Project Proposal – LVHN eKVM Remote Update (No Atera)

Document Control - **Version:** 1.0 - **Date:** 2025-11-11 - **Classification:** Internal – Technical Implementation - **Authors:** Ionic Technical Team - **Audience:** LVHN IT Leadership, Ionic Engineering - **Status:** Draft for Review

---

Configuration Custody Notice
Ionic Health engineering exclusively manages all eKVM configuration, firmware, and software changes. LVHN operations is solely responsible for provisioning, hardening, and maintaining the Windows jumper server environment. Any activity outside these custody boundaries requires written approval from both teams.

Network Visibility Scope
Ionic Health requires no insight into LVHN's internal network beyond the managed jumper server boundary and its controlled outbound path to Ionic eKVM devices.

Table of Contents

---

1. Executive Summary

1.1 Objective

Enable remote eKVM firmware and software updates without relying on Atera agents, using LVHN's existing SSL VPN infrastructure to access a dedicated Windows jumper server, which will then connect to eKVM devices via RDP,

WinRM, or SMB protocols during scheduled maintenance windows. This approach preserves the nCommand Lite peer-to-peer (P2P) and WebRTC clinical runtime architecture, ensuring zero impact on clinical operations outside maintenance periods.

1.2 Business Outcomes

- **Auditable Change Process:** Every update operation generates comprehensive audit trails with operator identity, timestamps, file integrity verification (SHA-256), and security scan results.
- **Integrity Verification:** Pre-transfer and post-installation hash validation ensures binary authenticity and detects unauthorized modifications.
- **Zero Clinical Impact:** Clinical workflows using nCommand Lite P2P/WebRTC remain completely unchanged during normal operations; updates occur only during approved maintenance windows.

1.3 Critical Ownership Statement

CUSTOMER RESPONSIBILITY

Security hardening, continuous monitoring, patch management, access control, and regulatory compliance of the Windows jumper server are **LVHN's sole and exclusive responsibility**. Ionic provides implementation guidance and best-practice recommendations but does not assume operational responsibility for customer infrastructure security.

---

2. Scope

2.1 In Scope

- **Access Architecture:** SSL VPN (MFA-protected) → Windows jumper server → eKVM devices
- **Security Hardening:** RDP with Network Level Authentication (NLA), TLS 1.2+ enforcement, account lockout policies
- **Access Control:** Named Just-In-Time (JIT) accounts with time-boxed privileges; no shared credentials
- **File Transfer Methods:**
  - HTTPS direct download to jumper server
  - RDP drive mapping (operator workstation → jumper server)
  - WinRM/SMB (jumper server → eKVM)
- **Audit & Evidence:** Comprehensive Windows event logging, PowerShell transcription, SHA-256 verification, AV/EDR scanning
- **Deployment Strategy:** Pilot phase (2-3 devices) followed by phased rollout

2.2 Out of Scope

- Modifications to clinical workflows or nCommand Lite P2P/WebRTC runtime architecture
- Installation of any new agents, services, or monitoring tools on eKVM devices outside approved update packages
- Day-to-day operational changes to eKVM clinical functionality
- 24/7 persistent remote access (access enabled only during approved maintenance windows)

---

3. Essential Prerequisites (Must-Have)

MANDATORY FOR PROJECT SUCCESS

These prerequisites are non-negotiable. Absence of any item constitutes a GO/NO-GO decision point.

#	Prerequisite	Validation Method	Owner
1	**eKVM OS Access via RDP/WinRM** during maintenance windows	Pre-window connectivity test with test account	LVHN IT
2	**HTTPS egress from jumper server** to allowlisted domains (e.g., `downloads.ionic.com`, `cdn.ionic.com`)	Pre-window `curl`/`wget` test to download small test file	LVHN IT
3	**RDP drive mapping enabled** on jumper server (GPO configuration)	Pre-window RDP session confirming `\\tsclient\C` visibility	LVHN IT
4	**File transfer jumper → eKVM** via one of: RDP drive mapping, WinRM `Copy-Item -ToSession`, or SMB temporary share	Pre-window file transfer dry-run (100 MB test file)	LVHN IT
5	**Named JIT accounts** configured with MFA and time-boxed access (no shared/service accounts)	Pre-window account provisioning verification	LVHN IT

