Product description

(This article briefly describes the physical product, features and main options.)

Table of contents
- CG2400 Carrier Grade Server
  - Main applications
  - Main features

CG2400 Carrier Grade Server

The Kontron CG2400 carrier grade 2U server is the 8th generation of Kontron platforms designed to meet NEBS-3/ETSI certification. This ruggedized yet sophisticated server has evolved to support more than your classic telco system used by communications service providers.

Main applications
- Most telecom fixed-wireless central office or mission-critical edge use cases that require High Availability
- Applications for security, fintech, surveillance, deep learning data and video analytics
- “Always-on” applications in harsh environments: manufacturing, industrial, oil and gas, utility and military
- Speeding up complex computations of various neural networks for deep learning inference applications (including image recognition, object detection and data analytics) thanks to Intel® Xeon® Scalable processors featuring Intel® Deep Learning Boost
- Deployment streamlining of deep learning inference of int8 data types thanks to Intel’s distribution of the OpenVINO™ toolkit

Main features
- Can withstand harsh environments: dust, high altitude, fire hazard, high-risk earthquakes and high ambient temperatures
- Compact 2U, 20-inch-deep form factor
- Dual 2nd Generation Intel® Xeon® Scalable processors (code-named Cascade Lake)
- Dual redundant AC or DC power options
- Hot-swapable and redundant power supply modules and fans
- High memory, flexible I/O and storage options
- Up to six hot-swapable 2.5-inch hard disk drives
- Up to two M.2 NVMe or SATA storage modules
- Auxiliary power for one 75W PCIe card provided directly by an internal Power Distribution Board
- Scalable architecture enabling support of a variety of operating systems
Overview
Specifications

(This article details dimensions, shipping weights, environmental specifications and power consumption and lists key hardware and software features.)

Table of contents
- CG2400 key hardware features
- CG2400 key software features
- CG2400 physical dimensions
- CG2400 packaging physical dimensions
- CG2400 shipping weights
- CG2400 environmental specifications

CG2400 key hardware features
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| System          | • Designed to meet NEBS GR-63 and GR-1089  
• RoHS 6/6 compliant  
• Extended lifecycle (5-7 years)                                                                                                                                  |
| Chassis         | • Ruggedized 2U x 508 mm (20 in)  
• Locking cover provides protection during hot-swap of system fans  
• Post plated external sheet metal                                                                                                                                     |
| Front panel buttons | • Power on/off  
• System reset  
• Chassis ID                                                                                                                                                    |
| Front panel LEDs | • Power status  
• Chassis identification  
• System status  
• Fan status  
• HDD activity/fault  
• NIC activity  
• Telco alarm LEDs (Critical, Major, Minor, Power)  
NOTE: LED populated, feature available via firmware update - future plan.                                                                                               |
| Storage         | • Up to six hot-swapable 2.5” SATA SSDs or SAS HDDs  
NOTE: SAS drive support requires an additional PCIe RAID or HBA controller. Refer to the Hardware compatibility list  
• Various third-party HW SAS/RAID controllers supported  
Refer to the Hardware compatibility list  
• Internal flash storage supported - M.2 SATA or NVMe (2280)  
Refer to the Hardware compatibility list  
• Integrated SATA 6 Gbps controller with RAID (5W)  
• Two front access SD card slots  
NOTE: LED populated, feature available via firmware update - future plan.                                                                                               |
| On-board hybrid RAID support | • Implemented through C622 chipset – on the motherboard  
• 6-port SATA with RAID 0/1/10 support built-in                                                                                                                           |
| HW RAID adapter support | • Optional SAS/HW RAID controller with six internal ports and maintenance-free (SuperCap) backup (flash-based)  
• Using a PCIe slot: slot 3 is preferred (mounting bracket included within chassis)  
• Optional SuperCap has its own bracket and separate chassis location                                                                                               |
| System cooling  | • Six 80-mm hot-swapable, redundant fans                                                                                                                                            |
| Power           | • Dual redundant 850W AC hot-swapable power supplies, 80Plus® Platinum  
• Dual redundant 850W DC hot-swapable power supplies  
• Common 850W Power Distribution Board (PDB)  
• PMBus 1.2 specification support  
• Internal auxiliary power cable for high-power PCIe card                                                                                                                 |
| Power consumption | Refer to Power consumption and power budget                                                                                                                  |
| Baseboard       | • Kontron KMB-IXS100 server board  
• SSI EEB (12 in x 13 in) form factor                                                                                                                                       |
| Processor       | • Two LGA3647 (Square socket) supporting Intel® Xeon® Scalable processors  
Refer to the Hardware compatibility list                                                                                                                                         |
| Chipset         | • Intel® C622 Chipset (PCH)                                                                                                                                                                           |
| Memory          | • 16 DIMM slots – 1 or 2 DIMM slots/channel – 6 memory channels per processor  
• Support for registered DDR4 memory (RDIMM) and load reduced DDR4 memory (LRDIMM)  
• Memory DDR4 data transfer rate of up to 2933 MT/s*  
Refer to the Hardware compatibility list  
* The maximum supported memory speed depends on the processor installed in the system.                                                                                       |
| I/O             | • Supports two PCIe risers (4 FL/FH cards) and 3 LP adapters for a total of 7 PCIe Gen 3 cards (6 with I/O, 1 without)  
• Two riser options for each of the two PCIe slots  
• 2 slot FL/FH PCIe x8 passive (right side* - Gen3)  
• 2 slot FL/FH PCIe x8 passive (left side* - Gen3)  
• 1 slot FL/FH PCIe x16 passive (right side* - Gen3)  
• 1 slot FL/FH PCIe x16 passive (left side* - Gen3)  
• Front panel: one serial port (RS45 connector), one USB 2.0 port  
• Rear panel: four USB 3.0 ports, one 1000BASE-T network port, two 10GBASE-T network ports, one VGA port, one TAM dry relay connector  
* Right or left-side orientation as looking from the front of the chassis                                                                                                       |
| Server management | • Integrated BMC, see details in CG2400 key software features  
• IPMI 2.0  
• WebUI with KVM and Media Redirection are included in base system  
NOTE: No need for additional module (e.g. AXKRMMLITE in previous CG platform generation)                                                                                  |
| Telco alarm management | • Relay connector on rear panel supports central office alarm systems  
NOTE: available via firmware update - future plan                                                                                                                                 |
| Video           | • Integrated 2D video graphics controller                                                                                                                                                               |

NOTES:  
1. SATA rotating HDDs are not recommended for use in this system because they are sensitive to rotational vibration from system fan blades and other HDDs.  
2. Drives can consume up to 12W of power each. Drives used in this system must be specified to run at a maximum ambient temperature of 40ºC.
### CG2400 key software features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform management</td>
<td>Integrated BMC – this subsystem consists of communication buses, sensors, system BIOS, and server management firmware; it supports standard IPMI features as well as OEM (supplemental) features that are not part of IPMI</td>
</tr>
<tr>
<td></td>
<td>• IPMI 2.0 feature support</td>
</tr>
<tr>
<td></td>
<td>• Firmware update and maintenance</td>
</tr>
<tr>
<td></td>
<td>• Fan monitoring</td>
</tr>
<tr>
<td></td>
<td>• Hot-swap fan support</td>
</tr>
<tr>
<td></td>
<td>• Integrated keyboard, video, and mouse (KVM)</td>
</tr>
<tr>
<td></td>
<td>• KVM redirection</td>
</tr>
<tr>
<td></td>
<td>• Power supply redundancy monitoring and support</td>
</tr>
<tr>
<td></td>
<td>• Management support for Power Management Bus (PMBus) 1.2 compliant power supplies</td>
</tr>
<tr>
<td></td>
<td>• Front panel management including system status LED and chassis ID LED (turned on/off using a front panel button or command)</td>
</tr>
<tr>
<td></td>
<td>• Embedded Web server UI</td>
</tr>
<tr>
<td></td>
<td>• Enhancements to embedded Web server:</td>
</tr>
<tr>
<td></td>
<td>- Human-readable SEL</td>
</tr>
<tr>
<td></td>
<td>- Additional system configurability</td>
</tr>
<tr>
<td></td>
<td>- Additional system monitoring capabilities</td>
</tr>
<tr>
<td></td>
<td>• Acoustic management</td>
</tr>
<tr>
<td></td>
<td>• Power Node Manager support</td>
</tr>
<tr>
<td></td>
<td>• Thermal management support</td>
</tr>
<tr>
<td></td>
<td>• BMC system management health monitoring</td>
</tr>
<tr>
<td></td>
<td>• E-mail alerting</td>
</tr>
<tr>
<td></td>
<td>• Integrated remote media redirection</td>
</tr>
<tr>
<td></td>
<td>• Lightweight Directory Access Protocol (LDAP)</td>
</tr>
<tr>
<td></td>
<td>• System globally unique identifier (GUID) storage and retrieval</td>
</tr>
<tr>
<td></td>
<td>• IPMI 2.0 features</td>
</tr>
<tr>
<td></td>
<td>- IPMI watchdog timer</td>
</tr>
<tr>
<td></td>
<td>- Messaging support, including command bridging and user/session support</td>
</tr>
<tr>
<td></td>
<td>- Chassis device functionality, including power/reset control and BIOS boot flags support</td>
</tr>
<tr>
<td></td>
<td>- System Event Log (SEL) device functionality</td>
</tr>
<tr>
<td></td>
<td>- Access to system Sensor Data Records (SDRs)</td>
</tr>
<tr>
<td></td>
<td>- Sensor device management and polling to monitor and report system health</td>
</tr>
<tr>
<td></td>
<td>- Serial over LAN (SOL)</td>
</tr>
<tr>
<td></td>
<td>- ACPI state synchronization to state changes provided by the BIOS</td>
</tr>
<tr>
<td></td>
<td>• IPMI interfaces:</td>
</tr>
<tr>
<td></td>
<td>- Host interfaces including system management software (SMS) with receive message queue support and server management mode (SMM)</td>
</tr>
<tr>
<td></td>
<td>- Intelligent Platform Management Bus (IPMB) interface</td>
</tr>
<tr>
<td></td>
<td>- LAN interface that supports the IPMI over LAN protocol (RMCP, RMCP+)</td>
</tr>
</tbody>
</table>

**Operating system**  
Refer to [Validated operating systems](#)

**Thermal management**  
- Platform Environment Control Interface (PECI) for thermal management support
- CPU thermal management

### CG2400 physical dimensions

<table>
<thead>
<tr>
<th>Chassis</th>
<th>Measurements (mm [in])</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Width</td>
<td>435.3 [17.14] max.</td>
<td>Body</td>
</tr>
<tr>
<td>Height</td>
<td>87.6 [3.45] max.</td>
<td>Body</td>
</tr>
<tr>
<td>Side clearance</td>
<td>25 [1]</td>
<td>Between rack mounting points</td>
</tr>
<tr>
<td>Front clearance</td>
<td>76 [2]</td>
<td>Recommended</td>
</tr>
<tr>
<td>Rear clearance</td>
<td>92 [3.6]</td>
<td>Recommended</td>
</tr>
</tbody>
</table>

### CG2400 packaging physical dimensions

<table>
<thead>
<tr>
<th>Depth (mm [in])</th>
<th>Width (mm [in])</th>
<th>Height (mm [in])</th>
</tr>
</thead>
</table>

### CG2400 shipping weights
<table>
<thead>
<tr>
<th>Component</th>
<th>Weight (kg)</th>
<th>Weight (lb)</th>
</tr>
</thead>
<tbody>
<tr>
<td>System weight – full configuration (all PCIe adapters, AC or DC PS)</td>
<td>20.0</td>
<td>44.0</td>
</tr>
<tr>
<td>System weight – base configuration (as shipped from factory)</td>
<td>14.0</td>
<td>30.8</td>
</tr>
<tr>
<td>Packaging (box + foam + bag)</td>
<td>2.8</td>
<td>6.2</td>
</tr>
<tr>
<td>Power supply (AC or DC)</td>
<td>1.1</td>
<td>2.4</td>
</tr>
</tbody>
</table>

**CG2400 environmental specifications**

<table>
<thead>
<tr>
<th>Environment</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature, operating</td>
<td>-5ºC to +55ºC (+23ºF to +131ºF)</td>
</tr>
<tr>
<td>Temperature, non-operating</td>
<td>-40ºC to +70ºC (-40ºF to +158ºF)</td>
</tr>
<tr>
<td>Humidity, operating</td>
<td>5% to 85%</td>
</tr>
<tr>
<td>Humidity, non-operating</td>
<td>95%, non-condensing</td>
</tr>
<tr>
<td>Altitude, operating</td>
<td>-60 m to 1,800 m (-197 ft to 5,906 ft) without temperature derating 3,900 m (12,795 ft) 40ºC</td>
</tr>
<tr>
<td>Vibration, operating</td>
<td>This product meets operational random vibration Test profile based on GR-63, clause 5.4.2 Office vibration levels and ETSI EN 300 019-1-4</td>
</tr>
<tr>
<td>Vibration, non-operating</td>
<td>This product meets transportation and storage random vibration Test profile based on GR-63, clause 5.4.3 Transportation vibration - packaged equipment and ETSI EN 300 019-2-2 class 2.3</td>
</tr>
<tr>
<td>Shock, operating</td>
<td>This product meets operational shock standards Test profile based on ETSI EN 300 019-2-3 class 3.2 (IEC 60068-2-27)</td>
</tr>
<tr>
<td>Acoustic</td>
<td>This product meets or exceeds GR-63 and ETSI EN 300 753 requirements</td>
</tr>
<tr>
<td>Drop/freeze fall</td>
<td>This product meets GR-63, clause 4.3.1</td>
</tr>
<tr>
<td>Electrostatic discharge</td>
<td>This product meets 8 kV contact, 15 kV air discharge using IEC 61000-4-2 test method</td>
</tr>
<tr>
<td>WEEE</td>
<td>This product complies with EU directive 2012/19/EU (WEEE)</td>
</tr>
</tbody>
</table>
Platform components

(This article describes the platform's various components: panels, LEDs, modules, fans and power supply units.)

Table of contents
- Platform front panel
- Platform rear panel
- Platform fan module
- Power supply units
  - AC power subsystem
  - Voltage and current requirements
  - DC power subsystem
  - Voltage and current requirements
- Platform button and LED behavior
  - Front panel
  - Rear panel

Platform front panel

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Front panel control buttons, status indicator and telco alarm LEDs</td>
<td>C</td>
<td>USB 2.0 port</td>
</tr>
<tr>
<td>B</td>
<td>RJ45 serial port</td>
<td>D</td>
<td>Bezel captive screw</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Drive slot 5</td>
<td>G</td>
<td>Front panel control buttons, status indicator and telco alarm LEDs</td>
</tr>
<tr>
<td>B</td>
<td>Drive slot 4</td>
<td>H</td>
<td>RJ45 serial port</td>
</tr>
<tr>
<td>C</td>
<td>Drive slot 3</td>
<td>I</td>
<td>USB 2.0 port</td>
</tr>
<tr>
<td>D</td>
<td>Drive slot 2</td>
<td>J</td>
<td>SD flash card slots</td>
</tr>
<tr>
<td>E</td>
<td>Drive slot 1</td>
<td>K</td>
<td>SD flash module LED</td>
</tr>
<tr>
<td>F</td>
<td>Drive slot 0</td>
<td>L</td>
<td>ESD ground strap attachment</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------</td>
<td>------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>A</td>
<td>Power button</td>
<td>G</td>
<td>Minor alarm (amber)</td>
</tr>
<tr>
<td>B</td>
<td>System reset button</td>
<td>H</td>
<td>Power alarm (amber)</td>
</tr>
<tr>
<td>C</td>
<td>System status LED</td>
<td>I</td>
<td>Drive activity LED</td>
</tr>
<tr>
<td>D</td>
<td>Fan status LED</td>
<td>J</td>
<td>NIC activity LED</td>
</tr>
<tr>
<td>E</td>
<td>Critical alarm (amber)</td>
<td>K</td>
<td>Chassis ID button</td>
</tr>
<tr>
<td>F</td>
<td>Major alarm (amber)</td>
<td>L</td>
<td>NMI button</td>
</tr>
</tbody>
</table>

## Platform rear panel

![Platform rear panel diagram]

### Platform rear panel

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Right 12-slot FL/FH PCIe assembly (slots 6 and 7)</td>
</tr>
<tr>
<td>B</td>
<td>Thumb screw to secure right PCIe assembly (A)</td>
</tr>
<tr>
<td>C</td>
<td>LP PCIe adapter (slot 5)</td>
</tr>
<tr>
<td>D</td>
<td>LP PCIe adapter (slot 4)</td>
</tr>
<tr>
<td>E</td>
<td>Thumb screw to secure left PCIe assembly (F)</td>
</tr>
<tr>
<td>F</td>
<td>Left 12-slot FL/FH PCIe assembly (slots 1 and 2)</td>
</tr>
<tr>
<td>G</td>
<td>Power supply 1 (shown with DC power supply installed)</td>
</tr>
<tr>
<td>H</td>
<td>Optional power supply 2 (shown with filler panel)</td>
</tr>
<tr>
<td>I</td>
<td>Chassis ground lug</td>
</tr>
<tr>
<td>J</td>
<td>GbE NIC2</td>
</tr>
<tr>
<td>K</td>
<td>GbE NIC1</td>
</tr>
<tr>
<td>L</td>
<td>USB#3 and USB#4 (both USB 3.0 and USB#3 is the one on top)</td>
</tr>
<tr>
<td>M</td>
<td>Dedicated server management NIC</td>
</tr>
<tr>
<td>N</td>
<td>USB#1 and USB#2 (both USB 3.0 and USB#1 is the one on top)</td>
</tr>
<tr>
<td>O</td>
<td>Video connector</td>
</tr>
<tr>
<td>P</td>
<td>TAM dry relay connector</td>
</tr>
<tr>
<td>Q</td>
<td>Power supply LED signals</td>
</tr>
<tr>
<td>R</td>
<td>Power supply 1 (shown with AC power supply installed)</td>
</tr>
</tbody>
</table>

### Platform fan module

The CG2400 platform is equipped with a module containing 6 hot-swappable fans. No service interruption is usually required to replace the fans. Follow the instructions below to service a fan.
Step_1  Press the quick release button (A) located on the top cover.

Step_2  Slide the top cover (B) back to the support cross bar so the fans and the CPU cables behind them are visible.

Step_3  Remove the fan (D) by grasping both sides of the fan assembly, using the plastic finger guard (C) on the left side and pulling the fan out of the metal enclosure that houses the fans and the power cables.

---

Power supply units

AC power subsystem

The AC power subsystem has up to two redundant AC power supply units and a power distribution board (PDB). Although this power supply output can deliver up to 850 W, the estimated maximum system power draw stated on the system rating label (located on the top cover) is calculated using a theoretical maximum configuration. A typical maximum configuration will consume much less power.

The AC input power supply subsystem has the following features:
- 850 W power module output capability throughout the full AC input voltage range
- Power Good indication LEDs
- Predictive fan failure warning
- Internal cooling fans with multi-speed capability
- AC_OK circuitry for brownout protection and recovery
- Brownout protection and recovery
- Built-in load sharing capability
- Built-in overload protection capability
- Onboard field replaceable unit (FRU) information
- PMBus 1.2 interface for server management functions
- Integrated handle for hot-swappable insertion/extraction
- The power supply module contains one 40-mm fan

Voltage and current requirements

The AC power supply input connector is an IEC320 C14 standard AC inlet connector.
### Voltage and current requirements

**NOTE**: The maximum current listed in the table below is the maximum current the system will draw from the power supply at -48 V input voltage.

<table>
<thead>
<tr>
<th>DC input voltage</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Nominal</td>
<td>-48 VDC</td>
</tr>
<tr>
<td>Minimum</td>
<td>-40 VDC</td>
</tr>
<tr>
<td>Rated</td>
<td>-48 VDC to -72 VDC</td>
</tr>
<tr>
<td>Maximum</td>
<td>-75 VDC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DC input current</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum</td>
<td>30 A at -40 VDC, 15 A at -72 VDC</td>
</tr>
</tbody>
</table>

1. The minimum steady-state DC input voltage at which the equipment remains fully operational is -40 VDC.

### DC power subsystem

The DC power subsystem consists of up to two DC power supply modules capable of operating in redundant mode, and a power distribution board (PDB). Although this power supply output can deliver up to 850 W, the estimated maximum system power draw stated on the system rating label (located on the top cover) is calculated using a theoretical maximum configuration. A typical maximum configuration will consume much less power.

The DC input power supply subsystem has the following features:
- 850 W power module output capability throughout the full DC input voltage range
- Power Good indication LEDs
- Predictive fan failure warning
- Internal cooling fans with multi-speed capability
- DC_OK circuitry for brownout protection and recovery
- Built-in load sharing capability
- Built-in overload protection capability
- Onboard field replaceable unit (FRU) information
- PMBus 1.2 interface for server management functions
- Integrated handle for hot-swappable insertion/extraction
- The power supply module contains one 40-mm fan

### Platform button and LED behavior

**Front panel**

CG2400_User_documentation_2-01-2023  www.kontron.com
<table>
<thead>
<tr>
<th>Item</th>
<th>Button/LED description</th>
<th>Color</th>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Power/sleep (on button)</td>
<td>Green</td>
<td>On</td>
<td>Legacy power on / ACPI S0 state</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green</td>
<td>Blinking</td>
<td>Sleep / ACPI S1 state</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-</td>
<td>Off</td>
<td>Power off / ACPI S4 or S5 state</td>
</tr>
<tr>
<td>B</td>
<td>System reset button</td>
<td>Button only, no LED</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>System status</td>
<td>Green</td>
<td>On</td>
<td>System ready / normal operation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green</td>
<td>Blinking</td>
<td>System ready, but degraded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Amber</td>
<td>On</td>
<td>Critical or non-recoverable condition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-</td>
<td>Off</td>
<td>System not ready: POST / system stop</td>
</tr>
<tr>
<td>D</td>
<td>Fan status</td>
<td>Amber</td>
<td>On</td>
<td>Fan fault</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-</td>
<td>Off</td>
<td>Fan subsystem OK - no fault</td>
</tr>
<tr>
<td>E</td>
<td>Critical alarm</td>
<td>Amber</td>
<td>On</td>
<td>Critical level condition asserted</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: Supported from BMC 2.9.0955AB31</td>
<td></td>
<td></td>
<td>No critical level condition or condition deasserted</td>
</tr>
<tr>
<td>F</td>
<td>Major alarm</td>
<td>Amber</td>
<td>On</td>
<td>Major level condition asserted</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: Supported from BMC 2.9.0955AB31</td>
<td></td>
<td></td>
<td>No major level condition or condition deasserted</td>
</tr>
<tr>
<td>G</td>
<td>Minor alarm</td>
<td>Amber</td>
<td>On</td>
<td>Minor level condition asserted</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: Supported from BMC 2.9.0955AB31</td>
<td></td>
<td></td>
<td>No minor level condition or condition deasserted</td>
</tr>
<tr>
<td>H</td>
<td>Power alarm</td>
<td>Amber</td>
<td>On</td>
<td>Power sub-system condition asserted</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: Supported from BMC 2.9.0955AB31</td>
<td></td>
<td></td>
<td>No power condition or condition deasserted</td>
</tr>
<tr>
<td>I</td>
<td>Drive activity</td>
<td>Green</td>
<td>Blinking</td>
<td>Hard disk drive activity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Amber</td>
<td>On</td>
<td>Hard disk drive fault</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-</td>
<td>Off</td>
<td>No access and no hard disk drive fault</td>
</tr>
<tr>
<td>J</td>
<td>NIC1/NIC2 activity</td>
<td>Green</td>
<td>On</td>
<td>LAN link for NIC1 and NIC2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green</td>
<td>Blinking</td>
<td>LAN activity for NIC1 and NIC2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-</td>
<td>Off</td>
<td>Idle / no link</td>
</tr>
<tr>
<td>K</td>
<td>Chassis ID (on button)</td>
<td>White</td>
<td>On</td>
<td>Chassis identification active via command or button</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-</td>
<td>Off</td>
<td>Chassis identification inactive</td>
</tr>
<tr>
<td>L</td>
<td>NMI button</td>
<td>Button only, no LED</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Signal name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Power button</td>
<td>Toggles the system power on/off, also functions as a sleep button if enabled by an ACPI-compliant operating system. A status LED is embedded in this button.</td>
</tr>
<tr>
<td>B</td>
<td>System reset button</td>
<td>Reboots and initializes the system.</td>
</tr>
<tr>
<td>K</td>
<td>Chassis ID button</td>
<td>Toggles the front panel chassis ID LED and the rear server board chassis ID LED on/off. The front panel LED is embedded in the button.</td>
</tr>
</tbody>
</table>
### Front panel

<table>
<thead>
<tr>
<th>Item</th>
<th>LED description</th>
<th>Color</th>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A, B, C, D, E, F</td>
<td>2.5-in HDD</td>
<td>Green</td>
<td>Solid</td>
<td>HDD present</td>
</tr>
<tr>
<td></td>
<td>Blinking</td>
<td></td>
<td></td>
<td>HDD activity</td>
</tr>
<tr>
<td></td>
<td>Amber</td>
<td>Solid</td>
<td></td>
<td>HDD fault</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>Off</td>
<td></td>
<td>SSD present</td>
</tr>
<tr>
<td></td>
<td>Blinking</td>
<td></td>
<td></td>
<td>SSD activity</td>
</tr>
<tr>
<td></td>
<td>Amber</td>
<td>Solid</td>
<td></td>
<td>SSD fault</td>
</tr>
<tr>
<td>H</td>
<td>RJ45 serial port</td>
<td></td>
<td></td>
<td>No LED</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Serial over RJ45 port</td>
</tr>
<tr>
<td>K</td>
<td>SD flash module</td>
<td>Green</td>
<td>Off</td>
<td>No SD card activity</td>
</tr>
<tr>
<td></td>
<td>Blinking</td>
<td></td>
<td></td>
<td>SD card activity</td>
</tr>
</tbody>
</table>

### Rear panel

<table>
<thead>
<tr>
<th>Item</th>
<th>LED description</th>
<th>Color</th>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>J, K</td>
<td>Link activity (left) NiC1 and NiC 2</td>
<td>Green</td>
<td>Off</td>
<td>No link established</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solid</td>
<td>Link is established</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Blinking</td>
<td>Link activity</td>
</tr>
<tr>
<td></td>
<td>Link speed (right) NiC1 and NiC 2</td>
<td>Green</td>
<td>Solid</td>
<td>10 Gbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yellow</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>M</td>
<td>Link activity (left) Dedicated management NiC</td>
<td>Green</td>
<td>Off</td>
<td>No link established</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solid</td>
<td>Link is established</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Blinking</td>
<td>Link activity</td>
</tr>
<tr>
<td></td>
<td>Link speed (right) Dedicated management NiC</td>
<td>Green</td>
<td>Solid</td>
<td>1000 Mbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yellow</td>
<td>100 Mbps</td>
</tr>
</tbody>
</table>
## AC power supply condition

<table>
<thead>
<tr>
<th>Condition</th>
<th>Dual-color LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>No AC power to all PSUs</td>
<td>Off</td>
</tr>
<tr>
<td>No AC power to this PSU only (for 1+1 configuration)</td>
<td>0.5 Hz blinking red</td>
</tr>
<tr>
<td>AC present / only 5 Vsb on (PSU off)</td>
<td>1 Hz blinking green</td>
</tr>
<tr>
<td>Power supply AC output on and OK</td>
<td>Green</td>
</tr>
<tr>
<td>Power supply failure</td>
<td>Red</td>
</tr>
<tr>
<td>Power supply warning</td>
<td>0.5 Hz blinking red/green*</td>
</tr>
</tbody>
</table>
* Blinking frequency: 1 Hz (0.5 s red / 0.5 s green)

## DC power supply condition

<table>
<thead>
<tr>
<th>Condition</th>
<th>Dual-color LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>No DC power to all PSUs</td>
<td>Off</td>
</tr>
<tr>
<td>No DC power to this PSU only (for 1+1 configuration)</td>
<td>0.5 Hz blinking red</td>
</tr>
<tr>
<td>DC present/only standby output on</td>
<td>1 Hz blinking green</td>
</tr>
<tr>
<td>Power supply DC output on and OK</td>
<td>Green</td>
</tr>
<tr>
<td>Power supply failure</td>
<td>Red</td>
</tr>
<tr>
<td>Power supply warning</td>
<td>0.5 Hz blinking red/green*</td>
</tr>
</tbody>
</table>
* Blinking frequency: 1 Hz (0.5 s red / 0.5 s green)
Product architecture

(This article provides visual representations of the system’s architecture and network interconnections as well as block diagrams.)

Table of contents
- Internal connections
- Network planes
- Block diagram

Internal connections

![Internal connections diagram]

Network planes

The CG2400 platform provides 2 network planes.

<table>
<thead>
<tr>
<th>Network planes</th>
<th>Description</th>
<th>Speed (GbE)</th>
<th>Component access</th>
<th>Default network scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management plane</td>
<td>The management plane carries platform administrative traffic. This plane is used to support hardware management, configuration and health/thermal/power monitoring.</td>
<td>1</td>
<td>BMC</td>
<td>DHCP</td>
</tr>
<tr>
<td>Data plane</td>
<td>The data plane carries customer data application traffic. This plane is used to deliver service to end users.</td>
<td>10</td>
<td>Server, BMC</td>
<td>DHCP</td>
</tr>
</tbody>
</table>

Block diagram

This block diagram summarizes the connections within the platform.

![Block diagram]
Description of system access methods

(This article lists interface access methods and their intended uses based on various use cases.)

Table of contents
- Paths to the operating system
- Paths to the BIOS
- Paths to the management interface (BMC)

To configure, monitor and troubleshoot the CG2400 platform and its components, several interfaces can be used:
- Operating system – through the management plane, data plane, serial port or VGA connection of the platform
- BIOS – through the management plane, serial port or VGA connection of the platform
- Management interface (BMC) – through the management plane of the platform

Paths to the operating system

For any type of connection to a server, an operating system (OS) must be installed. Redirection to the serial port must be configured in the OS. If the system delivered has an OS installed by Kontron, console redirection will be enabled by default.

To access the operating system through one of the paths, refer to Accessing the operating system of a server.

<table>
<thead>
<tr>
<th>Paths to the operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path description</td>
</tr>
</tbody>
</table>
| KVM (Keyboard Video Mouse) | • Initial OS installation  
• OS network interface configuration  
• OS video access  
• Remote access to the OS  
• Unable to establish an SSH session to the OS |
| Fail-safe path to access the server if any elements (OS, BIOS, etc.) get misconfigured. Accessible from the management plane. |
| Screen/monitor (VGA) | • Local access to the OS and system  
• Initial OS installation  
• OS network interface configuration  
• OS video access  
• Unable to establish an SSH session to the OS |
| This is the recommended path for first time out-of-the-box system configuration. Along with the use of a (USB) keyboard, this method provides direct access to the system. |
| SSH/RDP/Customer application protocols | • Operating the platform under normal operation  
• Remote access to the OS |
| Ideal path once OS installation and OS network interface configuration have been performed. Accessible from the data plane. |
| Serial over LAN (SOL) | • OS network interface configuration  
• Unable to establish an SSH session to the OS  
• OS serial console access |
| Accessible from the management plane. |
| Serial console (physical connection) | • Initial OS network interface configuration  
• No configuration performed on BMCs  
• Troubleshooting |
| Fail-safe path to access all server components when elements (OS, BMC, BIOS) get misconfigured. Accessible from the physical port. |

Paths to the BIOS

To access the BIOS through one of the paths, refer to Accessing the BIOS.

<table>
<thead>
<tr>
<th>Paths to the BIOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path description</td>
</tr>
</tbody>
</table>
| KVM (Keyboard Video Mouse) | • Initial BIOS configuration  
• BIOS video access |
| Fail-safe path to access the server if any elements (OS, BIOS, etc.) get misconfigured. Accessible from the management plane. |
| Screen/monitor (VGA) | • Initial BIOS configuration  
• No configuration performed on BMCs  
• BIOS video access  
• Troubleshooting |
| This is the recommended path for first time out-of-the-box system configuration. Along with the use of a (USB) keyboard, this method provides direct access to the system. |
| Serial over LAN (SOL) | • Initial BIOS configuration  
• BIOS serial console access  
• OS network interfaces not configured, but BMC network access is available |
| Accessible from the management plane. |
| Serial console (physical connection) | • Initial BIOS configuration  
• No configuration performed on BMCs  
• Troubleshooting |
| Fail-safe path to access all server components when elements (OS, BMC, BIOS) get misconfigured. Accessible from the physical port. |
**Paths to the management interface (BMC)**

To access the management interface (BMC) through one of the paths, refer to [Accessing a BMC](#).

<table>
<thead>
<tr>
<th>Path description</th>
<th>Main reasons for use</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BMC Web UI</strong>&lt;br&gt;This is the recommended path for first time out-of-the-box system configuration.&lt;br&gt;Accessible from the management plane.</td>
<td>• Remote server control and monitoring&lt;br&gt;• OS video access&lt;br&gt;• Firmware upgrades</td>
</tr>
<tr>
<td><strong>IPMI over LAN (IOL)</strong>&lt;br&gt;This is a good path for automated monitoring/control script once the platform has been configured for the first time.&lt;br&gt;Accessible from the management plane.</td>
<td>• Remote server control and monitoring&lt;br&gt;• Firmware upgrades</td>
</tr>
<tr>
<td><strong>IPMI/KCS</strong>&lt;br&gt;Accessible from the local operating system.</td>
<td>• Local access to the BMC from the operating system for server monitoring&lt;br&gt;• Initial BMC configuration</td>
</tr>
<tr>
<td><strong>Redfish</strong>&lt;br&gt;This is the ideal path for automated monitoring/control script once the platform has been configured for the first time.&lt;br&gt;Accessible from the management plane.</td>
<td>• Remote server monitoring&lt;br&gt;• Remote server control</td>
</tr>
<tr>
<td><strong>SNMP</strong>&lt;br&gt;This is the ideal path for automated monitoring/control script once the platform has been configured for the first time.&lt;br&gt;Accessible from the management plane.</td>
<td>• Remote server monitoring&lt;br&gt;• Remote server control</td>
</tr>
</tbody>
</table>
**Recommended technical expertise**

(This article describes the technical knowledge required to fully leverage the platform capabilities.)

Platforms are networking devices.

It is recommended that you identify the appropriate upstream topology with the help of the IT/network personnel managing the upstream network hardware and configuration. This will facilitate the process down the road.

IP addresses will also need to be assigned based on known MAC addresses, so appropriate IT expertise is required.
Getting started
Getting started - Application installation and performance benchmarking

This article provides step-by-step instructions to get a customer application installed for the first time in a lab environment and to get ready for application performance benchmarking.

Table of contents

- Introduction
  - Assumptions
- Unboxing the platform
  - What’s in the box
  - Unboxing steps
- Planning
  - Material and information required
    - Component installation and assembly
    - Power cables and tooling
    - Rack installation material
    - Network cables and modules
    - Network infrastructure
  - Software required
  - Installing components
    - Opening the enclosure
    - Removing the right riser card assembly
    - Removing the left riser card assembly
    - Removing the processor air duct
    - Installing the processors and heat sinks
      - Socket and processor handling and ESD precautions
      - ESD precautions
    - Processor location
    - Adding a processor in a PHM
      - Preparing the processor for assembly with the PHM
      - Installing the processor
      - Installing a PHM in the platform
  - Installing memory DIMMs
    - Locating the DIMMs
    - DIMM population guidelines for optimal performance
    - Installing memory DIMMs
  - Installing a hardware RAID controller
    - Locating the SAS cables
    - Disconnecting the SAS cables
    - Installing the controller
    - Installing the SuperCap battery backup module
    - Installing a low-profile PCIe card in slot 4 or 5
    - Installing a full height card mounted on the left riser
      - Assembling the PCIe riser card
      - Installing the PCIe add-in card on the riser assembly
    - Reinstalling the processor air duct
    - Reinstalling the left riser card assembly
    - Reinstalling the right riser card assembly
    - Closing the enclosure
- Racking the platform
  - TMLPMOUNT51 rack mount kit
  - Installing inner rails and mounting ears
  - Building the outer rail assembly
  - Attaching the outer rail assemblies to the rack posts
  - Securing the equipment
    - DC earth-grounding
  - Connecting the network cables
    - DC power supply input connector
      - Connector Description
        - The input connector for the DC power supply is a 3-pin Positronic. This connector is rated at 20 A/pin. An earth ground pin is not required because the platform is equipped with two earth ground studs on its rear panel.
      - Connector Assembly Process
        - Building the power cables
        - DC power supply connection
  - Confirming network links are established
  - Discovering the platform management IP address
    - Discovering the management IP in the BIOS using the VGA display port
      - Prerequisites
      - Port location
      - Accessing the BMC network configuration menu
  - Preparing for operating system installation
  - Installing an operating system
    - Prerequisites
    - Browser considerations
    - Connecting to the Web UI of the BMC
    - Changing the user name and password
    - Launching the KyM
    - Mounting the operating system image via virtual media
    - Accessing the BIOS setup menu
Before working with this product or performing instructions described in the getting started section or in other sections, read the Safety and regulatory information section pertaining to the product. Assembly instructions in this documentation must be followed to ensure and maintain compliance with existing product certifications and approvals. Use only the described, regulated components specified in this documentation. Use of other products/components will void the CSA certification and other regulatory approvals of the product and will most likely result in non-compliance with product regulations in the region(s) in which the product is sold.

### Introduction

This getting started section describes the network integration, platform access and operating system installation steps required to start operating a CG2400 platform equipped with two CPU, one or two power supply units, HDD or SSD drives and PCIe add-in cards provided by the customer, and used to leverage two segregated network links (one for the management plane and one for the data plane).

Below is the visual representation of the simplified architecture with one management plane and one data plane used throughout this Getting Started.

![Architecture Diagram](image)

Refer to Product architecture for the complete platform network architecture details.

### Assumptions

The scenario described in this getting started section is based on the following assumptions:

- The network connections of the system are as follows:
  - One management plane (red line) via the RJ45 management port
  - One data plane (green line) via the left RJ45 data port
  - One display connection via the VGA port is required to obtain the BMC management IP address
  - One display connection via the Vga port is required to obtain the BMC management IP address
  - The default IP scheme is DHCP
  - The preferred OS installation method is through the KVM (Keyboard Video Mouse)
  - The platform is equipped with two CPUs
  - The platform is equipped with at least one DC power supply

### Unboxing the platform

#### What's in the box

The CG2400 platform box includes:

- One CG2400 2U, 20-inch deep, carrier grade rackmount server
- Two heat sink boxes, one labeled “Front” and one labeled “Rear”

#### Unboxing steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Step_1 | Open the platform box and take out the small heat sink boxes (there will be one or two depending on your order). Set the boxes aside until you are ready to install the processors and heat sinks in the platform. Refer to Components installation and assembly for assembly instructions. | **NOTE:**
  - The processor with the “Front” heat sink must be installed onto the CPU1 socket
  - The processor with the “Rear” heat sink must be installed onto the CPU2 socket                                                                 |
| Step_2 | Carefully remove the platform from the box and remove the two foam pieces.   |                                                                                                                                                    |
| Step_3 | Remove the platform from the ESD bag.                                       |                                                                                                                                                    |
| Step_4 | Remove the plastic film from the platform. **Failure to do so may affect platform airflow efficiency, thus resulting in poor cooling capabilities.** |                                                                                                                                                    |
| Step_5 | Put all the packaging back in the box (two desiccant pouches, one ESD bag, two foam pieces). |                                                                                                                                                    |

### Planning

**Material and information required**

**Component installation and assembly**
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item_1</td>
<td>#1 Phillips (cross-point) screwdrivers (or interchangeable tip screwdriver with #1 and #2 Phillips bits)</td>
</tr>
<tr>
<td>Item_2</td>
<td>#2 Phillips (cross-point) screwdrivers (or interchangeable tip screwdriver with #1 and #2 Phillips bits)</td>
</tr>
<tr>
<td>Item_3</td>
<td>One T30 Torx screwdriver</td>
</tr>
<tr>
<td>Item_4</td>
<td>One 5-mm flat-head screwdriver</td>
</tr>
<tr>
<td>Item_5</td>
<td>Personal grounding device such as an anti-static wrist strap and a grounded conductive pad</td>
</tr>
</tbody>
</table>

This guide shows the installation of three PCIe add-in cards:
- One HW RAID/SAS card
- One low-profile Ethernet card (half-height/half-length)
- One card mounted on the left PCIe riser (full-height)

To install a SuperCap battery backup module for the RAID/SAS card, a mounting bracket is needed.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item_1</td>
<td>K00740-001 Mounting bracket for Intel Battery Backup unit</td>
</tr>
</tbody>
</table>

To install a full-height PCIe add-in card, a riser is needed.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item_1</td>
<td>CG2200-RISER25XBL Dual-slot, PCIe x8, Gen3 riser for slot 2 (left side)</td>
</tr>
</tbody>
</table>

**Power cables and tooling**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item_1</td>
<td>Black stranded 12 AWG wire to build the power cable based on the length required</td>
</tr>
<tr>
<td>Item_2</td>
<td>Red stranded 12 AWG wire to build the power cable based on the length required</td>
</tr>
<tr>
<td>Item_3</td>
<td>One Positronic DC power supply input mating connector (includes a strain relief assembly)</td>
</tr>
<tr>
<td>Item_4</td>
<td>Three Positronic gauge-16 crimp terminals</td>
</tr>
<tr>
<td>Item_5</td>
<td>Two strain relief screws</td>
</tr>
<tr>
<td>Item_6</td>
<td>One strain relief plate</td>
</tr>
<tr>
<td>Item_7</td>
<td>Two flat head Phillips screws</td>
</tr>
<tr>
<td>Item_8</td>
<td>One hand crimp tool, DMC AFB</td>
</tr>
<tr>
<td>Item_9</td>
<td>One manual extraction tool</td>
</tr>
<tr>
<td>Item_10</td>
<td>One 8 AWG ground cable based on the length required</td>
</tr>
<tr>
<td>Item_11</td>
<td>One ground lug right angle, 8 AWG (Kontron P/N 1064-4226)</td>
</tr>
<tr>
<td>Item_12</td>
<td>10 mm wrench or equivalent tool</td>
</tr>
<tr>
<td>Item_13</td>
<td>One hand crimp tool, Panduit CT-1700</td>
</tr>
</tbody>
</table>

**Rack installation material**

In this section, a 4-post, 19" rack of a depth between 20" and 24" is used as an example. For a different rack configuration, refer to the Rack installation section.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item_1</td>
<td>TMLPMOUNT51</td>
</tr>
</tbody>
</table>

**Network cables and modules**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item_1</td>
<td>One RJ45 Ethernet management plane cable</td>
</tr>
<tr>
<td>Item_2</td>
<td>Two RJ45 Ethernet data plane cables</td>
</tr>
<tr>
<td>Item_3</td>
<td>One RJ45 serial connection cable</td>
</tr>
</tbody>
</table>

**Network infrastructure**

IP addresses:
- 1 management plane IP
- Up to 2 data plane IPs

**Software required**

Relevant section: Common software installation

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item_1</td>
<td>A community version of ipmitool is installed on a remote computer to enable remote monitoring—it is recommended to use ipmitool version 1.8.18.</td>
</tr>
<tr>
<td>Item_2</td>
<td>A terminal emulator such as putTY is installed on a remote computer.</td>
</tr>
<tr>
<td>Item_3</td>
<td>A hardware detection tool such as pciutils is installed on the local server to view information about devices connected to the server PCI buses.</td>
</tr>
</tbody>
</table>

> You now have the material and software required. Proceed with installation of the PCIe add-in cards.
## Installing components

**ESD sensitive device!**

This equipment is sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this product in order to ensure product integrity at all times.

Disconnect the power supply cord before servicing the product to avoid electric shock. If the product has more than one power supply cord, disconnect them all.

## Opening the enclosure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Remove the hex HD Phillips 6 - 32 shipping screw at the front left side of the cover, if it is still attached, and save it for future use.</td>
</tr>
<tr>
<td>Step_2</td>
<td>Remove the two shoulder screws (one on each side) from the cover.</td>
</tr>
<tr>
<td>Step_3</td>
<td>While holding the blue unlocking button in the middle of the top cover, slide the cover backwards until it stops and the edge clears the lock bracket on the rear panel of the chassis.</td>
</tr>
<tr>
<td>Step_4</td>
<td>Lift the cover straight up to remove it from the chassis.</td>
</tr>
</tbody>
</table>

## Removing the right riser card assembly

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Loosen the two blue captive retention screws (A) at the front of the riser assembly and the blue captive screw at the rear of the chassis (B).</td>
</tr>
<tr>
<td>Step_2</td>
<td>Using the two blue touch points (C), lift the riser card assembly out of the chassis (D).</td>
</tr>
</tbody>
</table>

## Removing the left riser card assembly

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Loosen the two blue captive retention screws (A) at the front of the riser assembly and the blue captive screw at the rear of the chassis (B).</td>
</tr>
<tr>
<td>Step_2</td>
<td>Using the two blue touch points (C), lift the riser card assembly out of the chassis (D).</td>
</tr>
</tbody>
</table>
Removing the processor air duct

To remove the processor air duct, simply lift the air duct straight up out of the chassis.

Installing the processors and heat sinks

Socket and processor handling and ESD precautions

Handling precautions

**NOTICE**

Socket contacts are fragile and can be easily damaged if touched. Intel has developed a specific stackup subassembly to provide consistent, controlled motions for inserting and removing processors onto sockets. Kontron expects users and system integrators to use the Intel-designed methodology at all points in the procedures in this section where a processor is being removed or inserted in a socket.

The processor heat sink module (PHM) refers to the subassembly where the heat sink and processor are clipped together prior to installation. This allows for a more robust installation by providing better alignment features and keeping fingers away from the socket contact field.

The subassembly stackup consists of three different parts.

Image source: Intel Corporation

ESD precautions

Be mindful of the following points when handling the processors and sockets to reduce the risk of electrostatic discharge (ESD) damage to the processor:

- Touch the metal chassis before touching the processor or server board.
- Keep part of your body (hand, etc.) in contact with the metal chassis to dissipate the static charge while handling the processor.
- Avoid moving around unnecessarily.
- Use a ground strap attached to the front panel (with the bezel removed)

Processor location
Perform the following tasks for each processor.

**Adding a processor in a PHM**

**NOTICE**
The processor must be appropriate.
Severe damage to the platform board may occur if a processor that is inappropriate is installed. Refer to the Hardware compatibility list for a list of components.

**NOTICE**
Kontron recommends performing a CPU socket inspection before adding or replacing a processor to ensure there is nothing wrong with the fragile socket pins.

**Preparing the processor for assembly with the PHM**

**Step 1** Remove the cover of the processor packing tray. From this position, the processor will be ready to be clipped to the rest of the PHM components. **CAUTION:** Do not touch the processor.

**Installing the processor**

**Step 1** Remove the heat sink from its packaging box.
**NOTE:**
- The processor with the ‘Front’ heat sink must be installed onto the CPU1 socket (see Processor location)
- The processor with the ‘Rear’ heat sink must be installed onto the CPU2 socket (see Processor location)

**Step 2** Take the new PHM (processor carrier and heat sink) and place it above the processor, which is in its open packing tray. The assembly triangles (pin one indicator) must be in the appropriate positions before you lower the PHM.
**NOTE:** In this image, the heat sink was removed for clarity. Only the processor carrier and processor are shown.

**Step 3** Gently clip the processor in the PHM. Lift the assembly. The processor should be clipped in place.

**Installing a PHM in the platform**

**Step 1** Align the triangle of the bolster plate with that of the processor. Lay the PHM on the bolster plate.

**Step 2** Gradually (in a star pattern) and equally tighten each of the four screws in a diagonal pattern until each one is firmly tightened (12.0 in-Lb torque).

**Installing memory DIMMs**

**Locating the DIMMs**
DIMM population guidelines for optimal performance

There are 8 DIMM slots per CPU, but only 6 channels per CPU – A1 and A2 are on the same channel and D1 and D2 are on the same channel. Therefore, do not populate A2 and D2 unless you have already populated all other DIMM slots.

For optimal performance, both CPUs should have the same DIMM configuration, in single or dual CPU configuration.

For each CPU, populate DIMMs in accordance with the following guidelines to ensure optimal performance.

- For configurations with 1 to 3 DIMMs – populate slots A1, B1, C1, starting with A1.
- For configurations with 4 DIMMs – populate slots A1, B1, D1 and E1.
- For a configuration with 5 DIMMs are not recommended as they are unbalanced and will produce a less optimal performance.
- For a configuration with 6 DIMMs – populate slots A1, B1, C1, D1, E1 and F1.
- Configurations with 7 DIMMs are not recommended as they are unbalanced and will produce a less optimal performance.
- For a configuration with 8 DIMMs – populate all DIMM slots.

**NOTE**

Configuration with 8 DIMMs per CPU will reduce 2933 MHz DIMMs speed one step under its nominal value, so 2666 MHz.

If using 2666 or 2400 MHz memory (8 DIMMs per CPU), negotiated speed will stay to DIMM nominal, unless CPU Maximum memory speed is below DIMM nominal.

- Ex 1. Xeon Silver 4114T CPU @2400MHz will negotiate 2666 MHz DIMM at 2400 MHz
- Ex 2. Xeon Gold 5218T CPU @2666MHz will negotiate 2666 MHz DIMM at 2666 MHz

Installing memory DIMMs

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Open the levers of the DIMM slot. (A)</td>
</tr>
<tr>
<td>Step_2</td>
<td>Note the location of the alignment notch on the DIMM edge. (B)</td>
</tr>
<tr>
<td>Step_3</td>
<td>Insert the DIMM, making sure the connector edge of the DIMM aligns correctly with the slot. (E)</td>
</tr>
<tr>
<td>Step_4</td>
<td>Using both hands, push down firmly and evenly on both sides of the DIMM until it snaps into place and the levers close. (C and D)</td>
</tr>
<tr>
<td>Step_5</td>
<td>Visually inspect each lever to ensure they are fully closed and correctly engaged with the notches on the DIMM edge. (E)</td>
</tr>
</tbody>
</table>

Installing a hardware RAID controller

**NOTE** It is assumed that the platform is populated with two CPUs to permit the use of slot 2 (left riser) and slot 4 as detailed below in this Getting Started.

Locating the SAS cables
**Disconnecting the SAS cables**

**Step_1**  Disconnect the two SAS cables (SFF-8643 ends) from the motherboard.

**Installing the controller**

**Step_1**  Unfasten the screw holding the slot 3 RAID card bracket.
Remove the bracket from the chassis rear panel and the PCIe slot 4 filler.

**Step_2**  Fasten the bracket from the chassis to the RAID controller board using the two screws from the bracket (A).

**Step_3**  Match cable connected to Ports 0-3 of the HDD cage to Port 3-0 of the RAID/SAS card, connecting the loose end to the RAID card (B).
Match cable connected to Ports 4-5 of the HDD cage to Port 7-4 of the RAID/SAS card, connecting the loose end to the RAID card (B).
Optionally, if you are using a RAID SuperCap battery backup module:
- Affix the SuperCap battery backup holder to the chassis cross-brace (G).
- Connect the SuperCap battery module to the RAID card (C and F).

**Step_4**  Reinstall slot 4 PCIe filler (removed at Step_1), then insert the hardware RAID controller board in the PCIe slot 3 on the motherboard and press down to mate it with the header (D). Slot 3 bracket sits directly on top of the slot 4 filler.

**Step_5**  Secure the slot 3 faceplate by attaching it with the screw previously removed (Step_1).

**Installing the SuperCap battery backup module**
Step_1  Insert the module into the black plastic tray (A).

Step_2  Fasten the module and tray assembly to the sheet metal bracket by inserting the tabs into the cut-outs on the bracket (B).

Step_3  Slide the module/tray assembly towards the back (side with the connector) of the bracket until it locks into place.

Step_4  Connect the signal/power pigtail cable to the proper connector on the hardware RAID controller board (C) and the rear of the battery backup assembly (F).

Step_5  Place the battery backup bracket on the support cross-brace, lining it up with the center hole on the middle shelf (G).

Step_6  Use the blue retention screw to fasten the battery backup assembly bracket to the cross-brace.

**NOTE:** Once the platform is powered and functional, proceed with required software configurations.

---

**Installing a low-profile PCIe card in slot 4 or 5**

Motherboard PCIe slots available depends on the number of CPUs. For details, see CG2400 PCIe mapping.

**NOTE:** For the example in this Getting Started, it is assumed that the platform is populated with two CPUs to permit the use of slot 4.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Unfasten the screw holding the filler panel in the PCIe slot. Remove the blank filler panel and store it for future use.</td>
</tr>
<tr>
<td>Step_2</td>
<td>Insert the PCIe add-in card in the motherboard’s PCIe slot and press down to mate it with the header.</td>
</tr>
<tr>
<td>Step_3</td>
<td>Secure the PCIe add-in card to the chassis using the screw removed at step 1.</td>
</tr>
</tbody>
</table>

**Installing a full height card mounted on the left riser**

**Assembling the PCIe riser card**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Fasten the left riser card to its bracket with the two 6/32 screws (8 lbf·in torque).</td>
</tr>
</tbody>
</table>

The riser card is now ready to receive add-in cards.

**Installing the PCIe add-in card on the riser assembly**
Step 1: Remove the blank filler panel from the riser card assembly (A) by unfastening the screw of the selected slot (D).

Step 2: For a full-length add-in card, open the card edge retainer by loosening the blue captive screw (B). **NOTE:** An half-length card does not sit into the card edge retainer, simply go to the next step.

Step 3: Attach the add-in card to the appropriate riser card connector (C), making sure it is seated correctly in the riser card connector.

Step 4: Fasten the add-in card to the riser card assembly bracket using the rear retention screw (D). For full-length cards, also secure the card in the grooves on the retainer bracket (B).

**Reinstalling the processor air duct**

Step 1: Place the processor air duct on the processor sockets and DIMMs. Align the front tabs with the captive screws on the support cross-brace. Make sure the pin located on the rear of the chassis is inserted in the moulded groove on the back side of the processor air duct. The air duct is secured when the right riser card assembly is mounted on the support cross-brace above it.

**Reinstalling the left riser card assembly**

Step 1: Position the riser front tabs over the holes on the PCI support cross-brace.

Step 2: Using the blue touch points on the top of the assembly (A), press down to mate the riser card with the header on the server board (B, slot 2 for the left-side riser). **NOTES:**
- To avoid damaging the card edge, be sure that the card is lined up straight with the header, not on an angle.
- If a hardware RAID controller card is installed in PCI slot 3, be careful not to damage the diagnostic pins at the back of the card next to the rear chassis panel when reinstalling the left-side riser assembly.

Step 3: Align and then tighten the blue captive retention screws at the front of the assembly with the holes on the support cross-brace (D) and on the rear of the chassis (C).

**Reinstalling the right riser card assembly**
**Step_1** Position the riser front tabs over the holes on the PCI support cross-brace (over the processor air duct).

**Step_2** Using the blue touch points on the top of the assembly (A), press down to mate the riser card with the header on the server board (B, slot 6 for the right-side riser).

**NOTE:** To avoid damaging the card edge, be sure that the card is lined up straight with the header, not on an angle.

**Step_3** Align and then tighten the blue captive retention screws at the front of the assembly with the holes on the support cross-brace (D) and on the rear of the chassis (C).

---

**Closing the enclosure**

**Step_1** Starting from the rear of the chassis, align the tab on the rear right edge of the cover with the lock bracket on the outside of the rear panel and place the cover down over the chassis with the side edges outside the chassis walls.

**Step_2** Slide the cover forward until it clicks into place.

**Step_3** Put the two shoulder screws back in place (one on each side) to fasten the cover to the chassis frame.

**Step_4** Install the shipping screw if tooled entry is required or if the unit will be shipped.

**Step_5** Torque screws to 8 lbf·in.

---

**Racking the platform**

**CAUTION** Anchor the equipment rack — The equipment rack must be anchored to an unmovable support to prevent it from falling over when one or more servers are extended in front of it on slide assemblies. The equipment rack must be installed according to the manufacturer’s instructions. You must also consider the weight of any other device installed in the rack.

When using a rack, wait until the server is properly mounted in the rack before plugging the power cord(s).

**Mains power disconnect** — The power cord(s) is considered the mains disconnect for the server and must be readily accessible when installed. If the individual server power cord(s) will not be readily accessible for disconnection then you are responsible for installing a power disconnect for the entire rack unit. This main disconnect must be readily accessible, and it must be labeled as controlling power to the entire rack, not just to the server(s). To remove all power, two power cords must be removed.

**Grounding the rack installation** — To avoid the potential for an electrical shock hazard, for AC power you must include a third wire safety ground conductor with the rack installation. For DC power the two studs for chassis enclosure grounding must be used for proper safety grounding. With AC power, if the server power cord is plugged into an outlet that is part of the rack, then you must provide proper grounding for the rack itself. If the server power cord is plugged into a wall outlet, the safety ground conductor in the power cord provides proper grounding only for the server. You must provide additional, proper grounding for the rack and other devices installed in it.

**AC overcurrent protection** — When AC power is used, the server is designed for a line voltage source with up to 20 amperes of overcurrent protection per cord feed. If the power system for the rack assembly is installed on a branch circuit with more than 20 amperes of protection, you must provide supplemental protection for the server. The overall current rating of a server configured with two power supplies is less than 6 amperes.

Refer to the Safety and regulatory information section for more information about mains power disconnect, earth grounding and AC overcurrent protection.

**NOTICE** Temperature — The operating temperature of the server, when installed in an equipment rack, must not go below 5°C (41°F) or rise above 40°C (104°F). Extreme fluctuations in temperature can cause a variety of problems in the server.

**NOTE:** The platform shown in the installation instructions below is different from the CG2400 server and is used for demonstration purposes only.

**TMLPMOUNT51 rack mount kit**
<table>
<thead>
<tr>
<th>Item</th>
<th>Qty</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>LEFT INNER RAIL</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>RIGHT INNER RAIL</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>MOUNTING EAR</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>OUTER RAIL</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>19&quot; EIA L-BRACKET</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>2-POST MOUNTING BRACKET</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>EIA WIDE ADAPTER</td>
</tr>
<tr>
<td>10</td>
<td>12</td>
<td>B-32 X 1/4 SEMS SCREW</td>
</tr>
<tr>
<td>11</td>
<td>16</td>
<td>10-32 X 1/2 SEMS SCREW</td>
</tr>
<tr>
<td>12</td>
<td>14</td>
<td>B-32 KEPS NUT</td>
</tr>
<tr>
<td>13</td>
<td>4</td>
<td>1U EIA BARNUT</td>
</tr>
<tr>
<td>15</td>
<td>4</td>
<td>2U EIA BARNUT</td>
</tr>
<tr>
<td>17</td>
<td>12</td>
<td>M4x0.7 SCREWS FOR MS1300</td>
</tr>
</tbody>
</table>

**NOTE**: 2U barnuts allow the installation of a rail kit into a 1U rack slot when equipment is already installed both above and below that open slot.

**Installing inner rails and mounting ears**

**Step_1**
Attach the left inner rail (item 1) and the right inner rail (item 2) to the chassis using 3 screws (item 10) per inner rail.

**Step_2**
Attach the 2 mounting ears (item 3) to the chassis using 2 screws (item 10) per mounting ear.

Mounting ears (item 3) can be flipped to position the equipment further forward in the rack.

**Building the outer rail assembly**

**Step_1**
Insert 2 L-brackets (item 5 for 19" EIA, item 6 for 23" EIA or item 7 for 23" ETSI) on the threaded studs of an outer rail (item 4) as shown in the figure.

**Step_2**
Loosely screw on 2 nuts (item 12) per L-bracket.

**Step_3**
Adjust the L-brackets to the required length and tighten the nuts.

**Step_4**
Perform steps 1 to 3 again to build a total of 2 outer rail assemblies.

**Attaching the outer rail assemblies to the rack posts**

CG2400_User_documentation_2-01-2023 www.kontron.com // 33
If installing in a 4-post rack with EIA wide hole spacing, the EIA wide adapter (item 9) must be installed on top of the front L-brackets using 2 screws (item 11) per L-bracket as shown in the figure.

**Step 1**
Attach the outer rail assemblies (as built during the Building the outer rail assembly phase) to the rack using 8 or 12 screws (item 11). If the rack is designed to use cage nuts, no bar nuts will be required. If the rack has round holes, bar nuts (item 13 for EIA and item 14 for ETSI) should be used. Make sure the hole pattern of the bar nut matches the hole pattern of the L-bracket.

**NOTE:** If the rack is not designed for cage nuts and multiple 1U systems must be installed immediately one on top of the other, 2U bar nuts (item 15 for EIA and item 16 for ETSI) should be used for convenience purposes.

**Step 2**
Slide the equipment into the rack, making sure the inner rails slide into the outer rails. Support the weight of the system until the lock clicks into the outer rails.

**NOTE:** To take the equipment out, slide it forward until you can access the locks. Depress the locks on both sides and continue to pull out the equipment, while fully supporting the system weight.

**Securing the equipment**

**Step 1**
Fasten each mounting ear (item 3) to a front L-bracket using a total of 2 screws (item 11) as shown in the figures.

**Securing the equipment to a 4-post rack (EIA standard)**

**Securing the equipment to a 4-post rack (EIA Wide)**

**DC earth-grounding**
Step 1 If a ground lug is installed, remove the 2 nuts and washers from the ground lug studs. Take out the ground lug.

Step 2 Strip 19 mm (0.75 in) of the 8 AWG ground cable.

Step 3 Insert the 8 AWG ground cable in the ground lug. Crimp the lug on the cable using an appropriate hand crimp tool (e.g., Panduit CT-1700 crimp tool set at: Color Code = Red; Die Index No. = P21).

Step 4 Install the ground lug on the studs, fastening with the 2 nuts and washers.

Connecting the network cables

Connect the network cables according to the image below:
1. Connect one RJ45 cable to the MNGT port for the management plane.
2. Connect one RJ45 cable to the left data port (NIC1) for the data plane.

> You are now ready to build and connect the power cables.

Building and connecting a DC power cable

NOTE: For an AC PSU or for further information, refer to the Cabling section.

**DC power supply input connector**

- **Connector Description**

  The input connector for the DC power supply is a 3-pin Positronic. This connector is rated at 20 A/pin. An earth ground pin is not required because the platform is equipped with two earth ground studs on its rear panel.

- **Connector Assembly Process**
Building the power cables

**WARNING:** Installation of this product must be performed in accordance with national wiring codes and conform to local regulations.

To build the power cables (ends that will be plugged in the CG2400), the material, tools and wires specified below are required.

**NOTE:** The other ends of the cables will need to be built according to national wiring codes and conform to local regulations in addition to your data center power installation requirements.

<table>
<thead>
<tr>
<th>Description</th>
<th>Quantity</th>
<th>Manufacturer P/N</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Black stranded 12 AWG wire to build the power cable based on the length required</td>
<td>Length required</td>
<td>PLA03F7050/AA</td>
<td>Positronic catalog</td>
</tr>
<tr>
<td>Red stranded 12 AWG wire to build the power cable based on the length required</td>
<td>Length required</td>
<td>FC112N2/AA-14</td>
<td>Positronic catalog</td>
</tr>
<tr>
<td>Positronic DC power supply input mating connector (includes a strain relief assembly)</td>
<td>1</td>
<td>Part of kit 1059-8642</td>
<td>Refer to Platform, modules and accessories</td>
</tr>
<tr>
<td>Positronic gauge-16 crimp terminal</td>
<td>3</td>
<td>Part of kit 1059-8642</td>
<td>Refer to Platform, modules and accessories</td>
</tr>
<tr>
<td>Strain relief screw</td>
<td>2</td>
<td>Part of kit 1059-8642</td>
<td>Refer to Platform, modules and accessories</td>
</tr>
<tr>
<td>Strain relief plate</td>
<td>1</td>
<td>Part of kit 1059-8642</td>
<td>Refer to Platform, modules and accessories</td>
</tr>
<tr>
<td>Flat head Phillips screw</td>
<td>2</td>
<td>Part of kit 1059-8642</td>
<td>Refer to Platform, modules and accessories</td>
</tr>
<tr>
<td>DMC AFB hand crimp tool</td>
<td>1</td>
<td>AFB</td>
<td>DMC hand crimp tool catalog</td>
</tr>
<tr>
<td>Manual extraction tool</td>
<td>1</td>
<td>90B1-0-0</td>
<td>Molex extraction tool catalog</td>
</tr>
</tbody>
</table>
Refer to the Cabling section for a link to a video showing how to crimp pins and assemble them into the connector.

### DC power supply connection

**Step 1** Connect appropriately rated cables from an external power source to each power supply on the rear of the unit.

**Step 2** Check each power supply LED to make sure they are blinking green (payload off) or steady green (payload on). If this is not the case, refer to Platform components for a description of LED behavior.

---

**Confirming network links are established**

Once the CG2400 power LED is green ON (normal blink or ON), confirm LAN connection with the management plane and data plane:
- The right LED on the server management NIC (MNGT) should be green ON
- The right LED on the payload NIC1 should be green ON if connected to 10GbE equipment/port, and yellow ON if connected to 1GbE equipment/port.

Refer to Platform components for more information about LED behavior.

If LED behavior is not as expected, refer to your IT personnel to review upstream network status (the top-of-rack switch port might be disabled).

**Discovering the platform management IP address**

The platform management IP address can be discovered in the BIOS using the VGA display port (physical connection).

**Discovering the management IP in the BIOS using the VGA display port**

**Prerequisites**

1. A physical connection to the VGA display port of the device is required.
2. A mouse and/or keyboard is connected.

**Port location**

**Accessing the BMC network configuration menu**
Step_1 From the UEFI/BIOS menu, navigate to tab Server Mgmt.

Step_2 Select BMC network configuration.

Step_3 The BMC network configuration menu is displayed. NOTE: When the platform is powered up after being shut off, the UEFI/BIOS may load before the BMC has received its IP address. In this case, the UEFI/BIOS menu information will need to be refreshed by restarting the server and re-entering the UEFI/BIOS.

> With your management IP, you are now ready to access the management Web interface.

Preparing for operating system installation

Step_1 Choose the operating system needed based on the requirements of your application (CentOS 7.6 or latest version is recommended).

Step_2 Confirm the OS version to be installed includes or is compatible with the following network interface driver: i40e.

Step_3 If applicable, download the ISO file of the OS to be installed.

For a list of known compatible operating systems, refer to Validated operating systems. For information on components, refer to the PCI mapping.

Installing an operating system

Prerequisites

1. The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).
2. The remote computer has access to the management network subnet.

Browser considerations

<table>
<thead>
<tr>
<th>HTML5</th>
<th>To connect to the Web UI, a Web browser supporting HTML5 is required.</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS self-signed certificate</td>
<td>Upon connection to the Web UI, it is mandatory to accept the HTTPS self-signed certificate. For further information about accepting HTTPS self-signed certificates, please refer to your Web browser’s documentation.</td>
</tr>
<tr>
<td>File download permission</td>
<td>File download from the site needs to be permitted. For further information about file download permission, please refer to your Web browser’s documentation.</td>
</tr>
<tr>
<td>Cookies</td>
<td>Cookies must be enabled in order to access the website. For further information about enabling cookies, please refer to your Web browser’s documentation.</td>
</tr>
</tbody>
</table>
NOTE: The procedure may vary depending on the browser used. Examples provided use Firefox.

