vyškoleni tak, aby poskytovali individuální pomoc a zajistili rychlé a efektivní řešení jakéhokoli problému.

Telefonní čísla

Spojené státy americké	+1 (216) 2421223
Brazílie	+55 12 3600 0181
Evropa (Portugalsko)	+351 (300) 528 410
Austrálie	+1 (216) 2421223
Nový Zéland	+1 (216) 2421223

Platforma ITSM

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

E-mail

helpdesk@ionic.health



VAROVÁNÍ!

Jakýkoli závažný incident související s používáním tohoto zařízení musí být nahlášen výrobcí i zdravotnickému úřadu/příslušnému orgánu v místě, kde je zařízení instalováno.

Chcete-li nahlásit incident výrobcí: kontaktujte svého lokálního servisního zástupce nebo incident nahláste na: helpdesk@ionic.health

Uved'te tyto informace:

- Číslo verze systému, které se zobrazuje na přihlašovací obrazovce;
- Datum, kdy došlo k incidentu;
- Popis incidentu, včetně jakéhokoli postižení/zranění pacienta nebo uživatele;
- Vaše kontaktní údaje (zařízení, adresa, kontaktní jméno, oslovení a telefonní číslo).

Kapitola 6 Právní a regulační informace

Výrobce



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
Brazílie

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

Odpovědný technik

Alexandre Seiji Fukuda Ribas
CREA-SP: 5071085437

ANVISA

82585300004

Dovozce (USA)



Systém nCommand Lite

IONIC HEALTH USA INC.

11201 Cedar Avenue, STE 600
Cleveland, OH 44106
USA

+1 (216) 242 1223

Zástupce EU / Dovozce



nCommand Lite



Identifikační číslo oznámeného subjektu:
2803

EUROPE IONIC HEALTH DIGITAL TECHNOLOGIES, LDA

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

+351 (300) 528 410

Švýcarský zplnomocněný zástupce (CH-REP) / Dovozce**CH REP****REF**

nCommand Lite

FREYR LIFE SCIENCES GMBH

Bahnhofplatz
CH-6300 Zug
Švýcarsko

Odpovědná osoba/Dovozce pro Spojené království**REF**

nCommand Lite

FREYR LIFE SCIENCES LTD

9 Greyfriars Road
Reading, Berkshire
RG1 1NU
Anglie, Spojené království

Australský sponzor**REF**

nCommand Lite

TAEVAS LIFE SCIENCES PTY LTD

46 Dora St
Blacktown NSW 2148
Austrálie

Novozélandský sponzor**REF**

nCommand Lite

TAEVAS LIFE SCIENCES LIMITED

Patro 3, 1 Margaret Street
Lower Hutt 5010
Nový Zéland

ZÁKLADNÍ UDI-DI: 7898974112NCLITE2L

Požádejte o tištěnou kopii

Tištěné kopie Uživatelské příručky nCommand Lite budou poskytnuty na vyžádání bez dalších nákladů. Kontaktujte svého místního zástupce a požádejte o tištěnou kopii Uživatelské příručky.

Datum výroby

Datum vydání softwaru je uvedeno na přihlašovací stránce nCommand Lite ve formátu MĚSÍC/ROK.

Kapitola 7 Historie revizí

Revize	Popis změny	Datum
0	Aktualizována verze příručky z 2.3 v1 na 2.4	25. listopadu 2025
1	Aktualizovány popisky kapitoly 6	4. prosince 2025
2	Odstraněn požadavek na statickou IP adresu z konfigurace místního počítače v odstavci 1.3.11 Aktualizován symbol oprávněného zástupce EU v odstavci 1.3.12 Poznámka byla odstraněna z odstavce 1.3.14 Aktualizován obsah v kapitole 2 Aktualizován symbol oprávněného zástupce EU v kapitole 6	28. ledna 2026
3	Byl revidován překlad „Odpovědný technik“ v kapitole 6.	9. února 2026

PŘÍLOHA I – Kontrolní seznam pro zahájení služby

1. *Ověřte elektrické a síťové připojení:*

Ujistěte se, že jsou na počítači e-KVM, počítači skeneru a místním počítači správně zapojena elektrická připojení a síťové body.

2. *Zkontrolujte stav napájení:*

Ověřte, zda je zapnutý a správně funguje nepřerušitelný stabilizovaný zdroj napájení i počítač e-KVM.

3. *Rychlý přístup k platformě nC Lite:*

Ověřte, zda je na ploše dostupný zástupce platformy nC Lite pro rychlý přístup.

4. *Přístup a přihlášení k platformě nC Lite:*

Otevřete platformu nCommand a přihlaste se, abyste ověřili plný přístup a správnou funkčnost.

5. *Nastavení aplikace pro chat:*

Otevřete aplikaci pro chat v rámci platformy nC Lite pouze v jedné záložce a neminimalizujte ji, aby byla zajištěna plynulá komunikace.