#	Prerequisite	Validation Method	Owner
6	**SIEM ingestion** of Windows Security, RDP, PowerShell logs from both jumper server and eKVM	Pre-window log generation and SIEM query validation	LVHN IT

---

4. Architecture (Maintenance Path)

4.1 Maintenance Access Flow

```
Operator
Workstation
(MFA Token)

        SSL VPN (MFA)
        Port: 443


LVHN SSL VPN
Gateway




Windows Jumper Server
- Hardened Windows Server 2019/2022
- AV/EDR Active
- Scoped ACLs (jumper IP → eKVM only)
- HTTPS egress (allowlisted)
- Staging: C:\Staging\eKVM


        RDP 3389 (Primary)
        WinRM 5985/5986 (File Transfer)
        SMB 445 (Alternate Transfer)


eKVM Device
- RDP enabled (NLA, TLS 1.2+)
- WinRM enabled (TrustedHosts scoped)
- nCommand Lite P2P/WebRTC unaffected
```

```
Clinical Path (Unchanged):
          P2P/WebRTC
  Clinician            eKVM
    PC         Direct         Device
          Connection
```

4.2 Network Segmentation

- **Jumper → eKVM:** Scoped ACL permits only jumper server IP to reach eKVM on ports 3389, 5985/5986, 445
- **Internet → Jumper:** HTTPS egress only to allowlisted domains; no inbound from Internet
- **Clinical Network:** P2P/WebRTC traffic remains isolated from maintenance path
- **Temporary Rules:** All maintenance-specific ACLs revert immediately post-window (H+1)

---

5. Technical Design

5.1 Ports & Protocols

Protocol	Port(s)	Direction	Purpose	TLS/Encryption
RDP	3389	Jumper → eKVM	Primary management access	TLS 1.2+ with NLA
WinRM (HTTP)	5985	Jumper → eKVM	File transfer, remote execution	Kerberos/NTLM auth
WinRM (HTTPS)	5986	Jumper → eKVM	Secure file transfer (preferred)	TLS 1.2+
SMB	445	Jumper → eKVM	Alternate file transfer	SMB 3.1.1 with encryption
HTTPS	443	Jumper → Internet	Binary download from Ionic CDN	TLS 1.2+

5.2 Network Scoping Rules

Implementation:

```
# Example ACL (Palo Alto / Cisco ASA syntax conceptual)
# Rule: Allow Jumper → eKVM (Maintenance Window Only)
Source: 10.50.100.10 (jumper-server-01.lvhn.local)
Destination: 10.60.200.0/24 (eKVM-subnet)
Ports: 3389, 5985, 5986, 445
Schedule: Change-Window-Start to Change-Window-End + 1hr
Action: Permit
Logging: Full session logs

# Default Deny
Source: Any
Destination: 10.60.200.0/24
Ports: 3389, 5985, 5986, 445
Action: Deny
Logging: Denied connection attempts
```

Validation: - Pre-window: `Test-NetConnection -ComputerName ekvm-device-01 -Port 3389` (from jumper) - Pre-window: `Test-NetConnection -ComputerName ekvm-device-01 -Port 3389` (from unauthorized host → expect failure)

5.3 Accounts & Access Control

Account Type	Naming Convention	MFA	Time-Boxing	Usage
VPN Access	`firstname.lastname@lvhn.org`	Required	Session-based	SSL VPN authentication
Jumper Server	`LVHN\firstname.lastname.admin`	Required (PAM)	Change window ±2hr	RDP to jumper server
eKVM Local Admin	`.\ekvm-maint-CHANGENUM`	Password + hardware token	Window duration only	RDP/WinRM to eKVM

Prohibited Practices: - Shared accounts (e.g., `admin`, `serviceaccount`) - Permanent local admin rights on eKVM - Saved/cached credentials on jumper server - Non-expiring passwords