Connecting to the Web UI of the BMC

**Step 1**  From a remote computer that has access to the management network, open a browser window and enter the IP address discovered for the BMC.  
*NOTE: The HTTPS prefix is mandatory.*  
```https://[BMC MNGMT_IP]```

**Step 2**  Click on **Advanced** in order to start the HTTPS self-signed certificate acceptance process. Information on the error message will be displayed.

**Step 3**  Click on **Add Exception...** The Add Security Exception pop-up window will be displayed. Click on **Confirm Security Exception** to allow the browser to access the management Web UI of this interface.

**Step 4**  Log in to the BMC Web UI using the appropriate credentials.  
*NOTE: Default Web UI user name and password is admin/admin.*

**Step 5**  You now have access to the management Web UI of the BMC. You can use the interface.

Changing the user name and password

Note that the password field is mandatory, **must have a minimum of 8 characters and not use dictionary words**. It is recommended, but not mandatory, to enter a strong password consisting of at least one upper case letter, alpha-numeric character, and special character. You must avoid symbols from the extended ASCII table as they are not managed by the IPMI tool.
Step_1 Click on **Settings** in the left side menu and click on **User Management**.

Step_2 Select the user to manage.
**NOTE:** The first and second users are reserved fields, therefore, their usernames can't be modified.

Step_3 Change field **Username** if required.

Step_4 Check the **Change Password** box.

Step_5 Create a new password.
**NOTE:** It is recommended, but not mandatory, to enter a strong password consisting of at least one upper case letter, alpha-numeric character, and special character. You MUST avoid symbols from the extended ASCII table as they are not managed by the IPMI tool. Please note that password field is mandatory and should have a minimum of 8 characters when SNMP status is enabled.

Step_6 Confirm the password.

Step_7 Press **Save**.

**Launching the KVM**
The Web UI allows remote control of the server through a KVM (Keyboard, Video, Mouse) interface.
### Mounting the operating system image via virtual media

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step_1</strong></td>
<td>From the KVM view of the server screen, click on <strong>Browse File</strong> at the top right of the screen. Select the ISO file to be mounted and click on <strong>Open</strong>.</td>
</tr>
<tr>
<td><strong>Step_2</strong></td>
<td>Once the ISO file is loaded, click on <strong>Start Media</strong> at the top right of the screen. <strong>NOTE:</strong> Once clicked, the Start Media button becomes the <strong>Stop Media</strong> button.</td>
</tr>
</tbody>
</table>
Step 1: From the Power drop-down menu, select Reset Server to access the BIOS menu. Click on OK to confirm the operation.

**NOTE:** When a reset server command is launched, it may take a few seconds for the BIOS sign on screen to display.

Step 2: When the BIOS sign on screen is displayed, press the specified key to enter the BIOS setup menu.

**NOTE:** It may take a few seconds for the BIOS sign on screen to display confirmation message “Entering Setup…”

**Tip:**
Some users are pressing DEL/F2 many times and very rapidly, to make sure the server catches the key and enters the BIOS setup menu. Doing this may lead to following message on the KVM display: "HID Queue is about to get full. Kindly hold on a second(s)."
Kontron suggests modifying the Setup Prompt Timeout parameter to give users more time to react. Keeping the focus (single-tasking) on the KVM window is also a good practice to enter the BIOS setup menu each time it is needed.

Parameter Setup Prompt Timeout is found in the Boot tab of the BIOS setup menu.
The default value is 1 second, but changing it to a value between 3 and 10 seconds is a good target range.

Step 3: The BIOS sign on screen displays “Entering Setup…”.

**NOTE:** It will take several seconds to display and enter the BIOS setup menu.

Step 4: The BIOS setup menu will be displayed.

Selecting the boot order from boot override

Step 3: From the BIOS setup menu and using the keyboard arrows, select the Save & Exit menu. In the Boot Override section, select UEFI: AMI Virtual CDROM0 1.00 and press Enter. The server will reboot and the media installation process will start.

> You are now ready to complete operating system installation according to your application requirements.

Completing operating system installation

Step 1: Complete the installation by following the on-screen prompts of the specific OS installed.

> (Optional) After installation, if booting from network (PXE) occurs and is not desired, your operating system installer may not have modified the BIOS boot order. To correct this, enter BIOS setup again and follow the steps below.

Verifying operating system installation
All the results and commands may vary depending on the operating system and the devices added.
Step 1 Reboot the OS as recommended, then access the OS command prompt.

Step 2 Verify that no error messages or warnings are displayed in `dmesg` using the following commands.
```
LocalServer_OSPrompt:~# dmesg | grep -i fail
LocalServer_OSPrompt:~# dmesg | grep -i Error
LocalServer_OSPrompt:~# dmesg | grep -i Warning
LocalServer_OSPrompt:~# dmesg | grep -i "Call trace"
```
**NOTE:** If there are any messages or warnings displayed, refer to the operating system’s documentation to fix them.

Step 3 Verify that the DIMMs are detected.
```
LocalServer_OSPrompt:~# free -h
```

Step 4 Verify that all the storage devices are detected.
```
LocalServer_OSPrompt:~# lsblk
```

Step 5 Confirm the data plane network interface controllers are loaded by the i40e driver.
```
LocalServer_OSPrompt:~# dmesg | grep i40e
```
**NOTE:** You should discover two 10GbE NIC.

Step 6 Confirm that all the network interfaces are detected.
```
LocalServer_OSPrompt:~# ip address
```
**NOTE:** You should see two NIC interfaces.

Step 7 Configure network interface controllers based on your requirements.
**NOTE:** Interface names may change depending on the OS installed. However, parameters Bus:Device:Function stay the same for the interface regardless of the operating system.

Step 8 Install `ipmitool` and `pciutils` using the package manager, and update the operating system packages. The `ipmitool` version recommended is 1.8.18.
```
Example:
LocalServer_OSPrompt:~# yum update
LocalServer_OSPrompt:~# yum install ipmitool
LocalServer_OSPrompt:~# yum install pciutils
```
**NOTE:** Updating the packages may take a few minutes.

Step 9 (Optional) If PCIe add-in cards or other hardware components are installed, verify that they are detected.
```
LocalServer_OSPrompt:~# lspci | grep [KEYWORD]
```
**NOTE:** The keyword is a unique word helping to identify the hardware component. The product PCI mapping may help with this validation.

Step 10 Verify communication between the operating system and the BMC.
```
LocalServer_OSPrompt:~# ipmitool mc info
```
Install your application and proceed with benchmarking.

**Monitoring platform sensors**

NOTE: Refer to Accessing a BMC to access the BMC Web UI. The key sensors to look at are the following:
- Temperature sensors
- Power sensors

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Access the BMC Web UI.</td>
</tr>
<tr>
<td>Step_2</td>
<td>From the left-side menu, click on Sensor.</td>
</tr>
<tr>
<td>Step_3</td>
<td>The sensor list will be displayed.</td>
</tr>
<tr>
<td>Step_4</td>
<td>Scroll down to see the list of sensors.</td>
</tr>
<tr>
<td>Step_5</td>
<td>Click on a sensor to see more details.</td>
</tr>
</tbody>
</table>

For a list of all the sensors, refer to Sensor list. For more monitoring methods refer to Monitoring sensors.
Getting started - Platform configuration and application mass deployment
Getting started - Platform and application mass management
Key concepts

(This article provides an overview of key planning concepts relevant to the platform.)

Table of contents
Environmental considerations

(This article provides environmental guidelines in order to ensure the proper functioning of the platform.)

The CG2400 platform is intended to be deployed in data centers, but has been designed to work over the extended temperature range of -5°C to +55°C (23°F to +131°F) and to withstand non-condensing humidity levels up to 95%.

If you are installing the CG2400 in a hot environment, i.e. 30°C to 55°C, it is recommended to take additional measures to maximize the cooling and air circulation as a constant exposure to high temperatures reduces the life expectancy of electronic equipment.

Special considerations must be taken if you are exposing the CG2400 to a temperature shock, such as taking the equipment out of a service truck left outside for the night in sub zero temperatures and taking it inside for installation in a heated facility. In such situations, it is recommended to allow at least 4 hours for the equipment to be acclimated to the new ambient temperature before powering it up, in order to prevent condensation.

The CG2400 meets operational random vibration, operational shock, transportation and storage random vibration standards. Tests are based on ETSI EN 300 019-2-3 class 3.2, ETSI EN 300 019-2-2 class 2.3 and GR-63 clause 5.4.3 and section 5.3.

This equipment should not be exposed directly to the elements (sun, rain, wind, dust).
Power consumption and power budget

(This article provides power supply electrical specifications and explains how to estimate power consumption based on various use cases.)

Table of contents
- Power budget
  - Determining a power budget
  - Power consumption example for a medium-sized configuration
- Power supply output power based on temperature derating

General power information
- The nominal output power of the CG2400 is 850 W. This means the system must consume less than 850 W at all times during operation.
- In a two (redundant) PSU configuration, the current will automatically be shared between both PSUs. If a power feed or PSU becomes defective, the entire load will be carried by the healthy PSU.

Power budget

The overall power budget can be determined using the Kontron Power Budget Tool or by evaluating the power consumption using the estimation numbers below.

Determining a power budget

The power consumption is determined by adding the consumption of all the commodities in the final hardware configuration. Note that the system power consumption depends on the hardware configuration and the applications running, which will rarely require that all components simultaneously consume their maximum power. Therefore, estimations that use the numbers below constitute worst-case scenarios at ambient (room) temperature.

<table>
<thead>
<tr>
<th>Component type</th>
<th>Component</th>
<th>Watts per component</th>
<th>Quantity</th>
<th>Sub-total (Watts)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan</td>
<td>System fan</td>
<td>25</td>
<td>6</td>
<td>150</td>
</tr>
<tr>
<td>CPU</td>
<td>Xeon® Scalable Processor</td>
<td>Model-dependent</td>
<td>1 or 2</td>
<td>75 to 300</td>
</tr>
<tr>
<td>DIMM</td>
<td>Model-dependent</td>
<td>Rule of thumb: 8 GB DIMM: 5 W 16 GB DIMM: 6 W 32 GB DIMM: 7 W 64 GB DIMM: 8 W</td>
<td>1 to 16</td>
<td>5 to 128</td>
</tr>
<tr>
<td>Motherboard</td>
<td>Chipset, LAN, others</td>
<td>30</td>
<td>1</td>
<td>30</td>
</tr>
<tr>
<td>Storage</td>
<td>2.5-in HDD (SAS)</td>
<td>8</td>
<td>0 to 6</td>
<td>0 to 48</td>
</tr>
<tr>
<td></td>
<td>2.5-in SSD (SATA)</td>
<td>4</td>
<td>0 to 6</td>
<td>0 to 24</td>
</tr>
<tr>
<td></td>
<td>M.2 (SATA or NVMe)</td>
<td>2</td>
<td>0 to 2</td>
<td>0 to 4</td>
</tr>
<tr>
<td>PCIe</td>
<td>RAID / HBA</td>
<td>15</td>
<td>0 or 1</td>
<td>0 or 15</td>
</tr>
<tr>
<td></td>
<td>Typical low-wattage PCIe card (e.g. Ethernet adapter)</td>
<td>10</td>
<td>0 to 7</td>
<td>0 to 70</td>
</tr>
<tr>
<td></td>
<td>High-power card (e.g. GPU)</td>
<td>75 to 250 depending on the model</td>
<td>1</td>
<td>75 to 250</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td></td>
<td>335 to 1019</td>
</tr>
</tbody>
</table>

Power consumption example for a medium-sized configuration

In this example, the maximum consumption is 487 W, which leaves a 363 W margin versus the system’s 850 W limit.

<table>
<thead>
<tr>
<th>Component type</th>
<th>Component</th>
<th>Watts per component</th>
<th>Quantity</th>
<th>Sub-total (Watts)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan</td>
<td>System fan</td>
<td>25</td>
<td>6</td>
<td>150</td>
</tr>
<tr>
<td>CPU</td>
<td>Xeon® Gold 5218T</td>
<td>105</td>
<td>2</td>
<td>210</td>
</tr>
<tr>
<td>DIMM</td>
<td>16 GB DIMM</td>
<td>6</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>Motherboard</td>
<td>Chipset, LAN, others</td>
<td>30</td>
<td>1</td>
<td>30</td>
</tr>
<tr>
<td>Storage</td>
<td>2.5-in HDD (SAS)</td>
<td>8</td>
<td>4</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>M.2 (SATA or NVMe)</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>PCIe</td>
<td>RAID</td>
<td>15</td>
<td>1</td>
<td>15</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td></td>
<td>487</td>
</tr>
</tbody>
</table>

Power supply output power based on temperature derating

Temperature derating only applies when the CG2400 is powered by a single PSU.

In single PSU configurations, the nominal output power is affected by the inlet temperature at the PSU (50°C and above). In other words, the 850 W limit can be lower based on the inlet temperature. It is therefore recommended to plan the power budget while accounting for the inlet temperature. The numbers below can help with planning.

<table>
<thead>
<tr>
<th>Model</th>
<th>50 °C</th>
<th>55 °C</th>
<th>60 °C</th>
<th>65 °C</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC PSU (input = 90 VAC) nominal output power</td>
<td>850 W</td>
<td>705 W</td>
<td>650 W</td>
<td>600 W</td>
</tr>
<tr>
<td>DC PSU (input = -40 VDC) nominal output power</td>
<td>850 W</td>
<td>850 W</td>
<td>790 W</td>
<td>725 W</td>
</tr>
</tbody>
</table>
Network architecture

(This article provides network layout information regarding defaults, the customer’s architecture and redundancies.)

Table of contents
MAC addresses

(This article provides information on the product MAC addresses and on means of discovering them.)

Table of contents
- CG2400 MAC addresses
- Discovering the platform MAC addresses
  - Discovering a MAC address using IPMI
  - Procedure via ipmitool lan print
  - Procedure via ipmitool fru print
- Discovering a MAC address using the BIOS
  - Accessing the BIOS using the VGA display port (physical connection)
  - Accessing the BIOS using a serial console (physical connection)

CG2400 MAC addresses

<table>
<thead>
<tr>
<th>Interface description</th>
<th>MAC address</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMC MNGT port</td>
<td>MAC_BASE</td>
<td>Dedicated MGNT port (RMM4/RMM4Lite equivalent)</td>
</tr>
<tr>
<td>CPU X722 port 1</td>
<td>MAC_BASE + 3</td>
<td>Server data plane (payload 10G/1G)</td>
</tr>
<tr>
<td>CPU X722 port 2</td>
<td>MAC_BASE + 4</td>
<td>Server data plane (payload 10G/1G)</td>
</tr>
</tbody>
</table>

Discovering the platform MAC addresses

The platform MAC addresses can be discovered:
- Using IPMI
- Using the BIOS

Discovering a MAC address using IPMI

Prerequisite

1. A community version of ipmitool is installed on a remote computer to enable remote monitoring—it is recommended to use ipmitool version 1.8.18.

A MAC address can be discovered using IPMI with the following commands:
- lan print
- fru print

Procedure via ipmitool lan print

Step_3
From a remote computer that has access to the management network subnet, enter the desired command:
Procedure via `ipmitool fru print`

**Step 1**
From a remote computer that has access to the management network subnet, enter the desired command:

```
```

The MAC address is displayed in the **Board Extra** field.

---

Discovering a MAC address using the BIOS

There are two methods for discovering a MAC address from the BIOS:
- Using the **VGA display port** (physical connection)
- Using a **serial console** (physical connection)

**Accessing the BIOS using the VGA display port (physical connection)**

**Prerequisites**

1. A physical connection to the VGA display port of the device is required.
2. A mouse and/or keyboard is connected.

---

Accessing the BMC network configuration menu

**Step 1**
From the UEFI/BIOS menu, navigate to tab **Server Mgmt**.

**Step 2**
Select **BMC network configuration**.
Step 3: The BMC network configuration menu is displayed.

NOTE: When the platform is powered up after being shut off, the UEFI/BIOS may load before the BMC has received its IP address. In this case, the UEFI/BIOS menu information will need to be refreshed by restarting the server and re-entering the UEFI/BIOS.

Accessing the BIOS using a serial console (physical connection)

Prerequisites

1. A physical connection to the device is required.
   
   NOTE: The serial console port is compatible with Cisco 72-3383-01 cable.

2. A serial console tool is installed on the remote computer.
   - Speed (Baud): 115200
   - Data bits: 8
   - Stop bits: 1
   - Parity: None
   - Flow Control: None
   - Recommended emulation mode: VT100+
   
   NOTE: PuTTY is recommended.

Port location

Access procedure

Step 1: From a computer with a physical connection to the serial port, open a serial console tool and start the communication between the console and the port to which the device is connected.

Step 2: Perform a server reset (Ctrl-break hot key).
   
   NOTE: If an operating system is installed on the device, the hot key might not work properly. If this is the case, reset the server as recommended for the operating system.

   NOTE: When a server reset command is sent, it may take a few seconds for the BIOS sign on screen to display.
Step_3  When the BIOS sign on screen is displayed, press the specified key to enter the BIOS setup menu. 
**NOTE:** It may take a few seconds for the BIOS sign on screen to display confirmation message “Entering Setup...”.

Step_4  The BIOS sign on screen displays “Entering Setup...”. 
**NOTE:** It will take several seconds to display and enter the BIOS setup menu.

Step_5  The BIOS setup menu is displayed.

### Accessing the BMC network configuration menu

**Step_3**  From the UEFI/BIOS menu, navigate to tab **Server Mgmt**.

**Step_2**  Select **BMC network configuration**.

**Step_3**  The **BMC network configuration** menu is displayed. 
**NOTE:** When the platform is powered up after being shut off, the UEFI/BIOS may load before the BMC has received its IP address. In this case, the UEFI/BIOS menu information will need to be refreshed by restarting the server and re-entering the UEFI/BIOS.
The KMB-IXS100 can be populated with one or two CPUs. The number of CPUs affects how the PCI bus numbers are allocated during UEFI initialization and also which PCIe slots are available.

### PCI mapping

This article provides the PCI mapping of the product.

The following list shows PCI bus numbers with two CPUs present (and KMB-IXS100 motherboard slot numbers shown). The KMB-IXS100 can be populated with one or two CPUs. The number of CPUs affects how the PCI bus numbers are allocated during UEFI initialization and also which PCIe slots are available.

<table>
<thead>
<tr>
<th>CPU presence</th>
<th>CPU</th>
<th>PCI bus number range</th>
<th>PCIe slot numbers (on the KMB-IXS100 motherboard itself)</th>
<th>Slot numbers shown on CG2400 chassis (backside)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 CPU only</td>
<td>CPU1</td>
<td>0-255 (0xFFFF)</td>
<td>Slot 5 - x16 (does not support PCIe risers)</td>
<td>Slot 5 (motherboard) → Slot 5 (chassis)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Slot 6 - x16 (supports PCIe risers)</td>
<td>Slot 6 (motherboard) → Slots 6 and 7 (chassis)</td>
</tr>
<tr>
<td>2 CPUs present</td>
<td>CPU1</td>
<td>0-127 (0x7F)</td>
<td>Slot 5 - x16 (does not support PCIe risers)</td>
<td>Slot 5 (motherboard) → Slot 5 (chassis)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Slot 6 - x16 (supports PCIe risers)</td>
<td>Slot 6 (motherboard) → Slots 6 and 7 (chassis)</td>
</tr>
<tr>
<td></td>
<td>CPU2</td>
<td>12B-255 (0x80-0xFFFF)</td>
<td>Slot 2 (supports PCIe risers)</td>
<td>Slot 2 (motherboard) → Slots 1 and 2 (chassis)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Slot 3 - x16 (does not support PCIe risers)</td>
<td>Slot 3 (motherboard) → Slot 3 (chassis)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Slot 4 - x16 (does not support PCIe risers)</td>
<td>Slot 4 (motherboard) → Slot 4 (chassis)</td>
</tr>
</tbody>
</table>

To obtain the PCI mapping of your platform, use command `lspci -nn`. You may have to update the lspci description database with command `update-pciids`.

The following list shows PCI bus numbers with two CPUs present (and KMB-IXS100 motherboard slot numbers shown).

<table>
<thead>
<tr>
<th>Bus: Device. Function</th>
<th>Vendor ID</th>
<th>Device ID</th>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00.0</td>
<td>80B6</td>
<td>2020</td>
<td>Host bridge</td>
<td>Intel Corporation Sky Lake-E DMI3 Registers (rev 04)</td>
</tr>
<tr>
<td>00:04.0</td>
<td>80B6</td>
<td>2021</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CBDMO Registers (rev 04)</td>
</tr>
<tr>
<td>00:04.1</td>
<td>80B6</td>
<td>2021</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CBDMO Registers (rev 04)</td>
</tr>
<tr>
<td>00:04.2</td>
<td>80B6</td>
<td>2021</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CBDMO Registers (rev 04)</td>
</tr>
<tr>
<td>00:04.3</td>
<td>80B6</td>
<td>2021</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CBDMO Registers (rev 04)</td>
</tr>
<tr>
<td>00:04.4</td>
<td>80B6</td>
<td>2021</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CBDMO Registers (rev 04)</td>
</tr>
<tr>
<td>00:04.5</td>
<td>80B6</td>
<td>2021</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CBDMO Registers (rev 04)</td>
</tr>
<tr>
<td>00:04.6</td>
<td>80B6</td>
<td>2021</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CBDMO Registers (rev 04)</td>
</tr>
<tr>
<td>00:04.7</td>
<td>80B6</td>
<td>2021</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CBDMO Registers (rev 04)</td>
</tr>
<tr>
<td>00:05.0</td>
<td>80B6</td>
<td>2024</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E MM/VT-d Configuration Registers (rev 04)</td>
</tr>
<tr>
<td>00:05.2</td>
<td>80B6</td>
<td>2025</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E RAS (rev 04)</td>
</tr>
<tr>
<td>00:05.4</td>
<td>80B6</td>
<td>2026</td>
<td>PIC</td>
<td>Intel Corporation Sky Lake-E IDAPIC (rev 04)(prog-if 20 [IDX-APIC])</td>
</tr>
<tr>
<td>00:08.0</td>
<td>80B6</td>
<td>2014</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Ubox Registers (rev 04)</td>
</tr>
<tr>
<td>00:08.1</td>
<td>80B6</td>
<td>2015</td>
<td>Performance counters</td>
<td>Intel Corporation Sky Lake-E Ubox Registers (rev 04)</td>
</tr>
<tr>
<td>00:08.2</td>
<td>80B6</td>
<td>2016</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Ubox Registers (rev 04)</td>
</tr>
<tr>
<td>00:11.0</td>
<td>80B6</td>
<td>a1ec</td>
<td>Unassigned class</td>
<td>Intel Corporation C620 Series Chipset Family MROM 0 (rev 09)</td>
</tr>
<tr>
<td>00:11.5</td>
<td>80B6</td>
<td>a1d2</td>
<td>SATA controller</td>
<td>Intel Corporation C620 Series Chipset Family SSATA Controller [AHCI mode (rev 09) (prog-if 01 [AHCI 1.0])]</td>
</tr>
<tr>
<td>00:14.0</td>
<td>80B6</td>
<td>a1af</td>
<td>USB controller</td>
<td>Intel Corporation C620 Series Chipset Family USB 3.0 xHCI Controller (rev 09) (prog-if 30 [XHCI])</td>
</tr>
<tr>
<td>00:14.2</td>
<td>80B6</td>
<td>a1b1</td>
<td>Signal processing controller</td>
<td>Intel Corporation C620 Series Chipset Family Thermal Subsystem (rev 09)</td>
</tr>
<tr>
<td>00:16.0</td>
<td>80B6</td>
<td>a1ba</td>
<td>Communication controller</td>
<td>Intel Corporation C620 Series Chipset Family MEI Controller #1 (rev 09)</td>
</tr>
<tr>
<td>00:16.1</td>
<td>80B6</td>
<td>a1bb</td>
<td>Communication controller</td>
<td>Intel Corporation C620 Series Chipset Family MEI Controller #2 (rev 09)</td>
</tr>
<tr>
<td>00:16.4</td>
<td>80B6</td>
<td>a1be</td>
<td>Communication controller</td>
<td>Intel Corporation C620 Series Chipset Family MEI Controller #3 (rev 09)</td>
</tr>
<tr>
<td>00:17.0</td>
<td>80B6</td>
<td>a1b2</td>
<td>SATA controller</td>
<td>Intel Corporation C620 Series Chipset Family SATA Controller [AHCI mode (rev 09) (prog-if 01 [AHCI 1.0])]</td>
</tr>
<tr>
<td>00:1c.0</td>
<td>80B6</td>
<td>a190</td>
<td>PCI bridge</td>
<td>Intel Corporation C620 Series Chipset Family PCI Express Root Port #1 (rev f9) (prog-if 00 (Normal decode))</td>
</tr>
<tr>
<td>00:1c.2</td>
<td>80B6</td>
<td>a192</td>
<td>PCI bridge</td>
<td>Intel Corporation C620 Series Chipset Family PCI Express Root Port #3 (rev f9) (prog-if 00 (Normal decode))</td>
</tr>
<tr>
<td>00:1c.4</td>
<td>80B6</td>
<td>a194</td>
<td>PCI bridge</td>
<td>Intel Corporation Lewisburg PCI Express Root Port #5 (rev f9) (prog-if 00 (Normal decode))</td>
</tr>
<tr>
<td>00:1d.0</td>
<td>80B6</td>
<td>a198</td>
<td>PCI bridge</td>
<td>Intel Corporation Lewisburg PCI Express Root Port #9 (rev f9) (prog-if 00 (Normal decode))</td>
</tr>
<tr>
<td>00:1f.0</td>
<td>80B6</td>
<td>a1c2</td>
<td>ISA bridge</td>
<td>Intel Corporation C622 Series Chipset LPC/ACPI Controller (rev 09)</td>
</tr>
<tr>
<td>00:1f.2</td>
<td>80B6</td>
<td>a1a1</td>
<td>Memory controller</td>
<td>Intel Corporation C620 Series Chipset Family Power Management Controller (rev 09)</td>
</tr>
<tr>
<td>00:1f.4</td>
<td>80B6</td>
<td>a1a3</td>
<td>SMBus</td>
<td>Intel Corporation C620 Series Chipset Family SMBus (rev 09)</td>
</tr>
<tr>
<td>00:1f.5</td>
<td>80B6</td>
<td>a1a4</td>
<td>Serial bus controller</td>
<td>Intel Corporation C620 Series Chipset Family SPI Controller (rev 09)</td>
</tr>
</tbody>
</table>
Bus 17 is mapped as bus 16 if only 1 CPU is installed.

17:0.0:00.0 1a03 1150 PCI bridge ASPEED Technology, Inc. AST1150 PCI-to-PCI Bridge (rev 04) (prog-if 00 [Normal decode])

03:0.0:00.0 1a03 2000 VGA compatible controller ASPEED Technology, Inc. ASPEED Graphics Family (rev 41) (prog-if 00 [VGA controller])

04:0.0:00.0 NVMe XXXX XXXX 1st or only card in M.2 expansion slot -- depending on M.2 expansion card –

05:0.0:00.0 NVMe XXXX XXXX 2nd card in M.2 expansion slot (installed in J47-Rear) -- depending on M.2 expansion card –

17:0.2:00.0 8086 2032 PCI bridge Intel Corporation Sky Lake-E PCI Express Root Port C (rev 04) (prog-if 00 [Normal decode])

17:0.5:00.0 8086 2034 System peripheral Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04)

17:0.5:00.1 8086 2035 System peripheral Intel Corporation Sky Lake-E VT-d (rev 04)

17:0.5:01.0 8086 2036 System peripheral Intel Corporation Sky Lake-E IO(x)-APIC Configuration Registers (rev 04)

17:0.8:00.0 8086 208d PIC Intel Corporation Sky Lake-E IO(x)-APIC Configuration Registers (rev 04) (prog-if 20 [IO(X)-APIC])

17:0.8:01.0 8086 208d System peripheral Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04)

17:0.8:02.0 8086 208d System peripheral Intel Corporation Sky Lake-E VT-d (rev 04)

17:0.8:03.0 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:04.0 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:05.0 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:06.0 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:07.0 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:08.0 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:09.0 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0a.0 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0a.1 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0a.2 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0a.3 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0a.4 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0a.5 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0a.6 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0a.7 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0b.0 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0b.1 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0b.2 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0b.3 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0b.4 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0b.5 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0b.6 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0b.7 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0f.0 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0f.1 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0f.2 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0f.3 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0f.4 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0f.5 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0f.6 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0f.7 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0f.8 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0f.9 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0f.a 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0f.b 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0f.c 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0f.d 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0f.e 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0.8:0f.f 8086 208d System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)
<table>
<thead>
<tr>
<th>Slot</th>
<th>Vendor</th>
<th>Address</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>7</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>1</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>2</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>3</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>4</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>5</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>6</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>7</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>1</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>2</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>3</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>4</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>5</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>6</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>7</td>
<td>Intel Corporation</td>
<td>0B86</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
</tbody>
</table>

Bus 18, 19 and 1a are mapped as bus 17, 18 and 19 if only 1 CPU is installed.

**NOTE:**

- Bus 18, 19 and 1a are mapped as bus 17, 18 and 19 if only 1 CPU is installed.

- **Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04)**

- **Intel Corporation Sky Lake-E PCI Express Root Port B (rev 04)**

- **Intel Corporation Sky Lake-E PCI Express Root Port C (rev 04)**

- **Intel Corporation Sky Lake-E PCI Express Root Port D (rev 04)**

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

- Will be present if there is a riser of type (x4x4x4x4) and a card in the 3rd slot.

- Will be present if there is a riser of type (x4x4x4x4) and a card in the 2nd slot.

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

Bus 3a-3e are mapped as bus 6a-6b if only 1 CPU is installed.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

- Will be present if there is a riser of type (x4x4x4x4) and a card in the 3rd slot.

- Will be present if there is a riser of type (x4x4x4x4) and a card in the 2nd slot.

- Will be present if there is a riser of type (x4x4x4x4) and a card in the 1st slot.

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.

**NOTE:**

- Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.
<table>
<thead>
<tr>
<th>Slot</th>
<th>Register</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5d:0.0</td>
<td>8086</td>
<td>System peripheral</td>
</tr>
<tr>
<td>5d:0.1</td>
<td>8086</td>
<td>System peripheral</td>
</tr>
<tr>
<td>5d:0.2</td>
<td>8086</td>
<td>System peripheral</td>
</tr>
<tr>
<td>5d:0.3</td>
<td>8086</td>
<td>System peripheral</td>
</tr>
<tr>
<td>5d:0.4</td>
<td>8086</td>
<td>System peripheral</td>
</tr>
<tr>
<td>5d:0.5</td>
<td>8086</td>
<td>System peripheral</td>
</tr>
<tr>
<td>5d:0.6</td>
<td>8086</td>
<td>System peripheral</td>
</tr>
<tr>
<td>5d:0.7</td>
<td>8086</td>
<td>System peripheral</td>
</tr>
<tr>
<td>5d:0.8</td>
<td>8086</td>
<td>System peripheral</td>
</tr>
<tr>
<td>5d:0.9</td>
<td>8086</td>
<td>System peripheral</td>
</tr>
</tbody>
</table>

**NOTE:**
- Depending on PCIe expansion card.

Bus 5d-61 are mapped as bus b2-b6 if only 1 CPU is installed.
<table>
<thead>
<tr>
<th>Slot</th>
<th>Vendor</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5b:16.4</td>
<td>B8B6</td>
<td>2018</td>
<td>System peripheral</td>
</tr>
<tr>
<td>5b:17.0</td>
<td>B8B6</td>
<td>2018</td>
<td>System peripheral</td>
</tr>
<tr>
<td>5e:00.x Slot 5</td>
<td>XXXX XXXX</td>
<td>Card in expansion” Slot 5 or” Slot 5 + Riser 1” Slot 5 “ -- depending on PCIe expansion card –</td>
<td></td>
</tr>
<tr>
<td>5f:00.x Slot 5</td>
<td>XXXX XXXX</td>
<td>Card in expansion” Slot 5 + Riser 2” Slot 5 “ -- depending on PCIe expansion card –</td>
<td></td>
</tr>
<tr>
<td>5c:00.x Slot 5</td>
<td>XXXX XXXX</td>
<td>Card in expansion” Slot 5 + Riser 3” Slot 5 “ -- depending on PCIe expansion card –</td>
<td></td>
</tr>
<tr>
<td>5d:00.x Slot 5</td>
<td>XXXX XXXX</td>
<td>Card in expansion” Slot 5 + Riser 4” Slot 5 “ -- depending on PCIe expansion card –</td>
<td></td>
</tr>
</tbody>
</table>

Next buses are only available if a second CPU is installed

<table>
<thead>
<tr>
<th>Slot</th>
<th>Vendor</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>80:04.0</td>
<td>B8B6</td>
<td>2021</td>
<td>System peripheral</td>
</tr>
<tr>
<td>80:04.1</td>
<td>B8B6</td>
<td>2021</td>
<td>System peripheral</td>
</tr>
<tr>
<td>80:04.2</td>
<td>B8B6</td>
<td>2021</td>
<td>System peripheral</td>
</tr>
<tr>
<td>80:04.3</td>
<td>B8B6</td>
<td>2021</td>
<td>System peripheral</td>
</tr>
<tr>
<td>80:04.4</td>
<td>B8B6</td>
<td>2021</td>
<td>System peripheral</td>
</tr>
<tr>
<td>80:04.5</td>
<td>B8B6</td>
<td>2021</td>
<td>System peripheral</td>
</tr>
<tr>
<td>80:04.6</td>
<td>B8B6</td>
<td>2021</td>
<td>System peripheral</td>
</tr>
<tr>
<td>80:04.7</td>
<td>B8B6</td>
<td>2021</td>
<td>System peripheral</td>
</tr>
<tr>
<td>80:05.0</td>
<td>B8B6</td>
<td>2024</td>
<td>System peripheral</td>
</tr>
<tr>
<td>80:05.2</td>
<td>B8B6</td>
<td>2025</td>
<td>System peripheral</td>
</tr>
<tr>
<td>80:05.4</td>
<td>B8B6</td>
<td>2026</td>
<td>PIC</td>
</tr>
<tr>
<td>80:08.0</td>
<td>B8B6</td>
<td>2014</td>
<td>System peripheral</td>
</tr>
<tr>
<td>80:08.1</td>
<td>B8B6</td>
<td>2015</td>
<td>Performance counters</td>
</tr>
<tr>
<td>80:08.2</td>
<td>B8B6</td>
<td>2016</td>
<td>System peripheral</td>
</tr>
<tr>
<td>85:00.0 Slot 2</td>
<td>B8B6</td>
<td>2030</td>
<td>PCI bridge</td>
</tr>
<tr>
<td>85:01.0 Slot 2</td>
<td>B8B6</td>
<td>2031</td>
<td>PCI bridge</td>
</tr>
<tr>
<td>85:02.0 Slot 2</td>
<td>B8B6</td>
<td>2032</td>
<td>PCI bridge</td>
</tr>
<tr>
<td>85:03.0 Slot 2</td>
<td>B8B6</td>
<td>2033</td>
<td>PCI bridge</td>
</tr>
<tr>
<td>85:05.0</td>
<td>B8B6</td>
<td>2034</td>
<td>System peripheral</td>
</tr>
<tr>
<td>85:05.2</td>
<td>B8B6</td>
<td>2035</td>
<td>System peripheral</td>
</tr>
<tr>
<td>85:05.4</td>
<td>B8B6</td>
<td>2036</td>
<td>PIC</td>
</tr>
<tr>
<td>85:08.0</td>
<td>B8B6</td>
<td>208d</td>
<td>System peripheral</td>
</tr>
<tr>
<td>85:08.1</td>
<td>B8B6</td>
<td>208d</td>
<td>System peripheral</td>
</tr>
<tr>
<td>85:08.2</td>
<td>B8B6</td>
<td>208d</td>
<td>System peripheral</td>
</tr>
<tr>
<td>85:08.3</td>
<td>B8B6</td>
<td>208d</td>
<td>System peripheral</td>
</tr>
<tr>
<td>85:08.4</td>
<td>B8B6</td>
<td>208d</td>
<td>System peripheral</td>
</tr>
<tr>
<td>85:08.5</td>
<td>B8B6</td>
<td>208d</td>
<td>System peripheral</td>
</tr>
<tr>
<td>85:08.6</td>
<td>B8B6</td>
<td>208d</td>
<td>System peripheral</td>
</tr>
<tr>
<td>85:08.7</td>
<td>B8B6</td>
<td>208d</td>
<td>System peripheral</td>
</tr>
<tr>
<td>85:09.0</td>
<td>B8B6</td>
<td>208d</td>
<td>System peripheral</td>
</tr>
<tr>
<td>85:09.1</td>
<td>B8B6</td>
<td>208d</td>
<td>System peripheral</td>
</tr>
<tr>
<td>85:09.2</td>
<td>B8B6</td>
<td>208d</td>
<td>System peripheral</td>
</tr>
<tr>
<td>85:09.3</td>
<td>B8B6</td>
<td>208d</td>
<td>System peripheral</td>
</tr>
<tr>
<td>85:09.4</td>
<td>B8B6</td>
<td>208d</td>
<td>System peripheral</td>
</tr>
</tbody>
</table>

NOTE: Will be present if there is a riser of type (x4x4x4x4) and a card in the 4th slot.
<table>
<thead>
<tr>
<th>Offset</th>
<th>Value</th>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x09.5</td>
<td>0x806</td>
<td>20bd</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x09.6</td>
<td>0x806</td>
<td>20bd</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x09.7</td>
<td>0x806</td>
<td>20bd</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0a.0</td>
<td>0x806</td>
<td>20bd</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0a.1</td>
<td>0x806</td>
<td>20bd</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0a.2</td>
<td>0x806</td>
<td>20bd</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0a.3</td>
<td>0x806</td>
<td>20bd</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0a.4</td>
<td>0x806</td>
<td>20bd</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0a.5</td>
<td>0x806</td>
<td>20bd</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0a.6</td>
<td>0x806</td>
<td>20bd</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0a.7</td>
<td>0x806</td>
<td>20bd</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0b.0</td>
<td>0x806</td>
<td>20bd</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0b.1</td>
<td>0x806</td>
<td>20bd</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0b.2</td>
<td>0x806</td>
<td>20bd</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0b.3</td>
<td>0x806</td>
<td>20bd</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0e.0</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0e.1</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0e.2</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0e.3</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0e.4</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0e.5</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0e.6</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0e.7</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0f.0</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0f.1</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0f.2</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0f.3</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0f.4</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0f.5</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0f.6</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x0f.7</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x10.0</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x10.1</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x10.2</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x10.3</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x10.4</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x10.5</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x10.6</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x10.7</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x11.0</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x11.1</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x11.2</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x11.3</td>
<td>0x806</td>
<td>20be</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x1d.0</td>
<td>0x806</td>
<td>2054</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x1d.1</td>
<td>0x806</td>
<td>2055</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x1d.2</td>
<td>0x806</td>
<td>2056</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x1d.3</td>
<td>0x806</td>
<td>2057</td>
<td>System peripheral Intel Corporation Sky Lake-E CHA Registers (rev 04)</td>
</tr>
<tr>
<td>0x1e.0</td>
<td>0x806</td>
<td>2080</td>
<td>System peripheral Intel Corporation Sky Lake-E PCLU Registers (rev 04)</td>
</tr>
<tr>
<td>0x1e.1</td>
<td>0x806</td>
<td>2081</td>
<td>System peripheral Intel Corporation Sky Lake-E PCLU Registers (rev 04)</td>
</tr>
<tr>
<td>0x1e.2</td>
<td>0x806</td>
<td>2082</td>
<td>System peripheral Intel Corporation Sky Lake-E PCLU Registers (rev 04)</td>
</tr>
<tr>
<td>0x1e.3</td>
<td>0x806</td>
<td>2083</td>
<td>System peripheral Intel Corporation Sky Lake-E PCLU Registers (rev 04)</td>
</tr>
<tr>
<td>0x1e.4</td>
<td>0x806</td>
<td>2084</td>
<td>System peripheral Intel Corporation Sky Lake-E PCLU Registers (rev 04)</td>
</tr>
<tr>
<td>Slot</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Registers (rev 04)</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
<td>-----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Slot 2</td>
<td>XXXX</td>
<td>Card in expansion &quot;Slot 2 + Riser 1 th Slot&quot;</td>
<td></td>
</tr>
<tr>
<td>Slot 2</td>
<td>XXXX</td>
<td>Card in expansion &quot;Slot 2 + Riser 2 nd Slot&quot;</td>
<td></td>
</tr>
<tr>
<td>Slot 2</td>
<td>XXXX</td>
<td>Card in expansion &quot;Slot 2 + Riser 3 rd Slot&quot;</td>
<td></td>
</tr>
<tr>
<td>Slot 2</td>
<td>XXXX</td>
<td>Card in expansion &quot;Slot 2 + Riser 4 th Slot&quot;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Slot 2</th>
<th>System peripheral</th>
<th>Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E VT-d (rev 04)</td>
</tr>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04)</td>
</tr>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E IOX-APIC Configuration Registers (prog-if 20 (IO(X)-APIC))</td>
</tr>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)</td>
</tr>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)</td>
</tr>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)</td>
</tr>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)</td>
</tr>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)</td>
</tr>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)</td>
</tr>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)</td>
</tr>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)</td>
</tr>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)</td>
</tr>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)</td>
</tr>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)</td>
</tr>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)</td>
</tr>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)</td>
</tr>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)</td>
</tr>
<tr>
<td>Slot 2</td>
<td>System peripheral</td>
<td>Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)</td>
</tr>
</tbody>
</table>

---

CG2400_User_documentation_2-01-2023 www.kontron.com // 65
<table>
<thead>
<tr>
<th>Slot</th>
<th>Code</th>
<th>Offset</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>d7:10.0</td>
<td>8086</td>
<td>058</td>
<td>Performance counters Intel Corporation Sky Lake-E KTI 0 (rev 04)</td>
</tr>
<tr>
<td>d7:10.1</td>
<td>8086</td>
<td>059</td>
<td>System peripheral Intel Corporation Sky Lake-E UPI Registers (rev 04)</td>
</tr>
<tr>
<td>d7:12.0</td>
<td>8086</td>
<td>204c</td>
<td>Performance counters Intel Corporation Sky Lake-E M3KTI Registers (rev 04)</td>
</tr>
<tr>
<td>d7:12.1</td>
<td>8086</td>
<td>204d</td>
<td>Performance counters Intel Corporation Sky Lake-E M3KTI Registers (rev 04)</td>
</tr>
<tr>
<td>d7:12.2</td>
<td>8086</td>
<td>204e</td>
<td>System peripheral Intel Corporation Sky Lake-E M3KTI Registers (rev 04)</td>
</tr>
<tr>
<td>d7:12.4</td>
<td>8086</td>
<td>204c</td>
<td>Performance counters Intel Corporation Sky Lake-E M3KTI Registers (rev 04)</td>
</tr>
<tr>
<td>d7:12.5</td>
<td>8086</td>
<td>204d</td>
<td>Performance counters Intel Corporation Sky Lake-E M3KTI Registers (rev 04)</td>
</tr>
<tr>
<td>d7:15.0</td>
<td>8086</td>
<td>2018</td>
<td>System peripheral Intel Corporation Sky Lake-E M2PCI Registers (rev 04)</td>
</tr>
<tr>
<td>d7:16.0</td>
<td>8086</td>
<td>2018</td>
<td>System peripheral Intel Corporation Sky Lake-E M2PCI Registers (rev 04)</td>
</tr>
<tr>
<td>d7:16.4</td>
<td>8086</td>
<td>2018</td>
<td>System peripheral Intel Corporation Sky Lake-E M2PCI Registers (rev 04)</td>
</tr>
<tr>
<td>d7:17.0</td>
<td>8086</td>
<td>2018</td>
<td>System peripheral Intel Corporation Sky Lake-E M2PCI Registers (rev 04)</td>
</tr>
<tr>
<td>d8:00.x Slot 3</td>
<td>XXXX</td>
<td>XXXX</td>
<td>Card in expansion <em>Slot 3</em> -- depending on PCIe expansion card --</td>
</tr>
</tbody>
</table>

**NOTE:**

- Entry will be present if there is a card present in Slot n.
- NVMe: Entry will be present if there is a card present in the M.2 J47(Rear) and/or J49(Front) connector.
Platform, modules and accessories

(This article provides the complete list of compatible parts and components that can be ordered from Kontron.)

Table of contents

- Serviceable items (spare)
- Fans
- HDD/SSD carrier
- Front bezel
- Top cover
- Power supply units
- PCIe configurations and PCIe risers
  - PCIe slots
  - PCIe riser slots
  - PCIe risers
- Rackmount kits
- Accessories

Serviceable items (spare)

Fans

<table>
<thead>
<tr>
<th>Kontron P/N</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CG2200-FANSET</td>
<td>Fan assembly (6 fans)</td>
</tr>
</tbody>
</table>

HDD/SSD carrier

<table>
<thead>
<tr>
<th>Kontron P/N</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSNSASHDDCARDQ</td>
<td>SAS HDD/SATA SSD carrier</td>
</tr>
<tr>
<td></td>
<td>Contents: Carrier, black plastic filler, screws (4)</td>
</tr>
</tbody>
</table>

Front bezel

<table>
<thead>
<tr>
<th>Kontron P/N</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CG2100-BEZEL01</td>
<td>Chassis front bezel</td>
</tr>
</tbody>
</table>

Top cover

<table>
<thead>
<tr>
<th>Kontron P/N</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1067-1312</td>
<td>Chassis top cover kit</td>
</tr>
<tr>
<td></td>
<td>Contents: Top Cover and Safety Label</td>
</tr>
</tbody>
</table>

Power supply units
### PCIe configurations and PCIe risers

#### PCIe slots

The platform features 3 PCIe slots capable of supporting 3 single-width, half-height, half-length or full-length cards. These cards can be x16, x8, x4, x2 or x1. PCIe cards plugged in slots 3 and 4 connect to CPU 2 while PCIe cards in slot 5 connect to CPU 1.

The following table gives the characteristics of the 3 PCIe slots.

<table>
<thead>
<tr>
<th>Kontron P/N</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1056-8389</td>
<td>850 W AC PSU</td>
</tr>
<tr>
<td>1056-8385</td>
<td>850 W DC PSU</td>
</tr>
<tr>
<td>K00837-001</td>
<td>PSU filler panel</td>
</tr>
<tr>
<td>1061-0410</td>
<td>C13 to CEE 7/7 European AC power cord, 10A/250Vac, 1.8m long</td>
</tr>
<tr>
<td>1-340000-0</td>
<td>C13 to NEMA 5-15P AC power cord, 10A/125Vac, 2m long</td>
</tr>
<tr>
<td>1059-8642</td>
<td>DC PSU mating connector kit</td>
</tr>
<tr>
<td>1064-4226</td>
<td>Ground lug right angle, 8 AWG</td>
</tr>
</tbody>
</table>

#### PCIe riser slots

The platform also features two riser slots capable of supporting riser cards:

- PCIe slot 2 (left side facing front of the platform)
- PCIe slot 6 (right side facing front of the platform)

All riser card assemblies can support up to full-height, full-length cards.

The following table identifies the different configuration possibilities and the maximum number of PCIe cards that can be connected through riser cards.

<table>
<thead>
<tr>
<th>Riser configuration</th>
<th>PCIe cards</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 single-slot risers</td>
<td>2 single or double-width, x16 cards</td>
</tr>
<tr>
<td>1 single-slot riser</td>
<td>1 single or double-width, x16 card</td>
</tr>
<tr>
<td>1 dual-slot riser</td>
<td>2 single-width, x8 cards</td>
</tr>
<tr>
<td>2 dual-slot risers</td>
<td>4 single-width, x8 cards</td>
</tr>
</tbody>
</table>

#### NOTES:

- All cards installed on risers can have I/Os.
- Only one PCIe card requiring auxiliary power can be connected.
- To have such a connection, use the cable with an 8-pin connector available in the cable bundle bracket (plastic tray above the PSUs).
- Verify the pinout of the PCIe card to make sure it matches that of the platform auxiliary power connector.

#### PCIe riser cards

<table>
<thead>
<tr>
<th>Kontron P/N</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CG2200-RISER2SX8R</td>
<td>Dual-slot, PCIe x8, Gen3 riser for slot 6 (right side)</td>
</tr>
<tr>
<td>CG2200-RISER1SX16R</td>
<td>Single-slot, PCIe x16, Gen3 riser for slot 6 (right side)</td>
</tr>
<tr>
<td>CG2200-RISER2SX8L</td>
<td>Dual-slot, PCIe x8, Gen3 riser for slot 2 (left side)</td>
</tr>
<tr>
<td>CG2200-RISER1SX16L</td>
<td>Single-slot, PCIe x16, Gen3 riser for slot 2 (left side)</td>
</tr>
<tr>
<td>CG2200-RISER2SPCIX*</td>
<td>Dual-slot, PCI-X riser for slot 6 (right side)</td>
</tr>
<tr>
<td>1065-8218*</td>
<td>Triple-slot, PCIe x4 and x8, Gen3 riser for slot 5 (left side)</td>
</tr>
</tbody>
</table>

* The CG2200-RISER2SPCIX and 1065-8218 riser cards are specialty items. Contact your Kontron representative if you wish to use them or get supplementary information.
## Rackmount kits

<table>
<thead>
<tr>
<th>Product code</th>
<th>Description</th>
<th>Slide pull out locking</th>
<th>Minimum order quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>TMLCMOUNT21</td>
<td>Rack mount kit for mounting servers on 19-inch wide, 2-post racks</td>
<td>No</td>
<td>10</td>
</tr>
<tr>
<td>TMLPMOUNT41</td>
<td>Rack mount kit for mounting servers on 19-inch wide, 2-post or 4-post racks</td>
<td>No</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td><strong>NOTES:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2-post screw access is from the side</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Not compatible with HP Mulan racks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TMLPMOUNT51</td>
<td>Rack mount kit for mounting servers on 19-inch wide, 2-post or 4-post racks</td>
<td>Yes</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td><strong>NOTES:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Xylan finish</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TMLPMOUNT52</td>
<td>Rack Mount Kit for mounting servers on 23-inch wide, 2-post or 4-post racks</td>
<td>Yes</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td><strong>NOTES:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Xylan finish</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ETSI hole spacing compliant</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TMLPSLIDE01</td>
<td>Universal front mounting brackets</td>
<td>N/A</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>The Accuride 22-inch Model 305A-LR slide rails would use TMLPSLIDE01.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Each kit contains two Universal front mounting brackets that secure the server to the front of the rack.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1059-8187</td>
<td>19-in rail extension kit</td>
<td>N/A see rail model</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Maximum rack depth when using:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TMLPMOUNT41 -&gt; 36 inches</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TMLPMOUNT51 -&gt; 34 inches</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1061-2890</td>
<td>23-in rail extension kit</td>
<td>N/A</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Use with TMLPMOUNT52</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Accessories

<table>
<thead>
<tr>
<th>Kontron P/N</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1066-0224</td>
<td>Thermal probe</td>
</tr>
<tr>
<td>K00740-001</td>
<td>Mounting bracket for Battery Backup unit</td>
</tr>
<tr>
<td>1065-5409</td>
<td>TPM 2.0 module</td>
</tr>
</tbody>
</table>
Material, information and software required

This article details the material, information and software required for proper configuration and deployment.

Table of contents
- Material and information required
  - Optional adapter
  - Component installation and assembly
  - Power cables and tooling
  - Rack installation material
  - Network cables and modules
  - Network infrastructure
- Software required

Material and information required

Optional adapter

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item_1</td>
<td>RJ45 to DB9 serial adapter (Kontron P/N: 1015-9404)</td>
</tr>
</tbody>
</table>

Component installation and assembly

Relevant section: Components installation and assembly

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item_1</td>
<td>#1 Phillips (cross-point) screwdrivers (or interchangeable tip screwdriver with #1 and #2 Phillips bits)</td>
</tr>
<tr>
<td>Item_2</td>
<td>#2 Phillips (cross-point) screwdrivers (or interchangeable tip screwdriver with #1 and #2 Phillips bits)</td>
</tr>
<tr>
<td>Item_3</td>
<td>One T30 Torx screwdriver</td>
</tr>
<tr>
<td>Item_4</td>
<td>One 5-mm flat-head screwdriver</td>
</tr>
<tr>
<td>Item_5</td>
<td>Personal grounding device such as an anti-static wrist strap and a grounded conductive pad</td>
</tr>
</tbody>
</table>

Power cables and tooling

Relevant sections: Cabling, Rack installation

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item_1</td>
<td>Black stranded 12 AWG wire to build the power cable based on the length required</td>
</tr>
<tr>
<td>Item_2</td>
<td>Red stranded 12 AWG wire to build the power cable based on the length required</td>
</tr>
<tr>
<td>Item_3</td>
<td>One Positronic DC power supply input mating connector (includes a strain relief assembly)</td>
</tr>
<tr>
<td>Item_4</td>
<td>Three Positronic gauge-16 crimp terminals</td>
</tr>
<tr>
<td>Item_5</td>
<td>Two strain relief screws</td>
</tr>
<tr>
<td>Item_6</td>
<td>One strain relief plate</td>
</tr>
<tr>
<td>Item_7</td>
<td>Two flat head Phillips screws</td>
</tr>
<tr>
<td>Item_8</td>
<td>One hand crimp tool, DMC AF8</td>
</tr>
<tr>
<td>Item_9</td>
<td>One manual extraction tool</td>
</tr>
<tr>
<td>Item_10</td>
<td>One 8 AWG ground cable based on the length required</td>
</tr>
<tr>
<td>Item_11</td>
<td>One ground lug right angle, 8 AWG (Kontron P/N 1064-4226)</td>
</tr>
<tr>
<td>Item_12</td>
<td>10 mm wrench or equivalent tool</td>
</tr>
<tr>
<td>Item_13</td>
<td>One hand crimp tool, Panduit CT-1700</td>
</tr>
</tbody>
</table>

Rack installation material

Relevant section: Rack installation
Network cables and modules

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item_1</td>
<td>Rail kit (based on your installation requirements)</td>
</tr>
<tr>
<td>Item_2</td>
<td>Network cables and modules</td>
</tr>
<tr>
<td>Item_3</td>
<td>One RJ45 Ethernet management plane cable</td>
</tr>
<tr>
<td>Item_4</td>
<td>Two RJ45 Ethernet data plane cables</td>
</tr>
<tr>
<td>Item_5</td>
<td>One RJ45 serial connection cable</td>
</tr>
</tbody>
</table>

Network infrastructure

- IP addresses:
  - 1 management plane IP
  - Up to 2 data plane IPs

Software required

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item_1</td>
<td>A community version of ipmitool is installed on a remote computer to enable remote monitoring—it is recommended to use ipmitool version 1.8.18.</td>
</tr>
<tr>
<td>Item_2</td>
<td>A terminal emulator such as putTY is installed on a remote computer.</td>
</tr>
<tr>
<td>Item_3</td>
<td>A hardware detection tool such as pciutils is installed on the local server to view information about devices connected to the server PCI buses.</td>
</tr>
</tbody>
</table>
Hardware compatibility list

(This article provides the list of qualified and compatible hardware components.)

Table of contents
- CPU
- Memory RDIMM ECC module
- M.2 SSD (SATA or NVMe)
- SAS 2.5 in (SATA)
- HDD SAS 2.5 in (SAS)
- SAS and RAID PCIe cards
- PCIe NIC cards

CPU

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Description</th>
<th>Core</th>
<th>Frequency</th>
<th>Power</th>
<th>Status</th>
<th>Kontron P/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel</td>
<td>Xeon Silver 4114T, Skylake</td>
<td>10</td>
<td>2.2 GHz</td>
<td>85 W</td>
<td>Active</td>
<td>1061-9790</td>
</tr>
<tr>
<td>Intel</td>
<td>Xeon Gold 5218T, Cascade Lake</td>
<td>16</td>
<td>2.1 GHz</td>
<td>105 W</td>
<td>Active</td>
<td>1065-4808</td>
</tr>
<tr>
<td>Intel</td>
<td>Xeon Gold 6230T, Cascade Lake</td>
<td>20</td>
<td>2.1 GHz</td>
<td>125 W</td>
<td>Active</td>
<td>1065-5295</td>
</tr>
<tr>
<td>Intel</td>
<td>Xeon Silver 4209T, Cascade Lake</td>
<td>8</td>
<td>2.2 GHz</td>
<td>70 W</td>
<td>Active</td>
<td>1066-7572</td>
</tr>
</tbody>
</table>

The CG2400 delivers optimal performance when a CPU with a maximum consumption of 125 W per socket is used.

NOTES:
- The Silver 4114T and Gold 5218T are in Intel’s Embedded family and on the long life roadmap. They are recommended with the CG2400 for the highest performance and long availability and support. These two CPUs where successfully tested against NEBS Operating Temperature.
- Processors capable of drawing more power than 105 W are appropriate for applications that do not specifically require a long life support or compliance to the stringent NEBS (Operating Temperature) requirements.
- All the processors described above require a passive heatsink solution. Two heatsinks are included in the base system, no need to order separately. The heatsinks for CPU1 and CPU2 are different (the number of fins differ) to optimize airflow throughout the system. Make sure you respect the installation sequence.

WARNING: Specific configurations may be viable with CPUs consuming more than 125 W (e.g. 150 W, 165 W), if the system is configured and operated in precise conditions such as:
- Single-CPU configuration
- Thightly-controlled environment/conditions (e.g. maximum ambient = 20°C)
- Tailored in-system air baffling

The possible consequences of using a very high power CPU in non-adapted conditions are:
- Severe application performance degradation caused by frequent CPU throttling
- High acoustic level
- MTBF reduction

Please contact your Kontron sales representative if you are targeting a CPU consuming more than 125 W (i.e. 140 W, 150 W or 165 W). The CG2400 does not support 200 W and 205 W CPUs (in single or dual CPU configuration)

Memory RDIMM ECC module

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Vendor P/N</th>
<th>Type</th>
<th>Size</th>
<th>Status</th>
<th>Kontron P/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samsung</td>
<td>M393A2K40CB2-CVF</td>
<td>DDR4-2933</td>
<td>16 GB</td>
<td>Active</td>
<td>1065-6019</td>
</tr>
<tr>
<td>Micron</td>
<td>MTA1BA5F2G72PDZ-2G9E1</td>
<td>DDR4-2933</td>
<td>16 GB</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>Micron</td>
<td>MTA36ASF8G72PZ-2G9B2</td>
<td>DDR4-2933</td>
<td>64 GB</td>
<td>Active</td>
<td>1066-9555</td>
</tr>
<tr>
<td>Samsung</td>
<td>M393A8GB40MB2-CVF</td>
<td>DDR4-2933</td>
<td>64 GB*</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>Samsung</td>
<td>M393A1K430B1</td>
<td>DDR4-2933</td>
<td>8 GB</td>
<td>Active</td>
<td>1069-5684</td>
</tr>
<tr>
<td>Micron</td>
<td>MTA9ASF1G72PZ-3G2R1</td>
<td>DDR4-2933</td>
<td>8 GB</td>
<td>Active</td>
<td></td>
</tr>
</tbody>
</table>

*Only supported with Cascade Lake CPUs

M.2 SSD (SATA or NVMe)

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Vendor P/N</th>
<th>Type</th>
<th>Size</th>
<th>Dimension</th>
<th>DWPD</th>
<th>Status</th>
<th>Kontron P/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel</td>
<td>SSD500KB240GB01</td>
<td>SATA</td>
<td>240 GB</td>
<td>2280</td>
<td>1.9</td>
<td>Active</td>
<td>1065-5634</td>
</tr>
<tr>
<td>Intel</td>
<td>SSD500KB480GB01</td>
<td>SATA</td>
<td>480 GB</td>
<td>2280</td>
<td>1.3</td>
<td>Active</td>
<td>1065-5635</td>
</tr>
<tr>
<td>Intel</td>
<td>SSDPEKA256GB01</td>
<td>NVMe</td>
<td>256 GB</td>
<td>2280</td>
<td></td>
<td>Active**</td>
<td>1065-5636</td>
</tr>
<tr>
<td>Intel</td>
<td>SSDPEKA512GB01</td>
<td>NVMe</td>
<td>512 GB</td>
<td></td>
<td></td>
<td>Active**</td>
<td>1065-5632</td>
</tr>
<tr>
<td>Transcend</td>
<td>TS128GMTE55ZT1</td>
<td>NVMe</td>
<td>128 GB</td>
<td>2280</td>
<td></td>
<td>Active</td>
<td>1068-6586</td>
</tr>
</tbody>
</table>

**The module behaves and performs adequately under all temperatures in the system specified range, but the internal temperature returned by the module itself is inaccurate.

SSD 2.5 in (SATA)

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Vendor P/N</th>
<th>DWPD</th>
<th>Size</th>
<th>Operating temperature</th>
<th>Status</th>
<th>Kontron P/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samsung</td>
<td>MZ7LH240HAH0-00005</td>
<td>3 (3 years)</td>
<td>240 GB</td>
<td>0°C to 70°C</td>
<td>Active</td>
<td>1066-7175</td>
</tr>
<tr>
<td>Samsung</td>
<td>MZ7KH240HAA0-00005</td>
<td>5 (5 years)</td>
<td>240 GB</td>
<td>0°C to 70°C</td>
<td>Active</td>
<td>1065-6022</td>
</tr>
</tbody>
</table>

HDD SAS 2.5 in (SAS)
<table>
<thead>
<tr>
<th>Vendor</th>
<th>Vendor P/N</th>
<th>Fast format</th>
<th>Size</th>
<th>RPM</th>
<th>12 Gbps SAS</th>
<th>Operating temperature</th>
<th>Status</th>
<th>Kontron P/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seagate</td>
<td>ST300MM0048</td>
<td>512n</td>
<td>300 GB</td>
<td>10K</td>
<td>Yes</td>
<td>5°C to 55°C</td>
<td>Active</td>
<td>1061-6231</td>
</tr>
<tr>
<td>Toshiba</td>
<td>AL145EB030N</td>
<td>512n</td>
<td>300 GB</td>
<td>10K</td>
<td>Yes</td>
<td>5°C to 55°C</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>Toshiba</td>
<td>AL155EB030N</td>
<td>512n</td>
<td>300 GB</td>
<td>10K</td>
<td>Yes</td>
<td>5°C to 55°C</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>Toshiba</td>
<td>AL145EB060N</td>
<td>512n</td>
<td>600 GB</td>
<td>10K</td>
<td>Yes</td>
<td>5°C to 55°C</td>
<td>Active</td>
<td>1061-6070</td>
</tr>
<tr>
<td>Toshiba</td>
<td>AL155EB060N</td>
<td>512n</td>
<td>600 GB</td>
<td>10K</td>
<td>Yes</td>
<td>5°C to 55°C</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>Seagate</td>
<td>ST600MM0009</td>
<td>512n</td>
<td>600 GB</td>
<td>10K</td>
<td>Yes</td>
<td>5°C to 55°C</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>Seagate</td>
<td>ST1800MM0129</td>
<td>512e/4Kn</td>
<td>1.8 TB</td>
<td>10K</td>
<td>Yes</td>
<td>5°C to 55°C</td>
<td>Active</td>
<td>1061-7429</td>
</tr>
<tr>
<td>Toshiba</td>
<td>AL155EB18EP</td>
<td>512e/4Kn</td>
<td>1.8 TB</td>
<td>10K</td>
<td>Yes</td>
<td>5°C to 55°C</td>
<td>Not tested</td>
<td></td>
</tr>
<tr>
<td>Toshiba</td>
<td>AL155EB24EQ</td>
<td>512e</td>
<td>2.4 TB</td>
<td>10K</td>
<td>Yes</td>
<td>5°C to 55°C</td>
<td>Not tested</td>
<td>1062-4999</td>
</tr>
</tbody>
</table>

**SAS and RAID PCIe cards**

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Description</th>
<th>Type</th>
<th>Status</th>
<th>Kontron P/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSI/Broadcom</td>
<td>MegaRAID SAS 9361-8i</td>
<td>RAID/SAS</td>
<td>Active</td>
<td>1069-5357</td>
</tr>
<tr>
<td>LSI/Broadcom</td>
<td>CacheVault LSI/CVM02</td>
<td>Cache Vault</td>
<td>Active</td>
<td>1069-5358</td>
</tr>
<tr>
<td>LSI/Broadcom</td>
<td>SAS 9300-8i Host Bus Adapter</td>
<td>SAS</td>
<td>Active</td>
<td>1065-7730</td>
</tr>
</tbody>
</table>

**PCIe NIC cards**

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Description</th>
<th>Type</th>
<th>Status</th>
<th>Kontron P/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel</td>
<td>4-port Gigabit Ethernet, RJ-45 (copper) NIC card</td>
<td>Network Interface (10/100/1000 Mbps)</td>
<td>Active</td>
<td>1059-8279</td>
</tr>
</tbody>
</table>
Deployment infrastructure

(This article provides information and guidance on planning deployment infrastructure to facilitate mass configuration.)

Table of contents
Validated operating systems

This article provides the list of supported operating systems and their certification status.

Table of contents
- Status description
- OS certification status

Status description

<table>
<thead>
<tr>
<th>Status legend</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CERTIFIED</td>
<td>The product is certified by the OS vendor as compliant hardware.</td>
</tr>
<tr>
<td>VALIDATED</td>
<td>The product was internally tested.</td>
</tr>
<tr>
<td>TESTED CERT</td>
<td>The unit passed the certification tests, but the official OS vendor certificate was not published.</td>
</tr>
<tr>
<td>PLANNED</td>
<td>Certification is planned.</td>
</tr>
<tr>
<td>IN PROCESS</td>
<td>Certification is started.</td>
</tr>
</tbody>
</table>

OS certification status

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2016</td>
<td>CERTIFIED</td>
</tr>
<tr>
<td>Windows Server 2019</td>
<td>CERTIFIED</td>
</tr>
<tr>
<td>SUSE SLES 15 (Suse Enterprise)</td>
<td>PLANNED</td>
</tr>
<tr>
<td>Ubuntu 18.04</td>
<td>VALIDATED</td>
</tr>
<tr>
<td>Ubuntu 16.04</td>
<td>VALIDATED</td>
</tr>
<tr>
<td>RHEL 8.2 - 8.x</td>
<td>CERTIFIED</td>
</tr>
<tr>
<td>RHEL 7.8 - 7.x</td>
<td>CERTIFIED</td>
</tr>
<tr>
<td>VMware ESXi 6.7</td>
<td>VALIDATED</td>
</tr>
<tr>
<td>CentOS 7.6 (Included with RHEL)</td>
<td>VALIDATED</td>
</tr>
</tbody>
</table>
Security

(This article provides information and guidance on best practices to adopt in order to insure security.)

- Establish a plan to change default user names and password. Refer to Configuring and managing users.
- Determine the access paths that are to be closed or open. Refer to Configuration of system access methods.
- The platform features a Trusted Platform Module (TPM). Determine your requirement with regards to hardware-based, security-related functions. Refer to Configuring TPM.

For more information on security features, contact Kontron.
Installing
Mechanical installation and precautions

(This section details the steps and safety precautions required for the physical installation of the product.)

Children

- ESD protections
- Unboxing
- Components installation and assembly
- Airflow
- Rack installation
- Cabling
ESD protections

This article provides guidelines regarding ESD protection.

Electrostatic discharge (ESD) can damage electronic components (e.g. disk drives and boards). Look for this warning in the documentation as it indicates that the device is ESD sensitive and that precautions must be taken.

<table>
<thead>
<tr>
<th>ESD sensitive device!</th>
</tr>
</thead>
<tbody>
<tr>
<td>This equipment is sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this product in order to ensure product integrity at all times.</td>
</tr>
</tbody>
</table>

We recommend that you perform all the installation procedures described in the documentation at an ESD workstation. If this is not possible, apply ESD protections such as the following:

- Wear an antistatic wrist strap attached to a chassis ground (any unpainted metal surface) on the equipment when handling parts.
- Touch the metal chassis before touching an electronic component (e.g. a DIMM or board).
- Keep a part of your body (e.g. a hand) in contact with the metal chassis to dissipate the static charge while handling the electronic component.
- Avoid moving around unnecessarily.
- Use a ground strap attached to the front panel (with the bezel removed).
- Read and follow the safety precautions provided for a specific component by the manufacturer.
# Unboxing

[This article gives specific instructions to safely unbox the product and to validate the bill of materials.]

Table of contents

- What’s in the box
- Unboxing steps

> When handling components, follow the precautions described in section ESD protections.

## What’s in the box

The CG2400 platform box includes:

- One CG2400 2U, 20-inch deep, carrier grade rackmount server
- Two heat sink boxes, one labeled “Front” and one labeled “Rear”

## Unboxing steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| **Step_1** | Open the platform box and take out the small heat sink boxes (there will be one or two depending on your order). Set the boxes aside until you are ready to install the processors and heat sinks in the platform. Refer to Components installation and assembly for assembly instructions.  
  **NOTE:**  
  - The processor with the “Front” heat sink must be installed onto the CPU1 socket  
  - The processor with the “Rear” heat sink must be installed onto the CPU2 socket |
| **Step_2** | Carefully remove the platform from the box and remove the two foam pieces. |
| **Step_3** | Remove the platform from the ESD bag. |
| **Step_4** | Remove the plastic film from the platform. *Failure to do so may affect platform airflow efficiency, thus resulting in poor cooling capabilities.* |
| **Step_5** | Put all the packaging back in the box (two desiccant pouches, one ESD bag, two foam pieces). |
Components installation and assembly

(This article provides detailed instructions to safely assemble and install optional components.)

Table of contents

- **Tools and supplies needed**
- **Compatible parts and components**
- **Cable management**
- **Front bezel**
  - Removing the front bezel
  - Reinstalling the front bezel
- **Chasis top cover**
  - Removing the chassis top cover
  - Reinstalling the chasis cover
- **Drivers**
  - Removing a drive carrier from the chasis
  - Installing a drive in a carrier
- **System fans**
  - Removing a fan
- **Power supply unit**
  - Inserting or replacing a power supply unit
- **Riser card assemblies**
  - Removing a riser card assembly
  - Reinstalling the left riser card assembly
  - Reinstalling the right riser card assembly
- **Processor air duct**
  - Removing the processor air duct
  - Reinstalling the processor air duct
- **SuperCap battery backup**
  - Removing the SuperCap battery backup
  - Reinstalling the SuperCap battery backup
- **Support cross-brace**
  - Removing the support cross-brace
  - Reinstalling the support cross-brace
- **SAS hot-swap backplane (HSBP) board**
  - Removing the SAS hot-swap backplane (HSBP) board
  - Reinstalling the SAS hot-swap backplane (HSBP) board
- **Memory DIMMs**
  - Locating the DIMMs
  - DIMM population guidelines for optimal performance
  - Removing memory DIMMs
  - Installing memory DIMMs
- **Processor and heat sink**
  - Socket and processor handling and ESD precautions
  - Handling precautions
  - ESD precautions
  - Processor location
  - Disassembling the processor heat sink module (PHM)
  - Adding or replacing a processor in a PHM
    - Preparing the processor for assembly with the PHM
    - Installing the processor (new heat sink and processor carrier)
    - Installing a PHM in the platform
- **Raid controller**
  - Disconnecting the two SAS cables from the motherboard
  - Locating the SAS cables
  - Removing the SAS cables
  - Installing a hardware RAID controller
  - Installing the SuperCap battery backup module
- **PCIe add-in cards and riser cards**
  - PCIe add-in cards in slots 4 and 5
    - Installing a PCIe add-in card
    - Removing a PCIe card
  - PCIe riser cards
    - Assembling the PCIe riser cards
  - PCIe add-in cards on riser assemblies
    - Removing a PCIe add-in card
    - Installing PCIe add-in cards
- **M.2 storage**
  - Locating the M.2 storage
  - Removing an M.2 storage
  - Installing an M.2 storage
ESD sensitive device!
This equipment is sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this product in order to ensure product integrity at all times.

Disconnect the power supply cord before servicing the product to avoid electric shock. If the product has more than one power supply cord, disconnect them all.

When handling components, follow the precautions described in section ESD protections.

WARNING: The following sections present general removal procedures that are required before removing or installing various internal components that are not necessarily hot-swappable. Before working with the server product, pay close attention to the safety instructions provided in this manual.

All references to left, right, front, rear, top, and bottom assume that you are facing the front of the server, as it would be positioned for normal operation.

Tools and supplies needed
For a list of tools and supplies required for components installation and assembly, consult Material, information and software required.

Compatible parts and components
For the complete list of compatible parts and components that can be ordered from Kontron, consult Platform, modules and accessories.

Cable management
When adding, removing or replacing components in the platform, pay close attention to the cable management before proceeding. The platform components are tightly packed in the chassis and plugging back cables can prove to be more complex than expected.

Follow these guidelines to reduce difficulties related to cable management:
- Take pictures before moving, removing or unplugging components.
- All cables should fit snugly in the chassis without requiring force or pinching.
- Cable management should not impair proper ventilation within the platform.
- Cables will hold their folds and orientation once disconnected. Paying attention to those details will facilitate the task when plugging back cables and managing them.

Front bezel

Removing the front bezel
The front bezel has to be removed to perform tasks such as:
- Installing or removing hot-swappable hard disk drives or an SD flash card
- Observing the individual hard disk drive activity/fault indicators
- Replacing the control panel LED/switch board

NOTE: The system does not have to be powered down just to remove the front bezel.

Step_1: Loosen the captive bezel retention screw on the right side of the bezel (A).
Step_2: Rotate the bezel to the left to free it from the pins on the front panel (B) and remove it.

Reinstalling the front bezel

NOTE: The server does not have to be powered down just to reinstall the front bezel.

Step_1: Insert the tabs on the left side of the bezel into the slots on the front panel of the chassis.
Step_2: Move the bezel towards the right and align it on the front panel pins (A).
Step_3: Snap the bezel into place and tighten the retention screw to secure it (B).

Chassis top cover
Standby power is present inside the chassis whenever the power supply module(s) are connected to a power source. Before removing the top cover, always power down the server and unplug all peripheral devices and the power cable(s).

**NOTICE**
The CG2400 server must be operated with the top cover in place to ensure proper cooling.

**NOTICE**
A non-skid surface or a stop behind the server may be needed to prevent the server from sliding on the work surface.

### Removing the chassis top cover

**Step 1**  Remove the hex HD Phillips 6-32 shipping screw at the front left side of the cover, if it is still attached, and save it for future use.

**Step 2**  Remove the two shoulder screws (one on each side) from the cover.

**Step 3**  While holding the blue unlocking button in the middle of the top cover, slide the cover backwards until it stops and the edge clears the lock bracket on the rear panel of the chassis.

**Step 4**  Lift the cover straight up to remove it from the chassis.

### Reinstalling the chassis cover

**Step 1**  Starting from the rear of the chassis, align the tab on the rear right edge of the cover with the lock bracket on the outside of the rear panel and place the cover down over the chassis with the side edges outside the chassis walls.

**Step 2**  Slide the cover forward until it clicks into place.

**Step 3**  Install the shipping screw if tool entry is required or if the unit will be shipped.

**Step 4**  Put the two shoulder screws back in place (one on each side) to fasten the cover to the chassis frame. Torque screws to 8 lbf·in.

**Step 5**  Reconnect all peripheral devices and the power cord(s).

**CAUTION**  This unit must have the cover installed when it is running to ensure proper cooling.

### Drives

Before you can remove or install a drive, you must first remove (and afterwards put back in place):
- the front bezel

**NOTICE**  If you install fewer than six drives, to ensure proper cooling, the unused drive slots must contain the empty carriers with filler panels that ship with the platform.

### Removing a drive carrier from the chassis

**Step 1**  With the front bezel removed, select the drive slot where a drive will be installed or replaced.

**NOTE:** Drive slot 0 must be used first, then drive slot 1, and so on. Drive slot numbers are printed on the front panel below the drive slots.

**Step 2**  Remove the drive carrier by pressing the green button to open the lever that engages the drive with the backplane (A).

**Step 3**  Pull the drive carrier out of the chassis.
Installing a drive in a carrier

**NOTICE**

Drives must be installed in the proper orientation in the carrier. Failure to do so may damage the equipment.

**Step 1**
- If the drive carrier is empty (first time installation), remove the black plastic filler panel by unfastening the four screws that attach it to the carrier (A). Set the screws aside for use with the new drive.
- OR
- If a drive is already installed (drive replacement), remove it by unfastening the four screws that attach the drive to the drive carrier (A). Set the screws aside for use with the new drive.

**Step 2**
- Lift the drive (or filler panel) out of the carrier (B).

**Step 3**
- Install the new drive in the drive carrier (A) and secure the drive with the four screws (with 4 lbf·in torque, max) (B).

**NOTE:** Ensure proper drive orientation. The SATA connector must be exposed in the back of the carrier. When the carrier is in the position shown on the image, the SATA connector located in the back of the drive must not be visible. It should be in contact with the work surface.

**Step 4**
- With the drive carrier locking lever fully open, push the hard drive carrier into the drive slot in the chassis until it stops (A).

**Step 5**
- Press the locking lever until it snaps shut and secures the drive in the slot (B).

---

System fans

Fans are hot-swappable.

**CAUTION**

Because the fans are hot-swappable, you do not need to shut down the server system and disconnect the power and external devices. Instead of removing the chassis cover, as is customary for working with internal components, simply press the blue unlock button on the cover and slide the cover backwards on the shoulder screws to access the fan area.

Do not completely remove the top cover while the system is running because there is a 12 V energy hazard in the server when the power is on. If the top cover has been removed to access components internal to the system other than the hot-swappable fans, you must power off the server and unplug the power cords.

Replacing a fan
Step_1 Remove the shipping screw, if used, on the left side of the chassis cover.

Step_2 While holding the blue unlocking button (A) in the middle of the top cover, slide the top cover back (B). The two shoulder screws will stop the cover from sliding too far.

Step_3 Determine which fan has failed by finding the LED that is amber. (The LED is next to the blue grommet on the top of each fan assembly).

Step_4 Remove the failing fan by grasping both sides of the fan assembly, using the plastic finger guard on the left side and pulling the fan out of the metal enclosure (C and D).

Step_5 Replace the fan by inserting a new one into the same slot. Use the edges of the metal enclosure to align the fan assembly properly and to make sure the power connector is seated properly in the header on the left side of the metal enclosure.

Step_6 If this is the last task you are performing, close the chassis cover by sliding it forward until it clicks into place. Put the shipping screw back in place, if used.

Power supply unit

The platform can operate with AC or DC power supply units (PSU). A second PSU can be added to provide redundancy. The PSUs are hot-swappable. No chassis components have to be removed to add or replace a PSU. If you are replacing the main PSU and have a redundant PSU in your system, power will switch over to the redundant unit while you replace the main unit.

Inserting or replacing a power supply unit

Step_1 There are two possible scenarios:

Adding a PSU
Remove the filler panel by pressing and holding the green safety lock downward (A) and using the handle to pull the filler panel out of the slot (B).

OR

Replacing a PSU
To replace a PSU (check PSU status LED to confirm the one that failed), unplug the power cord from the PSU being replaced. Remove the defective PSU by pressing and holding the green safety lock downward (A) and using the handle to pull the filler panel out of the slot (B).

Step_2 Insert the new PSU by pressing and holding the green safety lock downward (A) and using the handle to slide the power supply into the slot until it latches into place (B).

Step_3 Plug the power cord. The PSU LED should be solid green.

Riser card assemblies

Before you can remove and reinstall a riser card assembly, you must first remove (and afterwards put back in place):

- the chassis top cover
One or both of the riser card assemblies have to be removed from the chassis to perform tasks such as:

- Installing or replacing a riser card or any PCIe add-in card(s)
- Working with any components on the platform board that are near the riser card assembly

## Removing a riser card assembly

### Removing the left riser card assembly

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Loosen the two blue captive retention screws (A) at the front of the riser assembly and the blue captive screw at the rear of the chassis (B).</td>
</tr>
<tr>
<td>2</td>
<td>Using the two blue touch points (C), lift the riser card assembly out of the chassis (D).</td>
</tr>
</tbody>
</table>

### Removing the right riser card assembly

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Loosen the two blue captive retention screws (A) at the front of the riser assembly and the blue captive screw at the rear of the chassis (B).</td>
</tr>
<tr>
<td>2</td>
<td>Using the two blue touch points (C), lift the riser card assembly out of the chassis (D).</td>
</tr>
</tbody>
</table>

## Reinstalling a riser card assembly

### Reinstalling the left riser card assembly

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Position the riser front tabs over the holes on the PCI support cross-brace.</td>
</tr>
</tbody>
</table>
| 2    | Using the blue touch points on the top of the assembly (A), press down to mate the riser card with the header on the server board (B, slot 2 for the left-side riser). **NOTES:**
  - To avoid damaging the card edge, be sure that the card is lined up straight with the header, not on an angle.
  - If a hardware RAID controller card is installed in PCI slot 3, be careful not to damage the diagnostic pins at the back of the card next to the rear chassis panel when reinstalling the left-side riser assembly. |
| 3    | Align and then tighten the blue captive retention screws at the front of the assembly with the holes on the support cross-brace (D) and on the rear of the chassis (C). |
Reinstalling the right riser card assembly

**Step 1** Position the riser front tabs over the holes on the PCI support cross-brace (over the processor air duct).

**Step 2** Using the blue touch points on the top of the assembly (A), press down to mate the riser card with the header on the server board (B, slot 6 for the right-side riser).
**NOTE:** To avoid damaging the card edge, be sure that the card is lined up straight with the header, not on an angle.

**Step 3** Align and then tighten the blue captive retention screws at the front of the assembly with the holes on the support cross-brace (D) and on the rear of the chassis (C).

---

**Processor air duct**

Before you can remove and reinstall processor air duct, you must first remove (and afterwards put back in place):

- the chassis top cover
- the riser card assemblies

**NOTICE** The black plastic processor air duct must be removed to access the processors and the memory DIMMs or to replace the platform board.

The air duct is required to ensure proper air flow within the chassis. It is important to make sure it is in place before reinstalling the riser card assemblies and the chassis cover.

---

**Removing the processor air duct**

**Step 1** To remove the processor air duct, simply lift the air duct straight up out of the chassis.

---

**Reinstalling the processor air duct**

**Step 1** Place the processor air duct over the processor sockets and DIMMs. Align the front tabs with the captive screws on the support cross-brace. Make sure the pin located on the rear of the chassis is inserted in the moulded groove on the back side of the processor air duct. The air duct is secured when the right riser card assembly is mounted on the support cross-brace above it.
SuperCap battery backup

The optional RAID battery backup and its bracket, if installed, have to be removed to install or remove components located on that area of the motherboard, such as a M.2 module. Since the SuperCap battery backup module is fastened to the support cross-brace, it has to be removed anytime the cross-brace is removed.

To detach and reattach the SuperCap battery backup from the cross-brace, it does not need to be disconnected or connected from the hardware RAID controller. For more information on the hardware RAID controller, refer to the Raid controller section.

Before you can remove and reinstall the SuperCap battery backup, you must first remove (and afterwards put back in place):

- the chassis top cover
- the left riser card assembly

Removing the SuperCap battery backup

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Loosen the captive screw that fastens the battery backup to the support cross-brace (A).</td>
</tr>
</tbody>
</table>
| Step 2 | Lift the assembly up and out of the chassis (B).  
**NOTE:** The SuperCap battery backup module does not need to be disconnected from the hardware RAID controller. |

Reinstalling the SuperCap battery backup

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Position the SuperCap backup battery assembly over the support cross-brace (A).</td>
</tr>
<tr>
<td>Step 2</td>
<td>Tighten the captive screw that fastens the battery backup to the support cross-brace (B).</td>
</tr>
</tbody>
</table>

Support cross-brace

The support cross-brace secures several components, some optional. It is the divider between the front and back. The top cover can be pushed back to the cross-brace without powering down the system in order to service hot-swappable components in the front of the chassis. In contrast, some components in the front of the chassis, such as the front panel board or the power distribution board, cannot be replaced without first removing the cross-brace (along with all the components attached to it). This procedure is necessary in order to have enough space to access these front chassis components.

Before you can remove and reinstall the support cross-brace, you must first remove (and afterwards put back in place):

- the chassis top cover
- the riser card assemblies
- the processor air duct
- the SuperCap battery backup

Removing the support cross-brace
Step 1  Make sure all components secured by the captive retention screws are removed:
- Riser card assemblies
- Processor air duct
- Optional hardware RAID battery backup assembly

Step 2  Remove the three small flat screws that fasten the cross-brace to the sides of the chassis:
- One on the left side
- Two on the right side

Step 3  Remove the support cross-brace from the chassis.

Reinstalling the support cross-brace

Step 1  Reposition the support cross-brace in the chassis.

Step 2  Secure the support cross-brace with the three reserved screws:
- One on the left side
- Two on the right side

SAS hot-swap backplane (HSBP) board

The SAS HSBP board has to be removed to replace the HSBP board or the power distribution board (PDB).
The six-slot SAS backplane board is located at the rear of the HDD drive bay assembly. It is held in place by a cover plate on top of the HDD bay assembly that goes over the top edge of the backplane board. There is also a black plastic air duct surrounding the drive bay on the right side and rear of the assembly.
Before you can remove and reinstall the HSBP board, you must first remove (and afterwards put back in place):
- the chassis top cover
- the front bezel

Removing the SAS hot-swap backplane (HSBP) board
<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Slide all drives out from the drive bay slots to disengage them from the backplane.</td>
</tr>
<tr>
<td>Step_2</td>
<td>Remove the cover plate on the HDD bay assembly by loosening the screw that fastens it to the HDD bay (A) and sliding it to the left towards the chassis wall to release the tabs (B).</td>
</tr>
<tr>
<td>Step_3</td>
<td>Lift the cover plate off of the HDD bay assembly (C).</td>
</tr>
<tr>
<td>Step_4</td>
<td>Lift the HSBP board and HDD air duct assembly up to access the connectors on the back of the board (A).</td>
</tr>
</tbody>
</table>
| Step_5 | Disconnect the four cables attached to the HSBP board (B):  
  - One SAS HDD backplane board power cable  
  - One SAS 1 cable  
  - One SAS 2 cable  
  - One HSBP I²C/HDD LED cable |
| Step_6 | Lift the backplane board and air duct up and out of the chassis (C). |

**Reinstalling the SAS hot-swap backplane (HSBP) board**
Step_1  Reconnect the four cables to the HSBP board (A):
- One SAS HDD backplane board power cable
- One SAS 1 cable
- One SAS 2 cable
- One HSBP 1 C/HDD LED cable

Step_2  Re-install the SAS backplane board and air duct (B).

Step_3  Secure the six-slot HDD backplane in place by placing the cover plate over the HDD bay assembly, the backplane and the air duct (A and B).

Step_4  Re-fasten the screw that holds the cover plate in place (C).

Step_5  Lock in all the drives so they engage with the backplane.

Memory DIMMs

Before you can remove or install memory DIMMs, you must first remove (and afterwards put back in place):
- the chassis top cover
- the right side riser card assembly
- the processor air duct

To reduce the risk of electrostatic discharge (ESD) damage to the processor or the DIMMs, be sure to follow these procedures:
- Touch the metal chassis before touching the DIMMs or server board.
- Keep part of your body (hand, etc.) in contact with the metal chassis to dissipate the static charge while handling the DIMMs.
- Avoid moving around unnecessarily.
- Use a ground strap attached to the front panel (with the bezel removed).

For the list of tested DIMM refer to Hardware compatibility list.

Locating the DIMMs
DIMM population guidelines for optimal performance

There are 8 DIMM slots per CPU, but only 6 channels per CPU – A1 and A2 are on the same channel and D1 and D2 are on the same channel. Therefore, do not populate A2 and D2 unless you have already populated all other DIMM slots.

For optimal performance, both CPUs should have the same DIMM configuration, in single or dual CPU configuration.

For each CPU, populate DIMMs in accordance with the following guidelines to ensure optimal performance.

- For configurations with 1 to 3 DIMMs – populate slots A1, B1, C1, starting with A1.
- For configurations with 4 DIMMs – populate slots A1, B1, D1 and E1.
- Configurations with 5 DIMMs are not recommended as they are unbalanced and will produce a less optimal performance.
- For a configuration with 6 DIMMs – populate slots A1, B1, D1, E1 and F1.
- Configurations with 7 DIMMs are not recommended as they are unbalanced and will produce a less optimal performance.
- For a configuration with 8 DIMMs – populate all DIMM slots.

**NOTICE**

Configuration with 8 DIMMs per CPU will reduce 2933 MHz DIMMs speed one step under its nominal value, so 2666 MHz.

If using 2666 or 2600 MHz memory (8 DIMMs per CPU), negotiated speed will stay to DIMM nominal, unless CPU Maximum memory speed is below DIMM nominal.

- Ex 1. Xeon Silver 4114T CPU @2400MHz will negotiate 2666 MHz DIMM at 2400 MHz
- Ex 2. Xeon Gold 5218T CPU @2666MHz will negotiate 2666 MHz DIMM at 2666 MHz

Removing memory DIMMs

**Step 1**
Open the DIMM slot levers for the DIMM to be removed (A).

**Step 2**
Using both hands, hold the DIMM by the edges and lift it from the slot. Store the DIMM in an anti-static package.

Installing memory DIMMs

**Step 1**
Open the levers of the DIMM slot. (A)

**Step 2**
Note the location of the alignment notch on the DIMM edge. (B)

**Step 3**
Insert the DIMM, making sure the connector edge of the DIMM aligns correctly with the slot. (E)

**Step 4**
Using both hands, push down firmly and evenly on both sides of the DIMM until it snaps into place and the levers close. (C and D)

**Step 5**
Visually inspect each lever to ensure they are fully closed and correctly engaged with the notches on the DIMM edge. (E)

Processor and heat sink

Before you can remove, add or replace a processor or heat sink, you must first remove (and afterwards put back in place):

- the chassis top cover
- the right side riser card assembly
- the processor air duct
Socket and processor handling and ESD precautions

Handling precautions

**NOTICE** Socket contacts are fragile and can be easily damaged if touched. Intel has developed a specific stackup subassembly to provide consistent, controlled motions for inserting and removing processors onto sockets. Kontron expects users and system integrators to use the Intel-designed methodology at all points in the procedures in this section where a processor is being removed or inserted in a socket.

The processor heat sink module (PHM) refers to the subassembly where the heat sink and processor are clipped together prior to installation. This allows for a more robust installation by providing better alignment features and keeping fingers away from the socket contact field. The subassembly stackup consists of three different parts.

Image source: Intel Corporation

**ESD precautions**

Be mindful of the following points when handling the processors and sockets to reduce the risk of electrostatic discharge (ESD) damage to the processor:

- Touch the metal chassis before touching the processor or server board.
- Keep part of your body (hand, etc.) in contact with the metal chassis to dissipate the static charge while handling the processor.
- Avoid moving around unnecessarily.
- Use a ground strap attached to the front panel (with the bezel removed).

**Processor location**

**Disassembling the processor heat sink module (PHM)**
Step 1
Loosen the four captive screws on the corners of the heat sink with a T30 Torx screwdriver. Loosen the screws gradually using a star pattern (i.e. corner one half a turn, corner 3 half a turn, corner 2 half a turn, corner 4 half a turn; then go back to corner 1 for another round). Take the PHM out.

Step 2
Disassemble the processor carrier (which contains the processor) from the heat sink. To do so, using your fingers:
1. Slightly unclip corner 1.
2. Slightly unclip corner 3.
3. Slightly unclip corner 2.

Step 3
Insert a 1/4" wide #1 flat-head screwdriver in the location indicated on the image (you will see a screwdriver engraving in the processor carrier in the appropriate location). Slightly turn the screwdriver to pop the processor carrier out of the heat sink.

NOTE: To protect the processor, place the processor carrier on the table in the orientation shown on the image, i.e. carrier on the table with the processor above it.

Step 4
Using your thumb, pull on the tab and flip the processor to release it from the processor carrier. Store the processor in an anti-static package.

Adding or replacing a processor in a PHM

**NOTICE**
The processor must be appropriate.
Severe damage to the platform board may occur if a processor that is inappropriate is installed. Refer to the Hardware compatibility list for a list of components.

**NOTICE**
Kontron recommends performing a CPU socket inspection before adding or replacing a processor to ensure there is nothing wrong with the fragile socket pins.

Preparing the processor for assembly with the PHM

Step 1
Remove the cover of the processor packing tray. From this position, the processor will be ready to be clipped to the rest of the PHM components.

CAUTION: Do not touch the processor.

Installing the processor (new heat sink and processor carrier)

Relevant section: Processor location
Step 1

Remove the heat sink from its packaging box.

NOTE:
- The processor with the “Front” heat sink must be installed onto the CPU1 socket (see Processor location).
- The processor with the “Rear” heat sink must be installed onto the CPU2 socket (see Processor location).

Step 2

Take the new PHM (processor carrier and heat sink) and place it above the processor, which is in its open packing tray. The assembly triangles (pin one indicator) must be in the appropriate positions before you lower the PHM.

NOTE: In this image, the heat sink was removed for clarity. Only the processor carrier and processor are shown.

Step 3

Gently clip the processor in the PHM. Lift the assembly. The processor should be clipped in place.

Installing a PHM in the platform

Step 1

Align the triangle of the bolster plate with that of the processor. Lay the PHM on the bolster plate.

Step 2

Gradually (in a star pattern) and equally tighten each of the four screws in a diagonal pattern until each one is firmly tightened (12.0 in-Lb torque).

Raid controller

Hardware RAID support requires an optional RAID/SAS controller.

The components used as examples in this section are from the Intel® RS3DC080 hardware.

The following figure shows the SAS hardware RAID controller board layout. The board’s gold edge connector attaches to a header on the motherboard as shown in the Installing a hardware RAID controller section.

Hardware RAID adapter layout

Before you can install or remove the hardware RAID controller board and the SuperCap battery backup module, you must first remove (and afterwards put back in place):
- the chassis top cover
- the left side riser card assembly

Disconnecting the two SAS cables from the motherboard

Locating the SAS cables
Disconnecting the SAS cables

Step_1 Disconnect the two SAS cables (SFF-8643 ends) from the motherboard.

Installing a hardware RAID controller

Step_1 Unfasten the screw holding the slot 3 RAID card bracket. Remove the bracket from the chassis rear panel and the PCIe slot 4 filler.

Step_2 Fasten the bracket from the chassis to the RAID controller board using the two screws from the bracket (A).

Step_3 Match cable connected to Ports 0-3 of the HDD cage to Port 3-0 of the RAID/SAS card, connecting the loose end to the RAID card (B). Match cable connected to Ports 4-5 of the HDD cage to Port 7-4 of the RAID/SAS card, connecting the loose end to the RAID card (B).

Optionally, if you are using a RAID SuperCap battery backup module:
- Affix the SuperCap battery backup holder to the chassis cross-brace (G).
- Connect the SuperCap battery module to the RAID card (C and F).

Step_4 Reinstall slot 4 PCIe filler (removed at Step_1), then insert the hardware RAID controller board in the PCIe slot 3 on the motherboard and press down to mate it with the header (D). Slot 3 bracket sits directly on top of the slot 4 filler.

Step_5 Secure the slot 3 faceplate by attaching it with the screw previously removed (Step_1).

Installing the SuperCap battery backup module

This module is a flash-based battery backup module for SAS drives. It comes as a part of the Intel RS3DC080 RAID controller kit and may not be compatible with other RAID products. The mounting bracket for the module must be ordered separately, see Platform, modules and accessories.
Step 1: Insert the module into the black plastic tray (A).

Step 2: Fasten the module and tray assembly to the sheet metal bracket by inserting the tabs into the cut-outs on the bracket (B).

Step 3: Slide the module/tray assembly towards the back (side with the connector) of the bracket until it locks into place.

Step 4: Connect the signal/power pigtail cable to the proper connector on the hardware RAID controller board (C) and the rear of the battery backup assembly (F).

Step 5: Place the battery backup bracket on the support cross-brace, lining it up with the center hole on the middle shelf (G).

Step 6: Use the blue retention screw to fasten the battery backup assembly bracket to the cross-brace.

NOTE: Once the platform is powered and functional, proceed with required software configurations.

PCIe add-in cards and riser cards

Only compatible PCIe riser cards and add-in cards can be used, refer to Platform, modules and accessories to select an appropriate riser card/add-in card combination.

CAUTION: Due to certain manufacturers not always following proper dimensions specification, there is a possibility of a mechanical conflict with a heatsink when inserting a PCIe card in slot 5. If the spacing is deemed insufficient when inserting a PCIe card, it is recommended to properly insulate the card by adding protection (i.e. Lexan / Kapton tape) to the heatsink in order to prevent a short-circuit.

PCIe add-in cards in slots 4 and 5

Two half-height, full-length PCIe cards can be inserted in PCIe slots 4 and 5 of the motherboard. Before you can install or remove a PCIe add-in card, you must first remove (and afterward put back in place):

- the chassis top cover

Installing a PCIe add-in card

Step 1: Unfasten the screw holding the filler panel in the PCIe slot. Remove the blank filler panel and store it for future use.

Step 2: Insert the PCIe add-in card in the motherboard’s PCIe slot and press down to mate it with the header.

Step 3: Secure the PCIe add-in card to the chassis using the screw removed at step 1.

Removing a PCIe card

Step 1: Unfasten the screw holding the PCIe add-in card installed in the slot.

Step 2: Remove the PCIe add-in card from the motherboard’s PCIe slot.

Step 3: Put the blank filler panel (removed when the card was installed) back in place and fasten it to the chassis using the screw removed at step 1.

NOTE: The filler panel is required for proper airflow.

PCIe riser cards

PCIe riser cards are not included with the platform, which contains only the sheet metal brackets to house the PCIe riser cards and add-in cards. Before you can install a PCIe riser card, you must first remove (and afterwards put back in place):

- the chassis top cover.
- the riser card assemblies.

Assembling the PCIe riser cards
Step_1  Fasten each riser card to its bracket with the two 6/32 screws (8 lbf·in torque).

Riser cards are now ready to receive add-in cards.

### PCIe add-in cards on riser assemblies

The figures in this section use the left-side riser card assembly (slot 2), a dual-slot riser card and a single PCIe add-in card as an example.

Before you can remove or add a PCIe add-in card, you must first remove (and afterwards put back in place):
- the chassis top cover

#### Removing a PCIe add-in card

**Step_1** Remove the riser card assembly.
- Loosen the two blue captive retention screws at the front of the riser assembly and the blue captive screw at the rear of the chassis.
- Using the two blue touch points, lift the riser card assembly out of the chassis.

**Step_2** Unfasten and remove the rear retention screw (D).

**Step_3** For a full-length card, prior to pulling out the card from the riser, open the card edge retainer in the front of the assembly by loosening the blue captive screw (B).
- Remove the PCIe add-in card assembly from the riser card socket (C).

**Step_4** Install the blank filler panel (A). Fasten the screw (D) to hold the filler panel in place (8 lbf·in torque).

**NOTE:** The filler panel is required for proper airflow.

#### Installing PCIe add-in cards

Before you can install a PCIe add-in card for the first time, **the riser card must be assembled**. If a PCIe add-in card is already in place, consult the removing PCIe add-in cards section for instructions on how to remove it (perform steps 1 to 3 only).

**Step_1** If you are installing a PCIe add-in card for the first time, remove the blank filler panel from the riser card assembly (A) by unfastening the screw of the selected slot (D).

**Step_2** If you are installing a PCIe add-in card for the first time, for a full-length add-in card, open the card edge retainer by loosening the blue captive screw (B).

**NOTE:** An half-length card does not sit into the card edge retainer, simply go to the next step.

**Step_3** Attach the add-in card to the appropriate riser card connector (C), making sure it is seated correctly in the riser card connector.

**Step_4** Fasten the add-in card to the riser card assembly bracket using the rear retention screw (D). For full-length cards, also secure the card in the grooves on the retainer bracket (B).

**Step_5** Using the two blue touch points (A), install the riser card assembly into its slot (slot 2 or slot 6) on the motherboard.

**Step_7** Secure the riser card assembly by tightening the captive screws (C and D).
M.2 storage

An optional M.2 storage can provide SATA or NVMe (PCIe) storage. The M.2 storage is installed on the platform board. Before you can remove or install an M.2 storage, you must first remove (and afterwards put back in place):

- the chassis top cover
- the left side inter card assembly

NOTE: Images show two M.2 storage drives. The procedures are described for one M.2 storage.

Locating the M.2 storage

Removing an M.2 storage
<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Remove the clip from the post to release the M.2 storage.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Remove the M.2 card from the connector.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Insert the clip back in the post to secure the M.2 storage.</td>
</tr>
</tbody>
</table>

**Installing an M.2 storage**
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Remove the clip from the post. <strong>NOTE:</strong> When only one M.2 storage is added, it is recommended to use the slot located near the fans.</td>
</tr>
<tr>
<td>Step_2</td>
<td>Insert one end of the M.2 card in the connector and seat the other end around the post on the motherboard.</td>
</tr>
<tr>
<td>Step_3</td>
<td>Secure the M.2 storage by inserting the clip in the post.</td>
</tr>
</tbody>
</table>
Airflow

This article provides guidelines to ensure proper airflow to the platform.

Table of contents

- Airflow direction
- Considerations for proper airflow

Airflow direction

![Airflow Diagram](image)

Considerations for proper airflow

Relevant section: Components installation and assembly

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Details</th>
</tr>
</thead>
</table>
| Consideration_1 | For proper airflow, the following components always need to be reinstalled after being taken out for component replacement or installation:  
  - Processor air duct  
  - Riser card assemblies (left and right)  
  - Top cover  
  - Drive carrier black plastic filler panel (when a drive is not installed in a slot) |
| Consideration_2 | Six fans must be installed at all times. |
| Consideration_3 | In a single PSU configuration, a PSU filler panel must be installed in the unused slot. |
| Consideration_4 | If no PCIe cards are installed in slots 4 and 5, filler panels must be installed on the rear of the chassis. |
Rack installation

[This article provides instructions on how to install and ground a platform in a rack.]

Table of contents
- Selecting a rail kit
- Rack mount kits
  - TMLCMOUNT21
  - TMLPMOUNT51
  - TMLPMOUNT52
- Bracket and extender kits
  - 1059-8187 extender kit
  - 1061-2890 extender kit
- Installing the server in a rack
  - Using TMLPMOUNT51 or TMLPMOUNT52
  - Installing inner rails and mounting ears
  - Building the outer rail assembly
    - Four-post installation – racks under 24-inches deep
    - Four-post installation – racks 24- to 31¾-inches deep
    - Four-post installation – racks 30½- to 34⅜-inches deep
    - Two-post installation
  - Attaching the outer rail assemblies to the rack posts
  - Securing the equipment
    - Securing the equipment to a 4-post rack
    - Securing the equipment to a 2-post rack
  - Using TMLPMOUNT21
- Earth grounding

Selecting a rail kit

The rack mounting kits offered for this product are designed to be used with 2-post or 4-post racks that have a width of a 19” or 23”.

All rack mount kits in the diagram below conform with the EIA standard.

All rack mount kits in the diagram below come with the appropriate hardware to mount the platform in a 20” to 24” deep rack. For racks deeper than 24”, an extender kit is also required.

TMLPMOUNT51 and TMLPMOUNT52 are designed with a slide-in rail-type system. Rails are designed to support a mounted server during fan service. TMLCMOUNT21 is only compatible with 2-post, 19” wide racks and anchors the chassis in place. Therefore, it is recommended for lab use only.

To select between TMLPMOUNT51 and TMLPMOUNT52, use the following diagram.
<table>
<thead>
<tr>
<th>Product code</th>
<th>Description</th>
<th>Slide pull out mechanism</th>
<th>Minimum order</th>
</tr>
</thead>
<tbody>
<tr>
<td>TMLCMOUNT21</td>
<td>Rack mount kit Used to mount servers on 19&quot; wide, 2-post racks. <strong>NOTE</strong>: For lab purposes only</td>
<td>No</td>
<td>10</td>
</tr>
<tr>
<td>TMLP Mount51</td>
<td>Rack mount kit Used to mount servers on 19&quot; wide, 2-post or 4-post racks. <strong>NOTE</strong>: Xylan finish</td>
<td>Yes</td>
<td>1</td>
</tr>
</tbody>
</table>
| TMLP Mount52 | Rack mount kit Used to mount servers on 23" wide, 2-post or 4-post racks. **NOTES**:  
  • Xylan finish  
  • ETSI brackets included | Yes                       | 1             |
| 1059-8187    | Rail extender kit Maximum rack depth when used with TMLP Mount51: 34".       | N/A                       | 1             |
| 1061-2890    | Rail extender kit Maximum rack depth when used with TMLP Mount52: 34".       | N/A                       | 1             |

**NOTES:**
- Using slide rails could result in non-compliance with Seismic Zone 4 requirements of NEBS-3.
- Xylan is a tough, low-friction coating similar to Teflon.
- ETSI Wide spacing doesn't have the interstitial hole that is present in EIA Universal spacing. TMLP Mount51 contains an ETSI Wide Adapter to overcome issue.

**Rack mount kits**

**TMLCMOUNT21**
Refer to [TMLCMOUNT21 installation instructions](#) for details.

**TMLP Mount51**

<table>
<thead>
<tr>
<th>Item</th>
<th>Qty</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>LEFT INNER RAIL</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>RIGHT INNER RAIL</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>MOUNTING EAR</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>OUTER RAIL</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>19&quot; EIA L-BRACKET</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>2-POST MOUNTING BRACKET</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>EIA WIDE ADAPTER</td>
</tr>
<tr>
<td>10</td>
<td>12</td>
<td>B-32 X 1/4 SEMS SCREW</td>
</tr>
<tr>
<td>11</td>
<td>16</td>
<td>10-32 X 1/2 SEMS SCREW</td>
</tr>
<tr>
<td>12</td>
<td>14</td>
<td>B-32 KEPS NUT</td>
</tr>
<tr>
<td>13</td>
<td>4</td>
<td>1U EIA BARNUT</td>
</tr>
<tr>
<td>15</td>
<td>4</td>
<td>2U EIA BARNUT</td>
</tr>
<tr>
<td>17</td>
<td>12</td>
<td>M4x0.7 SCREWS FOR MS1300</td>
</tr>
</tbody>
</table>
NOTE: 2U barnuts allow the installation of a rail kit into a 1U rack slot when equipment is already installed both above and below that open slot.

**TMLPMOUNT52**

<table>
<thead>
<tr>
<th>Item</th>
<th>Qty</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>LEFT INNER RAIL</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>RIGHT INNER RAIL</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>MOUNTING EAR</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>OUTER RAIL</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>23&quot; EIA L-BRACKET</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>23&quot; ETSI L-BRACKET</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>2-POST MOUNTING BRACKET</td>
</tr>
<tr>
<td>10</td>
<td>12</td>
<td>8-32 X 1/4 SEMS SCREW</td>
</tr>
<tr>
<td>11</td>
<td>16</td>
<td>10-32 X 1/2 SEMS SCREW</td>
</tr>
<tr>
<td>12</td>
<td>14</td>
<td>8-32 KEPS NUT</td>
</tr>
<tr>
<td>13</td>
<td>4</td>
<td>1U EIA BARNUT</td>
</tr>
<tr>
<td>14</td>
<td>4</td>
<td>1U ETSI BARNUT</td>
</tr>
<tr>
<td>15</td>
<td>4</td>
<td>2U EIA BARNUT</td>
</tr>
<tr>
<td>16</td>
<td>4</td>
<td>2U ETSI BARNUT</td>
</tr>
<tr>
<td>17</td>
<td>12</td>
<td>M4x0.7 SCREWS FOR MS1300</td>
</tr>
</tbody>
</table>

NOTE: 2U barnuts allow the installation of a rail kit into a 1U rack slot when equipment is already installed both above and below that open slot.

**Bracket and extender kits**

### 1059-8187 extender kit

<table>
<thead>
<tr>
<th>Item</th>
<th>Qty</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>2</td>
<td>24&quot; to 34&quot; EIA L-BRACKET FOR 19&quot; RACK</td>
</tr>
<tr>
<td>19</td>
<td>4</td>
<td>RETAINER BRACKET</td>
</tr>
</tbody>
</table>

### 1061-2890 extender kit

<table>
<thead>
<tr>
<th>Item</th>
<th>Qty</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>4</td>
<td>RETAINER BRACKET</td>
</tr>
<tr>
<td>20</td>
<td>2</td>
<td>24&quot; to 34&quot; EIA L-BRACKET FOR 23&quot; RACK</td>
</tr>
<tr>
<td>21</td>
<td>2</td>
<td>24&quot; to 34&quot; ETSI L-BRACKET FOR 23&quot; RACK</td>
</tr>
</tbody>
</table>
**CAUTION** Anchor the equipment rack – The equipment rack must be anchored to an unmovable support to prevent it from falling over when one or more servers are extended in front of it on slide assemblies. The equipment rack must be installed according to the manufacturer’s instructions. You must also consider the weight of any other device installed in the rack.

When using a rack, wait until the server is properly mounted in the rack before plugging the power cord(s).

**Mains power disconnect** — The power cord(s) is considered the mains disconnect for the server and must be readily accessible when installed. If the individual server power cord(s) will not be readily accessible for disconnection then you are responsible for installing a power disconnect for the entire rack unit. This main disconnect must be readily accessible, and it must be labeled as controlling power to the entire rack, not just to the server(s). To remove all power, two power cords must be removed.

**Grounding the rack installation** — To avoid the potential for an electrical shock hazard, for AC power you must include a third wire safety ground conductor with the rack installation. For DC power the two studs for chassis enclosure grounding must be used for proper safety grounding. With AC power, if the server power cord is plugged into an outlet that is part of the rack, then you must provide proper grounding for the rack itself. If the server power cord is plugged into a wall outlet, the safety ground conductor in the power cord provides proper grounding only for the server. You must provide additional, proper grounding for the rack and other devices installed in it.

**AC overcurrent protection** — When AC power is used, the server is designed for a line voltage source with up to 20 amperes of overcurrent protection per cord feed. If the power system for the equipment rack is installed on a branch circuit with more than 20 amperes of protection, you must provide supplemental protection for the server. The overall current rating of a server configured with two power supplies is less than 6 amperes.

Refer to the Safety and regulatory information section for more information about mains power disconnect, earth grounding and AC overcurrent protection.

**NOTE:** Temperature — The operating temperature of the server, when installed in an equipment rack, must not go below 5°C (41°F) or rise above 40°C (104°F). Extreme fluctuations in temperature can cause a variety of problems in the server.

---

**Using TMLPMOUNT51 or TMLPMOUNT52**

**Installing inner rails and mounting ears**

**Step 1** Attach the left inner rail (item 1) and the right inner rail (item 2) to the chassis using 3 screws (item 10) per inner rail.

**Step 2** Attach the 2 mounting ears (item 3) to the chassis using 2 screws (item 10) per mounting ear.

Mounting ears (item 3) can be flipped to position the equipment further forward in the rack.

**Building the outer rail assembly**

- For a 4-post installation for racks under 24" deep, go to Four-post installation – racks under 24-inches deep
- For a 4-post installation for racks 24" to 31¾" deep, go to Four-post installation – racks 24- to 31¾-inches deep
- For a 4-post installation for racks 30¾" to 34¾" deep, go to Four-post installation – racks 30¾- to 34¾-inches deep
- For a 2-post installation, go to Two-post installation

**Four-post installation – racks under 24-inches deep**

**Step 1** Insert 2 L-brackets (item 5 for 19” EIA, item 6 for 23” EIA or item 7 for 23” ETSI) on the threaded studs of an outer rail (item 4) as shown in the figure.

**Step 2** Loosely screw on 2 nuts (item 12) per L-bracket.

**Step 3** Adjust the L-brackets to the required length and tighten the nuts.

**Step 4** Perform steps 1 to 3 again to build a total of 2 outer rail assemblies.

**Four-post installation – racks 24- to 31¾-inches deep**

---
Step 1: Insert 1 L-bracket (item 5 for 19" EIA, item 6 for 23" EIA or item 7 for 23" ETSI) and 1 extender L-bracket (item 18 for 19" EIA, item 20 for 23" EIA or item 21 for 23" ETSI) on the threaded studs of an outer rail (item 4) as shown in the figure.

Step 2: Insert 2 retainer brackets (item 19) on the threaded studs as shown in the figure.

Step 3: Loosely screw on 2 nuts (item 12) per L-bracket.

Step 4: Adjust the L-brackets to the required length and tighten the nuts.

Step 5: Perform steps 1 to 4 again to build a total of 2 outer rail assemblies.

---

### Four-post installation – racks 30¼- to 34⅞-inches deep

Step 1: Insert 1 L-bracket (item 5 for 19" EIA, item 6 for 23" EIA or item 7 for 23" ETSI) and 1 extender L-bracket (item 18 for 19" EIA, item 20 for 23" EIA or item 21 for 23" ETSI) on the threaded studs of an outer rail (item 4) as shown in the figure.

Step 2: Insert 2 retainer brackets (item 19) on the threaded studs as shown in the figure.

Step 3: Loosely screw on 2 nuts (item 12) per L-bracket.

Step 4: Adjust the L-brackets to the required length and tighten the nuts.

Step 5: Perform steps 1 to 4 again to build a total of 2 outer rail assemblies.

---

### Two-post installation

Step 1: Insert 2 L-brackets (item 5 for 19" EIA, item 6 for 23" EIA or item 7 for 23" ETSI) on the threaded studs of an outer rail (item 4) as shown in the figure.

Step 2: Insert a 2-post mounting bracket (item 8) on the threaded studs as shown in the figure.

Step 3: Loosely screw on a total of 5 nuts (item 12) for both L-brackets.

Step 4: Adjust the L-brackets to the required length and tighten the nuts.

Step 5: Perform steps 1 to 4 again to build a total of 2 outer rail assemblies.

---

### Attaching the outer rail assemblies to the rack posts

If installing in a 4-post rack with EIA wide hole spacing, the EIA wide adapter (item 9) must be installed on top of the front L-brackets using 2 screws (item 11) per L-bracket as shown in the figure.
Step_1  Attach the outer rail assemblies (as built during the Building the outer rail assembly phase) to the rack using 8 or 12 screws (item 11). If the rack is designed to use cage nuts, no bar nuts will be required. If the rack has round holes, bar nuts (item 13 for EIA and item 14 for ETSI) should be used. Make sure the hole pattern of the bar nut matches the hole pattern of the L-bracket. **NOTE:** If the rack is not designed for cage nuts and multiple 1U systems must be installed immediately one on top of the other, 2U bar nuts (item 15 for EIA and item 16 for ETSI) should be used for convenience purposes.

Step_2  Slide the equipment into the rack, making sure the inner rails slide into the outer rails. Support the weight of the system until the lock clicks into the outer rails. **NOTE:** To take the equipment out, slide it forward until you can access the locks. Depress the locks on both sides and continue to pull out the equipment, while fully supporting the system weight.

Securing the equipment

- For a 4-post rack, go to [Securing the equipment to a 4-post rack](#).
- For a 2-post rack, go to [Securing the equipment to a 2-post rack](#).

Securing the equipment to a 4-post rack

Step_3  Fasten each mounting ear (item 3) to a front L-bracket using a total of 2 screws (item 11) as shown in the figures.

Securing the equipment to a 2-post rack
Step 1  Fasten each mounting ear (item 3) to a 2-post mounting bracket (item 8) using a total of 2 screws (item 11) as shown in the first figure.

Using TMLPMOUNT21

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Fasten each mounting bracket to the platform using a total of 3 screws as shown in the figure.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Fasten each mounting bracket to the rack using a total of 2 screws as shown in the figure.</td>
</tr>
</tbody>
</table>

Earth grounding

Relevant sections:
- Platform, modules and accessories
- Material, information and software required
- Safety and regulatory information

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>If a ground lug is installed, remove the 2 nuts and washers from the ground lug studs. Take out the ground lug.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Strip 19 mm (0.75 in) of the 8 AWG ground cable.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Insert the 8 AWG ground cable in the ground lug. Crimp the lug on the cable using an appropriate hand crimp tool (e.g. Panduit CT–1700 crimp tool set at: Color Code = Red; Die Index No. = P21).</td>
</tr>
<tr>
<td>Step 4</td>
<td>Install the ground lug on the studs, fastening with the 2 nuts and washers.</td>
</tr>
</tbody>
</table>
Cabling

(This article provides all necessary details to safely connect the platform: connection types, required cables, prerequisites, connection sequences.)

Table of contents
- AC power supply
  - Power cord usage guidelines
  - AC power supply connection
- DC power supply
  - DC power supply input connector
  - Connector Assembly Process
  - Building the power cables
  - DC power supply connection

AC power supply

If an AC power cord was not provided with your product, you can purchase one that is approved for use in your country.

WARNING
To avoid electrical shock or fire:
- Do not attempt to modify or use the AC power cord(s) if they are not the exact type required to fit into the grounded electrical outlets.
- The power cord must have an electrical rating that is greater than or equal to that of the electrical current rating marked on the product.
- The power cord must have a safety ground pin or contact that is suitable for the electrical outlet.
- The power supply cord(s) are the main disconnect device to AC power. The socket outlet(s) must be near the equipment and readily accessible for disconnection.
- The power supply cord(s) must be plugged into socket-outlet(s) that are provided with a suitable earth ground.

Power cord usage guidelines

The following guidelines may assist in determining the correct cord set. The power cord set used must meet local country electrical codes.

- For the U.S. and Canada, UL Listed and/or CSA Certified (UL is Underwriters’ Laboratories, Inc., CSA is Canadian Standards Association).
- For outside of the U.S. and Canada, cords must be certified according to local country electrical codes, with three 0.75-mm conductors rated 250 Vac.
- Wall outlet end connector:
  - Cords must be terminated in a grounding-type male plug designed for use in your region.
  - The connector must have certification marks showing certification by an agency acceptable in your region.
- Platform end connectors are IEC 320 C13 type female connectors.
- Maximum cord length is 2 m.

AC power supply connection

<table>
<thead>
<tr>
<th>Step_1</th>
<th>Connect appropriately rated cables from an external power source to each power supply on the rear of the platform.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image1.png" alt="Step_1 Image" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_2</th>
<th>Check each power supply LED to make sure they are blinking green (payload off) or steady green (payload on). If this is not the case, refer to Platform components for a description of LED behavior.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image2.png" alt="Step_2 Image" /></td>
</tr>
</tbody>
</table>

DC power supply

NOTICE Before working with this product or performing instructions described in the getting started section or in other sections, read the Safety and regulatory information section pertaining to the product. Assembly instructions in this documentation must be followed to ensure and maintain compliance with existing product certifications and approvals. Use only the described, regulated components specified in this documentation. Use of other products/components will void the CSA certification and other regulatory approvals of the product and will most likely result in non-compliance with product regulations in the region(s) in which the product is sold.

DC power supply input connector

![DC power supply input connector Image](image3.png)
**Connector Description**

The input connector for the DC power supply is a 3-pin Positronic. This connector is rated at 20 A/pin. An earth ground pin is not required because the platform is equipped with two earth ground studs on its rear panel.

**Connector Assembly Process**

![Diagram of connector assembly process]

**Building the power cables**

**WARNING:** Installation of this product must be performed in accordance with national wiring codes and conform to local regulations.

To build the power cables (ends that will be plugged in the CG2400), the material, tools and wires specified below are required.

**NOTE:** The other ends of the cables will need to be built according to national wiring codes and conform to local regulations in addition to your data center power installation requirements.
Black stranded 12 AWG wire to build the power cable based on the length required
Red stranded 12 AWG wire to build the power cable based on the length required
Positronic DC power supply input mating connector (includes a strain relief assembly)
Positronic gauge-16 crimp terminal
Strain relief screw
Strain relief plate
Flat head Phillips screw
DMC AF8 hand crimp tool
Manual extraction tool

Below is a link to a video showing how to crimp pins and assemble them into the connector.

NOTE: The process is valid for both the CG2300 and CG2400 connectors.

Step_1 Strip 6.6 mm [0.26 in] from the end of a black stranded 12 AWG wire.
Step_2 Strip 6.6 mm [0.26 in] from the end of a red stranded 12 AWG wire.
Step_3 Insert each wire in a crimp terminal. Follow the crimp terminal manufacturer’s procedure, using the appropriate hand crimp tool as specified in the DMC AF8 data sheet.
Step_4 Insert the crimped red wire and the crimped black wire in the appropriate sockets in the receptacle housing.
Step_5 Insert the strain relief plate in the appropriate strain relief assembly part.
Step_6 Insert the connector and wire assembly in the strain relief assembly sub assembly.
Step_7 Place the cover to complete the strain relief assembly.
Step_8 Insert and tighten the 2 flat head Phillips screws (one on each side) to secure the assembly.
Step_9 Insert and tighten the 2 strain relief screws to secure the strain relief plate.

DC power supply connection
Step 1  Connect appropriately rated cables from an external power source to each power supply on the rear of the unit.

Step 2  Check each power supply LED to make sure they are blinking green (payload off) or steady green (payload on).
If this is not the case, refer to Platform components for a description of LED behavior.
Software installation and deployment

(This section provides detailed software installation instructions and the steps required to prepare and to validate the deployment.)

Children

- Preparing for installation
- Installing an operating system on a server
- Verifying installation
- Platform installation for high availability
- Common software installation
Preparing for installation

(This article details the steps required to prepare for the installation: obtaining drivers, identifying MAC addresses, selecting a path to install the OS.)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose the operating system needed based on the requirements of your application (CentOS 7.6 or latest version is recommended).</td>
</tr>
<tr>
<td>Step 2</td>
<td>Confirm the OS version to be installed includes or is compatible with the following network interface driver: i40e.</td>
</tr>
<tr>
<td>Step 3</td>
<td>If applicable, download the ISO file of the OS to be installed.</td>
</tr>
</tbody>
</table>

For a list of known compatible operating systems, refer to [Validated operating systems](#). For information on components, refer to the [PCI mapping](#).
Installing an operating system on a server

(This article provides step-by-step OS installation instructions for all access paths.)

Table of contents
- Installing an OS on a server using the KVM
  - Prerequisites
  - Browser considerations
  - Connecting to the Web UI of the BMC
  - Changing the user name and password
  - Launching the KVM
  - Mounting the operating system image via virtual media
  - Accessing the BIOS setup menu
  - Selecting the boot order from boot override
  - Completing operating system installation
- Installing an OS on a server using PXE (Boot from LAN)
  - Completing operating system installation
- Installing an OS on a server using a USB storage device
  - Preparing the USB storage device
  - Configuring Boot Override
  - Completing operating system installation
- Installing a legacy OS
  - Installing RHEL/CentOS 7.3 and preparing for AST driver installation
  - Prerequisites
  - Enabling the USB keyboard for use in the boot loader in Legacy
  - Installing RHEL/CentOS 7.3 and preparing for AST driver installation
  - Installing the AST driver
  - Installing the network driver in RHEL/CentOS 7.3
  - Preventing yum from upgrading the kernel on RHEL/CentOS 7.3

The operating system can be installed using the following methods:
- Using the KVM
- Using PXE (Boot from LAN)
- Using a USB storage device

For a Legacy OS, refer to Installing a legacy OS.

Installing an OS on a server using the KVM

Relevant section:
- Accessing a BMC

Prerequisites

1. The BMC IP address is known (refer to section Configuring/Baseboard management controller – BMC to obtain the BMC MNGMT_IP).
2. The remote computer has access to the management network subnet.

Browser considerations

<table>
<thead>
<tr>
<th>Browser consideration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML5</td>
<td>To connect to the Web UI, a Web browser supporting HTML5 is required.</td>
</tr>
<tr>
<td>HTTPS self-signed certificate</td>
<td>Upon connection to the Web UI, it is mandatory to accept the HTTPS self-signed certificate. For further information about accepting HTTPS self-signed certificates, please refer to your Web browser’s documentation.</td>
</tr>
<tr>
<td>File download permission</td>
<td>File download from the site needs to be permitted. For further information about file download permission, please refer to your Web browser’s documentation.</td>
</tr>
<tr>
<td>Cookies</td>
<td>Cookies must be enabled in order to access the website. For further information about enabling cookies, please refer to your Web browser’s documentation.</td>
</tr>
</tbody>
</table>

NOTE: The procedure may vary depending on the browser used. Examples provided use Firefox.

Connecting to the Web UI of the BMC
Step_1 From a remote computer that has access to the management network, open a browser window and enter the IP address discovered for the BMC.

NOTE: The HTTPS prefix is mandatory.

https://[BMC MNGMT_IP]

Step_2 Click on Advanced in order to start the HTTPS self-signed certificate acceptance process. Information on the error message will be displayed.

Step_3 Click on Add Exception... The Add Security Exception pop-up window will be displayed. Click on Confirm Security Exception to allow the browser to access the management Web UI of this interface.

Step_4 Log in to the BMC Web UI using the appropriate credentials.

NOTE: Default Web UI user name and password is admin/admin.

Step_5 You now have access to the management Web UI of the BMC. You can use the interface.

Changing the user name and password

Note that the password field is mandatory, must have a minimum of 8 characters and not use dictionary words. It is recommended, but not mandatory, to enter a strong password consisting of at least one upper case letter, alpha-numeric character, and special character. You must avoid symbols from the extended ASCII table as they are not managed by the IPMI tool.
Step_1  Click on **Settings** in the left side menu and click on **User Management**.

Step_2  Select the user to manage.  
**NOTE:** The first and second users are reserved fields, therefore, their usernames can’t be modified.

Step_3  Change field **Username** if required.

Step_4  Check the **Change Password** box.

Step_5  Create a new password.  
**NOTE:** It is recommended, but not mandatory, to enter a strong password consisting of at least one upper case letter, alpha-numeric character, and special character. You **MUST** avoid symbols from the extended ASCII table as they are not managed by the IPMI tool. Please note that password field is mandatory and should have a minimum of 8 characters when SNMP status is enabled.

Step_6  Confirm the password.

Step_7  Press **Save**.

**Launching the KVM**

The Web UI allows remote control of the server through a KVM (Keyboard, Video, Mouse) interface.
### Mounting the operating system image via virtual media

#### Step 1
From the KVM view of the server screen, click on **Browse File** at the top right of the screen. Select the ISO file to be mounted and click on **Open**.

#### Step 2
Once the ISO file is loaded, click on **Start Media** at the top right of the screen. **NOTE:** Once clicked, the Start Media button becomes the **Stop Media** button.

### Accessing the BIOS setup menu
Step_1: From the Power drop-down menu, select Reset Server to access the BIOS menu. Click on OK to confirm the operation.

NOTE: When a reset server command is launched, it may take a few seconds for the BIOS sign on screen to display.

Step_2: When the BIOS sign on screen is displayed, press the specified key to enter the BIOS setup menu.

NOTE: It may take a few seconds for the BIOS sign on screen to display confirmation message "Entering Setup..."

Tip: Some users are pressing DEL/F2 many times and very rapidly, to make sure the server catches the key and enters the BIOS setup menu. Doing this may lead to following message on the KVM display: HID Queue is about to get full. Kindly hold on a second(s). Kontron suggests modifying the Setup Prompt Timeout parameter to give users more time to react. Keeping the focus (single-tasking) on the KVM window is also a good practice to enter the BIOS setup menu each time it is needed.

Parameter Setup Prompt Timeout is found in the Boot tab of the BIOS setup menu. The default value is 1 second, but changing it to a value between 3 and 10 seconds is a good target range.

Step_3: The BIOS sign on screen displays "Entering Setup..."

NOTE: It will take several seconds to display and enter the BIOS setup menu.

Step_4: The BIOS setup menu will be displayed.

Selecting the boot order from boot override

Step_3: From the BIOS setup menu and using the keyboard arrows, select the Save & Exit menu. In the Boot Override section, select UEFI: AMI Virtual CDROM0 1.00 and press Enter. The server will reboot and the media installation process will start.

Completing operating system installation

Step_1: Complete the installation by following the on-screen prompts of the specific OS installed.

> You are now ready to complete operating system installation according to your application requirements.

I nstalling an OS on a server using PXE (Boot from LAN)

Relevant section: CG2400_User_documentation_2-01-2023 www.kontron.com
NOTE: Using Boot from LAN requires a PXE server architecture.

Step_1 Access the BIOS menu. Refer to Accessing the BIOS.

Step_2 Select the Advanced tab and then the Network Stack Configuration submenu.

Step_3 Enable Network Stack.

Step_4 Enable IPv4 PXE Support or IPv6 PXE Support, depending on the application.

Step_5 Reboot the system and access the BIOS setup menu once again.

Step_6 Navigate to the Save & Exit menu and then to the Boot Override section.

Step_7 Choose the PXE option desired.

> You are now ready to complete operating system installation according to your application requirements.
Installing an OS on a server using a USB storage device

Relevant sections:
- Accessing the BIOS
- Platform power management

Preparing the USB storage device

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Create a bootable USB key using the appropriate software. <strong>NOTE:</strong> RUFUS is recommended</td>
</tr>
<tr>
<td>Step_2</td>
<td>Open the USB directory in a remote computer.</td>
</tr>
<tr>
<td>Step_3</td>
<td>Navigate to EFI then BGUID (e.g: E:/EFI/BOOT/).</td>
</tr>
<tr>
<td>Step_4</td>
<td>Open the grub.cfg file with any text editor.</td>
</tr>
</tbody>
</table>
| Step_5 | Edit the file and add the following line on the top to activate the serial installation:  
```
serial --speed=115200
terminal_input serial
terminal_output serial
```

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_6</td>
<td>In the “Test this media &amp; install CentOS 7” entry replace the “quiet” argument with “console=ttyS0,115200n81”.</td>
</tr>
<tr>
<td>Step_7</td>
<td>Save the file and eject the USB key.</td>
</tr>
</tbody>
</table>

Configuring Boot Override

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Connect the USB storage device on the platform.</td>
</tr>
<tr>
<td>Step_2</td>
<td>Power on the platform. Refer to Platform power management.</td>
</tr>
<tr>
<td>Step_3</td>
<td>Access the BIOS setup menu. Refer to Accessing the BIOS.</td>
</tr>
<tr>
<td>Step_4</td>
<td>Navigate to the <strong>Save &amp; Exit</strong> menu and then to the <strong>Boot Override</strong> section.</td>
</tr>
</tbody>
</table>

**NOTE:** The USB storage device should be named like this: "**UEFI: myUSBname, Partition X**".
You are now ready to complete operating system installation according to your application requirements.

Completing operating system installation

Step 1: Complete the installation by following the on-screen prompts of the specific OS installed.

Installing a legacy OS

Installing RHEL/CentOS 7.3 and preparing for AST driver installation

Prerequisites

1. An image of RHEL/CentOS 7.3 (or lower) is available on the installation media.

Enabling the USB keyboard for use in the boot loader in Legacy

Refer to Accessing the BIOS for access instructions.

Step 1: From the BIOS setup menu, select the Advanced menu and go to the USB Configuration section. Enable Port 60/64 Emulation.

Step 2: Press F4 to save and exit.

Installing RHEL/CentOS 7.3 and preparing for AST driver installation

The procedure described below is applicable to versions 7.3 or lower.
**Step 1**  
Boot from the chosen installation media.

**Step 2**  
Edit the Boot Option:  
- (UEFI) Press 'TAB' to edit the installation option in UEFI mode
- (Legacy) Press 'e' to edit the installation option in Legacy mode

**Step 3**  
Add a parameter (**modprobe.blacklist=ast**) in the command line displayed as shown in the image.

**Step 4**  
Start the OS installation by pressing CTRL+X or F10.

**Step 5**  
The server will reboot once the installation is completed. During the boot, press 'TAB' in UEFI mode or 'e' in Legacy mode to edit the item selected.

**Step 6**  
Append the number '2' at the end of the line that begins with linuxefi in UEFI mode or linux16 in Legacy mode.

**NOTE:** This edit is required to boot the system in runlevel 2 for AST driver installation.

**Step 7**  
Press CTRL+X or F10 to boot the OS.

---

**Installing the AST driver**

**Relevant links:**
The driver package can be downloaded from: [https://www.aspeedtech.com/support.php](https://www.aspeedtech.com/support.php)
The AST driver package version used in this procedure is: [http://upload.aspeedtech.com/BIOS/v11003_linux.zip](http://upload.aspeedtech.com/BIOS/v11003_linux.zip)
**Installing the network driver in RHEL/CentOS 7.3**

The i40e network driver must be installed for 10GbE ports.

**Step 1**
Download the latest version of the i40e driver from Sourceforge.
```
```

**Step 2**
Extract the content of the tar file.
```
LocalServer_OSPrompt--# tar xzvf i40e-2.9.21.tar.gz
```

**Step 3**
Install the build tools.
```
LocalServer_OSPrompt--# yum groupinstall 'Development Tools' -y
```

**Step 4**
Change directory.
```
LocalServer_OSPrompt--# cd ./i40e-2.9.21/src
```

**Step 5**
Compile the source.
```
LocalServer_OSPrompt--# make
LocalServer_OSPrompt--# make install
```

**Step 6**
Remove old driver version and load the new one.
```
LocalServer_OSPrompt--# rmmod i40e
LocalServer_OSPrompt--# modprobe i40e
```

**Preventing yum from upgrading the kernel on RHEL/CentOS 7.3**
Step 1: If you have no local vault/repository available and you need to prevent yum from installing/upgrading the latest kernel version.

