User Documentation – CG2400

POSSIBILITIES START HERE kontron

Table of Content

Product description

{This article briefly describes the physical product, features and main options.}
Table of contents

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-swappable and redundant power supply modules and fans
- High memory, flexible I/O and storage options
- Up to six hot-swappable 2.5-inch hard disk drives
- Up to two M.2 NVMe or SATA storage modules
- Up to seven PCIe expansion slots to integrate most I/O acceleration PCIe cards
- 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

Children

- Specifications
- Platform components
- Product architecture
- Description of system access methods
- Recommended technical expertise

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

Feature	Description
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-swappable 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 (SW) • Two front access SD card slots
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-swappable, redundant fans
Power	• Dual redundant 850W AC hot-swappable power supplies, 80Plus® Platinum • Dual redundant 850W DC hot-swappable 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 (RJ45 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 [Content under creation] 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. AXXRMM4LITE 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 40°C.

CG2400 k ey software features

Feature	Description
Platform management	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 • IPMI 2.0 feature support • Firmware update and maintenance • Fan monitoring • Hot-swap fan support • Integrated keyboard, video, and mouse (KVM) • KVM redirection • Power supply redundancy monitoring and support • Management support for Power Management Bus (PMBus) 1.2 compliant power supplies • Front panel management including system status LED and chassis ID LED (turned on/off using a front panel button or command) • Embedded Web server UI • Enhancements to embedded Web server: Human-readable SEL Additional system configurability Additional system monitoring capabilities • Acoustic management • Power Node Manager support • Thermal management support • BMC system management health monitoring • E-mail alerting • Integrated remote media redirection • Lightweight Directory Access Protocol (LDAP) • System globally unique identifier (GUID) storage and retrieval IPMI 2.0 features • IPMI watchdog timer • Messaging support, including command bridging and user/session support • Chassis device functionality, including power/reset control and BIOS boot flags support • System Event Log (SEL) device functionality • Access to system Sensor Data Records (SDRs) • Sensor device management and polling to monitor and report system health • Serial over LAN (SOL) • ACPI state synchronization to state changes provided by the BIOS • IPMI interfaces: Host interfaces including system management software (SMS) with receive message queue support and server management mode (SMM) Intelligent Platform Management Bus (IPMB) interface LAN interface that supports the IPMI over LAN protocol (RMCP, RMCP+)
Operating system	Refer to Validated operating systems
Thermal management	• Platform Environment Control Interface (PECI) for thermal management support • CPU thermal management

CG2400 p hysical dimensions

Chassis	Measurements (mm [in])	Notes
Depth	508 [20] max.	Body
Width	435.3 [17.14] max.	Body
Height	87.6 [3.45] max.	Body
Side clearance	25 [1]	Between rack mounting points
Front clearance	76 [2]	Recommended
Rear clearance	92 [3.6]	Recommended

CG2400 packaging physical dimensions

Depth (mm [in])	Width (mm [in])	Height (mm [in])
675 [26.57]	550 [21.65]	210 [8.27]

CG2400 s hipping weights

Component	Weight (kg)	Weight (lb)
System weight – full configuration (all PCIe adapters, AC or DC PS)	20.0	44.0
System weight – base configuration (as shipped from factory)	14.0	30.8
Packaging (box + foam + bag)	2.8	6.2
Power supply (AC or DC)	1.1	2.4

CG2400 environmental specifications

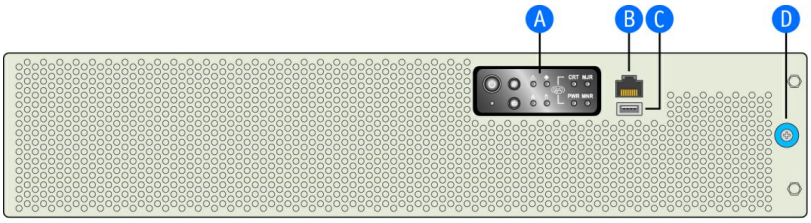
Environment	Specification
Temperature, operating	-5ºC to +55ºC (+23ºF to +131ºF)
Temperature, non-operating	-40ºC to +70ºC (-40ºF to +158ºF)
Humidity, operating	5% to 85%
Humidity, non-operating	95%, non-condensing
Altitude, operating	-60 m to 1,800 m (-197 ft to 5,906 ft) without temperature derating 3,900 m (12,795 ft) 40ºC
Vibration, operating	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
Vibration, non-operating	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
Shock, operating	This product meets operational shock standards Test profile based on ETSI EN 300 019-2-3 class 3.2 (IEC 60068-2-27)
A coustic	This product meets or exceeds GR-63 and ETSI EN 300 753 requirements
Drop/free fall	This product meets GR-63, clause 4.3.1
Electrostatic discharge	This product meets 8 kV contact, 15 kV air discharge using IEC 61000-4-2 test method
WEEE	This product complies with EU directive 2012/19/EU (WEEE)

Platform components

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

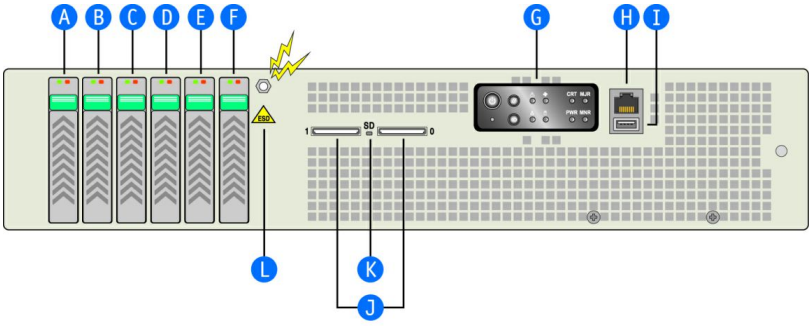
Table of contents

Platform front panel



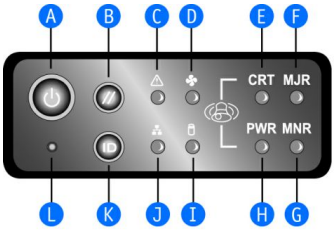
CG00004

Item	Description	Item	Description
A	Front panel control buttons, status indicator and telco alarm LEDs	C	USB 2.0 port
B	RJ45 serial port	D	Bezel captive screw



CG00005

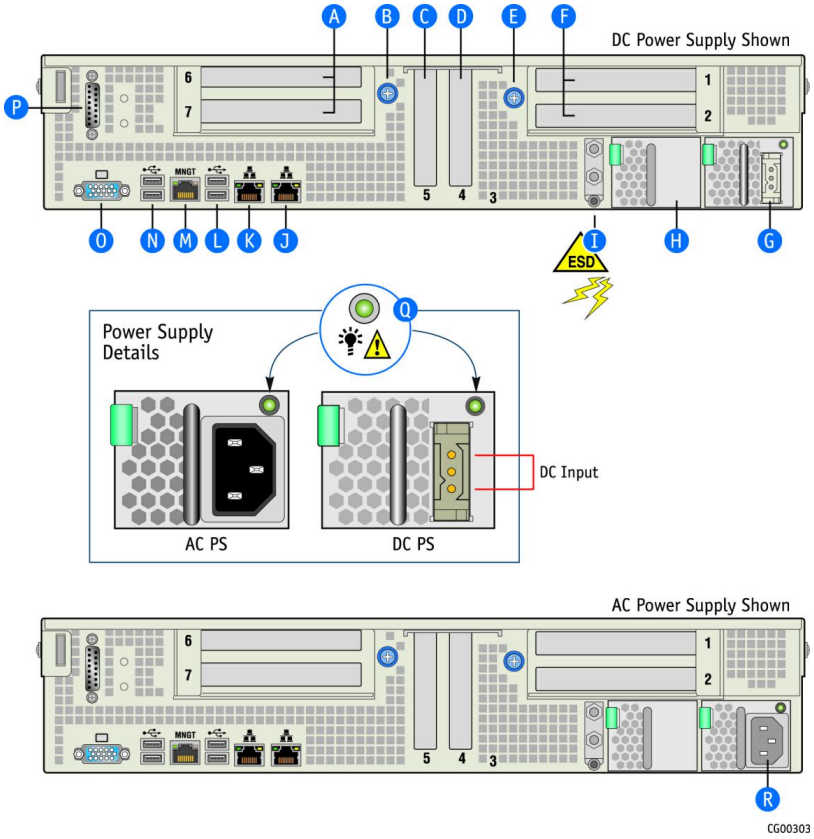
Item	Description	Item	Description
A	Drive slot 5	G	Front panel control buttons, status indicator and telco alarm LEDs
B	Drive slot 4	H	RJ45 serial port
C	Drive slot 3	I	USB 2.0 port
D	Drive slot 2	J	SD flash card slots
E	Drive slot 1	K	SD flash module LED
F	Drive slot 0	L	ESD ground strap attachment



CG00006

Item	Description	Item	Description
A	Power button	G	Minor alarm (amber)
B	System reset button	H	Power alarm (amber)
C	System status LED	I	Drive activity LED
D	Fan status LED	J	NIC activity LED
E	Critical alarm (amber)	K	Chassis ID button
F	Major alarm (amber)	L	NMI button

Platform rear panel

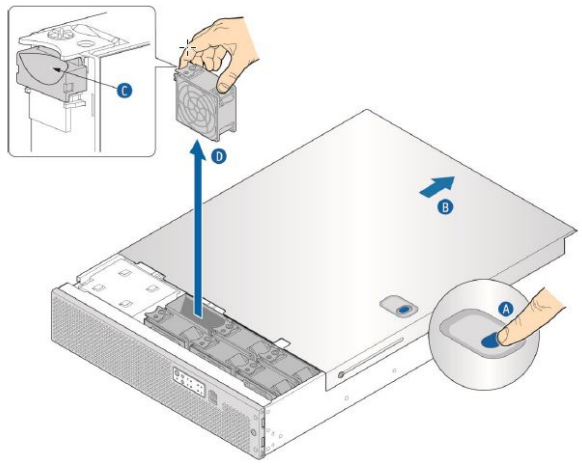


Item	Description	Item	Description
A	Right [1] 2-slot FL/FH PCIe assembly (slots 6 and 7)	J	GbE NIC2
B	Thumb screw to secure right PCIe assembly (A)	K	GbE NIC1
C	LP PCIe adapter (slot 5)	L	USB#3 and USB#4 (both USB 3.0 and USB#3 is the one on top)
D	LP PCIe adapter (slot 4)	M	Dedicated server management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

NOTES:
1. Right and left notation for PCIe assemblies are established while facing the front of the system.
2. In non-redundant configurations, power supply slot 2 must have a filler panel installed.

Platform fan module

The CG2400 platform is equipped with a module containing 6 hot - swappable fan s. N o service interruption is usually required t o 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 fan s and the CPU cables behind them are visible.
Step_3	Remove the fan (D) by grasping both sides of the f an assembly, using the plastic finger guard (C) on the left side and pulling the fan out of the metal enclosure that houses the fan s and the power cables.

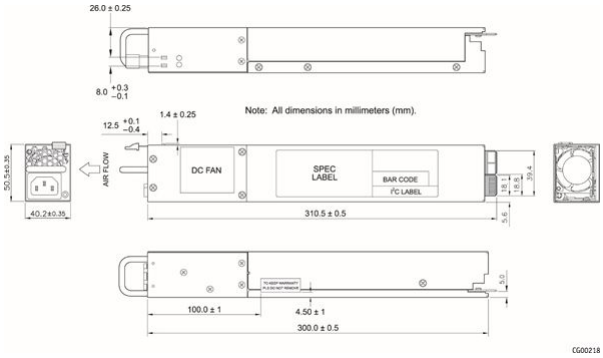
Power supply units

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

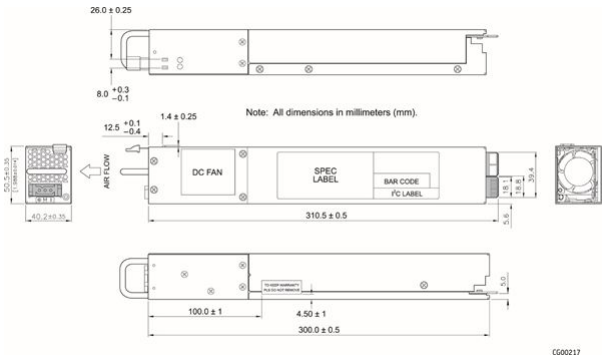
The AC power supply input connector is an IEC320 C14 standard AC inlet connector.

Line voltage	
Nominal 110 Vrms (low line)	
Minimum	90 V_{rms}
Rated	100-127 V_{rms}
Maximum	132 V_{rms}
Nominal 220 Vrms (high line)	
Minimum	180 V_{rms}
Rated	200-240 V_{rms}
Maximum	264 V_{rms}
Start-up voltage	85 Vrms ±5 Vrms
Power off voltage	75 Vrms ±5 Vrms
Line current	
Maximum	12 A at 100 Vrms / 6 A at 200 Vrms
Frequency	
Minimum	47 Hz
Rated	50/60 Hz
Maximum	63 Hz

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



Voltage and current requirements

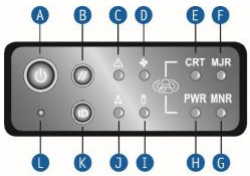
NOTE : The maximum current listed in the table below is the maximum current the system will draw from the power supply at -48 V input voltage.

DC input voltage	
Nominal	-48 VDC
Minimum [1]	-40 VDC
Rated	-48 VDC to -72 VDC
Maximum	-75 VDC
DC input current	
Maximum	30 A at -40 VDC , 15 A at -72 VDC

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

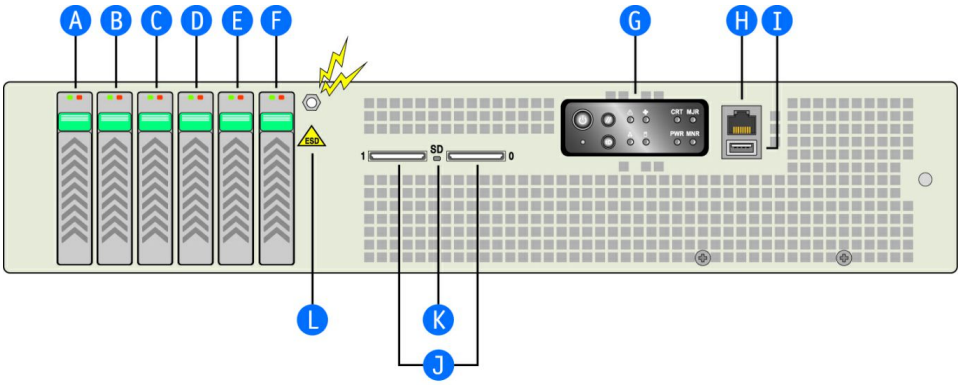
Platform button and LED behavior

Front panel



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

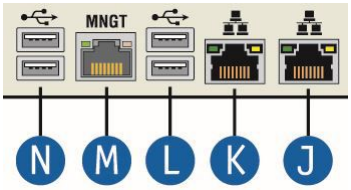
Item	Signal name	Description
A	Power button	Toggles the system power on/off, also functions as a sleep button if enabled by an ACPI-compliant operating system. A status LED is embedded in this button.
B	System reset button	Reboots and initializes the system.
K	Chassis ID button	Toggles the front panel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



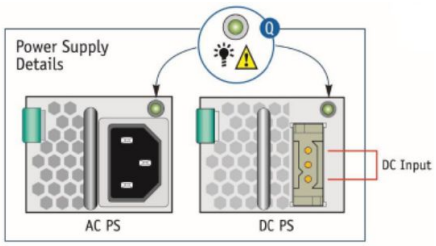
CG00005

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

Rear panel



Item	LED description	Color	Condition	Description
J,K	Link activity (left) NIC1 and NIC 2	Green	Off	No link established
			Solid	Link is established
			Blinking	Link activity
	Link speed (right) NIC 1 and NIC 2	Green	Solid	10 Gbps
		Yellow	Solid	1 Gbps
M	Link activity (left) Dedicated management NIC	Green	Off	No link established
			Solid	Link is established
			Blinking	Link activity
	Link speed (right) Dedicated management NIC	Green	Solid	1000 Mbps
		Yellow	Solid	100 Mbps



AC power supply condition	Dual-color LED
No AC power to all PSUs	Off
No AC power to this PSU only (for 1+1 configuration)	0.5 Hz blinking red
AC present / only 5 Vsb on (PSU off)	1 Hz blinking green
Power supply AC output on and OK	Green
Power supply failure	Red
Power supply warning	0.5 Hz blinking red/green*

* Blinking frequency: 1 Hz (0.5 s red / 0.5 s green)

DC power supply condition	Dual-color LED
No DC power to all PSUs	Off
No DC power to this PSU only (for 1+1 configuration)	0.5 Hz blinking red
DC present/only standby output on	1 Hz blinking green
Power supply DC output on and OK	Green
Power supply failure	Red
Power supply warning	0.5 Hz blinking red/green*

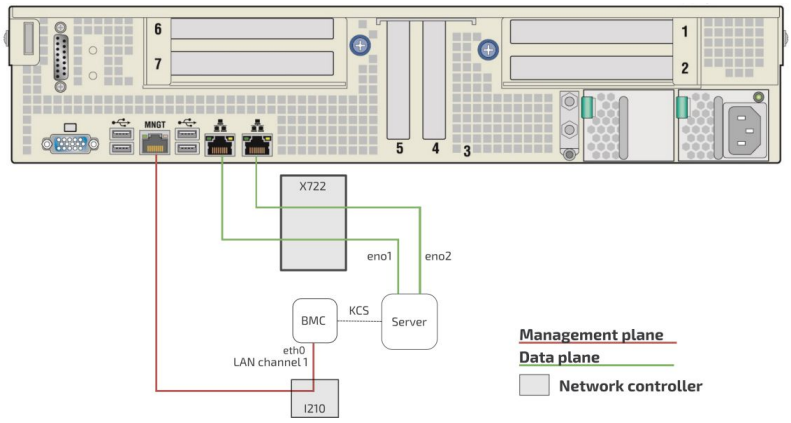
* Blinking frequency: 1 Hz (0.5 s red / 0.5 s green)

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



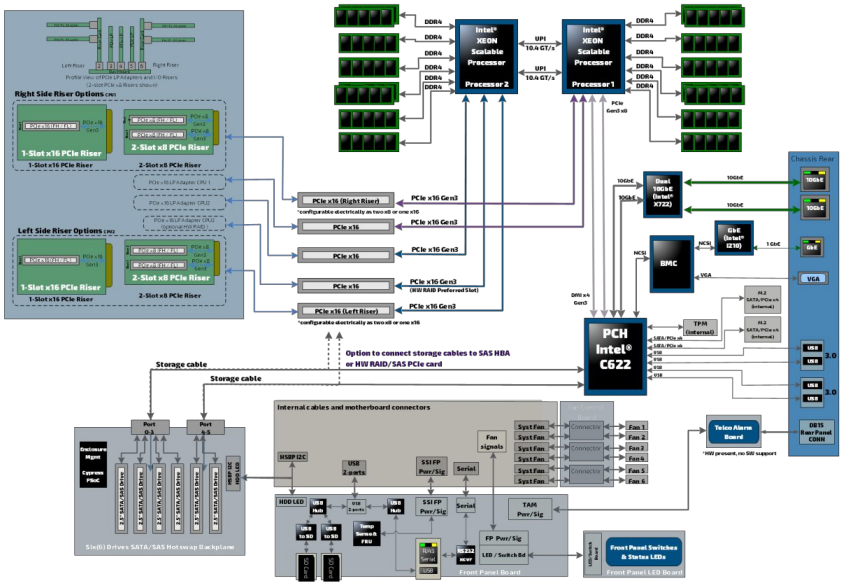
Network planes

The CG2400 platform provides 2 network planes.

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

Block diagram

This block diagram summarizes the connections within the platform.


Intel® XEON Scalable Processor 2
Intel® XEON Scalable Processor 1
UPI 10.4 GT/s
DDR4
Right Side Riser Options CPU2
1-Slot x16 PCIe Riser
2-Slot x8 PCIe Riser
Left Side Riser Options CPU1
PCIe x16 (Right Riser)
PCIe x16 (Left Riser)
PCIe x16 Gen3
*configurable electrically as two x8 or one x16
Chassis Rear
10GbE
GbE (Intel® I210)
BMC
NCSI
VGA
TPM (optional)
PCH Intel® C622
USB 3.0
Storage cable
Option to connect storage cables to SAS HBA or HW RAID/SAS PCIe card
Internal cables and motherboard connectors
Telco Alarm Board
*HW present, no SW support
DB15 Rear Panel CONN
Six(6) Drives SATA/SAS Hotswap Backplane
Front Panel Board
Front Panel LED Board
Front Panel Switches & Status LEDs

Description of system access methods

{This article lists interface access methods and their intended uses based on various use cases.}
Table of contents

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 .

Paths to the operating system	
Path description	**Main reasons for use**
KVM (Keyboard Video Mouse) *Fail-safe path to access the server if any elements (OS, BIOS, etc.) get misconfigured.* *Accessible from the management plane.*	• Initial OS installation • OS network interface configuration • OS video access • Remote access to the OS • Unable to establish an SSH session to the OS
Screen/monitor (VGA) ***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.*	• 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
SSH/RDP/Customer application protocols *Ideal path once OS installation and OS network interface configuration have been performed.* *Accessible from the data plane.*	• Operating the platform under normal operation • Remote access to the OS
Serial ov er LAN (SOL) *Accessible from the management plane.*	• OS network interface configuration • Unable to establish an SSH session to the OS • OS serial console access
Serial console (physical connection) *Fail-safe path to access all server components when elements (OS, BMC, BIOS) get misconfigured.* *Accessible from the physical port.*	• Initial OS network interface configuration • No configuration performed on BMCs • Troubleshooting

Paths to the BIOS

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

Paths to the BIOS	
Path description	**Main reasons for use**
KVM (Keyboard Video Mouse) *Fail-safe path to access the server if any elements (OS, BIOS, etc.) get misconfigured.* *Accessible from the management plane.*	• Initial BIOS configuration • BIOS video access
Screen/monitor (VGA) ***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.*	• Initial BIOS configuration • No configuration performed on BMCs • BIOS video access • Troubleshooting
Serial over LAN (SOL) *Accessible from the management plane.*	• Initial BIOS configuration • BIOS serial console access • OS network interfaces not configured, but BMC network access is available
Serial console (physical connection) *Fail-safe path to access all server components when elements (OS, BMC, BIOS) get misconfigured.* *Accessible from the physical port.*	• Initial BIOS configuration • No configuration performed on BMCs • Troubleshooting

Paths to the management interface (BMC)

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

Paths to the management interface (BMC)	
Path description	**Main reasons for use**
BMC Web UI ***This is the recommended path for first time out-of-the-box system configuration.*** *Accessible from the management plane.*	• Remote server control and monitoring • OS video access • Firmware upgrades
IPMI over LAN (IOL) *This is a good path for automated monitoring/control script once the platform has been configured for the first time.* *Accessible from the management plane .*	• Remote server control and monitoring • Firmware upgrades
IPMI/KCS *Accessible from the local operating system.*	• Local access to the BMC from the operating system for server monitoring • Initial BMC configuration
Redfish *This is the ideal path for automated monitoring/control script once the platform has been configured for the first time.* *Accessible from the management plane.*	• Remote server monitoring • Remote server control
SNMP *This is the ideal path for automated monitoring/control script once the platform has been configured for the first time.* *Accessible from the management plane.*	• Remote server monitoring • Remote server control

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

Children

- Getting started - Application installation and performance benchmarking
- [Content under creation] Getting started - Platform configuration and application mass deployment
- [Content under creation] Getting started - Platform and application mass management

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.]

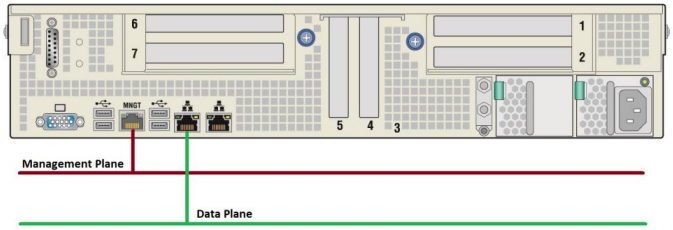
Table of contents

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.

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.



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
- 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

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

Item_1	#1 Phillips (cross-point) screwdrivers (or interchangeable tip screwdriver with #1 and #2 Phillips bits)
Item_2	#2 Phillips (cross-point) screwdrivers (or interchangeable tip screwdriver with #1 and #2 Phillips bits)
Item_3	One T30 Torx screwdriver
Item_4	One 5 -mm flat-head screwdriver
Item_5	Personal grounding device such as an anti-static wrist strap and a grounded conductive pad

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.

Item_1	K00740-001	Mounting bracket for Intel Battery Backup unit

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

Item_1	CG2200-RISER2SX8L	Dual-slot, PCIe x8, Gen3 riser for slot 2 (left side)

Power cables and tooling

Item_1	Black stranded 12 AWG wire to build the power cable based on the length required
Item_2	Red stranded 12 AWG wire to build the power cable based on the length required
Item_3	One Positronic DC power supply input mating connector (includes a strain relief assembly)
Item_4	Three Positronic gauge-16 crimp terminals
Item_5	Two strain relief screws
Item_6	One strain relief plate
Item_7	Two flat head Phillips screws
Item_8	One hand crimp tool, DMC AF8
Item_9	One manual extraction tool
Item_10	One 8 AWG ground cable based on the length required
item_11	One ground lug right angle, 8 AWG (Kontron P/N 1064-4226)
Item_12	10 mm wrench or equivalent tool
Item_13	One hand crimp tool, Panduit CT-1700

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.

Item_1	TMLPMOUNT51

Network cables and modules

Item_1	One RJ45 Ethernet management plane cable
Item_2	Two RJ45 Ethernet data plane cables
Item_3	One RJ45 serial connection cable

Network infrastructure

IP addresses:

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

Software required

Relevant section: Common software installation

Item_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.
Item_2	A terminal emulator such as **puTTY** is installed on a remote computer.
Item_3	A hardware detection tool such as **pciutils** is installed on the local server to view information about devices connected to the server PCI buses .

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

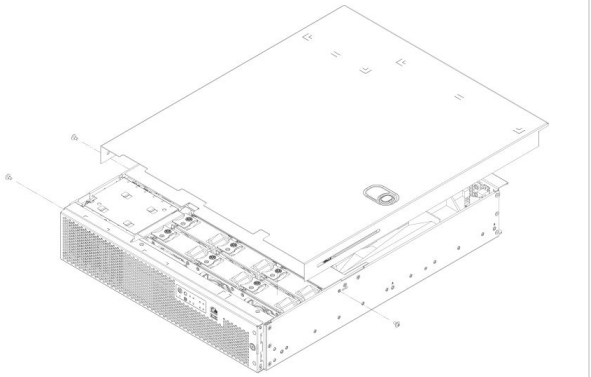
Installing components

	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.

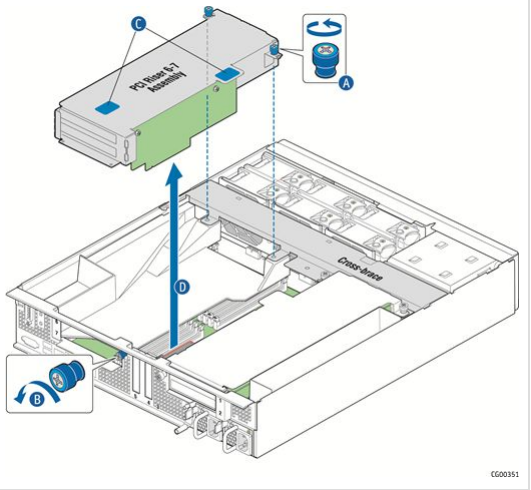
Opening the enclosure

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 bracke t on the rear panel of the chassis.
Step_4	Lift the cover straight up to remove it from the chassis.



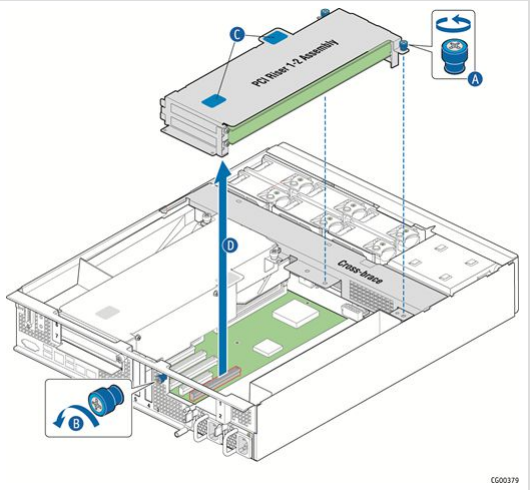
Removing the right riser card assembly

Step_1	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).
Step_2	Using the two blue touch points (C), lift the riser card assembly out of the chassis (D).

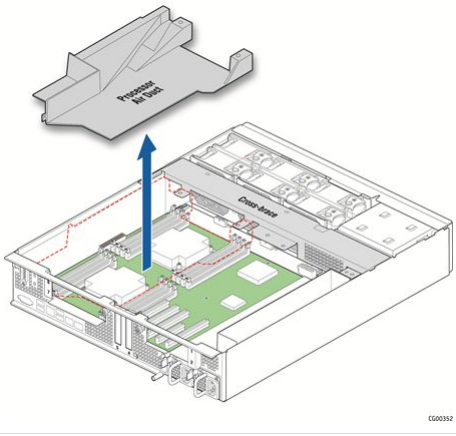


Removing the left riser card assembly

Step_1	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).
Step_2	Using the two blue touch points (C), lift the riser card assembly out of the chassis (D).



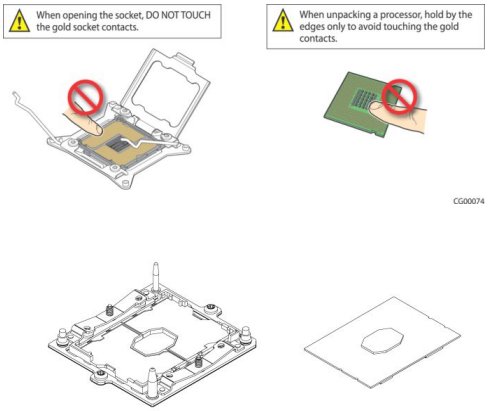
Removing the processor air duct

Step_1	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	

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.

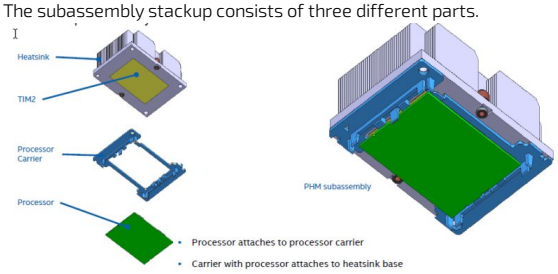
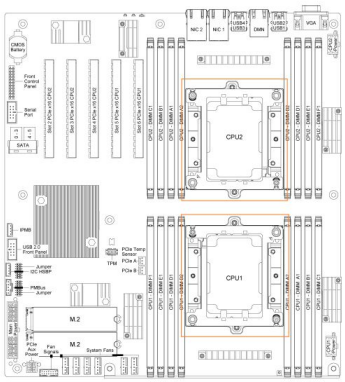


Image source: Intel Corporation

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

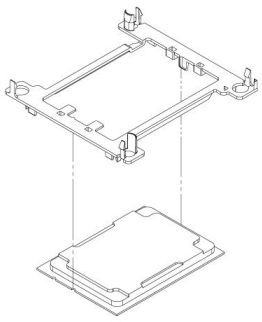
NOTICE	**The processor must be appropriate.** Severe damage to the platform board may occur if a processor that is inappropriate is installed. Refer to the Hardware compatibility list for a list of components.

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.

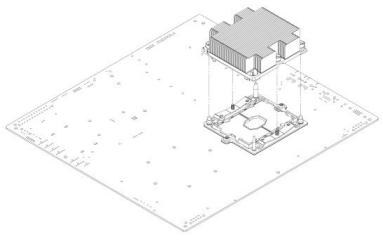
Preparing the processor for assembly with the PHM

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

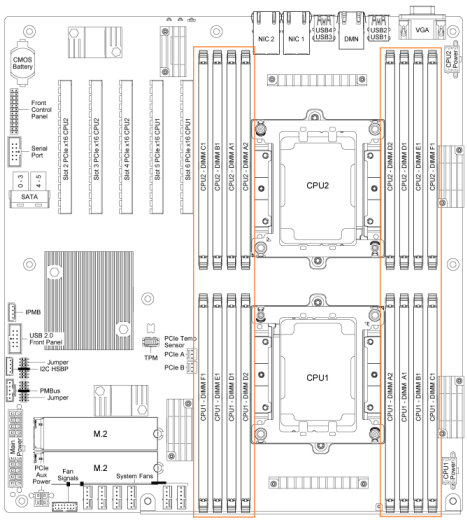
Step_1	Remove the heat sink from its packaging box. **NOTE:** • The processor with the "Front" heat sink must be installed onto the CPU1 socket (see Processor location) • The processor with the "Rear" heat sink must be installed onto the CPU2 socket (see Processor location)	
Step_2	Take the new PHM (processor 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 i n-Lb torque) .	

Installing memory DIMMs

Locating the DIMMs



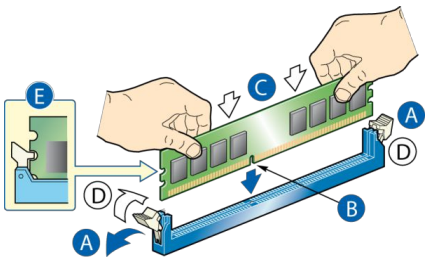
DIMM population guidelines for optimal performance

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, b oth 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, 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.