5.4 RDP Hardening (eKVM)

Group Policy / Local Policy Settings:

```
[Registry: HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server]
fDenyTSConnections = 0  # RDP enabled
SecurityLayer = 2        # Require TLS
UserAuthentication = 1   # Require NLA

[Registry: HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]
MinEncryptionLevel = 3   # High (128-bit)
SecurityLayer = 2        # TLS

[Account Lockout Policy]
Account lockout threshold = 5 invalid attempts
Account lockout duration = 30 minutes
Reset account lockout counter after = 30 minutes

[Legal Banner]
LegalNoticeCaption = "Authorized Access Only"
LegalNoticeText = "This system is for authorized LVHN personnel only. Unauthorized access is

[Disabled Features]
Clipboard redirection = Disabled
Printer redirection = Disabled
COM port redirection = Disabled
Drive redirection = Enabled (only during change window, for file transfer)
Audio redirection = Disabled
```

Validation: - Run `GPResult /H gpresult.html` on eKVM pre-window - Verify TLS 1.2+ with `Test-RDPConnection` script (custom validation)

5.5 Integrity & AV/EDR

Binary Integrity Process:

1. **Publication:** Ionic publishes SHA-256 hash alongside binary on secure portal (HTTPS, authentication required)

   ```
   Example:
   Filename: eKVM-Firmware-v3.2.1.exe
   SHA-256: a1b2c3d4e5f67890123456789012345678901234567890abcdef1234567890abcdef123456
   ```

2. **Pre-Transfer Verification (Jumper Server):**

   ```
   $expectedHash = "a1b2c3d4e5f67890123456789012345678901234567890abcdef1234567890abcdef123456"
   $downloadedFile = "C:\Staging\eKVM\eKVM-Firmware-v3.2.1.exe"
   $actualHash = (Get-FileHash -Path $downloadedFile -Algorithm SHA256).Hash
   if ($actualHash -ne $expectedHash) {
   ```

```
    Write-Error "HASH MISMATCH! File may be corrupted or tampered."
    exit 1
}
```

3. **AV/EDR Scan (Jumper Server):**

```
# Windows Defender example
Start-MpScan -ScanPath "C:\Staging\eKVM" -ScanType CustomScan
$threat = Get-MpThreat
if ($threat) { exit 1 }
```

4. **Post-Transfer Verification (eKVM):**

```
# After copying to eKVM
$actualHashEKVM = (Get-FileHash -Path "C:\Temp\eKVM-Firmware-v3.2.1.exe" -Algorithm SHA
if ($actualHashEKVM -ne $expectedHash) { exit 1 }
```

5. **Code Signature Validation (Optional):**

```
$signature = Get-AuthenticodeSignature -FilePath $downloadedFile
if ($signature.Status -ne "Valid") {
    Write-Warning "Code signature invalid or missing."
}
```

5.6 Data Loss Prevention (DLP) & Exfiltration Controls

Prohibitions: - No copying of clinical data (patient records, PHI) from eKVM → jumper server - No copying of eKVM logs containing PHI outside approved evidence collection

Allowed: - Installer binaries: jumper → eKVM (one-way) - Update logs (scrubbed): eKVM → jumper (for evidence package, PHI redacted) - System event logs (Windows Security, Application): filtered exports, no PHI

Detection: - SIEM alerts on large SMB/RDP file transfers from eKVM → jumper (>100 MB) - SIEM alerts on access to patient data directories during maintenance window - Periodic audit of jumper server `C:\Staging` for unauthorized files

---

6. File Transfer Design (Approved Paths)

6.1 Path A: Direct HTTPS Download (Preferred)

Description: Jumper server downloads eKVM binary directly from Ionic CDN via HTTPS.

Prerequisites: - Jumper server has internet egress to `https://downloads.ionic.com` - Firewall/proxy allows HTTPS to allowlisted domains - Operator has credentials for Ionic download portal

Procedure:

```
# Step 1: Download
$url = "https://downloads.ionic.com/ekvm/v3.2.1/eKVM-Firmware-v3.2.1.exe"
$output = "C:\Staging\eKVM\eKVM-Firmware-v3.2.1.exe"
Invoke-WebRequest -Uri $url -OutFile $output -UseBasicParsing

# Step 2: Verify SHA-256 (see section 5.5)
```

Advantages: - No operator workstation → jumper file transfer (reduces attack surface) - Automated, scriptable - Fastest method

6.2 Path B: RDP Drive Mapping (Operator Workstation → Jumper)

Description: Operator's local drive is mapped into RDP session as `\\tsclient\<drive>`.