```bash
#!/bin/bash

mkdir /etc/yum.repos.d/.disabled

mv /etc/yum.repos.d/CentOS-Base.repo /etc/yum.repos.d/.disabled/

mv /etc/yum.repos.d/CentOS-7.3.repo /etc/yum.repos.d/.disabled/

cat <<EOT >> /etc/yum.repos.d/CentOS-7.3.repo

[base-7.3]
name=CentOS-7.3 - Base
baseurl=http://vault.centos.org/centos/7.3.1611/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

[updates-7.3]
name=CentOS-7.3 - Updates
baseurl=http://vault.centos.org/centos/7.3.1611/updates/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

EOT

yum repolist

yum clean all

rm -rf /var/cache/yum

yum update

cat /etc/centos-release
```
Verifying installation

(This article details the tests to perform in order to validate that all of the platform’s devices are properly mounted and recognized by the OS.)

Relevant sections:
PCI mapping
Common software installation

<p>| All the results and commands may vary depending on the operating system and the devices added. |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Step 1 Reboot the OS as recommended, then access the OS command prompt.</td>
</tr>
</tbody>
</table>
| 2    | Step 2 Verify that no error messages or warnings are displayed in `dmesg` using the following commands.  
LocalServer_OSPrompt: ~ `dmesg | grep -i fail`  
LocalServer_OSPrompt: ~ `dmesg | grep -i Error`  
LocalServer_OSPrompt: ~ `dmesg | grep -i Warning`  
LocalServer_OSPrompt: ~ `dmesg | grep -i "Call trace"`  
**NOTE:** If there are any messages or warnings displayed, refer to the operating system’s documentation to fix them. |
| 3    | Step 3 Verify that the DIMMs are detected.  
LocalServer_OSPrompt: ~ `free -h` |
| 4    | Step 4 Verify that all the storage devices are detected.  
LocalServer_OSPrompt: ~ `lsblk` |
| 5    | Step 5 Confirm the data plane network interface controllers are loaded by the **i40e** driver.  
LocalServer_OSPrompt: ~ `dmesg | grep i40e`  
**NOTE:** You should discover two 10GbE NIC. |
| 6    | Step 6 Confirm that all the network interfaces are detected.  
LocalServer_OSPrompt: ~ `ip address`  
**NOTE:** You should see two NIC interfaces. |
| 7    | Step 7 Configure network interface controllers based on your requirements.  
**NOTE:** Interface names may change depending on the OS installed. However, parameters Bus:Device:Function stay the same for the interface regardless of the operating system. |
| 8    | Step 8 Install `ipmitool` and `pciutils` using the package manager, and update the operating system packages. The `ipmitool` version recommended is 1.8.18.  
Example:  
LocalServer_OSPrompt: ~ `yum update`  
LocalServer_OSPrompt: ~ `yum install ipmitool`  
LocalServer_OSPrompt: ~ `yum install pciutils`  
**NOTE:** Updating the packages may take a few minutes. |
| 9    | Step 9 (Optional) If PCIe add-in cards or other hardware components are installed, verify that they are detected.  
LocalServer_OSPrompt: ~ `lspci | grep [KEYWORD]`  
**NOTE:** The keyword is a unique word helping to identify the hardware component. The product PCI mapping may help with this validation. |
| 10   | Step 10 Verify communication between the operating system and the BMC.  
LocalServer_OSPrompt: ~ `ipmitool mc info` |
Platform installation for high availability

(This article details the specific configurations required to enable redundancies.)

Table of contents
Common software installation

(This article provides a list of required and recommended software tools for platform configuration, operation and troubleshooting.)

Table of contents
- Required software tools
- Recommended software tools
- Product specific software tools

Commands may vary depending on the OS and the package manager. Some tools may not be required depending on the functionalities supported for the platform.

Required software tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipmitool</td>
<td>IPMI utility for controlling and monitoring the devices through the IPMI interfaces of the platform.</td>
<td>From a command prompt: LocalServer_OSPrompt# sudo apt install ipmitool</td>
</tr>
<tr>
<td>pciutils</td>
<td>Tool used to manage PCIe cards connected to the platform.</td>
<td>From a command prompt: LocalServer_OSPrompt# sudo apt install pciutils</td>
</tr>
<tr>
<td>hdparm</td>
<td>Command line program for Linux.</td>
<td>From a command prompt: LocalServer_OSPrompt# sudo apt install hdparm</td>
</tr>
<tr>
<td>nvme-cli</td>
<td>Userspace tooling to control NVMe drives.</td>
<td>From a command prompt: LocalServer_OSPrompt# sudo apt install nvme-cli</td>
</tr>
<tr>
<td>snmpd</td>
<td>SNMP daemon.</td>
<td>From a command prompt:</td>
</tr>
<tr>
<td>ksnmpd</td>
<td>Kontron Linux sub-agent.</td>
<td>LocalServer_OSPrompt:~# yum install ./kontron-snmp-agent-1.2.2-1.x86_64.rpm</td>
</tr>
<tr>
<td>snmp</td>
<td>Net-SNMP default package.</td>
<td>From a command prompt: RemoteComputer_OSPrompt:-# yum install snmp</td>
</tr>
<tr>
<td>snmp-mibs-downloader</td>
<td>Tool used to install and manage MIB (Management Information Base) files.</td>
<td>From a command prompt: RemoteComputer_OSPrompt:-# yum install snmp-mibs-downloader</td>
</tr>
</tbody>
</table>

Recommended software tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PuTTY</td>
<td>Serial console tool recommended in the documentation.</td>
</tr>
<tr>
<td>jq</td>
<td>Command-line tool used to parse raw JSON data to make the Redfish API response human-readable.</td>
</tr>
<tr>
<td>cURL</td>
<td>HTTP/FTP client tool used to navigate the Web API using a command-line tool.</td>
</tr>
<tr>
<td>JSON viewer</td>
<td>browser add-on If the Redfish API is used through an Internet browser, a JSON viewer is recommended to make the output human-readable.</td>
</tr>
</tbody>
</table>

Product specific software tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>StorCLI</td>
<td>Configuration and monitoring tool for HW RAID configurations running on LSI Raid-On-Chip controller.</td>
<td>Refer to StorCLI utility.</td>
</tr>
<tr>
<td>net-snmp-utils</td>
<td>SNMP utility package.</td>
<td>From a command prompt: LocalServer_OSPrompt:-# yum install wget unzip net-snmp-utils net-snmp</td>
</tr>
</tbody>
</table>
Configuration of system access methods

(This article provides detailed setup instructions to enable system access for all available methods.)

Table of contents
- General considerations and warnings about network configuration
- Disabling IOL on a LAN channel
  - Disabling IOL on a LAN channel using IPMI
    - Accessing the BMC
    - Disabling IOL on a LAN channel
  - Enabling IOL on a LAN channel
    - Enabling IOL on a LAN channel using IPMI
    - Accessing the BMC
    - Enabling IOL on a LAN channel
    - Configuring Serial over LAN parameters using IPMI
      - Accessing the BMC
      - Viewing and configuring SOL parameters
    - Creating the Redfish root URL
      - Prerequisites
      - Procedure
- Enabling IOL on a LAN channel
  - Enabling IOL on a LAN channel using IPMI
  - Accessing the BMC
- Configuring Serial over LAN parameters using IPMI
  - Accessing the BMC
  - Viewing and configuring SOL parameters
- Creating the Redfish root URL
  - Prerequisites
  - Procedure
- Configuring SNMP
  - Enabling SNMP for a user using the BMC Web UI
    - Installing SNMP on a remote computer
    - Verifying SNMP communication for a user
  - Disabling SNMP access
  - Configuring Kontron linux snmp-agent on the platform
    - Installing the software required
    - Configuring Kontron linux snmp-agent
    - Running the Kontron linux snmp-agent and verifying installation and configuration
  - Disabling SELinux

General considerations and warnings about network configuration

The architecture of the CG2400 platform offers many entry points, including one LAN channel to the BMC. Use caution when configuring network accesses. Your access to the system could be interrupted should you disable the access point you entered through. As an example, if you access BMC LAN channel 1 through IOL to disable IOL on LAN channel 1, your connection will be interrupted and you will essentially have locked yourself out of the BMC as the only LAN channel will now be disabled. To get access to the BMC, you will need to connect to an OS on the server and use KCS to re-enable the LAN access.

Disabling IOL on a LAN channel

The procedures described below must be performed for one interface at a time. If the application requires multiple interfaces, configure them separately. On a LAN channel, IOL can be disabled:
- Using IPMI

NOTE: It is currently not possible to disable a LAN channel using the BIOS setup menu.

Disabling IOL on a LAN channel using IPMI

Accessing the BMC

The BMC can be accessed using two IPMI methods.
- If an OS is installed (BMC IP address known or not), IPMI via KCS can be used. Refer to Accessing a BMC using IPMI (KCS).
- If the IP address of the BMC is known (OS installed or not), IPMI over LAN can be used. Refer to Accessing a BMC using IPMI over LAN (IOL).

The following procedures will be executed using the Accessing a BMC using IPMI (KCS) method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password].

Disabling IOL on a LAN channel

NOTE: LAN channel 1 corresponds to the MNGT NIC port.
Enabling IOL on a LAN channel

The procedures described below must be performed for each interface in a time. If the application requires multiple interfaces, configure them separately.

On a LAN channel, IOL can be enabled:

- Using IPMI

**NOTE:** It is currently not possible to enable a LAN channel using the BIOS setup menu.

Enabling IOL on a LAN channel using IPMI

Accessing the BMC

The BMC can be accessed using two IPMI methods.

- If an OS is installed (BMC IP address known or not), IPMI via KCS can be used. Refer to Accessing a BMC using IPMI (KCS).
- If the IP address of the BMC is known (OS installed or not), IPMI over LAN can be used. Refer to Accessing a BMC using IPMI over LAN (IOL).

The following procedures will be executed using the Accessing a BMC using IPMI (KCS) method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: `-I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password]`.

Enabling IOL on a LAN channel

**NOTE:** LAN channel 1 corresponds to the MNGT NIC port.

### Configuring Serial over LAN parameters using IPMI

Accessing the BMC

The BMC can be accessed using two IPMI methods.

- If an OS is installed (BMC IP address known or not), IPMI via KCS can be used. Refer to Accessing a BMC using IPMI (KCS).
- If the IP address of the BMC is known (OS installed or not), IPMI over LAN can be used. Refer to Accessing a BMC using IPMI over LAN (IOL).

The following procedures will be executed using the Accessing a BMC using IPMI (KCS) method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: `-I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password]`.

Viewing and configuring SOL parameters

### Creating the Redfish root URL

**Prerequisites**

1. The BMC IP address is known (refer to section Configuring/Baseboard management controller – BMC to obtain the BMC MNGMT_IP).
2. An HTTP client tool is installed on the remote computer.
3. A JSON parser command-line tool such as `jq` is installed.

**Relevant sections:**
- Baseboard management controller - BMC
- Common software installation
- Default user names and passwords

**Procedure**
**Step 1** Begin URL with the **https** prefix.

**Step 2** Add the Redfish username and password separated by a colon.

**Step 3** Add `@` to the URL followed by the BMC management IP address.

**Step 4** Add the Redfish API suffix to the URL.

**Step 5** Access the API using an HTTP client and verify that the URL is valid.

```
When forced to change the default password, use the command:
curl -u Administrator:superuser -X PATCH -k -H 'Content-Type: application/json' -H 'If-Match: *' -i
'https://<BMC IP>/redfish/v1/AccountService/Accounts/1' --data '{"Password": "superuser"}'
```

### Configuring SNMP

![Diagram of SNMP and BMC integration]

**Configuring BMC SNMP**

Before configuring SNMP, the default user name and password must be changed as a minimum of 8 characters are required for both. Refer to Configuring BMC user names and passwords using the Web UI.

**NOTE**: The current implementation supports version 3 of the SNMP protocol. For the commands to work, snmpwalk version 5.8 or higher must be installed.

### Enabling SNMP for a user using the BMC Web UI

**Relevant section:**
Configuring and managing users

Refer to Accessing a BMC using the Web UI for access instructions.
Step 1: From the left menu, click on Settings and then User Management.

Step 2: Select the user.

Step 3: Click on the SNMP Access checkbox to give the user an SNMP access.

Step 4: Choose the SNMP Access Level.

   NOTE: Once SNMP access is enabled, the password's minimal security increases, a minimum of 8 characters will be required.

Step 5: Choose the SNMP Authentication Protocol.

Step 6: Choose the SNMP Privacy Protocol.

Step 7: Click on Save.

Installing SNMP on a remote computer

NOTE: The package manager may vary depending on the OS installed.

Step 1: From a remote computer that has access to the management network subnet, install SNMP.

   RemoteComputer:OSPrompt:~# yum install snmp

Step 2: (Optional) To be able to see human-readable MIBs (instead of seeing the OID), also install snmp-mibs-downloader.

   RemoteComputer:OSPrompt:~# yum install snmp-mibs-downloader

Then, to configure net-snmp command-line to use the MIBs, edit /etc/snmp/snmp.conf and comment out the following line:

   Verifying SNMP communication for a user
### Step 1
From a remote computer that has access to the management network subnet, verify that the BMC properly responds to the SNMP request.


### Disabling an SNMP access
Refer to [Accessing a BMC using the Web UI](#) for access instructions.

#### Step 1
Access the BMC Web UI.

#### Step 2
From the left menu, click on **Settings** and then **User Management**.

#### Step 3
Select the user.

#### Step 4
Click on the **SNMP Access** checkbox to disable the SNMP access of the user selected.

#### Step 5
Click on **Save**.

### Configuring Kontron linux snmp-agent on the platform
The Kontron Linux snmp-agent works only with RedHat/CentOS Linux operating systems. The following procedure will be performed under CentOS. Commands may vary depending on the operating system installed.

#### Installing the software required
Refer to [Accessing the operating system of a server](#) for access instructions.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Install the SNMP agent provided by Kontron.</td>
</tr>
<tr>
<td></td>
<td>LocalServer_OSPrompt:~# yum install ./kontron-snmp-agent-1.2.2-1.x86_64.rpm</td>
</tr>
<tr>
<td>Step_2</td>
<td>Install the net-snmp-utils tool.</td>
</tr>
<tr>
<td></td>
<td>LocalServer_OSPrompt:~# yum install net-snmp-utils</td>
</tr>
</tbody>
</table>

### Configuring Kontron Linux snmp-agent
This procedure will completely replace every existing `snmpd` configurations stored in the `snmpd.conf` file. If there are existing `snmpd` configurations, simply add lines from `rwcommunity` to `authtrapenable` at the end the `snmpd.conf` file.
Step 1
Save the current configuration.
LocalServer_OS Prompt:~# mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bak

Step 2
Create file snmpd.conf using the following command:
LocalServer_OS Prompt:~# nano /etc/snmp/snmpd.conf
The nano editor will open. Copy the following text in it:
   rwcommunity public
   rwcommunity public
   # Need to define default master agentx socket if net-snmp >=5.4
   agentXSocket tcp:localhost:1705
   agentXSocket tcp:localhost:1705
   # turn on agentx master agent support
   master agentx
   master agentx
   # Enable TRAPs
   trap2sink localhost public
   authtrapenable 1

Step 3
Set default credentials.
LocalServer_OS Prompt:~# /usr/bin/net-snmp-config --create-snmpv3-user -a [PASSWORD] [USERNAME]
NOTE: The password must have at least 8 characters. Rerunning this command deletes the previous user and replaces it with the new credentials. This method is not recommended to create and manage SNMP users. It only initializes the default credentials and it is strongly recommended to change the default credentials once the SNMP agent is up and running. Refer to Configuring and managing users for more instructions.

Running the Kontron Linux snmp-agent and verifying installation and configuration

Step 1
Run snmpd.
LocalServer_OS Prompt:~# service snmpd start

Step 2
Verify that snmpd is running properly.
LocalServer_OS Prompt:~# service snmpd status

Step 3
(Optional) If there are some issues with one or both services, it might be due to the SELinux security mechanism. Refer to Disabling SELinux for further instructions.

Step 4
Run ksnmpd.
LocalServer_OS Prompt:~# service ksnmpd start

Step 5
Verify that ksnmpd is running properly.
LocalServer_OS Prompt:~# service ksnmpd status

Step 6
Verify that the SNMP agent is working properly locally.
LocalServer_OS Prompt:~# snmpwalk -v 1 -c public -m /usr/local/ksnmpd/mibs/ksnmpd.mib localhost [MIBS]

Step 7
From a remote computer having access to the server network, verify that the server responds to the SNMP request properly.

Disabling SELinux
If there are some issues with one or both services, it might be due to the SELinux (Security-Enhanced Linux) security mechanism of the operating system. Proceed with the following procedure to fix the problem.

NOTE: Instead of entirely disabling the security mechanism, the SELinux configuration could be modified to enable SNMP on 1705 ports, but it is not documented here.
Step 1  Open the SELinux configuration file with any text editor.
LocalServer_OSPrompt:~# nano /etc/selinux/config

Step 2  Modify the file by changing the SELINUX parameter to disabled.

Step 3  Save the changes and reboot the operating system.
LocalServer_OSPrompt:~# reboot

Step 4  Log into the operating system of a server.

Step 5  Verify that the SNMP agent is working properly locally.
LocalServer_OSPrompt:~# snmpwalk -v 1 -c public -m /usr/local/ksnmpd/mibs/ksnmpd.mib localhost [MIBS]

Step 6  From a remote computer having access to the server network, verify that the server responds to the SNMP request properly.
Configuring and managing users

(This article provides detailed configuration instructions for platform users.)

Table of contents
- Configuring BMC users
  - Configuring BMC user names and passwords
  - Adding a BMC user
  - Deleting or disabling a BMC user
  - Configuring privilege level for BMC users
- Configuring SNMP users
  - Configuring SNMP users using BMC SNMP
  - Configuring SNMP users using the Kontron linux snmp-agent
- Managing Redfish users
  - Configuring Redfish user names and passwords
  - Adding a Redfish user
  - Deleting a Redfish user
  - Configuring Redfish privilege level
- Configuring OS users

Administrator rights are required to manage users.

Configuring BMC users

Configuring BMC user names and passwords

For default user names and passwords, refer to Default user names and passwords. BMC user names and passwords can be managed:
- Using the Web UI
- Using IPMI over LAN (OL)
- Using IPMI via KCS

Configuring BMC user names and passwords using the Web UI

Note that the password field is mandatory. Must have a minimum of 8 characters and not use dictionary words. It is recommended, but not mandatory, to enter a strong password consisting of at least one upper case letter, alpha-numeric character, and special character. You must avoid symbols from the extended ASCII table as they are not managed by the IPMI tool.

Refer to Accessing a BMC using the Web UI for access instructions.

Step_1 Click on Settings in the left side menu and click on User Management.

Step_2 Select the user to manage. NOTE: The first and second users are reserved fields, therefore, their usernames can’t be modified.

Step_3 Change field Username if required.

Step_4 Check the Change Password box.
Step 5 Create a new password.

**NOTE:** It is recommended, but not mandatory, to enter a strong password consisting of at least one upper case letter, alpha-numeric character, and special character. **You MUST avoid symbols from the extended ASCII table as they are not managed by the IPMI tool.** Please note that password field is mandatory and should have a minimum of 8 characters when SNMP status is enabled.

Step 6 Confirm the password.

Step 7 Press *Save*.

### Configuring BMC user names and passwords using IPMI over LAN (IOL)

Note that the password field is mandatory, **must have a minimum of 8 characters and not use dictionary words**. It is recommended, but not mandatory, to enter a strong password consisting of at least one upper case letter, alpha-numeric character, and special character. **You must avoid symbols from the extended ASCII table as they are not managed by the IPMI tool.**

Refer to [Accessing a BMC using IPMI over LAN](#) for access instructions.

---

**Step 1** From a remote computer that has access to the management network subnet, print the BMC user list.

```
```

**Step 2** Identify the ID number of the user to be changed.

```
```

**Step 3** Change the user name.

```
RemoteComputer_OSPrompt:~$ ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user set name [IPMI user ID] [new IPMI user name]
```

**NOTE:** The first and second user names of the user list are reserved fields and therefore can’t be modified.

**Step 4** Verify that the user name has been updated correctly by printing the user list.

```
```

**Step 5** Change the password.

```
```

**NOTE:** It is recommended, but not mandatory, to enter a strong password consisting of at least one upper case letter, alpha-numeric character, and special character. **You MUST avoid symbols from the extended ASCII table as they are not managed by the IPMI tool.** Please note that password field is mandatory and should have a minimum of 8 characters when SNMP status is enabled.
Configuring BMC user names and passwords using IPMI via KCS

Note that the password field is mandatory, must have a minimum of 8 characters and not use dictionary words. It is recommended, but not mandatory, to enter a strong password consisting of at least one upper case letter, alpha-numeric character, and special character. You must avoid symbols from the extended ASCII table as they are not managed by the IPMI tool.

Refer to Accessing a BMC using IPMI via KCS for access instructions.

Adding a BMC user

BMC users can be added:
- Using the Web UI
- Using IPMI over LAN (OIL)
- Using IPMI via KCS

Adding a BMC user using the Web UI

Note that the password field is mandatory, must have a minimum of 8 characters and not use dictionary words. It is recommended, but not mandatory, to enter a strong password consisting of at least one upper case letter, alpha-numeric character, and special character. You must avoid symbols from the extended ASCII table as they are not managed by the IPMI tool.

Refer to Accessing a BMC using the Web UI for access instructions.
Adding a BMC user using IPMI over LAN (IOL)

Note that the password field is mandatory, must have a minimum of 8 characters and not use dictionary words. It is recommended, but not mandatory, to enter a strong password consisting of at least one upper case letter, alpha-numeric character, and special character. You must avoid symbols from the extended ASCII table as they are not managed by the IPMI tool.

Refer to Accessing a BMC using IPMI over LAN for access instructions.

Adding a BMC user using IPMI via KCS

Step 1.
From a remote computer that has access to the management network subnet, print the list of users and select the ID of the user to add.

```
```

Step 2.
Create a user name.

```
RemoteServer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user set name [IPMI user ID] [new IPMI user name]
```

NOTE: The first and second user names of the user list are reserved fields and therefore can't be modified.

Step 3.
Create the password.

```
```

Step 4.
Enable channel access and configure privilege level.

```
```

Step 5.
Enable the user.

```
```

Adding a BMC user using IPMI over LAN (IOL)

Step 2.
Click on Settings in the left side menu and click on User Management.

Step 3.
Select the ID of the user to enable.

NOTE: The first and second users are reserved fields and therefore can't be modified.

Step 4.
Configure the user according to the application's requirements.

NOTE: Refer to Configuring privilege level for BMC users using the Web UI for further instructions on privilege level.

Step 5.
Enable the user on the desired channel(s).

Step 6.
Press Save to exit.
Note that the password field is mandatory, must have a minimum of 8 characters and not use dictionary words. It is recommended, but not mandatory, to enter a strong password consisting of at least one upper case letter, alpha-numeric character, and special character. You must avoid symbols from the extended ASCII table as they are not managed by the IPMI tool.

Refer to Accessing a BMC using IPMI (KCS) for access instructions.

**Step 1**
From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, print the list of users and select the ID of the user to add.

```
LocalServer_OSPrompt:~# ipmitool user list [LAN_CHANNEL]
```

**Step 2**
Create a user name.

```
LocalServer_OSPrompt:~# ipmitool user set name [IPMI user ID] [new IPMI user name]
```

**NOTE:** The first and second user names of the user list are reserved fields and therefore can't be modified.

**Step 3**
Create the password.

```
LocalServer_OSPrompt:~# ipmitool user set password [IPMI user ID] [new IPMI password]
```

**Step 4**
Enable channel access and configure privilege level.

```
LocalServer_OSPrompt:~# ipmitool channel setaccess [LAN_CHANNEL] [USER_ID] privilege=[PRIVILEGE_LEVEL]
```

**Step 5**
Enable the user.

```
LocalServer_OSPrompt:~# ipmitool user enable [USER_ID]
```

**Deleting or disabling a BMC user**

BMC users can be:
- Deleted using the Web UI
- Disabled using IPMI over LAN (IOL)
- Disabled using IPMI via KCS

**Deleting a BMC user using the Web UI**

Refer to Accessing a BMC using the Web UI for access instructions.

**Step 1**
Access the BMC Web UI of the server.

**Step 2**
Click on **Settings** in the left side menu and click on **User Management**.

**Step 3**
Select the ID of the user to delete.

**NOTE:** The first and second users are reserved fields and therefore can't be deleted.

**Step 4**
Press on **Delete** to delete the user.

**Disabling a BMC user using IPMI over LAN (IOL)**

Users can't be deleted using ipmitool. However, they can disabled.
Refer to Accessing a BMC using IPMI over LAN for access instructions.

**Step 1**
From a remote computer that has access to the management network subnet, print the list of users and select the ID of the user to disable.

```
```

**Step 2**
Disable the selected user.

```
```

**NOTE:** The first and second user names of the user list are reserved fields and therefore can’t be disabled.

### Disabling a BMC user using IPMI via KCS

Users can’t be deleted using `ipmitool`. However, they can disabled. Refer to Accessing a BMC using IPMI (KCS) for access instructions.

**Step 1**
From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, print the list of users and select the ID of the user to disable.

```
LocalServer.OSPrompt:~# ipmitool user list [LAN_CHANNEL]
```

**Step 2**
Disable the user selected.

```
LocalServer.OSPrompt:~# ipmitool user disable [USER_ID]
```

**NOTE:** The first and second user names of the user list are reserved fields and therefore can’t be disabled.

### Configuring privilege level for BMC users

BMC user privilege level can be configured:
- Using the Web UI
- Using IPMI over LAN (IOL)
- Using IPMI via KCS

### Configuring privilege level for BMC users using the Web UI

Refer to Accessing a BMC using the Web UI for access instructions.

**Step 1**
Access the BMC Web UI of the server.

**Step 2**
Click on Settings in the left side menu and click on User Management.

**Step 3**
Select the ID of the user to manage.

**NOTE:** The first and second users are reserved fields and therefore can’t be overwritten.

**Step 4**
Configure the privilege level for each channel according to the application’s requirements.
Configuring privilege level for BMC users using IPMI over LAN (IOL)

Refer to [Accessing a BMC using IPMI over LAN](#) for access instructions.

**Step 1** From a remote computer that has access to the management network subnet, print the list of users and select the ID of the user to manage.

```
```

**Step 2** List available privilege levels.

```
```

**Step 3** Set privilege level for each channel.

```
```

**NOTE:** The first and second user names of the user list are reserved fields and therefore can’t be modified.

Configuring privilege level for BMC users using IPMI via KCS

Refer to [Accessing a BMC using IPMI (KCS)](#) for access instructions.

**Step 1** From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, print the list of users and select the ID of the user to manage.

```
LocalServer_OSPrompt:~# ipmitool user list [LAN_CHANNEL]
```

**Step 2** List the privilege levels available.

```
LocalServer_OSPrompt:~# ipmitool channel help
```

**Step 3** Set the privilege level for each channel.

```
LocalServer_OSPrompt:~# ipmitool channel setaccess [LAN_CHANNEL] [USER_ID] privilege=[PRIVILEGE_LEVEL]
```

**NOTE:** The first and second user names of the user list are reserved fields and therefore can’t be modified.

Configuring SNMP users

Relevant sections:
- [Accessing a BMC using SNMP BMC](#)
- [Accessing a BMC using the Kontron linux snmp-agent](#)

**Configuring SNMP users using BMC SNMP**

BMC SNMP users are shared with BMC users.
- To configure a user, refer to [Configuring BMC users](#).
- To enable or disable SNMP access, refer to [Configuring SNMP BMC](#).

**Configuring SNMP users using the Kontron linux snmp-agent**

**NOTE:** The current implementation supports version 3 of the SNMP protocol. For the commands to work, snmpwalk version 5.8 or higher must be installed.

**Configuring SNMP passwords**

Refer to [Accessing a BMC using the Kontron linux snmp-agent](#) for access instructions.
### Adding an SNMP user

Refer to [Accessing a BMC using the Kontron Linux snmp-agent](#) for access instructions.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | From a remote computer that has access to the management network subnet, change the password.  
| 2    | To initialise the user created, clone its configurations from another existing user.  

### Deleting an SNMP user

Refer to [Accessing a BMC using the Kontron Linux snmp-agent](#) for access instructions.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | From a remote computer that has access to the management network subnet, delete an SNMP user.  

### Managing Redfish users

#### Configuring Redfish user names and passwords

Refer to [Accessing a BMC using Redfish](#) for access instructions.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Print the user list and select the ID of the user to modify.  
RemoteComputer_OSPrompt:~$ curl -k -s [ROOT_URL]/AccountService/Accounts | jq |
| 2    | Append the previous URL with the ID selected to display the user’s information.  
RemoteComputer_OSPrompt:~$ curl -k -s [ROOT_URL]/AccountService/Accounts/[USER_ID] | jq |
| 3    | Print the ETag of the URL of the desired account.  
RemoteComputer_OSPrompt:~$ curl -k -s [ROOT_URL]/AccountService/Accounts/[USER_ID] -X HEAD -i | grep ETag |
| 4    | Change the user name if necessary.  
RemoteComputer_OSPrompt:~$ curl -k -s [ROOT_URL]/AccountService/Accounts/[USER_ID] -X PATCH -d '{"UserName": "[NEW_USERNAME]"}' -H 'If-Match: [ETAG_VALUE]' -H 'Content-Type: application/json' | jq |
|      | NOTE: Once the user name is modified, it needs to be updated in the ROOT_URL. |
| 5    | Print the ETag of the URL of the desired account.  
RemoteComputer_OSPrompt:~$ curl -k -s [ROOT_URL]/AccountService/Accounts/[USER_ID] -X HEAD -i | grep ETag |
| 6    | Change the password if necessary.  
|      | NOTE: Once the password is modified, it needs to be updated in the ROOT_URL. |
| 7    | Verify that the credentials updated correctly by opening a new session in the Redfish API. |

### Adding a Redfish user

Refer to [Accessing a BMC using Redfish](#) for access instructions.
Step_1  Append the Root URL with the `AccountService/Accounts` suffix.

RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts | jq

Step_2  Create the user and get its ID in the response message.

RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts -X POST -d 
{"Password": [PASSWORD], "RoleID": [ROLE_ID], "UserName": [USER_NAME]} -H "Content-Type: application/json" | jq

NOTE: The ID of the user will be automatically created.

Step_3  Print the ETag of the URL of the account created.

RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts/[[USER_ID]] -X HEAD -i | grep ETag

Step_4  Enable the user.

RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts/[[USER_ID]] -X PATCH -d 
{"Enabled":true} -H "If-Match: [ETAG_VALUE]" -H "Content-type: application/json" | jq

Step_5  Verify that the user was created correctly by connecting to Redfish using its credentials.

Deleting a Redfish user
Refer to Accessing a BMC using Redfish for access instructions.

Step_1  Append the Root URL with the `AccountService/Accounts` suffix and select the user to delete.

RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts | jq

Step_2  Delete the user.

RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts/[[USER_ID]] -X DELETE | jq

Step_3  Verify that the user has been deleted properly.

RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts | jq

Note: Accounts 2 & 3 (HostAutoFW & HostAutoOS) are for internal use only and cannot be deleted, they cannot be used for management purposes.

Configuring Redfish privilege level
Refer to Accessing a BMC using Redfish for access instructions.

Step_1  Append the Root URL with the `AccountService/Accounts` suffix and select the desired user.

RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts | jq

Step_2  Print the ETag of the URL of the desired account.

RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts/[[USER_ID]] -X HEAD -i | grep ETag

Step_3  Set the privilege level.

RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts/[[USER_ID]] -X PATCH -d 
{"RoleID": [ROLE_ID]} -H "If-Match: [ETAG_VALUE]" -H "Content-type: application/json" | jq

Step_4  Verify that the `RoleID` has updated properly.

RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts/[[USER_ID]] | jq

Configuring OS users
Refer to Accessing the operating system of a server for access instructions.

Step_1  Access the OS using the preferred method.
Step_2  Configure the users as recommended by the OS documentation.

NOTE: The procedure to change OS credentials is application-specific and therefore not further documented.
Baseboard management controller - BMC

(This article provides detailed setup instructions for all BMC configuration methods.)

Table of contents
- BMC architecture
- Selecting an access method
- Discovering the platform management IP address
  - Discovering the platform management IP address with DHCP Dynamic DNS update
  - Discovering the platform management IP address using the BIOS
    - Discovering the management IP address in the BIOS using the VGA display port
    - Discovering the management IP address in the BIOS using a serial console (physical connection)
  - Discovering the platform management IP address using DHCP server logs
- Configuring a static IP address
  - Configuring a static IP address using the BIOS setup menu
  - Configuring a static IP address using IPMI
- Configuring a dynamic IP address using DHCP
  - Configuring a dynamic IP address using DHCP server logs
- Accessing the BMC

BMC architecture

One management IP address can be configured for the CG2400 platform (LAN channel 1).

By default, the IP addresses of the network interfaces of the BMC are obtained through the DHCP protocol.

Refer to Product architecture for more information on network connectivity.

Selecting an access method

The BMC can be configured using various access methods depending on specific parameters.
- If the BMC IP address is unknown and there is no OS installed:
  - Use the BIOS setup menu
- If the BMC IP address is unknown and an OS is installed:
  - Use IPMI via KCS
  - Use the BIOS setup menu
- If the BMC IP address is known and an OS is installed:
  - Use IPMI (KCS or IOL)
  - Use the BIOS setup menu

Discovering the platform management IP address

This IP address is the minimum required to access the Web management interface of the platform. It is also used to access the monitoring interface and the KVM/VM (Keyboard Video Mouse/Virtual Media) to install an operating system.

The management IP address can be discovered:
- Using DHCP Dynamic DNS update
- Using the BIOS via the VGA display port or a serial console (physical connection) – device with no OS installed and no known IP address
- Using the DHCP server logs

Discovering the platform management IP address with DHCP Dynamic DNS update

Prerequisites
1 A DHCP server with active Dynamic DNS update feature is available.

2 A remote computer configured with the same DNS information is available.

3 The MAC address of the BMC (LAN channel 1) is known.

**Procedure**

When requesting a DHCP lease, the platform BMC supplies the DHCP server with information to update the DNS system. If the DHCP server is configured for Dynamic DNS update, an entry will be added for a host name that is made up of the "CG2400" prefix and the BMC MAC address.

For example, if we use the MAC address discovered for the MGMT port of the CG2400 (i.e. `00:a0:a5:d2:e9:0a` , refer to section [MAC addresses](#)), the host name would be: `KMB-IXS100_00A0A5D2E90A`.

The following example illustrates the method using DNS auto-registration with a remote computer that has access to the DHCP server network.

**Discovering the platform management IP address using the BIOS**

The platform management IP address can be discovered in the BIOS:

- Using the **VGA display port** (physical connection)
- Using a **serial console** (physical connection)

**Discovering the management IP address in the BIOS using the VGA display port**

**Prerequisites**

1. A physical connection to the VGA display port of the device is required.
2. A mouse and/or keyboard is connected.

**Port location**

Accessing the BMC network configuration menu
Step 1 | From the UEFI/BIOS menu, navigate to tab **Server Mgmt**.

Step 2 | Select **BMC network configuration**.

Step 3 | The **BMC network configuration** menu is displayed.

**NOTE:** When the platform is powered up after being shut off, the UEFI/BIOS may load before the BMC has received its IP address. In this case, the UEFI/BIOS menu information will need to be refreshed by restarting the server and re-entering the UEFI/BIOS.

**Discovering the management IP address in the BIOS using a serial console (physical connection)**

**Prerequisites**

1. A physical connection to the device is required.
   **NOTE:** The serial console port is compatible with Cisco 72-3383-01 cable.

2. A serial console tool is installed on the remote computer.
   - Speed (Baud): 115200
   - Data bits: 8
   - Stop bits: 1
   - Parity: None
   - Flow Control: None
   - Recommended emulation mode: VT100+
   **NOTE:** PuTTY is recommended.

**Port Location**

![Serial Port Location Diagram]
## Access procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From a computer with a physical connection to the serial port, open a serial console tool and start the communication between the console and the port to which the device is connected.</td>
</tr>
</tbody>
</table>
| Step 2 | Perform a server reset (Ctrl-break hot key).  
**NOTE:** If an operating system is installed on the device, the hot key might not work properly. If this is the case, reset the server as recommended for the operating system.  
**NOTE:** When a server reset command is sent, it may take a few seconds for the BIOS sign on screen to display. |
| Step 3 | When the BIOS sign on screen is displayed, press the specified key to enter the BIOS setup menu.  
**NOTE:** It may take a few seconds for the BIOS sign on screen to display confirmation message "Entering Setup...". |
| Step 4 | The BIOS sign on screen displays "Entering Setup...".  
**NOTE:** It will take several seconds to display and enter the BIOS setup menu. |
| Step 5 | The BIOS setup menu is displayed. |

### Accessing the BMC network configuration menu
Discovering the platform management IP address using DHCP server logs

**Prerequisites**

1. Access to the DHCP server logs is required.
2. The MAC address of the BMC (LAN channel 1) is known.

**Relevant section:**

MAC addresses

**Procedure**

DHCP IP assignment is specific to the network infrastructure to which the platform is being integrated. The assistance of the network administrator may therefore be necessary to obtain the IP address of the device (e.g., BMC, switch NOS, server OS).

If you have the MAC address of the device, you can search the DHCP server logs to determine the IP address assigned to this specific device. Refer to section MAC addresses to determine those specific to a platform.

Various DHCP server services may offer other search capabilities. Please consult the network administrator or the DHCP server documentation. The following example illustrates a command prompt method for use with a Linux-based DHCP server. This may need to be adjusted to reflect a specific DHCP infrastructure (this action can generally also be done through a DHCP server Web interface).

```
DHCP_Server:~$ cat /var/log/messages | grep -i 00:a0:a5:d2:e9:0a
Mar  1 13:44:15 DHCP_Server dhcpd: DHCPDISCOVER from 00:a0:a5:d2:e9:0a via ens192
Mar  1 13:44:16 DHCP_Server dhcpd: DHCPOFFER on 172.16.211.126 to 00:a0:a5:d2:e9:0a via ens192
Mar  1 13:44:16 DHCP_Server dhcpd: DHCPREQUEST for 172.16.211.126 (172.16.0.10) from 00:a0:a5:d2:e9:0a via ens192
Mar  1 13:44:16 DHCP_Server dhcpd: DHCPACK on 172.16.211.126 to 00:a0:a5:d2:e9:0a via ens192
```

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:a0:a5:d2:e9:0a</td>
<td>MAC address discovered for the device (refer to section MAC addresses )</td>
</tr>
<tr>
<td>00:a0:a5:d2:e9:0a</td>
<td>Linux DHCP server network interface name</td>
</tr>
<tr>
<td>172.16.211.126</td>
<td>IP address assigned to the device by the DHCP server</td>
</tr>
<tr>
<td>172.16.0.10</td>
<td>Linux DHCP server IP address</td>
</tr>
</tbody>
</table>
Configuring a static IP address

The procedures described below must be performed for one interface at a time. If the application requires multiple interfaces, configure them separately.

A static IP address can be configured:
- Using the BIOS setup menu
- Using IPMI

Configuring a static IP address using the BIOS setup menu

Accessing the BIOS setup menu

The BIOS setup menu can be accessed using various methods:
- If there is no OS installed and no known IP address, it is mandatory to use a serial console. Refer to Accessing the BIOS using a serial console (physical connection).
- If the IP address of the BMC is known, any BIOS access methods will work. Refer to Accessing the BIOS to choose an access method.

Accessing the BMC network configuration menu

Step_1  From the UEFI/BIOS menu, navigate to tab Server Mgmt.

Step_2  Select BMC network configuration.

Step_3  The BMC network configuration menu is displayed.

NOTE: When the platform is powered up after being shut off, the UEFI/BIOS may load before the BMC has received its IP address. In this case, the UEFI/BIOS menu information will need to be refreshed by restarting the server and re-entering the UEFI/BIOS.

Configuring a static IP address

Step_1  From the BMC network configuration menu, select the Configuration Address source option for the LAN interface to configure (LAN channel 1 in this example).

Step_2  Select Static.
**Configuring a static IP address using IPMI**

**Accessing the BMC**

The BMC can be accessed using two IPMI methods.

- If an OS is installed (BMC IP address known or not), IPMI via KCS can be used. Refer to [Accessing a BMC using IPMI (KCS)](#).
- If the IP address of the BMC is known (OS installed or not), IPMI over LAN can be used. Refer to [Accessing a BMC using IPMI over LAN (IOL)](#).

The following procedures will be executed using the IPMI (KCS) method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: `-I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password]`.

**Configuring a static IP address**

**Step 1** Set the IP source to static.

```
LocalServer_OSPrompt:~# ipmitool lan set [LAN_CHANNEL] ipsrc static
```

**Step 2** Set the IP address to be used.

```
LocalServer_OSPrompt:~# ipmitool lan set [LAN_CHANNEL] ipaddr [NEW_IP]
```

**NOTE:** This is the BMC IP address (`BMC MNGMT_IP`).

**NOTE:** It can take several seconds for an IP address to be set.

**Step 3** Set the subnet mask.

```
LocalServer_OSPrompt:~# ipmitool lan set [LAN_CHANNEL] netmask [NEW_MASK]
```

**NOTE:** It can take several seconds for a subnet mask to be set.

**Step 4** Set the default gateway IP address.

```
LocalServer_OSPrompt:~# ipmitool lan set [LAN_CHANNEL] defgw ipaddr [ROUTER_IP]
```

**NOTE:** It can take several seconds for a default gateway IP address to be set.

**Step 5** Set the default gateway MAC address.

```
LocalServer_OSPrompt:~# ipmitool lan set [LAN_CHANNEL] defgw macaddress [ROUTER_MAC]
```

**Step 6** Verify that the configuration has changed.

```
LocalServer_OSPrompt:~# ipmitool lan print [LAN_CHANNEL]
```

**Configuring a dynamic IP address using DHCP**

---

CG2400_User_documentation_2-01-2023

www.kontron.com
The procedures described below must be performed for one interface at a time. If the application requires multiple interfaces, configure them separately.

A dynamic IP address can be configured:
- Using the BIOS setup menu
- Using IPMI

**Configuring a dynamic IP address using the BIOS setup menu**

**Accessing the BIOS setup menu**

The BIOS setup menu can be accessed using various methods:
- If there is no OS installed and no known IP address, it is mandatory to use a serial console. Refer to [Accessing the BIOS using a serial console (physical connection)].
- If the IP address of the BMC is known, any BIOS access methods will work. Refer to [Accessing the BIOS] to choose an access method.

**Accessing the BMC network configuration menu**

**Step_1** From the UEFI/BIOS menu, navigate to tab **Server Mgmt**.

**Step_2** Select **BMC network configuration**.

**Step_3** The **BMC network configuration** menu is displayed. **NOTE:** When the platform is powered up after being shut off, the UEFI/BIOS may load before the BMC has received its IP address. In this case, the UEFI/BIOS menu information will need to be refreshed by restarting the server and re-entering the UEFI/BIOS.

**Configuring a dynamic IP address using DHCP**
**Step 1**  From the BMC network configuration menu, select the Configuration Address source option of the LAN interface to configure (LAN channel 1 in this example).

**Step 2**  Select DynamicBmcDhcp.

**Step 3**  Navigate to Save & Exit.

**Step 4**  Select Save Changes and Exit, this will perform a server reset.

**Step 5**  When the BIOS sign on screen is displayed, press the specified key to enter the BIOS setup menu. Then, access the Server Mgmt menu and select BMC network configuration. The address displayed is your management IP address (BMC MNGMT_IP).

### Configuring a dynamic IP address using IPMI

#### Accessing the BMC

The BMC can be accessed using two IPMI methods.
- If an OS is installed (BMC IP address known or not), IPMI via KCS can be used. Refer to Accessing a BMC using IPMI (KCS).
- If the IP address of the BMC is known (OS installed or not), IPMI over LAN can be used. Refer to Accessing a BMC using IPMI over LAN (IOL).

The following procedures will be executed using the Accessing a BMC using IPMI (KCS) method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: `-I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password]`.

#### Configuring a dynamic IP address

**Step 1**  Set the IP source to DHCP.

```bash
LocalServer_OSPrompt:~# ipmitool lan set [LAN_CHANNEL] ipsrc dhcp
```

**NOTE:** Depending on the existing infrastructure, it may take several seconds to gather an IP from the DHCP server.

**Step 2**  Verify that the configuration has changed.

```bash
LocalServer_OSPrompt:~# ipmitool lan print [LAN_CHANNEL]
```

**NOTE:** This is the BMC IP address (BMC MNGMT_IP).
Configuring the network time protocol - NTP

This article describes how to configure the NTP using different methods.

Table of contents
- Configuring the NTP using the Web UI
  - Prerequisites
  - Procedure
- Configuring the NTP using IPMI (IOL or KCS)
  - Prerequisites (IOL)
  - Prerequisites (KCS)
  - Getting the BMC time and date
  - Setting the BMC time and date
  - Confirming configuration
  - Decoding NTP raw configuration data

The network time protocol (NTP) can be configured:
- Using the Web UI
- Using IPMI (IOL or KCS)

NOTE: The system time is not set after powering up the unit. Resetting the server is sufficient to set it automatically once the BMC NTP server is configured.

Configuring the NTP using the Web UI

Prerequisites

1. The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).
2. The remote computer has access to the management network subnet.

Relevant sections:
- Baseboard management controller - BMC
- Accessing a BMC

Procedure

Step_1  From a remote computer that has access to the management network subnet, access the BMC Web UI using the BMC IP address.

Step_2  Click on Settings from the left side menu. Then, click on Date & Time.

Step_3  In the Primary NTP Server field, enter the desired NTP server address.

Step_4  Verify that the time and date displayed matches the local time and date.

NOTE: It may take several seconds or minutes before the BMC synchronizes the time with the NTP server.
Configuring the NTP using IPMI (IOL or KCS)

Prerequisites (IOL)

1. The BMC IP address is known.
2. The remote computer has access to the management network subnet.
3. A community version of ipmitool is installed on a remote computer to enable remote monitoring—it is recommended to use ipmitool version 1.8.18.

Relevant sections:
Baseboard management controller - BMC
Accessing the operating system of a server

Prerequisites (KCS)

1. An OS is installed.
2. The remote computer has access to the server OS (SSH/RDP/platform serial port).
3. A community version of ipmitool is installed on the local server to enable local monitoring—it is recommended to use ipmitool version 1.8.18.

Relevant section:
Accessing the operating system of a server

Getting the BMC time and date

Step_1 Access the operating system using an IPMI method (IOL or KCS).
Step_2 Verify that the local time and date match the server’s time and date.

LocalServer_OSPrompt:~# ipmitool sel time get

Setting the BMC time and date

Relevant section:
Decoding NTP raw configuration data

Step_1 Enable the NTP service.
LocalServer_OSPrompt:~# ipmitool raw 0x32 0xA8 3 1
Step_2 Get the NTP configuration data to recover the current NTP server address.
LocalServer_OSPrompt:~# ipmitool raw 0x32 0xA7

Step_3 Decode the raw data table. Refer to Decoding NTP raw configuration data.

Decoded data for this example:
NTP Status: 0x01 — Enabled
Primary ntp: 70 6f 6f 6c 2e 6e 74 70 2e 6f 72 67 — "pool.ntp.org"
Secondary ntp: 74 69 6d 65 2e 6e 69 73 74 2e 67 6f 76 — "time.nist.gov"

Step_4 Set both NTP addresses with the following parameters:
- NTP_ADDRESS can either be 0x01 (for primary) or 0x02 (for secondary).
- DATA must be 128-byte long and needs to be padded with 0 until address length is 128 bytes.
- DATA format can either be in decimal or hexadecimal. If hexadecimal is used, every number requires the 0x prefix.

LocalServer_OSPrompt:~# ipmitool raw 0x32 0xA8 0x01 49 48 46 49 46 50 4B 46 49 48 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

Step_5 Restart NTP service in order to save the NTP configuration.
LocalServer_OSPrompt:~# ipmitool -H [BMC MNGMT_IP] -U [USER_NAME] -P [PASSWORD] -I lanplus raw 0x32 0xA8 4

Confirming configuration
Step_1  Get the BMC time and date.

LocalServer_OSPrompt:~# ipmitool sel time get

Step_2  Verify that the BMC time and date match with the local time and date.

NOTE: It may take several seconds or minutes before the BMC synchronizes time with the NTP server.

Decoding NTP raw configuration data

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Description</th>
<th>Possible values</th>
</tr>
</thead>
</table>
| 0     | Status of NTP                | • 0x00: Disabled
       |                               | • 0x01: Enabled
       |                               | • 0x02: Failure status          |
| 1:128 | Primary Server IP, MSB First | Hexadecimal values (0.255)       |
| 139:256 | Secondary Server IP, MSB First | Hexadecimal values (0.255)       |

This script can be used to convert string data to raw data and to pad the raw data with the required number of 0.

```
address_conversion

strings=$(printf "10.1.20.10" | od -t d1 | head -n1 | sed 's/00000000 //g' | sed 's/ //g')
length=$(echo $strings | wc -w)
string_padded="$strings"
for i in $(seq 0 $((127 - length))); do
   string_padded="$string_padded 0"
done
echo $string_padded
```

To convert ascii and hexadecimal data, you can use this online tool [https://www.rapidtables.com/convert/number/ascii-to-hex.html](https://www.rapidtables.com/convert/number/ascii-to-hex.html) and pad to 128 bytes with 0.
Basic BIOS option configuration

(This section details the most common configuration options related to the BIOS.)

Table of contents
- Changing the boot order
- Overriding the boot order
- Overriding the boot order using IPMI
- Enter the BIOS menu on the next boot using IPMI
- Enabling Retry Boot Order when CSM is disabled
- Configuring Secure Erase
- Enabling Secure Boot
- Configuring the TPM

Changing the boot order

Refer to Accessing the BIOS for access instructions.

Step_1  From the BIOS setup menu, use the keyboard arrows to select the Boot menu. Configure the boot order as desired.

Step_2  Using the keyboard arrows, select the Save & Exit menu, go to Save Changes and Exit and press Enter to confirm and save the new boot order.

Overriding the boot order

Refer to Accessing the BIOS for access instructions.

Step_1  From the BIOS setup menu, use the keyboard arrows to select the Save & Exit menu. In the Boot Override section, select the desired option and press Enter. The server will boot from a particular device.

NOTE: This selection will only affect the current boot.

Overriding the boot order using IPMI

The following procedures will be executed using the Accessing a BMC using IPMI via KCS method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password].

Step_1  Display the list of boot devices and select the desired option.
LocalServer_OSPrompt:~# ipmitool chassis bootdev help

NOTE: Not all devices are supported by ipmitool.

Step_2  Override the boot order.
LocalServer_OSPrompt:~# ipmitool chassis bootdev [DEVICE]
Enter the BIOS menu on the next boot using IPMI

The following procedures will be executed using the Accessing a BMC using IPMI on KCS method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password].

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Execute the following command to enter the BIOS menu automatically on the next boot.</td>
</tr>
<tr>
<td></td>
<td>LocalServer_0SPrompt:~# ipmitool chassis bootdev bios</td>
</tr>
</tbody>
</table>

Enabling Retry Boot Order when CSM is disabled

Refer to Accessing the BIOS for access instructions.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>To be able to retry the boot sequence indefinitely the EFI shell must be disabled in the list of boot options.</td>
</tr>
</tbody>
</table>

Configuring Secure Erase

Refer to Accessing the BIOS for access instructions.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>From the BIOS setup menu, select the Security menu and disable the HDD Security Freeze Lock option.</td>
</tr>
</tbody>
</table>

| Step_2 | Using the keyboard arrows, select the Save & Exit menu, go to Save Changes and Exit and press Enter to confirm and save the new boot order. |

<table>
<thead>
<tr>
<th>Step_3</th>
<th>Use the following application note to Secure Erase the applicable drive.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Erase</td>
<td></td>
</tr>
</tbody>
</table>

Enabling Secure Boot

Refer to Accessing the BIOS for access instructions.
Step 1  Access the Secure Boot submenu from the Security tab.

Step 2  Select the Secure Boot option and change it to Enabled.

Step 3  Use the following application notes to generate and configure secure boot keys.

- Generating custom secure boot keys
- Provisioning custom secure boot keys

Step 4  Using the keyboard arrows, select the Save & Exit menu, go to Save Changes and Exit and press Enter to confirm.

Configuring the TPM

Refer to Accessing the BIOS for access instructions.
Step_1  Select the Advanced menu, go to Trusted Computing and then Security Device Support. Verify that it is set to Enable. Possible values: [Enable / Disable]

   NOTE: TPM has to be inserted to see the menu.

Step_2  Select the Advanced menu, go to Trusted Computing and then TPM2.0 UEFI Spec Version. Select the applicable spec. Possible values: [TCG_1_2 / TCG_2]

   NOTE: TPM has to be inserted to see the menu.

Step_3  Select the Advanced menu, go to Trusted Computing and then Device Select. Select the applicable device. Possible values: [TPM 1.2 / TPM 2.0 / Auto]

   NOTE: TPM has to be inserted to see the menu.

Step_4  Using the keyboard arrows, select the Save & Exit menu, go to Save Changes and Exit and press Enter to confirm.
Customizing platform data

This article describes how to customize field replaceable unit data.

Table of contents
- Customizing platform FRU data using IPMI
- FRU customizing commands
  - Customizing product related informations
  - Customizing chassis related informations
  - Customizing logos

Customizing platform FRU data using IPMI

The BMC can be accessed using two IPMI methods.
- If an OS is installed (BMC IP address known or not), IPMI via KCS can be used. Refer to Accessing a BMC using IPMI (KCS).
- If the IP address of the BMC is known (OS installed or not), IPMI over LAN can be used. Refer to Accessing a BMC using IPMI over LAN (IOL).

The following procedures will be executed using the Accessing a BMC using IPMI (KCS) method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password].

---

For commands performed to customize FRU data, the version of ipmitool required is 1.8.13. The latest version of ipmitool recommended (1.8.18) will not yield the desired results.

Step 1
Display current FRU information.
LocalServer_OSPrompt:~# ipmitool fru print

```
Chassis Type : Main Server Classic
Chassis Part Number : C0040-00
Chassis Serial : C0040-004
Chassis Error : C0000
Board Mfg Date : Mon Aug 12 15:55:00 2019
Board Mfg : Kontron Canada Inc.
Board Product : KX3-30210
Board Serial : 910621702
Board Part Number : I062-050
Board Vendor : Kontron Canada Inc.
Product Manufacturer : Kontron Canada Inc.
Product Name : C0040-00
Product Part Number : C0040-00
Product Version : ........
Product Serial : C0040-004
Product Asset Tag : ........
```

Step 2
Use the following IPMI command to customize FRU data.
LocalServer_OSPrompt:~# ipmitool fru edit [FRU_ID] field [FRU_COMMAND] [VALUE]

NOTE: Refer to FRU commands for available commands.

```
Chassis Type : Main Server Classic
Chassis Part Number : C0040-00
Chassis Serial : C0040-004
Chassis Error : C0000
Board Mfg Date : Mon Aug 12 15:55:00 2019
Board Mfg : Kontron Canada Inc.
Board Product : KX3-30210
Board Serial : 910621702
Board Part Number : I062-050
Board Vendor : Kontron Canada Inc.
Product Manufacturer : Kontron Canada Inc.
Product Name : C0040-00
Product Part Number : C0040-00
Product Version : ........
Product Serial : C0040-004
Product Asset Tag : ........
```

Step 3
Confirm changes were properly applied.
LocalServer_OSPrompt:~# ipmitool fru print

```
Chassis Type : Main Server Classic
Chassis Part Number : C0040-00
Chassis Serial : C0040-004
Chassis Error : C0000
Board Mfg Date : Mon Aug 12 15:55:00 2019
Board Mfg : Kontron Canada Inc.
Board Product : KX3-30210
Board Serial : 910621702
Board Part Number : I062-050
Board Vendor : Kontron Canada Inc.
Product Manufacturer : Kontron Canada Inc.
Product Name : C0040-00
Product Part Number : C0040-00
Product Version : ........
Product Serial : C0040-004
Product Asset Tag : ........
```

FRU customizing commands

For commands performed to customize FRU data, the version of ipmitool required is 1.8.13. The latest version of ipmitool recommended (1.8.18) will not yield the desired results.

Customizing product related informations
### Customizing chassis related informations

<table>
<thead>
<tr>
<th>Command</th>
<th>FRU data</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>c 0</td>
<td>Chassis Part Number</td>
<td>LocalServer_OSPrompt:~# ipmitool fru edit 0 field c 0 [VALUE]</td>
</tr>
<tr>
<td>c 1</td>
<td>Chassis Serial Number</td>
<td></td>
</tr>
</tbody>
</table>

### Customizing logos

It is possible to get firmware customized with your company logo, under some specific conditions. Contact your Technical Support or Sales representative to get more information.
Network infrastructure integration

(This article provides all relevant information required to establish a successful network integration of the platform.)

Table of contents

- Configuring VLANs
  - Enabling the UEFI Network Stack and configuring CSM
  - Creating VLANs
  - Removing VLANs

Configuring VLANs

The BIOS setup menu provides menus to create/configure/remove VLANs on each of the two native 10GbE ports. However, the BIOS setup menus to configure VLANs are available only when the UEFI network services are active (not available when the CSM (Compatibility Support Module) legacy support is activated).

If UEFI network services are not active, they must be enabled before VLANs can be configured.

Enabling the UEFI Network Stack and configuring CSM

Refer to Accessing the BIOS for access instructions.

Step 1

From the BIOS setup menu, select the Advanced menu and go to the Network Stack Configuration section.

Enable Network Stack.

Step 2

From the Advanced menu, go to the Compatibility Support Module Configuration section.

If CSM Support is set to Disabled, go to Step 4.

If CSM Support is set to Enabled, go to Step 3.

Step 3

Under Option ROM execution, set Network to UEFI, if not already done.

NOTE: The other Option ROM execution options (Storage, Video, Other PCI devices) should also be set to UEFI (mixing Legacy and UEFI option ROMs may cause OS boot issues).

Step 4

Press F4 to save and exit.

Creating VLANs

Refer to Accessing the BIOS for access instructions.
Step 1: From the BIOS setup menu, select the **Advanced** menu and go to a VLAN Configuration (MAC:xxxxxxxxxxxx) section.

**NOTE:** The MAC address will be the one of the X722 10GbE port for which you want to configure VLANs.

Step 2: Create a new VLAN as needed by setting its VLAN ID and Priority:
- **VLAN ID:** value between 0 and 4094
- **Priority:** value between 0 and 7

The example in the image shows a VLAN ID of 1001, with 802.1Q Priority 2.

Step 3: Select **Add VLAN** to create the VLAN.

**NOTE:** You can also update an existing VLAN ID using steps 2 and 3.

Step 4: Add other VLANs as required, using steps 2 and 3.

Example: VLAN ID 2002, with 802.1Q Priority 4.

**NOTES:**
- The VLANs shown below the **Configured VLAN List** are active, whether they have the setting **Enabled** or **Disabled**. In this example, VLAN ID 1001 and 2002 are active (even if disabled).
- The settings (enabled or disabled) of the VLANs in the list are only used when removing VLANs.

Step 5: Repeat steps 1 to 4 to set VLANs in the other X722 10GbE port, as needed.

Step 6: Press F4 to save and exit.

**Removing VLANs**

Refer to Accessing the BIOS for access instructions.
Step_1  From the BIOS setup menu, select the **Advanced** menu and go to a VLAN Configuration (MAC:xxxxxxxxxxxxxx) section. Select **Enter Configuration Menu**.

**NOTE:** The MAC address will be the one of the X722 10GbE port for which you want to remove VLANs.

Step_2  Set the status of the VLAN or VLANs to remove to **Enabled**. Once all the VLANs to remove are selected, select **Remove VLAN**.

In the example in the image, VLAN ID 2002 will be removed and VLAN ID 1001 will be kept.

Step_3  Repeat steps 1 and 2 to remove VLANs in the other X722 10GbE port, as needed.

Step_4  Press F4 to save and exit.
High availability

(This article details platform integration use cases to achieve high availability.)

Table of contents
Configuring the BMC when in non-redundant PSU configuration

The default configuration of the CG2400 platform includes two redundant power supply units (PSU). If the final system configuration uses only one PSU, the BMC must be reconfigured.

<table>
<thead>
<tr>
<th>NOTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>The platform will not be fully healthy if the BMC is not reconfigured based on the actual number of PSUs used. The platform will return unhealthy indications because of a missing component (PSU) expected from the factory default. These indications could include:</td>
</tr>
<tr>
<td>System fans staying at maximum speed at all time</td>
</tr>
<tr>
<td>Front panel LED indicating alarm conditions (System Status LED)</td>
</tr>
<tr>
<td>Unhealthy events in the System Event Log</td>
</tr>
</tbody>
</table>

Relevant sections:
Components installation and assembly
Getting started - Application installation and performance benchmarking
The BMC can be accessed using two IPMI methods.
- If an OS is installed (IP address known or not), IPMI via KCS can be used. Refer to Accessing a BMC using IPMI (KCS).
- If the IP address of the BMC is known (OS installed or not), IPMI over LAN can be used. Refer to Accessing a BMC using IPMI over LAN (IOL).

The following procedures will be executed using the Accessing a BMC using IPMI (KCS) method, but some configurations can also be performed using IOL. To use IOL, add the IOL parameters to the command: `-I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password]`.

<table>
<thead>
<tr>
<th>Step_1</th>
<th>Write the redundancy count. When using only one PSU, the value will be 1.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~#</td>
<td><code>ipmitool -H 192.168.1.10 -I lanplus -U admin -P admin raw 0x3c 0x02 0x00 0x01 0x00 0x01</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_2</th>
<th>Read the redundancy count to confirm the change. The answer should be 1.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~#</td>
<td><code>ipmitool -H 192.168.1.10 -I lanplus -U admin -P admin raw 0x3c 0x02 0x00 0x00 0x00 0x00</code></td>
</tr>
</tbody>
</table>
Default user names and passwords

(This article lists all default user names and passwords per component.)

Table of contents
- Operating system
- BIOS
- Management interface (BMC)

Operating system

<table>
<thead>
<tr>
<th>User interface</th>
<th>User name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Application specific</td>
<td>Application specific</td>
</tr>
<tr>
<td>Kontron linux snmp-agent</td>
<td>Application specific</td>
<td>Refer to Configuration of system access methods</td>
</tr>
</tbody>
</table>

BIOS

No password is set by default.

Management interface (BMC)

The BMC can be accessed using SNMP. However, before configuring SNMP, the default user name and password must be changed as a minimum of 8 characters are required for both. Refer to Configuring BMC user names and passwords using the Web UI.

The CG2400 platform includes one BMC.

<table>
<thead>
<tr>
<th>User interface</th>
<th>User name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web UI</td>
<td>admin</td>
<td>admin</td>
</tr>
<tr>
<td>IPMI</td>
<td>admin</td>
<td>admin</td>
</tr>
<tr>
<td>Redfish</td>
<td>Administrator</td>
<td>superuser</td>
</tr>
<tr>
<td>SNMP</td>
<td>New B character minimum user name configured after first login</td>
<td>New B character minimum password configured after first login</td>
</tr>
</tbody>
</table>

NOTE: For security reasons it is important to change the default user names and passwords as soon as possible. Refer to Configuring and managing users.
Accessing platform components
Accessing the operating system of a server

Table of contents
- Accessing an OS using the KVM
  - Prerequisites
  - Browser considerations
  - Access procedure
    - Accessing the BMC of the server for which you want to access the OS
      -Launching the KVM
  - Accessing an OS using display port (VGA)
    - Prerequisites
    - Access procedure
  - Accessing an OS using SSH, RDP or customer application protocols
    - Prerequisites
    - Access procedure
  - Accessing an OS using Serial over LAN (SOL)
    - Prerequisites
    - Access procedure
  - Accessing an OS using a serial console (physical connection)
    - Prerequisites
    - Port location
    - Access procedure

An operating system can be accessed through various methods:
- Using the KVM (Keyboard Video Mouse)
- Using the display port (VGA) – this is the recommended path for first time out-of-the-box system configuration
- Using SSH/RDP/Customer application protocols
- Using Serial over LAN (SOL)
- Using a serial console (physical connection)
Refer to Description of system access methods for more information on the various paths.

Accessing an OS using the KVM

Prerequisites

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An OS is installed.</td>
</tr>
<tr>
<td>2</td>
<td>The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).</td>
</tr>
<tr>
<td>3</td>
<td>The remote computer has access to the management network subnet.</td>
</tr>
</tbody>
</table>

Relevant section:
Baseboard management controller - BMC

Browser considerations

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML5</td>
<td>To connect to the Web UI, a Web browser supporting HTML5 is required.</td>
</tr>
<tr>
<td>HTTPS self-signed certificate</td>
<td>Upon connection to the Web UI, it is mandatory to accept the HTTPS self-signed certificate. For further information about accepting HTTPS self-signed certificates, please refer to your Web browser’s documentation.</td>
</tr>
<tr>
<td>File download permission</td>
<td>File download from the site needs to be permitted. For further information about file download permission, please refer to your Web browser’s documentation.</td>
</tr>
<tr>
<td>Cookies</td>
<td>Cookies must be enabled in order to access the website. For further information about enabling cookies, please refer to your Web browser’s documentation.</td>
</tr>
</tbody>
</table>

NOTE: The procedure may vary depending on the browser used. Examples provided use Firefox.

Access procedure

Accessing the BMC of the server for which you want to access the OS

To obtain the list of default user names and passwords, refer to Default user names and passwords.
Step_1  From a remote computer that has access to the management network, open a browser window and enter the IP address discovered for the BMC.

   NOTE: The HTTPS prefix is mandatory.

   https://[BMC MNGMT_IP]

Step_2  Click on Advanced in order to start the HTTPS self-signed certificate acceptance process. Information on the error message will be displayed.

Step_3  Click on Add Exception... The Add Security Exception pop-up window will be displayed. Click on Confirm Security Exception to allow the browser to access the management Web UI of this interface.

Step_4  Log in to the BMC Web UI using the appropriate credentials.

   NOTE: Default Web UI user name and password is admin/admin.

Step_5  You now have access to the management Web UI of the BMC. You can use the interface.

Launching the KVM
Step_1 From the left menu, click on Remote Control.

Step_2 From the Remote Control menu, click on the Launch KVM button.

Step_3 A new browser window opens and displays the server screen.

NOTE: If an OS is installed, the image displayed might be that of the OS.

If the OS is not displayed, perform a server reset as described in Sending a power command using the Web UI. Then relaunch the KVM.

Accessing an OS using the display port (VGA)

Prerequisites

1 An OS is installed.
2 A physical connection to the VGA display port of the device is required.
3 A mouse and/or keyboard is connected.

Port location

Access procedure

Step_1 Connect the VGA cable to the monitor and the platform.
Step_2 The OS screen should be displayed on the monitor.

Accessing an OS using SSH, RDP or customer application protocols

Prerequisites

1 An OS is installed.
2 The OS IP address is known.
3 The remote computer has access to the OS subnet.

Access procedure

Step_1 Using the OS IP address, proceed with your preferred remote access method.
**Accessing an OS using Serial over LAN (SOL)**

**Prerequisites**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An OS is installed.</td>
</tr>
<tr>
<td>2</td>
<td>The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).</td>
</tr>
<tr>
<td>3</td>
<td>The remote computer has access to the management network subnet.</td>
</tr>
<tr>
<td>4</td>
<td>A community version of ipmitool is installed on a remote computer to enable remote monitoring—it is recommended to use ipmitool version 1.8.18.</td>
</tr>
</tbody>
</table>

**Relevant sections:**
- Baseboard management controller - BMC
- Common software installation

**Access procedure**

To obtain the list of default user names and passwords, refer to [Default user names and passwords](#).

**Step_1**  
From a remote computer that has access to the management network subnet, open the OS command prompt and deactivate any previous SOL session.

```
```

**Step_2**  
Activate an SOL session.