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 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

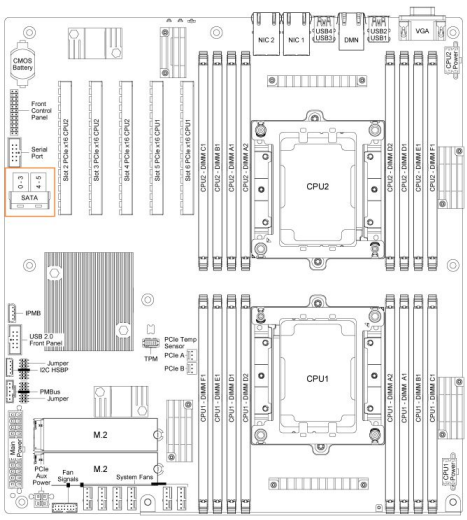
Installing memory DIMMs

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)	

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

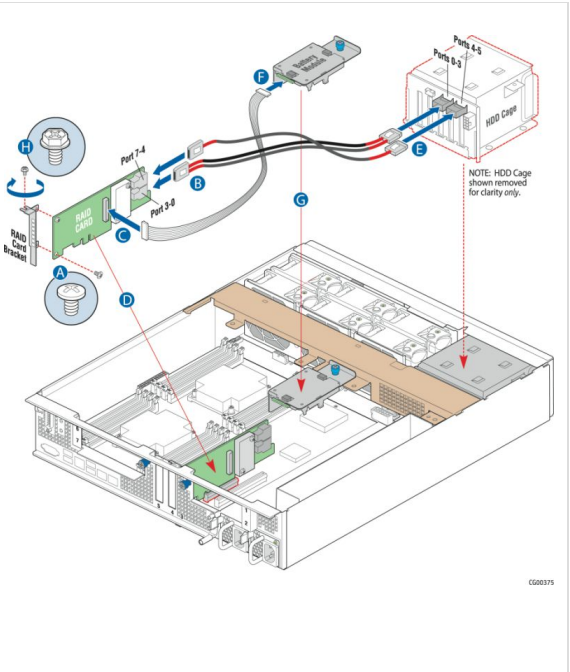


Disconnecting the SAS cables

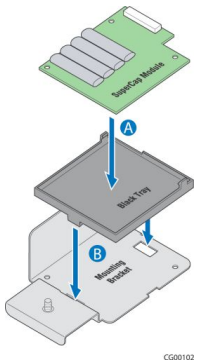
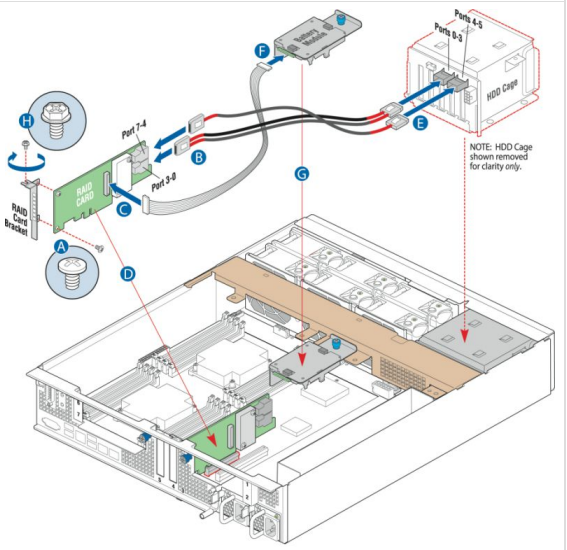
Step_1	Disconnect the two SAS cables (SFF-8643 ends) from the motherboard.

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 b attery 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, p roceed with required software configurations.	

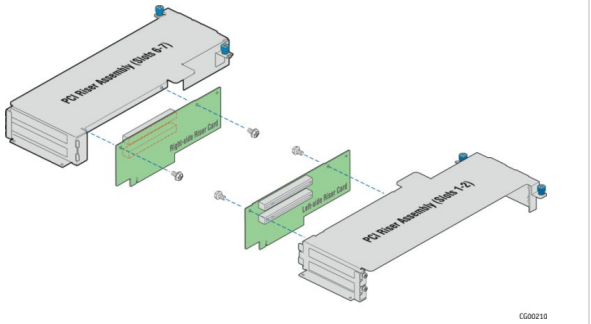
Installing a l ow-profile PCIe card in slot 4 or 5

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.

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.

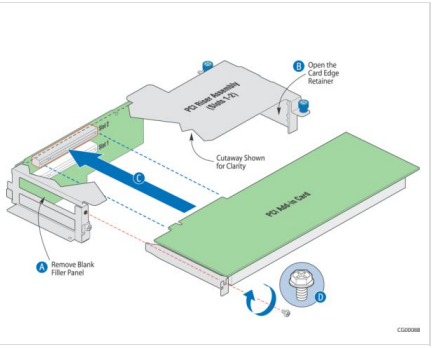
Installing a full height card mounted on the left riser

Assembling the PCIe riser card

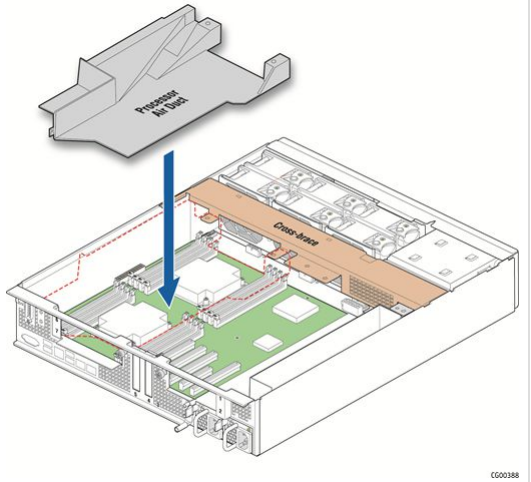
Step_1	Fasten the left riser card to its bracket with the two 6/32 screws (8 lbf·in torque) .	

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

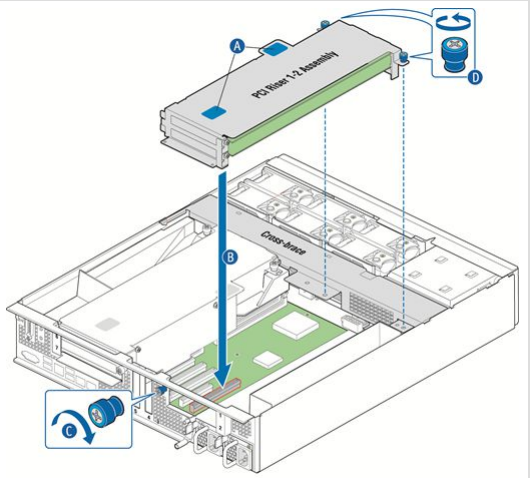
Installing the PCIe add-in card on the riser assembly

Step_1	Remove the blank filler panel from the riser card assembly (A) by u nfastening the screw of the selected slot (D).	
Step_2	F or 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).	

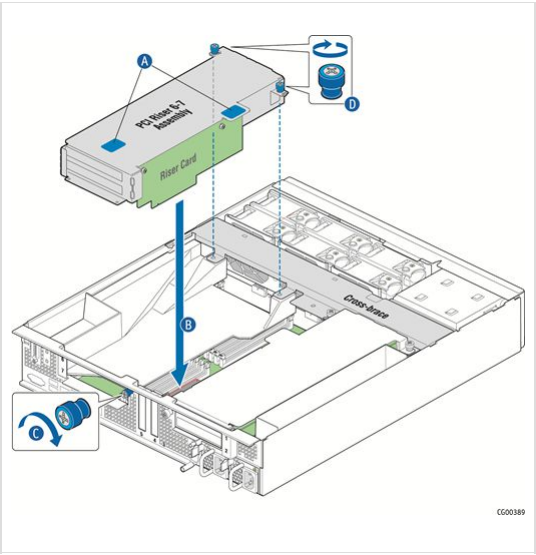
Reinstalling the processor air duct

Step_1	Place the processor air duct 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.	

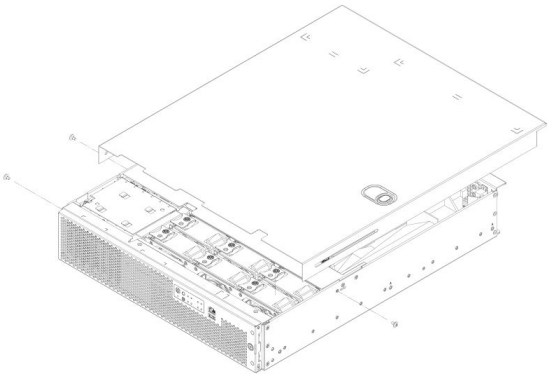
Reinstalling the left riser card assembly

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

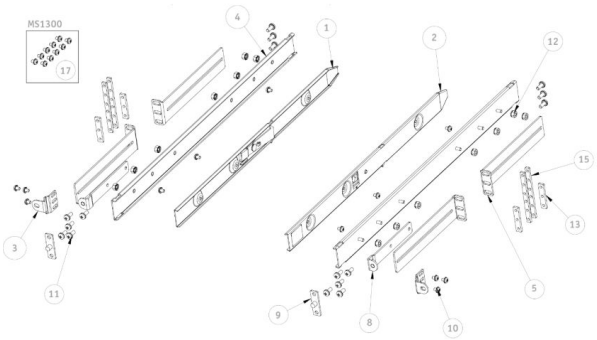
Step_1	Starting from the rear of the chassis, align the tab on the rear right edge of the cover with the lock bracket on the outside of the rear panel and place th e cover down over the chassis with the side edges outside the chassis walls.	
Step_2	Slide the cover forward until it clicks into place.	
Step_3	Install the shipping screw if tooled 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.	

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.
i	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 m ains 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.

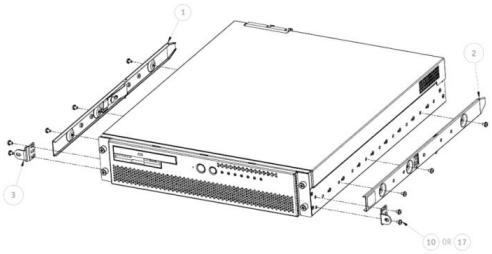
TMLPMOUNT51 rack mount kit



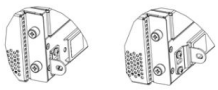
Item	Qty	Description
1	1	LEFT INNER RAIL
2	1	RIGHT INNER RAIL
3	2	MOUNTING EAR
4	2	OUTER RAIL
5	4	19″ EIA L-BRACKET
8	2	2-POST MOUNTING BRACKET
9	2	EIA WIDE ADAPTER
10	12	8-32 X 1/4 SEMS SCREW
11	16	10-32 X 1/2 SEMS SCREW
12	14	8-32 KEPS NUT
13	4	1U EIA BARNUT
15	4	2U EIA BARNUT
17	12	M4x0.7 SCREWS FOR MS1300

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.

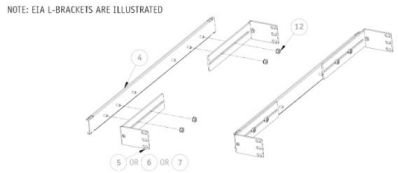
Installing inner rails and mounting ears

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.

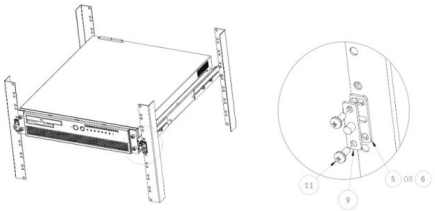


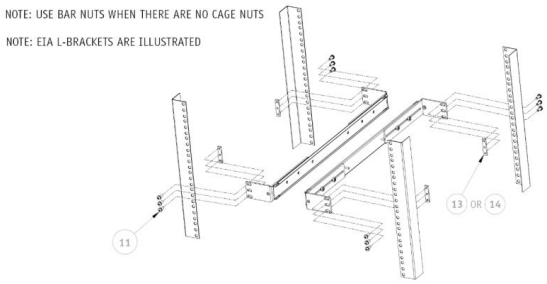
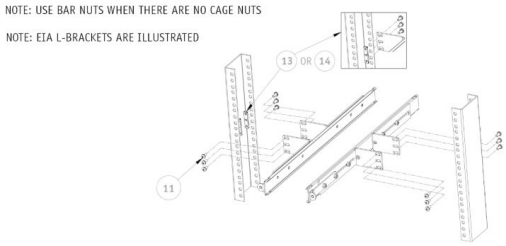
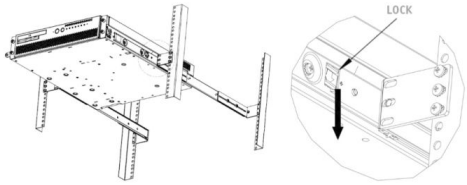
Building the outer rail assembly

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.	L-bracket assembly (4 posts under 24-inches deep) 
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.	

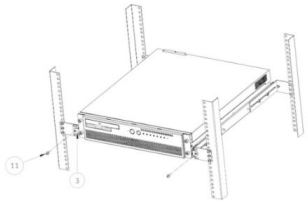
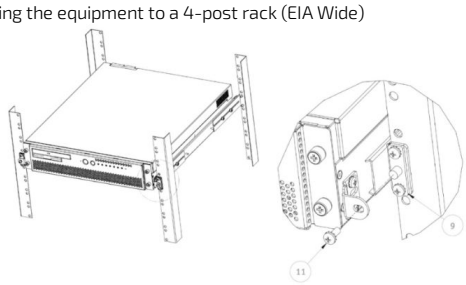
Attaching the outer rail assemblies to the rack posts

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.

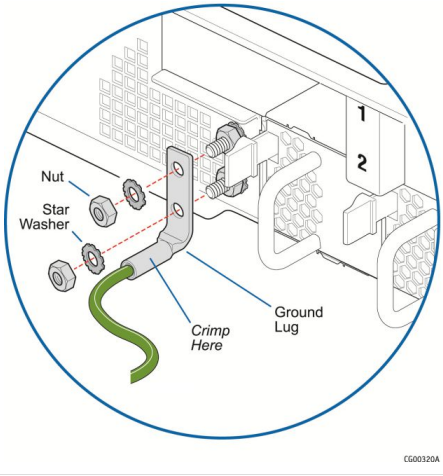


Step_1	Attach the outer rail assemblies (as built during the Building the outer rail assembly phase) to the rack using 8 or 12 screws (item 11). If the rack is designed to use cage nuts, no bar nuts will be required. If the rack has round holes, bar nuts (item 13 for EIA and item 14 for ETSI) should 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.	Outer rail assembly installation in a 4-post rack  Outer rail assembly installation in a 2-post rack 
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.	Lock release 

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) 

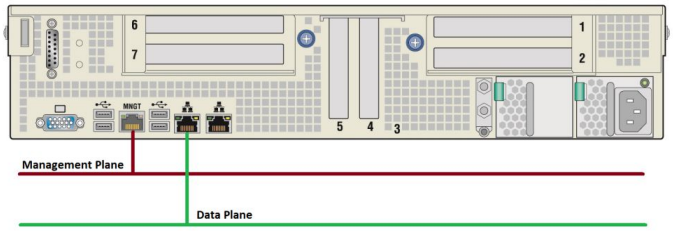
DC earth-grounding

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

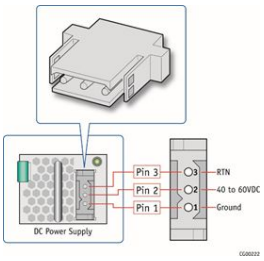
NOTE: For an AC PSU or for further information, refer to the Cabling section.

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.

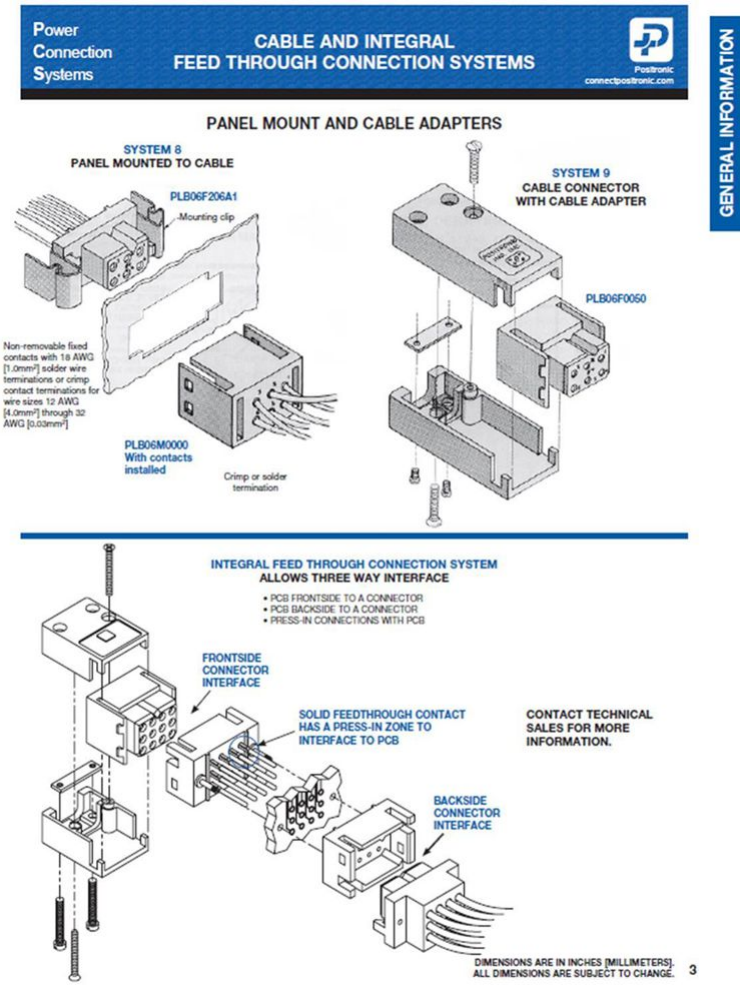
DC power supply input connector

- 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 Proccess



Building the power cables

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

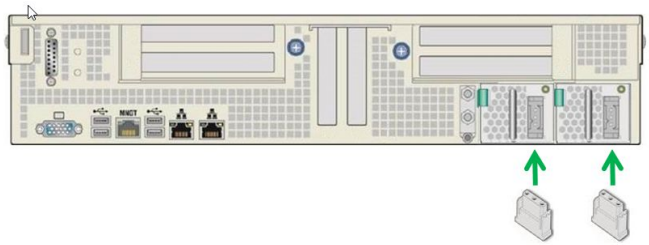
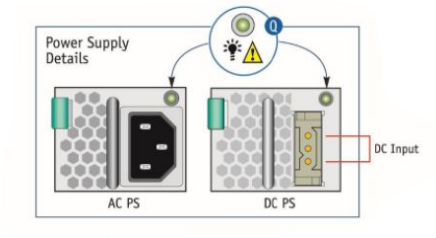
To build the power cables (ends that will be plugged in the CG2400), the material, tools and wires specified below are required.
NOTE: The other ends of the cables will need to be built according to national wiring codes and conform to local regulations in addition to your data center power installation requirements.

Description	Quantity	Manufacturer P/N	Link
Black stranded 12 AWG wire to build the power cable based on the length required	Length required		
Red stranded 12 AWG wire to build the power cable based on the length required	Length required		
Positronic DC power supply input mating connector (includes a strain relief assembly)	1 (provided with DC power supply module)	PLA03F7050/AA	• Positronic catalog
Positronic gauge-16 crimp terminal	3 (provided with DC power supply module)	FC112N2/AA-14	• Positronic catalog
Strain relief screw	2 (provided with DC power supply module)	Part of kit 1059-8642 Refer to [Content under creation] Platform, modules and accessories	
Strain relief plate	1 (provided with DC power supply module)	Part of kit 1059-8642 Refer to [Content under creation] Platform, modules and accessories	
Flat head Phillips screw	2 (provided with DC power supply module)	Part of kit 1059-8642 Refer to [Content under creation] Platform, modules and accessories	
DMC AF8 hand crimp tool	1	AF8	• DMC hand crimp tool catalog • DMC AF8 data sheet
Manual extraction tool	1	9081-0-0-0	• Molex extraction tool catalog • Application tooling specification sheet

Refer to the Cabling section for a link to a video showing how to crimp pins and assemble them into the connector.

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 .	

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

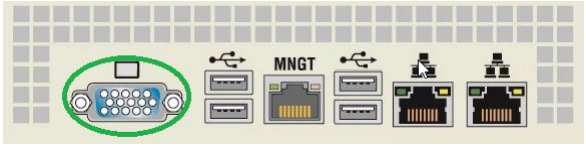
The platform management IP address can be discovered in the BIOS u sing the VGA display port (physical connection).

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

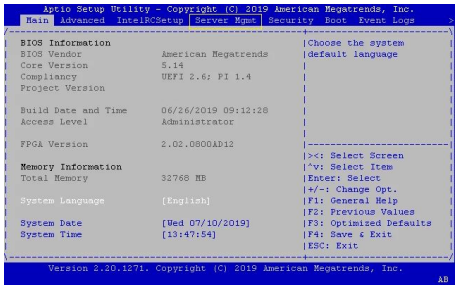
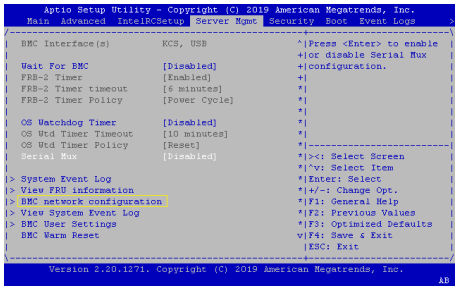
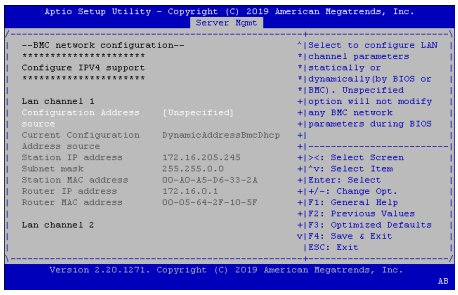
Prerequisites

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

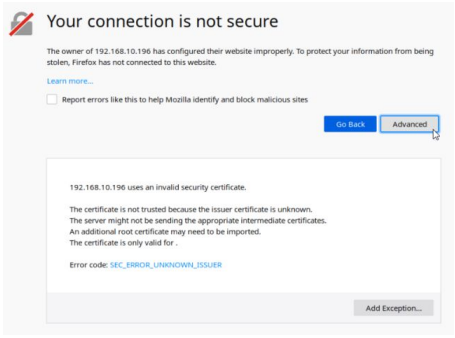
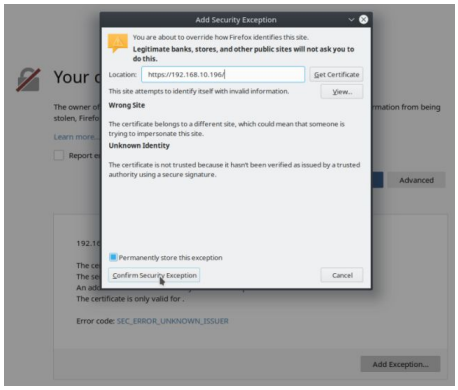
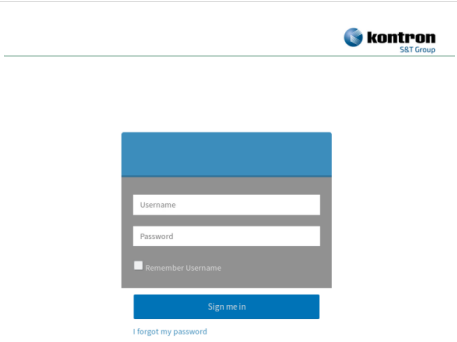
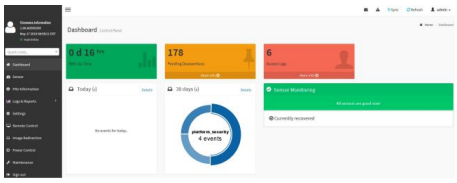
1	The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).
2	The remote computer has access to the management network subnet.

Browser considerations

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.

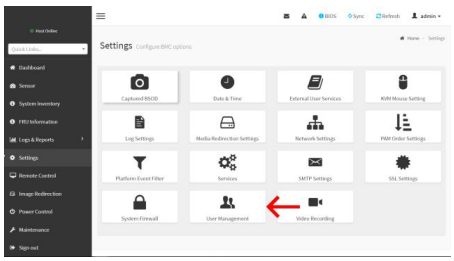
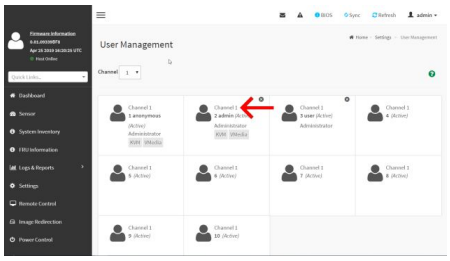
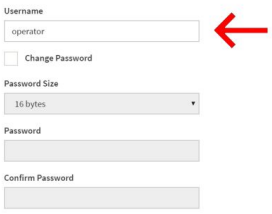
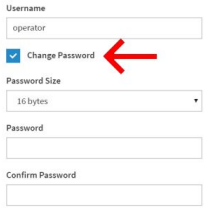
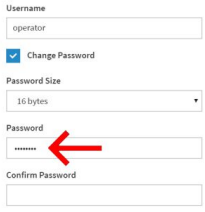
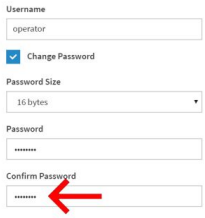
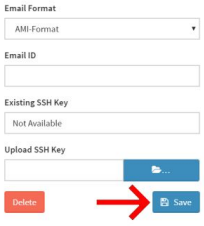
NOTE: The procedure may vary depending on the browser used. Examples provided use Firefox.

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 s tart 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.	

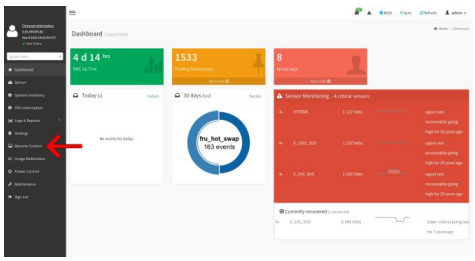
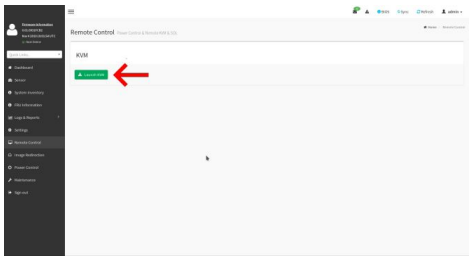
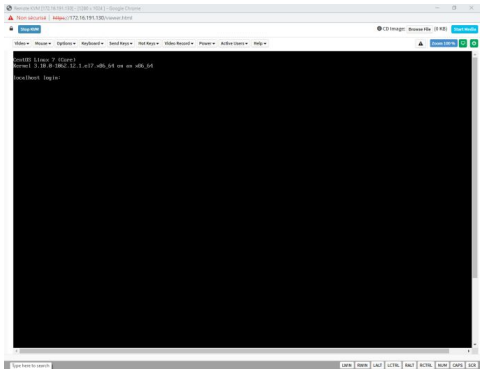
Changing the user name and password

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.**

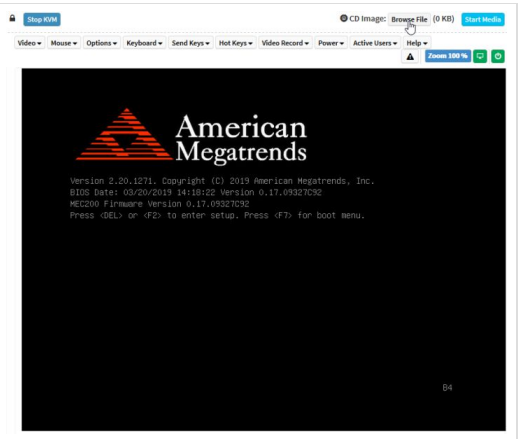
Step_1	Click on **Settings** in the left side menu and click on **User Management** .	
Step_2	Select the user to manage. **NOTE:** The first and second users are reserved fields, therefore, their usernames can't be modified.	
Step_3	Change field **Username** if required.	
Step_4	Check the **Change Password** 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

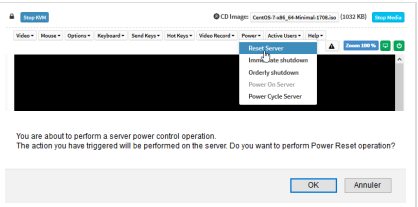
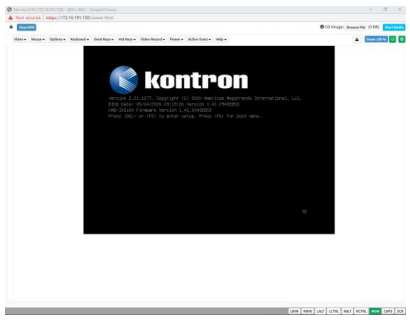
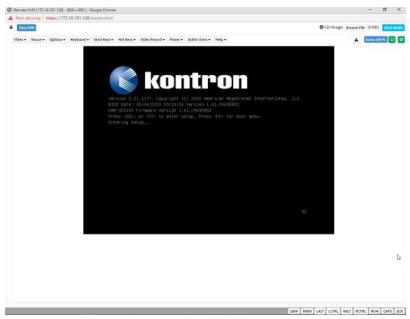
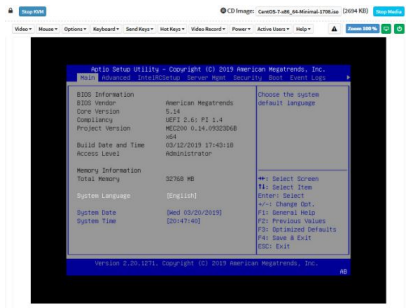
The Web UI allows remote control of the server through a KVM (Keyboard, Video, Mouse) interface.

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.	

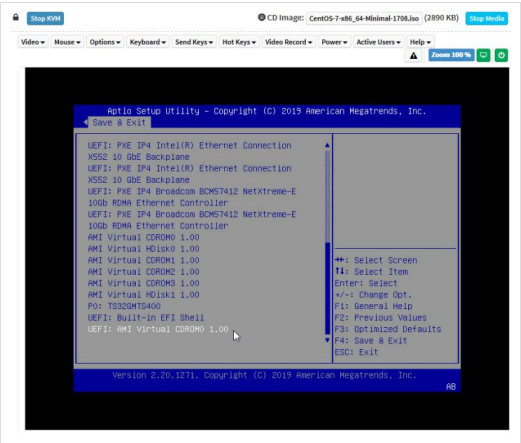
Mounting the operating system image via virtual media

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_1	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.

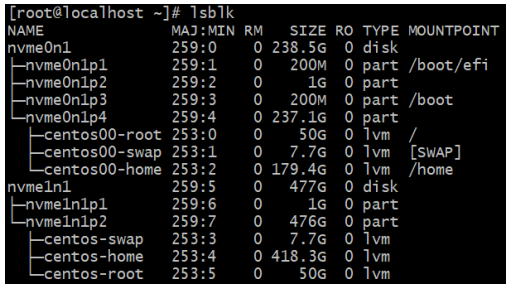
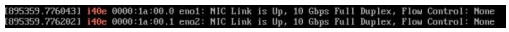
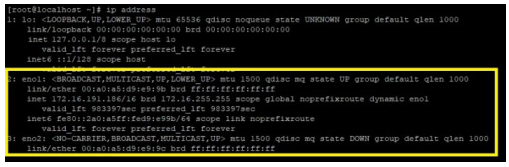
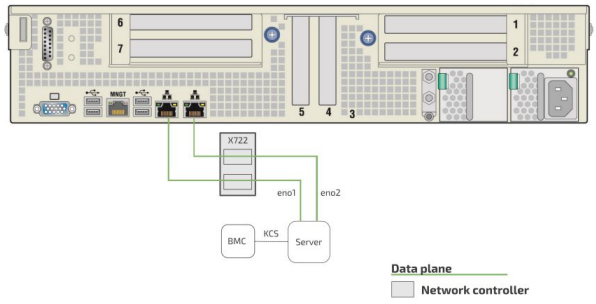
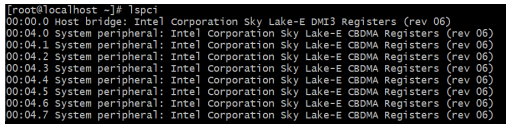
Completing operating system installation

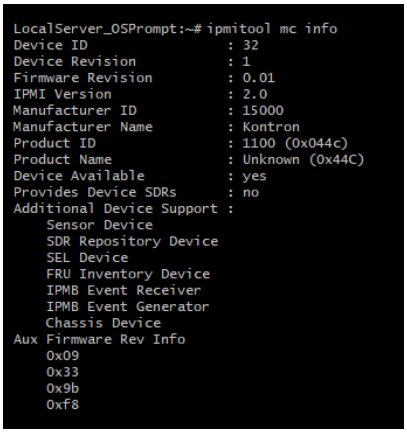
Step_1	Complete the installation by following the on-screen prompts of the specific OS installed.

> (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

i	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**	

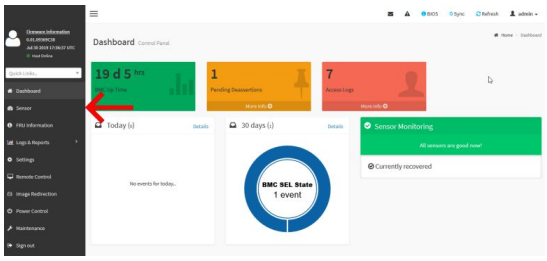
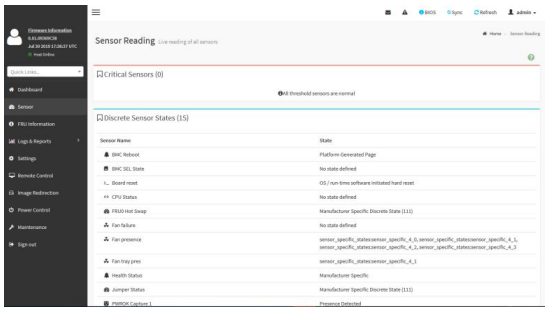
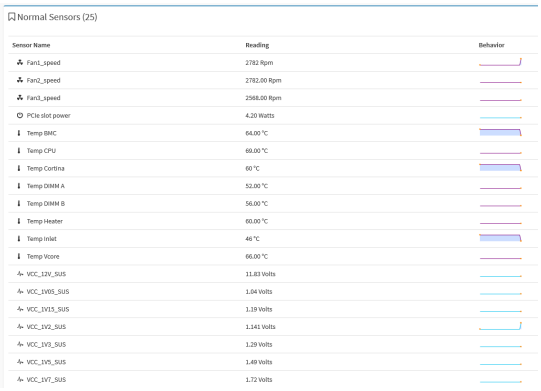
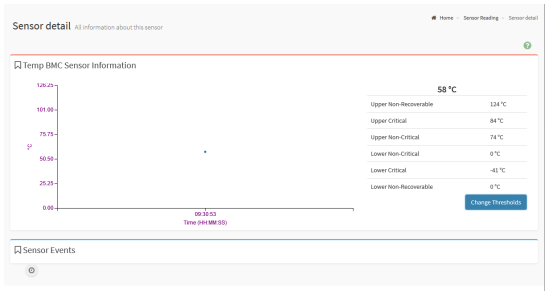
Benchmarking an application

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

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.	

For a list of all the sensors, refer to Sensor list .
For more monitoring methods refer to Monitoring sensors .

Planning

{This section describes key elements that need to be planned prior to platform configuration, network infrastructure integration and deployment.}

Children

- [Content under creation] Key concepts
- Environmental considerations
- Power consumption and power budget
- Network architecture
- MAC addresses
- PCI mapping
- Platform, modules and accessories
- Material, information and software required
- Hardware compatibility list
- [Content under creation] Deployment infrastructure
- Validated operating systems
- Security

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

General power information

- The nominal output power of the CG2400 is 850 W. This means t he 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.

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

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.

Component type	Component	Watts per component	Quantity	Sub-total (Watts)
Fan	System fan	25	6	150
CPU	Xeon® Scalable Gold 5218T	105	2	210
DIMM	16 GB DIMM	6	8	48
Motherboard	Chipset, LAN, others	30	1	30
Storage	2.5-in HDD (SAS)	8	4	32
	M.2 (SATA or NVMe)	2	1	2
PCIe	RAID	15	1	15
			Total	**487**

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.