Prerequisites: - GPO allows drive redirection on jumper server - Operator has binary on local workstation `C:\Downloads\eKVM-Firmware-v3.2.1.exe`

Procedure:

```
# In RDP session to jumper-server-01:
Copy-Item -Path "\\tsclient\C\Downloads\eKVM-Firmware-v3.2.1.exe" `
          -Destination "C:\Staging\eKVM\eKVM-Firmware-v3.2.1.exe"
```

Advantages: - No internet egress requirement - Works in air-gapped scenarios

Disadvantages: - Introduces operator workstation as potential compromise vector - Slower for large files

Security Controls: - Enable drive mapping only during change window (GPO time-based policy) - Scan transferred file with AV/EDR on jumper server immediately - SIEM alert on any `\\tsclient` access outside approved operators

6.3 Path C: Jumper → eKVM via WinRM (Preferred for eKVM Transfer)

Description: PowerShell Remoting to copy file from jumper server to eKVM.

Prerequisites: - WinRM enabled on eKVM (ports 5985/5986 open from jumper IP only) - TrustedHosts configured or Kerberos delegation

Procedure:

```
# On jumper-server-01:
$ekvmSession = New-PSSession -ComputerName ekvm-device-01 `
                             -Credential (Get-Credential LVHN\firstname.lastname.admin)

Copy-Item -Path "C:\Staging\eKVM\eKVM-Firmware-v3.2.1.exe" `
          -Destination "C:\Temp\" `
          -ToSession $ekvmSession
```

```powershell
# Verify hash on eKVM
Invoke-Command -Session $ekvmSession -ScriptBlock {
    $hash = (Get-FileHash -Path "C:\Temp\eKVM-Firmware-v3.2.1.exe" -Algorithm SHA256).Hash
    return $hash
}

Remove-PSSession $ekvmSession
```

Advantages: - Scriptable, auditable (PowerShell transcription) - No SMB file sharing required - Works over HTTPS (port 5986)

6.4 Path D: Jumper → eKVM via SMB (Alternate)

Description: Temporary SMB share on eKVM for file copy.

Prerequisites: - SMB 3.1.1 enabled on eKVM with encryption - Temporary share created with least-privilege access

Procedure:

```powershell
# On eKVM (via RDP):
New-Item -Path "C:\Temp\Update" -ItemType Directory
New-SmbShare -Name "eKVMUpdate$" -Path "C:\Temp\Update" `
             -FullAccess "LVHN\firstname.lastname.admin" `
             -EncryptData $true

# On jumper-server-01:
Copy-Item -Path "C:\Staging\eKVM\eKVM-Firmware-v3.2.1.exe" `
          -Destination "\\ekvm-device-01\eKVMUpdate$\" `
          -Credential (Get-Credential)

# On eKVM: Remove share immediately after transfer
Remove-SmbShare -Name "eKVMUpdate$" -Force
```

Advantages: - Familiar to Windows admins - High transfer speed for large files

Disadvantages: - Requires SMB port 445 open (additional attack surface) - Share must be created/removed per device (manual overhead)

6.5 Decision Matrix

Scenario	Recommended Path	Rationale
Internet egress available	A → C	Fastest, most secure
Air-gapped environment	B → C	No internet required
WinRM not available	B → D	SMB fallback
Large files (>500 MB)	A → D	SMB optimized for bulk transfer

7. Implementation Plan (MOP Summary)

Full Method of Procedure (MOP) detailed in `docs/procedures/MOP-eKVM-Update.md`.

7.1 Pre-Window (H-24 to H-2)

Time	Activity	Owner	Validation
H-24	Confirm target eKVM devices; verify inventory	LVHN IT	Asset list in change ticket
H-24	Enable prerequisites (RDP, WinRM, GPO for drive mapping)	LVHN IT	Connectivity dry-run
H-8	Open scoped network rules (jumper IP → eKVM)	LVHN IT	`Test-NetConnection` from jumper
H-4	Provision named JIT accounts (MFA, time-boxed)	LVHN IT	Account login test
H-2	Dry-run RDP/WinRM/SMB connectivity	Ionic + LVHN	Full path test with 10 MB test file
H-2	Validate SIEM ingestion (force event generation)	LVHN IT	Query SIEM for test event IDs
H-1	GO/NO-GO decision (all prerequisites green)	LVHN IT Lead	Email approval