```
```

**Step_3**  
The OS start screen will be displayed.  
**NOTE:** If the OS is not displayed, perform a server reset. Refer to [Platform power management](#).

**Accessing an OS using a serial console (physical connection)**

**Prerequisites**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An OS is installed.</td>
</tr>
</tbody>
</table>
| 2 | A physical connection to the device is required.  
**NOTE:** The serial console port is compatible with Cisco 72-3383-01 cable. |
| 3 | A serial console tool is installed on the remote computer.  
- Speed (Baud): 115200  
- Data bits: 8  
- Stop bits: 1  
- Parity: None  
- Flow Control: None  
- Recommended emulation mode: VT100+  
**NOTE:** PuTTY is recommended. |
| 4 | Redirection to the serial port is configured in the OS.  
**NOTE:** If the OS was installed by Kontron, console redirection is enabled by default. |

**Relevant section:**
- Baseboard management controller - BMC
Port location

Access procedure
To obtain the list of default user names and passwords, refer to Default user names and passwords.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>From a computer with a physical connection to the serial port, open a serial console tool and start the communication between the console and the port to which the device is connected.</td>
</tr>
<tr>
<td>Step_2</td>
<td>The OS start screen will be displayed.</td>
</tr>
</tbody>
</table>

NOTE: If the OS is not displayed, perform a server reset. Refer to Platform power management.
Accessing the BIOS

Table of contents

- Accessing the BIOS using the KVM
  - Prerequisites
  - Browser considerations
  - Access procedure
    - Accessing the BMC of the server for which you want to access the BIOS
  - Launching the KVM
  - Accessing the BIOS setup menu
- Accessing the BIOS using the display port (VGA)
  - Prerequisites
  - Port location
  - Access procedure
- Accessing the BIOS using Serial over LAN (SOL)
  - Prerequisites
  - Access procedure
- Accessing the BIOS using a serial console (physical connection)
  - Prerequisites
  - Port location
  - Access procedure

The BIOS can be accessed through various methods:
- Using the KVM (Keyboard Video Mouse)
- Using the display port (VGA) – this is the recommended path for first time out-of-the-box system configuration
- Using Serial over LAN (SOL)
- Using a serial console (physical connection)

Refer to Description of system access methods for more information on the various paths.

Accessing the BIOS using the KVM

Prerequisites

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).</td>
</tr>
<tr>
<td>2</td>
<td>The remote computer has access to the management network subnet.</td>
</tr>
</tbody>
</table>

Relevant section:
Configuring/Baseboard management controller - BMC

Browser considerations

**HTML5**
To connect to the Web UI, a Web browser supporting HTML5 is required.

**HTTPS self-signed certificate**
Upon connection to the Web UI, it is mandatory to accept the HTTPS self-signed certificate. For further information about accepting HTTPS self-signed certificates, please refer to your Web browser’s documentation.

**File download permission**
File download from the site needs to be permitted. For further information about file download permission, please refer to your Web browser’s documentation.

**Cookies**
Cookies must be enabled in order to access the website. For further information about enabling cookies, please refer to your Web browser’s documentation.

NOTE: The procedure may vary depending on the browser used. Examples provided use Firefox.

Access procedure

Accessing the BMC of the server for which you want to access the BIOS

To obtain the list of default user names and passwords, refer to Default user names and passwords.
Step 1  From a remote computer that has access to the management network, open a browser window and enter the IP address discovered for the BMC.  
**NOTE:** The HTTPS prefix is mandatory.  
- https://[BMC MNGMT_IP]

Step 2  Click on **Advanced** in order to start the HTTPS self-signed certificate acceptance process.  Information on the error message will be displayed.

Step 3  Click on **Add Exception...** The Add Security Exception pop-up window will be displayed. Click on **Confirm Security Exception** to allow the browser to access the management Web UI of this interface.

Step 4  Log in to the BMC Web UI using the appropriate credentials.  
**NOTE:** Default Web UI user name and password is admin/admin.

Step 5  You now have access to the management Web UI of the BMC. You can use the interface.

Launching the KVM
Step 1. From the left menu, click on Remote Control.

Step 2. From the Remote Control menu, click on the Launch KVM button.

Step 3. A new browser window opens and displays the server screen. 
**NOTE:** If an OS is installed, the image displayed might be that of the OS.

**Accessing the BIOS setup menu**
Step 1: From the Power drop-down menu, select Reset Server to access the BIOS menu. Click on OK to confirm the operation.

**NOTE:** When a reset server command is launched, it may take a few seconds for the BIOS sign on screen to display.

Step 2: When the BIOS sign on screen is displayed, press the specified key to enter the BIOS setup menu.

**NOTE:** It may take a few seconds for the BIOS sign on screen to display confirmation message "Entering Setup..."

**Tip:**
Some users are pressing DEL/F2 many times and very rapidly, to make sure the server catches the key and enters the BIOS setup menu. Doing this may lead to following message on the KVM display:

**HID Queue is about to get full. Kindly hold on a second(s).**

Kontron suggests modifying the Setup Prompt Timeout parameter to give users more time to react.

Parameter Setup Prompt Timeout is found in the Boot tab of the BIOS setup menu.

The default value is 1 second, but changing it to a value between 3 and 10 seconds is a good target range.

Step 3: The BIOS sign on screen displays "Entering Setup..."

**NOTE:** It will take several seconds to display and enter the BIOS setup menu.

Step 4: The BIOS setup menu will be displayed.

---

Accessing the BIOS using the display port (VGA)

**Prerequisites**

1. A physical connection to the VGA display port of the device is required.
2. A mouse and/or keyboard is connected.

**Port location**

**Access procedure**

1. Connect the VGA cable to the monitor and the platform.
2. Reset the platform.
3. The BIOS screen should be displayed on the monitor.
Accessing the BIOS using Serial over LAN (SOL)

Prerequisites

1. The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).
2. The remote computer has access to the management network subnet.
3. A community version of ipmitool is installed on a remote computer to enable remote monitoring—it is recommended to use ipmitool version 1.8.18.

Relevant sections:
- Baseboard management controller - BMC
- Common software installation

Access procedure

To obtain the list of default user names and passwords, refer to Default user names and passwords.

**Step 1**
From a remote computer that has access to the management network subnet, open the OS command prompt and deactivate any previous SOL session.

```
```

**Step 2**
Activate an SOL session.

```
```

**NOTE:** It may be required to press the Enter key for the operating system's screen to be displayed.

**Step 3**
Perform a server reset.

```
```

**NOTE:** When a reset server command is launched, it may take a few seconds for the BIOS sign on screen to display.

**Step 4**
When the BIOS sign on screen is displayed, press the specified key to enter the BIOS setup menu.

**NOTE:** It may take a few seconds for the BIOS sign on screen to display confirmation message "Entering Setup...".

**Step 5**
The BIOS sign on screen displays "Entering Setup...".

**NOTE:** It will take several seconds to display and enter the BIOS setup menu.

**Step 6**
The BIOS setup menu is displayed.
Accessing the BIOS using a serial console (physical connection)

Prerequisites

1. A physical connection to the device is required.
   NOTE: The serial console port is compatible with Cisco 72-3383-01 cable.

2. A serial console tool is installed on the remote computer.
   - Speed (Baud): 115200
   - Data bits: 8
   - Stop bits: 1
   - Parity: None
   - Flow Control: None
   - Recommended emulation mode: VT100+
   NOTE: PuTTY is recommended.

Port location

Access procedure

Step_1  From a computer with a physical connection to the serial port, open a serial console tool and start the communication between the console and the port to which the device is connected.

Step_2  Perform a server reset (Ctrl-break hot key).
   NOTE: If an operating system is installed on the device, the hot key might not work properly. If this is the case, reset the server as recommended for the operating system.
   NOTE: When a server reset command is sent, it may take a few seconds for the BIOS sign on screen to display.

Step_3  When the BIOS sign on screen is displayed, press the specified key to enter the BIOS setup menu.
   NOTE: It may take a few seconds for the BIOS sign on screen to display confirmation message “Entering Setup...”.

Step_4  The BIOS sign on screen displays “Entering Setup...”.
   NOTE: It will take several seconds to display and enter the BIOS setup menu.
Step 5: The BIOS setup menu is displayed.
Accessing a BMC

Table of contents
- Accessing a BMC using the Web UI
  - Prerequisites
  - Browser considerations
  - Access procedure
- Accessing a BMC using IPMI over LAN (IOL)
- Accessing a BMC using IPMI via KCS
- Accessing a BMC using SNMP
- Accessing a BMC using BMC SNMP
- Accessing a BMC using the Kontron linux snmp-agent
- Accessing a BMC using Redfish
- Accessing a BMC using Redfish

A BMC can be accessed through various methods:

- Using the Web UI – this is the recommended path for first time out-of-the-box system configuration
- Using IPMI over LAN (IOL)
- Using IPMI via KCS
- Using SNMP
- Using Redfish

Refer to Description of system access methods for more information on the various paths.

Accessing a BMC using the Web UI

Prerequisites

1. The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).
2. The remote computer has access to the management network subnet.

Relevant section:
Baseboard management controller - BMC

Browser considerations

<table>
<thead>
<tr>
<th>HTML5</th>
<th>To connect to the Web UI, a Web browser supporting HTML5 is required.</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS self-signed certificate</td>
<td>Upon connection to the Web UI, it is mandatory to accept the HTTPS self-signed certificate. For further information about accepting HTTPS self-signed certificates, please refer to your Web browser’s documentation.</td>
</tr>
<tr>
<td>File download permission</td>
<td>File download from the site needs to be permitted. For further information about file download permission, please refer to your Web browser’s documentation.</td>
</tr>
<tr>
<td>Cookies</td>
<td>Cookies must be enabled in order to access the website. For further information about enabling cookies, please refer to your Web browser’s documentation.</td>
</tr>
</tbody>
</table>

NOTE: The procedure may vary depending on the browser used. Examples provided use Firefox.

Access procedure

To obtain the list of default user names and passwords, refer to Default user names and passwords.
From a remote computer that has access to the management network, open a browser window and enter the IP address discovered for the BMC. **NOTE:** The HTTPS prefix is mandatory.

https://[BMC MNGMT_IP]

Click on **Advanced** in order to start the HTTPS self-signed certificate acceptance process. Information on the error message will be displayed.

Click on **Add Exception…**. The Add Security Exception pop-up window will be displayed. Click on **Confirm Security Exception** to allow the browser to access the management Web UI of this interface.

Log in to the BMC Web UI using the appropriate credentials. **NOTE:** Default Web UI user name and password is admin/admin.

You now have access to the management Web UI of the BMC. You can use the interface.

---

### Accessing a BMC using IPMI over LAN (IOL)

**Prerequisites**

1. The BMC IP address is known.
2. The remote computer has access to the management network subnet.
3. A community version of ipmitool is installed on a remote computer to enable remote monitoring—it is recommended to use ipmitool version 1.8.18.

**Relevant sections:**

- Baseboard management controller - BMC
- Common software installation

**Access procedure**

To obtain the list of default user names and passwords, refer to Default user names and passwords.
Step_1 From a remote computer that has access to the management network subnet, enter the desired command.

RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] [IPMI command]

For a list of supported IPMI commands, refer to Supported IPMI commands. For a list of all the sensors, refer to Sensor list.

### Accessing a BMC using IPMI via KCS

**Prerequisites**

1. An OS is installed.
2. The remote computer has access to the server OS (SSH/RDP/platform serial port).
3. A community version of ipmitool is installed on the local server to enable local monitoring—it is recommended to use ipmitool version 1.8.18.

**Relevant section:**
Common software installation

**Access procedure**

Step_1 From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, enter the desired command.

LocalServer_OSPrompt:~# ipmitool [IPMI command]

For a list of supported IPMI commands, refer to Supported IPMI commands. For a list of all the sensors, refer to Sensor list.

### Accessing a BMC using SNMP

The BMC can be accessed using:

- **BMC SNMP**
- The Kontron linux snmp-agent

**Accessing a BMC using BMC SNMP**

**Prerequisites**

1. The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).
2. The remote computer has access to the management network subnet.
3. An snmp client is installed on the remote computer.

**Relevant section:**
Configuration of system access methods

**Access procedure**

Step_1 From a remote computer that has access to the management network subnet, enter the desired command.


### Accessing a BMC using the Kontron linux snmp-agent

**Prerequisites**

1. An OS is installed.
2. The OS IP address is known.
3. The remote computer has access to the OS subnet.
4. The latest snmp-agent rpm package provided by Kontron is installed on the server.

**Relevant section:**
Configuration of system access methods
Access procedure

Step_1  From a remote computer that has access to the server network subnet, enter the desired command.


Accessing a BMC using Redfish

Prerequisites

1  The BMC IP address is known.
2  An HTTP client tool is installed on the remote computer.
3  A JSON parser command-line tool such as jq is installed.

Relevant sections:
- Configuring system access methods
- Supported Redfish commands

Access procedure

Step_1  Access the Redfish API using the root URL.

RemoteComputer_OSPrompt:~$ curl -k -s [ROOT_URL] | jq

Step_2  Add the Managers/Self extension.

Platform power management

(This article provides instructions to safely power on, power off or reboot a component.)

Table of contents
- Available power commands
- Power off
- Power on
- Reset (warm boot)
- Power cycle (cold boot)
- ACPI shutdown (clean shutdown)
- Sending a power command using the Web UI
- Power control policy on power outage
- Power Restore Delay on power outage

Available power commands

The power states of the CG2400 platform can be managed using various commands sent through the platform Web UI or an IPMI client (IOL or KCS).

It is recommended to use the Web UI, and automation of power management tasks requires an IPMI access.

The power commands are:
- **Power off**: Immediately powers off the platform. **WARNING**: This command does not initiate a clean shutdown of the operating system prior to powering down the system.
- **Power on**: Powers on the platform. **NOTE**: Due to the electrical setup of the system, there is a 30 seconds delay for the system to start.
- **Reset (warm boot)**: Reboots the platform without turning off power. **WARNING**: This command does not initiate a clean shutdown of the operating system prior to rebooting the system.
- **Power cycle (cold boot)**: Powers off the platform before rebooting it. **WARNING**: This command does not initiate a clean shutdown of the operating system prior to rebooting the system.
- **ACPI shutdown (clean shutdown)**: Initiates and completes the operating system’s shutdown prior to powering off the platform. **NOTE**: ACPI must be supported by the server’s operating system.

Power off

- Using the Web UI
- Using IPMI (IOL)
- Using IPMI (KCS)
- Using Redfish

Power off using IPMI (IOL)

Refer to [Accessing a BMC using IPMI over LAN (IOL)](http://example.com) for access instructions.

<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From a remote computer that has access to the management network subnet, open the OS command prompt and power off the platform. RemoteComputer_OSPrompt:~$ ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power off</td>
</tr>
<tr>
<td>2</td>
<td>Verify the power status to confirm the power action has succeeded. RemoteComputer_OSPrompt:~$ ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power status</td>
</tr>
</tbody>
</table>

Power off using IPMI (KCS)

Refer to [Accessing a BMC using IPMI via KCS](http://example.com) for access instructions.

<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, power off the platform. LocalServer_OSPrompt:~# ipmitool chassis power off</td>
</tr>
</tbody>
</table>

Power off using Redfish

Refer to [Accessing a BMC using Redfish](http://example.com) for access instructions.
### Step 1
Print the list of available power actions.
```
```

### Step 2
Power off the platform.
```
```

### Step 3
Verify the power status.
```
```

### Power on
- Using the Web UI
- Using IPMI (IOL)
- Using Redfish

### Power on using IPMI (IOL)
Refer to [Accessing a BMC using IPMI over LAN (IOL)] for access instructions.

#### Step 1
From a remote computer that has access to the management network subnet, open the OS command prompt and reset the platform.
```
```

#### Step 2
Verify the power status to confirm the power action has succeeded.
```
```

### Power on using Redfish
Refer to [Accessing a BMC using Redfish](#) for access instructions.

#### Step 1
Print the list of available power actions.
```
```

#### Step 2
Power on the platform.
```
```

#### Step 3
Verify the power status.
```
```

### Reset (warm boot)
- Using the Web UI
- Using IPMI (IOL)
- Using IPMI (KCS)
- Using Redfish

### Reset (warm boot) using IPMI (IOL)
Refer to [Accessing a BMC using IPMI over LAN (IOL)] for access instructions.

#### Step 1
From a remote computer that has access to the management network subnet, open the OS command prompt and reset the platform.
```
```

#### Step 2
Verify the power status to confirm the power action has succeeded.
```
```

### Reset (warm boot) using IPMI (KCS)
Refer to [Accessing a BMC using IPMI via KCS](#) for access instructions.

**NOTE:** It may take a moment for the OS to reboot.
Reset (warm boot) using Redfish
Refer to Accessing a BMC using Redfish for access instructions.

Power cycle (cold boot)

- Using the Web UI
- Using IPMI (IOL)
- Using IPMI (KCS)

Power cycle (cold boot) using IPMI (IOL)
Refer to Accessing a BMC using IPMI over LAN (IOL) for access instructions.

ACPI shutdown (clean shutdown)

- Using the Web UI
- Using IPMI (IOL)
- Using IPMI (KCS)
- Using Redfish

ACPI shutdown using IPMI (IOL)
Refer to Accessing a BMC using IPMI over LAN (IOL) for access instructions.

ACPI shutdown using IPMI (KCS)
Refer to Accessing a BMC using IPMI via KCS for access instructions.
Step_1

From a remote computer that has access to the server OS through SSH, RDP or the
platform serial port, perform an ACPI shutdown.
LocalServer_OSPrompt:~# ipmitool chassis power soft

ACPI shutdown using Redfish
Refer to Accessing a BMC using Redfish for access instructions.
Step_1

Print the list of available power actions.

Step_2 Perform the power action on the platform.
"Content-Type: application/json"
Step_3 Verify the power status.

Sending a power command using the Web UI
Refer to Accessing a BMC using the Web UI for access instructions.
Step_1

Access the BMC Web UI of a server.

Step_2 Once you are logged into the Web UI, click on Power Control from the left side menu.

Step_3 Select the desired power action. Press on the Perform Action button.

Step_4 A confirmation prompt will appear. Confirm the action by clicking on OK. Upon
confirmation, the selected action will be performed and the platform status will be
updated after a few minutes.

Step_5

Verify the power status by looking at the power status in the left side menu.

Power control policy on power outage
It is possible to configure how a system behaves in terms of power management in case of power loss or outage.
This feature was named Resume on AC Power Loss in Kontron’s previous CG generation (CG2200, CG2300).
This setting can be set using IPMI or using the BIOS menu.
Here are the possible values and the correspondance between IPMI and the BIOS menu.
IPMI

BIOS menu

Note

always-on

Power Restore

Platform powers up when power is restored

previous

Last Power State

Platform returns to previous state (before the power outage) when power is restored

always-off

Do Not Power Up

Platform stays unpowered even though input power is back

CG2400_User_documentation_2-01-2023

www.kontron.com

// 194


### Using IPMI

**Step 1** Using the `ipmitool chassis policy` command, set the power control policy.

```
LocalServer_OSPrompt:~# ipmitool chassis policy [POLICY]
```

### Using the BIOS menu

Refer to [Accessing the BIOS](#) for access instructions.

**Step 1** From the Server Mgmt menu, select the Power Control Policy value.

### Power Restore Delay on power outage

It is possible to add a certain amount of time before the platform powers up when power is restored. This setting can be set using IPMI or using the BIOS menu.

Here are the possible values that this feature supports:

<table>
<thead>
<tr>
<th>BIOS value</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>No Power Restore Delay will be set, platform starts automatically after power outage (default value)</td>
</tr>
<tr>
<td>Auto</td>
<td>Random value (between 55-300 sec) will be set, platform starts after this delay is elapsed</td>
</tr>
<tr>
<td>Fixed</td>
<td>Selected value (between 55-300 sec) will be set, platform starts after this delay is elapsed</td>
</tr>
</tbody>
</table>

### Using IPMI

**Step 1** Using this `ipmitool raw OEM` command, set the Power Restore Delay parameters.

```
LocalServer_OSPrompt:~# ipmitool raw 0x00 0x08 0x60 [DATA1] [DATA2]
```

Where `DATA1` possible values are:
- 0x00 is Disabled
- 0x01 is Auto (random delay between 55-300 seconds)
- 0x02 is Fixed (manual delay between 55-300 seconds)

Where `DATA2` contains delay value when Fixed setting is selected:
- minimum value 0x00 represents 55 seconds delay
- maximum value 0xF5 represents 300 seconds delay

**Step 2** Using this `ipmitool raw OEM` command, it is possible to verify current parameters.

```
LocalServer_OSPrompt:~# ipmitool raw 0x00 0x09 0x60 0x00 0x00
```

**NOTE:** answer will always contains 4 bytes of data: 01 60 [DATA1] [DATA2]

### Using the BIOS menu

Refer to [Accessing the BIOS](#) for access instructions.

**Step 1** From the Server Mgmt menu, select the Power Restore Delay parameter.

**NOTE:** when entering menu, default value will always be [unspecified]. It is imperative to select the desired value to trigger the change.

**Step 2** If parameter Fixed is selected, enter a value between 55 and 300 seconds in the numerical box Power Restore Delay Value.
Monitoring
Monitoring sensors

(This article details all available monitoring agents of the platform.)

Table of contents
- Monitoring using the BMC Web UI
  - Accessing sensor details
  - Configuring sensors
- Monitoring using IPMI
  - Viewing sensor details
  - Configuring sensors
- Monitoring using SNMP
  - Monitoring using BMC SNMP
  - Monitoring using the Kontron Linux snmp-agent
- Monitoring using Redfish
  - Creating URL extensions
  - Viewing sensor details

The platform has many sensors, you can refer to the Sensor list for details and to determine the sensor ID.

There are several methods to monitor platform sensors, including:
- Using the BMC Web UI
- Using IPMI
- Using SNMP
- Using Redfish

For sensor data interpretation instructions, refer to Interpreting sensor data.
For instructions on how to access the BMC, refer to Accessing a BMC.

Monitoring using the BMC Web UI

Accessing sensor details

Refer to Accessing a BMC using the Web UI for access instructions.
Step 1  Access the BMC Web UI.

Step 2  From the left-side menu, click on **Sensor**.

Step 3  The sensor list will be displayed.

Step 4  Scroll down to see the list of sensors.

Step 5  Click on a sensor to see more details.

---

**Configuring sensors**

**NOTE:** Sensor thresholds are set to factory default when resetting the platform.

**NOTICE**  Default platform sensor thresholds should not be changed. They have been set to ensure proper operation. Should you decide to change them, use caution as inappropriate settings could cause a property damage.
Step 1
From the sensor detail page, click on Change Thresholds.

Step 2
Set the thresholds as desired and click on Save. Optional: Check Retain Thresholds if you wish to keep the set thresholds after a BMC reboot.

Monitoring using IPMI
The following procedures will be executed using the Accessing a BMC using IPMI (KCS) method, but some configurations can also be performed using IOL ( Accessing a BMC using IPMI over LAN (IOL) ). To use IOL, add the IOL parameters to the command: -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password].

Viewing sensor details

Step 1
From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, enter the command.
LocalServer_OSPrompt:~# ipmitool sensor

Step 2
Use the sdr command to see more details about a specific sensor.
LocalServer_OSPrompt:~# ipmitool sdr get [SENSOR_ID]

Configuring sensors
NOTE: Sensor thresholds are set to factory default when resetting the platform.

Step 1
Change the threshold value of the desired sensor.
LocalServer_OSPrompt:~# ipmitool sensor thresh [SENSOR_ID] [THRESH_TYPE] [VALUE]
NOTE: For a negative threshold value add double dashes (--) before the sensor command and type the negative value.
LocalServer_OSPrompt:~# ipmitool -- sensor thresh [SENSOR_ID] [THRESH_TYPE] [NEG VALUE]

Monitoring using SNMP
The platform can be remotely monitored with the SNMP protocol:
- Using BMC SNMP
- Using the Kontron linux snmp-agent

Each method is independent.

When monitoring the platform, there are multiple factors to consider for each method:
- Each method gives access to different information. For instance, threshold values can only be read using the KontronLinux snmp-agent method.
- Each method has its own credentials. Refer to Default user names and passwords for default credentials.
- Some OIDs might differ depending on the access method.
- BMC SNMP is accessible from the dedicated LAN port on the management plane.
- The linux snmp-agent is accessible from the two 10GbE LAN ports on the data plane.
Monitoring using BMC SNMP

NOTE: The current implementation supports version 3 of the SNMP protocol. For the commands to work, snmpwalk version 5.8 or higher must be installed. Refer to Accessing a BMC using BMC SNMP for access instructions.

Viewing the sensor list

Step_1 To access all the sensors of the BMC, use the following command.

Viewing sensor details

Step_1 Use the following command to view sensor details.

NOTE: The space between the [TABLE_ENTRY_NUMBER] attribute and the quotes is required for the grep command to work properly.

Monitoring using the Kontron linux snmp-agent

Refer to Configuring Kontron linux snmp-agent on the platform for configuration instructions. See also Configuring SNMP users using the Kontron linux snmp-agent to manage SNMP users.

Kontron linux snmp-agent OIDs

<table>
<thead>
<tr>
<th>Group</th>
<th>Group OID</th>
<th>Sub-group</th>
<th>Sub-group OID</th>
<th>Numerical OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>powerGroup</td>
<td>Power unit</td>
<td>powerUnitTable</td>
<td>1.3.6.1.4.1.15000.2.10.3.5.400.10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Power supply</td>
<td>powerSupplyTable</td>
<td>1.3.6.1.4.1.15000.2.10.3.5.400.20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Voltages</td>
<td>voltageProbeTable</td>
<td>1.3.6.1.4.1.15000.2.10.3.5.400.30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Discrete voltage</td>
<td>discreteVoltageProbeTable</td>
<td>1.3.6.1.4.1.15000.2.10.3.5.400.40</td>
</tr>
<tr>
<td>Thermal</td>
<td>thermalGroup</td>
<td>Cooling unit</td>
<td>coolingUnitTable</td>
<td>1.3.6.1.4.1.15000.2.10.3.5.600.10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Discrete cooling device</td>
<td>discreteCoolingTable</td>
<td>1.3.6.1.4.1.15000.2.10.3.5.600.30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Temperature</td>
<td>temperatureProbeTable</td>
<td>1.3.6.1.4.1.15000.2.10.3.5.600.40</td>
</tr>
</tbody>
</table>

Viewing sensor details
**Step 1** Find the right sensor entry number in the table depending on the IPMI SENSOR NAME (i.e. BMC Temp is table entry 7).


**Step 2** View sensor details for a specific sensor.


**NOTE:** The space between the [TABLE_ENTRY_NUMBER] attribute and the quotes is required for the `grep` command to work properly.

### Configuring sensors

**NOTE:** Sensor thresholds are set to factory default when resetting the platform.

**Step 1** Find the OID of the value to change.


**Step 2** Set the value of the desired threshold.


### Monitoring using Redfish

Refer to [Accessing a BMC using Redfish](#) for access instructions.

### Creating URL extensions

<table>
<thead>
<tr>
<th>Type</th>
<th>Sensors</th>
<th>URL extensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>• All sensors of type 02h (Voltage)</td>
<td>Chassis/Self</td>
</tr>
<tr>
<td></td>
<td>• All sensors of type 01h (Temperature)</td>
<td>Chassis/Self</td>
</tr>
<tr>
<td></td>
<td>• Fan1_speed</td>
<td>Chassis/Self</td>
</tr>
<tr>
<td></td>
<td>• Fan2_speed</td>
<td>Chassis/Self</td>
</tr>
<tr>
<td></td>
<td>• Fan3_speed</td>
<td>Chassis/Self</td>
</tr>
<tr>
<td></td>
<td>• Fan4_speed</td>
<td>Chassis/Self</td>
</tr>
<tr>
<td>Health</td>
<td>• CPU Status</td>
<td>Managers/Self</td>
</tr>
<tr>
<td></td>
<td>• Health Status</td>
<td>Chassis/Self</td>
</tr>
</tbody>
</table>

### Viewing sensor details

**Step 1** Append the root URL with the appropriate extension depending on the type of sensor. Refer to the URL extensions table above.

RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL] [URL_EXTENSION]
## Sensor list

[This article details all sensors of the platform’s module.]

For information about Sensor type code and Event/Reading type code, refer to [Interpreting sensor data](#).

<table>
<thead>
<tr>
<th>Sensor name [Sensor_ID]</th>
<th>SNMP sensor number [Sensor_ID_number]</th>
<th>IPMI sensor number [Sensor_ID_number]</th>
<th>Sensor type code</th>
<th>Event / Reading type code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI Error</td>
<td>33h</td>
<td>13h</td>
<td>6Fh</td>
<td>Various PCI/PCIe errors detected by BIOS (GenId:21)</td>
<td></td>
</tr>
<tr>
<td>Memory Error</td>
<td>34h</td>
<td>0Ch</td>
<td>6Fh</td>
<td>Various Memory errors detected by BIOS (GenId:21)</td>
<td></td>
</tr>
<tr>
<td>Processor Error</td>
<td>35h</td>
<td>07h</td>
<td>6Fh</td>
<td>Various Processor errors detected by BIOS (GenId:21)</td>
<td></td>
</tr>
<tr>
<td>Direct Memory Access (DMA) Error</td>
<td>36h</td>
<td>07h</td>
<td>6Fh</td>
<td>Various DMA errors detected by BIOS (GenId:21)</td>
<td></td>
</tr>
<tr>
<td>OutBound Traffic Controller (OTC) Error</td>
<td>37h</td>
<td>07h</td>
<td>6Fh</td>
<td>Various OTC errors detected by BIOS (GenId:21)</td>
<td></td>
</tr>
<tr>
<td>InBound Traffic Controller (ITC) Error</td>
<td>38h</td>
<td>07h</td>
<td>6Fh</td>
<td>Various ITC errors detected by BIOS (GenId:21)</td>
<td></td>
</tr>
<tr>
<td>Intel VT-d Error</td>
<td>39h</td>
<td>07h</td>
<td>6Fh</td>
<td>Various VT-d errors detected by BIOS (GenId:21)</td>
<td></td>
</tr>
<tr>
<td>FP NMI Diag Int</td>
<td>3</td>
<td>05h</td>
<td>13h</td>
<td>IPMI Watchdog sensor</td>
<td></td>
</tr>
<tr>
<td>IPMI Watchdog</td>
<td>2</td>
<td>03h</td>
<td>23h</td>
<td>Management health watchdog</td>
<td></td>
</tr>
<tr>
<td>BMC Watchdog</td>
<td>6</td>
<td>0Ah</td>
<td>28h</td>
<td>Management health watchdog</td>
<td></td>
</tr>
<tr>
<td>VR Watchdog</td>
<td>7</td>
<td>08h</td>
<td>02h</td>
<td>Management health watchdog</td>
<td></td>
</tr>
<tr>
<td>System Event Log</td>
<td>5</td>
<td>07h</td>
<td>10h</td>
<td>Management health watchdog</td>
<td></td>
</tr>
<tr>
<td>System Event</td>
<td>5</td>
<td>08h</td>
<td>12h</td>
<td>Management health watchdog</td>
<td></td>
</tr>
<tr>
<td>Front Panel Temp</td>
<td>21h</td>
<td>01h</td>
<td>01h</td>
<td>Temperature of front panel</td>
<td></td>
</tr>
<tr>
<td>P1 Temp</td>
<td>64</td>
<td>C7h</td>
<td>01h</td>
<td>Processor 1 Temperature</td>
<td></td>
</tr>
<tr>
<td>P2 Temp</td>
<td>74</td>
<td>D2h</td>
<td>01h</td>
<td>Processor 2 Temperature</td>
<td></td>
</tr>
<tr>
<td>P1 TJMAX</td>
<td>18</td>
<td>20h</td>
<td>01h</td>
<td>Processor 1 Temperature: maximum temperature before thermal trip</td>
<td></td>
</tr>
<tr>
<td>P2 TJMAX</td>
<td>8</td>
<td>0Fh</td>
<td>01h</td>
<td>Processor 2 Temperature: maximum temperature before thermal trip</td>
<td></td>
</tr>
<tr>
<td>CPU Zone Temp</td>
<td>57</td>
<td>B5h</td>
<td>01h</td>
<td>Temperature of CPU Zone</td>
<td></td>
</tr>
<tr>
<td>PCH Temp</td>
<td>17</td>
<td>1Fh</td>
<td>01h</td>
<td>Temperature of PCH</td>
<td></td>
</tr>
<tr>
<td>BMC Temp</td>
<td>61</td>
<td>BAh</td>
<td>01h</td>
<td>BMC Temperature</td>
<td></td>
</tr>
<tr>
<td>PCIe A Temp</td>
<td>59</td>
<td>B7h</td>
<td>01h</td>
<td>PCIe A Temperature (J33 Extension cable) Managing extension probe</td>
<td></td>
</tr>
<tr>
<td>PCIe B Temp</td>
<td>60</td>
<td>B9h</td>
<td>01h</td>
<td>PCIe B Temperature (J37 Extension cable) Managing extension probe</td>
<td></td>
</tr>
<tr>
<td>X557 LAN1 Temp</td>
<td>62</td>
<td>BBh</td>
<td>01h</td>
<td>Temperature of X557 LAN 1</td>
<td></td>
</tr>
<tr>
<td>X557 LAN2 Temp</td>
<td>63</td>
<td>BCh</td>
<td>01h</td>
<td>Temperature of X557 LAN 2</td>
<td></td>
</tr>
<tr>
<td>M.2 Temp</td>
<td>56</td>
<td>B4h</td>
<td>01h</td>
<td>M.2 zone Temperature</td>
<td></td>
</tr>
<tr>
<td>Battery Temp</td>
<td>58</td>
<td>B6h</td>
<td>01h</td>
<td>Temperature of Battery</td>
<td></td>
</tr>
<tr>
<td>P1 DIMMA1 Temp</td>
<td>65</td>
<td>CBh</td>
<td>01h</td>
<td>Temp CPU1 DIMM Channel</td>
<td></td>
</tr>
<tr>
<td>P1 DIMMA2 Temp</td>
<td>66</td>
<td>C9h</td>
<td>01h</td>
<td>Temp CPU1 DIMM Channel</td>
<td></td>
</tr>
<tr>
<td>P1 DIMMB1 Temp</td>
<td>67</td>
<td>CAh</td>
<td>01h</td>
<td>Temp CPU1 DIMM Channel</td>
<td></td>
</tr>
<tr>
<td>P1 DIMMC1 Temp</td>
<td>68</td>
<td>CBh</td>
<td>01h</td>
<td>Temp CPU1 DIMM Channel</td>
<td></td>
</tr>
<tr>
<td>P1 DIMMD1 Temp</td>
<td>69</td>
<td>CCh</td>
<td>01h</td>
<td>Temp CPU1 DIMM Channel</td>
<td></td>
</tr>
<tr>
<td>P1 DIMMD2 Temp</td>
<td>70</td>
<td>CDh</td>
<td>01h</td>
<td>Temp CPU1 DIMM Channel</td>
<td></td>
</tr>
<tr>
<td>P1 DIMME1 Temp</td>
<td>71</td>
<td>CEh</td>
<td>01h</td>
<td>Temp CPU1 DIMM Channel</td>
<td></td>
</tr>
<tr>
<td>P1 DIMMF1 Temp</td>
<td>72</td>
<td>CFh</td>
<td>01h</td>
<td>Temp CPU1 DIMM Channel</td>
<td></td>
</tr>
<tr>
<td>P2 DIMMA1 Temp</td>
<td>75</td>
<td>D3h</td>
<td>01h</td>
<td>Temp CPU2 DIMM Channel</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>OID</td>
<td>Value 2</td>
<td>Value 1</td>
<td>Value 0</td>
<td>Value</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>P2 DIMMA2 Temp</td>
<td>76</td>
<td>D4h</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P2 DIMMB1 Temp</td>
<td>77</td>
<td>D5h</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P2 DIMMC1 Temp</td>
<td>78</td>
<td>D6h</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P2 DIMMD1 Temp</td>
<td>79</td>
<td>D7h</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P2 DIMMD2 Temp</td>
<td>80</td>
<td>D8h</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P2 DIMME1 Temp</td>
<td>81</td>
<td>DAh</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P1 DIMMA1 T Mrgn</td>
<td></td>
<td>F0h</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P1 DIMMA2 T Mrgn</td>
<td></td>
<td>F1h</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P1 DIMMB1 T Mrgn</td>
<td></td>
<td>F2h</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P1 DIMMC1 T Mrgn</td>
<td></td>
<td>F3h</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P1 DIMMD1 T Mrgn</td>
<td></td>
<td>F4h</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P1 DIMMD2 T Mrgn</td>
<td></td>
<td>F5h</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P1 DIMME1 T Mrgn</td>
<td></td>
<td>F6h</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P1 DIMMF1 T Mrgn</td>
<td></td>
<td>F7h</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P2 DIMMA1 T Mrgn</td>
<td></td>
<td>AAh</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P2 DIMMA2 T Mrgn</td>
<td></td>
<td>A8h</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P2 DIMMB1 T Mrgn</td>
<td></td>
<td>ACh</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P2 DIMMC1 T Mrgn</td>
<td></td>
<td>A0h</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P2 DIMMD1 T Mrgn</td>
<td></td>
<td>AEh</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P2 DIMMD2 T Mrgn</td>
<td></td>
<td>AFh</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P2 DIMME1 T Mrgn</td>
<td></td>
<td>B0h</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>P2 DIMMF1 T Mrgn</td>
<td></td>
<td>B1h</td>
<td>01h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>Fan Failure</td>
<td>26</td>
<td>34h</td>
<td>04h</td>
<td>06h</td>
<td></td>
</tr>
<tr>
<td>Fan1 Speed</td>
<td>20</td>
<td>2Dh</td>
<td>04h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>Fan2 Speed</td>
<td>21</td>
<td>2Eh</td>
<td>04h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>Fan3 Speed</td>
<td>22</td>
<td>2Fh</td>
<td>04h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>Fan4 Speed</td>
<td>23</td>
<td>30h</td>
<td>04h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>Fan5 Speed</td>
<td>24</td>
<td>31h</td>
<td>04h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>Fan6 Speed</td>
<td>25</td>
<td>32h</td>
<td>04h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>Fan1 Present</td>
<td>33</td>
<td>61h</td>
<td>04h</td>
<td>08h</td>
<td></td>
</tr>
<tr>
<td>Fan2 Present</td>
<td>34</td>
<td>62h</td>
<td>04h</td>
<td>08h</td>
<td></td>
</tr>
<tr>
<td>Fan3 Present</td>
<td>35</td>
<td>63h</td>
<td>04h</td>
<td>08h</td>
<td></td>
</tr>
<tr>
<td>Fan4 Present</td>
<td>36</td>
<td>64h</td>
<td>04h</td>
<td>08h</td>
<td></td>
</tr>
<tr>
<td>Fan5 Present</td>
<td>37</td>
<td>65h</td>
<td>04h</td>
<td>08h</td>
<td></td>
</tr>
<tr>
<td>Fan6 Present</td>
<td>38</td>
<td>66h</td>
<td>04h</td>
<td>08h</td>
<td></td>
</tr>
<tr>
<td>Pwr Unit Redund</td>
<td>1</td>
<td>02h</td>
<td>09h</td>
<td>08h</td>
<td></td>
</tr>
<tr>
<td>PS1 Status</td>
<td>13</td>
<td>1Ah</td>
<td>08h</td>
<td>6Fh</td>
<td></td>
</tr>
<tr>
<td>PS2 Status</td>
<td>14</td>
<td>18h</td>
<td>08h</td>
<td>6Fh</td>
<td></td>
</tr>
<tr>
<td>PS1 Input Power</td>
<td>9</td>
<td>16h</td>
<td>08h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>PS2 Input Power</td>
<td>10</td>
<td>17h</td>
<td>08h</td>
<td>01h</td>
<td></td>
</tr>
<tr>
<td>PS1 Output Power</td>
<td>15</td>
<td>1Ch</td>
<td>08h</td>
<td>01h</td>
<td></td>
</tr>
</tbody>
</table>

**CG2400_User_documentation_2-01-2023**

www.kontron.com
<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS2 Output Power</td>
<td>16</td>
<td>1Dh 08h 01h</td>
</tr>
<tr>
<td>PS1 Temp</td>
<td>11</td>
<td>18h 01h 01h</td>
</tr>
<tr>
<td>PS2 Temp</td>
<td>12</td>
<td>19h 01h 01h</td>
</tr>
<tr>
<td>CPU Missing</td>
<td>41</td>
<td>02h 07h 03h</td>
</tr>
<tr>
<td>P1 Status</td>
<td>86</td>
<td>EDh 07h 6fh</td>
</tr>
<tr>
<td>P2 Status</td>
<td>87</td>
<td>EEh 07h 6fh</td>
</tr>
<tr>
<td>P1 DTS Thrm Mrgn</td>
<td>83</td>
<td>DBh 01h 01h</td>
</tr>
<tr>
<td>P2 DTS Thrm Mrgn</td>
<td>84</td>
<td>0Ch 01h 01h</td>
</tr>
<tr>
<td>Voltage Fault</td>
<td>73</td>
<td>01h 02h 01h</td>
</tr>
<tr>
<td>V_2V5_AUX_X557</td>
<td>42</td>
<td>91h 02h 01h</td>
</tr>
<tr>
<td>V_2V1_AUX_X557</td>
<td>43</td>
<td>92h 02h 01h</td>
</tr>
<tr>
<td>V_TV2_AUX_X557</td>
<td>44</td>
<td>93h 02h 01h</td>
</tr>
<tr>
<td>V_OVB3_AUX_X557</td>
<td>45</td>
<td>94h 02h 01h</td>
</tr>
<tr>
<td>V_VNN_PCH_AUX</td>
<td>46</td>
<td>95h 02h 01h</td>
</tr>
<tr>
<td>V_TV05_PCH_AUX</td>
<td>47</td>
<td>96h 02h 01h</td>
</tr>
<tr>
<td>V_TV8_PCH_AUX</td>
<td>48</td>
<td>97h 02h 01h</td>
</tr>
<tr>
<td>V_TV18_AUX</td>
<td>49</td>
<td>98h 02h 01h</td>
</tr>
<tr>
<td>V_3V3_AUX</td>
<td>50</td>
<td>99h 02h 01h</td>
</tr>
<tr>
<td>V_3V3_AUX</td>
<td>51</td>
<td>9Ah 02h 01h</td>
</tr>
<tr>
<td>V_5V_AUX</td>
<td>52</td>
<td>9Bh 02h 01h</td>
</tr>
<tr>
<td>V_3V3</td>
<td>53</td>
<td>9Ch 02h 01h</td>
</tr>
<tr>
<td>V_5V</td>
<td>54</td>
<td>9Dh 02h 01h</td>
</tr>
<tr>
<td>V_12V</td>
<td>55</td>
<td>9Eh 02h 01h</td>
</tr>
<tr>
<td>V_3V_BAT</td>
<td>85</td>
<td>DEh 02h 01h</td>
</tr>
<tr>
<td>HDD0 Status</td>
<td>27</td>
<td>50h 00h 6fh</td>
</tr>
<tr>
<td>HDD1 Status</td>
<td>28</td>
<td>51h 00h 6fh</td>
</tr>
<tr>
<td>HDD2 Status</td>
<td>29</td>
<td>52h 00h 6fh</td>
</tr>
<tr>
<td>HDD3 Status</td>
<td>30</td>
<td>53h 00h 6fh</td>
</tr>
<tr>
<td>HDD4 Status</td>
<td>31</td>
<td>54h 00h 6fh</td>
</tr>
<tr>
<td>HDD5 Status</td>
<td>32</td>
<td>55h 00h 6fh</td>
</tr>
<tr>
<td>CPU Error</td>
<td>41</td>
<td>EFh 07h 6fh</td>
</tr>
<tr>
<td>Board Status</td>
<td>0C</td>
<td>C4h 07h 6fh</td>
</tr>
<tr>
<td>Power State</td>
<td>00h</td>
<td>01h 6fh</td>
</tr>
<tr>
<td>PWR_OK Capture 1</td>
<td>12h</td>
<td>08h 07h 6fh</td>
</tr>
<tr>
<td>PWR_OK Capture 2</td>
<td>13h</td>
<td>08h 07h 6fh</td>
</tr>
<tr>
<td>Ver Change FPGA</td>
<td>25h</td>
<td>2Bh 06h</td>
</tr>
<tr>
<td>Ver Change BMC</td>
<td>27h</td>
<td>2Bh 06h</td>
</tr>
</tbody>
</table>
Interpreting sensor data

(This article describes how to interpret sensor data.)

Table of contents

- Interpretation procedure
  - Interpreting non-discrete sensor data
  - Interpreting discrete sensor data
  - Accessing event data byte 2 and 3 (optional)
    - Accessing event data byte 2 using the BMC Web UI
    - Accessing event data byte 2 using IPMI
- Interpretation information
  - Sensor type
  - Sensor event/reading type
    - Threshold based event/reading type
    - Sensor-specific event/reading type
    - Other event/reading types
  - Event data byte 2
    - SMI handler generated event data bytes 2 and 3 description

Interpretation procedure

Before beginning the interpretation procedure, make sure to collect the following event information:

- Event ID
- Associated sensor
- Description

Refer for System event log for instructions.

NOTE: IOL and IPMI/KCS are the preferred methods for interpretation.

Step_1

In ipmitool, the sensor command returns a table. The columns are defined as:

- Name
- Numerical reading
- Event/reading type/unit
- Reading bytes 3 and 4
- Lower non-recoverable threshold value
- Lower critical threshold value
- Lower noncritical threshold value
- Upper noncritical threshold value
- Upper critical threshold value
- Upper non-recoverable threshold value

Step_2

Refer to the third column of the table or the platform Sensor list to verify if the specific sensor is discrete or non-discrete. The third column writes discrete for discrete sensors or a unit type for non-discrete sensors.

Step_3

Refer to Interpreting non-discrete sensor data or Interpreting discrete sensor data depending on the sensor’s event/reading type.

Interpreting non-discrete sensor data

Step_1

If the sensor event/reading type is non-discrete, the numerical reading value is shown in the second column.

Step_2

The fourth column indicates whether a threshold value has been surpassed by the numerical reading value or not. If the numerical reading value is within the expected range, the fourth column displays OK. Otherwise, the last threshold reached is displayed. Refer to Threshold based event/reading type for the definitions of threshold states.

Step_3

An event will be created according to the assertion enabled for the specified sensor.


Interpreting discrete sensor data
**Step 1** The second column of the `sensor` command should be ignored if the sensor is of discrete type. By default, discrete sensors should have a numerical reading value of 0x0.

**Step 2** The fourth column of the table is an aggregation of bytes 3 and 4 of the response given on sensor reading. Byte 3 is the less significant byte in the aggregation of bytes 3 and 4.

**Step 3** As for byte 3, all values should be 0x80, meaning all event messages are enabled for this sensor.

**Step 4** As for byte 4, it represents the states/event offsets defined for each type in the IPMI specification. Refer to `Sensor event/reading type` for lists of possible states for each sensor.

**Step 5** If specified in the event/reading type description of the sensor, refer to `Accessing event data byte 2` for additional information.

---

**Accessing event data byte 2 and 3 (optional)**

**NOTE:** This part of the procedure is needed only if the sensor concerned specifies it. Refer to `Sensor event/reading type`.

Even data can be obtained:
- Using the [BMC Web UI](https://www.kontron.com)
- Using [IPMI](https://www.kontron.com)

---

**A accessing event data byte 2 using the BMC Web UI**

Refer to [Accessing a BMC using the Web UI](https://www.kontron.com) for access instructions.

**Step 1** Convert the event ID to hexadecimal.

**Step 2** Access the BMC Web UI of the server.

**Step 3** Download the system event logs and open the file with any text editor.

**Step 4** In the SELLog file, find the event using its ID.

**Step 5** Event Data2 can be found in the second to the last column. Refer to [Event data byte 2](https://www.kontron.com) to interpret the event data byte.

---

**Accessing event data byte 2 using IPMI**

The following procedures will be executed using the [Accessing a BMC using IPMI over LAN (IOL)](https://www.kontron.com) method, but some tasks can also be performed using KCS ( [Accessing a BMC using IPMI via KCS](https://www.kontron.com) ). To use KCS, remove the IOL parameters from the command: `-I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password]`.

---
Step_1  Convert the event ID to hexadecimal.


Step_3  Recover the event data byte and the Sensor Number. The Event Data (RAW) row is an aggregation of the three event data byte, where the Event Data 2 byte is the second most significant byte.

Step_4  Refer to Event data byte 2 to interpret the event data byte:

Interpretation information
Each sensor has a Sensor type attribute and a Sensor event/reading type attribute. When a sensor created an event specified, more data about the event can be found in Event data byte 2. For more information about IPMI sensors refer to the IPMI documentation.

For a list of all the platform sensors, refer to Sensor list.

Sensor type
The sensor type attribute defines what the sensor is monitoring.

The following table lists all the IPMI sensor types present on the platform.

<table>
<thead>
<tr>
<th>Sensor type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01h (Temperature)</td>
<td>General information about temperatures of different components.</td>
</tr>
<tr>
<td>02h (Voltage)</td>
<td>General information about voltages either on the board or the power supply.</td>
</tr>
<tr>
<td>04h (Fan)</td>
<td>General information about the fan(s) of the platform (e.g. speed, presence, failure).</td>
</tr>
<tr>
<td>07h (Processor)</td>
<td>General information about the processor (e.g. presence, failure, health status).</td>
</tr>
<tr>
<td>08h (Power supply)</td>
<td>General information about the power supply (e.g. presence, failure, health status).</td>
</tr>
<tr>
<td>09h (Power Unit)</td>
<td>General information about the power unit.</td>
</tr>
<tr>
<td>0Ch (Memory)</td>
<td>General information about the memory (error).</td>
</tr>
<tr>
<td>0Dh (Drive Slot/Bay)</td>
<td>General information about storage devices slots and bay.</td>
</tr>
<tr>
<td>10h (Event logging disabled)</td>
<td>General information about the platform disabled system event log.</td>
</tr>
<tr>
<td>12h (System Event)</td>
<td>General information about the system events.</td>
</tr>
<tr>
<td>13h (Critical Interrupt)</td>
<td>General information about the critical interrupts on the system.</td>
</tr>
<tr>
<td>23h (Watchdog2)</td>
<td>General information about the IPMI watchdog.</td>
</tr>
<tr>
<td>28h (Management Subsys Health)</td>
<td>General information about the management subsystem health (BMC).</td>
</tr>
<tr>
<td>28h (Version Change)</td>
<td>Detection of firmware change (FPGA and BMC).</td>
</tr>
<tr>
<td>C6h (OEM board reset)</td>
<td>Kontron custom board reset type and sources sensor.</td>
</tr>
<tr>
<td>D7h (OEM Power State)</td>
<td>Kontron custom power state sensor.</td>
</tr>
</tbody>
</table>

Sensor event/reading type
The sensor event/reading type attribute defines how the reading of the value should be interpreted and how the sensor-related events are triggered. All event/reading types can either be discrete or non-discrete.

The following table describes the different event/reading types present on the platform.

<table>
<thead>
<tr>
<th>Event/reading type</th>
<th>7-bit event type code</th>
<th>Description</th>
<th>Offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold based</td>
<td>01h</td>
<td>Non-discrete, meaning it has a numerical reading and event triggers.</td>
<td>Offsets are standard and defined in the Threshold based event/reading type table.</td>
</tr>
<tr>
<td>Sensor-specific</td>
<td>6Fh</td>
<td>Discrete, meaning it has no numerical values, but it has event triggers.</td>
<td>Offsets are specific to the sensor's type and defined in the Sensor-specific event/reading type table.</td>
</tr>
</tbody>
</table>

Threshold based event/reading type
This type of sensor creates events as the numerical reading of a sensor reaches a pre-established threshold value. Threshold-based sensors on this platform can either
Report a voltage, a temperature or a fan speed.

<table>
<thead>
<tr>
<th>Event offset</th>
<th>Event trigger</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>00h</td>
<td>Lower noncritical - going low</td>
<td>nc</td>
</tr>
<tr>
<td>01h</td>
<td>Lower noncritical - going high</td>
<td></td>
</tr>
<tr>
<td>02h</td>
<td>Lower critical - going low</td>
<td>cr</td>
</tr>
<tr>
<td>03h</td>
<td>Lower critical - going high</td>
<td></td>
</tr>
<tr>
<td>04h</td>
<td>Lower non-recoverable - going low</td>
<td>nr</td>
</tr>
<tr>
<td>05h</td>
<td>Lower non-recoverable - going high</td>
<td></td>
</tr>
<tr>
<td>06h</td>
<td>Upper noncritical - going low</td>
<td>nc</td>
</tr>
<tr>
<td>07h</td>
<td>Upper noncritical - going high</td>
<td></td>
</tr>
<tr>
<td>08h</td>
<td>Upper critical - going low</td>
<td>cr</td>
</tr>
<tr>
<td>09h</td>
<td>Upper critical - going high</td>
<td></td>
</tr>
<tr>
<td>0Ah</td>
<td>Upper non-recoverable - going low</td>
<td>nr</td>
</tr>
<tr>
<td>0Bh</td>
<td>Upper non-recoverable - going high</td>
<td></td>
</tr>
</tbody>
</table>

**Sensor-specific event/reading type**

A sensor-specific event/reading type is a discrete type of sensor, meaning that it has no numerical value. When a sensor is of type sensor-specific, the event offset values are defined by the sensor type.

**NOTE:** Not all sensor-specific event offsets are supported by the platform. The following table lists the sensor-specific event offsets implemented on the platform.

<table>
<thead>
<tr>
<th>ID</th>
<th>Sensor name</th>
<th>Sensor type</th>
<th>Specific offset</th>
<th>Event trigger/state</th>
</tr>
</thead>
<tbody>
<tr>
<td>33h</td>
<td>PCI Error</td>
<td>13h (Critical Interrupt)</td>
<td>04h</td>
<td>PCI PERR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>05h</td>
<td>PCI SERR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>07h</td>
<td>Bus Correctable Error</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>08h</td>
<td>Bus Uncorrectable Error</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0Ah</td>
<td>Bus Fatal Error</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0Bh</td>
<td>LastBoot PCIe Error</td>
</tr>
<tr>
<td>34h</td>
<td>Memory Error</td>
<td>0Ch (Memory)</td>
<td>00h</td>
<td>Correctable ECC / Other correctable memory error</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>01h</td>
<td>Uncorrectable ECC / other uncorrectable memory error</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>02h</td>
<td>Parity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>05h</td>
<td>Correctable ECC / other correctable memory error logging limit reached</td>
</tr>
<tr>
<td>35h</td>
<td>Processor Error</td>
<td>07h (Processor)</td>
<td>05h</td>
<td>Configuration Error</td>
</tr>
<tr>
<td>36h</td>
<td>Direct Memory Access (DMA) Error</td>
<td>07h (Processor)</td>
<td>05h</td>
<td>Configuration Error</td>
</tr>
<tr>
<td>37h</td>
<td>OutBound Traffic Controller (OTC) Error</td>
<td>07h (Processor)</td>
<td>05h</td>
<td>Configuration Error</td>
</tr>
<tr>
<td>38h</td>
<td>InBound Traffic Controller (OTC) Error</td>
<td>07h (Processor)</td>
<td>05h</td>
<td>Configuration Error</td>
</tr>
<tr>
<td>39h</td>
<td>Intel VT-d Error</td>
<td>07h (Processor)</td>
<td>05h</td>
<td>Configuration Error</td>
</tr>
<tr>
<td>05h</td>
<td>FP NMI Diag Int</td>
<td>13h (Critical Interrupt)</td>
<td>00h</td>
<td>07h (Processor)</td>
</tr>
<tr>
<td>34h</td>
<td>Fan Failure</td>
<td>04h (Fan)</td>
<td>00h</td>
<td>Failure reported on fan #1</td>
</tr>
</tbody>
</table>
## IPMI Watchdog

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>05h</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>03h</td>
<td>Failure reported on fan #6</td>
<td></td>
<td>Failure reported on fan #6</td>
</tr>
<tr>
<td>07h</td>
<td>System Event Log</td>
<td></td>
<td>System event log cleared</td>
</tr>
<tr>
<td>08h</td>
<td>System Event Log</td>
<td></td>
<td>System event log full</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> See event data table below for more information.</td>
<td></td>
<td>System event log almost full</td>
</tr>
</tbody>
</table>

### Event Types

- **10h (Event Logging Disabled)**: System event log cleared
- **04h**: System event log full
- **05h**: System event log almost full

### Other Event/Reading Types

- **0Ch (Board Status)**: Board Status
- **C4h (OEM board reset)**: Power On
- **00h**: Power Button
- **02h**: Unknown
- **06h**: Cold Reset
- **07h**: IPMI Command
- **09h**: Power Up Reset
- **0Ah**: Power Down

## Power State

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>00h</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0Dh</td>
<td>Power State</td>
<td>Power ON</td>
<td>Power supply presence detected</td>
</tr>
<tr>
<td></td>
<td>Power State</td>
<td>Power OFF</td>
<td>Power supply failure detected</td>
</tr>
<tr>
<td></td>
<td>Power State</td>
<td>Power OFF Request</td>
<td>Firmware change detected</td>
</tr>
<tr>
<td></td>
<td>Power State</td>
<td>Power OFF Request</td>
<td>Firmware change detected</td>
</tr>
<tr>
<td></td>
<td>Power State</td>
<td>Power On Request</td>
<td>Firmware change detected</td>
</tr>
</tbody>
</table>

### Other Event/Reading Types

- **12h (PWROK Capture 1)**: Power supply
- **08h (Power supply)**: Power supply presence detected
- **13h (PWROK Capture 2)**: Power supply failure detected
- **25h (Ver Change FPGA)**: Version Change
- **2Bh (Version Change BMC)**: Firmware change detected
- **EFh (CPU Error)**: Machine Check Exception

### Other Event/Reading Types

- **07h (Processor)**: IERR
<table>
<thead>
<tr>
<th>ID</th>
<th>Sensor name</th>
<th>Sensor type</th>
<th>Specific offset</th>
<th>Event trigger/state</th>
</tr>
</thead>
<tbody>
<tr>
<td>0Ah</td>
<td>BMC Watchdog</td>
<td>03h (‘digital’ Discrete - Assert/Deassert)</td>
<td>01h</td>
<td>State asserted</td>
</tr>
<tr>
<td>08h</td>
<td>VR Watchdog</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>82h</td>
<td>CPU Missing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>61h</td>
<td>Fan1 Present</td>
<td>08h (‘digital’ Discrete - Present/Absent)</td>
<td>00h</td>
<td>Device absent</td>
</tr>
<tr>
<td>62h</td>
<td>Fan2 Present</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>63h</td>
<td>Fan3 Present</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64h</td>
<td>Fan4 Present</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>65h</td>
<td>Fan5 Present</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>66h</td>
<td>Fan6 Present</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>02h</td>
<td>Pwr Unit Redund</td>
<td>08h (Discrete)</td>
<td>00h</td>
<td>Fully Redundant</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>01h</td>
<td>Redundancy Lost</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>03h</td>
<td>Non-Redundant: Sufficient from Redundant</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>04h</td>
<td>Non-Redundant: Sufficient from Insufficient</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>05h</td>
<td>Non-Redundant: Insufficient Resources</td>
</tr>
</tbody>
</table>

### Event data byte 2

When a sensor triggers an event in the system event log, event data byte 2 might contain additional information about the event. This event data byte must be read solely on the specific offset listed in the following tables.

<table>
<thead>
<tr>
<th>ID</th>
<th>Sensor</th>
<th>Specific offset</th>
<th>Event data 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>03h</td>
<td>IPMI Watchdog</td>
<td>00h</td>
<td>[7:4] - Interrupt type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>01h</td>
<td>• 0x00 = None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>02h</td>
<td>• 0x10 = SMI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>03h</td>
<td>• 0x20 = NMI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>08h</td>
<td>• 0x30 = Messaging interrupt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0xF0 = Unspecified</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[3:0] - Timer use at expiration:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x00 = Reserved</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x01 = BIOS/FRCB2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x02 = BIOS/POST</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x03 = OS load</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x04 = SMS/OS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x05 = OEM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x0F = Unspecified</td>
</tr>
<tr>
<td>08h</td>
<td>System Event</td>
<td>04h PEF Action</td>
<td>The following bits reflect the PEF Actions that are about to be taken after the event filters have been matched. The event is captured before the actions are taken.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[7:6] - reserved</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x0 = event is first of pair.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x1 = event is second of pair.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[6:4] - reserved</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[3:0] - Timestamp Clock Type</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x0 = SEL Timestamp Clock updated (Also used when both SEL and SDR Timestamp clocks are linked together.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x1 = SDR Timestamp Clock updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 05h Timestamp Clock Synch.</td>
</tr>
<tr>
<td>0Ch</td>
<td>Board Status</td>
<td>00h</td>
<td>Report additional information about the reset type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>02h</td>
<td>Specific offset 00h:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>06h</td>
<td>• 0x02 = Push button reset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>07h</td>
<td>Specific offset 02h:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x04 = Straight to S5 condition</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x0d = Serial port reset</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• All others = Unknown reset cause</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specific offset 06h:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x05 = Cold reset without power cycle</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x0F = Cold reset with power cycle</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specific offset 07h:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x01 = Power reset IPMI command</td>
</tr>
<tr>
<td>25h</td>
<td>Ver Change FPGA</td>
<td>01h</td>
<td>0x11 Version change type is FPGA.</td>
</tr>
<tr>
<td>27h</td>
<td>Ver Change BMC</td>
<td>01h</td>
<td>0x02 Version change type is BMC.</td>
</tr>
</tbody>
</table>
This table defines the event data bytes 2 and 3 for OEM-defined sensors generated from the BIOS SMI Handler (Generator ID = 0x21).

<table>
<thead>
<tr>
<th>ID</th>
<th>Sensor Type</th>
<th>Specific Offset</th>
<th>Event Data 2</th>
<th>Event Data 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>33h</td>
<td>PCI Error</td>
<td>13h (Critical Interrupt)</td>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
</tr>
<tr>
<td>36h</td>
<td>Memory Error</td>
<td>0Ch (Memory)</td>
<td><img src="image3.png" alt="Image" /></td>
<td><img src="image4.png" alt="Image" /></td>
</tr>
<tr>
<td>35h</td>
<td>Processor Error</td>
<td>07h (Processor)</td>
<td><img src="image5.png" alt="Image" /></td>
<td><img src="image6.png" alt="Image" /></td>
</tr>
<tr>
<td>36h</td>
<td>Direct Memory Access (DMA)</td>
<td>07h (Processor)</td>
<td><img src="image7.png" alt="Image" /></td>
<td><img src="image8.png" alt="Image" /></td>
</tr>
<tr>
<td>37h</td>
<td>OutBound Traffic Controller (OTC) Error</td>
<td>07h (Processor)</td>
<td><img src="image9.png" alt="Image" /></td>
<td><img src="image10.png" alt="Image" /></td>
</tr>
<tr>
<td>38h</td>
<td>Inbound Traffic Controller (ITC) Error</td>
<td>07h (Processor)</td>
<td>05h</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>--------------------------------------</td>
<td>-----------------</td>
<td>-----</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[7:4] - CPU Socket Number:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0x0 = CPU1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0x1 = CPU2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[3:1] - CPU Stack Number</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[0] - Current/Last Boot Error:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0x0 = Current Boot</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0x1 = Last Boot</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>39h</th>
<th>Intel VT-d Error</th>
<th>07h (Processor)</th>
<th>05h</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[7:4] - CPU Socket Number:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0x0 = CPU1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0x1 = CPU2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[3:1] - CPU Stack Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[0] - Current/Last Boot Error:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0x0 = Current Boot</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0x1 = Last Boot</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6Ch = Parity error on incoming addr from IRP

[7:0] - Inbound Traffic Controller Error codes as per Skylake-EP EDS Specification:
• 80h = ITC IRP credit underflow
• 81h = ITC IRP credit overflow
• 82h = Parity error in the incoming data from PCIe
• 83h = Parity error in the ITC hdr_q RF
• 84h = Parity error in the ITC vtd_misc_info RF
• 85h = Parity error in the ITC addr_q RF
• 86h = ECC corrected error in the ITC dat_dword RF
• 87h = ECC uncorrected error in the ITC dat_dword RF
• 88h = Completer abort
• 89h = Master abort
• 8Ah = Multicast target error for ITC only

[7:0] - Intel VT-d Local Group error codes as per Skylake-EP EDS Specification:
• 90h = Data Parity Error during Context Cache Lookup
• 91h = Data Parity Error during L1 Lookup
• 92h = Data Parity Error during L2 Lookup
• 93h = Data Parity Error during L3 Lookup
• 94h = TLB0 Data Parity Error
• 95h = TLB1 Data Parity Error
• 96h = Unsuccessful completion status received in the coherent interface
• 97h = Illegal request to 0xFEE
• 98h = Protected Memory region space violated status
• A0h = Intel VT-d spec defined errors
Configuring and using SNMP traps

Setting up SNMP alarms using IPMI

The following procedures will be executed using the Accessing a BMC using IPMI (WCS) method, but some configurations can also be performed using IOL (Accessing a BMC using IPMI over LAN (IOL)). To use IOL, add the IOL parameters to the command: -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password].

NOTE: It is strongly recommended to be familiar with the following sections of the IPMI 2.0 specification:
- 17. Platform Event Filtering (PEF)
- 30. PEF and Alerting Commands
- 23. IPMI LAN Commands

NOTE: The following procedure is a typical configuration of SNMP trap and therefore may require additional customization.

Step_1
Enable Platform Event Filtering (PEF).
LocalServer_OSPrompt:~# ipmitool raw 0x04 0x12 0x1 0x03

Step_2
Enable alerts.
LocalServer_OSPrompt:~# ipmitool raw 0x04 0x12 0x2 0x01

Step_3
Configure destination address
LocalServer_OSPrompt:~# ipmitool raw 0x0c 0x01 [CHANNEL] 0x13 0x1 0x0 0x0 [CHANNEL_IP] [MAC_ADDR]
NOTE: In this case, the management plane would be on channel 1 and the data plane would be on channel 2.

Step_4
Configure an alert associated with the destination.
LocalServer_OSPrompt:~# ipmitool raw 0x0c 0x01 [CHANNEL] 0x12 0x01 0x00 [TIMEOUT_SEC] [RETRY_COUNT]
NOTE: A maximum of 16 event filter can be configured.

Step_5
Configure the alert policy.
LocalServer_OSPrompt:~# ipmitool raw 0x04 0x12 0x9 0x01 0x18 0x21 0x00

Step_6
Configure a new event filter. Refer to Alarm setup examples.
LocalServer_OSPrompt:~# ipmitool raw 0x04 0x12 0x6 0x0d 0x80 0x1 0x1 0x10 0x20 0x00 0x09 0x02 [SENSOR_ID] 0xff 0xff 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
NOTE: A maximum of 16 event filter can be configured.

Alarm setup examples

Detecting an HDD removal
- Event filter: 15

CG2400_User_documentation_2-01-2023 // 213
Alert policy: 1
Severity: informational

Detecting a fan removal
- Event filter: 14
- Alert policy: 1
- Severity: critical

Detecting an AC or DC power lost
- Event filter: 13
- Alert policy: 2
- Severity: critical
## System Inventory

The System Inventory provides information about the CPUs, memory DIMMS, storage, sensors, etc.

### Accessing Inventory

Refer to [Accessing a BMC using the Web UI](#) for access instructions.

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Access the BMC Web UI.</td>
</tr>
<tr>
<td>2</td>
<td>From the left-side menu, click on <strong>System Inventory</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>The system inventory will be displayed.</td>
</tr>
</tbody>
</table>
# Configuring and using SNMP traps in WebUI

## Setting up SNMP traps in WebUI

The following procedures will be executed using the WebUI method.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Go to Settings→ Platform Event Filter</td>
</tr>
<tr>
<td>Step_2</td>
<td>Go to Event Filters</td>
</tr>
</tbody>
</table>
| Step_3 | Choose PEF ID: #  
You can modify or add new event filters from here. By default, 15 event filter entries are configured among the 40 available slots. Choose All option to view available Configured and UnConfigured slots. Choose Configured/Unconfigured option to view available Configured/Unconfigured slots. Choose "x" icon to delete an event filter slot from the list |
| Step_4 | There you can configure your event with all the options within the Event Filter Configuration section |
| Step_5 | You can also configure the Alert Policies under Settings→ Platform Event Filter→ Alert policies→ Group: 1  
It shows all configured Alert policies and available slots. You can modify or add new alert policy entry from here. Click "x" icon to delete an alert policy from the list. A maximum of 60 slots are available. |
| Step_6 | There you can configure your Alert with all the options within Alert Policies section |
| Step_7 | You can also configure the LAN Destinations under |
Settings → Platform Envent
Filter → LAN Destinations →
LAN Channel: 1
This shows all LAN destination slots. You can modify or add a new LAN destination entry from here.
Click ‘x’ icon to delete an entry from the list.
A maximum of 15 slots are available.
Select an applicable LAN Channel from the list.
Send Test Alert: Select a configured slot and click 'Send Test Alert' to generate a sample alert message to the configured destination.
NOTE: Test alert for emails can be sent only when SMTP configuration is enabled. This can be done under 'Settings → SMTP'. Make sure that SMTP server address and port numbers are configured properly.

Step_B
There you can configure your Destination Type with all the options within LAN Destination Configuration.
Telco Alarm Manager

The Telco Alarm Manager (TAM) is a feature component of the BMC firmware. Alarm requests received by the BMC are processed and displayed on the Telco Alarm Panel according to the alarm panel model currently in use.

Telco Alarm Panel

The Telco Alarm Panel provides four indicators corresponding to the three Telco Alarm severities: Critical, Major, Minor and an independent Power alarm indicator.

Telco Alarm Models

The BMC TAM feature supports two different models to determine the state of the Telco Alarm Panel: 'Most Severe Only' model (default) and 'All Severities' model.

'Most Severe Only' Model (default)

With this model, only the Telco Alarm Panel indicator that corresponds to the most critical alarm severity is set. All the other panel indicators are reset. If the "most severe" alarm is a power one, then the "Power" indicator is set; otherwise it is reset.

'All Severities' Model

In this model, only the Telco Alarm Panel indicators that correspond to all asserted alarms are set. The Telco Alarm Panel state may indicate any combination of the three alarm severities. If any alarm is power-related, then the "Power" indicator is set; otherwise it is reset. The power alarm does not necessarily have to be the "most severe" alarm.

Telco Alarm Manager Configuration

The Telco Alarm Manager can be configured over IPMI, with the use of a Kontron OEM command.

Retrieving the Telco Alarm Manager Configuration

The following IPMI command will return the actual TAM configuration byte.
Setting the Telco Alarm Manager Configuration

The following IPMI command will set a new TAM configuration byte. A reset or power cycle of the BMC is required for the new configuration to be effective.