Model	50 °C	55 °C	60 °C	65 °C
AC PSU (input = 90 VAC) nominal output power	850 W	705 W	650 W	600 W
DC PSU (input = -40 VDC) nominal output power	850 W	850 W	790 W	725 W

Network architecture

{This article provides network layout information regarding defaults, the customer's architecture and redundancies.}
Table of contents

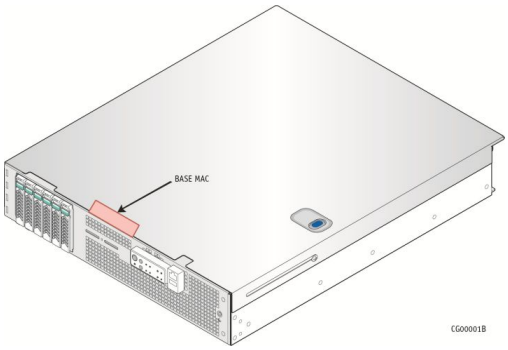
MAC addresses

{This article provides information on the product MAC addresses and on means of discovering them.}

Table of contents

CG2400 MAC addresses

Interface description	MAC address	Notes
BMC MNGT port	MAC_BASE	Dedicated MGNT port (RMM4/RMM4Lite equivalent)
CPU X722 port 1	MAC_BASE + 3	Server data plane (payload 10G/1G)
CPU X722 port 2	MAC_BASE + 4	Server data plane (payload 10G/1G)



Discovering the platform MAC addresses

The platform MAC addresses can be discovered:

- Using IPMI
- Using the [Content under creation] BIOS

Discovering a MAC address using IPMI

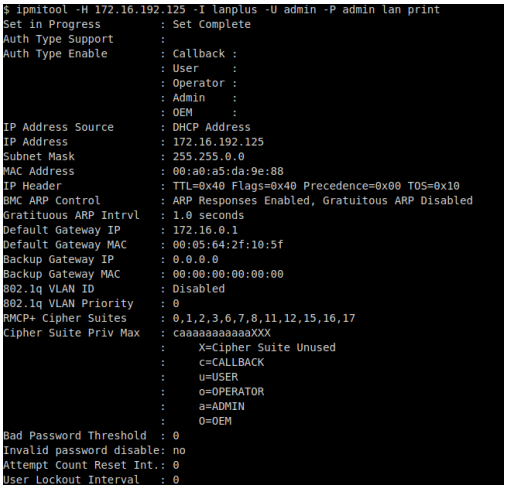
Prerequisite

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.

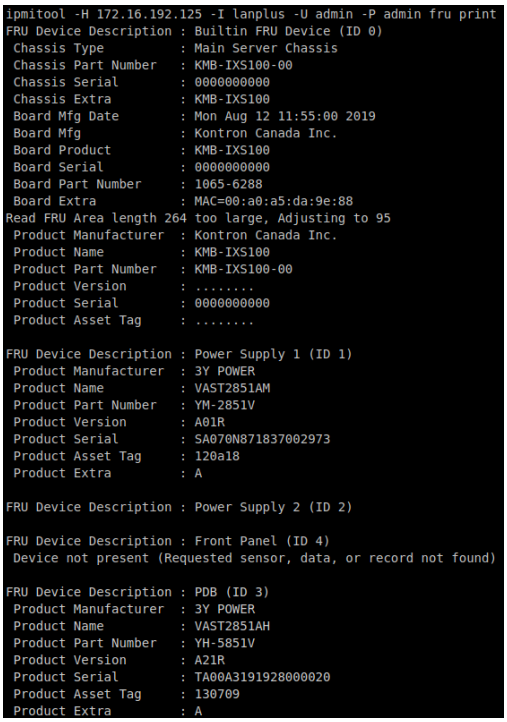
A MAC address can be discovered using IPMI with the following commands:

- lan print
- fru print

Procedure via ipmitool lan print

Step_1	From a remote computer that has access to the management network subnet, e nter the desired command. RemoteComputer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] lan print**	

Procedure via ipmitool fru print

Step_1	From a remote computer that has access to the management network subnet, e nter the desired command. RemoteComputer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] fru print** 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:

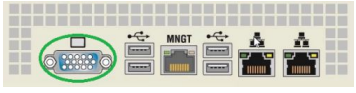
- Using the [Content under creation] VGA display port (physical connection)
- Using a [Content under creation] serial console (physical connection)

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

Prerequisites

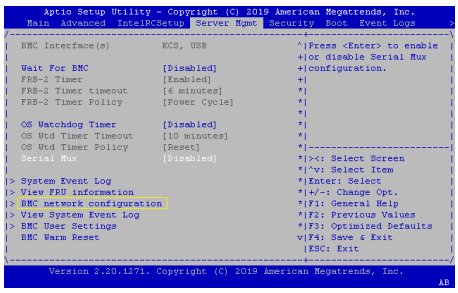
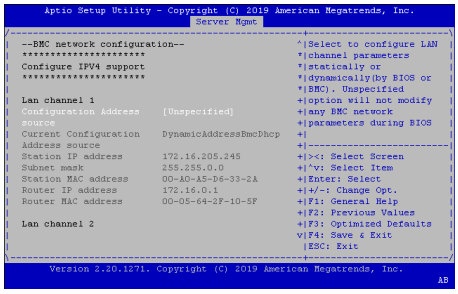
1	A physical connection to the VGA display port of the device is required.
2	A mouse and/or keyboard is connected.

Port location



Accessing the BMC network configuration menu

Step_1	From the UEFI/BIOS menu, navigate to tab **Server Mgmt** .	

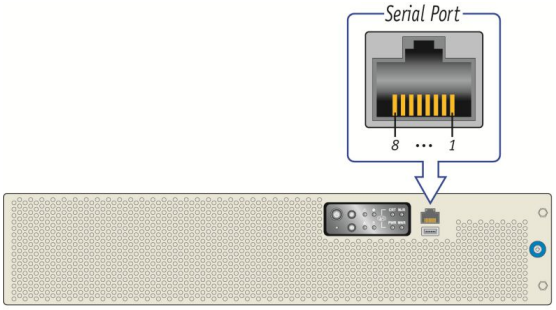
		
Step_2	Select **BMC network configuration** .	
Step_3	The **BMC network configuration** menu is displayed. **NOTE:** When the platform is powered up after being shut off, the UEFI/BIOS may load before the BMC has received its IP address. In this case, the UEFI/BIOS menu information will need to be refreshed by restarting the server and re-entering the UEFI/BIOS .	

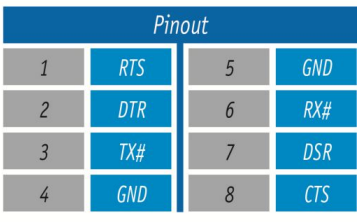
Accessing the BIOS using a serial console (physical connection)

Prerequisites

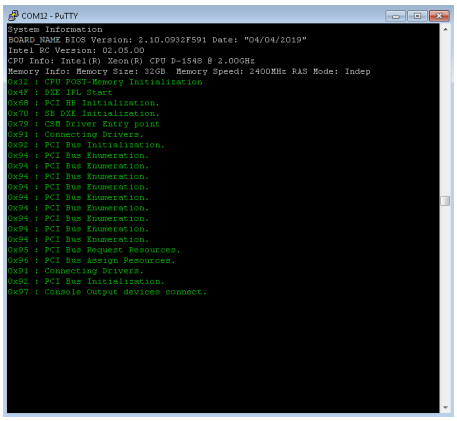
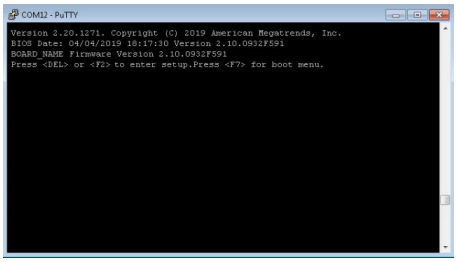
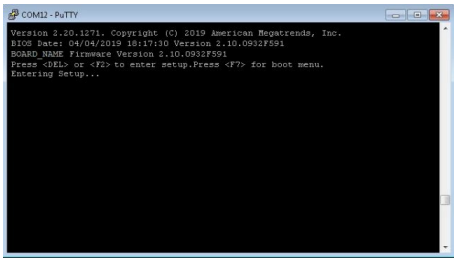
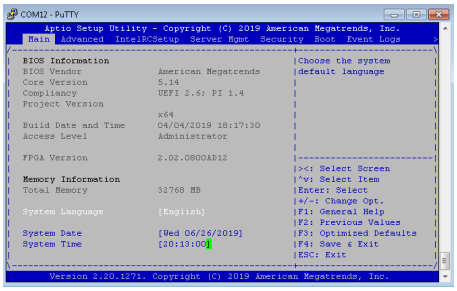
1	A physical connection to the device is required. **NOTE:** The serial console port is compatible with Cisco 72-3383-01 cable.
2	A serial console tool is installed on the remote computer. • Speed (Baud): 115200 • Data bits: 8 • Stop bits: 1 • Parity: None • Flow Control: None • Recommended emulation mode: VT100+ **NOTE:** PuTTY is recommended.

Port location

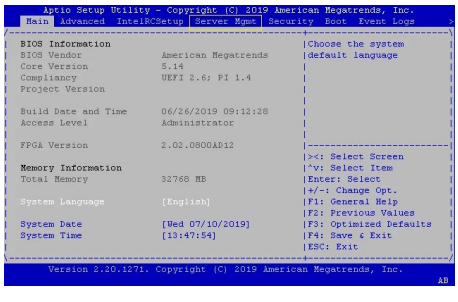
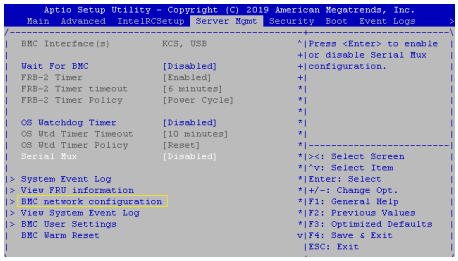


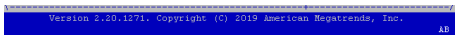
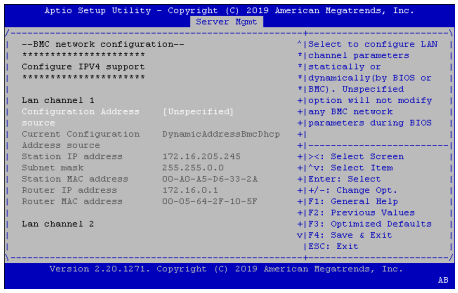


Access procedure

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_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 .	

PCI mapping

{This article provides the PCI mapping of the product.}

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.

CPU presence	CPU	PCI bus number range	PCIe slot numbers (on the KMB-IXS100 motherboard itself)	Slot numbers shown on CG2400 chassis (backside)
1 CPU only	CPU1	0-255 (0xFF)	Slot 5 - x16 (does not support PCIe risers) Slot 6 - x16 (supports PCIe risers)	Slot 5 (motherboard) → Slot 5 (chassis) Slot 6 (motherboard) → Slots 6 and 7 (chassis)
2 CPUs present	CPU1	0-127 (0x7F)	Slot 5 - x16 (does not support PCIe risers) Slot 6 - x16 (supports PCIe risers)	Slot 5 (motherboard) → Slot 5 (chassis) Slot 6 (motherboard) → Slots 6 and 7 (chassis)
	CPU2	128-255 (0x80-0xFF)	Slot 2 (supports PCIe risers) Slot 3 - x16 (does not support PCIe risers) Slot 4 - x16 (does not support PCIe risers)	Slot 2 (motherboard) → Slots 1 and 2 (chassis) Slot 3 (motherboard) → Slot 3 (chassis) Slot 4 (motherboard) → Slot 4 (chassis)

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).

Bus: Device. Function	Vendor ID	Device ID	Component	Description
00:00.0	8086	2020	Host bridge	Intel Corporation Sky Lake-E DMI3 Registers (rev 04)
00:04.0	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)
00:04.1	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)
00:04.2	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)
00:04.3	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)
00:04.4	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)
00:04.5	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)
00:04.6	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)
00:04.7	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)
00:05.0	8086	2024	System peripheral	Intel Corporation Sky Lake-E MM/Vt-d Configuration Registers (rev 04)
00:05.2	8086	2025	System peripheral	Intel Corporation Sky Lake-E RAS (rev 04)
00:05.4	8086	2026	PIC	Intel Corporation Sky Lake-E IOAPIC (rev 04) (prog-if 20 [IO(X)-APIC])
00:08.0	8086	2014	System peripheral	Intel Corporation Sky Lake-E Ubox Registers (rev 04)
00:08.1	8086	2015	Performance counters	Intel Corporation Sky Lake-E Ubox Registers (rev 04)
00:08.2	8086	2016	System peripheral	Intel Corporation Sky Lake-E Ubox Registers (rev 04)
00:11.0	8086	a1ec	Unassigned class	Intel Corporation C620 Series Chipset Family MROM 0 (rev 09)
00:11.5	8086	a1d2	SATA controller	Intel Corporation C620 Series Chipset Family SSATA Controller [AHCI mode] (rev 09) (prog-if 01 [AHCI 1.0])
00:14.0	8086	a1af	USB controller	Intel Corporation C620 Series Chipset Family USB 3.0 xHCI Controller (rev 09) (prog-if 30 [XHCI])
00:14.2	8086	a1b1	Signal processing controller	Intel Corporation C620 Series Chipset Family Thermal Subsystem (rev 09)
00:16.0	8086	a1ba	Communication controller	Intel Corporation C620 Series Chipset Family MEI Controller #1 (rev 09)
00:16.1	8086	a1bb	Communication controller	Intel Corporation C620 Series Chipset Family MEI Controller #2 (rev 09)
00:16.4	8086	a1be	Communication controller	Intel Corporation C620 Series Chipset Family MEI Controller #3 (rev 09)
00:17.0	8086	a182	SATA controller	Intel Corporation C620 Series Chipset Family SATA Controller [AHCI mode] (rev 09) (prog-if 01 [AHCI 1.0])
00:1c.0	8086	a190	PCI bridge	Intel Corporation C620 Series Chipset Family PCI Express Root Port #1 (rev f9) (prog-if 00 [Normal decode])
00:1c.2	8086	a192	PCI bridge	Intel Corporation C620 Series Chipset Family PCI Express Root Port #3 (rev f9) (prog-if 00 [Normal decode])
00:1c.4 NVMe	8086	a194	PCI bridge	Intel Corporation Lewisburg PCI Express Root Port #5 (rev f9) **NOTE:** Will be present if a card is present in the J47 - Rear M.2 connector.
00:1d.0 NVMe	8086	a198	PCI bridge	Intel Corporation Lewisburg PCI Express Root Port #9 (rev f9) **NOTE:** Will be present if a card is present in the J49 - Front M.2 connector.
00:1f.0	8086	a1c2	ISA bridge	Intel Corporation C622 Series Chipset LPC/eSPI Controller (rev 09)
00:1f.2	8086	a1a1	Memory controller	Intel Corporation C620 Series Chipset Family Power Management Controller (rev 09)
00:1f.4	8086	a1a3	SMBus	Intel Corporation C620 Series Chipset Family SMBus (rev 09)
00:1f.5	8086	a1a4	Serial bus controller	Intel Corporation C620 Series Chipset Family SPI Controller (rev 09)

02:00.0	1a03	1150	PCI bridge	ASPEED Technology, Inc. AST1150 PCI-to-PCI Bridge (rev 04) (prog-if 00 [Normal decode])
03:00.0	1a03	2000	VGA compatible controller	ASPEED Technology, Inc. ASPEED Graphics Family (rev 41) (prog-if 00 [VGA controller])
04:00.0 NVMe	XXXX	XXXX	1st or only card in M.2 expansion slot	*-- depending on M.2 expansion card –*
05:00.0 NVMe	XXXX	XXXX	2nd card in M.2 expansion slot (installed in J47-Rear)	*-- depending on M.2 expansion card –*
Bus 17 is mapped as bus 16 if only 1 CPU is installed				
17:02.0	8086	2032	PCI bridge	Intel Corporation Sky Lake-E PCI Express Root Port C (rev 04) (prog-if 00 [Normal decode])
17:05.0	8086	2034	System peripheral	Intel Corporation Sky Lake-E VT-d (rev 04)
17:05.2	8086	2035	System peripheral	Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04)
17:05.4	8086	2036	PIC	Intel Corporation Sky Lake-E IOxAPIC Configuration Registers (rev 04) (prog-if 20 [IO(X)-APIC])
17:08.0	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:08.1	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:08.2	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:08.3	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:08.4	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:08.5	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:08.6	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:08.7	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:09.0	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:09.1	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:09.2	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:09.3	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:09.4	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:09.5	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:09.6	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:09.7	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0a.0	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0a.1	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0a.2	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0a.3	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0a.4	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0a.5	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0a.6	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0a.7	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0b.0	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0b.1	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0b.2	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0b.3	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0e.0	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0e.1	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0e.2	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0e.3	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0e.4	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0e.5	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0e.6	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0e.7	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0f.0	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0f.1	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0f.2	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0f.3	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0f.4	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0f.5	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)

17:0f.6	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0f.7	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:10.0	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:10.1	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:10.2	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:10.3	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:10.4	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:10.5	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:10.6	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:10.7	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:11.0	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:11.1	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:11.2	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:11.3	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:1d.0	8086	2054	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:1d.1	8086	2055	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:1d.2	8086	2056	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:1d.3	8086	2057	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:1e.0	8086	2080	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
17:1e.1	8086	2081	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
17:1e.2	8086	2082	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
17:1e.3	8086	2083	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
17:1e.4	8086	2084	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
17:1e.5	8086	2085	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
17:1e.6	8086	2086	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
Bus 18, 19 and 1a are mapped as bus 17, 18 and 19 if only 1 CPU is installed				
18:00.0	8086	37c0	PCI bridge	Intel Corporation Device (rev 09) (prog-if 00 [Normal decode])
19:03.0	8086	37c5	PCI bridge	Intel Corporation Device (rev 09) (prog-if 00 [Normal decode])
1a:00.0	8086	37d2	Ethernet controller	Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09)
1a:00.1	8086	37d2	Ethernet controller	Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09)
Bus 3a-3e are mapped as bus 64-68 if only 1 CPU is installed				
3a:00.0 Slot 6	8086	2030	PCI bridge	Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04)
3a:01.0 Slot 6	8086	2031	PCI bridge	Intel Corporation Sky Lake-E PCI Express Root Port B (rev 04) **NOTE:** Will be present if there is a riser of type (x4x4x4x4) and a card in the 2nd slot. **NOTE:** Will be present if there is a riser of type (x4x4x8) and a card in the 2nd slot.
3a:02.0 Slot 6	8086	2032	PCI bridge	Intel Corporation Sky Lake-E PCI Express Root Port C (rev 04) **NOTE:** Will be present if there is a riser of type (x4x4x4x4) and a card in the 3rd slot. **NOTE:** Will be present if there is a riser of type (x8x4x4) and a card in the 2nd slot. **NOTE:** Will be present if there is a riser of type (x4x4x8) and a card in the 3rd slot. **NOTE:** Will be present if there is a riser of type (x8x8) and a card in the 2nd slot.
3a:03.0 Slot 6	8086	2033	PCI bridge	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.
3a:05.0	8086	2034	System peripheral	Intel Corporation Sky Lake-E VT-d (rev 04)
3a:05.2	8086	2035	System peripheral	Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04)
3a:05.4	8086	2036	PIC	Intel Corporation Sky Lake-E IOxAPIC Configuration Registers (rev 04) (prog-if 20 [IO(X)-APIC])
3a:08.0	8086	2066	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
3a:09.0	8086	2066	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
3a:0a.0	8086	2040	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
3a:0a.1	8086	2041	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
3a:0a.2	8086	2042	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
3a:0a.3	8086	2043	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
3a:0a.4	8086	2044	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
3a:0a.5	8086	2045	System peripheral	Intel Corporation Sky Lake-E LM Channel 1 (rev 04)
3a:0a.6	8086	2046	System peripheral	Intel Corporation Sky Lake-E LMS Channel 1 (rev 04)

3a:0a.7	8086	2047	System peripheral	Intel Corporation Sky Lake-E LMDP Channel 1 (rev 04)
3a:0b.0	8086	2048	System peripheral	Intel Corporation Sky Lake-E DECS Channel 2 (rev 04)
3a:0b.1	8086	2049	System peripheral	Intel Corporation Sky Lake-E LM Channel 2 (rev 04)
3a:0b.2	8086	204a	System peripheral	Intel Corporation Sky Lake-E LMS Channel 2 (rev 04)
3a:0b.3	8086	204b	System peripheral	Intel Corporation Sky Lake-E LMDP Channel 2 (rev 04)
3a:0c.0	8086	2040	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
3a:0c.1	8086	2041	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
3a:0c.2	8086	2042	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
3a:0c.3	8086	2043	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
3a:0c.4	8086	2044	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
3a:0c.5	8086	2045	System peripheral	Intel Corporation Sky Lake-E LM Channel 1 (rev 04)
3a:0c.6	8086	2046	System peripheral	Intel Corporation Sky Lake-E LMS Channel 1 (rev 04)
3a:0c.7	8086	2047	System peripheral	Intel Corporation Sky Lake-E LMDP Channel 1 (rev 04)
3a:0d.0	8086	2048	System peripheral	Intel Corporation Sky Lake-E DECS Channel 2 (rev 04)
3a:0d.1	8086	2049	System peripheral	Intel Corporation Sky Lake-E LM Channel 2 (rev 04)
3a:0d.2	8086	204a	System peripheral	Intel Corporation Sky Lake-E LMS Channel 2 (rev 04)
3a:0d.3	8086	204b	System peripheral	Intel Corporation Sky Lake-E LMDP Channel 2 (rev 04)
3b:00.x Slot 6	XXXX	XXXX	Card in expansion "`Slot 6 `" or "`Slot 6 + Riser 1 st Slot `"	-- *depending on PCIe expansion card* –
3c:00.x Slot 6	XXXX	XXXX	Card in expansion "`Slot 6 + Riser 2 nd Slot `"	-- *depending on PCIe expansion card* –
3d:00.x Slot 6	XXXX	XXXX	Card in expansion "`Slot 6 + Riser 3 rd Slot `"	-- *depending on PCIe expansion card* –
3e:00.x Slot 6	XXXX	XXXX	Card in expansion "`Slot 6 + Riser 4 th Slot `"	-- *depending on PCIe expansion card* –
Bus 5d-61 are mapped as bus b2-b6 if only 1 CPU is installed				
5d:00.0 Slot 5	8086	2030	PCI bridge	Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04)
5d:01.0 Slot 5	8086	2031	PCI bridge	Intel Corporation Sky Lake-E PCI Express Root Port B (rev 04) **NOTE:** Will be present if there is a riser of type (x4x4x4x4) and a card in the 2nd slot. **NOTE:** Will be present if there is a riser of type (x4x4x8) and a card in the 2nd slot.
5d:02.0 Slot 5	8086	2032	PCI bridge	Intel Corporation Sky Lake-E PCI Express Root Port C (rev 04) **NOTE:** Will be present if there is a riser of type (x4x4x4x4) and a card in the 3rd slot. **NOTE:** Will be present if there is a riser of type (x8x4x4) and a card in the 2nd slot. **NOTE:** Will be present if there is a riser of type (x4x4x8) and a card in the 3rd slot. **NOTE:** Will be present if there is a riser of type (x8x8) and a card in the 2nd slot.
5d:03.0 Slot 5	8086	2033	PCI bridge	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.
5d:05.0	8086	2034	System peripheral	Intel Corporation Sky Lake-E VT-d (rev 04)
5d:05.2	8086	2035	System peripheral	Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04)
5d:05.4	8086	2036	PIC	Intel Corporation Sky Lake-E IOxAPIC Configuration Registers (rev 04) (prog-if 20 [IO(X)-APIC])
5d:0e.0	8086	2058	Performance counters	Intel Corporation Sky Lake-E KTI 0 (rev 04)
5d:0e.1	8086	2059	System peripheral	Intel Corporation Sky Lake-E UPI Registers (rev 04)
5d:0f.0	8086	2058	Performance counters	Intel Corporation Sky Lake-E KTI 0 (rev 04)
5d:0f.1	8086	2059	System peripheral	Intel Corporation Sky Lake-E UPI Registers (rev 04)
5d:10.0	8086	2058	Performance counters	Intel Corporation Sky Lake-E KTI 0 (rev 04)
5d:10.1	8086	2059	System peripheral	Intel Corporation Sky Lake-E UPI Registers (rev 04)
5d:12.0	8086	204c	Performance counters	Intel Corporation Sky Lake-E M3KTI Registers (rev 04)
5d:12.1	8086	204d	Performance counters	Intel Corporation Sky Lake-E M3KTI Registers (rev 04)
5d:12.2	8086	204e	System peripheral	Intel Corporation Sky Lake-E M3KTI Registers (rev 04)
5d:12.4	8086	204c	Performance counters	Intel Corporation Sky Lake-E M3KTI Registers (rev 04)
5d:12.5	8086	204d	Performance counters	Intel Corporation Sky Lake-E M3KTI Registers (rev 04)
5d:15.0	8086	2018	System peripheral	Intel Corporation Sky Lake-E M2PCI Registers (rev 04)
5d:16.0	8086	2018	System peripheral	Intel Corporation Sky Lake-E M2PCI Registers (rev 04)

5d:16.0	8086	2018	System peripheral	Intel Corporation Sky Lake-E M2PCI Registers (rev 04)
5d:16.4	8086	2018	System peripheral	Intel Corporation Sky Lake-E M2PCI Registers (rev 04)
5d:17.0	8086	2018	System peripheral	Intel Corporation Sky Lake-E M2PCI Registers (rev 04)
5e:00.x Slot 5	XXXX	XXXX	Card in expansion "Slot 5 " or "Slot 5 + Riser 1 st Slot "	-- *depending on PCIe expansion card* –
5f:00.x Slot 5	XXXX	XXXX	Card in expansion "Slot 5 + Riser 2 nd Slot "	-- *depending on PCIe expansion card* –
60:00.x Slot 5	XXXX	XXXX	Card in expansion "Slot 5 + Riser 3 rd Slot "	-- *depending on PCIe expansion card* –
61:00.x Slot 5	XXXX	XXXX	Card in expansion "Slot 5 + Riser 4 th Slot "	-- *depending on PCIe expansion card* –
Next buses are only available if a second CPU is installed				
80:04.0	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)
80:04.1	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)
80:04.2	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)
80:04.3	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)
80:04.4	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)
80:04.5	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)
80:04.6	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)
80:04.7	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)
80:05.0	8086	2024	System peripheral	Intel Corporation Sky Lake-E MM/Vt-d Configuration Registers (rev 04)
80:05.2	8086	2025	System peripheral	Intel Corporation Sky Lake-E RAS (rev 04)
80:05.4	8086	2026	PIC	Intel Corporation Sky Lake-E IOAPIC (rev 04) (prog-if 20 [IO(X)-APIC])
80:08.0	8086	2014	System peripheral	Intel Corporation Sky Lake-E Ubox Registers (rev 04)
80:08.1	8086	2015	Performance counters	Intel Corporation Sky Lake-E Ubox Registers (rev 04)
80:08.2	8086	2016	System peripheral	Intel Corporation Sky Lake-E Ubox Registers (rev 04)
85:00.0 Slot 2	8086	2030	PCI bridge	Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04)
85:01.0 Slot 2	8086	2031	PCI bridge	Intel Corporation Sky Lake-E PCI Express Root Port B (rev 04) **NOTE:** Will be present if there is a riser of type (x4x4x4x4) and a card in the 2nd slot. **NOTE:** Will be present if there is a riser of type (x4x4x8) and a card in the 2nd slot.
85:02.0 Slot 2	8086	2032	PCI bridge	Intel Corporation Sky Lake-E PCI Express Root Port C (rev 04) **NOTE:** Will be present if there is a riser of type (x4x4x4x4) and a card in the 3rd slot. **NOTE:** Will be present if there is a riser of type (x8x4x4) and a card in the 2nd slot. **NOTE:** Will be present if there is a riser of type (x4x4x8) and a card in the 3rd slot. **NOTE:** Will be present if there is a riser of type (x8x8) and a card in the 2nd slot.
85:03.0 Slot 2	8086	2033	PCI bridge	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.
85:05.0	8086	2034	System peripheral	Intel Corporation Sky Lake-E VT-d (rev 04)
85:05.2	8086	2035	System peripheral	Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04)
85:05.4	8086	2036	PIC	Intel Corporation Sky Lake-E IOxAPIC Configuration Registers (rev 04) (prog-if 20 [IO(X)-APIC])
85:08.0	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:08.1	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:08.2	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:08.3	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:08.4	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:08.5	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:08.6	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:08.7	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:09.0	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:09.1	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:09.2	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:09.3	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:09.4	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)

85:09.5	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:09.6	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:09.7	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0a.0	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0a.1	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0a.2	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0a.3	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0a.4	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0a.5	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0a.6	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0a.7	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0b.0	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0b.1	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0b.2	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0b.3	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0e.0	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0e.1	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0e.2	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0e.3	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0e.4	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0e.5	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0e.6	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0e.7	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0f.0	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0f.1	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0f.2	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0f.3	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0f.4	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0f.5	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0f.6	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:0f.7	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:10.0	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:10.1	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:10.2	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:10.3	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:10.4	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:10.5	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:10.6	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:10.7	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:11.0	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:11.1	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:11.2	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:11.3	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:1d.0	8086	2054	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:1d.1	8086	2055	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:1d.2	8086	2056	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:1d.3	8086	2057	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
85:1e.0	8086	2080	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
85:1e.1	8086	2081	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
85:1e.2	8086	2082	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
85:1e.3	8086	2083	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
85:1e.4	8086	2084	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)

85:1e.5	8086	2085	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
85:1e.6	8086	2086	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
86:00.x Slot 2	XXXX	XXXX	Card in expansion "Slot 2 " or "Slot 2 + Riser 1 st Slot "	-- *depending on PCIe expansion card* –
87:00.x Slot 2	XXXX	XXXX	Card in expansion "Slot 2 + Riser 2 nd Slot "	-- *depending on PCIe expansion card* –
88:00.x Slot 2	XXXX	XXXX	Card in expansion "Slot 2 + Riser 3 rd Slot "	-- *depending on PCIe expansion card* –
89:00.x Slot 2	XXXX	XXXX	Card in expansion "Slot 2 + Riser 4 th Slot "	-- *depending on PCIe expansion card* –
ae:00.0 Slot 4	8086	2030	PCI bridge	Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04)
ae:05.0	8086	2034	System peripheral	Intel Corporation Sky Lake-E VT-d (rev 04)
ae:05.2	8086	2035	System peripheral	Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04)
ae:05.4	8086	2036	PIC	Intel Corporation Sky Lake-E IOxAPIC Configuration Registers (rev 04) (prog-if 20 [IO(X)-APIC])
ae:08.0	8086	2066	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
ae:09.0	8086	2066	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
ae:0a.0	8086	2040	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
ae:0a.1	8086	2041	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
ae:0a.2	8086	2042	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
ae:0a.3	8086	2043	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
ae:0a.4	8086	2044	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
ae:0a.5	8086	2045	System peripheral	Intel Corporation Sky Lake-E LM Channel 1 (rev 04)
ae:0a.6	8086	2046	System peripheral	Intel Corporation Sky Lake-E LMS Channel 1 (rev 04)
ae:0a.7	8086	2047	System peripheral	Intel Corporation Sky Lake-E LMDP Channel 1 (rev 04)
ae:0b.0	8086	2048	System peripheral	Intel Corporation Sky Lake-E DECS Channel 2 (rev 04)
ae:0b.1	8086	2049	System peripheral	Intel Corporation Sky Lake-E LM Channel 2 (rev 04)
ae:0b.2	8086	204a	System peripheral	Intel Corporation Sky Lake-E LMS Channel 2 (rev 04)
ae:0b.3	8086	204b	System peripheral	Intel Corporation Sky Lake-E LMDP Channel 2 (rev 04)
ae:0c.0	8086	2040	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
ae:0c.1	8086	2041	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
ae:0c.2	8086	2042	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
ae:0c.3	8086	2043	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
ae:0c.4	8086	2044	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
ae:0c.5	8086	2045	System peripheral	Intel Corporation Sky Lake-E LM Channel 1 (rev 04)
ae:0c.6	8086	2046	System peripheral	Intel Corporation Sky Lake-E LMS Channel 1 (rev 04)
ae:0c.7	8086	2047	System peripheral	Intel Corporation Sky Lake-E LMDP Channel 1 (rev 04)
ae:0d.0	8086	2048	System peripheral	Intel Corporation Sky Lake-E DECS Channel 2 (rev 04)
ae:0d.1	8086	2049	System peripheral	Intel Corporation Sky Lake-E LM Channel 2 (rev 04)
ae:0d.2	8086	204a	System peripheral	Intel Corporation Sky Lake-E LMS Channel 2 (rev 04)
ae:0d.3	8086	204b	System peripheral	Intel Corporation Sky Lake-E LMDP Channel 2 (rev 04)
af:00.x Slot 4	XXXX	XXXX	Card in expansion "Slot 4 "	-- *depending on PCIe expansion card* –
d7:00.0 Slot 3	8086	2030	PCI bridge	Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04)
d7:05.0	8086	2034	System peripheral	Intel Corporation Sky Lake-E VT-d (rev 04)
d7:05.2	8086	2035	System peripheral	Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04)
d7:05.4	8086	2036	PIC	Intel Corporation Sky Lake-E IOxAPIC Configuration Registers (rev 04) (prog-if 20 [IO(X)-APIC])
d7:0e.0	8086	2058	Performance counters	Intel Corporation Sky Lake-E KTI 0 (rev 04)
d7:0e.1	8086	2059	System peripheral	Intel Corporation Sky Lake-E UPI Registers (rev 04)
d7:0f.0	8086	2058	Performance counters	Intel Corporation Sky Lake-E KTI 0 (rev 04)
d7:0f.1	8086	2059	System peripheral	Intel Corporation Sky Lake-E UPI Registers (rev 04)

d7:01.1	8086	2059	System peripheral	Intel Corporation Sky Lake-E UPI Registers (rev 04)
d7:10.0	8086	2058	Performance counters	Intel Corporation Sky Lake-E KTI 0 (rev 04)
d7:10.1	8086	2059	System peripheral	Intel Corporation Sky Lake-E UPI Registers (rev 04)
d7:12.0	8086	204c	Performance counters	Intel Corporation Sky Lake-E M3KTI Registers (rev 04)
d7:12.1	8086	204d	Performance counters	Intel Corporation Sky Lake-E M3KTI Registers (rev 04)
d7:12.2	8086	204e	System peripheral	Intel Corporation Sky Lake-E M3KTI Registers (rev 04)
d7:12.4	8086	204c	Performance counters	Intel Corporation Sky Lake-E M3KTI Registers (rev 04)
d7:12.5	8086	204d	Performance counters	Intel Corporation Sky Lake-E M3KTI Registers (rev 04)
d7:15.0	8086	2018	System peripheral	Intel Corporation Sky Lake-E M2PCI Registers (rev 04)
d7:16.0	8086	2018	System peripheral	Intel Corporation Sky Lake-E M2PCI Registers (rev 04)
d7:16.4	8086	2018	System peripheral	Intel Corporation Sky Lake-E M2PCI Registers (rev 04)
d7:17.0	8086	2018	System peripheral	Intel Corporation Sky Lake-E M2PCI Registers (rev 04)
d8:00.x Slot 3	XXXX	XXXX	Card in expansion " `Slot 3 "`	*-- depending on PCIe expansion card –*

NOTE:

Slot n : 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

Kontron P/N	Description
CG2200-FANSET 	Fan assembly (6 fans)

HDD/SSD carrier

Kontron P/N	Description
NSNSASHDDCARQ 	SAS HDD/SATA SSD carrier Contents: Carrier, black plastic filler, screws (4)

Front bezel

Kontron P/N	Description
CG2100-BEZEL01 	Chassis front bezel

Top cover

Kontron P/N	Description
1067-1312 	Chassis top cover kit Contents: Top Cover and Safety Label

Power supply units

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

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 slot s.

