Technology Stack Specification – LVHN eKVM Remote Update

Document Control - **Version:** 1.0 - **Date:** 2025-11-11 - **Classification:** Internal – Technical Specification - **Owner:** Ionic Engineering Team - **Platform:** Microsoft Windows

---

Configuration Custody Notice
Ionic Health engineering exclusively manages all eKVM configuration, firmware, and software changes, including patching operations executed via the jumper server. LVHN operations is solely responsible for provisioning, hardening, and maintaining the Windows jumper server in line with the requirements defined in this specification. Any cross-domain action demands documented approval from both organizations.

Network Visibility Scope
The specification assumes Ionic Health requires no access to LVHN s internal network beyond the jumper server footprint and its controlled outbound route to Ionic eKVM devices hosted on public IP.

1. Executive Summary

This document defines the complete Microsoft Windows-based technology stack for the LVHN eKVM Remote Update project. All components are based on native Windows technologies to leverage existing LVHN infrastructure, minimize licensing costs, and align with LVHN IT expertise.

Core Principles: - **Native Windows:** Prefer built-in Windows features over third-party tools - **Zero New Agents:** No additional software installed on eKVM devices - **Enterprise-Ready:** Proven Microsoft technologies with long-term support - **Compliance-First:** FIPS 140-2, HIPAA, NIST SP 800-53 aligned - **Cost-Effective:** Leverage existing Windows Server licenses

---

1.1 Critical Infrastructure Ownership

IMPORTANT: Infrastructure Components are LVHN Responsibility

This document provides **RECOMMENDATIONS ONLY** for the following components. Final technology selection, procurement, configuration, and maintenance are **LVHN's sole responsibility**:

- **SSL VPN Solution** (e.g., Palo Alto, Cisco, Fortinet) – LVHN selects and manages

- **Privileged Access Management (PAM)** (e.g., CyberArk, BeyondTrust) – LVHN selects and manages
- **SIEM Platform** (e.g., Microsoft Sentinel, Splunk, QRadar) – LVHN selects and manages
- **Firewall** (e.g., Palo Alto, Cisco, Fortinet) – LVHN existing infrastructure
- **Active Directory** – LVHN existing infrastructure
- **DNS/DHCP** – LVHN existing infrastructure
- **Network Infrastructure** – LVHN existing infrastructure

Ionic Responsibilities: - Provide technical requirements and recommendations - Ensure eKVM devices are compatible with standard Windows protocols - Provide implementation guidance and best practices - Support eKVM device configuration within LVHN infrastructure

LVHN Responsibilities: - Select, procure, and deploy all infrastructure components - Configure and harden jumper server - Manage VPN, firewall, PAM, SIEM - Maintain compliance and security of infrastructure - Operational support and monitoring

---

2. Operating Systems

2.1 Windows Jumper Server

Recommended OS: Windows Server 2022 Standard Edition

Component	Version	Justification
OS Edition	Windows Server 2022 Standard	Latest LTS release (support until 2031); includes all required features
Alternative	Windows Server 2019 Standard	If 2022 not available; support until 2029
Build	20348.x or later	Latest cumulative updates applied
Installation Type	Server Core (preferred) or Desktop Experience	Server Core reduces attack surface; Desktop Experience for GUI management

Key Features Enabled: - Remote Desktop Services (RDP) - Windows Remote Management (WinRM) - File and Storage Services (SMB 3.1.1) - Windows Defender / Microsoft Defender for Endpoint - PowerShell 7.x - Event Log Forwarding

Hardening Baseline: - CIS Benchmark for Windows Server 2022 Level 1 (minimum) - Microsoft Security Compliance Toolkit (SCT) applied - STIG (Security Technical Implementation Guide) if DoD compliance required

---

2.2 eKVM Device OS

> **CRITICAL: eKVM OS is FIXED and NOT MODIFIABLE**
>
> The eKVM device operating system is pre-configured by Ionic and **cannot be changed** by LVHN. All configurations must work with the existing OS.

Fixed OS Specification (Provided by Ionic):

Component	Specification	Notes
OS Edition	Windows 11 Pro	**FIXED** – Cannot be changed
Architecture	64-bit	x64 processor architecture
Version	24H2	Latest Windows 11 feature update (October 2024)
OS Build	26100.4202	Current build as of 2025-11-11
Installation Type	Full Desktop Experience	Required for nCommand Lite GUI
Update Channel	General Availability Channel	Receives monthly cumulative updates

Pre-Installed Windows Features (Cannot Modify): - Remote Desktop (RDP) – **CAN be enabled/disabled via configuration** - Windows Remote Management (WinRM) – **CAN be enabled/disabled via configuration** - SMB Client – Built-in, available for file transfer - Windows Defender Antivirus – Built-in, active by default

Important Constraints: - Cannot reinstall or change Windows edition - Cannot downgrade to Windows 10 - Cannot switch to IoT Enterprise or

LTSC - CAN enable/disable RDP, WinRM during maintenance windows - CAN apply Windows Updates (monthly cumulative updates) - CAN configure security settings (GPO, registry, firewall)

Compatibility Notes: - Windows 11 Pro includes all features required for this project - RDP 10.12+ (native to Windows 11 24H2) - WinRM 3.0 (PowerShell 5.1 built-in) - SMB 3.1.1 with encryption support - TLS 1.3 support (native) - FIPS 140-2 validated cryptographic modules

---

3. Remote Access Technologies

3.1 Remote Desktop Protocol (RDP)

Version: RDP 10.x (Windows Server 2022) / RDP 8.x (Windows Server 2019)

Protocol Stack:

```
Application Layer:    Remote Desktop Services (TermSvcs)
Security Layer:       TLS 1.2 / TLS 1.3
Authentication:       Network Level Authentication (NLA) with Kerberos or NTLM
Encryption:           128-bit AES (minimum), 256-bit AES (preferred)
Port:                 TCP 3389 (default, can be changed)
```

Configuration Parameters:

```
# Registry: HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp
SecurityLayer = 2          # TLS
UserAuthentication = 1     # NLA required
MinEncryptionLevel = 3     # High (128-bit minimum)
fEnableWinStation = 1      # RDP enabled
```