7.2 Execution Window (H+0 to H+2)

Step	Activity	Command / Action	Validation
1	Connect to jumper server via SSL VPN + RDP	`mstsc /v:jumper-server-01.lvhn.local`	Legal banner displayed
2	Obtain binary (Path A or B)	`Invoke-WebRequest` or RDP copy	File present in `C:\Staging\eKVM`

Step	Activity	Command / Action	Validation
3	Verify SHA-256 (jumper)	`Get-FileHash`	Hash matches published value
4	Scan with AV/EDR	`Start-MpScan`	No threats detected
5	Transfer to eKVM (Path C or D)	`Copy-Item -ToSession` or SMB	File present on eKVM
6	Verify SHA-256 (eKVM)	`Get-FileHash` via RDP/WinRM	Hash matches published value
7	Run installer	`.\eKVM-Firmware-v3.2.1.exe /silent /log:C:\Temp\install.log`	Exit code 0
8	Verify services running	`Get-Service eKVM*`	All "Running"
9	Test P2P/WebRTC connectivity	nCommand Lite sanity check (1 test call)	Call connects successfully
10	Collect evidence (screenshots, logs, hashes)	Copy to `C:\Evidence\CHG0012345\` on jumper	Package complete

7.3 Post-Window (H+1 to H+4)

Time	Activity	Owner	Evidence
H+1	Remove temporary files/shares on eKVM	Ionic/LVHN	`Remove-Item C:\Temp\*.exe`
H+1	Remove JIT account privileges	LVHN IT	Account disabled in AD
H+1	Close network rules (revert ACLs)	LVHN IT	`Test-NetConnection` fails from jumper
H+1	Revert GPOs (disable drive mapping if enabled)	LVHN IT	`GPResult` shows policy reverted
H+2	Compile evidence package	Ionic	ZIP with logs, hashes, screenshots
H+4	Attach evidence to change ticket	Ionic	Change ticket updated, closed

Time	Activity	Owner	Evidence
H+24	Lessons learned review	LVHN + Ionic	Meeting notes; update runbook

---

8. Logging & Evidence (Audit Readiness)

8.1 Required Log Sources

System	Log Source	Key Event IDs	Retention	SIEM Integration
Jumper Server	Windows Security	4624, 4625, 4634, 4776, 4672	6 years	Required
Jumper Server	Microsoft-Windows-TerminalServices-RemoteConnectionManager	21, 24, 25	6 years	Required
Jumper Server	Microsoft-Windows-TerminalServices-LocalSessionManager	21, 22, 24, 25	6 years	Required
Jumper Server	PowerShell/Operational	4103, 4104 (ScriptBlock)	6 years	Required
Jumper Server	SMB-Server/Operational	1006, 1009 (file access)	6 years	Required
eKVM Device	Windows Security	4624, 4625, 4688, 4672	6 years	Required
eKVM Device	TerminalServices logs	21, 22, 24, 25	6 years	Required
eKVM Device	Application log	Installer events (1033, 1034)	6 years	Required

8.2 Key Event IDs Explained

- **4624:** Successful logon (Type 10 = RDP, Type 3 = network/SMB)
- **4625:** Failed logon (alerts on brute-force attempts)
- **4672:** Special privileges assigned to new logon (admin rights)
- **4776:** Domain controller account validation (Kerberos/NTLM)
- **4688:** New process creation (track installer execution)
- **4104:** PowerShell script block logging (captures all PowerShell commands)
- **21 (RDP):** Remote Desktop Services: Session logon succeeded
- **24 (RDP):** Remote Desktop Services: Session disconnected

