



Application Note: Video – ANV105

IPMI for Brivo Eagle Eye 620e and 820e CMVRs

2026-07-16 Revision 1.0

Target Audience

This Application Note is intended for installers and administrators who wish to use Intelligent Platform Management Interface (IPMI) on Brivo Eagle Eye 620e and 820e CMVRs.

Introduction

This application note provides standardized, field-ready guidance for using IPMI on Eagle Eye 620e and 820e CMVRs for out-of-band monitoring, troubleshooting, and recovery. It covers both command-line access (ipmitool) and the BMC Web UI, including Serial-over-LAN (SOL) for console access.

Scope and Supported Capabilities

Supported on 620e and 820e CMVRs

- Dedicated IPMI/BMC management Ethernet interface (dedicated NIC)
- BMC Web UI access (supported)
- IPMI over LAN (RMCP+)
- **SOL** (Serial-over-LAN) (supported)
- Health monitoring (sensors), event logs (SEL), chassis/power control

Not covered

- Any requirement for a specific “log bundle” format (none required)
- Any direct internet exposure of BMC (not permitted/recommended)

Network Naming and Deployment Standard

Brivo Eagle Eye site deployments must preserve the established network naming:

- **WAN** – customer/site network for cloud connectivity
- **CamLAN** – camera network

IPMI/BMC Management Network Requirement

- IPMI must be connected to a restricted management segment (preferred: a dedicated management VLAN/subnet on the WAN-side switching infrastructure), while still preserving the WAN and CamLAN naming and topology.
- IPMI must not be connected to CamLAN.

Why this matters: IPMI provides privileged, out-of-band access that must be isolated from camera traffic and protected from broad access.

Security Requirements (Release Policy)

Because IPMI is equivalent to “physical access over the network,” apply the following controls:

Required

- Place IPMI on a restricted management VLAN/subnet reachable only from approved admin/support networks.
- Restrict inbound access with ACLs/firewall rules.
- Use unique credentials per site/customer where possible.
- Rotate passwords per policy and remove unused accounts.

Strongly Recommended

- Do not expose BMC/IPMI to the public internet.
- Use a VPN or jump host for remote access.
- Disable unused services/ciphers in the BMC if your configuration allows it.

Physical Connectivity

Dedicated IPMI NIC (Required per platform design)

- Use the dedicated BMC/IPMI Ethernet port on the CMVR.
- Connect this port to the WAN-side switch infrastructure on a restricted management VLAN/subnet (do not connect to CamLAN).

Note: The CMVR host data interfaces remain connected per standard design to WAN and CamLAN. The IPMI interface is a separate, management-only connection.

Access Methods

You may use either method depending on the task:

6.1 BMC Web UI (Supported)

Use for:

- Quick health checks (temps/fans/voltages)
- Reviewing event logs (SEL)
- Power controls (on/off/reset)
- Console access features (if enabled in your BMC UI)

6.2 ipmitool (Recommended for Support Playbooks)

Use for:

- Repeatable, scriptable support workflows
- Capturing consistent outputs for escalation
- SOL sessions from a terminal

Required Information before Beginning

You need:

- BMC/IPMI IP address (static preferred; DHCP acceptable if documented)
- BMC username/password
- Layer-3 reachability to the management subnet (ACLs/VPN/jump host as applicable)

Ports (typical)

- IPMI RMCP+ : **UDP 623**
- BMC Web UI: **TCP 443** (may vary by configuration)
- SOL: rides over IPMI session (typically covered by UDP 623, vendor-dependent)

Field Procedure

Follow the steps in this section to set up IPMI in the field.

Step 1 — Confirm cabling

- Verify the dedicated IPMI NIC link is up at the switch.
- Confirm the IPMI NIC is on the restricted management segment associated with WAN infrastructure (not CamLAN).

Step 2 — Confirm IP addressing

- Confirm the BMC has a valid IP address on the management subnet.
- Document BMC IP in the site record.