Client Requirements: - Windows Remote Desktop Connection (mstsc.exe) 6.0 or later - Supports NLA (CredSSP or Kerberos) - TLS 1.2+ capable

Supported Operating Systems (Client): - Windows 10/11 Pro/Enterprise (built-in) - Windows Server 2016/2019/2022 (built-in) - macOS: Microsoft Remote Desktop (App Store) - Linux: Remmina, FreeRDP (with NLA support)

3.2 Windows Remote Management (WinRM)

Version: WinRM 3.0 (PowerShell 5.1+) / WinRM 5.1 (PowerShell 7.x)

Protocol Stack:

```
Application Layer:    WS-Management (SOAP-based)
Transport:            HTTP (port 5985) or HTTPS (port 5986)
Security:             Kerberos, NTLM, or CredSSP authentication
Encryption:           TLS 1.2+ for HTTPS transport
```

Configuration:

```
# Enable WinRM with HTTPS
Enable-PSRemoting -Force
New-SelfSignedCertificate -DnsName "jumper-server-01.lvhn.local" -CertStoreLocation Cert:\Lo
New-Item -Path WSMan:\localhost\Listener -Transport HTTPS -Address * -CertificateThumbprint
```

Firewall Rules: - Port 5985 (HTTP) – Allow from jumper server IP only - Port 5986 (HTTPS) – Preferred; allow from jumper server IP only

PowerShell Remoting: - New-PSSession, Enter-PSSession, Invoke-Command - Copy-Item -ToSession / -FromSession for file transfers

---

3.3 Server Message Block (SMB)

Version: SMB 3.1.1 (Windows Server 2022) / SMB 3.0.2 (Windows Server 2019)

Protocol Features:

```
Version:              SMB 3.1.1 (dialect 311)
Encryption:           AES-128-CCM or AES-128-GCM
Signing:              Required for all connections
Port:                 TCP 445
Multichannel:         Enabled (for high-speed transfers)
```

Security Configuration:

```
# Enforce SMB encryption
Set-SmbServerConfiguration -EncryptData $true -RequireSecuritySignature $true

# Disable SMB 1.0 (security risk)
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

Use Case: Alternate file transfer method when WinRM unavailable

---

4. File Transfer Technologies

4.1 HTTPS (Direct Download)

Technology: PowerShell Invoke-WebRequest / Invoke-RestMethod

Configuration:

```
# Download with TLS 1.2
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
Invoke-WebRequest -Uri "https://downloads.ionic.com/ekvm/firmware.exe" -OutFile "C:\Staging\
```

Requirements: - TLS 1.2 or TLS 1.3 support - Firewall allows HTTPS egress (port 443) to allowlisted domains - Proxy support (if required): -Proxy parameter

Allowlisted Domains: `- downloads.ionic.com - cdn.ionic.com - updates.ionic.com`

4.2 RDP Drive Mapping

Technology: Remote Desktop Services Client Drive Redirection

Configuration:

```
Group Policy: Computer Configuration
    Administrative Templates
        Windows Components
            Remote Desktop Services
                Remote Desktop Session Host
                    Device and Resource Redirection
                        Do not allow drive redirection = Disabled (during window)
```

Access Pattern:

```
\\tsclient\<drive-letter>\<path>
Example: \\tsclient\C\Downloads\firmware.exe
```

Security Controls: - Enable drive mapping only during maintenance window (GPO scheduled task) - Revert to "Do not allow drive redirection = Enabled" post-window - SIEM alert on any `\\tsclient` access outside approved operators

---

4.3 WinRM File Copy

Technology: PowerShell Remoting Copy-Item cmdlet

Syntax:

```
$session = New-PSSession -ComputerName ekvm-01 -Credential $cred
Copy-Item -Path "C:\Staging\firmware.exe" -Destination "C:\Temp\" -ToSession $session
Remove-PSSession $session
```

Performance: - Transfer speed: ~50-100 MB/s (depends on network) - Max file size: Limited by available memory (MaxMemoryPerShellMB) - Optimal for files: 10 MB - 500 MB

4.4 SMB File Share

Technology: Windows File Sharing (SMB 3.1.1)

Setup:

```
# On eKVM (temporary share)
New-SmbShare -Name "eKVMUpdate$" -Path "C:\Temp\Update" -FullAccess "LVHN\admin" -EncryptDat

# On jumper server
Copy-Item -Path "C:\Staging\firmware.exe" -Destination "\\ekvm-01\eKVMUpdate$\"

# Cleanup
Remove-SmbShare -Name "eKVMUpdate$" -Force
```

Security: - Hidden share name (trailing $) - SMB encryption enforced (-EncryptData $true) - Temporary share (create/remove per device) - Least privilege access (specific user only)

---

5. Security Technologies

5.1 Encryption

Component	Technology	Standard	Key Length
Transport Encryption (RDP)	TLS 1.2 / TLS 1.3	IETF RFC 5246, 8446	128-bit AES (min), 256-bit AES (preferred)
Transport Encryption (WinRM)	TLS 1.2 / TLS 1.3	IETF RFC 5246, 8446	128-bit AES (min), 256-bit AES (preferred)
File Transfer Encryption (SMB)	AES-128-GCM	SMB 3.1.1 spec	128-bit AES
Hash Algorithm	SHA-256	NIST FIPS 180-4	256-bit
Data at Rest (Jumper Server)	BitLocker	FIPS 140-2 validated	128-bit or 256-bit AES
Data at Rest (eKVM)	BitLocker (if enabled by Ionic)	FIPS 140-2 validated	128-bit or 256-bit AES

PowerShell Hash Verification:

```
Get-FileHash -Path "firmware.exe" -Algorithm SHA256
```

5.2 Anti-Malware / Endpoint Detection and Response (EDR)

Primary Solution: Microsoft Defender for Endpoint (MDE)

Component	Technology	Version	Deployment
Antivirus Engine	Microsoft Defender Antivirus	Built-in to Windows 10/11/Server	Enabled by default
EDR Platform	Microsoft Defender for Endpoint Plan 1 or Plan 2	Cloud-based	Optional (recommended)
Threat Intelligence	Microsoft Defender Threat Intelligence	Cloud-updated	Automatic updates
Scanning	Real-time protection + on-demand scans	N/A	Configured via GPO

Alternative Solutions (if MDE not available): - Symantec Endpoint Protection - CrowdStrike Falcon - Trend Micro Apex One - Any FIPS 140-2 validated AV/EDR

Configuration:

```
# Enable real-time protection
Set-MpPreference -DisableRealtimeMonitoring $false

# Scan file before transfer
Start-MpScan -ScanPath "C:\Staging\firmware.exe" -ScanType CustomScan

# Check for threats
Get-MpThreat
```

Update Frequency: Daily definition updates (automatic via Windows Update)

5.3 Firewall

Technology: Windows Defender Firewall with Advanced Security

Management: - Local: `wf.msc` (Windows Defender Firewall with Advanced Security snap-in) - Group Policy: `Computer Configuration → Policies → Windows Settings → Security Settings → Windows Defender Firewall` - PowerShell: `New-NetFirewallRule`, `Set-NetFirewallRule`

Profile Configuration:

```
Domain Profile:     Enabled (default deny inbound, allow outbound)
Private Profile:    Enabled (default deny inbound, allow outbound)
Public Profile:     Enabled (block all inbound, allow outbound)
```

Required Rules:

```
# RDP (scoped to jumper IP)
New-NetFirewallRule -Name "RDP-Jumper-Only" -DisplayName "RDP from Jumper Server" `
                    -Enabled True -Direction Inbound -Protocol TCP -LocalPort 3389 `
                    -RemoteAddress 10.50.100.10 -Action Allow -Profile Domain

# WinRM HTTPS (scoped to jumper IP)
New-NetFirewallRule -Name "WinRM-HTTPS-Jumper-Only" -DisplayName "WinRM HTTPS from Jumper Se
                    -Enabled True -Direction Inbound -Protocol TCP -LocalPort 5986 `
                    -RemoteAddress 10.50.100.10 -Action Allow -Profile Domain
```

Logging: - Path: `%SystemRoot%\System32\LogFiles\Firewall\pfirewall.log` - Log dropped packets: Yes - Log successful connections: Yes (for RDP/WinRM rules)

---

6. Authentication & Identity

6.1 Active Directory (AD)

Role: Centralized user and computer account management

Domain Controller OS: Windows Server 2016/2019/2022 (LVHN responsibility)

Functional Level: - Domain Functional Level: Windows Server 2016 (minimum) - Forest Functional Level: Windows Server 2016 (minimum)

Account Types:

```
User Accounts:        firstname.lastname@lvhn.local (UPN)
Admin Accounts:       firstname.lastname.admin (JIT accounts)
Computer Accounts:    JUMPER-SERVER-01$ (jumper server), EKVM-DEVICE-01$ (eKVM)
```

Group Policy Objects (GPOs): - `GPO-Jumper-Server-Hardening` - `GPO-eKVM-RDP-Hardening` - `GPO-eKVM-WinRM-Config` - `GPO-eKVM-Maintenance-Window` (time-based drive mapping)

6.2 Multi-Factor Authentication (MFA)

SSL VPN MFA: - **Technology:** LVHN SSL VPN solution (e.g., Palo Alto GlobalProtect, Cisco AnyConnect, Fortinet FortiClient) - **MFA Methods:** -

Hardware token (YubiKey, RSA SecurID) - Software token (Microsoft Authenticator, Duo Mobile) - SMS OTP (least preferred) - **Enforcement:** Mandatory for all VPN connections

Jumper Server MFA (Optional Enhancement): - **Technology:** Microsoft Entra ID (Azure AD) Multi-Factor Authentication - **Integration:** Windows Hello for Business or third-party MFA (Duo Security) - **Use Case:** Second MFA challenge when accessing jumper server via RDP

6.3 Privileged Access Management (PAM)

Recommended Solution: Microsoft LAPS (Local Administrator Password Solution)

Configuration:

```
# Install LAPS on jumper server
Install-WindowsFeature -Name RSAT-AD-PowerShell
Import-Module AdmPwd.PS

# Configure LAPS GPO
Set-AdmPwdComputerSelfPermission -Identity "OU=JumperServers,DC=lvhn,DC=local"
```

Alternative Solutions: - CyberArk Privileged Access Manager - BeyondTrust Privileged Remote Access - Thycotic Secret Server

JIT Account Workflow: 1. Operator requests JIT account (change ticket) 2. LVHN IT provisions `firstname.lastname.admin` with 4-hour expiration 3. Account disabled automatically at H+4 (post-window) 4. LAPS rotates local admin passwords daily

---

6.4 Certificate Services

Technology: Active Directory Certificate Services (AD CS)

Certificate Types:

```
1. RDP Server Certificate (jumper server, eKVM devices)
   - Subject: CN=jumper-server-01.lvhn.local
   - Key Usage: Server Authentication
   - Validity: 2 years

2. WinRM HTTPS Certificate (jumper server, eKVM devices)
   - Subject: CN=jumper-server-01.lvhn.local
   - SAN: DNS:jumper-server-01, DNS:jumper-server-01.lvhn.local
   - Key Usage: Server Authentication
   - Validity: 2 years
```

```
3. Code Signing Certificate (optional, for Ionic binaries)
   - Subject: CN=Ionic Inc, O=Ionic, C=US
   - Key Usage: Code Signing
   - Validity: 3 years
```

Certificate Enrollment: - Automatic via Group Policy (computer certificates) - Manual via `certreq` or MMC Certificates snap-in

Certificate Revocation: - CRL (Certificate Revocation List) published via HTTP - OCSP (Online Certificate Status Protocol) preferred

---

7. Monitoring & Logging

7.1 Windows Event Logging

Event Logs to Collect:

Log Name	Key Event IDs	Retention (Local)	Forward to SIEM
Security	4624, 4625, 4634, 4672, 4688, 4776	90 days	Yes
System	6005, 6006, 7036, 7040	90 days	Yes
Application	1000, 1001, 1033, 1034	90 days	Yes
Microsoft-Windows-TerminalServices-LocalSessionManager/Operational	21, 22, 24, 25	90 days	Yes
Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational	21, 24, 25, 39, 40	90 days	Yes
Microsoft-Windows-PowerShell/Operational	4103, 4104 (ScriptBlock Logging)	90 days	Yes
Microsoft-Windows-WinRM/Operational	6, 8, 142, 161	90 days	Yes
Microsoft-Windows-SMBServer/Operational	1006, 1009	30 days	Yes

Configuration:

```
# Enable PowerShell ScriptBlock Logging
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogg
                 -Name "EnableScriptBlockLogging" -Value 1

# Enable PowerShell Module Logging
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging"
                 -Name "EnableModuleLogging" -Value 1
```

Log Size Limits: - Security: 1 GB (auto-archive) - System: 512 MB - Application: 512 MB - TerminalServices logs: 100 MB each - PowerShell: 512 MB

7.2 SIEM (Security Information and Event Management)

Recommended Solutions (LVHN Choice):

SIEM Platform	Deployment	Log Ingestion Method	Cost Model
Microsoft Sentinel	Cloud (Azure)	Azure Monitor Agent (AMA) or Log Analytics Agent	Per GB ingested
Splunk Enterprise	On-premises or cloud	Splunk Universal Forwarder	Per GB/day license
IBM QRadar	On-premises or cloud	WinCollect agent	Per EPS (events/sec)
LogRhythm	On-premises or cloud	System Monitor agent	Per log source

Log Forwarding Technology: - **Windows Event Forwarding (WEF):** Built-in; push or pull model - **Agent-based:** Splunk UF, Azure Monitor Agent, QRadar WinCollect

Configuration Example (WEF):

```
# On jumper server / eKVM (source)
wecutil qc

# On SIEM collector (destination)
winrm quickconfig
wecutil cs subscription.xml  # Import subscription config
```

Sample Subscription XML:

```
<Subscription xmlns="http://schemas.microsoft.com/2006/03/windows/events/subscription">
  <SubscriptionId>LVHN-eKVM-Security-Events</SubscriptionId>
  <Query>
```

```
    <QueryList>
      <Query Id="0">
        <Select Path="Security">*[System[(EventID=4624 or EventID=4625)]]</Select>
      </Query>
    </QueryList>
  </Query>
</Subscription>
```

7.3 Performance Monitoring

Technology: Windows Performance Monitor (PerfMon)

Key Counters:

```
Processor:              % Processor Time
Memory:                 Available MBytes, % Committed Bytes In Use
LogicalDisk:            % Free Space, Avg. Disk Queue Length
Network Interface:      Bytes Total/sec, Packets/sec
Terminal Services:      Active Sessions, Inactive Sessions
```

Data Collector Sets: - Create custom DCS for jumper server baseline - Run 24-hour baseline before pilot - Alert on: CPU >80%, Memory <10% free, Disk <15% free

Optional: System Center Operations Manager (SCOM) for enterprise monitoring

---

8. Automation & Scripting

8.1 PowerShell

Version: PowerShell 7.4.x (latest LTS) or PowerShell 5.1 (Windows built-in)

Installation:

```
# Install PowerShell 7.x (on jumper server)
winget install Microsoft.PowerShell
```

Modules Required:

Module Name	Purpose	Installation
PSReadLine	Enhanced command-line editing	Built-in (PS 7.x)

Module Name	Purpose	Installation
PowerShellGet	Module installation from PSGallery	Built-in
Pester	Unit testing for scripts	`Install-Module -Name Pester`
PSScriptAnalyzer	Script linting and best practices	`Install-Module -Name PSScriptAnalyzer`
ActiveDirectory	AD cmdlets	`Install-WindowsFeature RSAT-AD-PowerShell`

Execution Policy:

```
# Set execution policy (allow signed scripts)
Set-ExecutionPolicy RemoteSigned -Scope LocalMachine

# Verify
Get-ExecutionPolicy -List
```

Script Examples: - `Validate-Prerequisites.ps1` (pre-window validation) - `Copy-FirmwareToEKVM.ps1` (WinRM file transfer) - `Verify-SHA256.ps1` (integrity verification) - `Collect-Evidence.ps1` (post-window evidence gathering)

PowerShell Transcription:

```
Start-Transcript -Path "C:\Evidence\CHG0012345\transcript-$(Get-Date -Format 'yyyyMMdd-HHmms
# ... operations ...
Stop-Transcript
```

8.2 Task Scheduler

Technology: Windows Task Scheduler

Use Cases: 1. **Pre-Window Automation:** - Task: Enable RDP drive mapping (GPO modification) - Trigger: 1 hour before maintenance window - Action: `Set-GPRegistryValue` (PowerShell)

2. **Post-Window Cleanup:**
   - Task: Disable JIT accounts, revert GPOs
   - Trigger: 1 hour after maintenance window end
   - Action: `Disable-ADAccount` (PowerShell)

Configuration:

```
# Create scheduled task (example)
$action = New-ScheduledTaskAction -Execute "PowerShell.exe" `
          -Argument "-File C:\Scripts\Enable-DriveMapping.ps1"
```

```
$trigger = New-ScheduledTaskTrigger -Once -At "18:00" -RepetitionInterval (New-TimeSpan -Day
Register-ScheduledTask -TaskName "Enable-DriveMapping-PreWindow" -Action $action -Trigger $t
```

8.3 Group Policy Management

Technology: Group Policy Management Console (GPMC)

Installation:

```
Install-WindowsFeature -Name GPMC
```

Key GPOs for Project:

GPO Name	Scope	Purpose
`GPO-Jumper-Hardening`	Jumper Server OU	RDP hardening, firewall rules, security baselines
`GPO-eKVM-RDP-Config`	eKVM OU	RDP settings (NLA, TLS, encryption)
`GPO-eKVM-WinRM-Config`	eKVM OU	WinRM listeners, TrustedHosts (if needed)
`GPO-eKVM-Maintenance-Window`	eKVM OU	Time-based drive mapping enable/disable
`GPO-Audit-Logging`	All systems	Enable advanced audit policies, log sizes

GPO Deployment:

```
# Link GPO to OU
New-GPLink -Name "GPO-Jumper-Hardening" -Target "OU=JumperServers,DC=lvhn,DC=local"