	Slot_3	Slot_4	Slot_5
Any half-height PCIe card, except RAID	No	Yes	Yes
RAID	Yes	No	No

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).

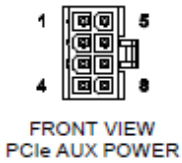
Each of these PCIe slots can support a single slot PCIe x16 riser or a dual slot PCIe x8 riser.
PCIe riser cards plugged in slot 2 connect to CPU 2 while PCIe riser cards in slot 6 connect to CPU 1.
All riser card assemblies can support up to full -height, full-length cards.
The following table identifies the different configuration possibilities and the maximum number of PCIe cards that can be connected through riser cards.

Riser configuration	PCIe cards
2 single-slot risers	2 single or double-width, x16 cards
1 single-slot riser 1 dual-slot riser	1 single or double-width, x16 card 2 single-width, x8 cards
2 dual-slot risers	4 single-width, x8 cards

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.

Pin	Signal	Color
1	GND	Black
2	GND	Black
3	GND	Black
4	GND	Black
5	+12V	Yellow
6	+12V	Yellow
7	+12V	Yellow
8	+12V	Yellow

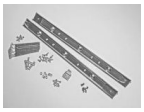


PCIe riser s

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

* 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

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

Accessories

Kontron P/N	Description
1066-0224	Thermal probe
K00740-001	Mounting bracket for Battery Backup unit
1065-5409	TPM 2.0 module

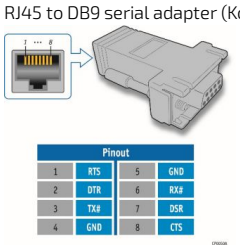
Material, information and software required

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

Table of contents

Material and information required

Optional adapter

Item_1	RJ45 to DB9 serial adapter (Kontron P/N: 1015-9404) 

Component installation and assembly

Relevant section:
Components installation and assembly

Item_1	#1 Phillips (cross-point) screwdrivers (or interchangeable tip screwdriver with #1 and #2 Phillips bits)
Item_2	#2 Phillips (cross-point) screwdrivers (or interchangeable tip screwdriver with #1 and #2 Phillips bits)
Item_3	One T30 Torx screwdriver
Item_4	One 5 -mm flat-head screwdriver
Item_5	Personal grounding device such as an anti-static wrist strap and a grounded conductive pad

Power cables and tooling

Relevant sections:
Cabling
Rack installation

Item_1	Black stranded 12 AWG wire to build the power cable based on the length required
Item_2	Red stranded 12 AWG wire to build the power cable based on the length required
Item_3	One Positronic DC power supply input mating connector (includes a strain relief assembly)
Item_4	Three Positronic gauge-16 crimp terminals
Item_5	Two strain relief screws
Item_6	One strain relief plate
Item_7	Two flat head Phillips screws
Item_8	One hand crimp tool, DMC AF8
Item_9	One manual extraction tool
Item_10	One 8 AWG ground cable based on the length required
item_11	One ground lug right angle, 8 AWG (Kontron P/N 1064-4226)
Item_12	10 mm wrench or equivalent tool
Item_13	One hand crimp tool, Panduit CT-1700

Rack installation material

Relevant section:
Rack installation

Item_1	Rail kit (based on your installation requirements)

Network cables and modules

Item_1	One RJ45 Ethernet management plane cable
Item_2	Two RJ45 Ethernet data plane cables
Item_3	One RJ45 serial connection cable

Network infrastructure

IP addresses:

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

Software required

Item_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.
Item_2	A terminal emulator such as **puTTY** is installed on a remote computer.
Item_3	A hardware detection tool such as **pciutils** is installed on the local server to view information about devices connected to the server PCI buses .

Hardware compatibility list

{This article provides the l ist of qualified and compatible hardware components .}

Table of contents

CPU

Vendor	Description	Core	Frequency	Power	Status	Kontron P/N
Intel	Xeon ® Silver 4114T, Skylake	10	2.2 GHz	85 W	Active	1061-9790
Intel	Xeon ® Gold 5218T, Cascade Lake	16	2.1 GHz	105 W	Active	1065-4808
Intel	Xeon ® Gold 6230T, Cascade Lake	20	2.1 GHz	125 W	Active	1065-5295

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

Vendor	Vendor P/N	Type	Size	Status	Kontron P/N
Samsung	M393A2K40CB2-CVF	DDR4-2933	16 GB	Active	1065-6019
Micron	MTA18ASF2G72PDZ-2G9E1	DDR4-2933	16 GB	Active	
Micron	MTA36ASF8G72PZ-2G9B2	DDR4-2933	64 GB*	Active	1066-9555
Samsung	M393A8G40MB2-CVF	DDR4-2933	64 GB*	Active	

*Only supported with Cascade Lake CPUs

M.2 SSD (SATA or NVMe)

Vendor	Vendor P/N	Type	Size	Dimension	DWPD	Status	Kontron P/N
Innodisk	DEM28-32GM41BC1DC	SATA	32 GB	2280		Active	N/A
Intel	SSDSCKKB240G801	SATA	240 GB	2280	1.9	Active	1065-5634
Intel	SSDSCKKB480G801	SATA	480 GB	2280	1.3	Active	1065-5635
Intel	SSDPEKKA256G801	NVMe	256 GB	2280		Active**	1065-5636
Intel	SSDPEKKA512G801	NVMe	512 GB	2280		Active**	1065-5632

**The m odule 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)

Vendor	Vendor P/N	DWPD	Size	Operating temperature	Status	Kontron P/N
Samsung	MZ7LH240HAHQ-00005	1.3 (3 years)	240 GB	0°C to 70°C	Active	1066-7175
Samsung	MZ7KH240HAHQ-00005	3 (5 years)	240 GB	0°C to 70°C	Active	1065-6022

SSD 2.5 in (SAS)

Vendor	Vendor P/N	DWPD	Size	Operating temperature	Status	Kontron P/N
Samsung	MZILT1T9HAJQ-00007	1 (5 years)	1.92 TB	0°C to 70°C	Active	N/A

HDD SAS 2.5 in (SAS)

Vendor	Vendor P/N	Fast format	Size	RPM	12 Gbps SAS	Operating temperature	Status	Kontron P/N
Seagate	ST300MM0048	512n	300 GB	10K	Yes	5°C to 55°C	Active	1061-6231
Toshiba	AL14SEB030N	512n	300 GB	10K	Yes	5°C to 55°C	Active	
Toshiba	AL15SEB030N	512n	300 GB	10K	Yes	5°C to 55°C	Active	
Toshiba	AL14SEB060N	512n	600 GB	10K	Yes	5°C to 55°C	Active	1061-6070
Toshiba	AL15SEB060N	512n	600 GB	10K	Yes	5°C to 55°C	Active	
Seagate	ST600MM0009	512n	600 GB	10K	Yes	5°C to 55°C	Active	
Seagate	ST1800MM0129	512e/4Kn	1.8 TB	10K	Yes	5°C to 55°C	Active	1061-7429
Toshiba	AL15SEB18EP	512e/4Kn	1.8 TB	10K	Yes	5°C to 55°C	Not tested	
Toshiba	AL15SEB24EQ	512e	2.4 TB	10K	Yes	5°C to 55°C	Not tested	1062-4999

SAS and RAID PCIe cards

Vendor	Description	Type	Status	Kontron P/N
LSI/Broadcom	MegaRAID SAS 9361-8i	RAID/SAS	Active	1065-5999
LSI/Broadcom	CacheVault LSICVM02	Cache Vault	Active	1065-7732
LSI/Broadcom	SAS 9300-8i Host Bus Adapter	SAS	Active	1065-7730
Adaptec/MicroSemi	SmartRAID 3162-8i/e	RAID/SAS	Active	N/A

PCIe NIC cards

Vendor	Description	Type	Status	Kontron P/N
Intel	4-port Gigabit Ethernet, RJ-45 (copper) NIC card	Network Interface (10/100/1000 Mbps)	Active	1059-8279

Validated operating systems

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

Table of contents

Status description

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

OS certification status

Operating system	CG2400
Windows Server 2016	CERTIFIED
Windows Server 2019	CERTIFIED
SUSE SLES 15 (Suse Entreprise)	PLANNED
Ubuntu 18.04	VALIDATED
Ubuntu 16.04	VALIDATED
RHEL 8.2 - 8.x	CERTIFIED
RHEL 7.8 - 7.x	CERTIFIED
VMware ESXi 6.7	VALIDATED
~~CentOS 7.6 (Included with RHEL)~~	VALIDATED

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

{This section provides Information about installing the platform hardware components, operating systems and softwares.}

Children

- Mechanical installation and precautions
  - ESD protections
  - Unboxing
  - Components installation and assembly
  - Airflow
  - Rack installation
  - Cabling
- Software installation and deployment
  - Preparing for installation
  - Installing an operating system on a server
  - Verifying installation
  - Platform installation for high availability
  - Common software installation

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.

	**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.

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

	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

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

	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.

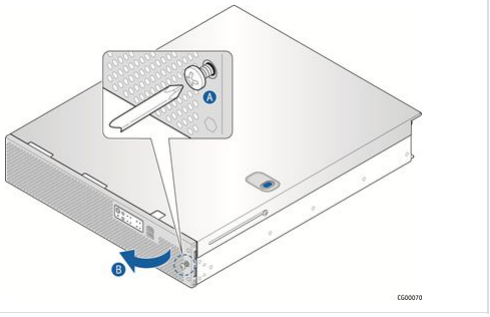
Front bezel

Removing the front bezel

The front bezel has to be removed to perform tasks such as:

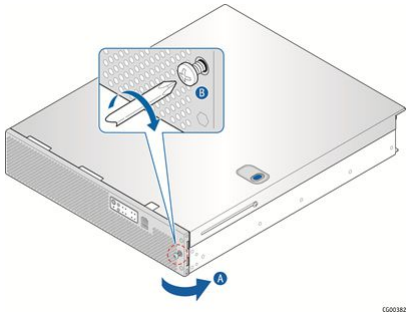
- Installing or removing hot-swappable hard disk drives or an SD flash card
- Observing the individual hard disk drive activity/fault indicators
- Replacing the control panel LED/switch board

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

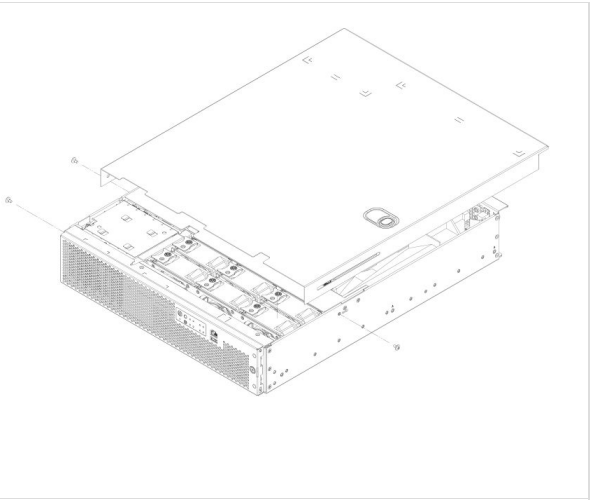
⚠	Standby power is present inside the chassis whenever the power supply module(s) are connected to a power source. Before removing the top cover, always power down the server and unplug all peripheral devices and the power cable(s).

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.

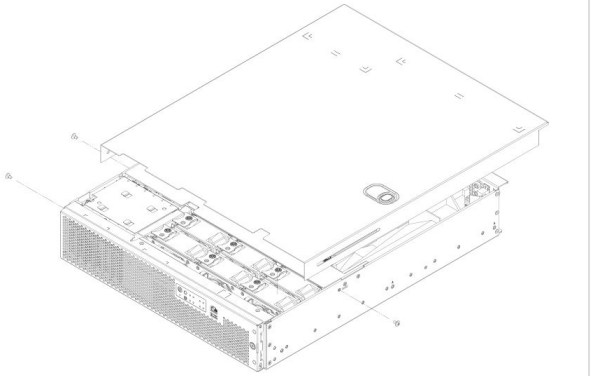
Removing the chassis top cover

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 bracke t 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 th e 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 tooled 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.



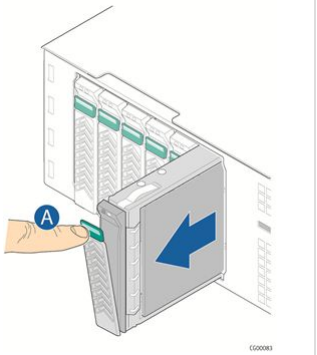
Drives

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

- the [Content under creation] front bezel

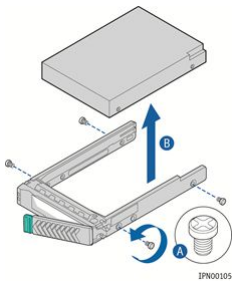
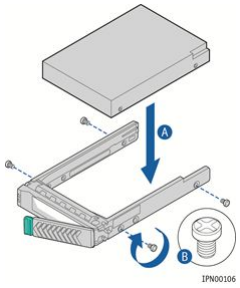
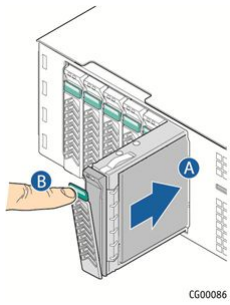
NOTICE	If you install fewer than six drives, to ensure proper cooling, the unused drive slots must contain the empty carriers with filler panels that ship with the platform.

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.

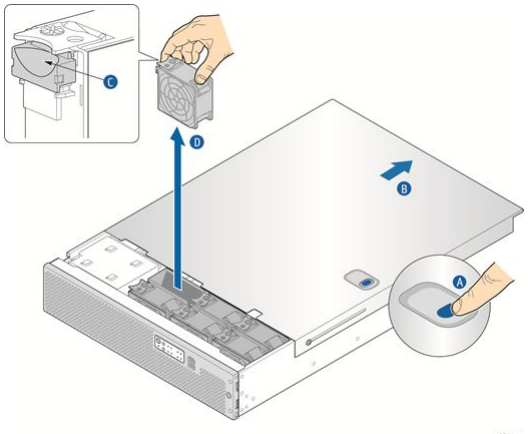
Step_1	If the drive carrier is empty (first time installation), remove the black plastic filler panel by unfastening the four screws that attach it to the carrier (A). Set the screws aside for use with the new drive. **OR** If a drive is already installed (drive replacement), remove it by unfastening 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.

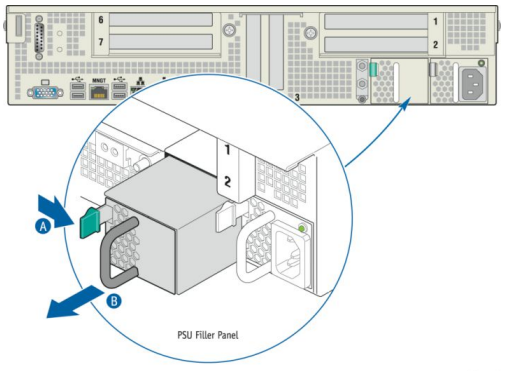
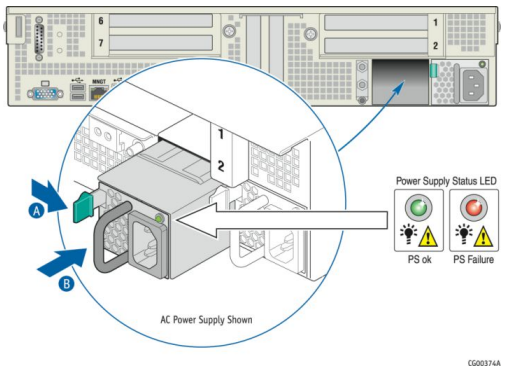
Replacing a fan

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, s lide 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), u nplug the power cord from the PSU being replaced. R emove 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):

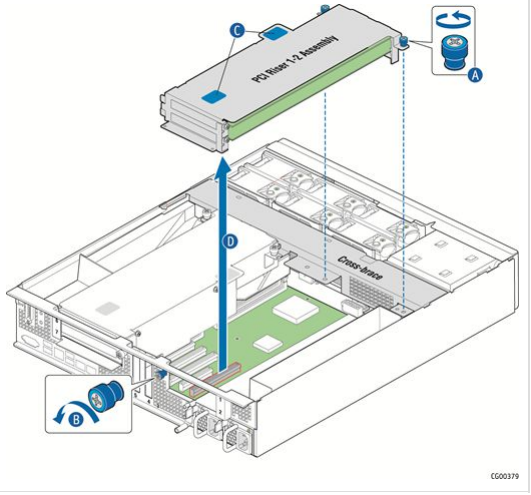
- the [Content under creation] chassis top cover

	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

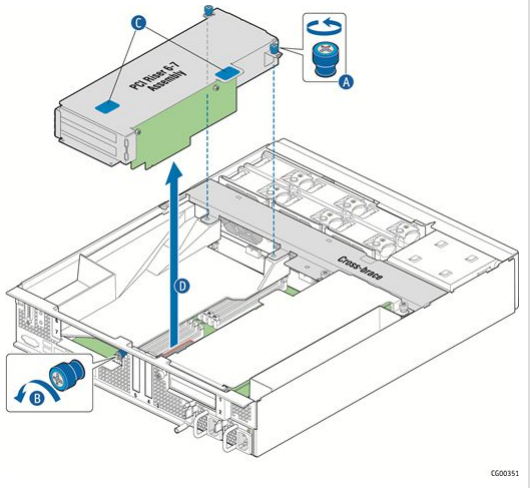
Removing the left riser card assembly

Step_1	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).
Step_2	Using the two blue touch points (C), lift the riser card assembly out of the chassis (D).



Removing the right riser card assembly

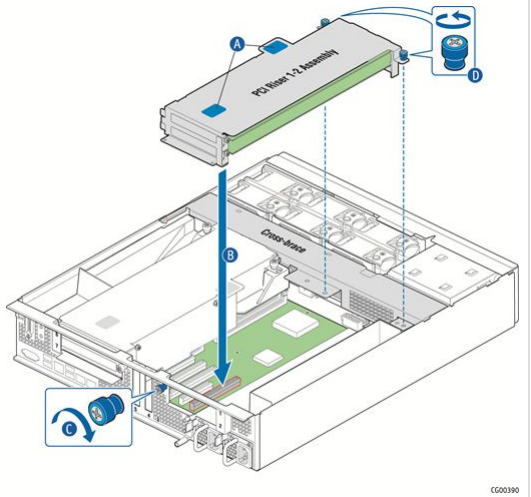
Step_1	Loosen the two blue captive retention screws (A) at the front of the riser assembly and the blue captive screw at the rear of the chassis (B).
Step_2	Using the two blue touch points (C), lift the riser card assembly out of the chassis (D).



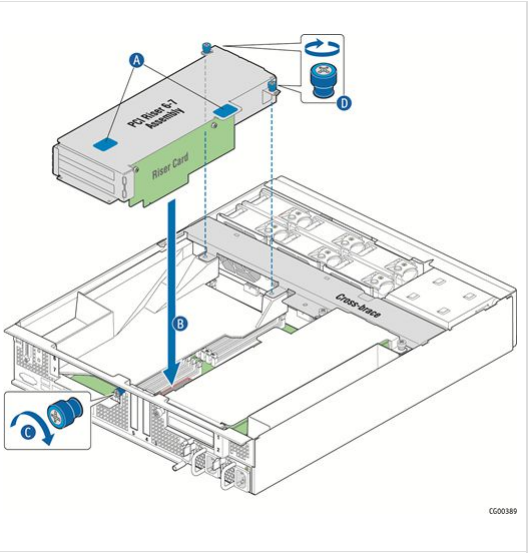
Reinstalling a riser card assembly

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).	

Processor air duct

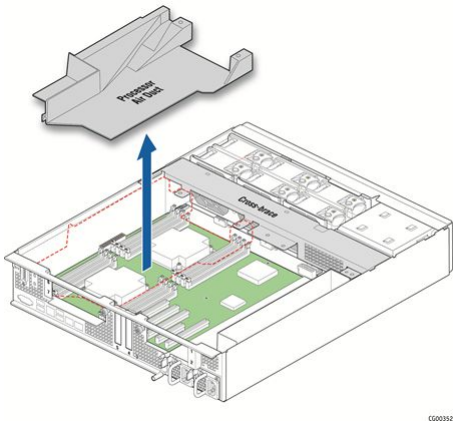
Before you can remove and reinstall processor air duct , you must first remove (and afterwards put back in place):

- the [Content under creation] chassis top cover
- the [Content under creation] riser card assemblies

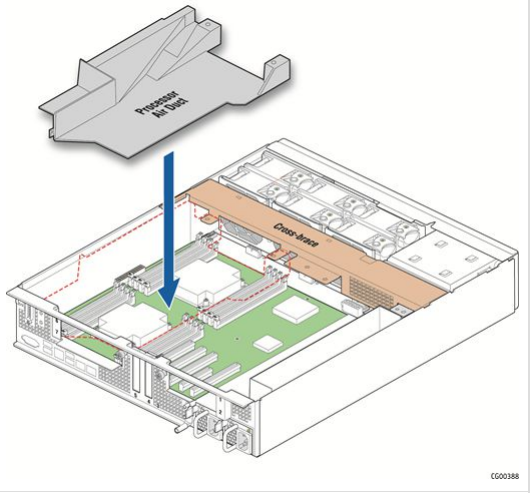
	The black plastic processor air duct must be removed to access the processors and the memory DIMMs or to replace the platform board.

NOTICE	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

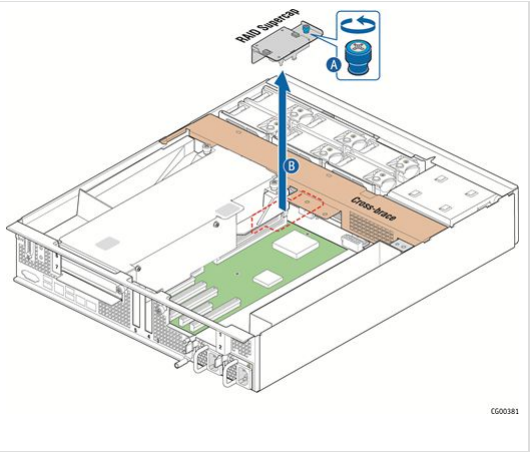
Step_1	Place the processor air duct over the processor sockets and DIMMs. Align the front tabs with the captive screws on the support cross-brace . Make sure the pin located on the rear of the chassis is inserted in the moulded groove on the back side of the processor air duct The air duct is secured when the right riser card assembly is mounted on the support cross-brace above it.	

SuperCap battery backup

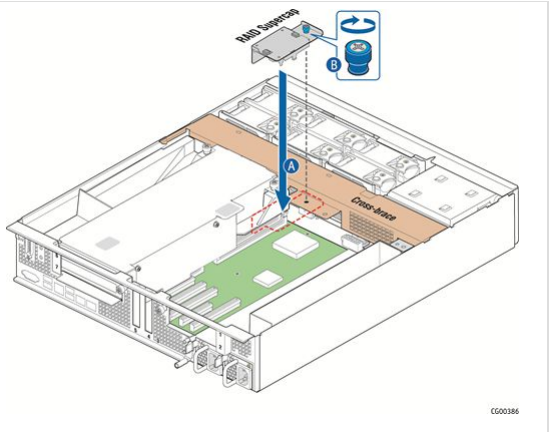
The optional RAID battery backup and its bracket, if installed, have to be removed to install or remove components located on that area of the motherboard, such as a M.2 module. Since t he SuperCap battery backup module is fastened to the support cross-brace , it has to be removed anytime the cross-brace 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 [Content under creation] Raid controller section.
Before you can remove and reinstall the SuperCap battery backup , you must first remove (and afterwards put back in place):

- the [Content under creation] chassis top cover
- the left [Content under creation] riser card assembly

Removing the SuperCap battery backup

Step_1	Loosen the captive screw that fastens the battery backup to the support cross-brace (A).	
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

Step_1	Position the SuperCap backup battery assembly over the support cross-brace (A).	
Step_2	Tighten the captive screw that fastens the battery backup to the support cross-brace (B).	

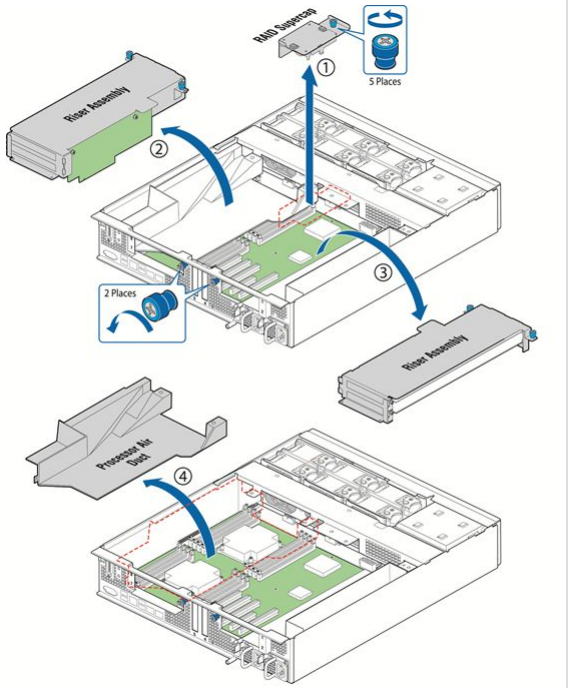
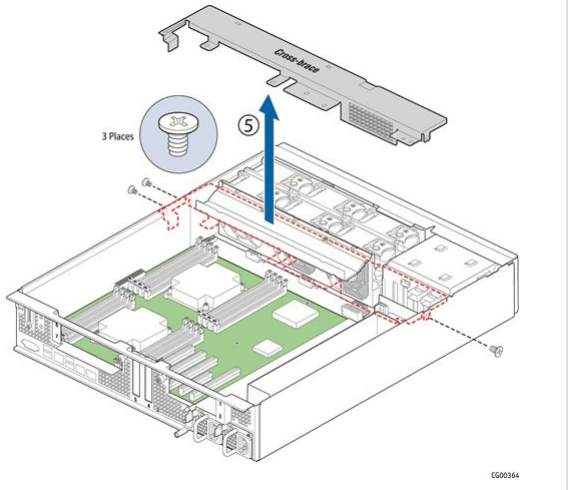
Support cross-brace

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

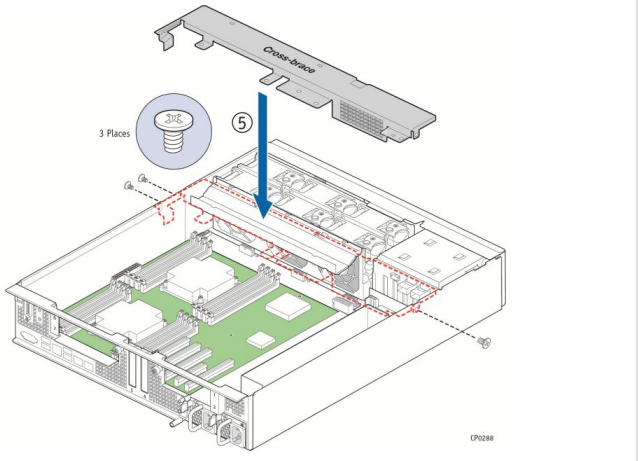
as the front panel board or the power distribution board, cannot be replaced without first removing the cross-brace (along with all the components attached to it). This procedure is necessary in order to have enough space to access these front chassis components.
Before you can remove and reinstall the support cross-brace , you must first remove (and afterwards put back in place):

- the [Content under creation] chassis top cover
- the [Content under creation] riser card assemblies
- the [Content under creation] processor air duct
- the [Content under creation] 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

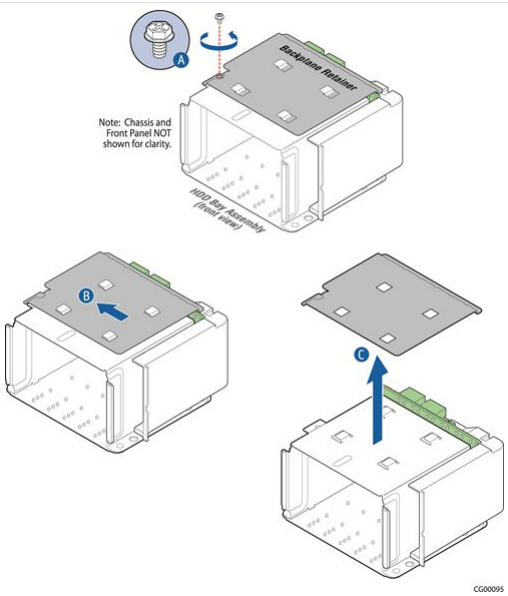
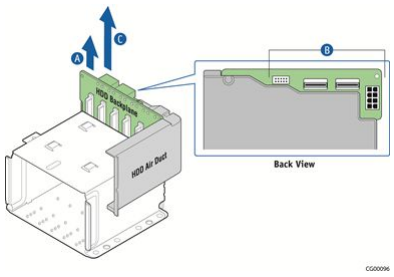
Step_1	Reposition the support cross-brace in the chassis.	
Step_2	Secure the support cross-brace with the three reserved screws: • One on the left side • Two on the right side	

SAS hot-swap backplane (HSBP) board

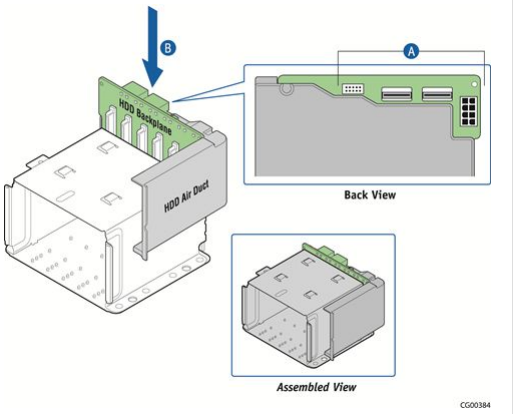
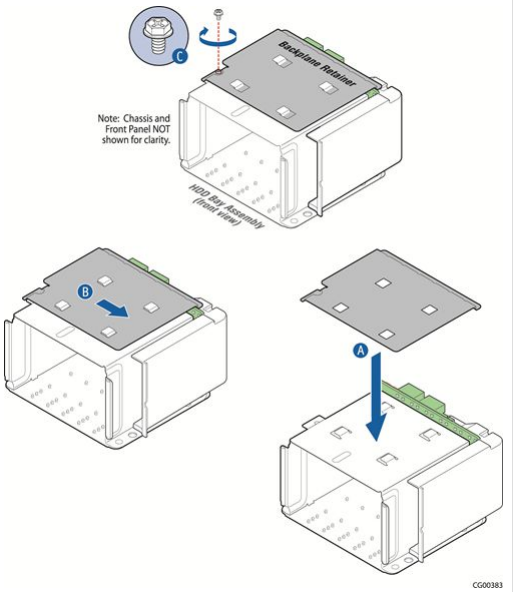
The SAS HSBP board has to be removed to replace the HSBP board or the p ower distribution board (PDB).
The six-slot SAS backplane board is located at the rear of the HDD drive bay assembly. It is held in place by a cover plate on top of the HDD bay assembly that goes over the top edge of the backplane 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 [Content under creation] chassis top cover
- the [Content under creation] front bezel

Removing the SAS hot-swap backplane (HSBP) board

Step_1	Slide all drives out from the drive bay slots to disengage them from the backplane.	
Step_2	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).	
Step_3	Lift the cover plate off of the HDD bay assembly (C).	
Step_4	Lift the HSBP board and HDD air duct assembly up to access the connectors on the back of the board (A).	
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 I ^{2}C/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 I ^{2}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

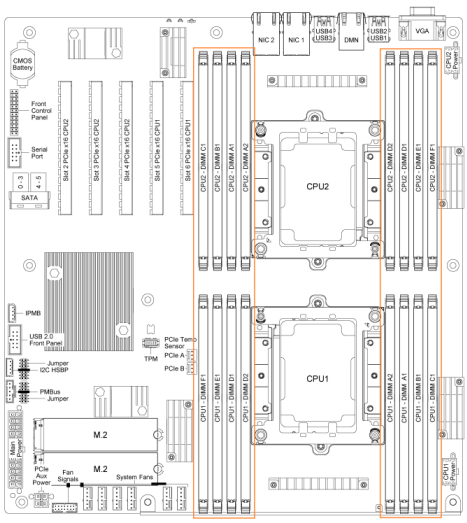
Before you can remove or install memory DIMMs , you must first remove (and afterwards put back in place):

- the [Content under creation] chassis top cover
- the right side [Content under creation] riser card assembly
- the [Content under creation] 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



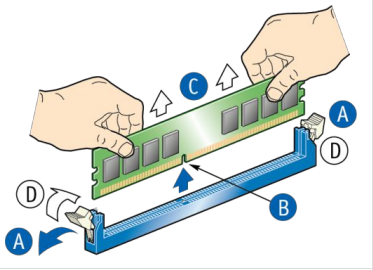
DIMM population guidelines for optimal performance

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, b oth 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.

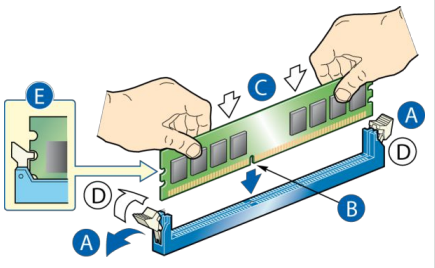
- For configurations with 1 to 3 DIMMs – populate slots A1, B1, C1, starting with A1.
- For configurations with 4 DIMMs – populate slots A1, B1, D1 and E1.
- Configurations with 5 DIMMs are not recommended as they are unbalanced and will produce a less optimal performance.
- For a configuration with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

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 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

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

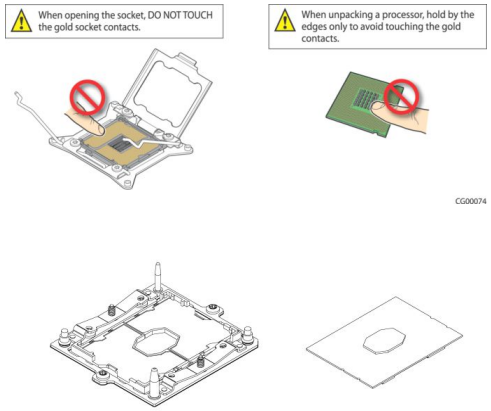
Before you can remove, add or replace a processor or heat sink, you must first remove (and afterwards put back in place):

- the [Content under creation] chassis top cover
- the right side [Content under creation] riser card assembly
- the [Content under creation] processor air duct

Socket and processor handling and ESD precautions

Handling precautions

NOTICE



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.