Step 3 — Verify reachability

From an authorized admin workstation:

- Ping the BMC IP (if ICMP permitted)
- Confirm UDP 623 and TCP 443 allowed from your admin network (per policy)

Operational Tasks Using ipmitool

Syntax standard

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> <command>
```

Use lanplus (RMCP+) rather than legacy lan.

9.1 Confirm chassis and power state

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> chassis status
```

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> power status
```

9.2 Power control (recovery actions)

Hard reboot (recommended first recovery action if OS is unresponsive)

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> power cycle
```

Power off / on

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> power off
```

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> power on
```

9.3 Sensor monitoring (health checks)

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> sensor
```

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> sdr type Temperature
```

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> sdr type Fan
```

9.4 Event Log (SEL)

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> sel info
```

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> sel list
```

Clear SEL (only after capturing it)

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> sel clear
```

Serial-Over-LAN (SOL) (Supported)

Use SOL when:

- The CMVR OS is down or unreachable on WAN
- You need boot visibility or console access during recovery

10.1 Check SOL configuration

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> sol info
```

10.2 Start SOL session

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> sol activate
```

10.3 Exit SOL session

Most terminals: ~. (tilde + dot)

If SOL fails: verify SOL is enabled in BMC settings and the platform console routing is configured per the CMVR baseline.

Recommended Support Workflows (Standard Playbooks)

Workflow A — CMVR offline in cloud, but site has power

1. Access BMC via management network
2. Run:
 - chassis status
 - power status
 - temps/fans (sdr type Temperature, sdr type Fan)
 - sel list
3. If sensors/SEL indicate hardware issue, escalate with outputs
4. If the hardware appears healthy, and a hung OS is suspected, perform a power cycle.

Workflow B — Suspected thermal issue / fan fault

1. Capture temps and fan speeds
2. Review SEL for thermal/fan events
3. Confirm airflow (filters, rack clearance, ambient temp)
4. Escalate if repeat events persist after environmental correction

Workflow C — Host network down but BMC reachable

1. Collect SEL + sensors
2. Use SOL for console visibility
3. If necessary, power cycle
4. If issue repeats, escalate with evidence

What to Capture for Escalation (No Log Bundle Required)

There is no required “log bundle” format for IPMI-based escalation. Capture the following text outputs (copy/paste is acceptable):

- CMVR model (620e / 820e) and serial number
- Date/time of issue and timezone
- chassis status
- power status
- sdr type Temperature
- sdr type Fan
- sel info and sel list

This set is sufficient for most hardware triage and RMA decisions.

Firmware Baseline Requirement (Release Standard)

A BMC/IPMI firmware baseline is required for 620e/820e CMVRs.

- CMVRs must remain aligned to the approved baseline for production support.
- Update BMC firmware only through approved release processes and documentation.
- If a unit is suspected to be off baseline, confirm firmware status during triage and follow internal update guidance.

CMVR BMC/BIOS Firmware Baseline – approved for production release:

Component	Approved Version	Build Time
BMC/IPMI	3.02.0	November 29, 2024 07:46:50 UTC
BIOS	V7.303	March 19, 2025 15:50:17

Verify current firmware via the BMC Web UI Dashboard (BMC revision) and Maintenance → Firmware Information, or in BIOS setup. If a unit is off baseline, do not update it in the field unless authorized; follow the approved release process.

Troubleshooting

This section provides troubleshooting information for common IPMI issues.

Timeout / No response

- Confirm you're on the approved management network path
- Confirm UDP 623 (IPMI) is permitted
- Validate cabling to dedicated IPMI NIC
- Validate BMC IP and subnet

Authentication failure

- Confirm correct credentials (case sensitive)
- Check for account lockouts per policy
- Verify user permissions in BMC UI

SOL won't activate

- Confirm SOL enabled in BMC settings and baseline
- Confirm policy allows SOL from your admin network

Appendix-Quick Command Cheat Sheet

Status

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> chassis status
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> power status
```

Sensors

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> sdr type Temperature
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> sdr type Fan
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> sensor
```

SEL

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> sel info
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> sel list
```

Power actions

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> power cycle
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> power off
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> power on
```

SOL

```
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> sol info
ipmitool -I lanplus -H <BMC_IP> -U <USER> -P <PASS> sol activate
```