```
# ipmitool raw 0x3c 0x0B 0x00 0x00
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>-- Get TAM configuration</td>
</tr>
<tr>
<td>-- TAM command</td>
</tr>
</tbody>
</table>
 -- Network Function (netfn): OEM command
```

### Configuration Byte

<table>
<thead>
<tr>
<th>Bit position</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0]</td>
<td>Enable/Disable</td>
<td>0: The Telco Alarm Manager feature is <strong>disabled</strong>. The four indicators can be controlled by the user with a dedicated IPMI command. 1: The Telco Alarm Manager feature is <strong>enabled</strong> (default).</td>
</tr>
<tr>
<td>[1]</td>
<td>Telco Alarm Model</td>
<td>0: 'All Severities Only' model. 1: 'Most Severe Only' model (default).</td>
</tr>
<tr>
<td>[2-7]</td>
<td>Unused</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
# Get the TAM configuration
# ipmitool raw 0x3c 0x0B 0x00 0x00
# 00
#
# Set TAM to Enable/'Most Severe Only' mode
# ipmitool raw 0x3c 0x0B 0x00 0x01 0x03
#
# Reset to BMC to apply the configuration change
# ipmitool mc reset cold
#
# Get the TAM configuration to verify
# ipmitool raw 0x3c 0x0B 0x00 0x00
# 03
```
Maintenance
System event log

(This article gives step-by-step instructions to view and manage system event logs.)

Table of contents
- Accessing the SEL using the BMC Web UI
  - Accessing the system event log
  - Clearing the system event log
  - Downloading the system event log
- Accessing the SEL using IPMI via KCS
  - Accessing the system event log
  - Clearing the system event log
  - Setting system event log time
- Known limitation
  - Accessing the SEL using Redfish
  - Accessing the system event log
  - Clearing the system event log

The system event log can be accessed:
- Using the BMC Web UI
- Using IPMI
- Using Redfish

Accessing the SEL using the BMC Web UI

Accessing the system event log

Refer to Accessing a BMC using the Web UI for access instructions.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Access the BMC Web UI of the server.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select Logs &amp; Reports from the left side menu.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select IPMI Event Log from the dropdown menu.</td>
</tr>
<tr>
<td>Step 4</td>
<td>The system event log is displayed.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click on an event and collect the following information: 1. Event ID 2. Associated sensor 3. Description 4. Time asserted</td>
</tr>
</tbody>
</table>

NOTE: Depending on the event, there may not be an associated sensor attribute. However, if this attribute is present, refer to Interpreting sensor data for further interpretation instructions.

Clearing the system event log
**Step_1** In the Event Log menu, select **Clear Event Logs**.

**Step_2** Confirm the action by clicking on **OK**.

### Downloading the system event log

**Step_1** In the Event Log menu, select **Download Event Logs**.

### Accessing the SEL using IPMI via KCS

The following procedures will be executed using the Accessing a BMC using IPMI (KCS) method, but some configurations can also be performed using IOL (Accessing a BMC using IPMI over LAN (IOL)). To use IOL, add the IOL parameters to the command: `-I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password]`.

### Accessing the system event log

**Step_1** From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, access the system event log information.

```
LocalServer_OSPrompt:~$ ipmitool sel
```

**Step_2** Access the system event log list.

```
LocalServer_OSPrompt:~$ ipmitool sel elist
```

**Step_3** Collect the following information for the specified event:
- Event ID - 1st column
- Time asserted - 2nd and 3rd column
- Associated sensor - 4th column (optional)
- Description - 5th column

**NOTE:** Depending on the event, there may not be an associated sensor attribute. However, if this attribute is present, refer to **Interpreting sensor data** for further interpretation instructions.

### Clearing the system event log

**Step_1** From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, clear the system event log.

```
LocalServer_OSPrompt:~# ipmitool sel clear
```

**Step_2** Verify that the system event log was properly cleared.

```
LocalServer_OSPrompt:~# ipmitool sel elist
```

### Setting system event log time

**Step_1** From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, set the system event log time.

```
LocalServer_OSPrompt:~# ipmitool sel time set "[MM/DD/YYYY HH:MM:SS]"
```

**Step_2** Verify that the sel time was properly set.

```
LocalServer_OSPrompt:~# ipmitool sel time get
```

### Known limitation

When setting the system event log time with ipmitool, multiple repeated System Event entries will be present in the SEL list.
This behavior has been observed with the latest version of ipmitool (1.8.18) released to date. However, the latest unreleased version fixes the issue.

To get latest unreleased version:

Step_1
Send the following commands:

git clone https://github.com/ipmitool/ipmitool.git

cd ipmitool

./bootstrap && ./configure && make && sudo make install

Step_2
After the installation of ipmitool, set the "-N 5" flag to use ipmitool sel set time. This flag sets the command timeout to prevent multiple sel event errors to be logged.

ipmitool -H <BMC IP> -U admin -P admin -I lanplus sel time set "11/14/2018 17:06:57" -N 5

Accessing the SEL using Redfish

Accessing the system event log

Refer to Accessing a BMC using Redfish for access instructions.

Step_1
From a remote computer that has access to the management network subnet, open a command prompt and access the system event log.

RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]Managers/Self/LogServices/SEL/Entries | jq

Step_2
Collect the following information for the specified event:

- Description or the EntryCode attribute
- Time asserted or the EventTimestamp attribute
- Event ID or the Id attribute
- Associated sensor or the SensorNumber attribute (optional)

NOTE: Depending on the event, there may not be an associated sensor attribute. However, if this attribute is present, refer to Interpreting sensor data for further interpretation instructions.

Clearing the system event log

Step_1
From a remote computer that has access to the management network subnet, open a command prompt and clear the system event log.


Step_2
Verify that the system event log was properly cleared.

RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]Managers/Self/LogServices/SEL/Entries | jq
Components replacement

(This article gives detailed instructions to safely replace components.)

To replace a component on a CG2400 platform, refer to Components installation and assembly.
# BIOS backup and restore

**Table of contents**
- Backing up the BIOS
- Restoring the BIOS
- Getting information on latest BIOS snapshot
- Description of creation and restoration steps

This article describes how to create a BIOS backup and perform a restore from the backup created. The following procedures are executed using IPMI over LAN. Refer to [Accessing a BMC using IPMI over LAN (IOL)](#).

Note: When sending the raw commands, it will turn off the payload. This is done in order to prevent the BMC from accessing the BIOS flash. Once the procedure is completed, the power will remain off.

## Backing up the BIOS

**Step_1** Backup the BIOS (this saves the BIOS and the configuration).

```
RemoteServer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] raw 0x3c 0x07 0x00 0x00
```

Completion code:
- 0x00: Recovery process started successfully
- 0xd6: Recovery process cannot be started

**Step_2** Verify the BIOS backup status.

```
RemoteServer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] raw 0x3c 0x07 0x00 0x01
```

The completion code is always 0x00.

[Byte0] Status:
- 0x00 = Success/Idle
- 0x01 = In-progress
- 0x02 = Failure

[Byte1] Current step (see [Description of creation and restoration steps](#))
[Byte2] Progress (in percent)

In the image, the status of the snapshot creation is **In-progress**, the current step is **Snapshot MTD Flash erase** and the progress is **4 % completed**.

## Restoring the BIOS

**Step_1** Restore the BIOS (this restores the BIOS and the configuration).

```
RemoteServer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] raw 0x3c 0x07 0x00 0x02
```

Completion code:
- 0x00: Recovery process started successfully
- 0xd6: Recovery process cannot be started

**Step_2** Verify the status of the restoration.

```
RemoteServer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] raw 0x3c 0x07 0x00 0x01
```

The completion code is Always 0x00.

[Byte0] Status:
- 0x00 = Success/Idle
- 0x01 = In-progress
- 0x02 = Failure

[Byte1] Current step (see [Description of creation and restoration steps](#))
[Byte2] Progress (in percent)

In the image, the status of the restoration is **In-progress**, the current step is **Snapshot MTD Flash write** and the progress is **5 % completed**.

## Getting information on latest BIOS snapshot

**Step_1** Get backed up BIOS information.

```
RemoteServer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] raw 0x3c 0x07 0x00 0x03
```

Completion code:
- 0x00: Snapshot is valid
- 0xd6: Snapshot is invalid
[Byte0] Version
[Byte1] Major
[Byte2] Minor
[Byte3:0] Aux
[Byte4:3] Status
[Byte4:0:7:4] Unix timestamp

In the image, the version is **1.33.00000000**, the status is 0x00 and the timestamp is **132531880**.

## Description of creation and restoration steps
<table>
<thead>
<tr>
<th>Step description</th>
<th>Step value (BYTE1)</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshot validation</td>
<td>0x00</td>
<td>Check if the saved snapshot is valid for restoration.</td>
</tr>
<tr>
<td>Check BIOS end of POST</td>
<td>0x01</td>
<td>Check if BIOS is valid and booted before creating a snapshot.</td>
</tr>
<tr>
<td>MTD partition detect</td>
<td>0x02</td>
<td>Check if the Flash device and partition are detected.</td>
</tr>
<tr>
<td>Server Power Off</td>
<td>0x03</td>
<td>Set server to Power Off state.</td>
</tr>
<tr>
<td>Force Intel ME Recovery mode</td>
<td>0x04</td>
<td>Force Intel ME to recovery mode.</td>
</tr>
<tr>
<td>Snapshot MTD Flash erase</td>
<td>0x05</td>
<td>Erasing of the snapshot flash.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Erase progress in percent (%) available in [BYTE2] of get status command (0x01).</td>
</tr>
<tr>
<td>Snapshot MTD Flash write</td>
<td>0x06</td>
<td>Writing of the snapshot flash.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Writing progress in percent (%) available in [BYTE2] of get status command (0x01).</td>
</tr>
<tr>
<td>Snapshot MTD Flash verify</td>
<td>0x07</td>
<td>Verifying of the snapshot flash.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verifying progress in percent (%) available in [BYTE2] of get status command (0x01).</td>
</tr>
<tr>
<td>Reset Intel ME to Normal mode</td>
<td>0x08</td>
<td>Reset Intel ME to return to normal mode.</td>
</tr>
</tbody>
</table>
Upgrading

(This article provides detailed instructions to safely upgrade the platform’s components.)

Table of contents

- General considerations
- Downloading the latest firmware versions
- Upgrading the BMC and the FPGA using ipmitool
  - Prerequisite
  - Procedure
- Upgrading the BIOS and 10GbE LAN
  - Linux method
    - Transferring and uncompressing the package
    - Upgrading the BIOS
    - Upgrading the 10GbE LAN
  - USB key method

General considerations

You may have been informed by Kontron that your running system would benefit from the latest firmware upgrades. Furthermore, newer versions of firmware components were possibly released between the platform manufacturing date and the delivery date. By using the new firmware loads, you will optimize the functionalities of your CG2400. The firmware package download and upgrade procedures are described below.

Downloading the latest firmware versions

Go to https://www.kontron.com/products/systems/telecom-systems/cg2400-carrier-grade-server.html to download the latest firmware versions available for the CG2400.

Then, proceed with the desired upgrade:

- Upgrading the BMC and the FPGA using ipmitool – recommended
- Upgrading the BIOS and 10GbE LAN

Upgrading the BMC and the FPGA using ipmitool

The following procedure will upgrade the BMC and FPGA at the same time.

Prerequisite

| 1 | A community version of ipmitool is installed on a remote computer to enable remote monitoring—it is recommended to use ipmitool version 1.8.18. |

NOTE: The upgrade process can be done with any recent version of ipmitool.

Procedure
### Step 1
From a remote computer that has access to the management network subnet, enter the desired command.

```
```

**NOTE:** The upgrade can be done without a power off and the power status verification; however, when an all activate command is executed, a complete system reboot will occur.

### Step 2
Confirm the server power status is off.

```
```

### Step 3
Verify that the upgrade version is adequate.

```
```

### Step 4
Proceed with firmware upgrade.

```
```

**NOTE:** Wait for the upgrade to finish before performing any action on the platform. If the upgrade is interrupted, it might corrupt the data.

### Step 5
Verify that the different components upgraded properly.

```
```

---

## Upgrading the BIOS and 10GbE LAN

### NOTICE
- Do NOT power off or restart the computer device when the system is reading the BIOS or updating the BIOS.
- To prevent any errors when updating the FLASH, DO NOT remove the hard disk or USB or any devices in any inappropriate way. An incorrect manipulation will result in a BIOS crash and could prevent the board from booting.
- Secure boot must be disabled to perform the upgrades.
- When scripts end, a full power cycle is performed. This also affects the management controller.

### Relevant section:
Accessing the operating system of a server

### Linux method

#### Transferring and uncompressing the package

### Step 1
Transfer the latest upgrade package compressed file (zip or tar.gz) to an installed Linux residing on a storage device (M.2, HDD/SSD) of the CG2400.

### Step 2
From an OS command prompt, uncompress the zip file. **NOTE:** To uncompress a zip file, you might need to install an additional Linux package.

```
tar xzvf <update package tar.gz>
```

**OR**

```
unzip <update package .zip>
```

### Step 3
Select the proper directory.

```
cd bios-bundle-<version>
```

Select the upgrade to perform:
- Upgrading the BIOS
- Upgrading the 10GbE LAN

### Upgrading the BIOS

### Step 1
From an OS command prompt, start the upgrade process.

```
sudo bash ./bios-update.sh
```

### Step 2
Follow the instructions on screen until the upgrade process is finished. Note that the system will reboot a few times.
### Upgrading the 10GbE LAN

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From an OS command prompt, start the upgrade process. &lt;br&gt;<strong>sudo bash ./lan-update.sh</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td>Follow the instructions on screen until the upgrade process is finished.</td>
</tr>
</tbody>
</table>

### USB key method

This method requires a physical access to the system.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Uncompress and copy files to the root of a USB key formatted as FAT32.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Insert the USB key in the CG2400, using the front or rear USB port of the CG2400 platform.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Reset the system. See <a href="#">Platform power management</a> for reset methods.</td>
</tr>
<tr>
<td>Step 4</td>
<td>When the system has restarted, press F6 to activate the boot menu and select USB key. &lt;br&gt;<strong>NOTE:</strong> You can also press F2 or DEL, enter the BIOS menu, go to the Save &amp; Exit tab and select the USB key under Boot Override. Do not press &lt;ESC&gt;. This will bring you in the EFI shell, thus requiring to reboot the CG2400 again to boot from the USB key.</td>
</tr>
<tr>
<td>Step 5</td>
<td>A menu will appear. Select what you want to do: &lt;br&gt;• Exit (press 1) &lt;br&gt;• Update BIOS (press 2) &lt;br&gt;• Update 10Gb LAN (press 3) &lt;br&gt;<strong>NOTE:</strong> The system will perform a full power cycle after updating the BIOS or the 10Gb LAN.</td>
</tr>
</tbody>
</table>
Scaling

(This article provides an overview of scaling considerations and step-by-step instructions to scale components up or down.)

Table of contents
Platform cooling and thermal management

This article provides information about platform cooling and thermal management mechanism and describes specific behavior across platform operating temperature range.

Table of contents
- Platform cooling subsystem
  - CPU heatsinks
  - AC and DC power supply airflow
- Platform thermal management
  - CG2400 aggregated temperature sensors
  - AC and DC power supply thermal protection

Platform cooling subsystem

The CG2400 is equipped with three sets of paired fans ensuring appropriate cooling of basic to complex component arrangements. All system components, except the power distribution board and power supply modules, are cooled by the six fans mounted near the front of the chassis behind the front panel board, as shown in the figure below.

The CG2400 platform has six 80 mm x 38 mm fans, configured as three redundant pairs. There are three cooling zones delimited by the colored dotted lines in the figure above:
- Zone 1 (green dotted lines) contains fans 1 and 2, which cool both CPUs, half of the DIMMs and all the other components in this zone. Air flows through the front bezel to the rear of the chassis (zone 1 arrow).
- Zone 2 (red dotted lines) contains fans 3 and 4, which cool the other half of the DIMMs, the right-side PCI riser assembly, and all the other components in this zone. Air flows through the front bezel to the rear of the chassis (zone 2 arrow).
- Zone 3 (blue dotted lines) contains fans 5 and 6, which cool the six HDDs, the two LP PCI adapters in baseboard slots 3 and 4, the left-side PCI riser assembly and all the other components in this area. Air flows from the front bezel over the drive bay to the fans and then takes two routes for this zone: straight back to the rear of the chassis (left zone 3 arrow) and back over the power supplies to the rear of the chassis (right zone 3 arrow).
- Internal power supply fans as well as system fans 5 and 6 cool the power distribution board (PDB) and power supply modules.

The right riser card assembly (right when facing the front of the platform) sits above the CPU/memory air duct in zone 2. The vertical baffles on the top surface of the CPU/memory air duct combined with the riser card assembly and its sheet metal housing form an air duct for the PCI adapters installed in the right riser card assembly. The left riser card assembly (left when facing the front of the platform) sits above the left-most portion of the baseboard and power supply module 2 in zone 3. The left riser card assembly, its sheet metal housing and the air baffle installed to the left of the riser card assembly form an air duct for the PCI adapters installed in the left riser card assembly.

CPU heatsinks

Both CPU heatsinks are included in platform’s base system (PN CG2400-00). They are packed in individual boxes, along with the chassis, in the platform box. The heatsinks are not identical and need to be installed in the proper configuration to achieve optimal thermal behavior of the platform.

Each heatsink is tagged with a label that indicates its position: "FRONT" or "REAR."

Refer to the figure below for the proper positioning of the heatsinks.
AC and DC power supply airflow

Each power supply has one 40-mm fan for self-cooling. The fans provide no less than 10 CFM of airflow through the power supply when installed in the system and operating at maximum fan speed. The cooling air enters the power supply module from the PDB side. Variable fan speed is based on output load and ambient temperature. Under standby mode, the fans must run at the minimum RPM.

Platform thermal management

The thermal management of the platform is handled by the motherboard’s integrated BMC. The BMC uses information collected from on-board temperature sensors to adjust the speed of the fans and regulate the temperature of the platform according to a PID algorithm. The temperature sensors are aggregated as an input value to the system temperature PID regulator, which provides a speed command for the fans. 

NOTE: For a tailored thermal management solution, it is possible to include up to two additional optional probes in the cooling algorithm to monitor customer specific zones.

See Optional thermal probe for more details.

CG2400 aggregated temperature sensors

<table>
<thead>
<tr>
<th>ID(hex)</th>
<th>Sensor Type</th>
<th>Description</th>
<th>Sensor Type</th>
<th>Event/reading type code</th>
</tr>
</thead>
<tbody>
<tr>
<td>2Th</td>
<td>Front Panel Temp</td>
<td>Temperature of front panel</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>C7h</td>
<td>P1 Temp</td>
<td>Processor 1 Temperature</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>D2h</td>
<td>P2 Temp</td>
<td>Processor 2 Temperature</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>20h</td>
<td>P1 TMax</td>
<td>Processor 1 Temperature maximum temperature/thermal trip (throttling) point.</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>0Fh</td>
<td>P2 TMax</td>
<td>Processor 2 Temperature maximum temperature/thermal trip (throttling) point.</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>B5h</td>
<td>CPU Zone Temp</td>
<td>Temperature of CPU Zone</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>1Eh</td>
<td>PCH Temp</td>
<td>Temperature of PCH</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>BAh</td>
<td>BMC Temp</td>
<td>Temperature of BMC</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>B7h</td>
<td>PCIe A Temp</td>
<td>Temperature of PCIe A (optional Thermal Probe cable*)</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>B9h</td>
<td>PCIe B Temp</td>
<td>Temperature of PCIe B (optional Thermal Probe cable*)</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>B8h</td>
<td>X557 LAN1 Temp</td>
<td>Temperature of X557 LAN 1</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>BCh</td>
<td>X557 LAN2 Temp</td>
<td>Temperature of X557 LAN 1</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>BAh</td>
<td>M.2 Temp</td>
<td>Temperature of M.2 Zone</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>B6h</td>
<td>Battery Temp</td>
<td>Temperature of Battery</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>CBh</td>
<td>P1 DIMMA1 Temp</td>
<td>Temperature of Processor 1 DIMM Channel</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>C9h</td>
<td>P1 DIMMA2 Temp</td>
<td>Temperature of Processor 1 DIMM Channel</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>CAh</td>
<td>P1 DIMMB1 Temp</td>
<td>Temperature of Processor 1 DIMM Channel</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>CBh</td>
<td>P1 DIMMB2 Temp</td>
<td>Temperature of Processor 1 DIMM Channel</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>CHh</td>
<td>P1 DIMMI1 Temp</td>
<td>Temperature of Processor 1 DIMM Channel</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>CFe</td>
<td>P1 DIMMF1 Temp</td>
<td>Temperature of Processor 1 DIMM Channel</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>D3h</td>
<td>P2 DIMMA1 Temp</td>
<td>Temperature of Processor 2 DIMM Channel</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>D4h</td>
<td>P2 DIMMA2 Temp</td>
<td>Temperature of Processor 2 DIMM Channel</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>D5h</td>
<td>P2 DIMMB1 Temp</td>
<td>Temperature of Processor 2 DIMM Channel</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>D6h</td>
<td>P2 DIMMC1 Temp</td>
<td>Temperature of Processor 2 DIMM Channel</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>D7h</td>
<td>P2 DIMMD1 Temp</td>
<td>Temperature of Processor 2 DIMM Channel</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>D8h</td>
<td>P2 DIMMD2 Temp</td>
<td>Temperature of Processor 2 DIMM Channel</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>D9h</td>
<td>P2 DIMMFI Temp</td>
<td>Temperature of Processor 2 DIMM Channel</td>
<td>Temperature (0x01)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>36h</td>
<td>Fan Failure</td>
<td>Current FANs Failure status</td>
<td>Fan (0x04)</td>
<td>0x4</td>
</tr>
<tr>
<td>20h</td>
<td>Fan1 Speed</td>
<td>Current FAN 1 Speed (RPM)</td>
<td>Fan (0x04)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>2Eh</td>
<td>Fan2 Speed</td>
<td>Current FAN 2 Speed (RPM)</td>
<td>Fan (0x04)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>2Fh</td>
<td>Fan3 Speed</td>
<td>Current FAN 3 Speed (RPM)</td>
<td>Fan (0x04)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>30h</td>
<td>Fan4 Speed</td>
<td>Current FAN 4 Speed (RPM)</td>
<td>Fan (0x04)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>31h</td>
<td>Fan5 Speed</td>
<td>Current FAN 5 Speed (RPM)</td>
<td>Fan (0x04)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>32h</td>
<td>Fan6 Speed</td>
<td>Current FAN 6 Speed (RPM)</td>
<td>Fan (0x04)</td>
<td>0x01 (Threshold Based)</td>
</tr>
<tr>
<td>61h</td>
<td>Fan1 Present</td>
<td>Presence state of FAN1</td>
<td>Fan (0x04)</td>
<td>0x8</td>
</tr>
<tr>
<td>62h</td>
<td>Fan2 Present</td>
<td>Presence state of FAN2</td>
<td>Fan (0x04)</td>
<td>0x8</td>
</tr>
<tr>
<td>63h</td>
<td>Fan3 Present</td>
<td>Presence state of FAN3</td>
<td>Fan (0x04)</td>
<td>0x8</td>
</tr>
<tr>
<td>64h</td>
<td>Fan4 Present</td>
<td>Presence state of FAN4</td>
<td>Fan (0x04)</td>
<td>0x8</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
<td>Details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------</td>
<td>----------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>65h</td>
<td>Fan5 Present</td>
<td>Presence state of FAN5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>66h</td>
<td>Fan6 Present</td>
<td>Presence state of FAN6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18h</td>
<td>PS1 Temp</td>
<td>Temperature of Power supply 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19h</td>
<td>PS2 Temp</td>
<td>Temperature of Power supply 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D8h</td>
<td>P1 DTS Thrm Mrgn</td>
<td>Thermal margin before Processor 1 Thermal trip</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCh</td>
<td>P2 DTS Thrm Mrgn</td>
<td>Thermal margin before Processor 1 Thermal trip</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**AC and DC power supply thermal protection**

The power supply subsystem is protected against over-temperature conditions (OTP) caused by loss of fan cooling or elevated ambient temperature. In an over-temperature condition, the +12 V output of the power supply module shuts down. When the power supply temperature lowers within the specified limits, the power supply restores power automatically while the standby power remains on. The OTP circuit features built-in hysteresis to prevent the power supply from oscillating on and off because of temperature recovering conditions. The OTP trip level is set for a minimum of 4°C of ambient temperature hysteresis.
Managing customer-specific sensors

(This article provides information and instructions to monitor and integrate customer-specific sensors in the cooling mechanism of the platform)

Table of contents
- Thermal probe
  - Description
  - Location
  - Probe installation
  - Probe reading
  - Including thermal probes into the platform's cooling algorithm
- Guidelines for setting thermal probe thresholds

Thermal probe

Description

The CG2400 platform offers the flexibility to add up to two specific temperature measurement points by connecting optional temperature probes to the platform's motherboard. The probes have to be installed or affixed near thermal measurement points of interest. For example, a measurement point can be a specific chip or a known hot zone found on a PCIe card. Such probes are included in the temperature sensor list of the fan cooling algorithm and influence the speed of the platform’s fans. For the CG2400 thermal probe ordering part number, click here.

Location

The thermal probes, named PCIe A Temp and PCIe B Temp, are included in the list of IPMI sensors. Refer to the diagram below for the location of their connectors on the motherboard.

![Diagram of thermal probe connectors](image)

Probe installation

For each probe:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Connect the probe’s 3-pin connector to the motherboard. <strong>NOTE:</strong> The connector is keyed to ensure proper connection of the thermal probe to the motherboard.</td>
</tr>
<tr>
<td>Step_2</td>
<td>Affix the thermal probe’s endpoint/transistor to the element to be monitored (e.g. chip). <strong>NOTE:</strong> Kapton tape, hot glue, RTV silicone or any other suitable binding material can be used.</td>
</tr>
<tr>
<td>Step_3</td>
<td>Route the cable in the platform making sure it does not interfere with other components.</td>
</tr>
</tbody>
</table>

Probe reading

PCIe A Temp and PCIe B Temp sensors are always shown in the list of IPMI sensors. They return a ‘No Reading’ value if no thermal probes are installed.

Thermal probes are detected at BMC boot up. Therefore, it is recommended to power down the platform and disconnect power cords prior to installing thermal probes.

Including thermal probes into the platform’s cooling algorithm

The thermal management of the CG2400 platform is handled by the motherboard’s integrated BMC. The BMC uses information collected from on-board temperature sensors to adjust the speed of the fans and to regulate the temperature of the platform according to a PID algorithm. The temperature sensors are aggregated to provide an input value to the system temperature PID regulator, which provides a speed command for the fans. Optional thermal probes, when populated, are part of these temperature sensors’ aggregation process. The PCIe A Temp and PCIe B Temp sensor thresholds must be adjusted according to the desired temperature of the monitored component. The platform’s cooling algorithm regulates the speed of the fans to keep all components just below their Upper Non-Critical threshold value.

Guidelines for setting thermal probe thresholds

- Upper Non-Critical threshold should correspond to the component’s temperature at 100% load, under typical ambient temperature (e.g. 20°C).
- Upper Critical threshold should correspond to the component’s temperature at 100% load, at the upper limit for ambient temperature (e.g. 35°C).

Refer to Configuring sensors for details about sensor threshold modification methods.
Minimum Fan Speed Override

The CG2400 gives the possibility to override the Minimum Fan Speed (available in SUP04 or newer version). This Feature can be useful in particular situations to avoid overheating of parts/elements unmanaged by the CG2400 thermal management. For example, PCIe cards that have no thermal sensors connected to the BMC.

An IPMI OEM command can be sent to override the Minimum Speed value used by the BMC Fan manager.

User can set the value thru 2 ways:

1. Via the BIOS Menu, in the “server mgmt” tab: The current Minimum Fan Speed value will be shown and the possibility to set a new one will be available. The new value is saved by the BMC on “quit and save” of the BIOS Setup menu.
2. Via ipmitool command, as shown below:

```bash
$ # Get current minimal speed (returns 0xA = 10%)
$ ipmitool -H 192.168.1.10 -I lanplus -U admin -P admin raw 0x3c 0xA 0x00 0x01 0xA

$ # Set new minimal speed of 50% (0x32).
$ ipmitool -H 192.168.1.10 -I lanplus -U admin -P admin raw 0x3c 0x0A 0x00 0x01 0x32
```

This Minimum Fan Speed value is saved in non-volatile memory by the BMC, which means that on BMC reboots and/or firmware updates this value is preserved.
Troubleshooting
Collecting diagnostics

(This article explains how to generate system logs.)

Table of contents

- Collecting FRU information
  - Collecting FRU information using the BMC Web UI
  - Collecting FRU information using IPMI
- Collecting the firmware version
  - Collecting the firmware version using the BMC Web UI
  - Collecting the firmware version using IPMI
- Collecting the system event logs
  - Collecting the system event logs using the BMC Web UI
  - Accessing the system event log
  - Downloading the system event log
  - Collecting the system event logs using IPMI

When the support team is contacted, the following data is required to make the proper board health diagnostics:

- FRU information
- Firmware version
- System event log

Collecting all this data beforehand can accelerate the process.

Collecting FRU information

FRU information can be collected:

- Using the BMC Web UI
- Using IPMI

Collecting FRU information using the BMC Web UI

Refer to Accessing a BMC using the Web UI for access instructions.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Access the BMC Web UI of the server.</td>
</tr>
<tr>
<td>Step_2</td>
<td>Select FRU Information from the left side menu.</td>
</tr>
</tbody>
</table>

Step_3 The FRU information is displayed.

![BMC Web UI FRU Information](image)

Collecting FRU information using IPMI

The following procedures will be executed using the Accessing a BMC using IPMI (VCS) method, but some configurations can also be performed using IOL (Accessing a BMC using IPMI over LAN). To use IOL, add the IOL parameters to the command: -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password].

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, access the FRU information. LocalServer_OSPrompt:~$ ipmitool fru print</td>
</tr>
</tbody>
</table>

Collecting the firmware version

The firmware version can be collected:

- Using the BMC Web UI
- Using IPMI
Collecting the firmware version using the BMC Web UI

Refer to Accessing a BMC using the Web UI for access instructions.

| Step 1 | Access the BMC Web UI of the server. |
| Step 2 | From the left side menu, select Maintenance and then Firmware Information. |
| Step 3 | The firmware version is displayed. |

Collecting the firmware version using IPMI

The following procedures will be executed using the Accessing a BMC using IPMI (KCS) method, but some configurations can also be performed using IOL (Accessing a BMC using IPMI over LAN). To use IOL, add the IOL parameters to the command: -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password].

| Step 1 | From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, access the firmware information. |
|         | LocalServer_OSPrompt:~$ ipmitool hpm check |

Collecting the system event logs

System event logs can be collected:
- Using the BMC Web UI
- Using IPMI

Collecting the system event logs using the BMC Web UI

Accessing the system event log

Refer to Accessing a BMC using the Web UI for access instructions.
Step 1: Access the BMC Web UI of the server.

Step 2: Select Logs & Reports from the left side menu.

Step 3: Select IPMI Event Log from the dropdown menu.

Step 4: The system event log is displayed.

Step 5: Click on an event and collect the following information:
1. Event ID
2. Associated sensor
3. Description
4. Time asserted

Downloading the system event log

Step 1: In the Event Log menu, select Download Event Logs.

Collecting the system event logs using IPMI

The following procedures will be executed using the Accessing a BMC using IPMI (KCS) method, but some configurations can also be performed using IOL (Accessing a BMC using IPMI over LAN). To use IOL, add the IOL parameters to the command: -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password].

Step 1: From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, access the system event log information.
```
LocalServer(OSPrompt)~$ ipmitool sel
```

Step 2: Access the system event log list.
```
LocalServer(OSPrompt)~$ ipmitool sel elist
```

Step 3: Collect the following information for the specified event:
- Event ID - 1st column
- Time asserted - 2nd and 3rd column
- Associated sensor - 4th column (optional)
- Description - 5th column
Working with logs

(This article details how to interpret system logs.)

Table of contents
Working with error messages

(This article lists common error messages, their meaning and their troubleshooting steps.)

Table of contents
Networking issues

(This article details common networking issues, their causes and possible solutions.)

Table of contents
Recovering corrupted BIOS

Normal BIOS upgrade process did not completed successfully, BIOS is now corrupted.

Corrupted BIOS can be recovered if a BIOS backup has been generated.
See BIOS backup and restore for details.
Factory default

(This article provides detailed instructions to reset the platform to factory default.)

Table of contents
- Restoring default BIOS settings
  - Restoring default BIOS settings using the BIOS menu
  - Restoring default BIOS settings using IPMI
  - Restoring default BIOS settings using a jumper
- Restoring default BMC settings
  - Restoring default BMC settings using the BMC Web UI
  - Restoring default BMC settings using Redfish

Restoring default BIOS settings

The BIOS settings can be reset to factory default:
- Using the BIOS menu
- Using IPMI
- Using a jumper

Restoring default BIOS settings using the BIOS menu

Refer to Accessing the BIOS for access instruction.

Step 1
From the BIOS setup menu, access the Save & Exit menu and select Restore Defaults. 
**NOTE:** For a shortcut, you can press F3 from anywhere in BIOS menu and answer Yes to “Load Optimized Defaults”.

Step 2
Select Save Changes and Reset. 
**NOTE:** For a shortcut, you can press F4 from anywhere in the BIOS menu and answer Yes to “Save configuration and exit?”

Step 3
Wait for the platform to reset. The BIOS settings should have been reset to default values.

Restoring default BIOS settings using IPMI

The following procedures will be executed using the Accessing a BMC using IPMI via KCS method, operations could also be performed using IOL (Accessing a BMC using IPMI over LAN (IOL)). To use IOL, add the IOL parameters to the command: -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password].

Step 1
Restore default settings.
LocalServer_OSPrompt:~$ ipmitool chassis bootdev none clear-cmos=yes

Step 2
Perform a platform reset. The BIOS settings should be reset to default values.
LocalServer_OSPrompt:~$ ipmitool chassis power reset
**NOTE:** This step needs to be done within 1 minute after the IPMI command has been sent. Otherwise, the BMC will automatically clear the “bootdev” command.

Restoring default BIOS settings using a jumper

Relevant sections:
Safety and regulatory information
Components installation and assembly

Step 1
Power down the CG2400.

Step 2
Put a jumper between pins 11-12 of connector J36 (designated “Clear BIOS or BIOS Default” on the CG2400).

Step 3
Power up the CG2400. The BIOS will reset BIOS settings to “Optimized defaults” (default options are saved at the end of POST, before OS booting).

Step 4
Power down the CG2400.

Step 5
Remove the jumper between pins 11-12 of connector J36.

Step 6
Power up the CG2400. The BIOS settings should still be to optimized defaults.

Restoring default BMC settings

Default BMC settings can be reset to factory default:
Restoring default BMC settings using the BMC Web UI

Refer to Accessing a BMC for access instructions.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step_1</td>
<td>Access the BMC Web UI of the server.</td>
</tr>
<tr>
<td>Step_2</td>
<td>From the left side menu, select <strong>Maintenance</strong> and then <strong>Restore Factory Defaults</strong>.</td>
</tr>
<tr>
<td>Step_3</td>
<td>If necessary, click on <strong>preserve configuration</strong> to change the list of unaffected configurations.</td>
</tr>
<tr>
<td>Step_4</td>
<td>Modify the list of preserved configurations, as required. Click on <strong>Save</strong> and then <strong>Restore Factory Defaults</strong> to return to the previous menu.</td>
</tr>
<tr>
<td>Step_5</td>
<td>Click on <strong>Save</strong>.</td>
</tr>
<tr>
<td>Step_6</td>
<td>Confirm the factory default restoration by clicking on <strong>OK</strong>. <strong>NOTE:</strong> The platform will reset.</td>
</tr>
</tbody>
</table>

Restoring default BMC settings using Redfish

Refer to Accessing a BMC using Redfish for access instructions.
Step 1 | Restore the default BMC settings.
RemoteComputer_OSPrompt:~$ curl -k -s [ROOT_URL]Managers/Actions/RedfishDBReset -X POST -d '{"FactoryResetType":"ResetAll"}' -H "Content-Type: application/json" | jq

Step 2 | Verify the power state. Wait for the power state to be On.

Step 3 | After reset, the BMC settings should have been restored to their default values.
Support information

(This article provides a list of additional support resources.)

Kontron's technical support team can be reached through the following means:

- By phone: 1-888-635-6676
- By email: support-na@kontron.com
- Via the website: www.kontron.com
Scripting - KVM and Network Manager cause SSH session to hang for couple of seconds

NOTES:
This bug is applicable to BMC load 1.01. 0939ACA9
Behavior observed using CentOS 7.3.
KVM refers to H5Viewer window.

Konton observed that an automated routine rebooting the payload and then waiting for the host to ping back again may fail if KVM is opened.
Same routine executes correctly when no KVM is opened.

When a KVM is opened
In the Centos 7.3 console/SSH you can do "ip a" command:

```
1 ip a
```
to list the network interfaces, where USB0 can be seen.

Checking dmesg log, it is observable that USB0 interface causes problem with the Network Manager:
Network Manager hangs, SSH service not being able to start for around 10 seconds.

WORKAROUND: close the KVM window by closing the browser window or using the Stop KVM button.

FIX: situation will be fixed within next CG2400 BMC release.
Raid Controller SNMP

(This section describes how to install and use the snmp agent for broadcom RAID cards)

Table of contents
- Prerequisites
- Installing the RAID controller SNMP
  - Downloading SNMP Installer
  - Extracting the content
- Using the RAID controller SNMP
  - Where are the mibs ?
  - What is the difference between SAS and SAS_IR ?
    - Meaning
    - Difference

Prerequisites

1. Kontron linux snmp-agent is installed and running on the platform. Refer to Configuring Kontron linux snmp-agent on the platform.
2. The net-snmp-utils package is installed. Refer to Common software installation.

NOTE: It is recommended to configure snmpd according to the application requirements before starting to configure RAID Controller SNMP.

Installing the RAID controller SNMP

Download SNMP Installer

The latest version of the SNMP installer from the Broadcom website is recommended. For example purposes, this version will be used throughout the documentation: https://docs.broadcom.com/docs-and-downloads/raid-controllers/raid-controllers-common-files/MR_SAS_SNMP_Installer_6.14-17.05.00.02.zip

Step_1
From, the platform command prompt, download the installer.
LocalServer_OSPrompt:~# wget [SNMP_INSTALLER_URL]

Extracting the content

NOTE: For example purposes, the operating system is Centos 7.3. Please note that commands may vary depending on the operating system installed.

Step_1
Extract the content from the archive.
LocalServer_OSPrompt:~# unzip MR_SAS_SNMP_Installer_6.14-17.05.00.02.zip

Step_2
From the decompressed files, extract the content from the generated archive matching the operating system of the platform.
LocalServer_OSPrompt:~# unzip [ARCHIVE_NAME]

Step_3
Extract the file from the archive generated.
LocalServer_OSPrompt:~# unzip [ARCHIVE_NAME]

Step_4
Extract the content from the following archive:
LocalServer_OSPrompt:~# tar -zvxf sas_snmp_64bit.tar.gz

Installing the software

NOTE: Please note that commands may vary depending on the operating system installed.

Step_1
Install the software
LocalServer_OSPrompt:~# rpm -ivh [RPM_PACKAGE]

Step_2
Restart the snmpd and th ksnmpd service using the following commands:
LocalServer_OSPrompt:~# service snmpd restart
LocalServer_OSPrompt:~# service ksnmpd restart

Using the RAID controller SNMP
<table>
<thead>
<tr>
<th>Step</th>
<th>Using the mib file and the command below, you should get all the information about your controller.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LocalServer_OSPrompt:~# snmpwalk -v 2c -c public -m /etc/lsi_mrdsnmp/sas/LSI-AdapterSAS.mib localhost 1.3.6.1.4.1.3582.4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Use this command to see the physical devices table.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LocalServer_OSPrompt:~# snmptable -v 1 -c public -m /etc/lsi_mrdsnmp/sas/LSI-AdapterSAS.mib localhost 1.3.6.1.4.1.3582.4.1.4.2.1.2</td>
</tr>
</tbody>
</table>

**Where are the mibs?**

In the current setup (Centos 7.3), the mib file is located at: `/etc/lsi_mrdsnmp/sas/LSI-AdapterSAS.mib`

**What is the difference between SAS and SAS_IR?**

**Meaning**

The SAS-IR stand for Integrated Raid.

This example uses the SAS implementation (megaraid_sas). The platform's RAID card is physically plugged into the PCIe Slot.

**Difference**

The SNMP difference between SAS and SAS-IR,

If the SAS version is installed, this OID needs to be used to get the data: `1.3.6.1.4.1.3582.4.1.4.2.1.2`

If the SAS-IR version is installed, this OID needs to be used to get the data: `1.3.6.1.5.1.3582.4.1.4.2.1.2`
Application notes
Secure Erase

Table of contents
- Secure Erase on a SATA disk
  - Prerequisites
  - Procedure
- Secure Erase on an NVME disk
  - Prerequisites
  - Procedure
- Known issues
  - Command time-out during erase with larger drives

NOTE: After a Secure Erase, all data on the disk will be deleted and can not be recovered by any means.

Secure Erase on a SATA disk

Prerequisites

1. An OS is installed.
2. Option HDD Security Freeze Lock BIOS is disabled.
3. The `hdparm` command line tool is installed on the local server — it is recommended to use `hdparm` version 9.58.

Relevant sections:
- Basic BIOS - Secure Erase
- Common software installation

Procedure

Refer to Accessing the operating system of a server for access instructions.

Step_1
Retrieve the disk device name.

LocalServer_OSPrompt:~# ls -al /dev/disk/by-id

Step_2
Verify that the disk is not frozen.

LocalServer_OSPrompt:~# hdparm -I [DEVICE_NAME]

Step_3
Verify that the disk contains data.

LocalServer_OSPrompt:~# df [DEVICE_NAME]

Step_4
Set disk password.

LocalServer_OSPrompt:~# hdparm --user-master [USER] --security-set-pass [PASSWORD] [DEVICE_NAME]

Step_5
Perform Secure Erase on the disk.

LocalServer_OSPrompt:~# hdparm --user-master [USER] --security-erase [PASSWORD] [DEVICE_NAME]

Step_6
Verify that the data has been erased.

LocalServer_OSPrompt:~# df [DEVICE_NAME]

Secure Erase on an NVME disk

Prerequisites

1. An OS is installed.
2. Option HDD Security Freeze Lock BIOS is disabled.
3. The `nvme-cli` command line tool is installed on the local server.

Relevant sections:
- Basic BIOS - Secure Erase
- Common software installation
Refer to Accessing the operating system of a server for access instructions.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Command Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>List NVME devices and get device name.</td>
<td><code>LocalServer_OSPrompt:~# nvme list</code></td>
</tr>
<tr>
<td>2</td>
<td>Get NVME device properties. Formatting and secure erase need to be supported.</td>
<td><code>LocalServer_OSPrompt:~# nvme id-ctrl -H [DEVICE_NAME]</code></td>
</tr>
<tr>
<td>3</td>
<td>Get IBAF format type.</td>
<td><code>LocalServer_OSPrompt:~# nvme id-ns [DEVICE_NAME]</code></td>
</tr>
<tr>
<td>4</td>
<td>Perform Secure Erase on the NVME disk.</td>
<td><code>LocalServer_OSPrompt:~# nvme format --ibaf=[IBAF] --ses=1 [DEVICE_NAME]</code></td>
</tr>
</tbody>
</table>

**Known issues**

**Command time-out during erase with larger drives**

The versions of hdparm that came before version 9.31 hard-coded the time-out for the erase command to 2 hours.

If your drive requires longer than 2 hours to perform a security erase, then it will be reset part-way through the erase command.

If your drive reports that it needs longer than 120 minutes to perform the security erase operation, then you should ensure that you are using version 9.31 or a newer version.

If such a time-out has occurred, the output of the “time” command will be just slightly longer than 120 minutes, and the drive will not be erased correctly.

The drive will be reset when the time-out occurs, and while this appeared to do no harm to a 1GB Seagate ES.2, it is probably not a very well tested part of the drive firmware and should be avoided. In the case of the Seagate, the password was still enabled after the partial-erase and subsequent time-out/reset.
StorCLI utility

This article covers the basic instructions to configure and operate the StorCLI utility.

Table of contents
- References
  - StorCLI documentation
  - Software download URL
- Vocabulary
  - Command arguments
  - Abbreviations
- Installing StorCLI
  - Prerequisites
  - Compatibility list
  - Installation
  - Installing StorCLI on CentOS / RHEL
  - Installing StorCLI on Debian / Ubuntu
  - Installing StorCLI on Windows
- Using the StorCLI utility
  - Commands
    - Help
    - Show
    - Add
    - Delete
    - Set
  - Foreign configuration
    - Display foreign configuration
    - Delete foreign configuration
    - Import foreign configuration
  - Migrate RAID configuration
    - Adding a drive to an existing drive group
    - Remove a drive from a RAID
    - Possible RAID configurations
  - Global Hot Spare
    - Set a drive as Global Hot Spare
    - Delete a Global Hot Spare drive

The StorCLI utility lets users manage the RAID controller cards within the platform’s operating system.

References

StorCLI documentation

This application note only covers the basic configuration and operation procedures. For further details, refer to Broadcom documentation at https://docs.broadcom.com/docs/MR-TM-StorCLI-UG102.

The PDF file provided by Broadcom contains more focused information about the software.

Software download URL

To download the Intel software package, go to https://downloadcenter.intel.com/download/29533/StorCLI-Standalone-Utility

Vocabulary

Command arguments

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>/cx</td>
<td>Controller specific commands</td>
</tr>
<tr>
<td>/ex</td>
<td>Enclosure specific commands</td>
</tr>
<tr>
<td>/sx</td>
<td>Slot/PD specific commands</td>
</tr>
<tr>
<td>/vx</td>
<td>Virtual drive specific commands</td>
</tr>
<tr>
<td>/dx</td>
<td>Disk group specific commands</td>
</tr>
<tr>
<td>/fall</td>
<td>Foreign configuration specific commands</td>
</tr>
<tr>
<td>/px</td>
<td>Phy specific commands</td>
</tr>
<tr>
<td>/bbu or /cv</td>
<td>Battery Backup Unit or Cachevault commands</td>
</tr>
<tr>
<td>/jbd/x</td>
<td>JBOD drive specific commands</td>
</tr>
</tbody>
</table>

NOTE: The x in an argument represents the ID of a specific element.

Abbreviations
<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>EID</td>
<td>Enclosure ID</td>
</tr>
<tr>
<td>Slt</td>
<td>Slot Number</td>
</tr>
<tr>
<td>VD</td>
<td>Virtual Drive</td>
</tr>
<tr>
<td>DID</td>
<td>Device ID</td>
</tr>
<tr>
<td>DG</td>
<td>Drive Group</td>
</tr>
<tr>
<td>DHS</td>
<td>Dedicated Hot Spare</td>
</tr>
<tr>
<td>UGood</td>
<td>Unconfigured Good</td>
</tr>
<tr>
<td>GHS</td>
<td>Global Hot Spare</td>
</tr>
<tr>
<td>UBad</td>
<td>Unconfigured Bad</td>
</tr>
<tr>
<td>Online</td>
<td>Online</td>
</tr>
<tr>
<td>Offline</td>
<td>Offline</td>
</tr>
<tr>
<td>Intf</td>
<td>Interface</td>
</tr>
<tr>
<td>Med</td>
<td>Media Type</td>
</tr>
<tr>
<td>SED</td>
<td>Self Encryptive Drive</td>
</tr>
<tr>
<td>PI</td>
<td>Protection Info</td>
</tr>
<tr>
<td>SeSz</td>
<td>Sector Size</td>
</tr>
<tr>
<td>Sp</td>
<td>Spun</td>
</tr>
<tr>
<td>U</td>
<td>Up</td>
</tr>
<tr>
<td>D</td>
<td>Down/PowerSave</td>
</tr>
<tr>
<td>T</td>
<td>Transition</td>
</tr>
<tr>
<td>F</td>
<td>Foreign</td>
</tr>
<tr>
<td>UGUnsp</td>
<td>Unsupported</td>
</tr>
<tr>
<td>UGShld</td>
<td>UnConfigured Shielded</td>
</tr>
<tr>
<td>HSPShld</td>
<td>Hotspare Shielded</td>
</tr>
<tr>
<td>CFShld</td>
<td>Configured Shielded</td>
</tr>
<tr>
<td>Cpybck</td>
<td>Copyback</td>
</tr>
<tr>
<td>CBShld</td>
<td>Copyback Shielded</td>
</tr>
</tbody>
</table>

### Installing StorCLI

#### Prerequisites

1. The OS installed on the platform is supported by the Broadcom StorCLI software. Refer to pages 6 and 7 of the [StorCLI documentation](#).
2. The RAID controller cards installed are in line with the [Compatibility list](#).
3. The Intel StorCLI package has been downloaded from the [Software download URL](#).

#### Compatibility list

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Manufacturer P/N and description</th>
<th>Kontron P/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel</td>
<td>RS3DC080 SCM xB PCIe 3.0 LSI SAS3108 RAID-On-Chip</td>
<td>1061-7348</td>
</tr>
<tr>
<td>Intel</td>
<td>RS3DC040 RAID-CTRL_RS3DC040_PCIE_4x-SAS/SATA</td>
<td>1062-0561</td>
</tr>
<tr>
<td>LSI/Broadcom</td>
<td>MegaRAID SAS 9341-8i (Support up to 8 HDD/SSD)</td>
<td>1065-7734</td>
</tr>
<tr>
<td>LSI/Broadcom</td>
<td>MegaRAID SAS 9341-4i (Support up to 4 HDD/SSD)</td>
<td>1065-7736</td>
</tr>
<tr>
<td>LSI/Broadcom</td>
<td>MegaRAID SAS 9361-8i (8-port)</td>
<td>1065-5999</td>
</tr>
<tr>
<td>LSI/Broadcom</td>
<td>MegaRAID SAS 9361-4i (4-port)</td>
<td>1065-7726</td>
</tr>
</tbody>
</table>

#### Installation

**NOTE:** For detailed explanations, refer to the [StorCLI documentation](#) - Chapter 2.5, pages 8 and 9.

StorCLI can be installed:
- On CentOS / RHEL
- On Debian / Ubuntu
- On Windows
Installing StorCLI on CentOS / RHEL

**NOTE:** To perform the following instructions, root privileges are required.

<table>
<thead>
<tr>
<th>Step_1</th>
<th>Download the package from the following URL.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~# wget <a href="https://downloadmirror.intel.com/27654/eng/StorCLI_MR7.4p1.zip">https://downloadmirror.intel.com/27654/eng/StorCLI_MR7.4p1.zip</a></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_2</th>
<th>Unzip the archive downloaded from the Intel website.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~# unzip StorCLI_MR7.4p1.zip</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_3</th>
<th>Navigate to StorCLI_MR7.4p1/Linux and execute the following commands.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~# rpm -Uvh storcli-007.0415.0000.0000-1.noarch.rpm</td>
<td></td>
</tr>
<tr>
<td>LocalServer_OSPrompt:~# ln -s /opt/MegaRAID/storcli/storcli64 /bin/storcli</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_4</th>
<th>Reboot the operating system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~# reboot</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_5</th>
<th>Test the StorCLI installation by displaying the version number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~# storcli -v</td>
<td></td>
</tr>
</tbody>
</table>

Installing StorCLI on Debian / Ubuntu

**NOTE:** To perform the following instructions, root privileges are required.

<table>
<thead>
<tr>
<th>Step_1</th>
<th>Download the package from the following URL.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~# wget <a href="https://downloadmirror.intel.com/27654/eng/StorCLI_MR7.4p1.zip">https://downloadmirror.intel.com/27654/eng/StorCLI_MR7.4p1.zip</a></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_2</th>
<th>Unzip the archive downloaded from the Intel website.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~# unzip StorCLI_MR7.4p1.zip</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_3</th>
<th>Navigate to StorCLI_MR7.4p1/Ubuntu and execute the following commands.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~# dpkg -i storcli_007.0415.0000.0000_all.deb</td>
<td></td>
</tr>
<tr>
<td>LocalServer_OSPrompt:~# ln -s /opt/MegaRAID/storcli/storcli64 /bin/storcli</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_4</th>
<th>Reboot the operating system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~# reboot</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_5</th>
<th>Test the StorCLI installation by displaying the version number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~# storcli -v</td>
<td></td>
</tr>
</tbody>
</table>

Installing StorCLI on Windows

**NOTE:** To perform the following instructions, administrator privileges are required.

<table>
<thead>
<tr>
<th>Step_1</th>
<th>Download the .zip file from the Software download URL and extract the content from it.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_2</th>
<th>Open a command prompt with administrator privileges and navigate to the extracted folder.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~# dir StorCLI_MR7.4p1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_3</th>
<th>Execute the storcli64.exe file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~# start storcli64.exe</td>
<td></td>
</tr>
</tbody>
</table>

Using the StorCLI utility

**Commands**

The commands described in this section are:

- **Help**
- **Show**
- **Add**
- **Delete**
- **Insert**
- **Set**

**Help**

**NOTE:** For detailed explanations, refer to the StorCLI documentation - Chapter 2.5, pages 9 to 11.
Step 1. To retrieve possible commands use the `storcli` command.

`LocalServer_OSPrompt:~# storcli`

Step 2. To retrieve all possible commands use the `help` command.

`LocalServer_OSPrompt:~# storcli help`

Step 3. Add the `help` keyword in order to access more precise information about the specified command.

`LocalServer_OSPrompt:~# storcli [COMMAND] help`

Show

The `show` command displays the list of available elements.

**NOTE:** For detailed explanations, refer to the StorCLI documentation - Chapter 2.6.1, pages 11 and 12. Here are examples of show commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>LocalServer_OSPrompt:~# storcli /c0 show</code></td>
<td>Shows details about the first controller.</td>
</tr>
<tr>
<td><code>LocalServer_OSPrompt:~# storcli /c0 /p0 show</code></td>
<td>Shows details about the first physical drive of the first controller.</td>
</tr>
<tr>
<td><code>LocalServer_OSPrompt:~# storcli /c0 /v0 show</code></td>
<td>Shows details about the first virtual drive of the first controller.</td>
</tr>
<tr>
<td><code>LocalServer_OSPrompt:~# storcli /c0 show all</code></td>
<td>Shows all details about the first controller.</td>
</tr>
<tr>
<td><code>LocalServer_OSPrompt:~# storcli /c0 /v0 show all</code></td>
<td>Shows all details about the first virtual drive of the first controller.</td>
</tr>
</tbody>
</table>

Add

The `add` command creates a new element to a controller. Immediately after adding a new element, the drive will automatically be available in the operating system. There is no need to reboot the system.

**NOTE:** For detailed explanations, refer to the StorCLI documentation - Chapter 2.6.4.1, pages 38 to 40.
Step_1  Display all the physical drives.
LocalServer_OSPrompt:~# storcli /[CX] show

Step_2  Add and configure a virtual drive.

Step_3  Initialize the drive.
LocalServer_OSPrompt:~# storcli /[CX]/[VX] start init full force

Step_4  Monitor initialization.
LocalServer_OSPrompt:~# storcli /[CX]/[VX] show init

Step_5  Verify consistency after initialization has succeeded.
LocalServer_OSPrompt:~# storcli /[CX]/[VX] start cc

Step_6  Verify that the drive is added to the controller.
LocalServer_OSPrompt:~# storcli /[CX] show

Step_7  Verify that the drive is available in the operating system of the platform.
LocalServer_OSPrompt:~# lsblk

Delete
NOTE: For detailed explanations, refer to the StorCLI documentation - Chapter 2.6.4.2, pages 40 and 41.

The delete commands described in this section are:
- Deleting a virtual drive
- Deleting a hot spare drive from a virtual drive

Deleting a virtual drive
NOTE: The drive will automatically be removed from the OS after executing this procedure.

Step_1  Display every element of the controller.
LocalServer_OSPrompt:~# storcli /[CX] show

Step_2  Delete the virtual drive.
LocalServer_OSPrompt:~# storcli /[CX]/[VX] del

Step_3  Confirm suppression has succeeded.
LocalServer_OSPrompt:~# storcli /[CX] show

Deleting a hot spare drive from a virtual drive
NOTE: The hot spare drive is identified as DHS in the drive list.

Step_1  Display every element of the controller.
LocalServer_OSPrompt:~# storcli /[CX]/[EX] show

Step_2  Delete the hot spare drive.
LocalServer_OSPrompt:~# storcli /[CX]/[EX]/[SX] delete hotsparedrive

Step_3  Confirm suppression has succeeded.
LocalServer_OSPrompt:~# storcli /[CX]/[EX] show
**Insert**

The _**insert**_ command replaces the configured drive that is identified as missing.

**NOTE:** For detailed explanations, refer to the [StorCLI documentation](https://www.kontron.com) - Chapter 2.6.3.2, pages 28 and 29.

---

**Step 1**
Retrieve the drive group, array and row.

LocalServer_OSPrompt:~# `storcli /[CX] show`

LocalServer_OSPrompt:~# `storcli /[CX]/dall show`

---

**Step 2**
(Optional)
Set the drive to UGood.

LocalServer_OSPrompt:~# `storcli /[CX]/[EX]/[SX] set good force`

---

**Step 3**
Insert the drive into the drive group.

LocalServer_OSPrompt:~# `storcli /[CX]/[EX]/[SX] insert dg=1 array=0 row=1`

**NOTE:** If the setting that allows automatic rebuild (GHS) is enabled, this step is unnecessary.

---

**Step 4**
Set the drive state to _**online**_.

LocalServer_OSPrompt:~# `storcli /[CX]/[EX]/[SX] set online`

---

**Step 5**
Get the rebuild progress.

LocalServer_OSPrompt:~# `storcli /[CX]/[EX]/[SX] show rebuild`

---

**Set**

**NOTE:** For detailed explanations, refer to the [StorCLI documentation](https://www.kontron.com) - Chapter 2.6.2, pages 12 to 18.

The set commands described in this section are:

- Set drive state
- Set alarm actions
- Set EGHS configuration

---

**Set drive state**

**NOTE:** For detailed explanations, refer to the [StorCLI documentation](https://www.kontron.com) - Chapter 2.6.3.3, pages 29 and 30.

**Step 1**
Display all drives and identify the drive’s state.

LocalServer_OSPrompt:~# `storcli /[CX] show`

---

**Step 2**
Set the drive state using one of the following states:

- Unconfigured good (good)
- JBOD (jbod)
- Online (online)
- Offline (offline)
- Missing (missing)
- Boot drive (bootdrive=[on|off])

LocalServer_OSPrompt:~# `storcli /[CX]/[EX]/[SX] set [STATE]`

**OR**
Configure all drives with one command.

LocalServer_OSPrompt:~# `storcli /[CX]/[EX]/sallset [STATE]`

---

**Step 3**
Display all drives using the following command to ensure the states updated successfully.

LocalServer_OSPrompt:~# `storcli /[CX] show`

---

**Set alarm actions**
Enable or disable an alarm on critical errors. The option silence silences the alarm.

Possible values:
- on
- off
- silence

Set EGHS configuration

This command is used to configure the emergency rebuild:
- State – enables or disables the service.
- Smarter – sets the service to replace predictive failed drive or not.
- EUG – sets the EUG drive to be used automatically for rebuild or not.

Set the EGHS configuration.

Possible values for state | smarter | eug:
- on
- off

Foreign configuration

When a drive already contains a configuration from another controller, the controller will identify it as a foreign configuration.

NOTE: For detailed explanations, refer to the StorCLI documentation - Chapter 2.6.6, pages 51 and 52.

The foreign configuration commands described in this section are:
- Display foreign configuration
- Delete foreign configuration
- Import foreign configuration

Display foreign configuration

Display all the drives considered as foreign configured.

LocalServer_OSPrompt:~# storcli /[CX]/fall show all

Delete foreign configuration

Delete the foreign configuration.

LocalServer_OSPrompt:~# storcli /[CX]/fall del

Import foreign configuration

Import a foreign configuration.

LocalServer_OSPrompt:~# storcli /[CX]/fall import

Migrate RAID configuration

NOTE: For detailed explanations, refer to the StorCLI documentation - Chapter 2.6.4.8, pages 45 to 47.

This section describes the following:
- Adding a drive to an existing drive group
- Removing a drive from a RAID
- Possible RAID configurations

Adding a drive to an existing drive group

Add a drive to an existing drive group.

LocalServer_OSPrompt:~# storcli /[CX]/[VX] start migrate type=[RAID_TYPE] option=add drives=[DRIVES]

Removing a drive from a RAID

Remove a drive from a RAID.

LocalServer_OSPrompt:~# storcli /[CX]/[VX] start migrate type=[RAID_TYPE] option=remove drives=[DRIVES]

Possible RAID configurations
Initial RAID level | Migrated RAID level
--- | ---
RAID 0 | RAID 1
RAID 0 | RAID 5
RAID 0 | RAID 6
RAID 1 | RAID 0
RAID 1 | RAID 5
RAID 1 | RAID 6
RAID 5 | RAID 0
RAID 5 | RAID 6
RAID 6 | RAID 0
RAID 6 | RAID 5

**Global Hot Spare**

**NOTE:** For detailed explanations, refer to the [StorCLI documentation](https://www.kontron.com) - Chapter 2.6.3.12, pages 35 and 36.

The commands described in this section are:

- Setting a drive as Global Hot Spare
- Deleting a Global Hot Spare drive

**Set a drive as Global Hot Spare**

**Step_1**

Set a drive as Global Hot Spare.

```
LocalServer_OSPrompt:~# storcli /[CX]/[VX]/[SX] add hotsparedrive
```

**Delete a Global Hot Spare drive**

**Step_1**

Delete a Global Hot Spare drive.

```
LocalServer_OSPrompt:~# storcli /[CX]/[VX]/[SX] delete hotsparedrive
```
Software RAID (VRoC)

- **Introduction**
  - Supported RAID
  - How to enable the RAID options
  - UEFI
    - VRoC SATA Driver
      - Main Menu
      - Create RAID
      - Delete RAID
  - Legacy
    - VRoC Option ROM
    - Accessing the Management Console
    - Hardware Specification
    - VRoC Option ROM & Dashboard
    - Raid Creation
    - Raid Deletion
    - Raid to Non-Raid
    - How the OS manage the RAID ?
    - Can an OS be install on this volume ?
      - Ubuntu 16.04
      - Centos 7.4

**Introduction**

VRoC (Virtual RAID on CPU) is the new name for RSTe (A.K.A "Fake RAID" or "Software RAID). This is a RAID solution implemented in software/firmware.

**Supported RAID**

VRoC support many types of RAID
- RAID 0 (2 Disks minimum)
- RAID 1 (2 Disks minimum)
- RAID 5 (3 Disks minimum)
- RAID 10 (4 Disks minimum)

**How to enable the RAID options**

In order to use VRoC, you need to put the SATA Controller in RAID mode
1. Go into the BIOS Setup Utility, Platform Configuration → PCH Configuration → PCH SATA Configuration → Configure SATA as → RAID
2. Other options are necessary to make it works, but are different depending on if you will be using UEFI or Legacy setup
3. Save and reset (F4)

Install at least 1 drive in the front drive array (in order to see the menu)
Go into the BIOS Setup Utility, Advanced will have an entry called "Intel(R) VRoC SATA Controller"

**UEFI**

**VROC SATA Driver**

**Main Menu**

![Main Menu Image]
Create RAID

Choose the RAID Type (0 or 1)
Choose which drive will be used.
Choose the capacity

The RAID is a software RAID, the size and type can be different using multiple partition with same drives.

The VRDC Module allow to create up to two different RAID using the same Drives.

Delete RAID

Choose the RAID from the main menu list, then choose Delete and apply the change.

Legacy
VRoC Option ROM

The Option ROM is only available when at least one drive is plugged in the SATA/SAS front module.

Acceding the Management Console

In order to access the Management console in Legacy, user must
1. Go into the BIOS Setup Utility, Platform Configuration → PCH Configuration → PCH SATA Configuration → Configure SATA as → RAID
2. Go to Advanced → CSM Configuration → CSM Support → Enabled
3. Put the Option ROM execution → Storage → Legacy
4. Put the Option ROM execution → Video → Legacy
5. Then, Put the Option ROM Messages → Force BIOS
6. Save and Reset (F4)

To access the Management console, during the boot, press CTRL+I

WARNING : CTRL+I only works via the Serial Console Redirection

Hardware Specification

The CG2400M system is limited to six drives connected in the front bay.

VRoC Option ROM & Dashboard

![Image of VRoC Option ROM & Dashboard]

Raid Creation

The tool provide by the Option ROM allow to create easily a RAID 0, 1, 5 or 10

To change the Raid option, use the up/down arrow
To navigate through the menu, use the TAB

Raid Deletion

Choose the Volume. Press DEL

Raid to Non-Raid

Convert a raid array to non-raid (Restore the configuration to default). This is the equivalent of a JBOD option.
To select a drive, use SPACE.
To complete the process, Press ENTER.
How the OS manage the RAID?

The Linux see a mdadm RAID.

```
[root @SYSTEM ]# lsblk
...
   sdd  8:0 894 .3G  0 disk
   -md126 9:126 0 1.7T 0 raid0
   sde  8:64 894 .3G  0 disk
   -md126 9:126 0 1.7T 0 raid0
```

Can an OS be install on this volume?