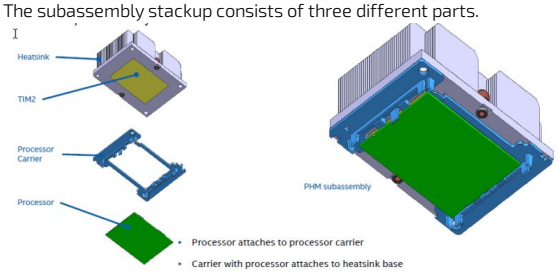


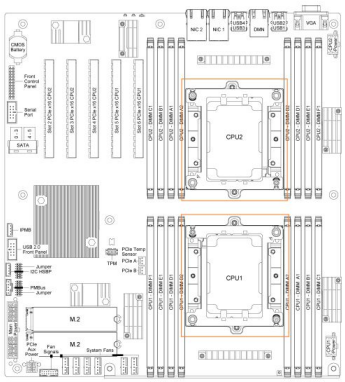
Image source: Intel Corporation

ESD precautions

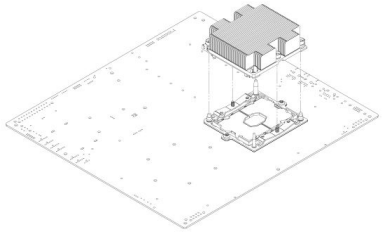
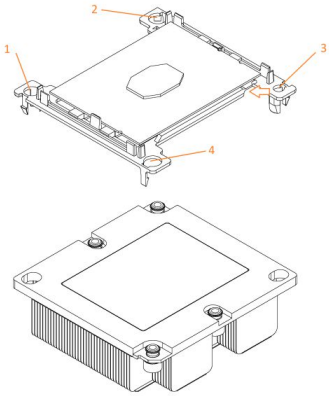
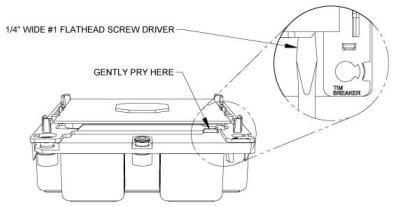
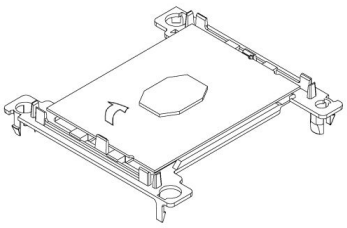
Be mindful of the following points when handling the processors and sockets to reduce the risk of electrostatic discharge (ESD) damage to the processor:

- 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. 4. Slightly unclip corner 4.	
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

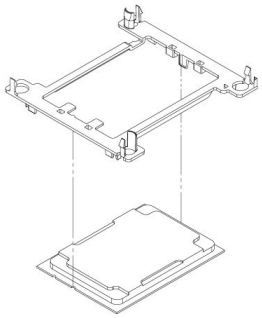
NOTICE	**The processor must be appropriate.** Severe damage to the platform board may occur if a processor that is inappropriate is installed. Refer to the Hardware compatibility list for a list of components.
NOTICE	Kontron recommends performing a CPU socket inspection before adding or replacing a processor to ensure there is nothing wrong with the fragile socket pins.

Preparing the processor for assembly with the PHM

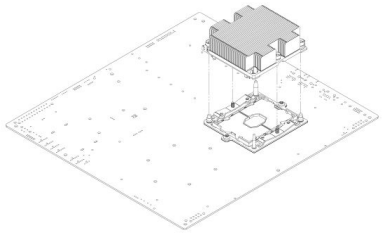
Step_1	Remove the cover of the processor packing tray. From this position, the processor will be ready to be clipped to the rest of the PHM components. **CAUTION:** Do not touch the processor.

Installing the processor (new heat sink and processor carrier)

Relevant section: [Content under creation] 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

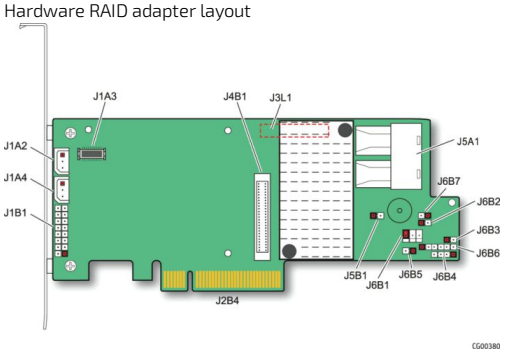
Step_1	Align the triangle of the bolster plate with that of the processor. Lay the PHM on the bolster plate.	
Step_2	Gradually (in a star pattern) and equally tighten each of the four screws in a diagonal pattern until each one is firmly tightened (12.0 i n-Lb torque) .	

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

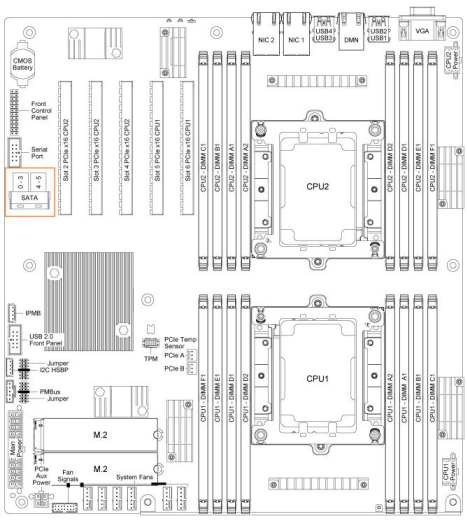


Before you can install or remove the hardware RAID controller board and the SuperCap battery backup module, you must first remove (and afterwards put back in place):

- the [Content under creation] chassis top cover
- the left side [Content under creation] riser card assembly

Disconnecting the two SAS cables from the motherboard

Locating the SAS cables

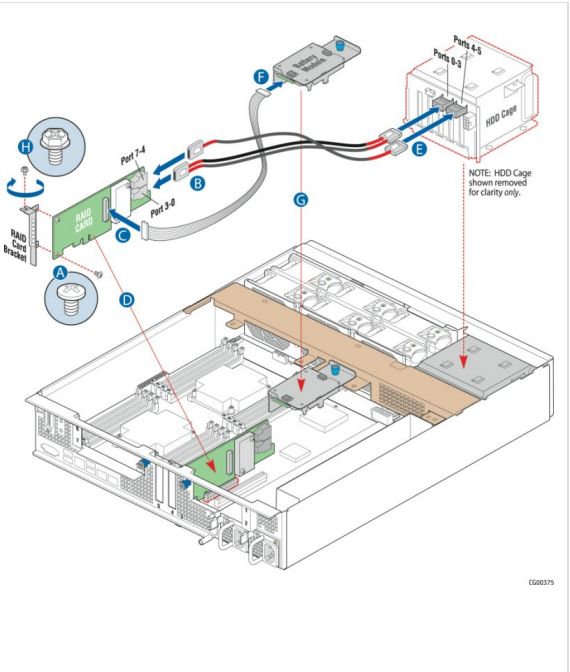


Disconnecting the SAS cables

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

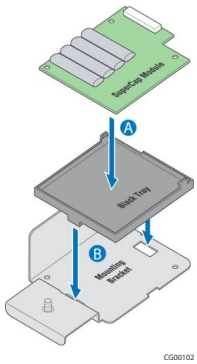
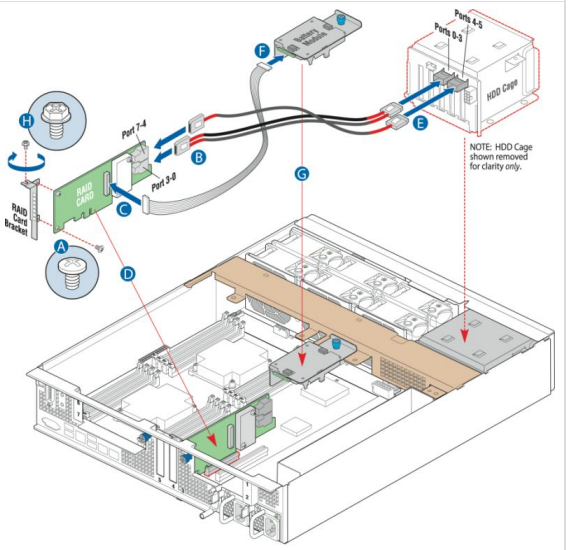
Installing a hardware RAID controller

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 b attery 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, p roceed 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 [Content under creation] 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

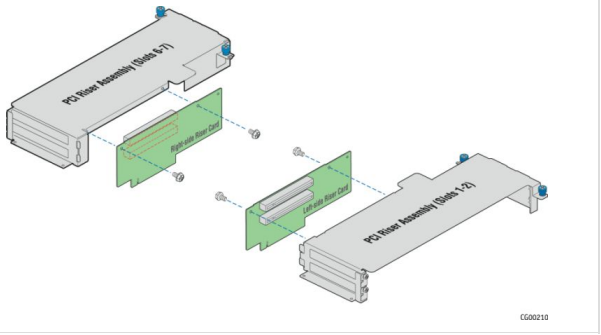
Step_1	Unfasten the screw holding the PCIe add-in card installed in the slot.
Step_2	Remove the PCIe add-in card from the motherboard's PCIe slot.
Step_3	Put the blank filler panel (removed when the card was installed) back in place and fasten it to the chassis using the screw removed at step 1. **NOTE:** 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 [Content under creation] chassis top cover
- the [Content under creation] 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.

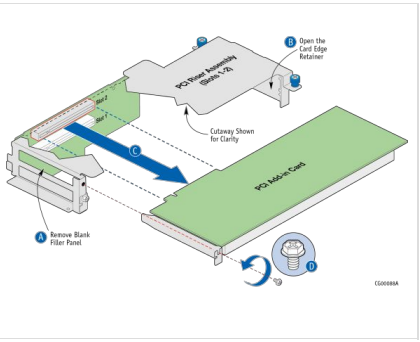
PCIe add-in cards on riser assemblies

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):

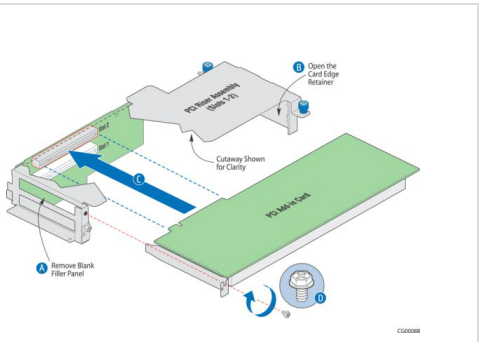
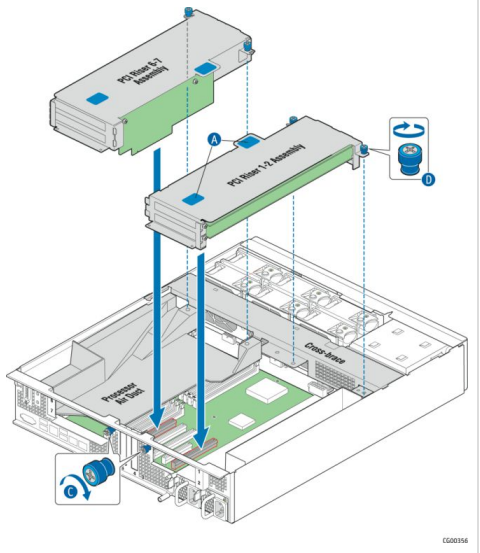
- the [Content under creation] chassis top cover

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 , [Content under creation] the riser card must be assembled . If a PCIe add-in card is already in place, consult the [Content under creation] 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 u nfastening the screw of the selected slot (D).	
Step_2	If you are installing a PCIe add-in card for the first time, f or 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).	

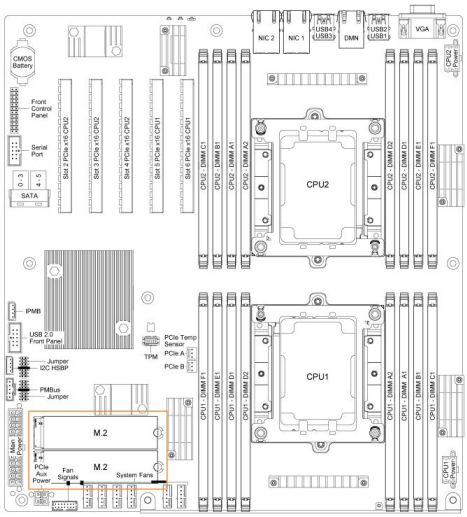
M.2 storage

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):

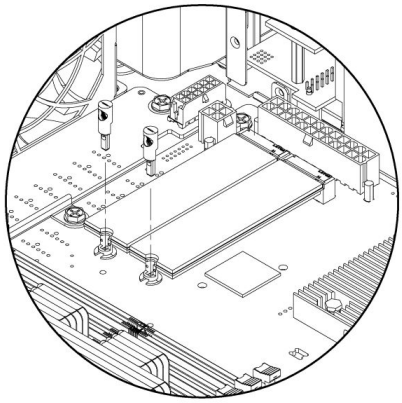
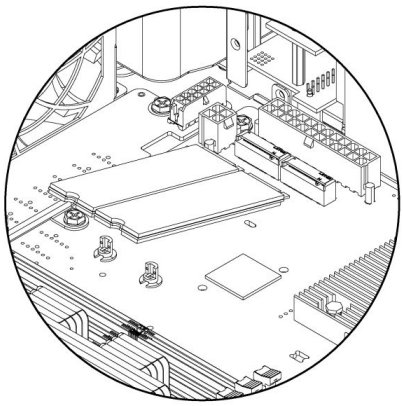
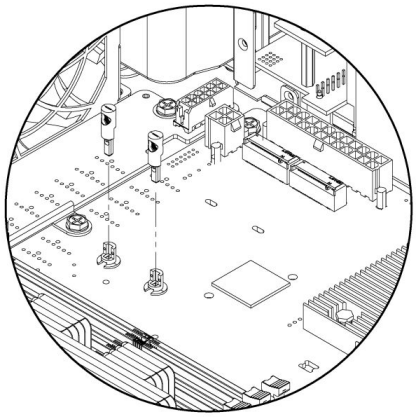
- the [Content under creation] chassis top cover
- the left side [Content under creation] riser card assembly

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

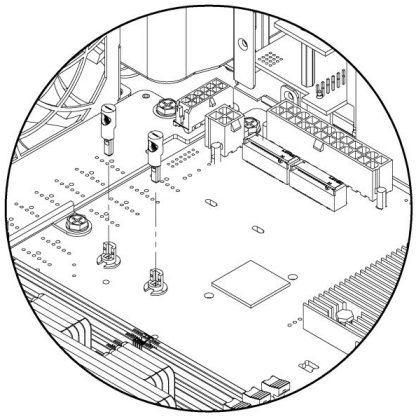
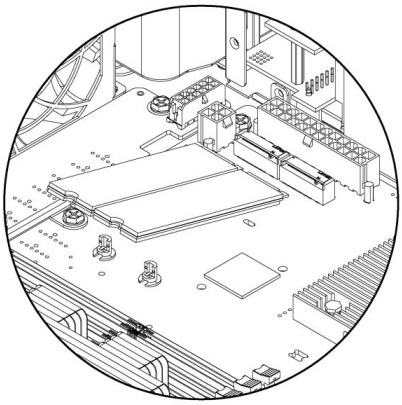
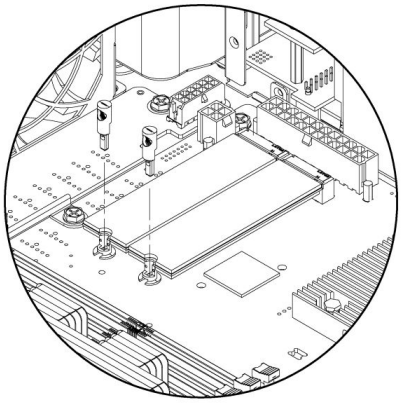
Locating the M.2 storage



Removing an M.2 storage

Step_1	Remove the clip from the post to release the M.2 storage.	
Step_2	Remove the M.2 card from the connector.	
Step_3	Insert the clip back in the post to secure the M.2 storage.	

Installing an M.2 storage

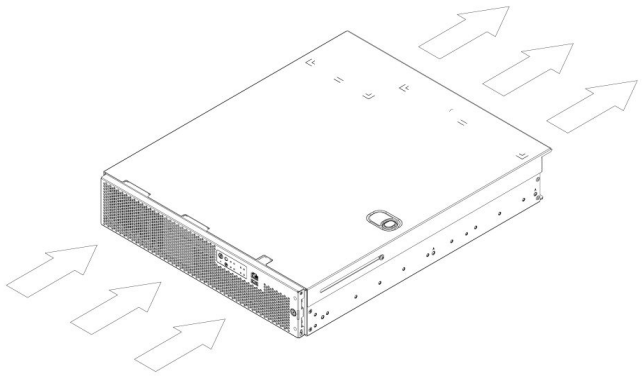
Step_1	Remove the clip from the post. **NOTE:** When only one M.2 storage is added, it is recommended to use the slot located near the fans.	
Step_2	Insert one end of the M.2 card in the connector and seat the other end around the post on the motherboard.	
Step_3	Secure the M.2 storage by inserting the clip in the post.	

Airflow

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

Table of contents

Airflow direction



Considerations for proper airflow

Relevant section:

Components installation and assembly

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.

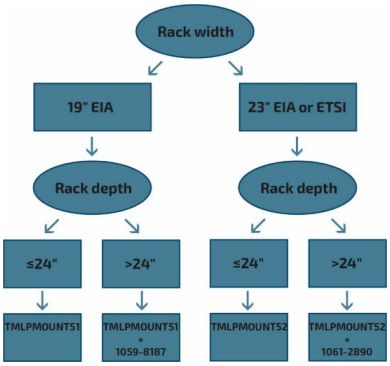
Rack installation

{This article provides instructions on how to install and ground a platform in a rack . }

Table of contents

Selecting a rail kit

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.



Product code	Description	Slide pull out mechanism	Minimum order
TMLCMOUNT21 	Rack mount kit Used to mount servers on 19" wide, 2-post racks. **NOTE** : For lab purposes only	No	10
TMLPMOUNT51 	Rack mount kit Used to mount servers on 19" wide, 2-post or 4-post racks. **NOTE:** Xylan finish	Yes	1
TMLPMOUNT52 	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 M aximum rack depth when used with TMLPMOUNT51: 34".	N/A	1
1061-2890 	Rail extender kit Maximum rack depth when used with TMLPMOUNT52: 34".	N/A	1

NOTES:

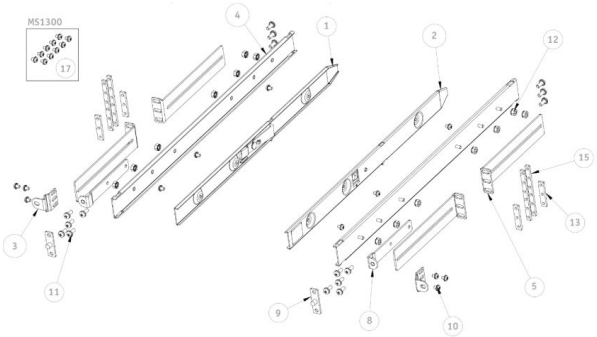
- Using slide rails could result in non-compliance with Seismic Zone 4 requirements of NEBS-3.
- Xylan is a tough, low-friction coating similar to Teflon.
- EIA Wide spacing doesn't have the interstitial hole that is present in EIA Universal spacing. TMLPMOUNT51 contains an EIA Wide Adapter to overcome issue.

Rack mount kits

TMLCMOUNT21

Refer to [Content under creation] TMLCMOUNT21 installation instructions for details.

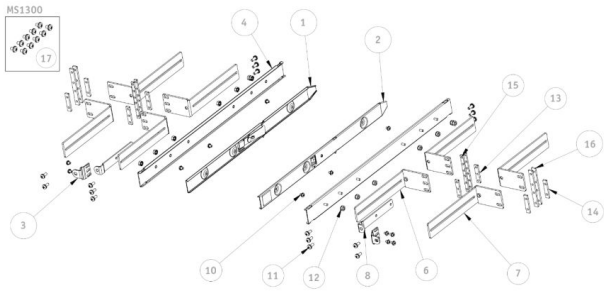
TMLPMOUNT51



Item	Qty	Description
1	1	LEFT INNER RAIL
2	1	RIGHT INNER RAIL
3	2	MOUNTING EAR
4	2	OUTER RAIL
5	4	19″ EIA L-BRACKET
8	2	2-POST MOUNTING BRACKET
9	2	EIA WIDE ADAPTER
10	12	8-32 X 1/4 SEMS SCREW
11	16	10-32 X 1/2 SEMS SCREW
12	14	8-32 KEPS NUT
13	4	1U EIA BARNUT
15	4	2U EIA BARNUT
17	12	M4x0.7 SCREWS FOR MS1300

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

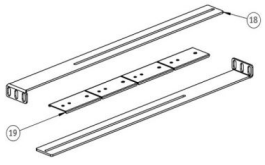


Item	Qty	Description
1	1	LEFT INNER RAIL
2	1	RIGHT INNER RAIL
3	2	MOUNTING EAR
4	2	OUTER RAIL
6	4	23″ EIA L-BRACKET
7	4	23″ ETSI L-BRACKET
8	2	2-POST MOUNTING BRACKET
10	12	8-32 X 1/4 SEMS SCREW
11	16	10-32 X 1/2 SEMS SCREW
12	14	8-32 KEPS NUT
13	4	1U EIA BARNUT
14	4	1U ETSI BARNUT
15	4	2U EIA BARNUT
16	4	2U ETSI BARNUT
17	12	M4x0.7 SCREWS FOR MS1300

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.

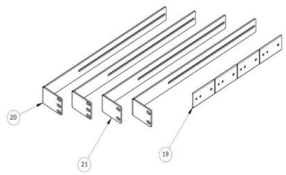
Bracket and extender kits

1059-8187 extender kit



Item	Qty	Description
18	2	24″ to 34″ EIA L-BRACKET FOR 19″ RACK
19	4	RETAINER BRACKET

1061-2890 extender kit



Item	Qty	Description
19	4	RETAINER BRACKET
20	2	24″ to 34″ EIA L-BRACKET FOR 23″ RACK
21	2	24″ to 34″ ETSI L-BRACKET FOR 23″ RACK

Installing the server in a rack

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 m ains power disconnect, earth grounding and AC overcurrent protection.

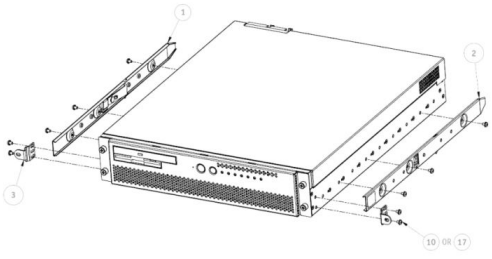
NOTICE	**Temperature** — The operating temperature of the server, when installed in an equipment rack, must not go below 5°C (41°F) or rise above 40°C (104°F). Extreme fluctuations in temperature can cause a variety of problems in the server.

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

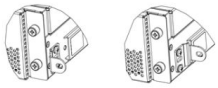
Using TMLPMOUNT51 or TMLPMOUNT52

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.

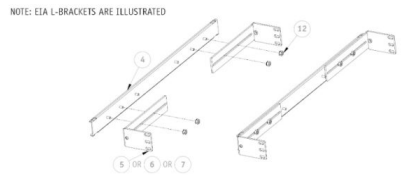


Building the outer rail assembly

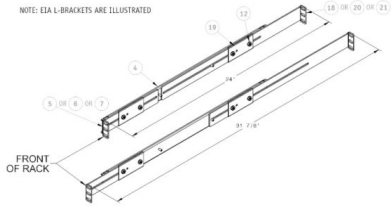
- For a 4-post installation for racks under 24″ deep, go to [Content under creation] Four-post installation – racks under 24-inches deep
- For a 4-post installation for racks 24″ to 31⅞″ deep, go to [Content under creation] Four-post installation – racks 24- to 31⅞-inches deep
- For a 4-post installation for racks 30¼″ to 34⅜″ deep, go to [Content under creation] Four-post installation – racks 30¼- to 34⅜-inches deep

- For a 2-post installation, go to [Content under creation] Two-post installation

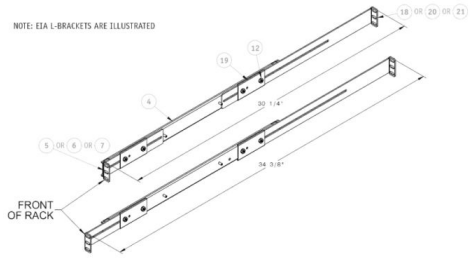
Four-post installation – racks under 24-inches deep

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.	L-bracket assembly (4 posts under 24-inches deep) 
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.	

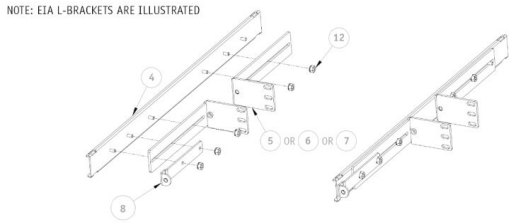
Four-post installation – racks 24- to 31⅞-inches deep

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.	L-bracket assembly using an extender kit (4-post racks 24″ to 31⅞″ deep) 
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 34⅜-inches deep

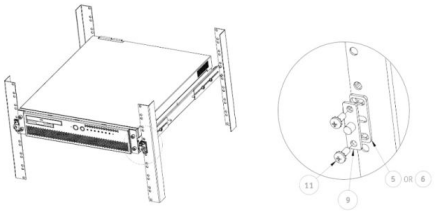
Step_1	Insert 1 L-bracket (item 5 for 19″ EIA, item 6 for 23″ EIA or item 7 for 23″ ETSI) and 1 extender L-bracket (item 18 for 19″ EIA, item 20 for 23″ EIA or item 21 for 23″ ETSI) on the threaded studs of an outer rail (item 4) as shown in the figure.	L-bracket assembly using an extender kit (4-post racks 30¼″ to 34⅜″ deep) 
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.	

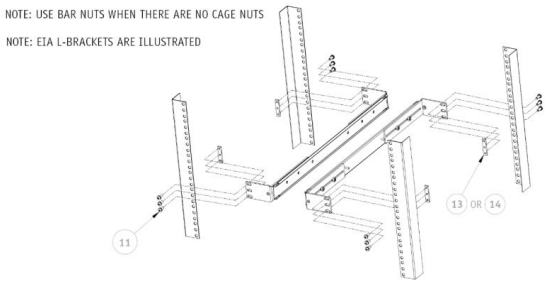
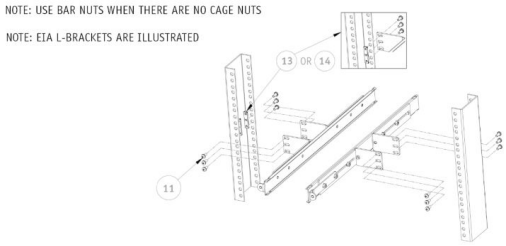
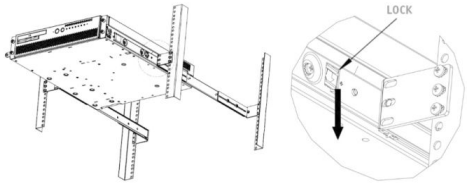
Two-post installation

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.	L-bracket assembly (2 posts) 
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.

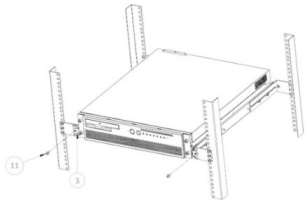
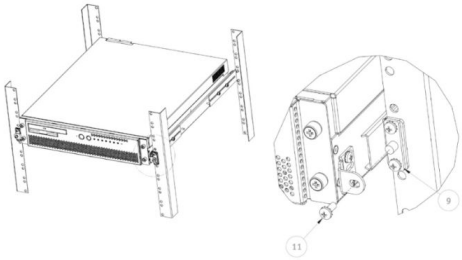


Step_1	Attach the outer rail assemblies (as built during the Building the outer rail assembly phase) to the rack using 8 or 12 screws (item 11). If the rack is designed to use cage nuts, no bar nuts will be required. If the rack has round holes, bar nuts (item 13 for EIA and item 14 for ETSI) should 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.	Outer rail assembly installation in a 4-post rack  Outer rail assembly installation in a 2-post rack 
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.	Lock release 

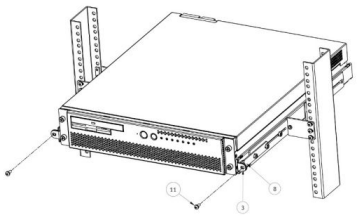
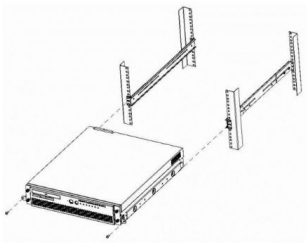
Securing the equipment

- 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

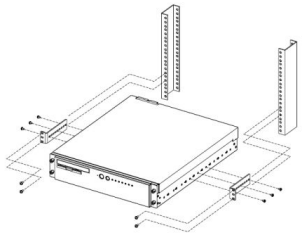
Securing the equipment to a 4-post rack

Step_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) 

Securing the equipment to a 2-post rack

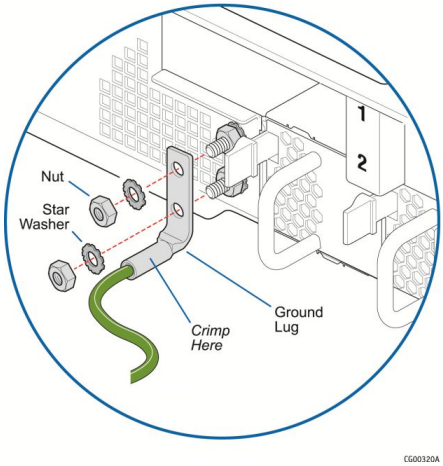
Step_1	Fasten each mounting ear (item 3) to a 2-post mounting bracket (item 8) using a total of 2 screws (item 11) as shown in the first figure.	 

Using TMLPMOUNT21

Step_1	Fasten each mounting bracket to the platform using a total of 3 screws as shown in the figure.	
Step_2	Fasten each mounting bracket to the rack using a total of 2 screws as shown in the figure.	

Earth grounding

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

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.	

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

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.

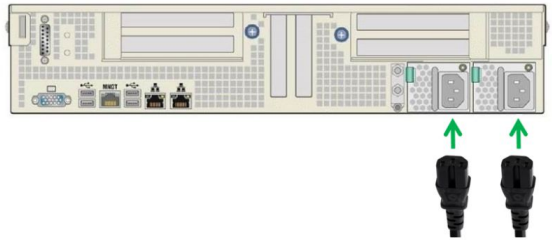
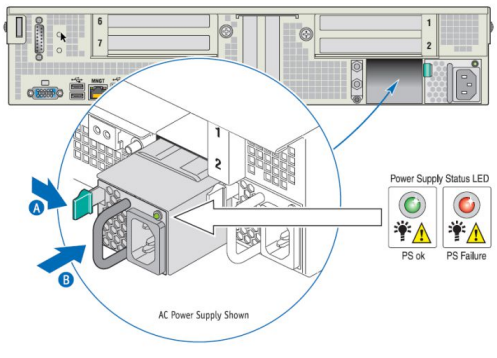
Power cord usage guidelines

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

Step_1	Connect appropriately rated cables from an external power source to each power supply on the rear of the platform.	
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.	

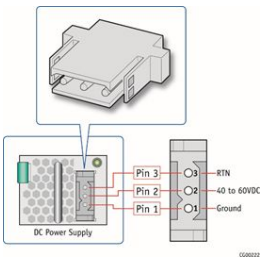
DC power supply

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.

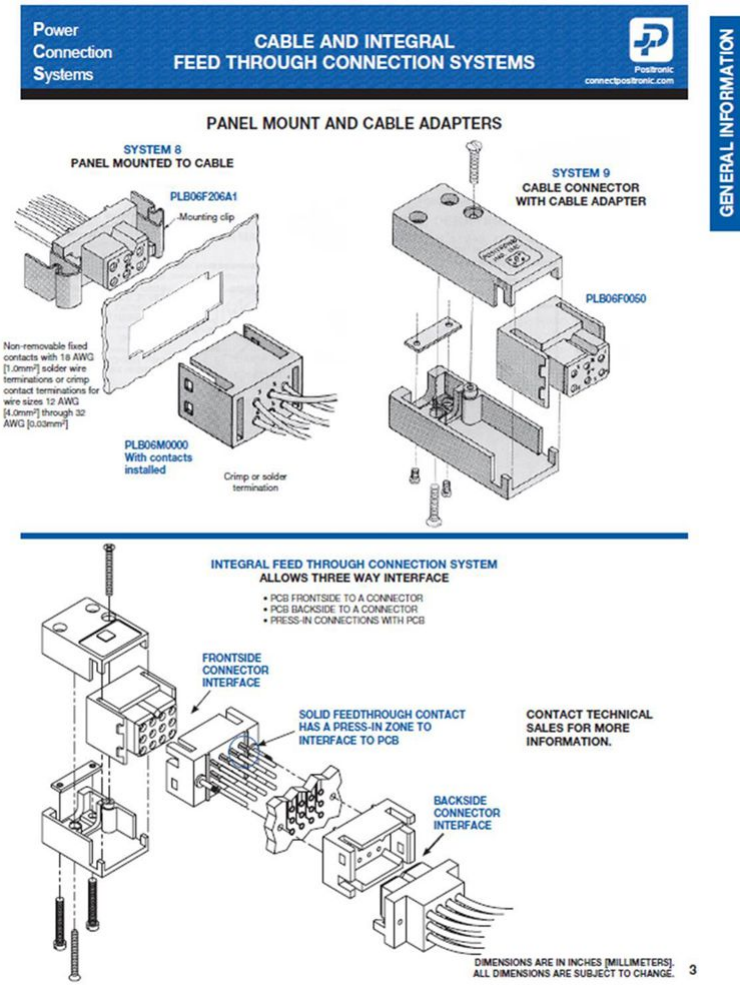
DC power supply input connector

- 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 Proccess



Building the power cables

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

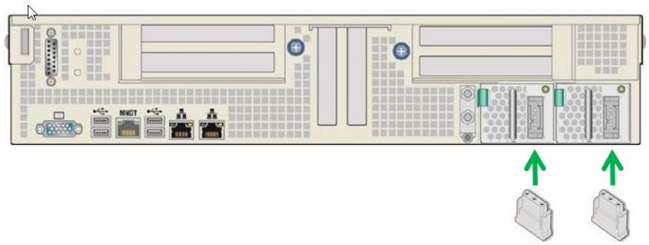
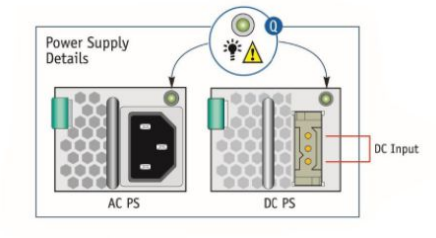
To build the power cables (ends that will be plugged in the CG2400), the material, tools and wires specified below are required.
NOTE: The other ends of the cables will need to be built according to national wiring codes and conform to local regulations in addition to your data center power installation requirements.