- **1006 (SMB):** File accessed on SMB share

8.3 Evidence Package Contents

For each update operation, compile a ZIP archive named `LVHN-eKVM-CHG{ChangeNumber}-Evidence.zip`:

```
Evidence Package Structure:
  00_Metadata.txt
      Change ticket number
      Operator name(s)
      Start/end timestamps
      Target eKVM device(s)
      Update version applied
  01_Hashes_Pre_Transfer.txt
      SHA-256 of binary on jumper server
      AV scan results (jumper)
  02_Transfer_Logs.txt
      PowerShell transcript (jumper → eKVM copy)
      File transfer timestamp
  03_Hashes_Post_Transfer.txt
      SHA-256 of binary on eKVM
      AV scan results (eKVM, if applicable)
  04_Installation_Log.txt
      Installer output (C:\Temp\install.log from eKVM)
  05_Service_Verification.txt
      Get-Service output (eKVM services running)
  06_Connectivity_Test.txt
      nCommand Lite sanity check results
  07_Windows_Event_Logs/
      Jumper_Security_4624.evtx (filtered)
      Jumper_PowerShell_4104.evtx (filtered)
      eKVM_Security_4624.evtx (filtered)
      eKVM_Application_Installer.evtx (filtered)
  08_Screenshots/
       01_RDP_Legal_Banner.png
       02_SHA256_Verification_Jumper.png
       03_SHA256_Verification_eKVM.png
       04_Service_Status.png
```

Retention Policy: 6 years (align with healthcare record retention requirements).

8.4 SIEM Queries for Real-Time Monitoring

Example: Detect Unauthorized RDP to eKVM

```
SecurityEvent
| where TimeGenerated >= ago(24h)
```

```
| where EventID == 4624
| where LogonType == 10  // RDP
| where Computer contains "ekvm"
| where IpAddress != "10.50.100.10"  // Jumper server IP
| project TimeGenerated, Account, IpAddress, Computer
| order by TimeGenerated desc
```

Example: Detect Failed Logon Attempts (Brute Force)

```
SecurityEvent
| where TimeGenerated >= ago(1h)
| where EventID == 4625
| where Computer == "ekvm-device-01"
| summarize FailedAttempts = count() by Account, IpAddress
| where FailedAttempts > 5
| order by FailedAttempts desc
```

---

9. Acceptance Criteria

Each update operation must satisfy **all** criteria below to be considered successful:

#	Criterion	Validation Method	Evidence Required
1	Essential prerequisites enabled and validated	Pre-window checklist signed off	Checklist in change ticket
2	Network scoping enforced (jumper IP only)	`Test-NetConnection` from unauthorized host fails	Screenshot of failed test
3	Named JIT account used (no shared accounts)	Windows Security Event 4624 with correct username	Event log export
4	SHA-256 verified pre-transfer (jumper)	Hash comparison script output	`01_Hashes_Pre_Transfer.txt`
5	AV/EDR scan passed (jumper)	`Get-MpThreatDetection` returns no threats	Scan log in evidence package

#	Criterion	Validation Method	Evidence Required
6	SHA-256 verified post-transfer (eKVM)	Hash comparison script output	`03_Hashes_Post_Transfer.txt`
7	Installer exit code = 0	Check `$LASTEXITCODE` in PowerShell	`04_Installation_Log.txt`
8	eKVM services running	`Get-Service eKVM* | Where Status -eq 'Running'`	`05_Service_Verification.txt`
9	P2P/WebRTC connectivity unaffected	nCommand Lite test call successful	`06_Connectivity_Test.txt`
10	Evidence package complete and attached	Review ZIP contents against section 8.3	Change ticket attachment
11	Temporary files/shares removed	Verify `C:\Temp` on eKVM is clean	Post-window validation script
12	Network rules reverted	`Test-NetConnection` from jumper fails post-window	Screenshot of failed test

Rollback Trigger: If any criterion 1-9 fails, do NOT proceed with installation; execute rollback plan (see `docs/procedures/Rollback-Plan.md`).