**Ubuntu 16.04**

The installation works and the entire system is running on the RSTE RAID.
(During the installation, the root / has been set to the RAID volume)

**Centos 7.4**

Using a kickstart installation script, the process go through automatically and the installation work successfully.
CG2400 in 10/100Mbps infrastructure

CG2400 Built-in 10GbE ports can operate at 1 or 10GbE. Kontron recommends the use of an additional PCIe (NIC) card to deploy the CG2400 in a 10 or 100Mbps only infrastructure. Intel I350, 2 or 4 ports, is a good example of such a compatible product since ports are 10,100 and 1000 Mbps capable. This product is available under Kontron Part Number 1059-8279.

PXE Boot configuration

Below is the procedure to get the I350 NIC card configured and ready to PXE boot. Before configuring your NIC card, you will be able to see the additional interfaces in the operating system, but cards and associated Ethernet interfaces will not be available in the BIOS menu, unless you do the following procedure.

Bootutil installation

Links

<table>
<thead>
<tr>
<th>Download center link</th>
<th><a href="https://downloadcenter.intel.com/download/29137v=1">https://downloadcenter.intel.com/download/29137v=1</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootutil documentation</td>
<td><a href="https://downloadmirror.intel.com/29137/eng/bootutil.txt">https://downloadmirror.intel.com/29137/eng/bootutil.txt</a></td>
</tr>
<tr>
<td>Tool for Linux</td>
<td><a href="https://downloadmirror.intel.com/29137/eng/Preboot.tar.gz">https://downloadmirror.intel.com/29137/eng/Preboot.tar.gz</a></td>
</tr>
</tbody>
</table>

Installation procedure

<table>
<thead>
<tr>
<th>Step_1</th>
<th>Get the archive from the following link.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~#</td>
<td><code>wget https://downloadmirror.intel.com/29137/eng/Preboot.tar.gz</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_2</th>
<th>Extract the content of the archive.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~#</td>
<td><code>tar xvzf Preboot.tar.gz</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_3</th>
<th>Change directory.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~#</td>
<td><code>cd APPS/BootUtil/Linux_x64/</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_4</th>
<th>Make the file executable.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~#</td>
<td><code>chmod +x bootutil64e</code></td>
</tr>
</tbody>
</table>

Interface configuration

<table>
<thead>
<tr>
<th>Step_1</th>
<th>List the current settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~#</td>
<td><code>./bootutil64e</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_2</th>
<th>Identify which interfaces are the one associated to your 10/100/1000 Mbps NIC card (NIC number 3 and 4 in the example below) and enable FLASH using the following command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~#</td>
<td><code>./bootutil64e -FLASHENABLE NIC=[PORT_NUMBER]</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_3</th>
<th>To apply the modifications, reboot the system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalServer_OSPrompt:~#</td>
<td><code>reboot</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step_4</th>
<th>Access the BIOS menu. Refer to Accessing the BIOS for access instructions.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Step_5</th>
<th>From the Boot menu, navigate to Boot Option Priorities. You should be able to configure the network interfaces as a boot option.</th>
</tr>
</thead>
</table>

Download center link | https://downloadcenter.intel.com/download/29137v=1 |
Bootutil documentation | https://downloadmirror.intel.com/29137/eng/bootutil.txt |
Tool for Linux | https://downloadmirror.intel.com/29137/eng/Preboot.tar.gz |
Provisioning custom secure boot keys

Table of contents
- Introduction
  - Updating secure boot keys from the UEFI setup utility
    - Prerequisites
    - Procedure

Introduction

This article describes how to provision a custom set of Secure Variables used as part of the Secure Boot feature. Secure Boot is a UEFI-defined feature used to authenticate a UEFI executable, such as an OS loader, using digital signing mechanisms based on the Public Key Infrastructure process, reducing the risks of pre-boot malware attacks. The feature uses a database of authorized signatures to confirm the UEFI executable integrity prior to execution. Boards will typically have a pre-loaded set of Platform Key (PK), Key Exchange Keys (KEK), authorized signature database (db) and blacklisted / revoked signature database (dbx) as defined by the OEM, as well as some industry-standard certificates issued by Microsoft that allow booting Windows or well-known Linux distributions such as Ubuntu. It may be desirable for an end customer to update these keys with their own set for security reasons. This document assumes the reader has some knowledge about the Secure Boot process, and that the required set of keys and certificates has been properly generated. The following link provides guidelines on creating and managing such keys and certificates:
https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/windows-secure-boot-key-creation-and-management-guidance

Updating secure boot keys from the UEFI setup utility

Prerequisites

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A set of Secure Boot keys has been created (PK, KEK and db).</td>
</tr>
<tr>
<td>2</td>
<td>Public Key certificates that are to be provisioned are in DER format.</td>
</tr>
<tr>
<td>3</td>
<td>Public Key certificates are present on a FAT-partitioned USB drive, which is connected to the board. If Virtual Media redirection is available, it is also possible to use a corresponding ISO image instead.</td>
</tr>
</tbody>
</table>

As the current time is verified against certificate timestamps as a security measure, make sure the system time is valid prior to manipulating Secure Boot variables. Otherwise, a Security Violation error will be obtained and no change will be possible.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Access the UEFI Setup Utility by pressing F2 or DEL when the sign-on screen is displayed during boot.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Access the Secure Boot submenu from the Security tab.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Access the Key Management page by selecting the Key Management menu item.</td>
</tr>
</tbody>
</table>
Step_4  Default Factory Keys should already be provisioned, as identified by the "Factory" attribute in the Key Source column in the Secure Boot variable table. To replace the default Platform Key with your own, select Platform Key(PK).

Step_5  Select Update from the pop-up window.

Step_6  Select No to load a key from an external media.

Step_7  A list of available file systems will be displayed, using their corresponding UEFI device path. Select the USB device where the Public key certificates are located. Note that if Virtual Media redirection is used, the device will be identified as a CDROM.

Step_8  From the list of files, select the Public Certificate file for the Platform Key (PK.cer in this example).
Step_9 Specify that the file format is Public Key Certificate.

Step_10 Select Yes to confirm Platform Key update.

Step_11 Confirm that the update completed successfully. The table should now show that a key was added from an “External” Key Source.

Step_12 Select Key Exchange Keys to update or append the KEK database with your own. In this case:
- Selecting Update from the pop-up window will erase the pre-provisioned KEK entries and add a new KEK as a single entry;
- Selecting Append will add the new KEK to the database.

Step_13 Follow steps 4 to 11 to add a new KEK entry. If the KEK was appended to the database, the Key Source will be “Mixed”.
| Step 14 | Select **Authorized Signatures** to add an authorized Public Key certificate to the db. As for KEK:  
| | - Selecting **Update** from the pop-up window will erase the pre-provisioned db entries and add a new certificate as a single entry.  
| | - Selecting **Append** will add the new certificate to the database.  
| | Follow steps 4 to 11 to add a new db entry. If the certificate was appended to the database, the Key Source will be "Mixed".  
| Step 15 | Select **Save Changes and Exit** from the Setup Utility.  

To take advantage of the Secure Boot feature, make sure it is enabled in the **Security → Secure Boot** submenu.
Generating custom secure boot keys

To provision custom secure boot keys, keys may have to be generated. This article provides an example using CentOS 7.

Prerequisites

- Packages efitools and sbsigntools must be available. These packages are not official CentOS packages.

Procedure

Step 1
- Run the following commands on the system you need to generate keys for:
  - `mkdir make_keys`
  - `cd make_keys`
  - `wget https://github.com/freshautomations/efitools-centos/releases/download/2019-05-12/efitools-v1.9.2-1.x86_64.rpm`
  - `wget https://github.com/freshautomations/efitools-centos/releases/download/2019-05-12/sbsigntools-v0.9.2-1.x86_64.rpm`
  - `wget https://www.rodsbooks.com/efi-bootloaders/mkkeys.sh`
  - `chmod +x mkkeys.sh`
  - `yum install sbsigntools-v0.9.2-1.x86_64.rpm efitools-v1.9.2-1.x86_64.rpm ./mkkeys.sh`

Step 2
- The commands will generate a lot of files. You need the ".cer file to use in the provisioning procedure."
Reference guides
Supported IPMI commands

Table of contents
- Application commands
  - IPM device commands
  - Watchdog timer commands
  - BMC device and messaging commands
- IPMI 2.0 specific commands
- Chassis commands
- Bridge commands
  - Bridge management commands
  - Bridge discovery commands
  - Bridging commands
  - Bridge event commands
- Sensor event commands
- Storage commands
  - FRU information commands
  - SDR repository commands
  - SEL device commands
- Transport commands
  - IPM device commands
  - Serial over LAN commands
- AMI commands
  - AMI restore factory default settings command

Application commands

IPM device commands

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x06</td>
<td>0x01</td>
<td>Get Device ID</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x06</td>
<td>0x02</td>
<td>Cold Reset</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x03</td>
<td>Warm Reset</td>
<td>Un_supported *</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x04</td>
<td>Get Self Test Results</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x06</td>
<td>0x05</td>
<td>Manufacturing Test On</td>
<td>Un_supported *</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x06</td>
<td>Set ACPI Power State</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x07</td>
<td>Get ACPI Power State</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x08</td>
<td>Get Device GUID</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x09</td>
<td>Get NetFn Support</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x0A</td>
<td>Get Command Support</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x0C</td>
<td>Get Configurable Commands</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x60</td>
<td>Set Command Enables</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x61</td>
<td>Get Command Enables</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x64</td>
<td>Get OEM NetFn IANA Support</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x0B</td>
<td>Get Command Sub-function Support</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x0D</td>
<td>Get Configurable Command Sub-functions</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x62</td>
<td>Set Command Sub-function Enables</td>
<td>Un-supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x63</td>
<td>Get Command Sub-function Enables</td>
<td>Un-supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x52</td>
<td>Master Write-Read</td>
<td>Supported</td>
<td>O</td>
</tr>
</tbody>
</table>

* Commands are not rejected and can cause unpredictable behavior.

Watchdog timer commands

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x06</td>
<td>0x22</td>
<td>Reset Watchdog Timer</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x06</td>
<td>0x24</td>
<td>Set Watchdog Timer</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x06</td>
<td>0x25</td>
<td>Get Watchdog Timer</td>
<td>Supported</td>
<td>M</td>
</tr>
</tbody>
</table>

BMC device and messaging commands
<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x06</td>
<td>0x2E</td>
<td>Set BMC Global Enables</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x06</td>
<td>0x2F</td>
<td>Get BMC Global Enables</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x06</td>
<td>0x30</td>
<td>Clear Message Flags</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x06</td>
<td>0x31</td>
<td>Get Message Flags</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x06</td>
<td>0x32</td>
<td>Enable Message Channel Receive</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x33</td>
<td>Get Message</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x06</td>
<td>0x34</td>
<td>Send Message</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x06</td>
<td>0x35</td>
<td>Read Event Message Buffer</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x37</td>
<td>Get System GUID</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x38</td>
<td>Get Channel Authentication Capabilities</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x39</td>
<td>Get Session Challenge</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x3A</td>
<td>Activate Session</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x3B</td>
<td>Set Session Privilege Level</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x3C</td>
<td>Close Session</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x3D</td>
<td>Get Session Info</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x3F</td>
<td>Get AuthCode</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x40</td>
<td>Set Channel Access</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x41</td>
<td>Get Channel Access</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x42</td>
<td>Get Channel Info Command</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x43</td>
<td>Set User Access Command</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x44</td>
<td>Get User Access Command</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x45</td>
<td>Set User Name</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x46</td>
<td>Get User Name Command</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x47</td>
<td>Set User Password Command</td>
<td>Supported</td>
<td>D</td>
</tr>
<tr>
<td>0x06</td>
<td>0x52</td>
<td>Get System Info Parameters</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x06</td>
<td>0x59</td>
<td>Get System Info Parameters</td>
<td>Supported</td>
<td>D</td>
</tr>
</tbody>
</table>

**IPMI 2.0 specific commands**

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x06</td>
<td>0x48</td>
<td>Activate Payload</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x49</td>
<td>Deactivate Payload</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x4A</td>
<td>Get Payload Activation Status</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x4B</td>
<td>Get Payload Instance Info</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x4C</td>
<td>Set User Payload Access</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x4D</td>
<td>Get User Payload Access</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x4E</td>
<td>Get Channel Payload Support</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x4F</td>
<td>Get Channel Payload Version</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x50</td>
<td>Get Channel OEM Payload Info</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x54</td>
<td>Get Channel Cipher Suites</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x55</td>
<td>Suspend/Resume Payload Encryption</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x56</td>
<td>Set Channel Security Keys</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x06</td>
<td>0x57</td>
<td>Get System Interface Capabilities</td>
<td>Supported</td>
<td>O</td>
</tr>
</tbody>
</table>

**Chassis commands**
<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>0x00</td>
<td>Get Chassis Capabilities</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x00</td>
<td>0x01</td>
<td>Get Chassis Status</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x00</td>
<td>0x02</td>
<td>Chassis Control</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x00</td>
<td>0x04</td>
<td>Chassis Identify</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x00</td>
<td>0x05</td>
<td>Set Chassis Capabilities</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x00</td>
<td>0x06</td>
<td>Set Power Restore Policy</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x00</td>
<td>0x07</td>
<td>Get System Restart Cause</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x00</td>
<td>0x08</td>
<td>Set System Boot Options</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x00</td>
<td>0x09</td>
<td>Get System Boot Options</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x00</td>
<td>0x0A</td>
<td>Set Front Panel Button Enables</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x00</td>
<td>0x0B</td>
<td>Set Power Cycle Interval</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x00</td>
<td>0x0F</td>
<td>Get PDH Counter</td>
<td>Supported</td>
<td>O</td>
</tr>
</tbody>
</table>

**Bridge commands**

**Bridge management commands**

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x02</td>
<td>0x00</td>
<td>Get Bridge State</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x01</td>
<td>Set Bridge State</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x02</td>
<td>Get ICMB Address</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x03</td>
<td>Set ICMB Address</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x04</td>
<td>SetBridgeProxyAddress</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x05</td>
<td>Get Bridge Statistics</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x06</td>
<td>Get ICMB Capabilities</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x08</td>
<td>Clear Bridge Statistics</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x09</td>
<td>GetBridgeProxyAddress</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x0A</td>
<td>Get ICMB Proxy Address</td>
<td>Unsupported</td>
<td>M</td>
</tr>
</tbody>
</table>

**Bridge discovery commands**

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x02</td>
<td>0x10</td>
<td>Prepare For Discovery</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x11</td>
<td>Get Addresses</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x12</td>
<td>Set Discovered</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x13</td>
<td>Get Chassis Device Id</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x14</td>
<td>Set Chassis Device Id</td>
<td>Unsupported</td>
<td>O</td>
</tr>
</tbody>
</table>

**Bridging commands**

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x02</td>
<td>0x20</td>
<td>Bridge Request</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x21</td>
<td>Bridge Message</td>
<td>Unsupported</td>
<td>O</td>
</tr>
</tbody>
</table>

**Bridge event commands**

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x02</td>
<td>0x30</td>
<td>Get Event Count</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x31</td>
<td>Set Event Destination</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x32</td>
<td>Set Event Reception State</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x33</td>
<td>SendICMB Event Message</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x34</td>
<td>Get Event Destination</td>
<td>Unsupported</td>
<td>O</td>
</tr>
<tr>
<td>0x02</td>
<td>0x35</td>
<td>Get Event Reception State</td>
<td>Unsupported</td>
<td>O</td>
</tr>
</tbody>
</table>
### Sensor event commands

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x04</td>
<td>0x00</td>
<td>Set Event Receiver</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x04</td>
<td>0x01</td>
<td>Get Event Receiver</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x04</td>
<td>0x02</td>
<td>Platform Event</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x04</td>
<td>0x10</td>
<td>Get PEF Capabilities</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x04</td>
<td>0x11</td>
<td>Arm PEF Postpone Timer</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x04</td>
<td>0x12</td>
<td>Set PEF Configuration Parameters</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x04</td>
<td>0x13</td>
<td>Get PEF Configuration Parameters</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x04</td>
<td>0x14</td>
<td>Set Last Processed Event ID</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x04</td>
<td>0x15</td>
<td>Get Last Processed Event ID</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x04</td>
<td>0x16</td>
<td>Alert Immediate</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x04</td>
<td>0x17</td>
<td>PET Acknowledge</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x04</td>
<td>0x20</td>
<td>Get Device SDR Info</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x04</td>
<td>0x21</td>
<td>Get Device SDR</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x04</td>
<td>0x22</td>
<td>Reserve Device SDR Repository</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x04</td>
<td>0x23</td>
<td>Get Sensor Reading Factors</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x04</td>
<td>0x24</td>
<td>Set Sensor Hysteresis</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x04</td>
<td>0x25</td>
<td>Get Sensor Hysteresis</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x04</td>
<td>0x26</td>
<td>Set Sensor Threshold</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x04</td>
<td>0x27</td>
<td>Get Sensor Threshold</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x04</td>
<td>0x28</td>
<td>Set Sensor Event Enable</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x04</td>
<td>0x29</td>
<td>Get Sensor Event Enable</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x04</td>
<td>0x2A</td>
<td>Re-arm Sensor Events</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x04</td>
<td>0x2B</td>
<td>Get Sensor Event Status</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x04</td>
<td>0x2D</td>
<td>Get Sensor Reading</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x04</td>
<td>0x2E</td>
<td>Set Sensor Type</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x04</td>
<td>0x2F</td>
<td>Get Sensor Type</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x04</td>
<td>0x30</td>
<td>Set Sensor Reading And Event Status</td>
<td>Supported</td>
<td>O</td>
</tr>
</tbody>
</table>

### Storage commands

#### FRU information commands

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0a</td>
<td>0x10</td>
<td>Get FRU Inventory Area Info</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x11</td>
<td>Read FRU Data</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x12</td>
<td>Write FRU Data</td>
<td>Supported</td>
<td>M</td>
</tr>
</tbody>
</table>

#### SDR repository commands
<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0a</td>
<td>0x20</td>
<td>Get SDR Repository Info</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x21</td>
<td>Get SDR Repository Allocation Info</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x22</td>
<td>Reserve SDR Repository</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x23</td>
<td>Get SDR</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x24</td>
<td>Add SDR</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x25</td>
<td>Partial Add SDR</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x26</td>
<td>Clear SDR Repository</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x27</td>
<td>Get SDR Repository Time</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x28</td>
<td>Run Initialization Agent</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x29</td>
<td>Delete SDR Repository</td>
<td>Supported</td>
<td>M</td>
</tr>
</tbody>
</table>

**SEL device commands**

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0a</td>
<td>0x40</td>
<td>Get SEL Info</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x41</td>
<td>Get SEL Allocation Info</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x42</td>
<td>Reserve SEL</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x43</td>
<td>Get SEL Entry</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x44</td>
<td>Add SEL Entry</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x45</td>
<td>Partial Add SEL Entry</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x46</td>
<td>Clear SEL</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x47</td>
<td>Get SEL Time</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x48</td>
<td>Set SEL Time</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x49</td>
<td>Get SEL Time UTC Offset</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x0a</td>
<td>0x50</td>
<td>Set SEL Time UTC Offset</td>
<td>Supported</td>
<td>O</td>
</tr>
</tbody>
</table>

**Transport commands**

**IPM device commands**

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0c</td>
<td>0x01</td>
<td>Set LAN Configuration Parameters</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0c</td>
<td>0x02</td>
<td>Get LAN Configuration Parameters</td>
<td>Supported</td>
<td>M</td>
</tr>
<tr>
<td>0x0c</td>
<td>0x03</td>
<td>Suspend BMC ARPs</td>
<td>Supported</td>
<td>O</td>
</tr>
</tbody>
</table>

**Serial over LAN commands**

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0c</td>
<td>0x22</td>
<td>Get SOL Configuration Parameters</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x0c</td>
<td>0x21</td>
<td>Set SOL Configuration Parameters</td>
<td>Supported</td>
<td>O</td>
</tr>
</tbody>
</table>

**AMI commands**
AMI restore factory default settings command

<table>
<thead>
<tr>
<th>Net function</th>
<th>Command</th>
<th>Command name</th>
<th>Supported / Unsupported</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x32</td>
<td>0x66</td>
<td>Restore Defaults</td>
<td>Supported</td>
<td>O</td>
</tr>
</tbody>
</table>

NOTE: M/O = Mandatory/Optional

Kontron OEM commands

<table>
<thead>
<tr>
<th>Net Function</th>
<th>Command</th>
<th>Command Name</th>
<th>Supported/Unsupported</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x3c</td>
<td>0x0A</td>
<td>Override Minimum Fan Speed</td>
<td>Supported</td>
<td>O</td>
</tr>
<tr>
<td>0x3c</td>
<td>0x06</td>
<td>GUID provisioning</td>
<td>Supported</td>
<td>O</td>
</tr>
</tbody>
</table>
Supported Redfish commands

Table of contents
- Miscellaneous URLs
- System URLs
- Manager URLs
- Telemetry URLs
- Chassis URLs
- Account service URLs

The information is presented in the following format:
- Description | Method | URL

## Miscellaneous URLs
- Root resource of the Redfish service | -GET | /redfish/v1/
- Collection of Dynamic Extension types | -GET | /redfish/v1/DynamicExtension
- Collection of Dynamic Extensions | -GET | /redfish/v1/DynamicExtension/[DYNAMIC_EXTENSION_INSTANCE]
- Collection of log services for this system | -GET | /redfish/v1/DynamicExtension/LogServices
- Composition Service | -GET | /redfish/v1/CompositionService
- Collection of Resource Blocks | -GET or -PATCH | /redfish/v1/CompositionService/ResourceBlocks
- Collection of Resource Zones | -GET | /redfish/v1/CompositionService/ResourceZones
- Event service | -GET or -PATCH | /redfish/v1/EventService
- Collection of event subscriptions | -GET | /redfish/v1/EventService/Subscriptions
- Task service | -GET | /redfish/v1/TaskService
- Task collection | -GET | /redfish/v1/TaskService/Tasks
- List of OEM ISDS schemas and extensions | -GET | /redfish/v1/OemSchemas
- Returns information about a specified ISDS schema | -GET | /redfish/v1/OemSchemas/[JSON_SCHEMA_NAME]
- Collection of sessions | -GET or -POST | /redfish/v1/SessionService/Sessions
- Session service | -GET or -PATCH | /redfish/v1/SessionService
- Returns information about a specified session | -GET or -DELETE | /redfish/v1/SessionService/Sessions/[SESSION_ID]
- Registry repository | -GET | /redfish/v1/Registries
- Returns the summary of a specified registry | -GET | /redfish/v1/Registries/[REGISTRY_INSTANCE]
- Returns detailed information about a specified registry | -GET | /redfish/v1/Registries/[REGISTRY_INSTANCE].json
- Redfish update service | -GET or -PATCH | /redfish/v1/UpdateService

## System URLs
- Collection of computer systems | -GET | /redfish/v1/Systems
- Information about a specified system | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]
- Computer system reset action | -POST | /redfish/v1/Systems/[SYSTEM_INSTANCE]/Actions/ComputerSystem.Reset
- Collection of memories for this system | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/Memory
- Collection of processors for this system | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/Processors
- Collection of ethernet interfaces for this system | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/EthernetInterfaces
- Collection of simple storage for this system | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/SimpleStorage
- Collection of log services for this system | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/LogServices
- IPMI SEL events for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/BIOS
- Collection of event log service entries for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/EventLog
- Collection of event log service entries for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/EventLog/Entries
- Clear every entry of a specified log service for this manager | -POST | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/[LOG_SERVICE_INSTANCE]/Actions/LogService.ClearLog
- Information about a specified manager | -GET or -PATCH | /redfish/v1/Managers/[MANAGER_INSTANCE]
- Cold reset action for this manager | -POST | /redfish/v1/Managers/[MANAGER_INSTANCE]/Actions/Manager.Reset
- Collection of network protocol interfaces | -GET or -PATCH | /redfish/v1/Managers/[MANAGER_INSTANCE]/NetworkProtocol
- Collection of serial interfaces for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/SerialInterfaces
- Information about a specified serial interface | -GET or -PATCH | /redfish/v1/Managers/[MANAGER_INSTANCE]/SerialInterfaces/[SERIALINTERFACE_INSTANCE]
- Collection of virtual media | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/VirtualMedia
- Collection of host interfaces | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/HostInterfaces
- Information about a specified host interface | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/HostInterfaces/[HOSTINTERFACE_INSTANCE]
- Collection of ethernet interfaces connected to this host interface on this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/HostInterfaces/[HOSTINTERFACE_INSTANCE]/HostEthernetInterfaces
- Configures the number of CD/DVD devices that are supported for virtual media redirection | -POST | /redfish/v1/Managers/[MANAGER_INSTANCE]/VirtualMedia/Actions/Manager.Reset

## Manager URLs
- Collection of managers | -GET | /redfish/v1/Managers
- Collection of ethernet interfaces for a specified manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/EthernetInterfaces
- Information about a specified ethernet interface | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/EthernetInterfaces/[ETHERNETINTERFACE_INSTANCE]
- Collection of log services for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices
- Audit log service for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/AuditLog
- Collection of audit log service entries for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/AuditLog/Entries
- IPMI SEL service for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/SEL
- Collection of entries for the IPMI SEL service | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/SEL/Entries
- Event log service for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/EventLog
- Collection of event log service entries for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/EventLog/Entries
- Clear every entry of a specified log service for this manager | -POST | /redfish/v1/Managers/[MANAGER_INSTANCE]/LogServices/[LOGSERVICE_INSTANCE]/Actions/LogService.ClearLog
- Information about a specified manager | -GET or -PATCH | /redfish/v1/Managers/[MANAGER_INSTANCE]
- Cold reset action for this manager | -POST | /redfish/v1/Managers/[MANAGER_INSTANCE]/Actions/Manager.Reset
- Collection of network protocol interfaces | -GET or -PATCH | /redfish/v1/Managers/[MANAGER_INSTANCE]/NetworkProtocol
- Collection of serial interfaces for this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/SerialInterfaces
- Information about a specified serial interface | -GET or -PATCH | /redfish/v1/Managers/[MANAGER_INSTANCE]/SerialInterfaces/[SERIALINTERFACE_INSTANCE]
- Collection of virtual media | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/VirtualMedia
- Collection of host interfaces | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/HostInterfaces
- Information about a specified host interface | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/HostInterfaces/[HOSTINTERFACE_INSTANCE]
- Collection of ethernet interfaces connected to this host interface on this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/HostInterfaces/[HOSTINTERFACE_INSTANCE]/HostEthernetInterfaces
- Configures the number of CD/DVD devices that are supported for virtual media redirection | -POST | /redfish/v1/Managers/[MANAGER_INSTANCE]/VirtualMedia/Actions/Manager.Reset
Telemetry URLs

- Collection of log services for this telemetry service | -GET | /redfish/v1/TelemetryService/LogServices
- Information about the metric report log service | -GET | /redfish/v1/TelemetryService/LogServices/MetricReportLog
- Metric report log service entries | -GET | /redfish/v1/TelemetryService/LogServices/MetricReportLog/Entries
- Information about the telemetry service | -GET | /redfish/v1/TelemetryService
- Generates a test metric report | -POST | /redfish/v1/TelemetryService/Actions/TelemetryService.SubmitTestMetricReport
- Collection of metric definitions | -GET | /redfish/v1/TelemetryService/MetricDefinitions
- Collection of metric definitions | -GET or -POST | /redfish/v1/TelemetryService/MetricReportDefinitions
- Information about a specified metric definition | -GET or -PATCH or -DELETE | /redfish/v1/TelemetryService/MetricReportDefinitions/[METRIC_REPORT_DEF]
- Collection of metric reports | -GET | /redfish/v1/TelemetryService/MetricReports
- Information about a specified metric report instance | -GET | /redfish/v1/TelemetryService/MetricReports/[METRIC_REPORT_INSTANCE]
- Collection of triggers | -GET or -POST | /redfish/v1/TelemetryService/Triggers
- Information about a specified trigger | -GET or -DELETE | /redfish/v1/TelemetryService/Triggers/[TRIGGER_INSTANCE]
- Metric report log service | -GET | /redfish/v1/TelemetryService/LogServices/MetricReportLog
- Clears the metric report log service | -POST | /redfish/v1/TelemetryService/LogServices/MetricReportLog/Actions/LogService.ClearLog
- Collection of metric report log service entries | -GET | /redfish/v1/TelemetryService/LogServices/MetricReportLog/Entries/[LOG_ENTRY]

Chassis URLs

- Chassis collection | -GET | /redfish/v1/Chassis
- Information about a specified chassis instance | -GET or -PATCH | /redfish/v1/Chassis/[CHASSIS_INSTANCE]
- Resets the chassis | -POST | /redfish/v1/Chassis/[CHASSIS_INSTANCE]/Actions/Chassis.Reset
- Collection of voltage sensors | -GET | /redfish/v1/Chassis/[CHASSIS_INSTANCE]/Power
- Collection of thermal sensors | -GET | /redfish/v1/Chassis/[CHASSIS_INSTANCE]/Thermal
- Collection of network adapters | -GET | /redfish/v1/Chassis/[CHASSIS_INSTANCE]/NetworkAdapters

Account service URLs

- Redfish account service | -GET or -PATCH | /redfish/v1/AccountService
- Collection of Redfish user accounts | -GET or -POST | /redfish/v1/AccountService/Accounts
- Information about a specified Redfish account | -GET or -PATCH or -DELETE | /redfish/v1/AccountService/Accounts/[ACCOUNT_INSTANCE]
- Collection of available roles | -GET or -POST | /redfish/v1/AccountService/Roles
- Information about a specified role | -GET or -PATCH or -DELETE | /redfish/v1/AccountService/Roles/[ROLE_INSTANCE]
- Collection of account service configurations | -GET or -PATCH | /redfish/v1/AccountService/Configurations
Here's a table of the possible informations that can be found via SNMP.

<table>
<thead>
<tr>
<th>OID</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv2-MIB::sysObjectID.0</td>
<td>The time (in hundreds of a second) since the network management portion of the system was last re-initialized.</td>
<td>GET</td>
</tr>
<tr>
<td>DISMAN-EVENT-MIB::sysUpTimeInstance</td>
<td>The textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is the zero-length string.</td>
<td>GET</td>
</tr>
<tr>
<td>SNMPv2-MIB::sysContact.0</td>
<td>An administratively-assigned name for this managed node. By convention, this is the node’s fully-qualified domain name.</td>
<td>GET</td>
</tr>
<tr>
<td>SNMPv2-MIB::sysName.0</td>
<td>The physical location of this node (e.g., ‘telephone closet, 3rd floor’).</td>
<td>GET</td>
</tr>
<tr>
<td>SNMPv2-MIB::sysLocation.0</td>
<td>The value of sysUpTime at the time of the most recent change in state or value of any instance of sysORID.</td>
<td>GET</td>
</tr>
<tr>
<td>SNMPv2-MIB::sysORTable</td>
<td>The (conceptual) table listing the capabilities of the local SNMP application acting as a command responder with respect to various MIB modules. SNMP entities having dynamically-configurable support of MIB modules will have a dynamically-varying number of conceptual rows.</td>
<td>GET</td>
</tr>
<tr>
<td>IF-MIB::ifNumber.0</td>
<td>The network of number interfaces (regardless of their current state) present on this system.</td>
<td>GET</td>
</tr>
<tr>
<td>IF-MIB::ifTable</td>
<td>A list of interface entries. The number of entries is given by the value of ifNumber. The entries consist of these fields.</td>
<td>GET</td>
</tr>
<tr>
<td>IF-MIB::ifIndex</td>
<td>The interface on which this entry’s equivalence is effective. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.</td>
<td>GET</td>
</tr>
<tr>
<td>IF-MIB::ifDescr</td>
<td>The media-dependent ‘physical’ address.</td>
<td>GET</td>
</tr>
<tr>
<td>IF-MIB::ifMtu</td>
<td>The NetworkAddress (e.g., the IP address) corresponding to the media-dependent ‘physical’ address.</td>
<td>GET</td>
</tr>
<tr>
<td>IP-MIB::ipForwarding</td>
<td>The indication of whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP gateways forward datagrams. IP hosts do not (except those source-routed via the host).</td>
<td>GET</td>
</tr>
<tr>
<td>IP-MIB::ipDefaultTTL</td>
<td>The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, wherever a TTL value is not supplied by the transport layer protocol.</td>
<td>GET</td>
</tr>
<tr>
<td>IP-MIB::ipInOctets</td>
<td>The total number of input datagrams received from interfaces, including those received in error.</td>
<td>GET</td>
</tr>
<tr>
<td>IP-MIB::ipInAddrErrors</td>
<td>The number of input datagrams discarded because the IP address in their IP header’s destination field was not a valid address to be received at this entity. This counter includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entries which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.</td>
<td>GET</td>
</tr>
<tr>
<td>IP-MIB::ipInUcastPkts</td>
<td>The number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams discarded while awaiting re-assembly.</td>
<td>GET</td>
</tr>
<tr>
<td>IP-MIB::ipInOctets</td>
<td>The total number of output IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space).</td>
<td>GET</td>
</tr>
<tr>
<td>IP-MIB::ipInDiscards</td>
<td>The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space).</td>
<td>GET</td>
</tr>
<tr>
<td>IP-MIB::ipInNoRoutes</td>
<td>The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.</td>
<td>GET</td>
</tr>
<tr>
<td>IP-MIB::ipReasmReqds</td>
<td>Number of IP fragments received which needed to be reassembled at this entity.</td>
<td>GET</td>
</tr>
<tr>
<td>IP-MIB::ipReasmOKs</td>
<td>Number of IP datagrams successfully re-assembled.</td>
<td>GET</td>
</tr>
</tbody>
</table>
IP-MIB::ipv6IpForwarding
The indication of whether this entity is acting as an IPv6 router on any interface in respect to the forwarding of datagrams received by, but not addressed to, this entity. IPv6 routers forward datagrams. IPv6 hosts do not (except those source-routed via the host). When this object is written, the entity SHOULD save the change to non-volatile storage and restore the object from non-volatile storage upon re-initialization of the system.

IP-MIB::ipv6DefaultHopLimit
The default value inserted into the Hop Limit field of the IPv6 header of datagrams originated at this entity whenever a Hop Limit value is not supplied by the transport layer protocol. When this object is written, the entity SHOULD save the change to non-volatile storage and restore the object from non-volatile storage upon re-initialization of the system.

IP-MIB::ipSystemStatsTable
The table containing system wide, IP version specific traffic statistics. This table and the ipIfStatsTable contain similar objects whose difference is in their granularity. Where this table contains system wide traffic statistics, the ipIfStatsTable contains the same statistics but counted on a per-interface basis.

IP-MIB::ipIfStatsTableLastChange
The value of sysUpTime on the most recent occasion at which a row in the ipIfStatsTable was added or deleted. If new objects are added to the ipIfStatsTable that require the ipIfStatsTableLastChange to be updated when they are modified, they must specify that requirement in their description clause.

IP-MIB::ipIfStatsTable
The table containing per-interface traffic statistics. This table and the ipSystemStatsTable contain similar objects whose difference is in their granularity. Where this table contains per-interface statistics, the ipSystemStatsTable contains the same statistics, but counted on a system wide basis.

IP-MIB::ipAddressPrefixTable
This table allows the user to determine the source of an IP address or set of IP addresses, and allows other tables to share the information via pointer rather than by copying. More information can be found here http://oidref.com/1.3.6.1.2.1.4.32

IP-MIB::ipAddressSpinLock
An advisory lock used to allow cooperating SNMP managers to coordinate their use of the set operation in creating or modifying rows within this table. More information can be found here http://oidref.com/1.3.6.1.2.1.4.33

IP-MIB::ipAddressTable
This table contains addressing information relevant to the entity’s interfaces. More information can be found here http://oidref.com/1.3.6.1.2.1.4.34

IP-MIB::ipNetToPhysicalTable
The IP Address Translation table used for mapping from IP addresses to physical addresses. The Address Translation tables contain the IP address to ‘physical’ address equivalences. Some interfaces do not use translation tables for determining address equivalences (e.g., DDN-X.25 has an algorithmic method); if all interfaces are of this type, then the Address Translation table is empty, i.e., has zero entries. While many protocols may be used to populate this table, ARP and Neighbor Discovery are the most likely options.

IP-MIB::ipv6ScopeZoneIndexTable
The table used to describe IPv6 unicast and multicast scope zones. For those objects that have names rather than numbers, the names were chosen to coincide with the names used in the IPv6 address architecture document.

IP-MIB::ipDefaultRouterTable
The table used to describe the default routers known to this entity.

IP-MIB::icmpInMsgs
The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.

IP-MIB::icmpInErrors
The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).

IP-MIB::icmpInDestUnreachs
The number of ICMP Destination Unreachable messages received.

IP-MIB::icmpInTimeExcds
Number of ICMP Time Exceeded messages received.

IP-MIB::icmpInParmProbs
Number of ICMP Parameter Problem messages received.

IP-MIB::icmpInSrcQuenches
Number of ICMP Source Quench messages received.

IP-MIB::icmpInRedirects
Number of ICMP Redirect messages received.

IP-MIB::icmpInEchos
Number of ICMP Echo (request) messages received.
TCP-MIB::tcpConnectionState
The state of this TCP connection.

TCP-MIB::tcpOutRsts
The number of TCP segments sent containing the RST flag.

TCP-MIB::tcpInErrs
The total number of segments received in error (e.g., bad TCP checksums).

TCP-MIB::tcpConnTable
A table containing TCP connection-specific information.

TCP-MIB::tcpRetransSegs
The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.

TCP-MIB::tcpOutSegs
The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.

TCP-MIB::tcpInSegs
The total number of segments received, including those received in error. This count includes segments received on currently established connections.

TCP-MIB::tcpPassiveOpens
The number of times TCP connections have made a direct transition to the SYN-SENT state from the LISTEN state.

TCP-MIB::tcpRetransMax
The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.

TCP-MIB::tcpRetransMin
The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.

TCP-MIB::tcpAttemptFails
The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.

TCP-MIB::tcpActiveOpens
The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.

TCP-MIB::tcpConnTable
A table containing TCP connection-specific information.

TCP-MIB::tcpCurrEstab
The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.

TCP-MIB::tcpInErrs
The total number of segments received in error (e.g., bad TCP checksums).

TCP-MIB::tcpOutRsts
The number of TCP segments sent containing the RST flag.

TCP-MIB::tcpPassiveOpens
The number of times TCP connections have made a direct transition to the SYN-SENT state from the LISTEN state.

TCP-MIB::tcpActiveOpens
The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.

TCP-MIB::tcpAttemptFails
The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.

TCP-MIB::tcpConnTable
A table containing TCP connection-specific information.

TCP-MIB::tcpCurrEstab
The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.

TCP-MIB::tcpPassiveOpens
The number of times TCP connections have made a direct transition to the SYN-SENT state from the LISTEN state.

TCP-MIB::tcpActiveOpens
The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.

TCP-MIB::tcpAttemptFails
The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.

TCP-MIB::tcpConnTable
A table containing TCP connection-specific information.

TCP-MIB::tcpCurrEstab
The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.

TCP-MIB::tcpPassiveOpens
The number of times TCP connections have made a direct transition to the SYN-SENT state from the LISTEN state.

TCP-MIB::tcpActiveOpens
The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.

TCP-MIB::tcpAttemptFails
The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
The total number of packets received on this connection. This count includes retransmitted data.

A table containing information about TCP listeners. More information can be found here https://oidref.com/1.3.6.1.2.1.6.20

The total number of UDP datagrams delivered to UDP users.

The total number of received UDP datagrams for which there was no application at the destination port.

The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

The total number of UDP datagrams sent from this entity.

A table containing UDP listener information.

The total number of messages delivered to the SNMP entity from the transport service.

The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.

The total number of SNMP messages which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.

The total number of SNMP Messages delivered to the SNMP protocol entity which used a SNMP community name not known to said entity.

The total number of community-based SNMP messages (for example, SNMPv1) delivered to the SNMP entity which represented an SNMP operation that was not allowed for the SNMP community named in the message. The precise conditions under which this counter is incremented (if at all) depend on how the SNMP entity implements its access control mechanism and how its applications interact with that access control mechanism. It is strongly RECOMMENDED that the documentation for any access control mechanism which is used to control access to and visibility of MIB instrumentation specify the precise conditions that contribute to this value.

The total number ofASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.

The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was 'tooBig'.

The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was 'NoSuchName'.

The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was 'badValue'.

The total number of SNMP Messages delivered to the SNMP protocol entity which used a SNMP community name not known to said entity.

The total number of SNMP Messages delivered to the SNMP protocol entity which were for an unsupported SNMP version.

The total number of messages delivered to the SNMP entity from the transport service.

The total number of UDP datagrams sent from this entity.

The total number of UDP datagrams sent from this entity.

The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

The total number of received UDP datagrams for which there was no application at the destination port.

More information can be found here www.kontron.com
SNMPv2-MIB::snmpOutGetResponses  The total number of SNMP Get-Response PDUs which have been generated by the SNMP protocol entity.

SNMPv2-MIB::snmpOutTraps  The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity.

SNMPv2-MIB::snmpEnableAuthenTraps  Indicates whether the SNMP entity is permitted to generate authenticationFailure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authenticationFailure traps may be disabled. Note that it is strongly recommended that this object be stored in non-volatile memory so that it remains constant across re-initializations of the network management system.

SNMPv2-MIB::snmpSilentDrops  The total number of Confirmed Class PDUs (such as GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs) delivered to the SNMP entity which were silently dropped because the size of a reply containing an alternate Response Class PDUs (such as a Response-PDU) with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.

SNMPv2-MIB::snmpProxyDrops  The total number of Confirmed Class PDUs (such as GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs) delivered to the SNMP entity which were silently dropped because the transmission of the (possibly translated) message to a proxy target failed in a manner (other than a time-out) such that no Response Class PDUs (such as a Response-PDU) could be returned.

HDST-RESOURCES-MIB::hrSystemUptime  The amount of time since this host was last initialized. Note that this is different from sysUpTime in MIB-II [3] because sysUpTime is the uptime of the network management portion of the system.

HDST-RESOURCES-MIB::hrSystemDate  The host’s notion of the local date and time of day.

HDST-RESOURCES-MIB::hrSystemInitialLoadDevice  The index of the hrDeviceEntry for the device from which this host is configured to load its initial operating system configuration.

HDST-RESOURCES-MIB::hrSystemInitialLoadParameters  This object contains the parameters (e.g. a pathname and parameter) supplied to the load device when requesting the initial operating system configuration from that device.

MTA-MIB::mtaTable  The table holding information specific to an MTA.

MTA-MIB::mtaGroupTable  The table holding information specific to each MTA group.

IF-MIB::ifTable  A list of interface entries. The number of entries is given by the value of ifNumber. This table contains additional objects for the interface table.

IF-MIB::ifTableLastChange  The value of sysUpTime at the time of the last creation or deletion of an entry in the ifTable. If the number of entries has been unchanged since the last re-initialization of the local management subsystem, then this object contains a zero value.

IPV6-MIB::ipv6Forwarding  The indication of whether this entity is acting as an IPv6 router in respect to the forwarding of datagrams received by, but not addressed to, this entity. IPv6 routers forward datagrams. IPv6 hosts do not (except those source-routed via the host). More information can be found here [https://oidref.com/1.3.6.1.2.1.55.1.1]

IPV6-MIB::ipv6DefaultHopLimit  The default value inserted into the Hop Limit field of the IPv6 header of datagrams originated at this entity, whenever a Hop Limit value is not supplied by the transport layer protocol.

IPV6-MIB::ipv6Interfaces  The number of IPv6 interfaces (regardless of their current state) present on this system.

IPV6-MIB::ipv6IfTable  The IPv6 Interfaces table contains information on the entity’s internetwork-layer interfaces. An IPv6 interface constitutes a logical network layer attachment to the layer immediately below IPv6 including internet layer ‘tunnels’, such as tunnels over IPv4 or IPv6 itself.

DISMAN-EVENT-MIB::mteResourceSampleMinimum  The minimum mteTriggerFrequency this system will accept. A system may use the larger values of this minimum to lessen the impact of constant sampling. For larger sampling intervals the system samples less often and suffers less overhead. This object provides a way to enforce such lower overhead for all triggers created after it is set. More information can be found here [https://oidref.com/1.3.6.1.2.1.55.1.1]

DISMAN-EVENT-MIB::mteResourceSampleInstanceMaximum  The maximum number of instance entries this system will support for sampling. More information can be found here [https://oidref.com/1.3.6.1.2.1.55.1.1]

DISMAN-EVENT-MIB::mteResourceSampleInstances  The number of currently active instance entries as defined for mteResourceSampleInstanceMaximum.

DISMAN-EVENT-MIB::mteResourceSampleInstancesHigh  The highest value of mteResourceSampleInstances that has occurred since initialization of the management system.

DISMAN-EVENT-MIB::mteResourceSampleInstancesLocks  The number of times this system could not take a new sample because that allocation would have exceeded the limit set by mteResourceSampleInstanceMaximum.

DISMAN-EVENT-MIB::mteTriggerFailures  The minimum mteTriggerFrequency this system will accept. A system may use the larger values of this minimum to lessen the impact of constant sampling. For larger sampling intervals the system samples less often and suffers less overhead. This object provides a way to enforce such lower overhead for all triggers created after it is set.

DISMAN-EVENT-MIB::mteObjectsTable  A table of objects that can be added to notifications based on the trigger, trigger test, or event, as pointed to by entries in those tables.

DISMAN-EVENT-MIB::mteEventTable  A table of management event action information.

DISMAN-EVENT-MIB::mteEventNotificationTable  A table of information about notifications to be sent as a consequence of management events.

NOTIFICATION-LOG-MIB::nlmConfigGlobalEntryLimit  The maximum number of notification entries that may be held in nlmLogTable for all nlmLogNames added together. A particular setting does not guarantee that much data can be held. More information can be found here [https://oidref.com/1.3.6.1.2.1.55.1.1]
NOTIFICATION-LOG-MIB::nlmConfigGlobalAgeOut

The number of minutes a Notification SHOULD be kept in a log before it is automatically removed. If an application changes the value of nlmConfigGlobalAgeOut, Notifications older than the new value MAY be discarded to meet the new time. A value of 0 means no age out. Please be aware that contention between multiple managers trying to set this object to different values MAY affect the reliability and completeness of data seen by each manager.

NOTIFICATION-LOG-MIB::nlmStatsGlobalNotificationsBumped

The number of log entries discarded to make room for a new entry due to lack of resources or the value of nlmConfigGlobalEntryLimit or nlmConfigLogEntryLimit. This does not include entries discarded due to the value of nlmConfigGlobalAgeOut.

SNMPv2-SMI::enterprises.3582

NET-SNMP-VACM-MIB::nsVacmContextMatch

The MIB view authorised for the appropriate style of processing (as indicated by nsVacmToken). The interpretation of this value is the same as for the standard VACM ViewName objects.

NET-SNMP-VACM-MIB::nsVacmStorageType

The storage type for this (group of) conceptual rows. Conceptual rows having the value 'permanent' need not be cached. Conceptual rows having the value 'volatile' need to be cached.

NET-SNMP-VACM-MIB::nsVacmStatus

The status of this (group of) conceptual rows. The RowStatus TC [RFC2579] requires that this DESCRIPTION clause states under which circumstances other objects in this row can be modified. The value of this object has no effect on whether other objects in this conceptual row can be modified. The value of this object should be consistent across all nsVacmAccessEntries corresponding to a single row of the vacmAccessTable.

SNMPv2-SMI::enterprises.20974.554.1

AMI SNMP Hostname Extension

SNMPv2-SMI::enterprises.20974.554.2

AMI SNMP MIB library to return the system health status like power and sensor status.

SNMPv2-SMI::enterprises.20974.554.3

AMI SNMP Platform Info Extension
Parallel configuration

(This article details automation of platform configuration and application deployment use cases.)

Table of contents
- Introduction
  - AMISCE download
  - BIOS default values
  - Tool name to use
- Defining what values need to be configured
- Installing AMISCE
  - UEFI Shell
- Operating the AMISCE tool - use case 1 - multiple changes
  - Extracting all the BIOS options
  - Extracting only modified BIOS options
  - Importing the modified set of BIOS options
- Operating the AMISCE tool - use case 2 - few changes
  - Set all BIOS setup options
  - Set one BIOS Setup option
    - Getting one BIOS Setup option with Map String value
    - Getting one BIOS Setup option without Map String value
  - Set one BIOS Setup option
    - Set one BIOS Setup option with a Map String value
    - Set one BIOS setup option without a Map String value
- Operating the AMISCE tool - use case 3 - changing the boot order
- Operating the AMISCE tool - use case 4 - passwords
  - Setting a password
  - Modifying a password

Introduction

The AMISCE command line tool is recommended for parallel and/or automated BIOS configuration. The AMISCE tool is mainly used to extract the modified BIOS Setup option values in a file. It can then be used to either modify these values or ultimately apply these changes to other similar systems.

The AMISCE tool:
- Is offered in both 32-bit and 64-bit versions
- Provides an easy way to update NVRAM variables from within a UEFI Shell, Linux or Windows-based environment
- Produces a script file that lists all setup questions on the system where AMISCE is running

The AMISCE tool lets users:
- Extract variables directly from the BIOS
- Modify variables using either a text editor or a setup program
- Update the BIOS option values

Each of these actions can be performed on a different system. Extracting only the modified option values and comparing them with the default BIOS values might make the procedure faster when updating a system. This process is therefore recommended.

NOTE: These use cases assume that there is currently no administrator password. If a password is set, add the following attributes to the command: /cpwd <current admin password>, where /cpwd is the admin password of type Unicode and <current admin password> is your password.

NOTE: Kontron releases the BIOS Setup in English and this is specified in AMISCE using the "//lang en-US" attribute.

AMISCE download

AMISCE tools are available at www.kontron.com, under the CG2400 page.

BIOS default values

The BIOS Setup option values are preset with default values. Each new BIOS release may have different default values. These values can be restored using the Optimized Defaults option in the BIOS menu. Refer to Restoring default BIOS settings using the BIOS menu for further instructions.

Tool name to use

AMISCE tools have different names depending on which operating system is used. Simply change the [AMISCE ] attribute in the examples below according to the specific operating system version name. This article uses the following tool:

<table>
<thead>
<tr>
<th>OS environment</th>
<th>64bits - application name</th>
</tr>
</thead>
<tbody>
<tr>
<td>UEFI shell</td>
<td>SceEfi64.efi</td>
</tr>
</tbody>
</table>

Defining what values need to be configured

Before proceeding with the following procedure, define the BIOS Setup options that will be configured on all the systems. This list of BIOS Setup option names will be required to perform the steps described.

Installing AMISCE

The AMISCE tool can be installed on various environments:
- UEFI Shell - described in this article
- Linux - not discussed
- Windows - not discussed

UEFI Shell

Launch the UEFI Shell and copy the tool to a USB key or SSD.

CG2400_User_documentation_2-01-2023 // 288
Operating the AMISCE tool - use case 1 - multiple changes

This section describes how to extract every BIOS option to apply them to another system. It provides one typical use case for using the AMISCE tool.

Extracting all the BIOS options

Refer to Accessing the BIOS for access instructions.

### Step 1
(Optional) Access the BIOS. Go into the BIOS Setup menu. Navigate to Save & Exit → Restore Defaults (or use F3: Optimized Defaults). Navigate to Save Changes and Reset.

### Step 2
From the OS, use the following command to extract the BIOS Setup data.

```
[ AMISCE ] /o /s MySet.txt /sd Duplicate.txt /h MySet.db /b /lang en-US /sp /g /v
```

Command description:
- `/o` - Indicates generate Setup script file from HII (Human Interface Infrastructure) data.
- `/s` - Indicates Setup script file that is to be generated.
- `/sd` - Optional command line option to export duplicate questions into a separate script file.
- `/h` - Indicates the HII Dump file.
- `/b` - Optional CMD line option that enables export of boot order controls in the generated script file.
- `/lang` - Optional CMD line option that enables exportation of boot order controls in the generated script file. **This is really important.**
- `/sp` - Enables Expression Evaluation for Suppressif Opcode (options that are hidden in the BIOS Setup because of other option values).
- `/g` - Enables Expression Evaluation for Grayoutif Opcode (options that are shown in grey in the BIOS Setup).
- `/v` - Optional CMD line option that produces a verbose script file.

This command creates a file called `MySet.txt` with all the BIOS Setup options (referred to as "Setup Question") exported.

**Output example:**

```
// Script File Name : MySet.txt
// Created on 10/21/19 at 10:11:12
// Copyright (c) 1985-2019, American Megatrends International LLC.
// AMISCE Utility. Ver 5.03.1129
HICrc32= 9A25240A
Setup Question = Network Stack
Map String = NWSK000
Token =01 // Do NOT change this line
Offset =00
Width =01
BIOS Default=[01]Enabled
Options=[00]Disabled // Move "*" to the desired Option
[01]Enabled
Setup Question = Ipv4 PXE Support
Map String = NWSK001
[...]
```

### NOTES:
- In the Setup script file generated (`MySet.txt`):
  - Do not modify the content of the fields "Setup Question", "Map String", "Token", "Offset", "Width" and "BIOS Default".
  - Modify the content of the "Options" fields for questions that you want to change by moving "*" to the desired option.
- Some "Setup Question" fields may not have a "Map String" defined in the current BIOS source code. These setup questions will not be imported/changed by this tool.
- AMISCE considers questions with the same storage location as duplicates. By default, these duplicates will be exported to the main script file, but will be commented out. To export the duplicates into a separate script file, use the `/sd` option.
- AMISCE will not import commented out questions (generated mainly by `/v`). It will treat commented out questions as if they do not exist in the script. To import a commented out question, users have to remove the comment out symbols `//`. The comments will also show BIOS Setup menu titles, which may be useful to correctly identify setup questions and their map strings for when BIOS Setup sub-menus have similar options (e.g. for the PCIe Bridges).

Extracting only modified BIOS options

The goal is to create a script file with only the required setup questions needed and remove any setup questions that you do not wish to update.
Step 1 | Reset and go into AptioV Setup Option.

Step 2 | Change all the options that you wish to change.

Step 3 | Navigate to Save & Exit → Save Changes and Reset.

Step 4 | From the OS, use the following command to extract only the modified BIOS options.
[ AMISCE ] /o /s MySet_changed.txt /sd Duplicate_changed.txt /h MySet_changed.db /b /lang en-US /sp /g

Step 5 | With your favorite tool to compare files (e.g. Notepad++), find the differences between the MySet_changed.txt and the MySet.txt for the next step.

Step 6 | Build a MyFutureOptions.txt file with the following content (bold elements are the ones to change). This is an example based on the output example in the previous section.

Summary of changes to make:
1. Keep the header of original MySet.txt up to and including the HitCr32 line.
2. Add a comment in the header to describe the modifications.
3. All the fields of each changed Setup option are needed. Cut and paste lines "Setup Question", "Map String", "Token", "Offset", "Width", "BIOS Default", "Option" and "Value".

// Script File Name: MySet.txt
// Created on 10/21/19 at 10:11:12
// All rights reserved. Subject to AMI licensing agreement.
// AMISCE Utility. Ver 5.03.1129
// Comment on change made
HitCr32 = 9A25240A
Setup Question = Network Stack
Map String = NWSK000
Token = 01 // Do NOT change this line
Offset = 00
Width = 01
BIOS Default = [01]Enabled
Options = [00]Disabled // Move "\" to the desired Option
[01]Enabled
Setup Question = Ipv4 PXE Support
Map String = NWSK001

Importing the modified set of BIOS options

Step 1 | Using the MyFutureOptions.txt file created in the previous section and from the OS, use the following command to import the modified set of BIOS options.

Command description:
- /i - Indicates Import modified script file to the NVRAM (into the BIOS Setup).
- /s - Indicates the NVRAM script file to use to read data.
- /ds - Optional CMD line option that indicates set BIOS defaults from script question value (WILL ALSO MAKE THEM NEW DEFAULT ONES).
- /b - Optional CMD line option that enables import of boot order controls from the generated script file.
- /lang - An optional CMD line option that enables mapping language mode which will import questions with the specified lang codes. Lang code indicates the code for a particular language like English(en-US), AMI(x-AMI), etc.

Step 2 | Validate that the tool does not produce errors.

NOTES:
- Changes will be effective during the next system reboot.
- Sometimes, AMISCE can report this warning:

WARNING: Error in writing variable Setup to NVRAM
Import completed with some errors, see warnings given.
This means that some of the changes will not be applied on the next system reboot. To apply all changes, do one of the following:
- Reboot in BIOS Setup to Restore Defaults (or use F3: Optimized Defaults).
- Use the IPMI command described in Factory default to reset the new default options. However, the Boot menu device order may also reset. Refer to examples below for additional AMISCE commands to adjust the Boot order.
- It cannot be used over different BIOS versions. Extracting in BIOS version X and importing in BIOS version Y is not possible nor recommended.
- There is an optional command /reboot to reboot/restart the system after any variable modification by AMISCE. Please close other processes in the OS before using this command.
- There is an optional command /shutdown to shut down the system after any variable modification by AMISCE. Please close other processes in the OS before using this command.

Operating the AMISCE tool - use case 2 - few changes

This section describes how to extract every BIOS option to apply them to another system when there are few changes. It provides one typical use cases for using the AMISCE tool.
The AMISCE tool provides many command-line options.

Get all BIOS setup options

---

CG2400_User_documentation_2-01-2023  www.kontron.com // 290
Step 1 | (Optional) Access the BIOS. Go into the BIOS Setup menu. Navigate to **Save & Exit** → **Restore Defaults** (or use F3: Optimized Defaults). Navigate to **Save Changes and Reset**.

Step 2 | From the OS, use the following command to extract the BIOS Setup data.

```shell
```

**Command description:**
- **/o** - Indicates generate Setup script file from Hill (Human Interface Infrastructure) data.
- **/en-US** - Indicates Setup script file that is to be generated.
- **/ms** - Optional command line option to export duplicate questions into a separate script file.
- **/h** - Indicates the Hill Dump file.
- **/b** - Optional CMD line option that enables export of boot order controls in the generated script file. 
  - **/en-US** - Optional CMD line option that enables exportation of boot order controls in the generated script file. This is really important.
- **/sp** - Enables Expression Evaluation for Suppressif Opcode (options that are hidden in the BIOS Setup because of other option values).
- **/g** - Enables Expression Evaluation for Grayoutif Opcode (options that are shown in grey in the BIOS Setup).
- **/v** - Optional CMD line option that produces a verbose base file.

This command creates a file called **MySet.txt** with all the BIOS Setup options (referred to as “Setup Question”) exported.

**Notes:**
- In the Setup script file generated (**MySet.txt**):
  - Do not modify the content of the fields “Setup Question”, “Map String”, “Token”, “Offset”, “Width” and “BIOS Default”.
  - Modify the content of the “Options” fields for questions that you want to change by moving “*” to the desired option.
- Some “Setup Question” fields may not have a “Map String” defined in the current BIOS source code. These setup questions will not be imported/changed by this tool.
- AMISCE considers questions with the same storage location as duplicates. By default, these duplicates will be exported to the main script file but will be commented out. To export the duplicates into a separate script file, use the **/sd** option.
- AMISCE will not import commented out questions (generated mainly by */v*). It will treat commented out questions as if they do not exist in the script. To import a commented out question, users have to remove the comment out symbols //. The comments will also show BIOS Setup menu titles, which may be useful to correctly identify setup questions and their map strings for when BIOS Setup sub-menus have similar options (e.g. for the PCIe Bridges).

### Get one BIOS Setup option

There are two cases when getting one BIOS Setup options:
- When there is a Map String value
- When there is no Map String value

**Important:** If a BIOS Setup option has a Map String it is highly recommended to use it to set the option as this is much faster. The AMISCE can read/modify such options without a Map String, but according to our tests, it takes a very long time (about 1 minute) to complete.

### Getting one BIOS Setup option with Map String value

**Step 1**

To read the value of the BIOS Setup option, its Map String value is needed. Get the Map String value of the BIOS Setup option you want to extract by searching in the Setup file extracted in the previous step (**MySet.txt**). In the example, the Map String of Setup Question “SR-IOV Support” is “PCIS007”.

**Example:**

```shell
Setp Question = SR-IOV Support
Map String = PCIS007
Token = 52
// Do NOT change this line
Offset = 00
Width = 01
BIOS Default = [0] Enabled // Move “*” to the desired Option
```

**Step 2**

From the OS, use the following command to get one BIOS Setup option with Map String value.

```shell
```

**Command description:**
- **/o** - Outputs content to the standard output (screen)
- **/en-US** - Enables mapping language mode (Lang Code = en-US and/or x-UEFI-AMI and/or nothing)
- **/ms** - Indicates Map String of the Setup Question
- **/i** - Indicates Quiet mode
- **/d** - Skip checking for AptioV BIOS and behave normally
- **/hb** - Hides tool information banner
- **/ds** - Indicates BIOS Standard Default Value

**Example:**

```shell
FS1:/> ScEfi64.efi /o /en-US /ms PCIS007 /d /hb BIOS Default = [0] Enabled Options = [0] Disabled // Move “*” to the desired Option
```

**Step 3**

Note the BIOS Setup option and proceed to set it if required (see next section).

### Getting one BIOS Setup option without Map String value

**Relevant section:**

BIOS configuration of CG2300 compared to CG2400
### Set one BIOS Setup option

There are two cases when setting one BIOS Setup options:

- **When there is a Map String value**
- **When there is no Map String value**

### Set one BIOS Setup option with a Map String value

**Step 1**
Set one BIOS Setup option using the Map String and the question value.

```
[AMISCE] /i /rs [QUESTION_MAP_STRING] /qv <QUESTION_VALUE> /l <language> /s /d /ms "" /bt <device type> /r
do not hit enter
```

**Command description:**
- `/i` - Imports the value into NVRAM
- `/ms` - Indicates Map String of the Setup Question
- `/qv` - Indicates Question Value to be set for the Setup Question
- `/bt` - Indicates the device type for legacy boot device
- `/q` - Indicates Quiet mode
- `/d` - Skip checking for AptioV BIOS and behave normally
- `/ms` - Indicates BIOS Standard Default Value
- `/hb` - Hides tool information banner
- `/ni` - To create Utility Indication variable to indicate variable modification by AMISCE
- `/shutdown` - Shutdown after programming
- `/reboot` - Reboot after programming

**Example:**
```
SceEfi64.efi /i /ms PCIS007 /qv 01 /l en-US /d /s
```

**Notes:**
- The `/qv` value format varies depending on the type of question. String type questions are not currently supported. A decimal numeric value (including negative numbers) has to be mentioned with angular brackets `<>` and mentioning the angular brackets without quotation might lead to file redirection warnings. Numeric value will be taken as hexadecimal value (0x prefix is optional) if not mentioned in decimal format.
- Sometimes, AMISCE can report this warning:

**WARNING:** Error in writing variable Setup to NVRAM

Import completed with some errors, see warnings given.

This means that some of the changes will not be applied on the next system reboot. To apply all changes, do one of the following:
- Reboot in BIOS Setup to Restore Defaults (or use F3: Optimized Defaults).
- Use IPMI command described in Factorydefault to reset the new default options. However, the Boot menu device order may also reset. Refer to examples below for additional AMISCE commands to adjust Boot order.

### Set one BIOS setup option without a Map String value

**Step 1**
Set one BIOS Setup option without the Map String using only the Setup Question and the question value.

```
[AMISCE] /i /rs "SETUP_QUESTION" /qv <QUESTION_VALUE> /d
```

**Command description:**
- `/i` - Imports the value into NVRAM
- `/ms` - Indicates Map String of the Setup Question
- `/qv` - Indicates Question Value to be set for the Setup Question
- `/bt` - Indicates the device type for legacy boot device
- `/q` - Indicates Quiet mode
- `/d` - Skip checking for AptioV BIOS and behave normally
- `/ms` - Indicates BIOS Standard Default Value
- `/hb` - Hides tool information banner
- `/ni` - To create Utility Indication variable to indicate variable modification by AMISCE
- `/shutdown` - Shutdown after programming
- `/reboot` - Reboot after programming

**Example:**
```
SceEfi64.efi /i /ms "SR-IOV Support" /qv 01 /l en-US /d
```

**Output example:**
```
BIOS Default = [01] PCI Mode
Options = [00] Disabled // Move **
```

**Step 2**
Validate the BIOS Setup value was changed.

```
[AMISCE] /o /rs "SETUP_QUESTION"
```

---

**Operating the AMISCE tool - use case 3 - changing the boot order**

CG2400_User_documentation_2-01-2023  www.kontron.com // 292
This section describes how to change the boot order using indexes in an option list. It provides one typical use cases for using the AMISCE tool.

The Map String to define the Boot Order device list is “SETUP006”.

**Step 1**
Get the current Boot Order.

```
```

That example returns a list with 7 boot devices, with indexes: [000f], [0001], [000d], etc.

**NOTE:** The index allocated to a boot device (for instance [000f] for the “UEFI: Built-in EFI Shell” in the above example) can vary from system to system. This means that before changing the Boot Order of a particular system, its current device list must be read first to be able to define and import a new boot order.

```
Output example: ListOrder =
[000f] UEFI: Built-in EFI Shell
[0001] CentOS
[000d] UEFI: PXE IP4 Intel(R)
Ethernet Connection X722 for 10GBASE-T
[0006] UEFI: SanDisk, Partition 1
[0005] UEFI: Memorex TD Classic 003B PMAP, Partition 1
[000e] UEFI: PXE IP4 Intel(R)
Ethernet Connection X722 for 10GBASE-T
[0002] UEFI: PXE IP4 American Megatrends Inc.
```

**Step 2**
To change the Boot Order, set the new Boot Order using the list of indexes with the command `/qv`.

```
[ AMISCE ] /i /lang en-US /ms SETUP006 /qv "index1,index2,index3,index4,index5,index6,index7" /hb
```

Example:
```
Question value imported successfully
```

---

**Operating the AMISCE tool - use case 4 - passwords**

Passwords can be set using the AMISCE tools. These passwords (user and administrator) can subsequently be changed.

### Setting a password

**Step 1**

```
```

**OR**

```
```

### Modifying a password

**Step 1**

```
```

**OR**

```
```

Examples:
```
SceEfi64.efi /cpwd test123 /apwd 123test /upwd test
OR
SceEfi64.efi /cpwdf admin.bin /apwdf newadmin.bin /upwdf user.bin
OR
SceEfi64.efi /cpwd test123 /apwdf newadmin.bin /upwdf user.bin
```

**NOTE:** The `.bin` files mentioned above should have the unicode password in UTF-16 format. User can use file variant password switch and command line password switch together as shown above.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[/cpwd]</td>
<td>Indicates the admin password of type Unicode.</td>
</tr>
<tr>
<td>[/cpwds]</td>
<td>Indicates the admin password of type scan code.</td>
</tr>
<tr>
<td>[/cpwde]</td>
<td>Indicates the admin password of type EFI key.</td>
</tr>
<tr>
<td>[/apwd]</td>
<td>Indicates the new admin password of type Unicode.</td>
</tr>
<tr>
<td>[/apwds]</td>
<td>Indicates new admin password of type scan code.</td>
</tr>
<tr>
<td>[/apwde]</td>
<td>Indicates new admin password of type EFI key.</td>
</tr>
<tr>
<td>[/upwd]</td>
<td>Indicates new user password of type Unicode.</td>
</tr>
<tr>
<td>[/upwds]</td>
<td>Indicates new user password of type scan code.</td>
</tr>
<tr>
<td>[/upwde]</td>
<td>Indicates new user password of type EFI key.</td>
</tr>
<tr>
<td>[/cpwdf]</td>
<td>Indicates file having admin password of type Unicode.</td>
</tr>
<tr>
<td>[/cpwdsf]</td>
<td>Indicates file having admin password of type scan code.</td>
</tr>
<tr>
<td>[/cpwdef]</td>
<td>Indicates file having admin password of type EFI key.</td>
</tr>
<tr>
<td>[/apwdf]</td>
<td>Indicates file having new admin password of type Unicode.</td>
</tr>
<tr>
<td>[/apwdsf]</td>
<td>Indicates file having new admin password of type scan code.</td>
</tr>
<tr>
<td>[/apwdef]</td>
<td>Indicates file having new admin password of type EFI key.</td>
</tr>
<tr>
<td>[/upwdf]</td>
<td>Indicates file having new user password of type Unicode.</td>
</tr>
<tr>
<td>[/upwdsf]</td>
<td>Indicates file having new user password of type scan code.</td>
</tr>
<tr>
<td>[/upwdef]</td>
<td>Indicates file having new user password of type EFI key.</td>
</tr>
<tr>
<td>[/hb]</td>
<td>Optional command-line option to hide the tool information banner.</td>
</tr>
</tbody>
</table>
SNMP is a protocol used to exchange management information between different devices connected on a network. This guide will walk you through the process to get basic access to the BMC.