Description	Quantity	Manufacturer P/N	Link
Black stranded 12 AWG wire to build the power cable based on the length required	Length required		
Red stranded 12 AWG wire to build the power cable based on the length required	Length required		
Positronic DC power supply input mating connector (includes a strain relief assembly)	1 (provided with DC power supply module)	PLA03F7050/AA	• Positronic catalog
Positronic gauge-16 crimp terminal	3 (provided with DC power supply module)	FC112N2/AA-14	• Positronic catalog
Strain relief screw	2 (provided with DC power supply module)	Part of kit 1059-8642 Refer to [Content under creation] Platform, modules and accessories	
Strain relief plate	1 (provided with DC power supply module)	Part of kit 1059-8642 Refer to [Content under creation] Platform, modules and accessories	
Flat head Phillips screw	2 (provided with DC power supply module)	Part of kit 1059-8642 Refer to [Content under creation] Platform, modules and accessories	
DMC AF8 hand crimp tool	1	AF8	• DMC hand crimp tool catalog • DMC AF8 data sheet
Manual extraction tool	1	9081-0-0-0	• Molex extraction tool catalog • Application tooling specification sheet

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.}

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 on a server

{This article provides step-by-step OS installation instructions for all access paths.}

Table of contents

The operating system can be installed using the following methods:

- Using the [Content under creation] KVM
- Using [Content under creation] PXE (Boot from LAN)
- Using a [Content under creation] USB storage device

For a Legacy OS, refer to [Content under creation] Installing a legacy OS .

Installing an OS on a server using the KVM

Relevant section:

- Accessing a BMC

Prerequisites

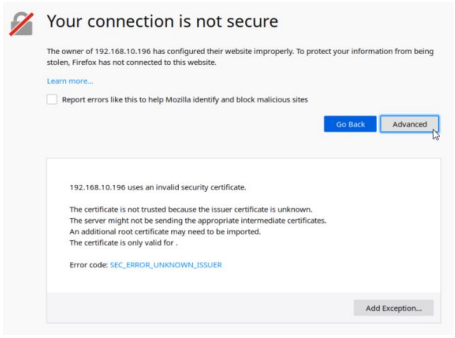
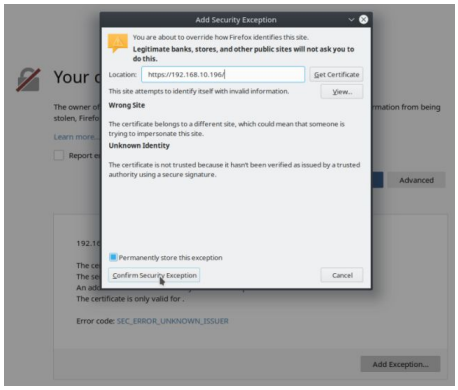
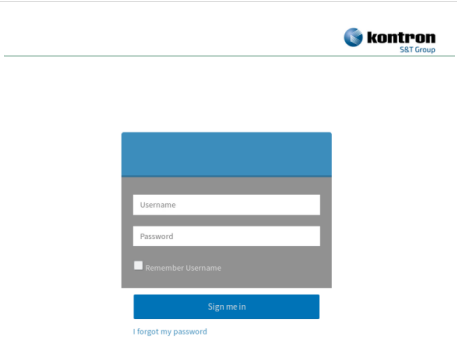
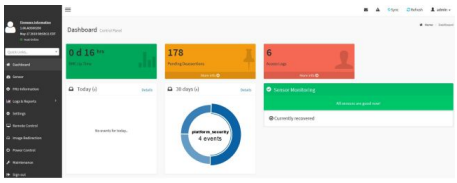
1	The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).
2	The remote computer has access to the management network subnet.

Browser considerations

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.

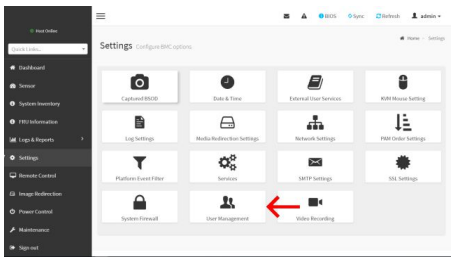
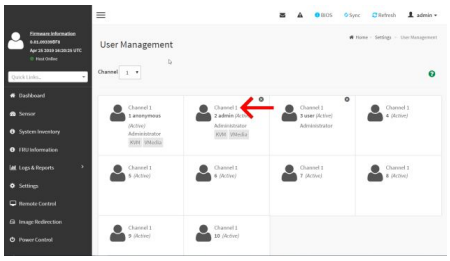
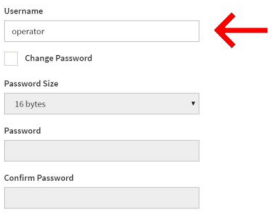
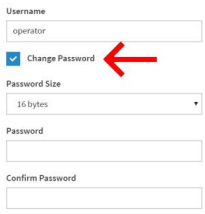
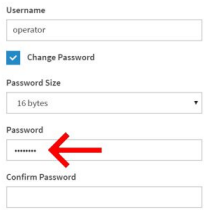
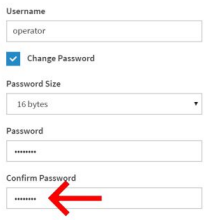
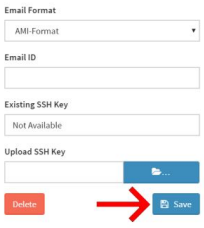
NOTE: The procedure may vary depending on the browser used. Examples provided use Firefox.

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 s tart 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.	

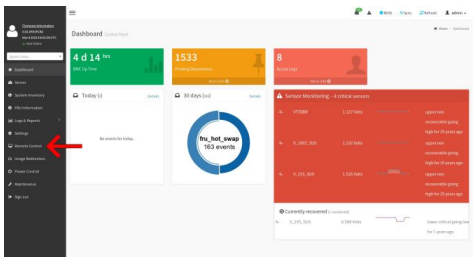
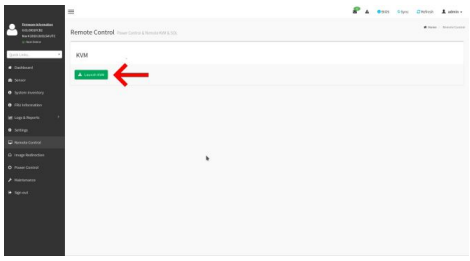
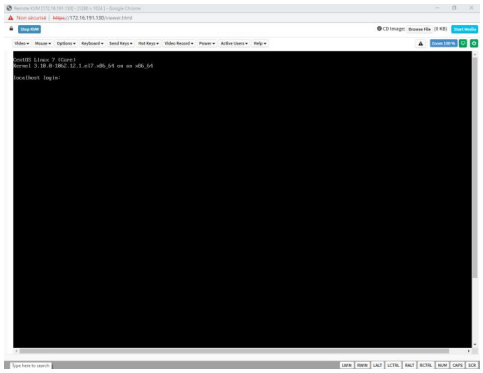
Changing the user name and password

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.**

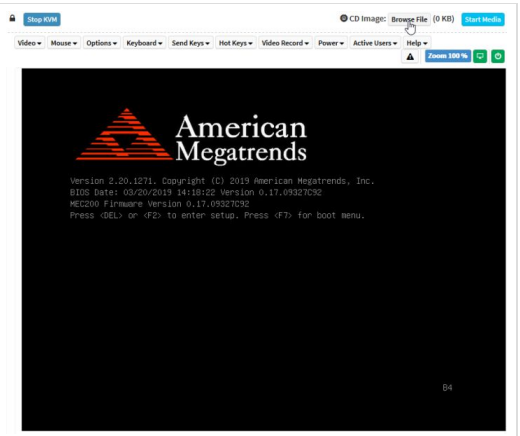
Step_1	Click on **Settings** in the left side menu and click on **User Management** .	
Step_2	Select the user to manage. **NOTE:** The first and second users are reserved fields, therefore, their usernames can't be modified.	
Step_3	Change field **Username** if required.	
Step_4	Check the **Change Password** 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

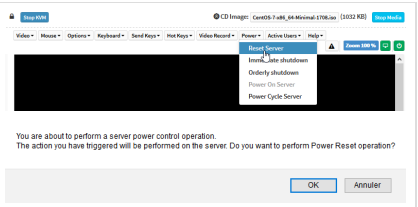
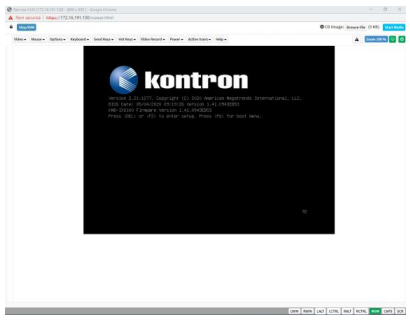
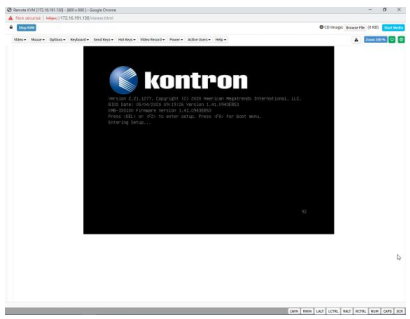
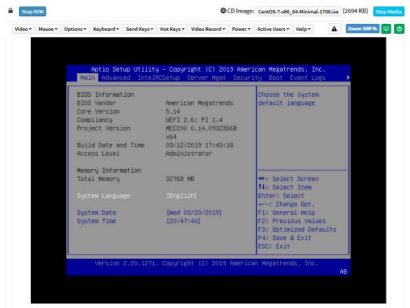
The Web UI allows remote control of the server through a KVM (Keyboard, Video, Mouse) interface.

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.	

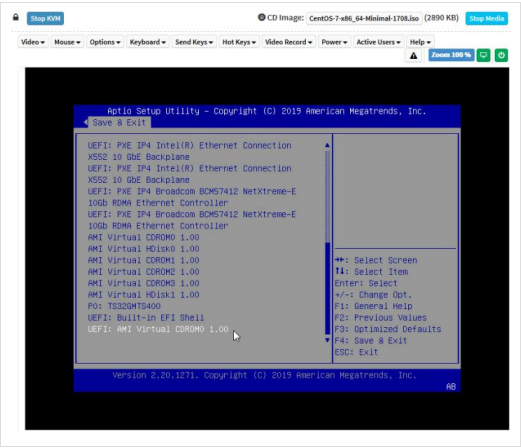
Mounting the operating system image via virtual media

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_1	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

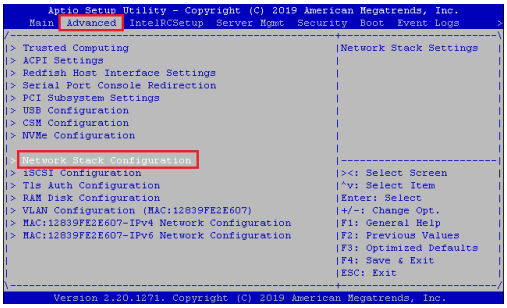
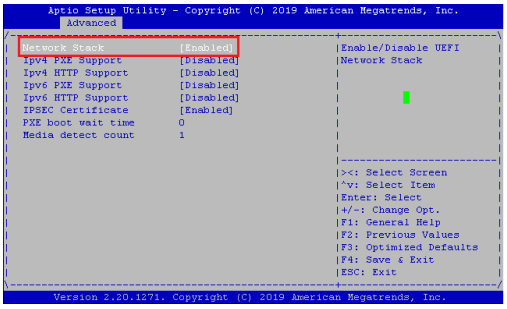
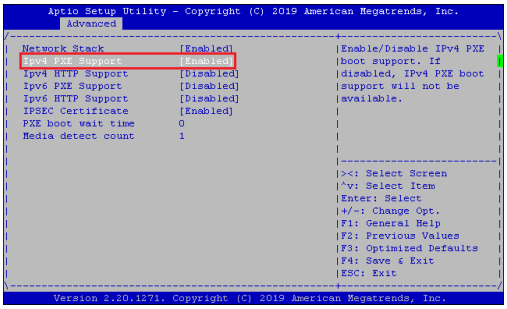
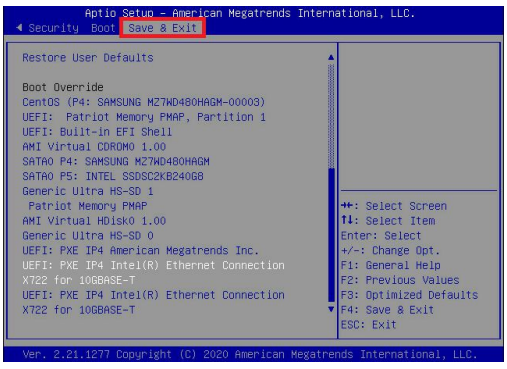
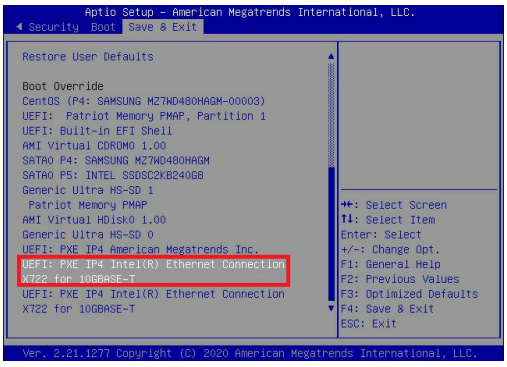
Step_1	Complete the installation by following the on-screen prompts of the specific OS installed.

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

Relevant section:

- Accessing the BIOS

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.

Completing operating system installation

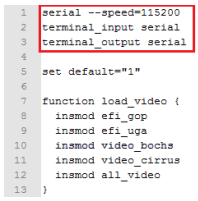
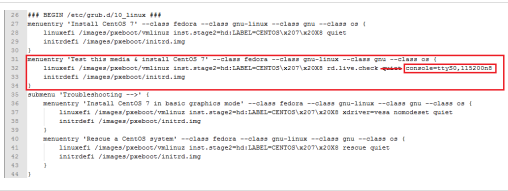
Step_1	Complete the installation by following the on-screen prompts of the specific OS installed.

Installing an OS on a server using a USB storage device

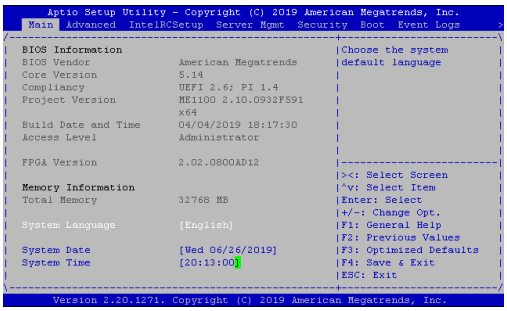
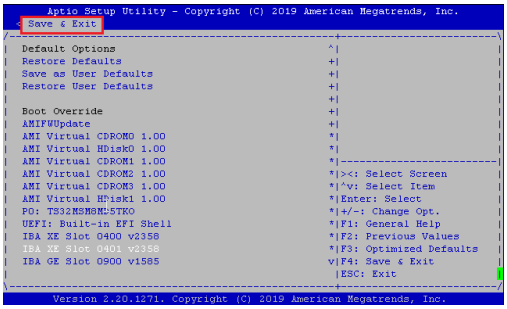
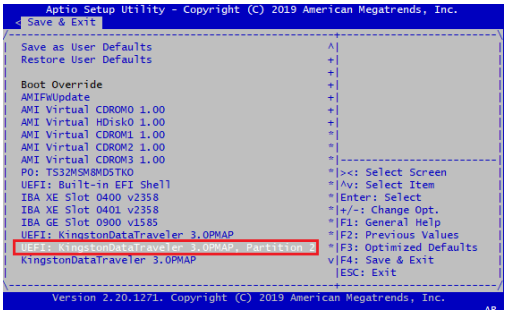
Relevant sections:

- Accessing the BIOS
- Platform power management

Preparing the USB storage device

Step_1	Create a bootable USB key using the appropriate software. **NOTE:** RUFUS is recommended	
Step_2	Open the USB directory in a remote computer.	
Step_3	Navigate to EFI then BOOT (e.g: E:/EFI/BOOT/).	
Step_4	Open the grub.cfg file with any text editor.	
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*	
Step_6	In the " ***Test this media & install CentOS 7*** " entry replace the " ***quiet*** " argument with " ***console=ttyS0,115200n81*** ".	
Step_7	Save the file and eject the USB key.	

Configuring Boot Override

Step_1	Connect the USB storage device on the platform.	
Step_2	Power on the platform. Refer to Platform power management.	
Step_3	Access the BIOS setup menu. Refer to Accessing the BIOS.	
Step_4	Navigate to the **Save & Exit** menu and then to the **Boot Override** section.	
Step_5	Choose your USB storage device. **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

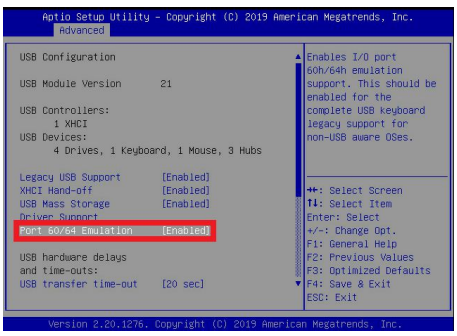
Installing RHEL/CentOS 7.3 and preparing for AST driver installation

Prerequisites

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

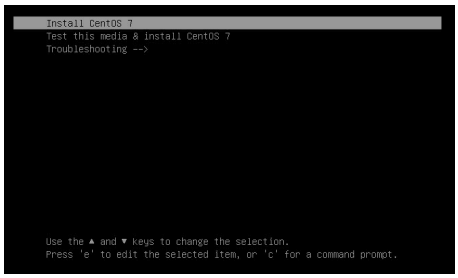
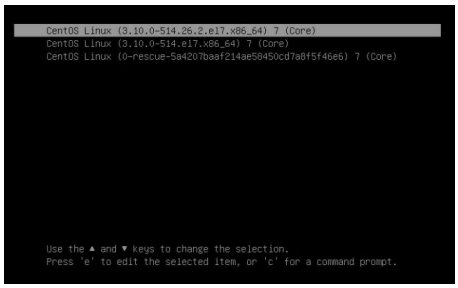
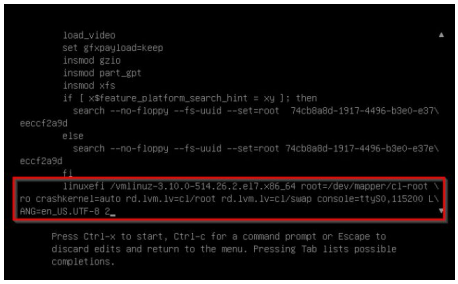
Enabling the USB keyboard for use in the boot loader in Legacy

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.	

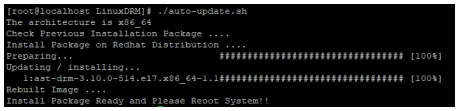
Installing RHEL/CentOS 7.3 and preparing for AST driver installation

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 **OR** • (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 show in the image. The parameter is inserted before the quiet parameter at the end of linuxefi line.	
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.	

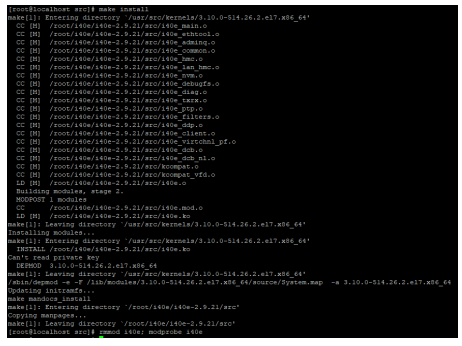
Installing the AST driver

Relevant links:
The driver package can be downloaded from: https://www.aspeedtech.com/support.php
The AST driver package version used in this procedure is: http://upload.aspeedtech.com/BIOS/v11003_linux.zip

Step_1	From a remote computer that has access to the server OS (through SSH, RDP, etc) , e nter the command to download and copy the package. LocalServer_OSPrompt:~# **wget** https://downloadmirror.intel.com/29072/eng/ASPEED_v11003_linux.zip	
Step_2	Extract the content. LocalServer_OSPrompt:~# **unzip ASPEED_v11003_linux.zip**	
Step_3	Change directory. LocalServer_OSPrompt:~# **cd LinuxDRM/**	
Step_4	Extract the content. LocalServer_OSPrompt:~# **tar xvzf lxdrm.tar.gz**	
Step_5	Install the driver. LocalServer_OSPrompt:~# **./auto-update.sh**	
Step_6	Reboot the platform. LocalServer_OSPrompt:~# **reboot**	
Step_7	(Optional) If your kernel version is different than 3.10.0-514.el7.x86_64, you may get this error: *The kernel version is not in RPMs support list, Please try SRPMS instead!!* This is caused by the output of uname -r, it does not match at 100% the file name structure of the AST driver. You can change the script or the filename. LocalServer_OSPrompt:~# **uname -r** 3.10.0-514.26.2.el7.x86_64 LocalServer_OSPrompt:~# **sed -e "s/kver=\`uname -r\`/kver=\`uname -r | sed 's\/26.2.\/\/'\`/" ./auto-update.sh**	
Step_8	(Optional) After updating the auto-update file with your kernel, you can perform the update. LocalServer_OSPrompt:~# **./auto-update.sh**	

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. LocalServer_OSPrompt:~# **wget -nc --random-file /root/.bashrc --content-disposition** http://sourceforge.net/projects/e1000/files/i40e%20stable/2.9.21/i40e-2.9.21.tar.gz/download	
Step_2	Extract the content of the tar file. LocalServer_OSPrompt:~# **tar xvzf 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

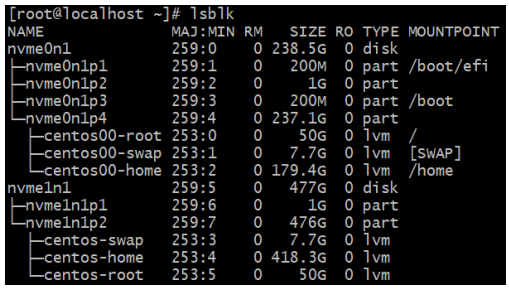
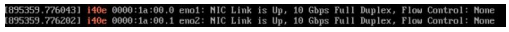
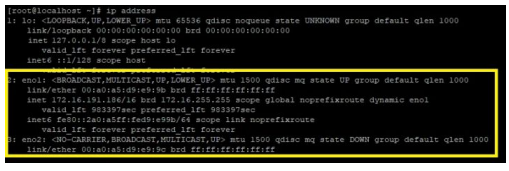
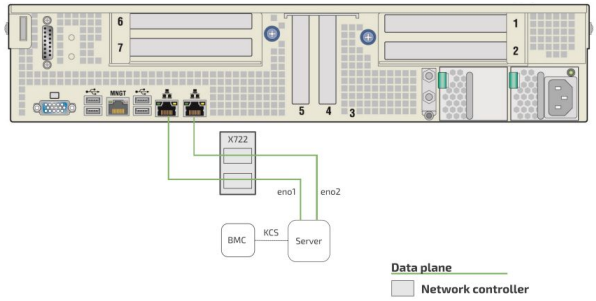
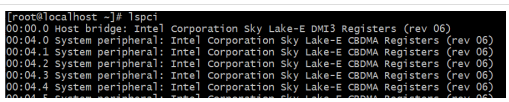
Step_1	If you have no local vault/repository available and you need to prevent yum from installing/upgrading the latest kernel version. **#! /bin/bash** **mkdir /etc/yum.repos.d/.disabled** **mv /etc/yum.repos.d/CentOS-Base.repo /etc/yum.repos.d/.disabled/** **cat <<EOT >> /etc/yum.repos.d/CentOS-7.3.repo** **[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

i	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.	00:04.6 System peripheral: Intel Corporation Sky Lake-E CBDMA Registers (rev 06) 00:04.7 System peripheral: Intel Corporation Sky Lake-E CBDMA Registers (rev 06)
Step_10	Verify communication between the operating system and the BMC. LocalServer_OSPrompt:~# **ipmitool mc info**	LocalServer_OSPrompt:~# ipmitool mc info Device ID : 32 Device Revision : 1 Firmware Revision : 0.01 IPMI Version : 2.0 Manufacturer ID : 15000 Manufacturer Name : Kontron Product ID : 1100 (0x044c) Product Name : Unknown (0x44C) Device Available : yes Provides Device SDRs : no Additional Device Support : Sensor Device SDR Repository Device SEL Device FRU Inventory Device IPMB Event Receiver IPMB Event Generator Chassis Device Aux Firmware Rev Info 0x09 0x33 0x9b 0xf8

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

	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

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

Recommended software tools

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

Product specific software tools

Tool	Description	Installation
StorCLI	Configuration and monitoring tool for HW RAID configurations running on LSI Raid-On-Chip controller.	Refer to StorCLI utility
net-snmp-utils	SNMP utility package.	From a command prompt: LocalServer_OSPrompt:~# **yum install wget unzip net-snmp-utils net-snmp**

Configuring

{This section provides all the information related to the platform's configurations: system access, platform management, baseboard management, network infrastructure, switch, parallel configuration and redundancies. }

Children

- Configuration of system access methods
- Configuring and managing users
- Baseboard management controller - BMC
- Configuring the network time protocol - NTP
- Basic BIOS option configuration
- Customizing platform data
- Network infrastructure integration
- [Content under creation] High availability
- Configuring the BMC when in non-redundant PSU configuration

Configuration of system access methods

{This article provides detailed setup instructions to enable system access for all available methods.}

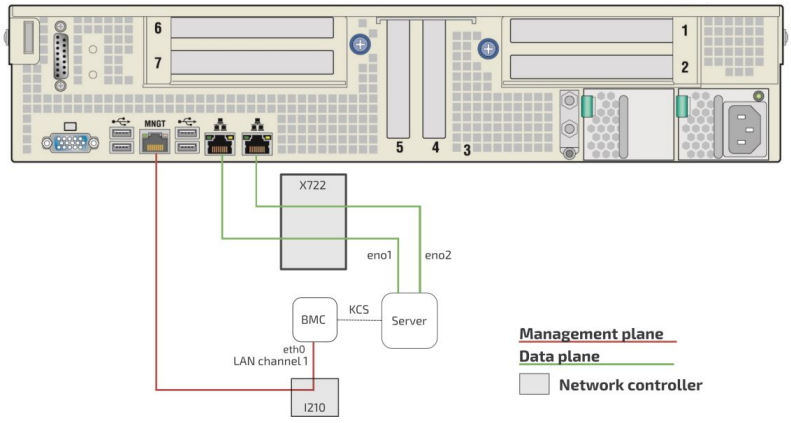
Table of contents

General considerations and warnings about network configuration

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 [Content under creation] 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 I P address known or not), IPMI via KCS can be used. R efer to [Content under creation] 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 [Content under creation] Accessing a BMC using IPMI over LAN (IOL) .

The following procedures will be executed using the [Content under creation] 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.

Step_1	Disable the LAN access. LocalServer_OSPrompt:~# **ipmitool lan set [LAN_CHANNEL] access off**	

Enabling 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 enabled:

- Using [Content under creation] 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 I P address known or not), IPMI via KCS can be used. R efer to [Content under creation] 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 [Content under creation] Accessing a BMC using IPMI over LAN (IOL) .

The following procedures will be executed using the [Content under creation] 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.

Step_1	Enable the LAN access. LocalServer_OSPrompt:~# **ipmitool lan set [LAN_CHANNEL] access on**	

Configuring Serial over LAN parameters using IPMI

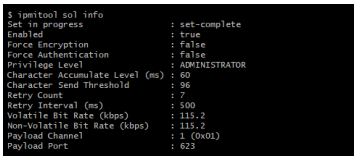
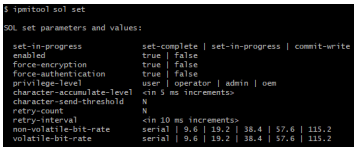
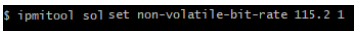
Accessing the BMC

The BMC can be accessed using two IPMI methods.

- If an OS is installed (BMC I P address known or not), IPMI via KCS can be used. R efer to [Content under creation] 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 [Content under creation] Accessing a BMC using IPMI over LAN (IOL) .

The following procedures will be executed using the [Content under creation] 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

Step_1	Display SOL parameters. LocalServer_OSPrompt:~# **ipmitool sol info**	
Step_2	Display SOL parameters available for configuration. LocalServer_OSPrompt:~# **ipmitool sol set**	
Step_3	Set the desired parameters. LocalServer_OSPrompt:~# **ipmitool sol set [PARAMETER] [PARAMETER_VALUE] [LAN_CHANNEL]**	

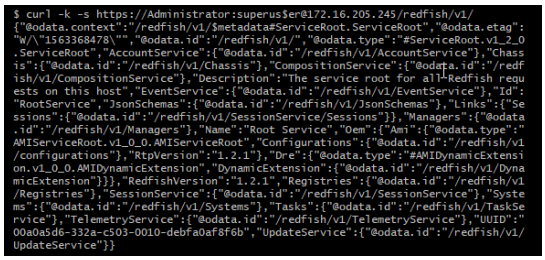
Creating the Redfish root URL

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 parsor command-line tool such as **jq** is installed.

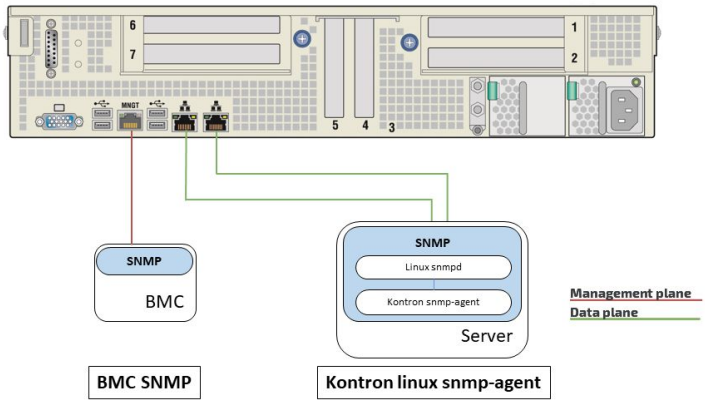
Relevant sections:
Baseboard management controller - BMC
Common software installation
Default user names and passwords

Procedure

Step_1	Begin URL with the **https** prefix.	https://
Step_2	Add the Redfish username and password separated by a colon.	https://Administrator:superuser
Step_3	Add **@** to the URL followed by the BMC management IP address.	https://Administrator:superuser@172.16.205.245
Step_4	Add the Redfish API suffix to the URL.	https://Administrator:superuser@172.16.205.245/redfish/v1/
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



Configuring BMC SNMP

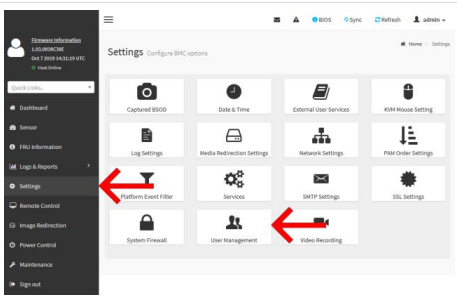
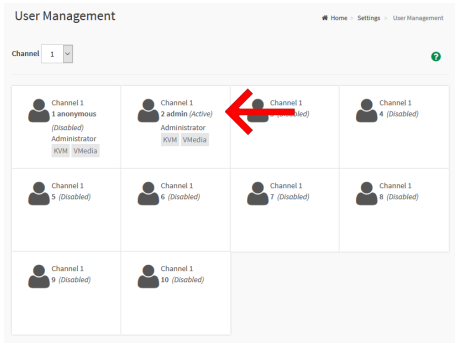
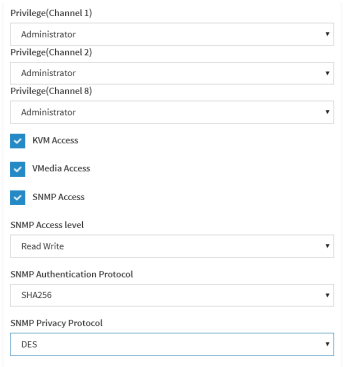
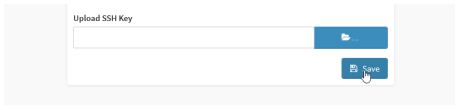
Before configuring SNMP, the default user name and password must be changed as a minimum of 8 characters are required for both. Refer to Configuring BMC user names and passwords using the Web UI .

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

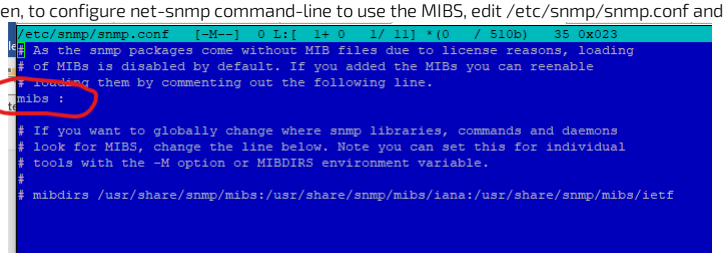
Relevant section:
Configuring and managing users

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 Authentification Protocol** .	
Step_6	Choose the **SNMP Privacy Protocol** .	
Step_7	Click on **Save** .	

