

VMS Device IT Compatibility Checklist

Please confirm each item below to ensure your network environment is compatible with the CompScience VMS device. Share this completed checklist with your CompScience contact prior to the scheduled installation.

1. Network & Connectivity

- ☐ **VMS device connected to local network**
 - Ethernet preferred; Wi-Fi preconfigured before shipping
- ☐ **VMS device on same subnet as cameras**
 - Or routable cross-subnet
- ☐ **DHCP available (or static IP assigned)**
- ☐ **Minimum 10 Mbps upload speed available**
 - Required for video data exports

2. Firewall Rules (Required — Outbound)

- ☐ **TLS/443 (HTTPS) to *.viam.com & *.viam.cloud**
 - Remote device management
- ☐ **TLS/443 (HTTPS) to *.compscience.com**
 - Video upload & API
- ☐ **TLS/443 (HTTPS) to storage.googleapis.com**
 - Device software downloads
- ☐ **TLS/443 (HTTPS) to pypi.org & files.pythonhosted.org**
 - Python packages for device modules
- ☐ **HTTP/80 to archive, security & ports.ubuntu.com**
 - OS security updates
- ☐ **Persistent outbound WebSocket connections allowed**
 - Required for device management

No wildcard support on your firewall? Also list packages.viam.com, safety.compscience.com & uploader.prod.compscience.com.

3. Firewall Rules (Optional / Fallback)

- ☐ **Inbound port 8080 open to VMS device**
 - Only needed if WebRTC fails
- ☐ **STUN/TURN relay fallback — TCP/UDP 3478 & 5349**
 - Keeps all traffic outbound if direct WebRTC is blocked; TCP 443 works in most corporate networks

4. Camera Access

- ☐ **Camera username & password available for RTSP**
 - Provided to CompScience team
- ☐ **RTSP streaming enabled on each camera**
 - Must be enabled in camera settings
- ☐ **Stream resolution set to 1080p or 2K**
 - Preferred resolution range
- ☐ **Camera model confirmed to support RTSP**
 - Battery-powered cams usually do not
- ☐ **Camera IPs documented (if cross-subnet)**