**Note** that only SNMP v3 is supported

### Installing

You can access the BMC via SNMP on any Linux node, but this tutorial will be focused on Ubuntu. First, you need to install SNMP.

```bash
$ apt-get install snmp
```

To be able to see Human readable MIB (instead of seeing the OID), also install the following package:

```bash
$ apt-get install snmp-mibs-downloader
```

### Configuration

Now that SNMP is installed, the next thing to do is to modify a user to enable SNMP.

**IMPORTANT:** Change the password to something longer than admin (minimum 8 characters) and enable SNMP access.

### Operating

To see a specific OID, use the following command, using the user created at the previous step:

```bash
snmpwalk -v3 -l authPriv -u admin -a SHA -A "superuser" -x DES -X "superuser" <host_IP> <OID>
```

To access sensors of the BMC, use the following command:

```bash
$ snmpwalk -v3 -l authPriv -u admin -a SHA -A "superuser" -x DES -X "superuser" <host_IP> SNMPv2-SMI::enterprises.20974.554
```

You can also grep the sensor of your choice:

```bash
$ snmpwalk -v3 -l authPriv -u admin -a SHA -A "superuser" -x DES -X "superuser" <host_IP> SNMPv2-SMI::enterprises.20974.554 | grep 2\.1\..\.21
```

The following MIBs are supported on CG2400:

- CG2400 User documentation 2-01-2023
- www.kontron.com
Here’s a table of the possible informations that can be found via SNMP on the BMC.

<table>
<thead>
<tr>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv2-MIB::sysObjectID.0</td>
<td>The value of sysUpTime at the time of the most recent change in state or value of any instance of sysORID.</td>
</tr>
<tr>
<td>DSMAN-EVENT-MIB::sysUpTimeInstance</td>
<td>The time (in hundreds of a second) since the network management portion of the system was last re-initialized.</td>
</tr>
<tr>
<td>SNMPv2-MIB::sysContact.0</td>
<td>The textual identification of the contact person for this managed node, together with information on how to contact this person if no contact information is known, the value is the zero-length string.</td>
</tr>
<tr>
<td>SNMPv2-MIB::sysName.0</td>
<td>An administratively-assigned name for this managed node. By convention, this is the node’s fully-qualified domain name.</td>
</tr>
<tr>
<td>SNMPv2-MIB::sysLocation.0</td>
<td>The physical location of this node (e.g., ‘telephone closet, 3rd floor’).</td>
</tr>
<tr>
<td>SNMPv2-MIB::sysORLastChange.0</td>
<td>The value of sysUpTime at the time of the most recent change in state or value of any instance of sysORID.</td>
</tr>
<tr>
<td>SNMPv2-MIB::sysORTable</td>
<td>The (conceptual) table listing the capabilities of the local SNMP application acting as a command responder with respect to various MIB modules. SNMP entities having dynamically-configurable support of MIB modules will have a dynamically- varying number of conceptual rows.</td>
</tr>
<tr>
<td>IF-MIB::ifNumber.0</td>
<td>The number of network interfaces (regardless of their current state) present on this system.</td>
</tr>
<tr>
<td>IF-MIB::ifTable</td>
<td>A list of interface entries. The number of entries is given by the value of ifNumber. The entries consist of these fields.</td>
</tr>
<tr>
<td>IF-MIB::ifIndex.0</td>
<td>Index, Descr, Type, Mtu, Speed, PhysAddress, AdminStatus, OperStatus, LastChange, InOctets, InUcastPkts, InNUcastPkts, InErrors, InUnknownProtos, OutOctets, OutUcastPkts, OutNUcastPkts, OutDiscards, OutErrors, OutOctets.</td>
</tr>
<tr>
<td>IP-MIB::ipForwDatagrams</td>
<td>The number of input datagrams discarded because the IP address in their IP header’s destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.</td>
</tr>
<tr>
<td>IP-MIB::ipDefaultTTL</td>
<td>The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol.</td>
</tr>
<tr>
<td>IP-MIB::ipInReceives</td>
<td>The total number of input datagrams received from interfaces, including those received in error.</td>
</tr>
<tr>
<td>IP-MIB::ipInAddrErrors</td>
<td>The number of input datagrams discarded because the IP address in their IP header’s destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.</td>
</tr>
<tr>
<td>IP-MIB::ipInUnknownProtos</td>
<td>The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.</td>
</tr>
<tr>
<td>IP-MIB::ipInDiscards</td>
<td>The number of input datagrams discarded while awaiting re-assembly.</td>
</tr>
<tr>
<td>IP-MIB::ipInDelivers</td>
<td>The total number of input datagrams successfully delivered to IP user-protocols.</td>
</tr>
<tr>
<td>IP-MIB::ipOutRequests</td>
<td>The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for...</td>
</tr>
<tr>
<td>MIB Object</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>ip-out-discards</td>
<td>The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipforwarded datagrams if any such packets met this (discretionary) discard criterion.</td>
</tr>
<tr>
<td>ip-out-no-routes</td>
<td>The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipforwarded datagrams which meet this 'no-route' criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.</td>
</tr>
<tr>
<td>ip-reasm-timeout</td>
<td>The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.</td>
</tr>
<tr>
<td>ip-reasm-reqds</td>
<td>Number of IP fragments received which needed to be reassembled at this entity.</td>
</tr>
<tr>
<td>ip-reasm-dqos</td>
<td>Number of IP datagrams successfully re-assembled.</td>
</tr>
<tr>
<td>ip-reasm-fails</td>
<td>The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 2116) can lose track of the number of fragments by combining them as they are received.</td>
</tr>
<tr>
<td>ip-frag-creates</td>
<td>Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.</td>
</tr>
<tr>
<td>ip-frag-fails</td>
<td>The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.</td>
</tr>
<tr>
<td>ip-frag-dqos</td>
<td>Number of IP datagrams that have been successfully fragmented at this entity.</td>
</tr>
<tr>
<td>ip-addr-table</td>
<td>Table of addressing information relevant to this entity's IP addresses.</td>
</tr>
<tr>
<td>ip-routing-discards</td>
<td>The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.</td>
</tr>
<tr>
<td>ip-routing-table</td>
<td>This entity's IP Routing table.</td>
</tr>
<tr>
<td>ip-net-to-media-table</td>
<td>IP Address Translation table used for mapping from IP addresses to physical addresses.</td>
</tr>
<tr>
<td>ip-routing-discards</td>
<td>The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.</td>
</tr>
<tr>
<td>ip-system-stats-table</td>
<td>The table containing system wide, IP version specific traffic statistics. This table and the ipIfStatsTable contain similar objects whose difference is in their granularity. Where this table contains system wide traffic statistics, the ipIfStatsTable contains the same statistics but counted on a per-interface basis. The ipSystemStatsTable contains the same statistics but counted on a per-interface basis.</td>
</tr>
<tr>
<td>ipIfStatsTableLastChange</td>
<td>The value of sysUpTime on the most recent occasion at which a row in the ipIfStatsTable was added or deleted. If new objects are added to the ipIfStatsTable that require the ipIfStatsTableLastChange to be updated when they are modified, they must specify that requirement in their description clause.</td>
</tr>
<tr>
<td>ipIfStatsTable</td>
<td>The table containing per-interface traffic statistics. This table and the ipSystemStatsTable contain similar objects whose difference is in their granularity. Where this table contains per-interface statistics, the ipSystemStatsTable contains the same statistics, but counted on a system wide basis.</td>
</tr>
<tr>
<td>ipAddressPrefixTable</td>
<td>This table allows the user to determine the source of an IP address or set of IP addresses, and allows other tables to share the information via pointer rather than by copying. More information can be found here <a href="http://oidref.com/1.3.6.1.2.1.4.33">http://oidref.com/1.3.6.1.2.1.4.33</a></td>
</tr>
<tr>
<td>ipAddressSpinLock</td>
<td>An advisory lock used to allow cooperating SNMP managers to coordinate their use of the set operation in creating or modifying rows within this table. More information can be found here <a href="http://oidref.com/1.3.6.1.2.1.4.33">http://oidref.com/1.3.6.1.2.1.4.33</a></td>
</tr>
<tr>
<td>ipAddressTable</td>
<td>This table contains addressing information relevant to the entity's interfaces. More information can be found here <a href="http://oidref.com/1.3.6.1.2.1.4.33">http://oidref.com/1.3.6.1.2.1.4.33</a></td>
</tr>
<tr>
<td>ipNetToPhysicalTable</td>
<td>The IP Address Translation table used for mapping from IP addresses to physical addresses. The Address Translation tables contain the IP address to 'physical' address equivalences. Some interfaces do not use translation tables for determining address equivalences (e.g., DDN-X.25 has an algorithmic method); if all interfaces are of this type, then the Address Translation table is empty, i.e., has zero entries. While many protocols may be used to populate this table, ARP and Neighbor Discovery are the most likely options.</td>
</tr>
<tr>
<td>ipv5ScopeZoneIndexTable</td>
<td>The table used to describe IPv5 unicast and multicast scope zones. For those objects that have names rather than numbers, the names were chosen to coincide with the names used in the IPv5 address architecture document.</td>
</tr>
<tr>
<td>ipv5DefaultRouterTable</td>
<td>The table used to describe the default routers known to this entity.</td>
</tr>
<tr>
<td>icmpinMsgs</td>
<td>The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpinErrors.</td>
</tr>
</tbody>
</table>
IP-MIB::icmpInErrors
The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).

GET

IP-MIB::icmpInDestUnreachs
The number of ICMP Destination Unreachable messages received.

GET

IP-MIB::icmpInTimeExcds
Number of ICMP Time Exceeded messages received.

GET

IP-MIB::icmpInParmProbs
Number of ICMP Parameter Problem messages received.

GET

IP-MIB::tcpAttemptFails
The number of times that TCP connections have made a direct transition to the CLOSED state from either the SYN-RCVD state, or the SYN-SENT state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.

GET

IP-MIB::tcpMaxConn
The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

GET

IP-MIB::tcpMaxConn
The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

GET

IP-MIB::tcpMaxConn
The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

GET

IP-MIB::tcpMaxConn
The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

GET

IP-MIB::tcpMaxConn
The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

GET

IP-MIB::tcpMaxConn
The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

GET

IP-MIB::tcpMaxConn
The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

GET

TCP-MIB::tcpRtoMin
The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.

GET

TCP-MIB::tcpRtoMax
The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.

GET

TCP-MIB::tcpActiveOpens
The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.

GET

TCP-MIB::tcpResets
The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.

GET

TCP-MIB::tcpEstabResets
The number of times that TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times that TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.

GET

TCP-MIB::tcpCurrEstab
The number of currently established connections.

GET

TCP-MIB::tcpInSegs
The total number of segments received, including those received in error. This count includes segments received on currently established connections.

GET
<p>| <strong>SNMPv2-MIB::snmpOutTooBigs</strong> | The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field was <code>tooBig</code>. |
| <strong>SNMPv2-MIB::snmpInTraps</strong> | The total number of SNMP Trap PDUs which have been accepted and processed by the SNMP protocol entity. |
| <strong>SNMPv2-MIB::snmpInGetResponses</strong> | The total number of SNMP Get-Response PDUs which have been accepted and processed by the SNMP protocol entity. |
| <strong>SNMPv2-MIB::snmpInSetRequests</strong> | The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity. |
| <strong>SNMPv2-MIB::snmpInGetRequests</strong> | The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity. |
| <strong>SNMPv2-MIB::snmpInTotalSetVars</strong> | The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs. |
| <strong>SNMPv2-MIB::snmpInTotalReqVars</strong> | The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request PDUs. |
| <strong>SNMPv2-MIB::snmpInReadOnlys</strong> | The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was <code>readOnly</code>. |
| <strong>SNMPv2-MIB::snmpInBadValues</strong> | The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was <code>badValue</code>. |
| <strong>SNMPv2-MIB::snmpInNoSuchNames</strong> | The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was <code>noSuchName</code>. |
| <strong>SNMPv2-MIB::snmpInTooBigs</strong> | The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was <code>tooBig</code>. |
| <strong>SNMPv2-MIB::snmpInBadVersions</strong> | The total number of SNMP Messages which were delivered to the SNMP protocol entity and were for an unsupported SNMP version. |
| <strong>SNMPv2-MIB::snmpInBadCommunityNames</strong> | The total number of SNMP Messages delivered to the SNMP protocol entity which used a SNMP community name not known to said entity. |
| <strong>SNMPv2-MIB::snmpInBadCommunityUsers</strong> | The total number of community-based SNMP messages (for example, SNMPv1) delivered to the SNMP entity which represented an SNMP operation that was not allowed for the SNMP community named in the message. |
| <strong>UDP-MIB::udpNoPorts</strong> | The total number of UDP datagrams delivered to UDP users. |
| <strong>TCP-MIB::tcpOutRsts</strong> | The number of TCP segments sent containing the RST flag. |
| <strong>TCP-MIB::tcpConnectionProcess</strong> | The state of this TCP connection. More information can be found here <a href="https://oidref.com/1.3.6.1.2.1.6.12">https://oidref.com/1.3.6.1.2.1.6.12</a>. |
| <strong>TCP-MIB::tcpListenerTable</strong> | A table containing TCP connection-specific information. |
| <strong>TCP-MIB::tcpInErrs</strong> | The total number of segments received in error (e.g., bad TCP checksums). |
| <strong>TCP-MIB::tcpOutErrors</strong> | The number of TCP segments sent containing the RST flag. |
| <strong>UDP-MIB::udpInDatagrams</strong> | The total number of UDP datagrams delivered to UDP users. |
| <strong>UDP-MIB::udpInDatagrams</strong> | The total number of UDP datagrams delivered to UDP users. |
| <strong>UDP-MIB::udpInErrors</strong> | The total number of UDP datagrams which could not be delivered for reasons other than the lack of an application at the destination port. |
| <strong>UDP-MIB::udpOutDatagrams</strong> | The total number of UDP datagrams sent from this entity. |
| <strong>UDP-MIB::udpInTable</strong> | A table containing UDP listener information. |
| <strong>UDP-MIB::udpOutTable</strong> | A table containing UDP listener information. |
| <strong>SNMPv2-MIB::snmpInPkts</strong> | The total number of messages delivered to the SNMP entity from the transport service. |
| <strong>SNMPv2-MIB::snmpOutPkts</strong> | The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service. |
| <strong>UDP-MIB::udpInDatagrams</strong> | The total number of UDP datagrams delivered to UDP users. |
| <strong>UDP-MIB::udpOutDatagrams</strong> | The total number of UDP datagrams sent from this entity. |
| <strong>UDP-MIB::udpTable</strong> | A table containing UDP listener information. |</p>
<table>
<thead>
<tr>
<th>MIB</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISMAN-EVENT-MIB::mteTriggerFailures</td>
<td>The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field was 'tooBig'.</td>
<td>GET</td>
</tr>
<tr>
<td>DISMAN-EVENT-MIB::mteTriggerRequests</td>
<td>The total number of SNMP Get-Request PDUs which have been generated by the SNMP protocol entity.</td>
<td>GET</td>
</tr>
<tr>
<td>DISMAN-EVENT-MIB::mteTriggerGetRequests</td>
<td>The total number of SNMP Get-Next PDUs which have been generated by the SNMP protocol entity.</td>
<td>GET</td>
</tr>
<tr>
<td>DISMAN-EVENT-MIB::mteTriggerSetRequests</td>
<td>The total number of SNMP Set-Request PDUs which have been generated by the SNMP protocol entity.</td>
<td>GET</td>
</tr>
<tr>
<td>DISMAN-EVENT-MIB::mteResourceSampleInstancesHigh</td>
<td>The highest number of instance entries as defined for mteResourceSampleInstanceMaximum.</td>
<td>GET</td>
</tr>
<tr>
<td>DISMAN-EVENT-MIB::mteResourceSampleInstances</td>
<td>The number of currently active instance entries as defined for mteResourceSampleInstanceMaximum.</td>
<td>GET</td>
</tr>
<tr>
<td>DISMAN-EVENT-MIB::mteTriggerFailuresHigh</td>
<td>The highest value of mteResourceSampleInstances that has occurred since initialization of the management system.</td>
<td>GET</td>
</tr>
<tr>
<td>DISMAN-EVENT-MIB::mteTriggerFailuresLow</td>
<td>The number of times this system could not take a new sample because that allocation would have exceeded the limit set by mteResourceSampleInstanceMaximum.</td>
<td>GET</td>
</tr>
<tr>
<td>DISMAN-EVENT-MIB::mteTriggerFailures</td>
<td>The minimum mteTriggerFrequency this system will accept. A system may use the larger values of this minimum to lessen the impact of constant sampling. For larger sampling intervals the system samples less often and suffers less overhead. This object provides a way to enforce such lower overhead for all triggers.</td>
<td>GET</td>
</tr>
<tr>
<td>IPV6-MIB::ipv6DefaultHopLimit</td>
<td>The default value inserted into the Hop Limit field of the IPv6 header of datagrams originated at this entity, whenever a Hop Limit value is not supplied by the transport layer protocol.</td>
<td>GET</td>
</tr>
<tr>
<td>IPV6-MIB::ipv6DefaultInterfaces</td>
<td>The number of IPv6 interfaces (regardless of their current state) present on this system.</td>
<td>GET</td>
</tr>
<tr>
<td>IPV6-MIB::ipv6IfTable</td>
<td>The IPv6 Interfaces table contains information on the entity's internetwork-layer interfaces. An IPv6 interface constitutes a logical network layer attachment to the layer immediately below IPv6 including internet layer 'tunnels', such as tunnels over IPv4 or IPv6 itself.</td>
<td>GET</td>
</tr>
<tr>
<td>HOST-RESOURCES-MIB::hrSystemDate</td>
<td>The host's notion of the local date and time of day.</td>
<td>GET</td>
</tr>
<tr>
<td>HOST-RESOURCES-MIB::hrSystemUptime</td>
<td>The amount of time since this host was last initialized. Note that this is different from sysUpTime in MIB-II [3] because sysUpTime is the uptime of the network management portion of the system.</td>
<td>GET</td>
</tr>
<tr>
<td>HOST-RESOURCES-MIB::hrSystemInitialLoadParameters</td>
<td>This object contains the parameters (e.g. a pathname and parameter) supplied to the load device when requesting the initial operating system configuration from that device.</td>
<td>GET</td>
</tr>
<tr>
<td>HOST-RESOURCES-MIB::hrSystemInitialLoadDevice</td>
<td>The index of the hrDeviceEntry for the device from which this host is configured to load its initial operating system configuration.</td>
<td>GET</td>
</tr>
<tr>
<td>HOST-RESOURCES-MIB::hrSystemInitialLoadParameters</td>
<td>This object contains the parameters (e.g. a pathname and parameter) supplied to the load device when requesting the initial operating system configuration from that device.</td>
<td>GET</td>
</tr>
<tr>
<td>MTA-MIB::mtaTable</td>
<td>The table holding information specific to an MTA.</td>
<td>GET</td>
</tr>
<tr>
<td>MTA-MIB::mtaGroupTable</td>
<td>The table holding information specific to each MTA group.</td>
<td>GET</td>
</tr>
<tr>
<td>IF-MIB::ifTable</td>
<td>A list of interface entries. The number of entries is given by the value of ifNumber. This table contains additional objects for the interface table.</td>
<td>GET</td>
</tr>
<tr>
<td>IF-MIB::ifTableLastChange</td>
<td>The value of sysUpTime at the time of the last creation or deletion of an entry in the ifTable. If the number of entries has been unchanged since the last re-initialization of the local network management subsystem, then this object contains a zero value.</td>
<td>GET</td>
</tr>
<tr>
<td>IPV6-MIB::ipv6Forwarding</td>
<td>The indication of whether this entity is acting as an IPv6 router in respect to the forwarding of datagrams received by, but not addressed to, this entity. IPv6 routers forward datagrams. IPv6 hosts do not (except those source-routed via the host). More information can be found here [3].</td>
<td>GET</td>
</tr>
<tr>
<td>IPV6-MIB::ipv6DefaultHopLimit</td>
<td>The default value inserted into the Hop Limit field of the IPv6 header of datagrams originated at this entity, whenever a Hop Limit value is not supplied by the transport layer protocol.</td>
<td>GET</td>
</tr>
<tr>
<td>IPV6-MIB::ipv6DefaultInterfaces</td>
<td>The number of IPv6 interfaces (regardless of their current state) present on this system.</td>
<td>GET</td>
</tr>
<tr>
<td>IPV6-MIB::ipv6IfTable</td>
<td>The IPv6 Interfaces table contains information on the entity's internetwork-layer interfaces. An IPv6 interface constitutes a logical network layer attachment to the layer immediately below IPv6 including internet layer 'tunnels', such as tunnels over IPv4 or IPv6 itself.</td>
<td>GET</td>
</tr>
<tr>
<td>DISMAN-EVENT-MIB::mteResourceSampleMinimum</td>
<td>The minimum mteTriggerFrequency this system will accept. A system may use the larger values of this minimum to lessen the impact of constant sampling. For larger sampling intervals the system samples less often and suffers less overhead. This object provides a way to enforce such lower overhead for all triggers created after it is set. More information can be found here [3].</td>
<td>GET</td>
</tr>
</tbody>
</table>
minimum to lessen the impact of constant sampling. For larger sampling intervals the system samples less often and suffers less overhead. This object provides a way to enforce such lower overhead for all triggers created after it is set.

**DISMAN-EVENT-MIB::mteObjectsTable**
A table of objects that can be added to notifications based on the trigger, trigger test, or event, as pointed to by entries in those tables.

**DISMAN-EVENT-MIB::mteEventTable**
A table of management event action information.

**DISMAN-EVENT-MIB::mteEventNotificationTable**
A table of information about notifications to be sent as a consequence of management events.

**NOTIFICATION-LOG-MIB::nlmStatsGlobalNotificationsBumped**
The number of log entries discarded to make room for a new entry due to lack of resources or the value of nlmConfigGlobalEntryLimit or nlmConfigLogEntryLimit. This does not include entries discarded due to the value of nlmConfigGlobalAgeOut.

**NOTIFICATION-LOG-MIB::nlmStatsGlobalNotificationsLogged**
The number of Notifications put into the nlmLogTable. This counts a Notification once for each log entry, so a Notification put into multiple logs is counted multiple times.

**NOTIFICATION-LOG-MIB::nlmConfigGlobalAgeOut**
The number of minutes a Notification SHOULD be kept in a log before it is automatically removed. If an application changes the value of nlmConfigGlobalAgeOut, Notifications older than the new time MAY be discarded to meet the new time. A value of 0 means no age out. Please be aware that contention between multiple managers trying to set this object to different values MAY affect the reliability and completeness of data seen by each manager.

**NOTIFICATION-LOG-MIB::nlmStatsGlobalNotificationsLogged**
The number of Notifications put into the nlmLogTable. This counts a Notification once for each log entry, so a Notification put into multiple logs is counted multiple times.

**SNMPv2-SMI::enterprises.3582**

**NET-SNMP-VACM-MIB::nsVacmContextMatch**
If the value of this object is exact(1), then all rows where the contextName exactly matches vacmContextPrefix are selected. If the value of this object is prefix(2), then all rows where the contextName whose starting octets exactly match vacmContextPrefix are selected. This allows for a simple form of wildcarding. The value of this object should be consistent across all nsVacmAccessEntries corresponding to a single row of the vacmAccessTable.

**NET-SNMP-VACM-MIB::nsVacmViewName**
The MIB view authorised for the appropriate style of processing (as indicated by nsVacmToken). The interpretation of this value is the same as for the standard VACM ViewName objects.

**NET-SNMP-VACM-MIB::nsVacmStorageType**
The storage type for this (group of) conceptual rows. Conceptual rows having the value ‘permanent’ need not allow write-access to any columnar objects in the row. The value of this object should be consistent across all nsVacmAccessEntries corresponding to a single row of the vacmAccessTable.

**NET-SNMP-VACM-MIB::nsVacmStatus**
The status of this (group of) conceptual rows. The RowStatus TC [RFC2579] requires that this DESCRIPTION clause states under which circumstances other objects in this row can be modified. The value of this object has no effect on whether other objects in this conceptual row can be modified. The value of this object should be consistent across all nsVacmAccessEntries corresponding to a single row of the vacmAccessTable.

**SNMPv2-SMI::enterprises.20974.554.1**
AMI SNMP Hostname Extension

**SNMPv2-SMI::enterprises.20974.554.2**
AMI SNMP MIB library to return the system health status like power and sensor status.

**SNMPv2-SMI::enterprises.20974.554.3**
AMI SNMP Platform Info Extension
**Tool**

The `snmptranslate` command is useful to translate numeric OID to the MIB module name.

```
$ snmptranslate 1.3.6.1.4.1.2021
UCD-SNMP-MIB::ucdavis
```
# BIOS configuration of CG2300 compared to CG2400

## Table of contents
- Boot configuration
- Networking
  - Network interface availability
  - Preboot Execution Environment (PXE)
  - iSCSI
  - Network stack
- BIOS password
- Power management
- Virtualization
  - Compatibility Support Module (CSM)
- Security
  - Secure boot
  - Trusted Platform Module (TPM)
  - Trusted Execution Technology (TXT)
- Console redirection
- Error logging

The following tables provide menu paths for the CG2300 and the CG2400. This is a partial list that includes the most common configuration parameters. Since the CG2300 uses the Intel EFI code base and the CG2400 uses the AMI EFI code base, the setup menus are referred to as the INTEL SETUP and the AMI SETUP. In the lists of possible values, the value in **bold, underline** is the default value.

## Boot configuration

<table>
<thead>
<tr>
<th>CG2300</th>
<th>CG2400</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu → Boot Manager</td>
<td>Menu → Save &amp; Exit → Section Boot Override</td>
<td></td>
</tr>
<tr>
<td>Menu → Boot Maintenance Manager → Advanced Boot Options → Boot Option Retry [Enabled / Disabled]</td>
<td>Not present in AMI SETUP</td>
<td>Boot Option Retry is always enabled on the CG2400.</td>
</tr>
<tr>
<td>Menu → Boot Maintenance Manager → Advanced Boot Options → USB Boot Priority [Enabled / Disabled]</td>
<td>Not present in AMI SETUP</td>
<td></td>
</tr>
<tr>
<td>Menu → Boot Maintenance Manager → Add EFI Boot Option → &lt;Dynamic list of EFI Boot Options&gt;</td>
<td>Menu → Boot → Section Boot Option Priorities</td>
<td></td>
</tr>
<tr>
<td>Menu → Boot Maintenance Manager → Delete EFI Boot Option → &lt;Dynamic list of EFI Boot Options&gt;</td>
<td>Not present in AMI SETUP</td>
<td></td>
</tr>
<tr>
<td>Menu → Boot Maintenance Manager → Change Boot Order → &lt;Dynamic list of EFI Boot Options&gt;</td>
<td>Not present in AMI SETUP</td>
<td></td>
</tr>
</tbody>
</table>

## Networking

### Network interface availability

<table>
<thead>
<tr>
<th>CG2300</th>
<th>CG2400</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu → Advanced → PCI Configuration → NIC Configuration → Nic1 Controller [Enabled / Disabled]</td>
<td>Menu → Socket Configuration → IIO Configuration → Socket0 Configuration → Socket 0 PcieBr1D02F0 - Port 1C (PCIe Uplink) → PCI-E Port [Auto / Disable / Enable]</td>
<td>On the CG2400, both controllers are auto/enabled/disabled at the same time.</td>
</tr>
<tr>
<td>Menu → Advanced → PCI Configuration → NIC Configuration → Nic1 Port1 [Enabled / Disabled]</td>
<td>Menu → Advanced → PCI Configuration → NIC Configuration → Nic1 Port2 [Enabled / Disabled]</td>
<td>On the CG2300, this option is only available if Nic1 Controller is enabled.</td>
</tr>
</tbody>
</table>

### Preboot Execution Environment (PXE)

<table>
<thead>
<tr>
<th>CG2300</th>
<th>CG2400</th>
<th>Notes</th>
</tr>
</thead>
</table>

### iSCSI

<table>
<thead>
<tr>
<th>CG2300</th>
<th>CG2400</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu → Advanced → PCI Configuration → UEFI Option ROM Control → iSCSI Configuration</td>
<td>Menu → Advanced → iSCSI Configuration →</td>
<td></td>
</tr>
</tbody>
</table>

### Network stack
### BIOS password

<table>
<thead>
<tr>
<th>CG2300</th>
<th>CG2400</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu → Advanced → Security → Set Administrator Password</td>
<td>Menu → Security → Administrator Password</td>
<td></td>
</tr>
<tr>
<td>Menu → Security → Set User Password</td>
<td>Menu → Security → User Password</td>
<td></td>
</tr>
</tbody>
</table>

### Power management

<table>
<thead>
<tr>
<th>CG2300</th>
<th>CG2400</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu → Advanced → PCI Configuration → UEFI Option ROM Control → Intel(R) I350 Gigabit Network Connection - MAC Address of NIC1 → NIC Configuration → Link Speed [Auto Negotiated / 10 Mbps Half / 10 Mbps Full / 100 Mbps Half / 100 Mbps Full]</td>
<td>Menu → Advanced → Intel(R) Ethernet Connection X722 for 10GBASE-T - MAC-ADDRESS-1 → NIC Configuration → Link Speed [Auto Negotiated]</td>
<td>On the CG2400, this option is read only.</td>
</tr>
<tr>
<td>Menu → Advanced → PCI Configuration → UEFI Option ROM Control → Intel(R) I350 Gigabit Network Connection - MAC Address of NIC1 → Blink LEDs [0 / &lt;Number&gt;]</td>
<td>Menu → Advanced → Intel(R) Ethernet Connection X722 for 10GBASE-T - MAC-ADDRESS-1 → Blink LEDs [0 / &lt;0-15&gt;]</td>
<td></td>
</tr>
<tr>
<td>Menu → Advanced → PCI Configuration → UEFI Option ROM Control → Intel(R) I350 Gigabit Network Connection - MAC Address of NIC1 → VLAN Configuration → Enter Configuration Menu</td>
<td>Menu → Advanced → VLAN Configuration (MAC, MAC-ADDRESS-1) → Enter Configuration Menu</td>
<td></td>
</tr>
<tr>
<td>Menu → Advanced → PCI Configuration → UEFI Option ROM Control → Intel(R) I350 Gigabit Network Connection - MAC Address of NIC1 → IPv4 Current settings</td>
<td>Menu → Advanced → MAC: MAC-ADDRESS-1 → IPv4 Network Configuration → Enter Configuration Menu</td>
<td></td>
</tr>
<tr>
<td>Menu → Advanced → PCI Configuration → UEFI Option ROM Control → Intel(R) I350 Gigabit Network Connection - MAC Address of NIC1 → IPv6 Current settings</td>
<td>Menu → Advanced → MAC: MAC-ADDRESS-1 → IPv6 Network Configuration → Enter Configuration Menu</td>
<td></td>
</tr>
</tbody>
</table>
**Virtualization**

<table>
<thead>
<tr>
<th>CG2300</th>
<th>CG2400</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CG2300</td>
<td>CG2400</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Not present in INTEL SETUP</td>
<td>Menu → Advanced → CSM Configuration → CSM Support [Enabled / Disabled]</td>
<td></td>
</tr>
<tr>
<td>Menu → Boot Maintenance Manager → Advanced Boot Options → Boot Mode [UEFI / Legacy]</td>
<td>Menu → Advanced → CSM Configuration → Boot option filter [UEFI and Legacy / Legacy only / UEFI only]</td>
<td>On CG2400, this option is only available if CSM Support is enabled.</td>
</tr>
<tr>
<td>Menu → Boot Maintenance Manager → Advanced Boot Options → Video BIOS [UEFI / Legacy]</td>
<td>Menu → Advanced → CSM Configuration → Video [UEFI / Legacy]</td>
<td>On CG2400, this option is only available if CSM Support is enabled.</td>
</tr>
</tbody>
</table>

## Security

### Secure boot

<table>
<thead>
<tr>
<th>CG2300</th>
<th>CG2400</th>
<th>Notes</th>
</tr>
</thead>
</table>

## Trusted Platform Module (TPM)

<table>
<thead>
<tr>
<th>CG2300</th>
<th>CG2400</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu → Security → TPM2 Operation [NoAction / TPM2 ClearControl(NO) + Clear]</td>
<td>Menu → Advanced → Trusted Computing → TPM2.0 UEFI Spec Version [TCG_1.2_ / TCG_2 ]</td>
<td>On both platforms, TPM has to be inserted to see the menu.</td>
</tr>
<tr>
<td>Menu → Security → TPM FW Update [Enabled / Disabled]</td>
<td>Not present in AMI SETUP</td>
<td></td>
</tr>
<tr>
<td>Menu → Advanced → PCI Configuration → UEFI Option ROM Control [Dynamic Menu]→ TrEE Configuration → Attempt TPM Device [Disable / TPM 1.2_ / TPM 2.0 (DTPM)]</td>
<td>Menu → Advanced → Trusted Computing → Device Select [TPM 1.2 / TPM 2.0 / Auto]</td>
<td>On both platforms, TPM has to be inserted to see the menu.</td>
</tr>
</tbody>
</table>

## Trusted Execution Technology (TXT)

<table>
<thead>
<tr>
<th>CG2300</th>
<th>CG2400</th>
<th>Notes</th>
</tr>
</thead>
</table>

## Console redirection

<table>
<thead>
<tr>
<th>CG2300</th>
<th>CG2400</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu → Server Management → Console Redirection → SOL for Baseboard Mgmt [Enabled / Disabled]</td>
<td>Not present in AMI SETUP</td>
<td></td>
</tr>
<tr>
<td>Menu → Server Management → Console Redirection → Console Redirection [Disabled / Serial Port A / Serial Port B]</td>
<td>Menu → Advanced → Serial Port Console Redirection → Console Redirection Settings → Flow Control [None / Hardware RTS/CTS]</td>
<td>On the CG2300, the option is only shown if Console Redirection is enabled.</td>
</tr>
<tr>
<td>Menu → Server Management → Console Redirection → Flow Control [None / RTS/CTS ]</td>
<td>Menu → Advanced → Serial Port Console Redirection → Console Redirection Settings → Flow Control [None / Hardware RTS/CTS]</td>
<td>On the CG2300, the option is only shown if Console Redirection is enabled.</td>
</tr>
<tr>
<td>Menu → Server Management → Console Redirection → Baud Rate [9.6k / 19.2k / 38.4k / 57.6k / 115.2k ]</td>
<td>Menu → Advanced → Serial Port Console Redirection → Console Redirection Settings → Baud Rate [9600 / 19200 / 38400 / 57600 / 115200]</td>
<td>On the CG2300, the option is only shown if Console Redirection is enabled.</td>
</tr>
<tr>
<td>Menu → Server Management → Console Redirection → Terminal Type [PC-ANSI / VT100 / VT100+ / VT-UTF8]</td>
<td>Menu → Advanced → Serial Port Console Redirection → Console Redirection Settings → Terminal Type [VT100 / VT100+ / VT-UTF8 / ANSI]</td>
<td>On the CG2300, the option is only shown if Console Redirection is enabled.</td>
</tr>
<tr>
<td>Menu → Server Management → Console Redirection → Legacy OS Redirection [Enabled / Disabled]</td>
<td>Menu → Advanced → Serial Port Console Redirection → Legacy Console Redirection Settings → Redirect After POST [Always Enable / BootLoader]</td>
<td>On the CG2300, the option is only shown if Console Redirection is enabled.</td>
</tr>
<tr>
<td>Menu → Server Management → Console Redirection → Terminal Resolution [80x24 / 100x31]</td>
<td>Menu → Advanced → Serial Port Console Redirection → Legacy Console Redirection Settings → Resolution [80x24 / 80x25]</td>
<td>On the CG2300, the option is only shown if Console Redirection is enabled.</td>
</tr>
<tr>
<td>CG2300</td>
<td>CG2400</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Menu → Server Management → Clear System Event Log &lt;ENTER&gt;</td>
<td>Menu → Server Mgmt → System Event Log → Erase SEL → No / Yes, On next reset / Yes, On every reset</td>
<td></td>
</tr>
<tr>
<td>Menu → Server Mgmt → System Event Log → When SEL is Full</td>
<td>Do Nothing / Erase immediately / Delete Oldest Record</td>
<td></td>
</tr>
<tr>
<td>Menu → Server Mgmt → System Event Log → Log EFI Status</td>
<td>Do Nothing / Erase immediately / Delete Oldest Record</td>
<td></td>
</tr>
<tr>
<td>Codes (Disabled / Both / Error code / Progress code)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Menu → Advanced → Memory Configuration → Select Memory</td>
<td>Menu → Socket Configuration → Memory Configuration → Memory RAS Configuration → System Physical Address</td>
<td>On the CG2400, the option shown varies according to the type of memory installed in the system.</td>
</tr>
<tr>
<td>RAS and Performance Configuration → Static Virtual Lockstep Mode</td>
<td>[Enable / Disable]</td>
<td></td>
</tr>
<tr>
<td>Menu → Advanced → Memory Configuration → Memory</td>
<td>Menu → Socket Configuration → Memory Configuration → Memory RAS Configuration → System Physical Address</td>
<td></td>
</tr>
<tr>
<td>RAS and Performance Configuration → Demand Scrub [Enabled / Disabled]</td>
<td>[Enable / Disable]</td>
<td></td>
</tr>
<tr>
<td>Menu → Advanced → Memory Configuration → Memory</td>
<td>Menu → Socket Configuration → Memory Configuration → Memory RAS Configuration → System Physical Address</td>
<td></td>
</tr>
<tr>
<td>RAS and Performance Configuration → Correctable Error</td>
<td>[Enable / Disable]</td>
<td></td>
</tr>
<tr>
<td>Threshold [20 / All / 5 / None]</td>
<td>[Enable / Disable]</td>
<td></td>
</tr>
<tr>
<td>Menu → Advanced → Memory Configuration → Memory</td>
<td>Menu → Socket Configuration → Memory Configuration → Memory RAS Configuration → System Physical Address</td>
<td></td>
</tr>
<tr>
<td>RAS and Performance Configuration → Memory</td>
<td>[Enable / Disable]</td>
<td></td>
</tr>
<tr>
<td>Correctable Error Enabling [RAS and Performance Configuration]</td>
<td>[Enable / Disable]</td>
<td></td>
</tr>
<tr>
<td>Memory Configuration → Memory</td>
<td>[Enable / Disable]</td>
<td></td>
</tr>
<tr>
<td>Correctable Error Threshold [20 / 10 / 5 / All / None]</td>
<td>[Enable / Disable]</td>
<td></td>
</tr>
<tr>
<td>Menu → Server Management → Assert NMI on SERR [Enabled / Disabled]</td>
<td>Not present in AMI SETUP</td>
<td></td>
</tr>
<tr>
<td>Menu → Server Management → Assert NMI on PERR [Enabled / Disabled]</td>
<td>Not present in AMI SETUP</td>
<td></td>
</tr>
<tr>
<td>Menu → Server Management → PCIe AER Support [Enabled / Disabled]</td>
<td>Not present in AMI SETUP</td>
<td></td>
</tr>
<tr>
<td>Menu → Server Management → Log Correctable Errors</td>
<td>Menu → Platform Configuration → Runtime Error Logging → IIOD Error Enabling → IIOD PCIe AER Spec Compliant [Enable / Disable ]</td>
<td></td>
</tr>
<tr>
<td>[Enabled / Disabled]</td>
<td>Not present in AMI SETUP</td>
<td></td>
</tr>
<tr>
<td>Menu → Server Management → WHEA Support [Enabled / Disabled]</td>
<td>Not present in AMI SETUP</td>
<td></td>
</tr>
<tr>
<td>Menu → Server Management → Enable Cloaking [Enabled / Disabled]</td>
<td>Not present in AMI SETUP</td>
<td></td>
</tr>
<tr>
<td>Menu → Server Management → PCIe Correctable Error Threshold [20 / All / 5 / 10]</td>
<td>Not present in AMI SETUP</td>
<td></td>
</tr>
<tr>
<td>Menu → Server Management → Reset on CATERR [Enabled / Disabled]</td>
<td>Not present in AMI SETUP</td>
<td></td>
</tr>
<tr>
<td>Menu → Server Management → Reset on ERR2 [Enabled / Disabled]</td>
<td>Not present in AMI SETUP</td>
<td></td>
</tr>
</tbody>
</table>
mcelog - Identifying a faulty DIMM from error log

Machine check exceptions (MCEs) can occur for a variety of reasons ranging from undesired voltages from the power supply, from cosmic radiation flipping bits in memory DIMMs or the CPU, or from other miscellaneous faults, including faulty software triggering hardware errors.

The mcelog daemon

On modern x86 Linux systems, mcelog logs and accounts machine checks errors and exceptions. All errors are logged to `/var/log/mcelog` or `/syslog` or the journal in the following form:

```
Hardware event. This is not a software error.
MCE 0
CPU 0 BANK 1B
MISC 908400800000282B ADDR 9ce494000
TIME 1499161840 Tue Jul 4 09:50:40 2021
MCG status:
MG status:
Corrected error
MG_MISC register valid
MG_ADDR register valid
MCA: MEMORY CONTROLLER MS_CHANNEL2_ERR
Transaction: Memory scrubbing error
MemCtrl: Corrected patrol scrub error
STATUS Bc000001000B0002 MCGSTATUS 0
MCCAP 7000c16 APICID 0 SOCKETID 0
CPUID Vendor Intel Family 6 Model 05
```

On the processor family used on the CG2400, the following Machine Check banks are related to errors coming from one of the Internal Memory Controllers (IMC).

<table>
<thead>
<tr>
<th>Machine Bank Number</th>
<th>Processor Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>IMC 0, Main</td>
</tr>
<tr>
<td>8</td>
<td>IMC 1, Main</td>
</tr>
<tr>
<td>13</td>
<td>IMC 0, channel 0</td>
</tr>
<tr>
<td>14</td>
<td>IMC 0, channel 1</td>
</tr>
<tr>
<td>15</td>
<td>IMC 1, channel 0</td>
</tr>
<tr>
<td>16</td>
<td>IMC 1, channel 1</td>
</tr>
<tr>
<td>17</td>
<td>IMC 0, channel 2</td>
</tr>
<tr>
<td>18</td>
<td>IMC 1, channel 2</td>
</tr>
</tbody>
</table>

DIMMs location

There are 8 DIMM slots per CPU, but only 6 channels per CPU – A1 and A2 are on the same channel and D1 and D2 are on the same channel. Therefore, if the error is coming from either Machine Bank 13 or 15, it will not be possible to identify the exact faulty DIMM if A2 and/or D2 are populated.
Document symbols and acronyms

Symbols

The following symbols are used in Kontron documentation.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="DANGER" /></td>
<td>DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.</td>
</tr>
<tr>
<td><img src="image" alt="WARNING" /></td>
<td>WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.</td>
</tr>
<tr>
<td><img src="image" alt="CAUTION" /></td>
<td>CAUTION indicates a hazardous situation which, if not avoided, may result in minor or moderate injury.</td>
</tr>
<tr>
<td><img src="image" alt="NOTICE" /></td>
<td>NOTICE indicates a property damage message.</td>
</tr>
</tbody>
</table>

**Electric Shock!**
This symbol and title warn of hazards due to electrical shocks (> 60 V) when touching products or parts of them. Failure to observe the precautions indicated and/or prescribed by the law may endanger your life/health and/or result in damage to your material. Please also refer to the “High-Voltage Safety Instructions” portion below in this section.

**ESD Sensitive Device!**
This symbol and title inform that the electronic boards and their components are sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this product in order to ensure product integrity at all times.

**HOT Surface!**
Do NOT touch! Allow to cool before servicing.

This symbol indicates general information about the product and the documentation. This symbol also indicates detailed information about the specific product configuration.

This symbol precedes helpful hints and tips for daily use.

Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACPI</td>
<td>Advanced Configuration and Power Interface</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>ASIC</td>
<td>Application Specific Integrated Circuit</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic Input/Output System</td>
</tr>
<tr>
<td>BMC</td>
<td>Baseboard Management Controller</td>
</tr>
<tr>
<td>BSP</td>
<td>Board Support Package</td>
</tr>
<tr>
<td>CBIT</td>
<td>Continuous Built-In Test</td>
</tr>
<tr>
<td>CE</td>
<td>Community European (EU mark)</td>
</tr>
<tr>
<td>CLI</td>
<td>Command-Line Interface</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>CRMS</td>
<td>Communications Rack Mount Servers</td>
</tr>
<tr>
<td>CSA</td>
<td>Canadian Standards Association</td>
</tr>
<tr>
<td>DC</td>
<td>Direct Current</td>
</tr>
<tr>
<td>DDR4</td>
<td>Double Data Rate Fourth Generation</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DIMM</td>
<td>Dual Inline Memory Module</td>
</tr>
<tr>
<td>DRAM</td>
<td>Dynamic Random Access Memory</td>
</tr>
<tr>
<td>DTS</td>
<td>Digital Thermal Sensor</td>
</tr>
<tr>
<td>DU</td>
<td>Distributed Unit</td>
</tr>
<tr>
<td>ECC</td>
<td>Error Checking and Correcting</td>
</tr>
<tr>
<td>EEPROM</td>
<td>Electrically Erasable Programmable Read-Only Memory</td>
</tr>
<tr>
<td>EMC</td>
<td>Electromagnetic Compatibility</td>
</tr>
<tr>
<td>EMI</td>
<td>Electromagnetic Interference</td>
</tr>
<tr>
<td>ESD</td>
<td>Electrostatic Discharge</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>eUSB</td>
<td>Embedded Universal Serial Bus</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FH/FL</td>
<td>Full Height/Full Length</td>
</tr>
<tr>
<td>FPGA</td>
<td>Field Programmable Gate Array</td>
</tr>
<tr>
<td>FRAU</td>
<td>Field Replaceable Unit</td>
</tr>
<tr>
<td>FRU</td>
<td>Field Replaceable Unit</td>
</tr>
<tr>
<td>Gb, Gbit</td>
<td>Gigabit</td>
</tr>
<tr>
<td>GB, Gbyte</td>
<td>Gigabyte – 1024 MB</td>
</tr>
<tr>
<td>GbE</td>
<td>Gigabit Ethernet</td>
</tr>
<tr>
<td>GND</td>
<td>Ground</td>
</tr>
<tr>
<td>GPI</td>
<td>General Purpose Input</td>
</tr>
<tr>
<td>GPIO</td>
<td>General Purpose Input/Output</td>
</tr>
<tr>
<td>GPO</td>
<td>General Purpose Output</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GPU</td>
<td>Graphics Processing Unit</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>HDD</td>
<td>Hard Disk Drive</td>
</tr>
<tr>
<td>Hz</td>
<td>Hertz – 1 cycle/second</td>
</tr>
<tr>
<td>I/O</td>
<td>Input/Output</td>
</tr>
<tr>
<td>I²C</td>
<td>Inter-Integrated Circuit Bus</td>
</tr>
<tr>
<td>iBMC</td>
<td>Integrated Baseboard Management Controller</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IMU</td>
<td>Inertial Measurement Unit</td>
</tr>
<tr>
<td>IOL</td>
<td>IPMI over LAN</td>
</tr>
<tr>
<td>IPMB</td>
<td>Intelligent Platform Management Bus</td>
</tr>
<tr>
<td>IPMI</td>
<td>Intelligent Platform Management Interface</td>
</tr>
<tr>
<td>IRQ</td>
<td>Interrupt Request Line</td>
</tr>
<tr>
<td>KB, Kbyte</td>
<td>Kilobyte – 1024 bytes</td>
</tr>
<tr>
<td>KCS</td>
<td>Keyboard Controller Style</td>
</tr>
<tr>
<td>KEAPI</td>
<td>Kontron Embedded Application Programming Interface</td>
</tr>
<tr>
<td>KVM</td>
<td>Keyboard, Video, Mouse</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LED</td>
<td>Light-Emitting Diode</td>
</tr>
<tr>
<td>LP</td>
<td>Low Profile</td>
</tr>
<tr>
<td>LPC</td>
<td>Low Pin Count</td>
</tr>
<tr>
<td>LVDS</td>
<td>Low Voltage Differential SCSI</td>
</tr>
<tr>
<td>MAT</td>
<td>Maximum Ambient Temperature</td>
</tr>
<tr>
<td>MB, Mbyte</td>
<td>Megabyte – 1024 KB</td>
</tr>
<tr>
<td>MCU</td>
<td>Microcontroller</td>
</tr>
<tr>
<td>MEC</td>
<td>Multi-Access Edge Computing</td>
</tr>
<tr>
<td>MoM</td>
<td>Mobile PCI Express Module</td>
</tr>
<tr>
<td>NCSI</td>
<td>Network Communications Services Interface</td>
</tr>
<tr>
<td>NEBS</td>
<td>Network Equipment-Building System</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card, or Network Interface Controller, or Network Interface Controller port</td>
</tr>
<tr>
<td>NMI</td>
<td>Non-Maskable interrupt</td>
</tr>
<tr>
<td>NOS</td>
<td>Network Operating System</td>
</tr>
<tr>
<td>NVMe</td>
<td>Non-Volatile Memory Express</td>
</tr>
<tr>
<td>OCXO</td>
<td>Oven-Controlled Crystal Oscillator</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OTP</td>
<td>Over-Temperature Protection</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>OVP</td>
<td>Over-Voltage Protection</td>
</tr>
<tr>
<td>PBIT</td>
<td>Power On Built-In Test</td>
</tr>
<tr>
<td>PCH</td>
<td>Platform Controller Hub</td>
</tr>
<tr>
<td>PCI</td>
<td>Peripheral Component Interconnect</td>
</tr>
<tr>
<td>PCIe</td>
<td>Peripheral Component Interconnect Express</td>
</tr>
<tr>
<td>PECI</td>
<td>Platform Environment Control Interface</td>
</tr>
<tr>
<td>PIRQ</td>
<td>PCI Interrupt Request Line</td>
</tr>
<tr>
<td>PMbus</td>
<td>Power Management Bus</td>
</tr>
<tr>
<td>PMM</td>
<td>POST Memory Manager</td>
</tr>
<tr>
<td>PnP</td>
<td>Plug and Play</td>
</tr>
<tr>
<td>POST</td>
<td>Power-On Self Test</td>
</tr>
<tr>
<td>PSU</td>
<td>Power Supply Unit</td>
</tr>
<tr>
<td>PTP</td>
<td>Precision Time Protocol</td>
</tr>
<tr>
<td>PXE</td>
<td>Preboot eXecution Environment</td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Independent Disks</td>
</tr>
<tr>
<td>RAN</td>
<td>Radio Access Network</td>
</tr>
<tr>
<td>RAS</td>
<td>Reliability, Availability, and Serviceability</td>
</tr>
<tr>
<td>RDIMM</td>
<td>Registered Dual In-Line Memory Module</td>
</tr>
<tr>
<td>RDP</td>
<td>Remote Desktop</td>
</tr>
<tr>
<td>RMM</td>
<td>Remote Management Module</td>
</tr>
<tr>
<td>RoHS</td>
<td>Restriction of Hazardous Substances</td>
</tr>
<tr>
<td>SAS</td>
<td>Serial Attached SCSI (Small Computer System Interface)</td>
</tr>
<tr>
<td>SATA</td>
<td>Serial Advanced Technology Attachment</td>
</tr>
<tr>
<td>SCSI</td>
<td>Small Computer Systems Interface</td>
</tr>
<tr>
<td>SDRAM</td>
<td>Synchronous Dynamic RAM</td>
</tr>
<tr>
<td>SEL</td>
<td>System Event Log</td>
</tr>
<tr>
<td>SFP+</td>
<td>Small Form-factor Pluggable that supports data rates up to 10.0 Gbps</td>
</tr>
<tr>
<td>SMBus</td>
<td>System Management Bus</td>
</tr>
<tr>
<td>SMS</td>
<td>Server Management Software</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SOC</td>
<td>System on a Chip</td>
</tr>
<tr>
<td>SOL</td>
<td>Serial over LAN</td>
</tr>
<tr>
<td>SSD</td>
<td>Solid State Drive</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>THOL</td>
<td>Tested Hardware and Operating System List</td>
</tr>
<tr>
<td>TPM</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>TUV</td>
<td>Technischer Überwachungs-Verein (A safety testing laboratory with headquarters in Germany)</td>
</tr>
<tr>
<td>UART</td>
<td>Universal Asynchronous Receiver Transmitter</td>
</tr>
<tr>
<td>UEFI</td>
<td>Unified Extensible Firmware Interface</td>
</tr>
<tr>
<td>UL</td>
<td>Underwriter's Laboratory</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>UV</td>
<td>Under-Voltage</td>
</tr>
<tr>
<td>V</td>
<td>Volt</td>
</tr>
<tr>
<td>VA</td>
<td>Volt-Ampere (volts multiplied by amps)</td>
</tr>
<tr>
<td>Vac</td>
<td>Volts Alternating Current</td>
</tr>
<tr>
<td>Vdc</td>
<td>Volts Direct Current</td>
</tr>
<tr>
<td>VDE</td>
<td>Verband Deutscher Electrotechniker (German Institute of Electrical Engineers)</td>
</tr>
<tr>
<td>VGA</td>
<td>Video Graphics Array</td>
</tr>
<tr>
<td>vRAN</td>
<td>Virtualized Radio Access Network</td>
</tr>
<tr>
<td>VSB</td>
<td>Voltage Standby</td>
</tr>
<tr>
<td>W</td>
<td>Watt</td>
</tr>
<tr>
<td>WEEE</td>
<td>Waste Electrical and Electronic Equipment</td>
</tr>
</tbody>
</table>
Safety and regulatory information

Table of contents
- General safety warnings and cautions
  - Elevated operating ambient temperature
  - Mechanical loading
  - Circuit overloading
- AC power supply safety
  - Main AC power disconnect
  - Reliable earth-grounding
  - Overcurrent protection
- DC power supply safety
  - Main DC power disconnect
  - Overcurrent protection
  - Reliable earth-grounding
- Regulatory specifications
  - RoHS
  - Waste electrical and electronic equipment directive
  - Air Filter

NOTICE
Before working with this product or performing instructions described in the getting started section or in other sections, read the Safety and regulatory information section pertaining to the product. Assembly instructions in this documentation must be followed to ensure and maintain compliance with existing product certifications and approvals. Use only the described, regulated components specified in this documentation. Use of other products/components will void the CSA certification and other regulatory approvals of the product and will most likely result in non-compliance with product regulations in the region(s) in which the product is sold.

General safety warnings and cautions

WARNING
To prevent a fire or shock hazard, do not expose this product to rain or moisture. The chassis should not be exposed to dripping or splashing liquids and no objects filled with liquids should be placed on the chassis cover.

ESD sensitive device!
This equipment is sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this product in order to ensure product integrity at all times.

CAUTION
The equipment rack must provide sufficient airflow to the front of the server to maintain proper cooling.

Elevated operating ambient temperature

If this product is installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, be careful to install the product in an environment that is compatible with the maximum operating temperature specified by the manufacturer in the specifications.

Mechanical loading

Do not load the equipment unevenly when mounting this product in a rack as it may create hazardous conditions.
The power supply in this product contains no user-serviceable parts. There may be more than one supply in this product. Refer servicing only to qualified personnel.

Do not attempt to modify or use the supplied AC power cord if it is not the exact type required. A product with more than one power supply will have a separate AC power cord for each supply.

The power button on the system does not turn off system AC power. To remove AC power from the system, always unplug each AC power cord from the wall outlet or power supply.

The power cord(s) is considered the disconnect device to the main (AC) power. The socket outlet that the system plugs into must be installed near the equipment and must be easily accessible.

SAFETY STEPS: Before removing the chassis covers to access the inside of the system, follow these steps:

1. Turn off all peripheral devices connected to the system.
2. Turn off the system by pressing the power button.
3. Unplug all AC power cords from the system or from wall outlets.
4. Label and disconnect all cables connected to I/O connectors or ports on the back of the system.
5. Provide electrostatic discharge (ESD) protection by wearing an antistatic wrist strap attached to chassis ground of the system—any unpainted metal surface—when handling components.

After completing the six SAFETY STEPS above, you can remove the system covers. To do this:

1. Unlock and remove the padlock from the back of the system if a padlock has been installed.
2. Remove and save all screws from the covers.
3. Remove the covers.
4. Do not operate the system with the chassis covers removed.

For proper cooling and airflow, always reinstall the chassis covers before turning on the system. Operating the system without the covers in place can damage system parts. To install the covers:

1. Check first to make sure no loose tools or parts were left inside the system.
2. Check that cables, add-in boards, and other components are properly installed.
3. Attach the covers to the chassis with the screws removed earlier, and tighten them firmly.
4. Insert and lock the padlock to the system to prevent unauthorized access inside the system.
5. Connect all external cables and the AC power cord(s) to the system.

A microprocessor and heat sink may be hot if the system has been running. Also, there may be sharp pins and edges on some board and chassis parts. Contact should be made with care. Consider wearing protective gloves.

Danger of explosion if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the equipment manufacturer. Dispose of used batteries according to manufacturer’s instructions.

The system is designed to operate in a typical office environment. Choose a site that is:

- Clean and free of airborne particles (other than normal room dust).
- Well ventilated and away from sources of heat including direct sunlight.
- Away from sources of vibration or physical shock.
- Isolated from strong electromagnetic fields produced by electrical devices.
- In regions that are susceptible to electrical storms, we recommend plugging the system into a surge suppressor and disconnecting telecommunication lines to the modem during an electrical storm.
- Provided with a properly grounded wall outlet.
- Provided with sufficient space to access the power supply cord(s), because they serve as the product’s main power disconnect.
Circuit overloading

Do not overload the circuits when connecting this product to the supply circuit as this can adversely affect overcurrent protection and supply wiring. Check the supply equipment nameplate ratings for correct use.

AC power supply safety

Main AC power disconnect

The AC power cord(s) is considered the main disconnect for the server and must be readily accessible when installed. If the individual server power cord(s) will not be readily accessible for disconnect then you must install an AC power disconnect for the entire rack unit. This main disconnect must be readily accessible, and it must be labeled as controlling power to the entire rack, not just to the server(s).

Reliable earth-grounding

To avoid the potential for an electrical shock hazard, you must include a third wire safety ground conductor with the rack installation. If the server power cord is plugged into an AC outlet that is part of the rack, then you must provide proper grounding for the rack itself. If the server power cord is plugged in a wall AC outlet, the safety ground conductor in the power cord provides proper grounding only for the server. You must provide additional, proper grounding for the rack and other devices installed in it.

Overcurrent protection

The server is designed for an AC line voltage source with up to 20 amperes of overcurrent protection per cord feed. If the power system for the equipment rack is installed on a branch circuit with more than 20 amperes of protection, you must provide supplemental protection for the server. The overall current rating of a configured server is less than 6 amperes.

Do not attempt to modify or use an AC power cord set that is not the exact type required. You must use a power cord set that meets the following criteria:

- **Rating**
  - U.S. and Canada: Cords must be UL (Underwriters Laboratories, Inc.) Listed/CSA (Canadian Standards Association) Certified type SJT, 18 - 3 AWG (American Wire Gauge).
  - Outside of the U.S. and Canada: Cords must be flexible harmonized (<HAR>) or VDE (Verbena Deutscher Elektrotechniker, German Institute of Electrical Engineers) certified cords with 3x 0.75 mm conductors rated 250 VAC.

- **Connector, wall outlet end**
  - Cords must be terminated in a grounding - type male plug designed for use in your region. The connector must have certification marks showing certification by an agency acceptable in your region and for U.S. must be listed and rated for 125% of the overall current rating of the server.

- **Connector, server end**
  - The connectors that plug into the AC receptacle on the server must be an approved IEC (International Electrotechnical Commission) 320, sheet C13, type female connector.

- **Cord length and flexibility**
  - Cords must be less than 4.5 meters (14.8 feet) long.

DC power supply safety

Platforms equipped with a DC power supply must be installed in a restricted access area in accordance with articles 110 - 26 and 110 - 27 of the National Electric Code, ANSI/NFPA 70. When powered by DC supply, this equipment must be protected by a listed branch circuit protector with a maximum 25 A rating. The DC source must be electrically isolated from any hazardous AC source by double or reinforced insulation. The DC source must be capable of providing up to 1000 watts of continuous power per feed pair.

The DC power supply is protected from reverse polarity by internal diodes and will not operate at all if wired incorrectly.

This equipment is designed for the earth grounded conductor (return) in the DC supply circuit to be connected to the earth grounding conductor on the equipment (ground lug).

Main DC power disconnect

A properly rated DC power disconnect must be installed for the server system. This main disconnect must be readily accessible, and it must be labeled as controlling power to the server. The UL listed circuit breaker of a centralized DC power system may be used as a disconnect device when easily accessible.

Overcurrent protection

Overcurrent protection UL Listed circuit breakers must be provided as part of each host equipment rack and must be incorporated in the field wiring between the DC source and the server. The branch circuit protection shall be rated minimum 75 VDC, maximum 2.5 A per feed pair.
Reliable earth-grounding

This server is intended for installation with an isolated DC return (DC - I per NEBS GR - 1089, Issue 3). To avoid the potential for an electrical shock hazard, you must reliably connect an earth grounding conductor to the server. The earth grounding conductor must be a minimum 10AWG connected to the earth ground stud(s) on the rear of the server. The safety ground conductor should be connected to the chassis stud with a listed closed two - hole crimp terminal having 5/8 - inch pitch. The nuts on the chassis earth ground studs should be installed with a torque of 10 in - lbs. The safety ground conductor provides proper grounding only for the server. You must provide additional, proper grounding for the rack and other devices installed in it.

Earth ground lug location

Regulatory specifications

The platform meets the requirements of the following regulatory tests and standards:

Safety compliance

<table>
<thead>
<tr>
<th>Region</th>
<th>Compliance Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA/Canada</td>
<td>This product is marked cCSAus. This product complies with UL 60950-1 2nd Edition and CSA C22.2 No. 60950-1:07 2nd Edition.</td>
</tr>
<tr>
<td>Europe</td>
<td>This CE marked product complies with the Low Voltage Directive 2014/35/EU and EN 62368-1.</td>
</tr>
<tr>
<td>International</td>
<td>This product has a CB report and certificate to IEC 62368-1.</td>
</tr>
</tbody>
</table>

Electromagnetic compatibility
<table>
<thead>
<tr>
<th>Region</th>
<th>Compliance Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA/Canada</td>
<td>This product meets FCC Title 47 Part 15/ICES-003 Class A.</td>
</tr>
</tbody>
</table>
| Europe               | This CE marked product complies with the Electromagnetic Compatibility Directive 2014/30/EU based on the following standards: EN55032, Class A Limit, Radiated & Conducted Emissions  
|                      | EN55035 Immunity  
|                      | EN61000 - 4 - 2 ESD Immunity  
|                      | EN61000 - 4 - 3 Radiated Immunity  
|                      | EN61000 - 4 - 4 Electrical Fast Transient  
|                      | EN61000 - 4 - 5 Surge  
|                      | EN61000 - 4 - 6 Conducted RF  
|                      | EN61000 - 4 - 11 Voltage Fluctuations and Short Interrupts  
|                      | EN61000 - 3 - 2 Harmonic Currents  
|                      | EN61000 - 3 - 3 Voltage Flicker  
| Australia/New Zealand| This product complies with AS/NZS CISPR 32 Class A Limit. This product is marked RCM.                                                                                                                                                                                                                                                                                                                                                                                                     |
| Japan                | This product complies with VCCI Class A ITE (CISPR 32 Class A Limit).                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Korea                | This product is marked KCC.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| International        | This product complies with CISPR 32 Class A Limit and CISPR 35 Immunity.                                                                                                                                                                                                                                                                                                                                                                                                                  |

**RoHS**

The CE marking on this product indicates that it is in compliance with the RoHS directive.

**Waste electrical and electronic equipment directive**

This product contains electrical or electronic materials. If not disposed of properly, these materials may have potential adverse effects on the environment and human health. The presence of this logo on the product means it should not be disposed of as unsorted waste and must be collected separately. Dispose of this product according to the appropriate local rules, regulations and laws.

**Air Filter**

The CG2400 server can be configured with an optional air filter that is installed behind the front bezel. The air filter material is UAF Quadrafoam (25 PPI), has a thickness of 6.35mm, flammability rating of UL94-HF1, and meets the minimum dust arrestance of 65% (ASHRAE 52.1-1992) per documentation found at [http://www.uaf.com](http://www.uaf.com). The air filter can be purchased directly from Universal Air Filter (UAF) by calling (618) 271-7300 or emailing uaf@uaf.com and ordering part number K00737-001. When placing an order provide the attached drawing to verify receipt of the proper air filter. Recommended Air Filter Replacement Schedule: Every 6 months.
Warranty and support

Table of contents
- Limited warranty
- Disclaimer
- Customer support
- Customer service

Limited warranty
Please refer to the full terms and conditions of the Standard Warranty on Kontron's website at:

Disclaimer
Kontron would like to point out that the information contained in this manual may be subject to alteration, particularly as a result of the constant upgrading of Kontron products. This document does not entail any guarantee on the part of Kontron with respect to technical processes described in the manual or any product characteristics set out in the manual. Kontron assumes no responsibility or liability for the use of the described product(s), conveys no license or title under any patent, copyright or mask work rights to these products and makes no representations or warranties that these products are free from patent, copyright or mask work right infringement unless otherwise specified. Applications that are described in this manual are for illustration purposes only. Kontron makes no representation or warranty that such application will be suitable for the specified use without further testing or modification. Kontron expressly informs the user that this manual only contains a general description of processes and instructions which may not be applicable in every individual case. In cases of doubt, please contact Kontron.

This manual is protected by copyright. All rights are reserved by Kontron. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the express written permission of Kontron. Kontron points out that the information contained in this manual is constantly being updated in line with the technical alterations and improvements made by Kontron to the products and thus this manual only reflects the technical status of the products by Kontron at the time of publishing.

Brand and product names are trademarks or registered trademarks of their respective owners.

©2022 by Kontron

Customer support
Kontron's technical support team can be reached through the following means:
- By phone: 1-888-835-6676
- By email: support-na@kontron.com
- Via the website: www.kontron.com

Customer service
Kontron, a trusted technology innovator and global solutions provider, uses its embedded market strengths to deliver a service portfolio that helps companies break the barriers of traditional product lifecycles.

Through proven product expertise and collaborative, expert support, Kontron provides unparalleled peace of mind when it comes to building and maintaining successful products. To learn more about Kontron's service offering—including enhanced repair services, an extended warranty, and the Kontron training academy—visit www.kontron.com/support-and-services.