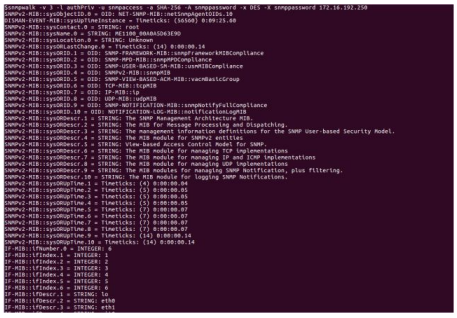
Installing SNMP on a remote computer

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: 

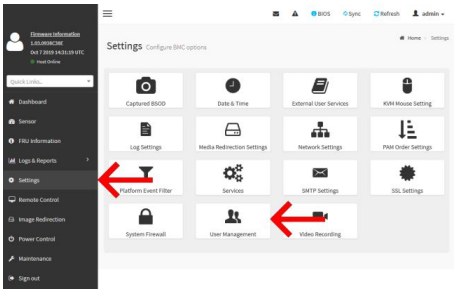
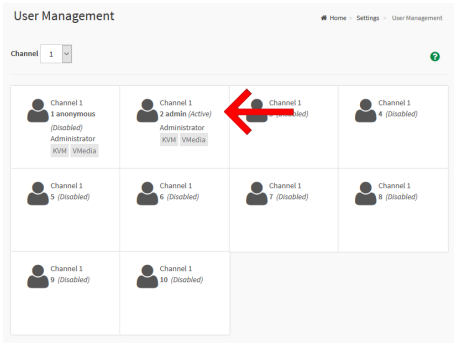
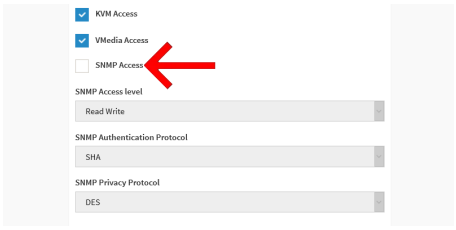
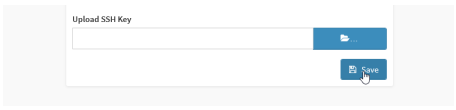
```
/etc/snmp/snmp.conf   [-M--]  0 L:[  1+ 0   1/ 11] *(0    / 510b)   35 0x023
# As the snmp packages come without MIB files due to license reasons, loading
# of MIBs is disabled by default. If you added the MIBs you can reenable
# loading them by commenting out the following line.
mibs :

# If you want to globally change where snmp libraries, commands and daemons
# look for MIBS, change the line below. Note you can set this for individual
# tools with the -M option or MIBDIRS environment variable.
#
# mibdirs /usr/share/snmp/mibs:/usr/share/snmp/mibs/iana:/usr/share/snmp/mibs/ietf
```

Verifying SNMP communication for a user

Step_1	From a remote computer that has access to the management network subnet, v erify that the BMC properly responds to the SNMP request. RemoteComputer_OSPrompt:~# **snmpwalk -v 3 -l [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [SNMP_PASSWORD] -x [PRIVACY_PROTOCOL] -X [SNMP_PASSWORD] [BMC MNGMT_IP]**	

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.

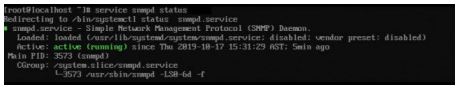
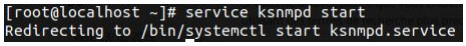
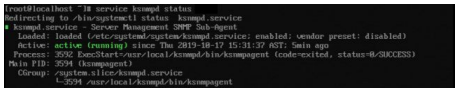
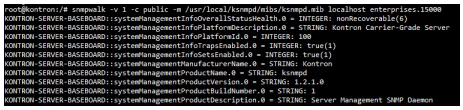
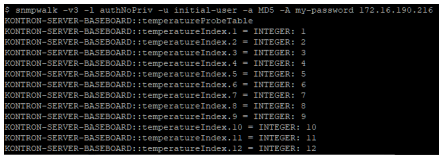
Step_1	Install the SNMP agent provided by Kontron. LocalServer_OSPrompt:~# **yum install ./ kontron-snmp-agent-1.2.2-1.x86_64.rpm**
Step_2	Install the net-snmp-utils tool. LocalServer_OSPrompt:~# **yum install net-snmp-utils**

Configuring Kontron linux snmp-agent

i	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.

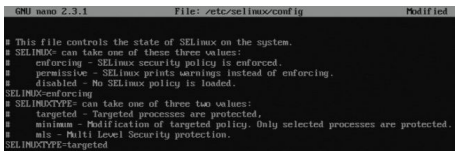
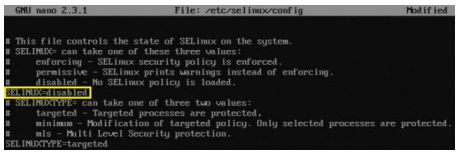
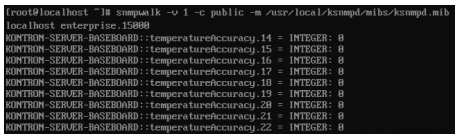
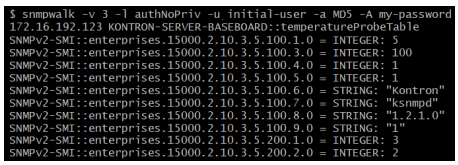
Step_1	Save the current configuration. LocalServer_OSPrompt:~# **mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bak**	
Step_2	Create file snmpd.conf using the following command: LocalServer_OSPrompt:~# **nano /etc/snmp/snmpd.conf** The nano editor will open. Copy the following text in it: **rwcommunity public** **# Need to define default master agentx socket if net-snmp >=5.4** **agentXSocket tcp:localhost:1705** **# turn on agentx master agent support** **master agentx** **# Enable TRAPs** **trap2sink localhost public** **authtrapenable 1**	
Step_3	Set default credentials. LocalServer_OSPrompt:~# **/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_OSPrompt:~# **service snmpd start**	
Step_2	Verify that snmpd is running properly. LocalServer_OSPrompt:~# **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 [Content under creation] Disabling SELinux for further instructions.	
Step_4	Run ksnmpd. LocalServer_OSPrompt:~# **service ksnmpd start**	
Step_5	Verify that ksnmpd is running properly. LocalServer_OSPrompt:~# **service ksnmpd status**	
Step_6	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_7	From a remote computer having access to the server network, verify that the server responds to the SNMP request properly. RemoteComputer_OSPrompt:~# **snmpwalk -v3 -l [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [PASSWORD] [SERVER_IP] [ODI]**	

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. RemoteComputer_OSPrompt:~# **snmpwalk -v3 -l [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [PASSWORD] [SERVER_IP] [ODI]**	

Configuring and managing users

{This article provides detailed configuration instructions for platform users.}

Table of contents

Configuring BMC users

	Administrator rights are required to manage users.

Configu ring BMC user names and passwords

For default user names and passwords, refer to Default user names and passwords .

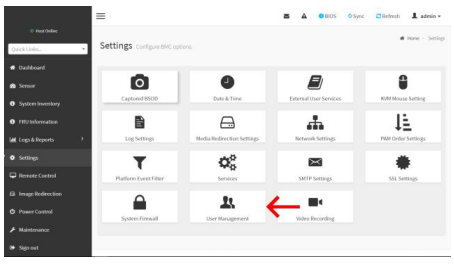
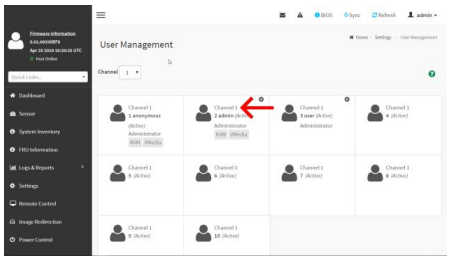
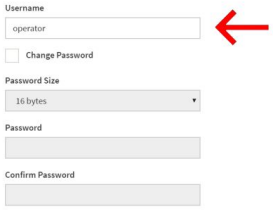
BMC user names an d passwords can be managed:

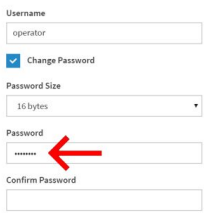
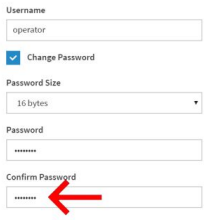
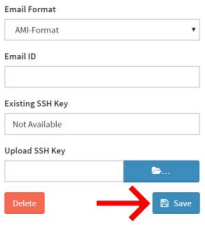
- Using the [Content under creation] Web UI
- Using [Content under creation] IPMI over LAN (IOL)
- Using [Content under creation] IPMI via KCS

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.

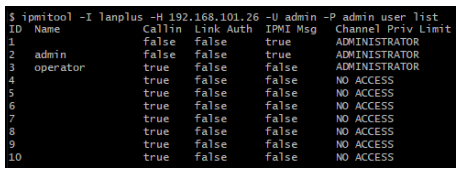
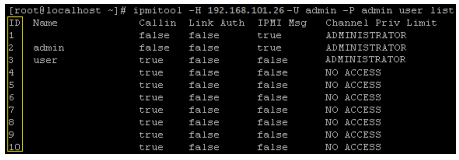
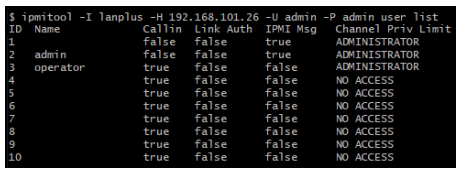
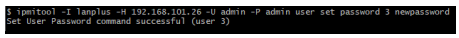
Step_1	Click on **Settings** in the left side menu and click on **User Management** .	
Step_2	Select the user to manage. **NOTE:** The first and second users are reserved fields, therefore, their usernames can't be modified.	
Step_3	Change field **Username** if required.	
Step_4	Check the **Change Password** box.	

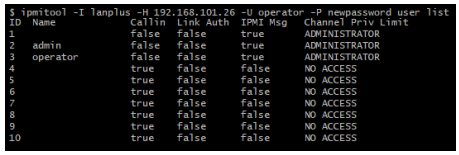
		
Step_5	Create a new password. **NOTE:** It is recommended, but not mandatory, to enter a strong password consisting of at least one upper case letter, alpha-numeric character, and special character. **You MUST avoid symbols from the extended ASCII table as they are not managed by the IPMI tool.** Please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

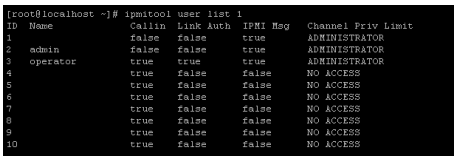
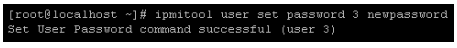
Step_1	From a remote computer that has access to the management network subnet, print the BMC user list. RemoteComputer_OSPrompt:~$ **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user list**	
Step_2	Identify the ID number of the user to be changed.	
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. RemoteComputer_OSPrompt:~$ **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user list**	
Step_5	Change the password. RemoteComputer_OSPrompt:~$ **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administratorIPMI user name] -P [administrator IPMI password] user set password [IPMI user ID] [new IPMI 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	Enable the user. RemoteComputer_OSPrompt:~$ **ipmitool user enable [IPMI user ID]**	
Step_7	Configure privilege level. RemoteComputer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] channel setaccess [LAN_CHANNEL] [USER_ID] privilege= [PRIVILEGE_LEVEL]**	
Step_8	Verify that credentials updated correctly by using any **ipmitool** command. RemoteComputer_OSPrompt:~$ **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [new IPMI user name] -P [new IPMI password] [IPMI command]** **NOTE:** Other parameters could limit the accessibility of the user that is trying to manage the BMC. Refer to **ipmitool** documentation for further information.	

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.

Step_1	From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, print the BMC user list. LocalServer_OSPrompt:~# **ipmitool user list [LAN_CHANNEL]**	
Step_2	Identify the ID number of the user to be changed.	
Step_3	Change the 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_4	Verify that the user name has updated correctly by printing the user list. LocalServer_OSPrompt:~# **ipmitool user list [LAN_CHANNEL]**	
Step_5	Change the password. LocalServer_OSPrompt: ~# **ipmitool user set password [IPMI user ID] [new IPMI password]**	
Step_6	Verify that the credentials updated correctly by using an access method that requires a login. **NOTE:** Other parameters could limit the accessibility of the user that is trying to manage the BMC. Refer to ipmitool documentation.	

Adding a BMC user

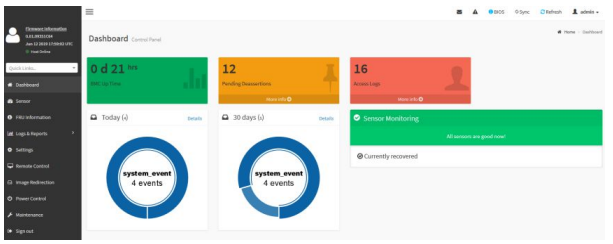
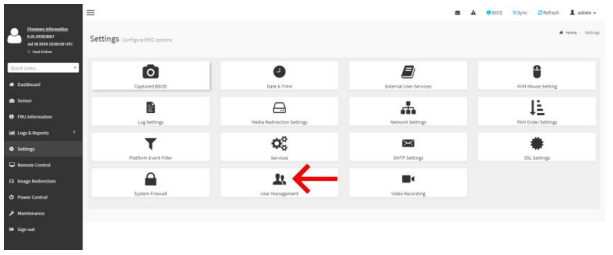
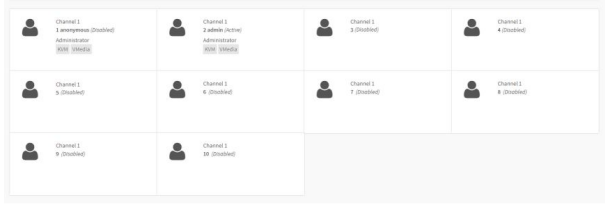
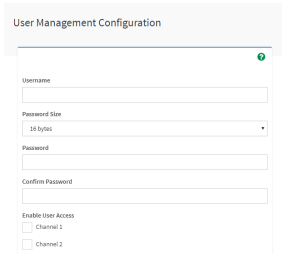
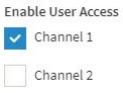
BMC users can be added :

- Using the [Content under creation] Web UI
- Using [Content under creation] IPMI over LAN (IOL)
- Using [Content under creation] 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.**

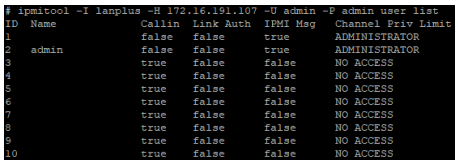
Refer to Accessing a BMC using the Web UI for access instructions.

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 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.	

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.

Step_1	From a remote computer that has access to the management network subnet, p rint the list of users and select the ID of the user to add. RemoteServer_ OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user list**	
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.	

	RemoteServer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user set password [IPMI user ID] [new IPMI password]**
Step_4	Enable channel access and configure privilege level. RemoteServer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] channel setaccess [LAN_CHANNEL] [USER_ID] privilege=[PRIVILEGE_LEVEL]**
Step_5	Enable the user. RemoteServer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user enable [USER_ID]**

Adding a BMC user 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 (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, p rint the list of users and select the ID of the user to add. LocalServer_ OSPrompt:~# **ipmitool user li st [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]**	

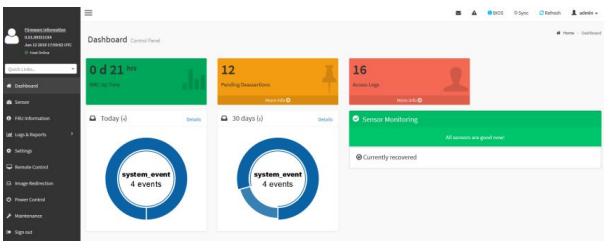
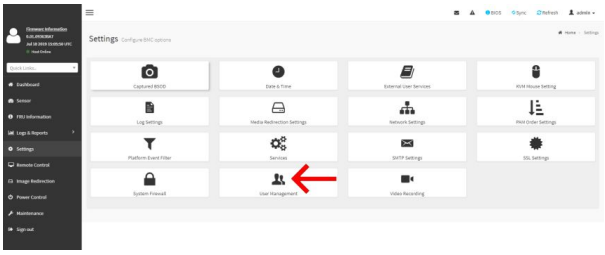
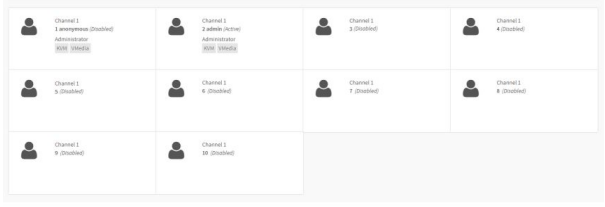
Deleting or disabling a BMC user

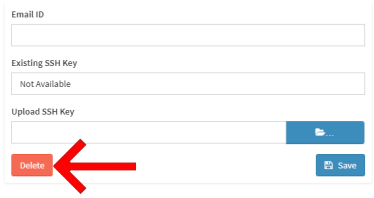
BMC users can be :

- Deleted using the [Content under creation] Web UI
- Disabled using [Content under creation] IPMI over LAN (IOL)
- Disabled using [Content under creation] IPMI via KCS

Deleting a BMC user using the Web UI

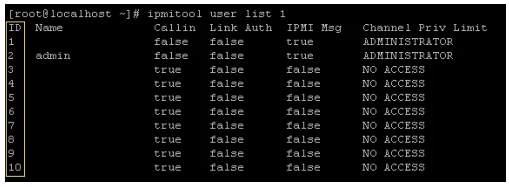
Refer to Accessing a BMC using the Web UI for access instructions.

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.	

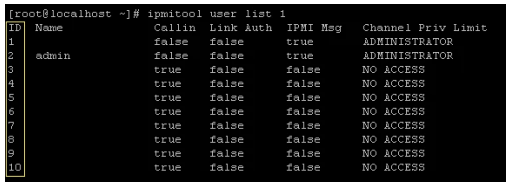
Disabling a BMC user using IPMI over LAN (IOL)

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, p rint the list of users and select the ID of the user to disable. RemoteServer_ OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user list**	
Step_2	Disable the selected user. RemoteServer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user disable [USER_ID]** **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.	

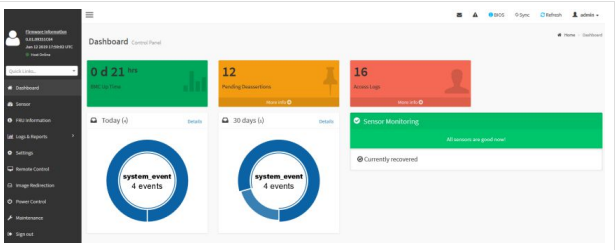
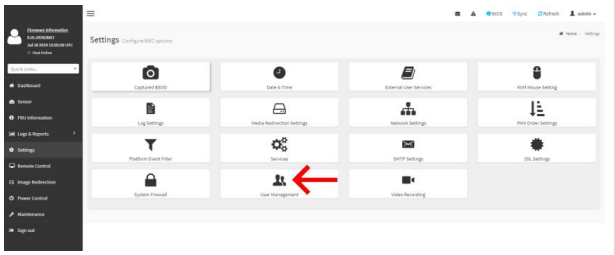
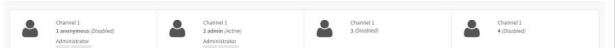
Configuring privilege level for BMC users

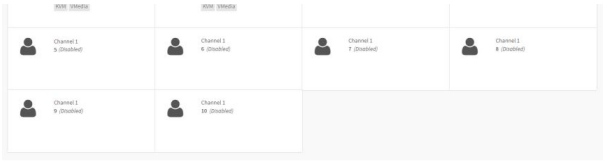
BMC user privilege level can be configured :

- Using the [Content under creation] Web UI
- Using [Content under creation] IPMI over LAN (IOL)
- Using [Content under creation] 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.	
Step_5	Press on **Save** to exit.	

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, p rint the list of users and select the ID of the user to manage. RemoteComputer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] user list**	
Step_2	List available privilege levels. RemoteComputer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] channel help**	
Step_3	Set privilege level for each channel. RemoteComputer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [administrator IPMI user name] -P [administrator IPMI password] 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 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, p rint 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.	

Co nfiguring 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.

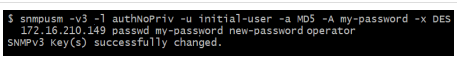
- To configure a user, refer to [Content under creation] Configuring BMC users .
- To enable or disable SNMP access, refer to [Content under creation] Configuring SNMP BMC .

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.

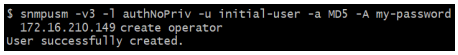
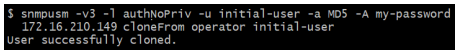
Configuring SNMP passwords

Refer to Accessing a BMC using the Kontron linux snmp-agent for access instructions.

Step_1	From a remote computer that has access to the management network subnet, c hange the password. RemoteComputer_OSPrompt:~# **snmpusm -v3 -l [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [PASSWORD] -x [PRIVACY_PROTOCOL] [SERVER_IP] passwd [OLD_PASSWORD] [NEW_PASSWORD] [USER]**	

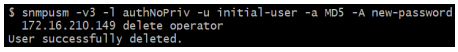
Adding an SNMP user

Refer to Accessing a BMC using the Kontron linux snmp-agent for access instructions.

Step_1	From a remote computer that has access to the management network subnet, c reate an SNMP user. RemoteComputer_OSPrompt:~# **snmpusm -v3 -l [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [PASSWORD] [SERVER_IP] create [NEW_USER]**	
Step_2	To initialise the user created, clone its configurations from another existing user. RemoteComputer_OSPrompt:~# **snmpusm -v3 -l [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [PASSWORD] [SERVER_IP] cloneFrom [NEW_USER] [CLONE_FROM_USER]**	

Deleting an SNMP user

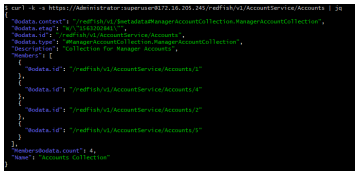
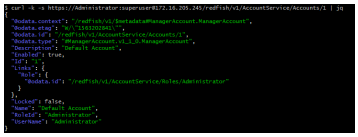
Refer to Accessing a BMC using the Kontron linux snmp-agent for access instructions.

Step_1	From a remote computer that has access to the management network subnet, delete an SNMP user. RemoteComputer_OSPrompt:~# **snmpusm -v3 -l [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [PASSWORD] [SERVER_IP] delete [USER]**	

Managing Redfish users

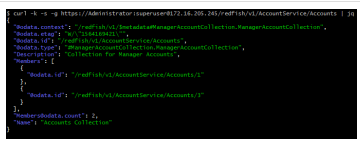
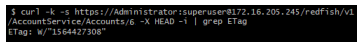
Configuring Redfish user names and passwords

Refer to Accessing a BMC using Redfish for access instructions.

Step_1	Print the user list and select the ID of the user to modify. RemoteComputer_OSPrompt:~$ **curl -k -s [ROOT_URL]/AccountService/Accounts | jq**	
Step_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**	
Step_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**	
Step_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.	
Step_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**	
Step_6	Change the password if necessary. RemoteComputer_OSPrompt:~$ **curl -k -s [ROOT_URL]/AccountService/Accounts/[USER_ID] -X PATCH -d '{"Password":"[NEW_PASSWORD]"}' -H 'If-Match: [ETAG_VALUE]' -H 'Content-type: application/json' | jq** **NOTE:** Once the password is modified, it needs to be updated in the ROOT_URL.	
Step_7	Verify that the credentials updated correctly by opening a new session in the Redfish API.	

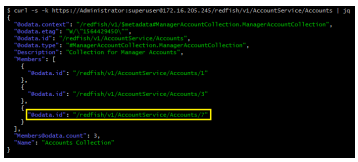
Adding a Redfish user

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

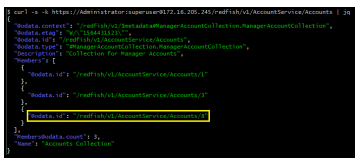
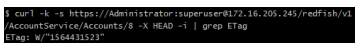
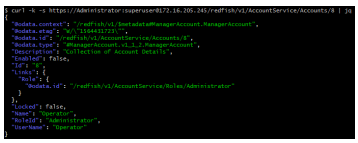
Refer to Accessing a BMC using Redfish for access instructions.

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.

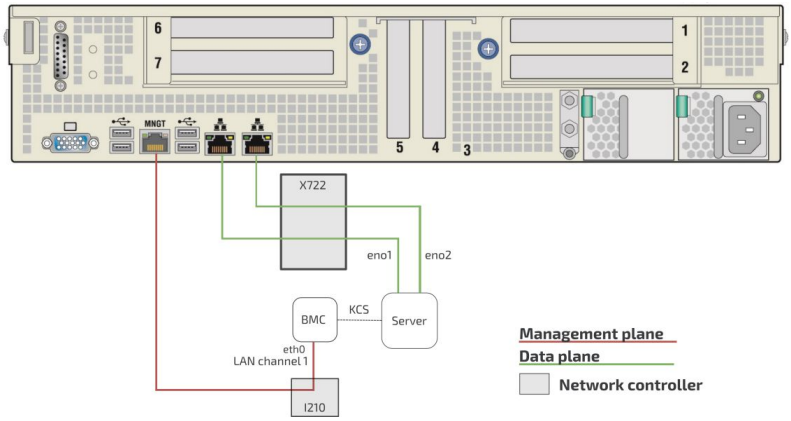
Step_1	Access the OS using the preferred method.
Step_2	Configure the users as recommended by the OS documentation. **NOTE:** The procedure to change OS credentials is application-specific and therefore not further documented.

Baseboard management controller - BMC

{This article provides detailed setup instructions for all BMC configuration methods.}

Table of contents

BMC architecture



- 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 [Content under creation] DHCP Dynamic DNS update
- Using the [Content under creation] BIOS [Content under creation] via the VGA display port or a serial console (physical connection) – device with no OS installed and no known IP address
- Using the [Content under creation] 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 server 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.

Step_1	Ping the host name. RemoteComputer_OSPrompt:~$ **ping [BOARD_NAME]_00A0A5D2E90A**	Pinging BOARD_NAME_00A0A5D2E90A[172.16.211.126] with 32 bytes of data: Reply from 172.16.211.126: bytes=32 time<1ms TTL=60 Reply from 172.16.211.126: bytes=32 time<1ms TTL=60 Reply from 172.16.211.126: bytes=32 time=1ms TTL=60 Reply from 172.16.211.126: bytes=32 time<1ms TTL=60 Ping statistics for 172.16.211.126: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms

Discovering the platform management IP address using the BIOS

The platform management IP address can be discovered in the BIOS:

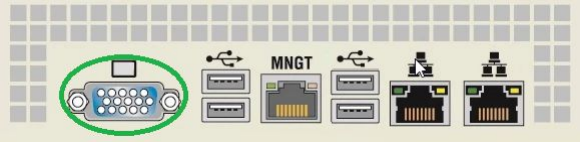
- Using the [Content under creation] VGA display port (physical connection)
- Using a serial console (physical connection)

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

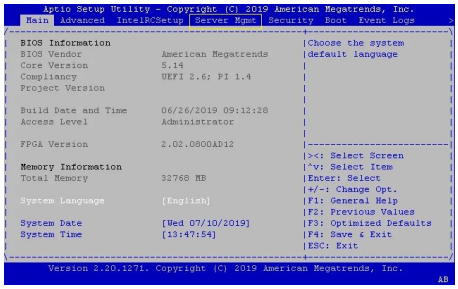
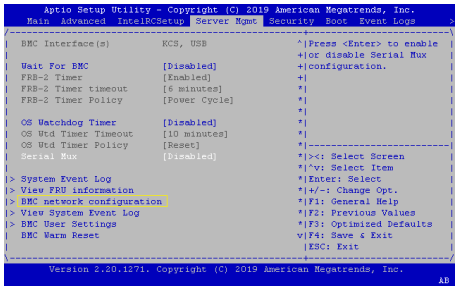
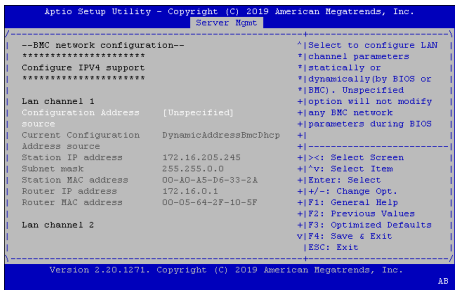
Prerequisites

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

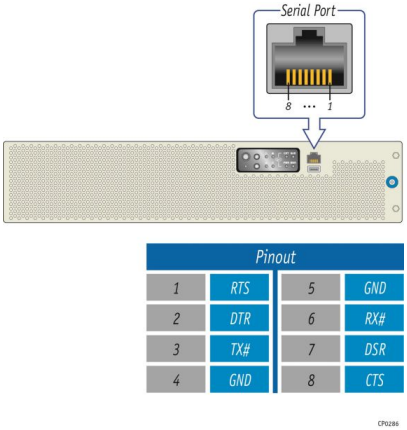
Step_1	From the UEFI/BIOS menu, navigate to tab **Server Mgmt** .	
Step_2	Select **BMC network configuration** .	
Step_3	The **BMC network configuration** menu is displayed. **NOTE:** When the platform is powered up after being shut off, the UEFI/BIOS may load before the BMC has received its IP address. 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 s erial console (physical connection)

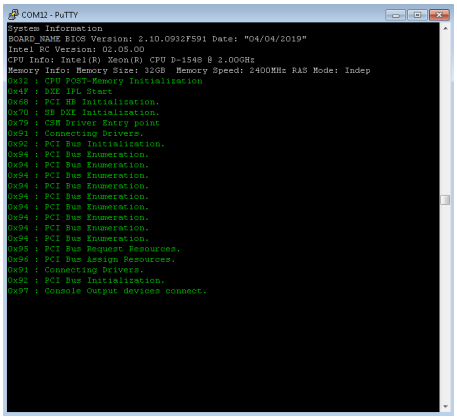
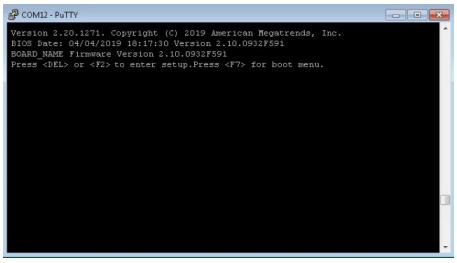
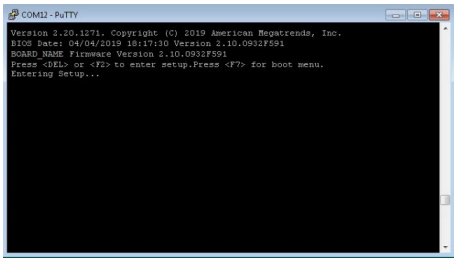
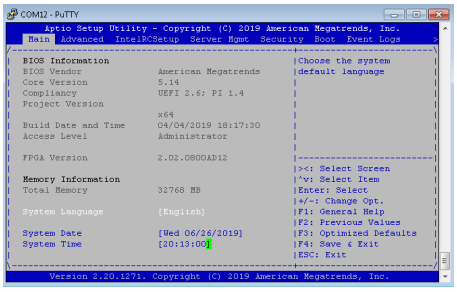
Prerequisites

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.