# Force GPO update
gpupdate /force
```

8.4 Desired State Configuration (DSC)

Technology: PowerShell Desired State Configuration (DSC)

Use Case: Automated jumper server baseline configuration

Example DSC Configuration:

```
Configuration JumperServerBaseline {
    Node "jumper-server-01" {
        WindowsFeature RDS {
            Ensure = "Present"
```

```
            Name = "RDS-RD-Server"
        }

        Registry RDPEncryption {
            Ensure = "Present"
            Key = "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tc
            ValueName = "MinEncryptionLevel"
            ValueData = 3
            ValueType = "Dword"
        }

        Service WinRM {
            Name = "WinRM"
            State = "Running"
            StartupType = "Automatic"
        }
    }
}
```

Deployment:

```
JumperServerBaseline -OutputPath "C:\DSC"
Start-DscConfiguration -Path "C:\DSC" -Wait -Verbose
```

---

9. Network Infrastructure

9.1 Virtual Private Network (VPN)

Technology Options (LVHN Existing):

VPN Solution	Vendor	Protocol	MFA Support
GlobalProtect	Palo Alto Networks	SSL/TLS	Yes (SAML, RADIUS)
AnyConnect	Cisco	SSL/TLS, IPsec	Yes (Duo, RSA, RADIUS)
FortiClient	Fortinet	SSL/TLS, IPsec	Yes (FortiToken, RADIUS)
Always On VPN	Microsoft (Windows Server)	IKEv2, SSTP	Yes (via NPS/RADIUS)

Configuration Requirements: - Split tunneling: Allow (only Ionic CDN and eKVM subnet routed via VPN) - MFA: Mandatory - Allowed client OS: LVHN-managed Windows 10/11 devices only - Session timeout: 8 hours (re-authenticate)

9.2 Firewall

Recommended Solutions (LVHN Existing):

Firewall Platform	Management	Features Used
Palo Alto PA-Series	Panorama (centralized)	App-ID, User-ID, URL Filtering, Threat Prevention
Cisco ASA / Firepower	ASDM / FMC	Access rules, VPN, IPS
Fortinet FortiGate	FortiManager	Firewall policies, SD-WAN, SSL Inspection
Check Point	SmartConsole	Firewall rules, IPS, Application Control

Required ACL Rules:

```
Rule 1: Allow VPN → Jumper Server (RDP)
  Source: SSL-VPN-Pool (10.200.0.0/24)
  Destination: Jumper-Server-01 (10.50.100.10)
  Service: TCP/3389
  Action: Allow
  Logging: Yes

Rule 2: Allow Jumper → eKVM Subnet (RDP, WinRM, SMB)
  Source: Jumper-Server-01 (10.50.100.10)
  Destination: eKVM-Subnet (10.60.200.0/24)
  Service: TCP/3389, 5985, 5986, 445
  Schedule: Maintenance-Window-Only
  Action: Allow
  Logging: Yes

Rule 3: Allow Jumper → Internet (HTTPS for downloads)
  Source: Jumper-Server-01 (10.50.100.10)
  Destination: ionic.com, *.ionic.com
  Service: TCP/443
  Action: Allow
  Logging: Yes

Rule 4: Default Deny
  Source: Any
  Destination: eKVM-Subnet (10.60.200.0/24)
  Service: Any
```

```
Action: Deny
Logging: Yes (denied connections)
```

9.3 DNS

Technology: Windows DNS Server (Active Directory-integrated)

DNS Records Required:

```
A Record:     jumper-server-01.lvhn.local → 10.50.100.10
A Record:     ekvm-device-01.lvhn.local → 10.60.200.101
A Record:     ekvm-device-02.lvhn.local → 10.60.200.102
PTR Record:   10.10.50.100.in-addr.arpa → jumper-server-01.lvhn.local
```

DNS Security: - DNSSEC: Recommended (if supported by LVHN) - DNS over HTTPS (DoH): Optional enhancement

---

9.4 Network Time Protocol (NTP)

Technology: Windows Time Service (W32Time)

Configuration:

```
# Configure NTP server (on jumper server)
w32tm /config /manualpeerlist:"time.nist.gov,0x8" /syncfromflags:manual /reliable:YES /updat
w32tm /resync

# Verify
w32tm /query /status
```

Importance: Accurate time synchronization critical for: - Kerberos authentication (±5 min tolerance) - Log correlation across systems - Certificate validation

---

10. Development & DevOps Tools

10.1 Version Control

Technology: Git (command-line) + GitHub (repository hosting)

Installation:

```
winget install Git.Git
```

Repository Structure:

```
jumpserver/
  .github/
```

```
docs/
runbooks/
specs/
scripts/          # PowerShell automation scripts
   pre-window/
   execution/
   post-window/
tests/            # Pester tests
```

Commit Workflow:

```
git checkout -b feature/update-mop-section-5
# Make changes
git add docs/procedures/MOP-eKVM-Update.md
git commit -m "docs: Update MOP section 5 with new validation steps"
git push origin feature/update-mop-section-5
```

10.2 Documentation Tools

Primary: Markdown (.md files)

Editors: - Visual Studio Code with extensions: - Markdown All in One - markdownlint - Markdown Preview Enhanced - Typora (WYSIWYG Markdown editor)

Diagram Tools: - draw.io (diagrams.net) – for architecture diagrams - PlantUML – for sequence diagrams (as code) - Microsoft Visio (if available)

10.3 Testing Tools

PowerShell Testing: Pester

Installation:

```
Install-Module -Name Pester -Force
```

Example Test:

```
# tests/Validate-Prerequisites.Tests.ps1
Describe "Pre-Window Prerequisites" {
    It "Jumper server RDP port is reachable" {
        $result = Test-NetConnection -ComputerName jumper-server-01 -Port 3389
        $result.TcpTestSucceeded | Should -Be $true
    }

    It "SHA-256 hash matches expected value" {
        $actualHash = (Get-FileHash -Path "C:\Staging\firmware.exe" -Algorithm SHA256).Hash
```

```
        $expectedHash = "a1b2c3d4e5f6..."
        $actualHash | Should -Be $expectedHash
    }
}
```

Run Tests:

```
Invoke-Pester -Path ".\tests\" -Output Detailed
```

---

11. Licensing & Cost Model

11.1 Windows Server Licensing

Jumper Server: - **License:** Windows Server 2022 Standard (1 license) - **CAL Requirements:** None (RDP connections use eKVM device CALs or VDA) - **Estimated Cost:** $972 (Standard) or $6,155 (Datacenter) retail (LVHN may have volume licensing)

Note: LVHN likely has existing Enterprise Agreement (EA) or volume licensing; incremental cost may be $0.

11.2 Remote Desktop Services (RDS) Licensing

RDS CAL Requirements: - Not required if jumper server only used for administrative access (not user sessions) - If RDS required: ~$120/device CAL or ~$168/user CAL

Project Assessment: RDS CALs not required (administrative use only)

11.3 Microsoft Defender for Endpoint

License: Microsoft Defender for Endpoint Plan 1 or Plan 2

Edition	Cost (per device/month)	Features
Plan 1	~$3-5	Next-gen AV, attack surface reduction, EDR
Plan 2	~$5-7	Plan 1 + automated investigation, threat hunting, advanced hunting

Project Scope: 1 jumper server + ~50-100 eKVM devices = $150-700/month (Plan 1)

Alternative: Use built-in Windows Defender Antivirus (free) without EDR capabilities

---

11.4 SIEM Licensing

SIEM	Cost Model	Estimated Cost (100 devices)
Microsoft Sentinel	Per GB ingested	~$200-500/month (estimate: 50-100 GB/month)
Splunk	Per GB/day	~$150/GB/day (~$2,250/month for 15 GB/day)
QRadar	Per EPS	~$10,000-20,000/year (500 EPS)

Project Assumption: LVHN has existing SIEM; incremental cost = log ingestion only

---

11.5 Total Cost of Ownership (TCO) – 3 Years

Component	Year 1	Year 2	Year 3	3-Year Total
Jumper Server Hardware (if new)	$5,000	$0	$0	$5,000
Windows Server License	$1,000	$0	$0	$1,000
MDE Plan 1 (100 devices)	$6,000	$6,000	$6,000	$18,000
SIEM (incremental)	$2,400	$2,400	$2,400	$7,200
VPN Licenses (if new)	$0	$0	$0	$0 (existing)
Labor (LVHN IT)	$10,000	$2,000	$2,000	$14,000
Labor (Ionic)	$15,000	$3,000	$3,000	$21,000
TOTAL	$39,400	$13,400	$13,400	**$66,200**

Cost Savings vs. Atera: - Atera RMM: ~$100/month/technician × 5 technicians = $6,000/year - 3-year Atera cost: $18,000 - Net savings: $18,000 - $7,200 (incremental SIEM) = **$10,800 over 3 years**

---

12. System Requirements

12.1 Jumper Server Hardware

Minimum Specifications:

Component	Minimum	Recommended	Notes
CPU	4 vCPUs (2.0 GHz)	8 vCPUs (2.5 GHz+)	Intel Xeon or AMD EPYC
RAM	8 GB	16 GB	For concurrent RDP/WinRM sessions
Storage	100 GB	250 GB SSD	C: (OS) + D: (staging)
Network	1 Gbps NIC	10 Gbps NIC or dual 1 Gbps (teamed)	Low latency preferred
Form Factor	Virtual Machine (VMware, Hyper-V)	Physical server (if required)	VM preferred for flexibility

Storage Layout:

```
C:\ (OS)              80 GB  (NTFS)
D:\ (Staging)         150 GB (NTFS, BitLocker encrypted)
E:\ (Evidence)        20 GB  (NTFS, BitLocker encrypted)
```

12.2 eKVM Device Hardware and Software

CRITICAL: eKVM specifications are FIXED and NOT MODIFIABLE by LVHN

Provided and Managed by Ionic (Fixed Specifications):

Component	Fixed Specification	Modifiable by LVHN?
CPU	Intel Core i5 or i7 (8th gen+)	No (hardware)
RAM	8-16 GB DDR4	No (hardware)
Storage	256-512 GB SSD	No (hardware)
Network	Dual 1 Gbps NICs (redundancy)	No (hardware)
GPU	Integrated or discrete (for video processing)	No (hardware)
OS Edition	**Windows 11 Pro**	No (cannot change edition)
OS Architecture	**64-bit (x64)**	No
OS Version	**24H2 (2024 Update)**	No (cannot downgrade)

Component	Fixed Specification	Modifiable by LVHN?
OS Build	**26100.4202** (as of 2025-11-11)	Updates via Windows Update only
nCommand Lite	Ionic proprietary application	No (managed by Ionic)

What LVHN CAN Configure: - Enable/disable RDP (via registry or GPO) - Enable/disable WinRM (via PowerShell or GPO) - Windows Firewall rules (ports 3389, 5985, 5986, 445) - Apply Windows Updates (monthly cumulative updates) - Configure security settings (NLA, TLS, encryption levels) - Create local user accounts (for maintenance access) - Install Windows Defender definitions (automatic)

What LVHN CANNOT Do: - Reinstall or reimage the operating system - Change from Windows 11 Pro to Enterprise/IoT/LTSC - Downgrade to Windows 10 - Modify hardware components (CPU, RAM, storage) - Uninstall or modify nCommand Lite application - Change OS architecture (64-bit to 32-bit)

Important Notes: - eKVM hardware and software managed entirely by Ionic - LVHN responsible only for network connectivity and remote access configuration - All maintenance procedures must work with existing Windows 11 Pro 24H2 Build 26100.4202 - Jumper server must support standard Windows protocols compatible with Windows 11

12.3 Network Requirements

Bandwidth: - Jumper → eKVM: 100 Mbps minimum (for 500 MB firmware transfer in <1 min) - Jumper → Internet: 50 Mbps minimum (for CDN downloads) - VPN → Jumper: 10 Mbps minimum (for operator RDP sessions)

Latency: - Jumper → eKVM: <10 ms (same data center preferred) - Jumper → Internet: <100 ms (CDN) - VPN → Jumper: <50 ms (acceptable for RDP responsiveness)

Availability: - Jumper Server: 99.5% uptime (planned maintenance windows allowed) - eKVM Network: 99.9% uptime (clinical requirement)

---

13. Technology Roadmap

13.1 Current State (Phase 1 – Q4 2025)

Technologies Deployed: - Windows Server 2022 (jumper server) - RDP with NLA and TLS 1.2 - WinRM over HTTPS - PowerShell 7.x automation - Win-

dows Defender Antivirus - Windows Event Forwarding to existing SIEM

Status: Foundation established; ready for pilot

13.2 Near-Term Enhancements (Phase 2 – Q1 2026)

Planned Upgrades: 1. **Microsoft Defender for Endpoint:** Deploy Plan 1 on jumper + eKVM devices 2. **PowerShell DSC:** Automate jumper server baseline configuration 3. **Azure Automation:** Integrate with Azure Automation for runbook execution (optional) 4. **Enhanced MFA:** Add conditional access policies via Microsoft Entra ID

Dependencies: - MDE requires Microsoft 365 E5 or standalone license - Azure Automation requires Azure subscription

---

13.3 Long-Term Vision (Phase 3 – 2027+)

Future Technologies:

Technology	Benefit	Timeline
Windows Server 2025	Latest security features, ARM support	Q3 2027
Zero Trust Network Access (ZTNA)	Replace VPN with per-app access (Azure AD App Proxy, Zscaler)	Q2 2027
Microsoft Sentinel SOAR	Automated incident response playbooks	Q4 2026
Windows 365 Cloud PC	Cloud-based jumper server (eliminate on-prem hardware)	Q1 2028
AI-Powered Threat Detection	Microsoft Security Copilot for advanced threat hunting	Q3 2027

---

14. Technology Decision Matrix

14.1 Key Technology Choices

Decision Point	Option A	Option B	Chosen	Rationale
Jumper OS	Windows Server 2022	Windows Server 2019	**2022**	Latest LTS; support until 2031; TLS 1.3 native
Remote Access	RDP	SSH	**RDP**	Native Windows; NLA support; LVHN expertise
File Transfer	WinRM	SMB	**WinRM**	Scriptable; encrypted by default; no share management
Scripting	PowerShell 7.x	PowerShell 5.1	**7.x**	Cross-platform; better performance; LTS support
AV/EDR	Microsoft Defender for Endpoint	Third-party (Symantec, Crowd-Strike)	**MDE**	Native integration; lower cost; existing M365 license
SIEM	Microsoft Sentinel	Splunk	**LVHN Choice**	Depends on existing LVHN investment
Certificate	Self-signed	AD CS	**AD CS**	Trusted CA; automatic renewal; Kerberos integration

---

15. Compliance & Standards Alignment

15.1 Microsoft Security Baselines

Applied Baselines: - Microsoft Security Compliance Toolkit - Windows Server 2022 Security Baseline - Microsoft Edge Security Baseline - Microsoft Defender Antivirus Baseline

Implementation:

```
# Import baseline GPO
Import-GPO -BackupGpoName "MSFT Windows Server 2022 - Computer" -Path "C:\Baselines" -Target
```

15.2 CIS Benchmarks

Relevant Benchmarks: - **CIS Microsoft Windows Server 2022 Benchmark v1.0.0 (Level 1)** – For jumper server - **CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0 (Level 1)** – Adapted for eKVM (Windows 11 Pro)

Note on eKVM CIS Benchmark: - CIS provides benchmarks for Windows 11 Enterprise, not specifically for Pro edition - Most Level 1 controls applicable to Windows 11 Pro - Some Enterprise-only features (e.g., AppLocker, Credential Guard) may not be available in Pro - Apply CIS Windows 11 Enterprise Benchmark with Pro edition limitations documented

Automated Assessment: - CIS-CAT Pro (automated scanning tool) - Microsoft Secure Score (for cloud-connected devices) - Manual validation for Pro-specific limitations

---

15.3 FIPS 140-2 Compliance

FIPS-Validated Components: - Windows 10/11/Server 2022: FIPS 140-2 validated cryptographic modules - BitLocker: FIPS 140-2 compliant (when enabled) - TLS 1.2/1.3: Uses FIPS-approved algorithms (AES, SHA-256)

Enable FIPS Mode:

```
# Registry (not recommended unless required by policy)
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy" `
                 -Name "Enabled" -Value 1
```

Note: FIPS mode can break some third-party applications; test thoroughly.

---

16. Migration from Atera

16.1 Atera vs. Native Windows Comparison

Feature	Atera	Native Windows	Notes
Agent Required	Yes (Atera Agent)	No (built-in RDP/WinRM)	No new agent = lower attack surface

Feature	Atera	Native Windows	Notes
Remote Desktop	Via Atera console	Via RDP (mstsc)	Native Windows experience
File Transfer	Drag-and-drop	WinRM Copy-Item	WinRM requires scripting
Automation	Atera scripts	PowerShell	PowerShell more powerful
Monitoring	Atera dashboard	SIEM + PerfMon	Requires SIEM integration
Alerting	Email/SMS	SIEM alerts	SIEM more flexible
Cost	$100/month/tech	SIEM logs only	Lower cost
Audit Logging	Atera logs	Windows Event Logs	Native, tamper-resistant

---

16.2 Migration Steps

Phase 1: Parallel Operation (Month 1) 1. Deploy jumper server with native Windows stack 2. Test RDP/WinRM access to 3 pilot eKVM devices 3. Keep Atera active as backup

Phase 2: Pilot Migration (Month 2) 4. Perform 3 updates via native Windows (pilot) 5. Compare evidence quality: Atera logs vs. Windows Event Logs 6. Validate SIEM ingestion

Phase 3: Full Migration (Month 3-4) 7. Migrate all eKVM devices to native Windows management 8. Decommission Atera agents from eKVM devices 9. Cancel Atera subscription

Phase 4: Optimization (Month 5-6) 10. Tune PowerShell automation scripts 11. Optimize SIEM alert rules 12. Document lessons learned

---

17. Support & Maintenance

17.1 Vendor Support Contacts

Technology	Vendor	Support Level	Contact
Windows Server	Microsoft	Premier Support or Unified Support	support.microsoft.com
Microsoft Defender	Microsoft	Included with license	security.microsoft.com
Active Directory	Microsoft	Premier Support	support.microsoft.com
PowerShell	Microsoft (open source)	Community + Premier	github.com/PowerShell/PowerShell
SIEM (if Sentinel)	Microsoft	Azure Support	portal.azure.com

17.2 Patch Management

Windows Update Strategy:

Component	Update Frequency	Method	Testing
Jumper Server	Monthly (Patch Tuesday)	WSUS or SCCM	Test in lab 1 week before production
eKVM Devices	Monthly (Patch Tuesday)	WSUS or SCCM	Coordinate with firmware updates
PowerShell 7.x	Quarterly (LTS releases)	Manual update	Test scripts in lab
AV Definitions	Daily (automatic)	Windows Update	No testing required

Windows Update Commands:

```
# Check for updates
Get-WindowsUpdate

# Install updates (PSWindowsUpdate module)
Install-WindowsUpdate -AcceptAll -AutoReboot

# Exclude specific updates
Get-WindowsUpdate -Hide -KBArticleID KB5001234
```

17.3 Backup & Recovery

Jumper Server Backup: - **Technology:** Windows Server Backup or Veeam Backup & Replication - **Frequency:** Daily incremental, weekly full - **Retention:** 30 days - **Recovery Point Objective (RPO):** 24 hours - **Recovery Time Objective (RTO):** 4 hours

Backup Scope: - C: (OS and configuration) - D: (staging area) – optional - E: (evidence archive) – mandatory - System State (AD-related if domain-joined)

Disaster Recovery Plan: - Document jumper server rebuild procedure (6-8 hours) - Maintain offline copy of hardening scripts - Test DR annually

---

18. Acceptance Criteria

18.1 Technology Validation

Each technology component must satisfy:

Jumper Server Validation

Component	Validation Method	Pass Criteria
Windows Server 2022	`winver`, check build number	Build 20348.x
RDP (NLA + TLS)	`Get-ItemProperty HKLM:\SYSTEM\...\RDP-Tcp`	UserAuthentication=1, SecurityLayer=2
WinRM (HTTPS)	`Test-WSMan -UseSSL`	No errors; valid certificate
PowerShell 7.x	`$PSVersionTable`	PSVersion 7.4.0
SHA-256 Support	`Get-FileHash -Algorithm SHA256`	Hash output 64 chars
Windows Defender	`Get-MpComputerStatus`	AntivirusEnabled=True, RealTimeProtectionEnabled=True
Event Logging	`Get-WinEvent -LogName Security -MaxEvents 1`	Events present
SIEM Forwarding	Query SIEM for jumper server logs	Logs visible within 5 min

eKVM Device Validation

Component	Validation Method	Pass Criteria
Windows 11 Pro	`winver`	Version 24H2, Build 26100.4202 or later

Component	Validation Method	Pass Criteria
OS Edition	`Get-ComputerInfo | Select OsName`	Windows 11 Pro (confirm not Home/Enterprise)
RDP Capability	`Test-NetConnection -Port 3389` (from jumper)	TcpTestSucceeded=True (when enabled)
WinRM Capability	`Test-WSMan -ComputerName ekvm-01`	ProductVersion 3.0+
PowerShell 5.1	`$PSVersionTable` (on eKVM)	PSVersion = 5.1.x (built-in)
Windows Defender	`Get-MpComputerStatus` (on eKVM)	AntivirusEnabled=True
nCommand Lite Running	Check processes	nCommand Lite process active

---

19. Glossary

Term	Definition
AD CS	Active Directory Certificate Services
AES	Advanced Encryption Standard
CAL	Client Access License
CredSSP	Credential Security Support Provider
DSC	Desired State Configuration (PowerShell)
EDR	Endpoint Detection and Response
FIPS	Federal Information Processing Standards
GPO	Group Policy Object
JIT	Just-In-Time (access provisioning)
LAPS	Local Administrator Password Solution
LTSC	Long-Term Servicing Channel (Windows edition)
MDE	Microsoft Defender for Endpoint
MFA	Multi-Factor Authentication
NLA	Network Level Authentication
OCSP	Online Certificate Status Protocol
PAM	Privileged Access Management
RDP	Remote Desktop Protocol
SIEM	Security Information and Event Management
SMB	Server Message Block
TLS	Transport Layer Security
UPN	User Principal Name (user@domain.com)
WinRM	Windows Remote Management
WSUS	Windows Server Update Services

20. Appendix: Quick Reference Commands

20.1 RDP Commands

```
# Connect to jumper server
mstsc /v:jumper-server-01.lvhn.local /f

# Check RDP configuration
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\R

# Enable RDP
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server" -Name "fDeny
```

20.2 WinRM Commands

```
# Test WinRM
Test-WSMan -ComputerName ekvm-device-01

# Create session
$s = New-PSSession -ComputerName ekvm-device-01 -Credential (Get-Credential)

# Copy file
Copy-Item -Path "C:\file.exe" -Destination "C:\Temp\" -ToSession $s

# Close session
Remove-PSSession $s
```

20.3 File Hash Verification

```
# Compute SHA-256
$hash = (Get-FileHash -Path "firmware.exe" -Algorithm SHA256).Hash

# Compare
if ($hash -eq "a1b2c3d4...") { Write-Host "PASS" } else { Write-Host "FAIL" }
```

20.4 Firewall Commands

```
# Create rule
New-NetFirewallRule -Name "RDP-Jumper" -DisplayName "RDP from Jumper" `
                    -Direction Inbound -Protocol TCP -LocalPort 3389 `
                    -RemoteAddress 10.50.100.10 -Action Allow

# List rules
Get-NetFirewallRule | Where-Object {$_.DisplayName -like "*RDP*"}
```

```powershell
# Remove rule
Remove-NetFirewallRule -Name "RDP-Jumper"
```

20.5 Event Log Queries

```powershell
# Successful RDP logons (last 24 hours)
Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4624; StartTime=(Get-Date).AddDays(-1
  Where-Object {$_.Properties[8].Value -eq 10}

# Failed logons
Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4625; StartTime=(Get-Date).AddHours(-
```

Document Owner: Ionic Engineering Team **Last Updated:** 2025-11-11 **Review Cycle:** Quarterly or after technology changes

---

End of Technology Stack Specification