---

10. Risks & Mitigations

Risk	Likelihood	Impact	Mitigation	Owner
Missing download/drive mapping permissions	Medium	High (blocks execution)	Pre-window dry-run; GO/NO-GO gate at H-1	LVHN IT

Risk	Likelihood	Impact	Mitigation	Owner
Port exposure beyond jumper server	Low	Critical (unauthorized access)	Deny-by-default ACLs; time-boxed rules (auto-revert H+1); SIEM alerts on violations	LVHN IT
Access failure during window	Medium	High (failed change)	Dry-run at H-2; documented rollback plan; on-call escalation path	LVHN IT + Ionic
Shared/no MFA accounts used	Low	Critical (audit failure)	Enforce named JIT accounts in MOP; quarterly privileged access reviews	LVHN IT
Integrity compromise (hash mismatch)	Low	Critical (malware)	Mandatory pre/post SHA-256 verification; AV/EDR scans; alert on mismatch	Ionic + LVHN IT
Clinical workflow disruption	Low	Critical (patient safety)	Updates only during approved windows; sanity check P2P/WebRTC post-install; rollback if issues	Ionic
Evidence package incomplete	Medium	Medium (audit gap)	Automated evidence collection script; validation checklist; quarterly audits	Ionic
Jumper server compromise	Low	Critical (lateral movement)	LVHN responsibility: hardening, patching, monitoring, EDR; Ionic provides guidance only	LVHN IT

11. Roles & Responsibilities (RACI)

RACI Legend: R = Responsible, A = Accountable, C = Consulted, I = Informed

Activity	LVHN IT	Ionic Engineering	LVHN Security	LVHN Compliance
Pre-Window Setup				
Provision SSL VPN access	**R/A**	I	C	I
Harden jumper server	**R/A**	C	C	I
Configure network ACLs	**R/A**	C	C	I
Provision JIT accounts	**R/A**	I	C	I
Enable SIEM ingestion	**R/A**	I	C	C
Execution				
Download/transfer binary	**R**	**A**	I	I
Verify SHA-256	**R**	**A**	I	I
Install update on eKVM	**R**	**A**	I	I
Test P2P/WebRTC	**R**	**A**	I	I
Collect evidence	**R**	**A**	I	C
Post-Window				
Remove JIT privileges	**R/A**	I	C	I
Revert network rules	**R/A**	I	C	I

Activity	LVHN IT	Ionic Engineering	LVHN Security	LVHN Compliance
Review evidence package	C	**R**	**A**	**A**
Update compliance records	C	I	**R**	**A**
Ongoing				
Jumper server patching	**R/A**	I	C	I
Jumper server monitoring	**R/A**	I	C	I
Incident response (jumper)	**R/A**	C	**R**	I
Annual security audit	C	I	**R**	**A**

---

12. Timeline / Milestones

Phase	Duration	Milestone	Deliverable	Owner
Planning	D-10 to D-5	Project kickoff; confirm prerequisites	Prerequisites checklist	LVHN IT + Ionic
Preparation	D-5 to D-3	Share hardening baseline; configure jumper server	Hardened jumper server; GPO configs	LVHN IT
Pre-Window	D-2 to D-1	Setup ACLs, JIT accounts; dry-run connectivity	Dry-run report; GO/NO-GO decision	LVHN IT + Ionic
Pilot	Day D	Execute pilot (2-3 devices)	Pilot execution report; evidence packages	Ionic

Phase	Duration	Milestone	Deliverable	Owner
Validation	D+1	Review pilot results; lessons learned	Lessons learned document; updated MOP	LVHN IT + Ionic
Rollout Phase 1	D+7 to D+14	25% of eKVM fleet	Rollout report (Phase 1)	Ionic
Rollout Phase 2	D+21 to D+28	50% of eKVM fleet	Rollout report (Phase 2)	Ionic
Rollout Phase 3	D+35 to D+42	100% of eKVM fleet	Final rollout report	Ionic
Project Closure	D+49	Final audit review; project retrospective	Closure report; compliance sign-off	LVHN Compliance

Critical Path Items: - D-3: Jumper server hardening complete (prerequisite for pilot) - D-1: Dry-run successful and GO/NO-GO approved - D+1: Pilot evidence reviewed and approved before Phase 1

---

13. Deliverables

Deliverable	Description	Format	Owner	Delivery Date
Method of Procedure (MOP)	Step-by-step execution guide (15-20 pages)	Markdown / PDF	Ionic	D-5
Runbook: WinRM File Transfer	Detailed WinRM configuration and usage	Markdown	Ionic	D-5
Runbook: SMB File Transfer	Hardened SMB share configuration	Markdown	Ionic	D-5
Runbook: RDP Hardening	eKVM RDP security configuration	Markdown	Ionic	D-5
Network Rules Template	ACL syntax for Palo Alto/Cisco/Fortinet	Firewall configs	LVHN IT	D-3
Logging & Evidence Matrix	Event IDs, retention, SIEM queries	Spreadsheet	LVHN IT	D-3

Deliverable	Description	Format	Owner	Delivery Date
Acceptance Criteria Checklist	Pass/fail validation for each criterion	Spreadsheet	Ionic	D-5
Rollback Plan	Step-by-step rollback procedure	Markdown / PDF	Ionic	D-5
Pilot Execution Report	Results from 2-3 pilot devices	PDF	Ionic	D+1
Evidence Packages (Pilot)	ZIP archives per section 8.3	ZIP files	Ionic	D+1
Lessons Learned	Pilot findings; MOP updates	Markdown	LVHN + Ionic	D+1
Phase 1-3 Rollout Reports	Progress, issues, metrics	PDF	Ionic	Per phase +1
Final Compliance Report	Audit summary; evidence retention	PDF	LVHN Compliance	D+49

---

14. Assumptions & Dependencies

14.1 Assumptions

- LVHN has an existing SSL VPN infrastructure with MFA support.
- A Windows Server 2019 or 2022 instance is available for jumper server role.
- LVHN IT has firewall/ACL management capabilities (Palo Alto, Cisco ASA, or equivalent).
- LVHN has a SIEM solution (Splunk, Sentinel, QRadar, or equivalent) with capacity for additional log sources.
- Maintenance windows can be scheduled with 7-day notice (minimum).
- eKVM devices are Windows-based with RDP/WinRM capabilities.
- Target eKVM inventory is documented and accessible to LVHN IT.
- No more than one additional agent will be installed on eKVM devices; this project installs **zero** new agents.

14.2 Dependencies

Dependency	Description	Owner	Status	Risk
SSL VPN availability	Operator access to LVHN network	LVHN IT	Assumed in place	Low
Jumper server provisioning	Dedicated Windows Server for maintenance	LVHN IT	**Pending**	Medium
Internet egress (jumper)	HTTPS to Ionic CDN	LVHN IT	**Pending**	Medium
RDP/WinRM on eKVM	Remote management protocols enabled	LVHN IT	**Pending**	High
Change approval process	CAB approval for pilot and rollout windows	LVHN IT	In progress	Medium
Operator training	Technicians trained on MOP procedures	Ionic + LVHN	**Pending**	Medium
SIEM integration	Log forwarding from jumper and eKVM	LVHN IT	**Pending**	Medium
Binary hosting	Ionic CDN availability	Ionic	In place	Low

Critical Dependencies (High Risk): - RDP/WinRM on eKVM: If eKVM devices do not support remote management, project is blocked. Mitigation: Pre-project device audit (week of D-14).

---

15. Approval

This project proposal requires formal approval from the following stakeholders before proceeding to implementation:

Name	Role	Organization	Approval Date	Signature
[Name]	Director, IT Infrastructure	LVHN	_____	_____

Name	Role	Organization	Approval Date	Signature
[Name]	CISO / Information Security Lead	LVHN		
[Name]	Compliance Officer	LVHN		
[Name]	Clinical Engineering Manager	LVHN		
[Name]	Project Lead	Ionic		

Approval Criteria: - All essential prerequisites (section 3) acknowledged and feasible - Risk mitigations (section 10) acceptable to LVHN Security and Compliance - Timeline (section 12) aligns with LVHN change management calendar - LVHN IT acknowledges sole responsibility for jumper server security hardening, monitoring, and compliance

Digital Signatures Accepted: DocuSign, Adobe Sign, or equivalent with timestamp and identity verification.

Document History:

Version	Date	Author	Changes
0.1	2025-11-01	Ionic Technical Team	Initial draft for internal review
0.9	2025-11-05	Ionic + LVHN IT	Incorporated LVHN feedback; added prerequisite details
1.0	2025-11-11	Ionic Technical Team	Final version for approval

---

Distribution: - LVHN IT Leadership - LVHN Information Security - LVHN Compliance - Ionic Engineering - Ionic Program Management

Confidentiality: This document contains proprietary technical information and is intended solely for LVHN and Ionic personnel involved in this project.

End of Proposal