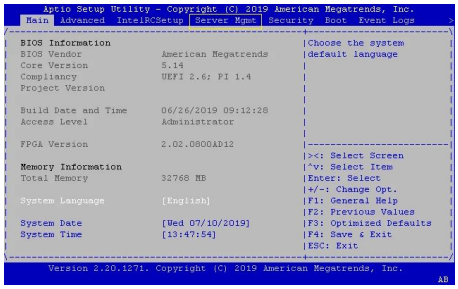
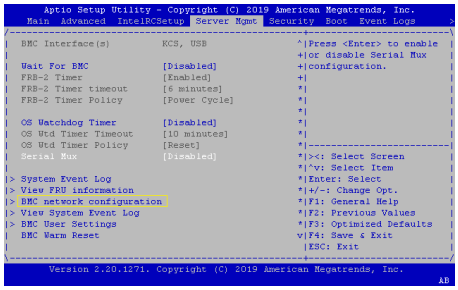
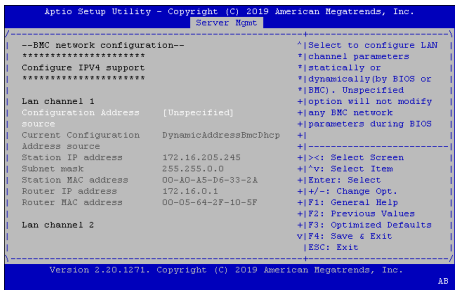
Port location



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_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 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 BMC IP address.
If you have the MAC address of the BMC, you can search the DHCP server logs to determine the IP address assigned to this specific BMC. Refer to section MAC addresses to determine those specific to a platform.
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
```

Variable	Description
00:a0:a5:d2:e9:0a	MAC address discovered for the BMC using the QR code (refer to section MAC Addresses)
ens192	Linux DHCP server network interface name
172.16.211.126	**IP address assigned to the BMC by the DHCP server**
172.16.0.10	Linux DHCP server IP address

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 [Content under creation] BIOS setup menu
- Using [Content under creation] IPMI

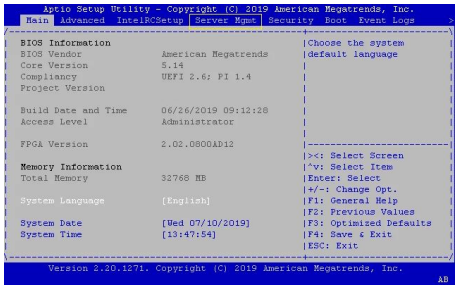
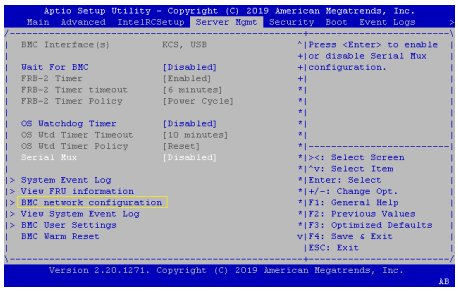
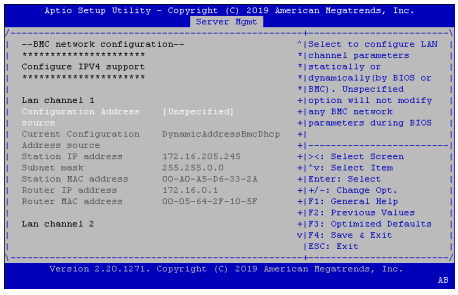
Configuring a static IP address using the BIOS setup menu

Accessing the BIOS setup menu

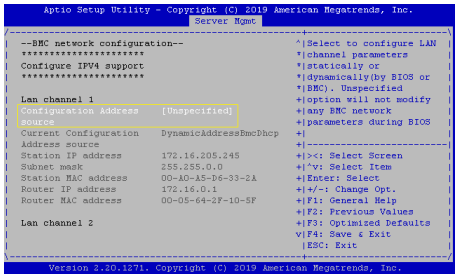
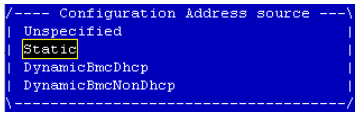
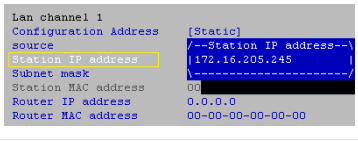
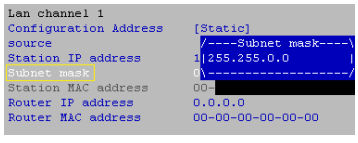
The BIOS setup menu can be accessed using various methods:

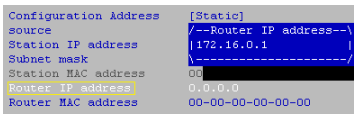
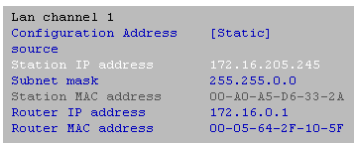
- If there is no OS installed and no known IP address, it is mandatory to use a serial console. Refer to [Content under creation] Accessing the BIOS using a serial console (physical connection) .
- If the IP address of the BMC is known, any BIOS access methods will work. Refer to Accessing the BIOS to 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**.	
Step_3	Change the **Station IP address** . **NOTE:** This is the management IP address (**BMC MNGMT_IP**).	
Step_4	Change the **Subnet mask** .	
Step_5	(Optional) Change the **Router IP address** .	

Step_5	(Optional) Change the **Router IP address** .	
Step_6	Confirm the configuration has changed and exit **BMC network configuration** using the **ESC** key.	

Configuring a static IP address using IPMI

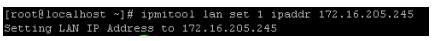
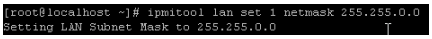
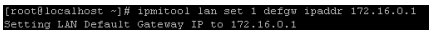
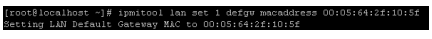
Accessing the BMC

The BMC can be accessed using two IPMI methods.

- If an OS is installed (BMC I P address known or not), IPMI via KCS can be used. R efer to [Content under creation] 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 [Content under creation] Accessing a BMC using IPMI over LAN (IOL) .

The following procedures will be executed using the [Content under creation] 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 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

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 [Content under creation] BIOS setup menu
- Using [Content under creation] IPMI

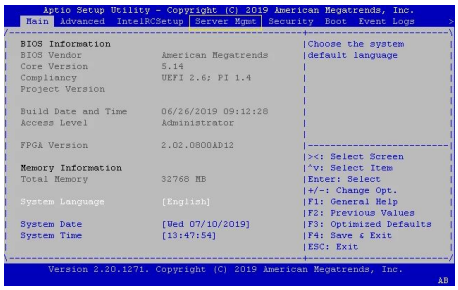
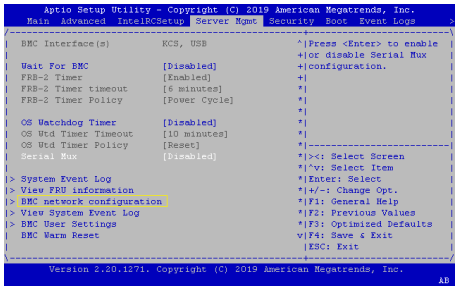
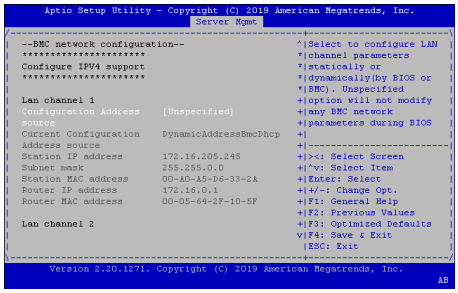
Configuring a dynamic IP address using the BIOS setup menu

Accessing the BIOS setup menu

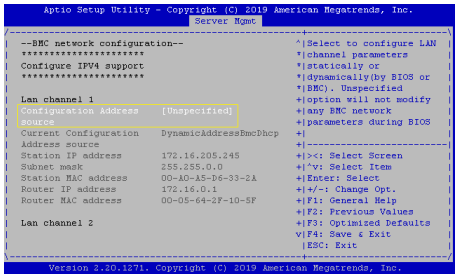
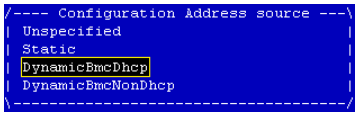
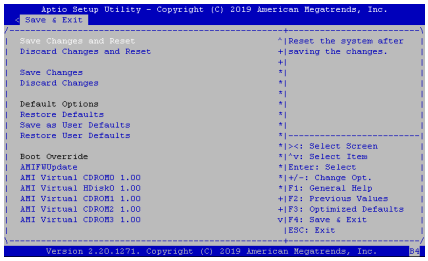
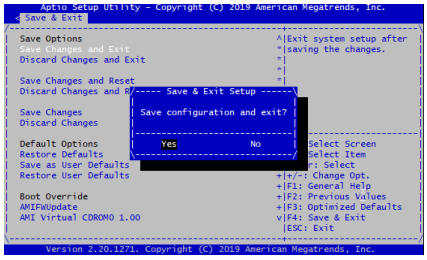
The BIOS setup menu can be accessed using various methods:

- If there is no OS installed and no known IP address, it is mandatory to use a serial console. Refer to [Content under creation] 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** . T he address displayed is your management IP address (BMC MNGMT_IP).	

Configuring a dynamic IP address using IPMI

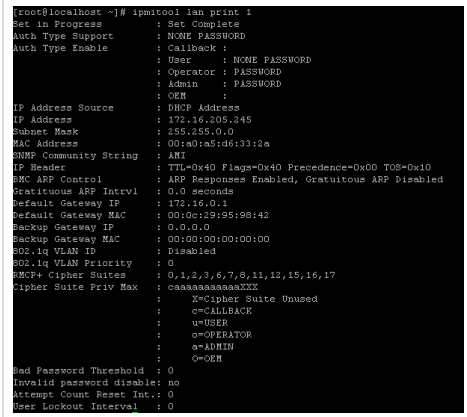
Accessing the BMC

The BMC can be accessed using two IPMI methods.

- If an OS is installed (BMC I P address known or not), IPMI via KCS can be used. R efer to [Content under creation] 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 [Content under creation] Accessing a BMC using IPMI over LAN (IOL) .

The following procedures will be executed using the [Content under creation] 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. 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. 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

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

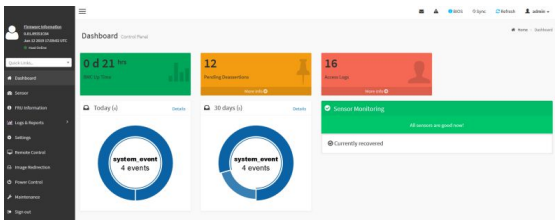
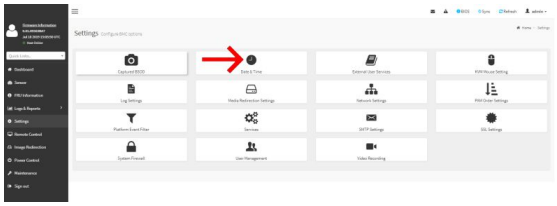
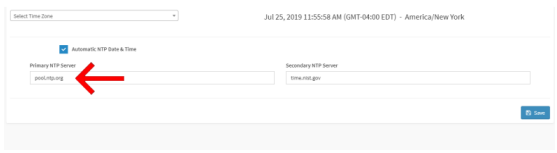
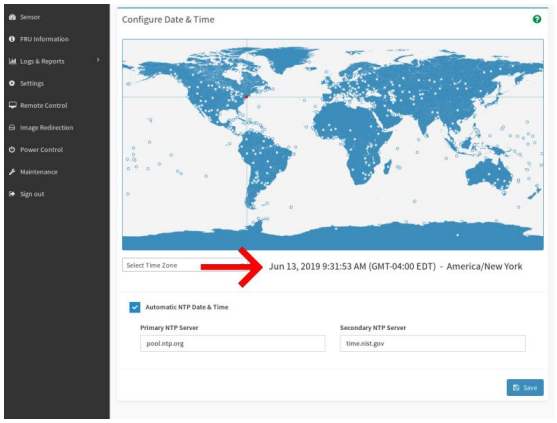
1	The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).
2	The remote computer has access to the management network subnet.

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 u sing 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**	`[root@localhost ~]# ipmitool sel time get` `07/16/2019 23:14:24`

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**	[root@localhost ~]# ipmitool raw 0x32 0xA7 01 70 6f 6f 6c 2e 6e 74 70 2e 6f 72 67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 74 69 6d 65 2e 6e 69 73 74 2e 67 6f 76 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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 converted from string to raw. • **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 [NTP_ADDRESS] [DATA]**	ipmitool raw 0x32 0xA8 0x01 49 48 46 49 46 50 48 46 49 48 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**	[root@localhost ~]# ipmitool sel time get 07/16/2019 23:14:24
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

Bytes	Description	Possible values
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

```
string="$(printf "10.1.20.10" | od -t d1 | head -n1 | sed 's/0000000 //g' | sed 's/ //g')"
length=$(echo $string | wc -w)

string_padded="$string"
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 and pad to 128 bytes with **0**.

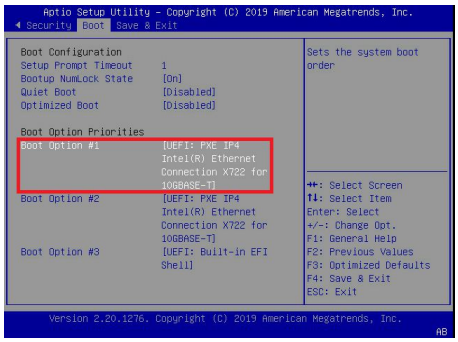
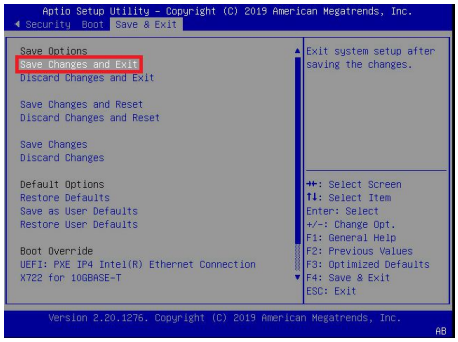
Basic BIOS option configuration

{This section details the most common configuration options related to the BIOS.}

Table of contents

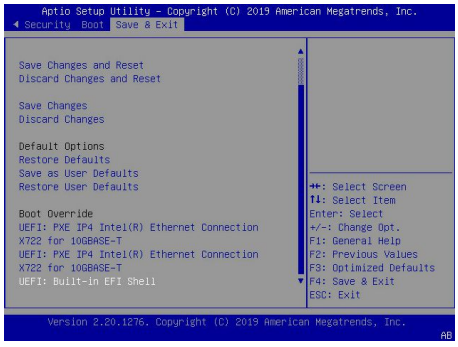
Changing the boot order

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:** T his selection will only affect the current boot.	

Overriding the boot order using IPMI

The following procedures will be executed using the [Content under creation] 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.
		`$ ipmitool chassis bootdev help`
		`bootdev <device> [clear-cmos=yes|no]`
		`bootdev <device> [options=help,...]`
		`none : Do not change boot device order`
		`pxe : Force PXE boot`
		`disk : Force boot from default Hard-drive`
		`safe : Force boot from default Hard-drive, request Safe Mode`
		`diag : Force boot from Diagnostic Partition`
		`cdrom : Force boot from CD/DVD`
		`bios : Force boot into BIOS Setup`
		`floppy: Force boot from Floppy/primary removable media`

Step_2	Override the boot order. LocalServer_OSPrompt:~# **ipmitool chassis bootdev [DEVICE]**	`$ ipmitool chassis bootdev pxe` `Set Boot Device to pxe`

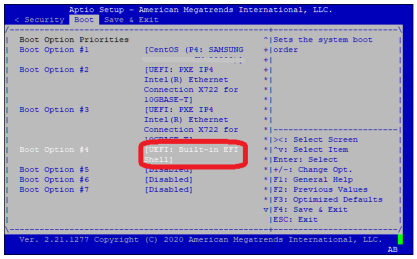
Enter the BIOS menu on the next boot using IPMI

The following procedures will be executed using the [Content under creation] 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	Execute the following command to enter the BIOS menu automatically on the next boot. LocalServer_OSPrompt:~# **ipmitool chassis bootdev bios**	`$ ipmitool chassis bootdev bios` `Set Boot Device to bios`

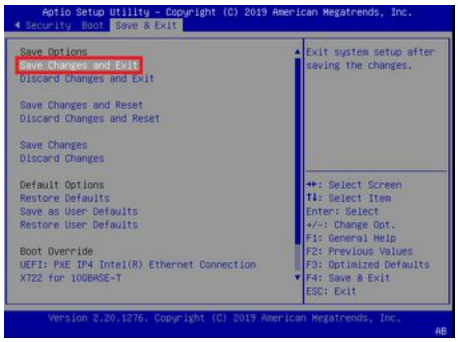
Enabling Retry Boot Order when CSM is disabled

Refer to Accessing the BIOS for access instructions.

Step_1	To be able to retry the boot sequence indefinitely the EFI shell must be disabled in the list of boot options.	

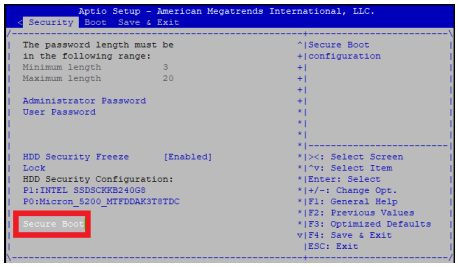
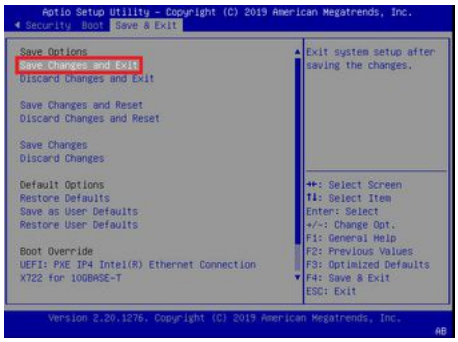
Configuring Secure Erase

Refer to Accessing the BIOS for access instructions.

Step_1	From the BIOS setup menu, select the **Security** menu and disable the **HDD Security Freeze Lock** option.	
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.	
Step_3	Use the following application note to Secure Erase the applicable drive.	Secure Erase

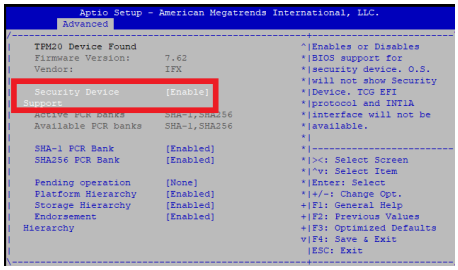
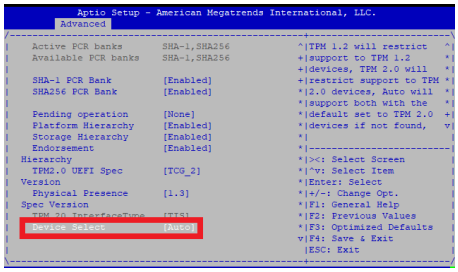
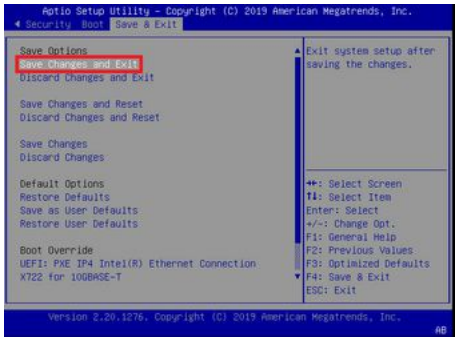
Enabling Secure Boot

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

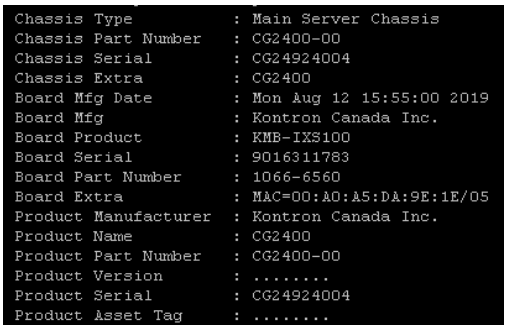
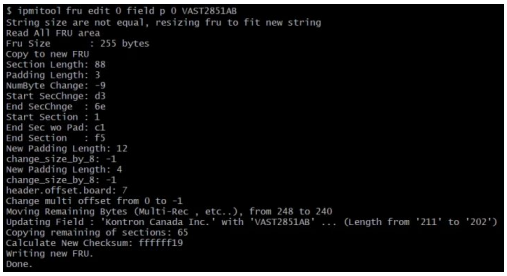
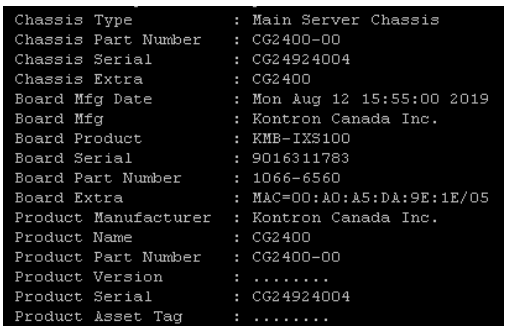
Customizing platform FRU data using IPMI

The BMC can be accessed using two IPMI methods.

- If an OS is installed (BMC I P address known or not), IPMI via KCS can be used. R efer to [Content under creation] 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 [Content under creation] Accessing a BMC using IPMI over LAN (IOL) .

The following procedures will be executed using the [Content under creation] 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:~# **i pmitool fru print**	
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 [Content under creation] FRU commands for available commands.	
Step_3	Confirm changes were properly applied. LocalServer_OSPrompt:~# **ipmitool fru print**	

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

Command	FRU data	Example
p 0	Product Manufacturer	LocalServer_OSPrompt:~# **ipmitool fru edit 0 field p 0 [VALUE]**
p 1	Product Name	
p 2	Product Part Number	
p 3	Product Version	
p 4	Product Serial Number	
p 5	Product Asset Tag	

Customizing chassis related informations

Command	FRU data	Example
c 0	Chassis Part Number	LocalServer_OSPrompt:~# **ipmitool fru edit 0 field c 0 [VALUE]**
c 1	Chassis Serial Number	

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

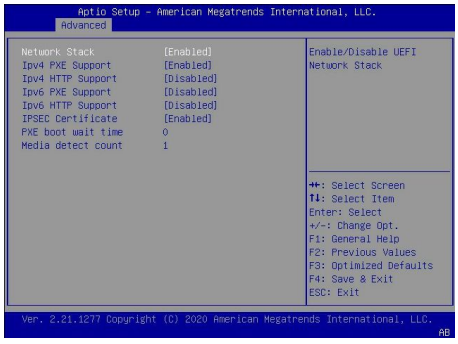
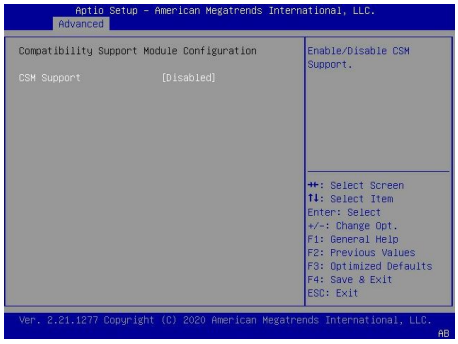
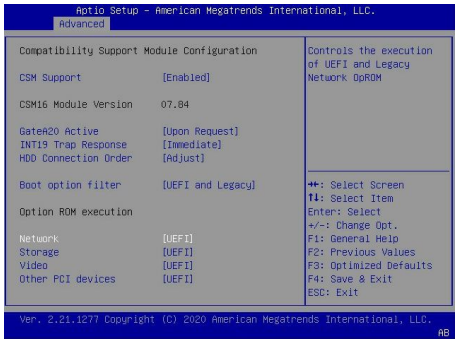
{This article provides all relevant information required to establish a successful network integration of the platform.}
Table of contents

Configuring VLANs

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.

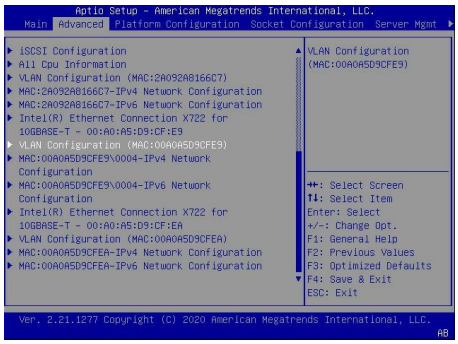
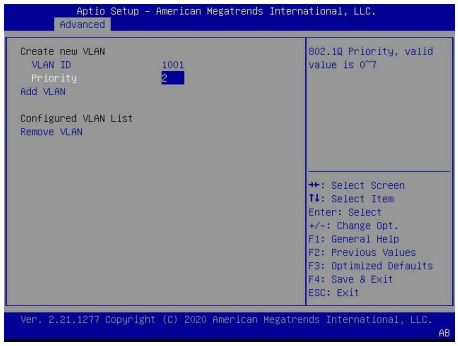
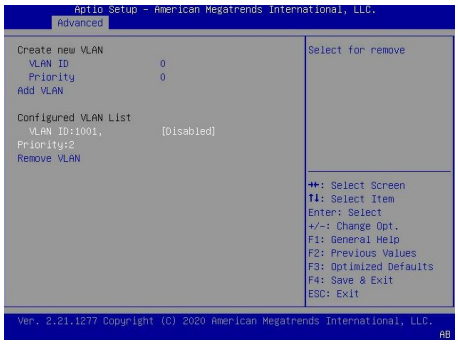
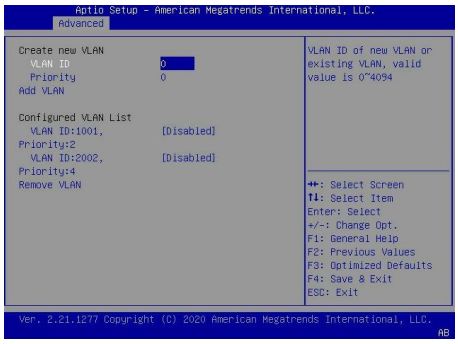
Enabling the UEFI Network Stack and configuring CSM

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.	

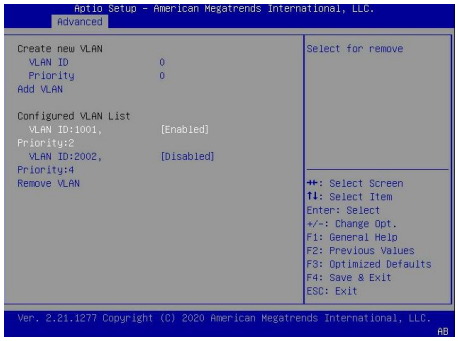
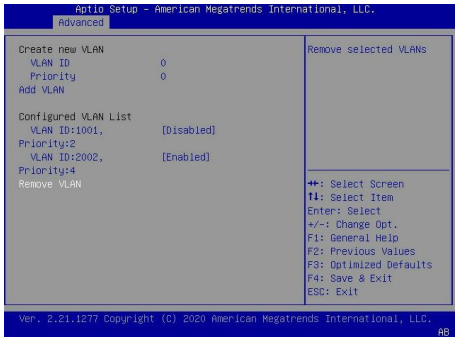
Creating VLANs

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. Select **Enter Configuration Menu** . **NOTE:** The MAC address will be the one o f 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:xxxxxxxxxxxx)** section. Select **Enter Configuration Menu** . **NOTE:** The MAC address will be the one o f 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.	

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.

NOTICE	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: • System fans staying at maximum speed at all time • Front panel LED indicating alarm conditions (System Status LED) • Unhealthy events in the System Event Log

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 (BMC I P address known or not), IPMI via KCS can be used. R efer to [Content under creation] 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 [Content under creation] Accessing a BMC using IPMI over LAN (IOL) .

The following procedures will be executed using the [Content under creation] 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]** .

Step_1	Write the redundancy count. When using only one PSU, the value will be 1. LocalServer_OSPrompt:~# **ipmitool -H 192.168.1.10 -I lanplus -U admin -P admin raw 0x3c 0x02 0x00 0x01 0x00 0x01**
Step_2	Read the redundancy count to confirm the change. The answer should be 1. LocalServer_OSPrompt:~# **ipmitool -H 192.168.1.10 -I lanplus -U admin -P admin raw 0x3c 0x02 0x00 0x00 0x00**

Operating

{This section contains all the information required to operate, manage, monitor, maintain and upgrade the platform.}

Children

- Default user names and passwords
- Accessing platform components
- Platform power management
- Monitoring
- Maintenance
- Platform cooling and thermal management

Default user names and passwords

{This article lists all default user names and passwords per component . }

Table of contents

Operating system

User interface	User name	Password
Operating system	Application specific	Application specific
Kontron linux snmp-agent	Application specific Refer to Configuration of system access methods	Application specific Refer to Configuration of system access methods

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 [Content under creation] Configuring BMC user names and passwords using the Web UI .

The CG2400 platform includes one BMC.

User interface	User name	Password
Web UI	admin	admin
IPMI	admin	admin
Redfish	Administrator	superuser
SNMP	New 8 character minimum user name configured after first login	New 8 character minimum password configured after first login

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

{This article provides access paths to the prompts and interfaces that allow configuration, monitoring or troubleshooting.}

Children

- Accessing the operating system of a server
- Accessing the BIOS
- Accessing a BMC

Accessing the operating system of a server

Table of contents

An operating system can be accessed through various methods:

- Using the [Content under creation] KVM (Keyboard Video Mouse)
- Using the [Content under creation] display port (VGA) – this is the recommended path for first time out-of-the-box system configuration
- Using [Content under creation] SSH/RDP/Customer application protocols
- Using [Content under creation] Serial over LAN (SOL)
- Using a [Content under creation] 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

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

Relevant section:
Baseboard management controller - BMC

Browser considerations

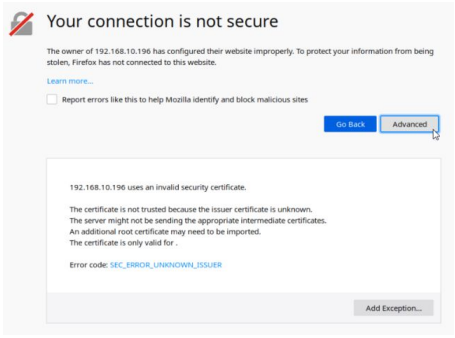
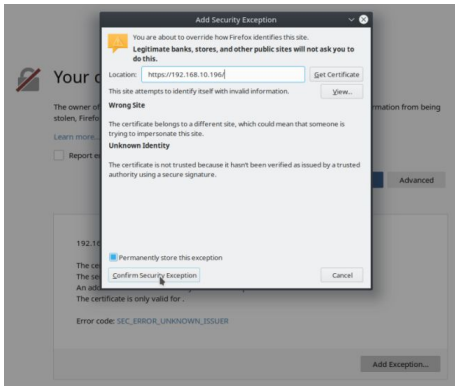
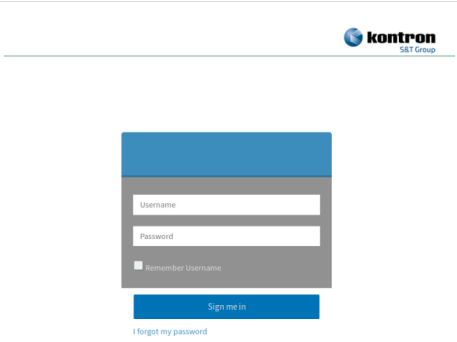
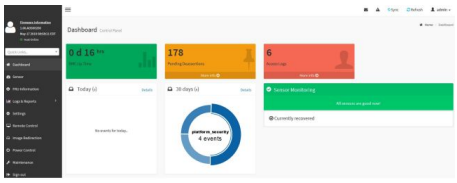
HTML5	To connect to the Web UI, a Web browser supporting HTML5 is required.
HTTPS self-signed certificate	Upon connection to the Web UI, it is mandatory to accept the HTTPS self-signed certificate. For further information about accepting HTTPS self-signed certificates, please refer to your Web browser's 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.

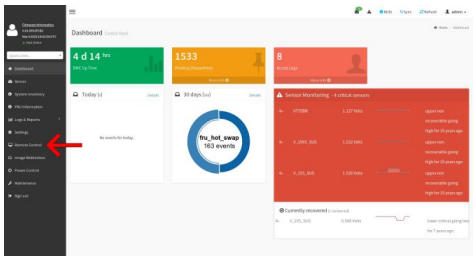
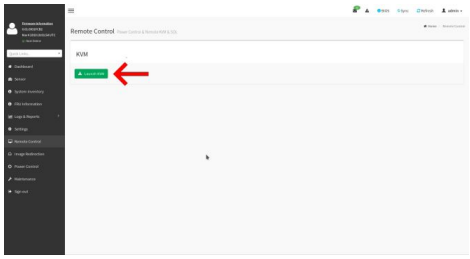
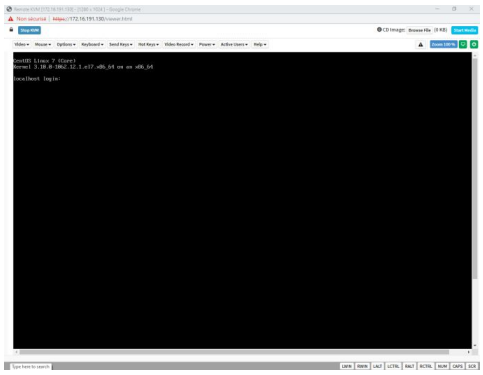
Access procedure

Accessing the BMC of the server for which you want to access the 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 s tart 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.	

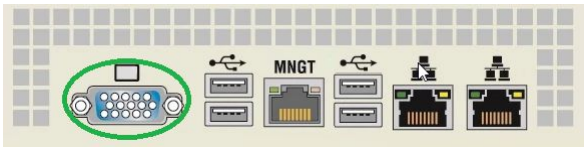
If the OS is not displayed, perform a server reset as described in Sending a power command using the Web UI . Then relaunch the KVM.

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)

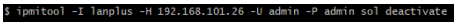
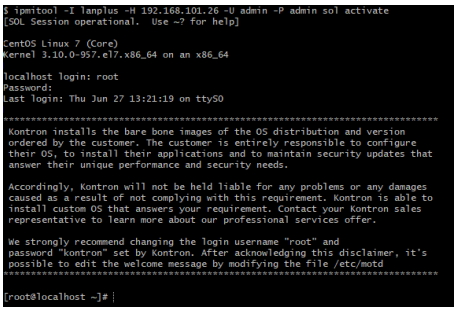
Prerequisites

1	An OS is installed.
2	The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).
3	The remote computer has access to the management network subnet.
4	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. RemoteComputer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name]-P [IPMI password] sol deactivate**	
Step_2	Activate an SOL session. RemoteComputer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name]-P [IPMI password] sol activate**	
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 .

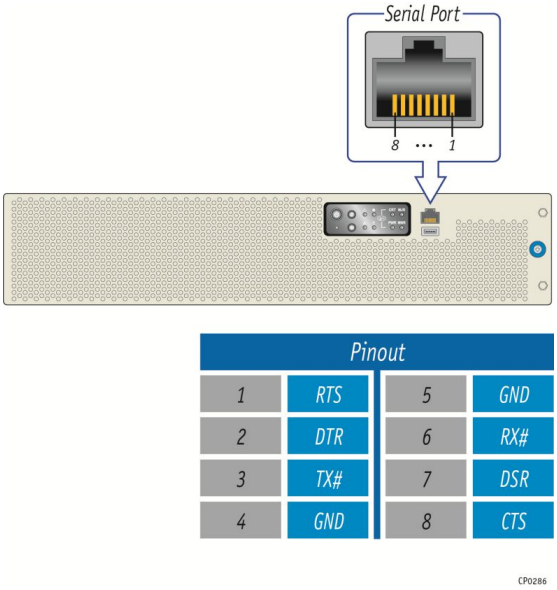
Accessing an OS using a s erial console (physical connection)

Prerequisites

1	An OS is installed.
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.

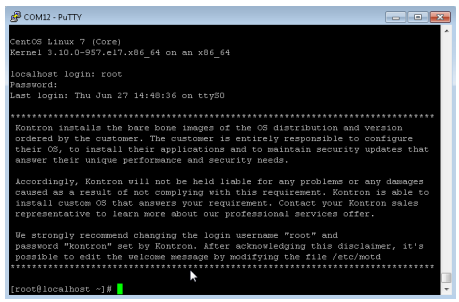
Relevant section:
Baseboard management controller - BMC

Port location



Access procedure

To obtain the list of default user names and passwords, refer to Default user names and passwords .

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	The OS start screen will be displayed.	

NOTE : If the OS is not displayed, perform a server reset. Refer to Platform power management .

Accessing the BIOS

Table of contents

The BIOS can be accessed through various methods:

- Using the [Content under creation] KVM (Keyboard Video Mouse)
- Using the display port (VGA) – this is the recommended path for first time out-of-the-box system configuration
- Using [Content under creation] Serial over LAN (SOL)
- Using a [Content under creation] 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

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

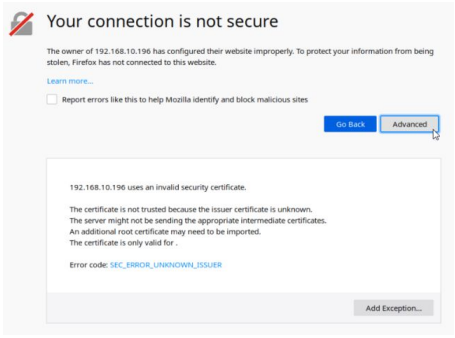
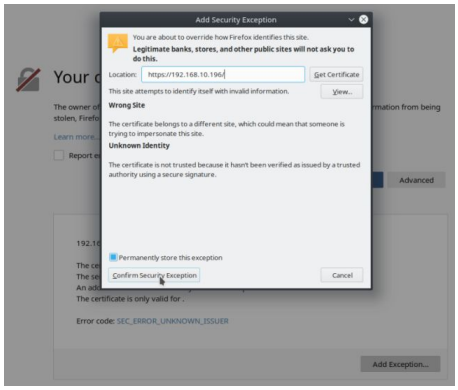
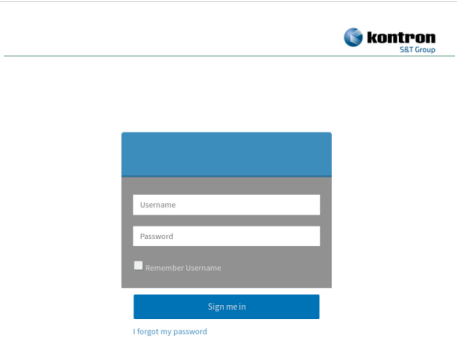
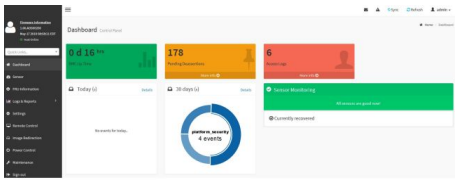
HTML5	To connect to the Web UI, a Web browser supporting HTML5 is required.
HTTPS self-signed certificate	Upon connection to the Web UI, it is mandatory to accept the HTTPS self-signed certificate. For further information about accepting HTTPS self-signed certificates, please refer to your Web browser's 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.

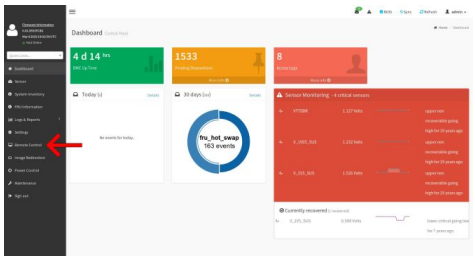
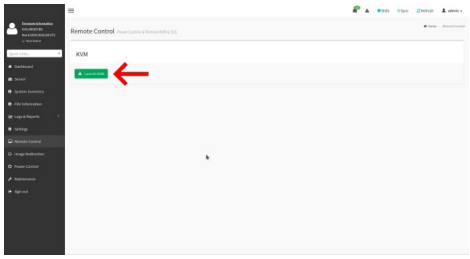
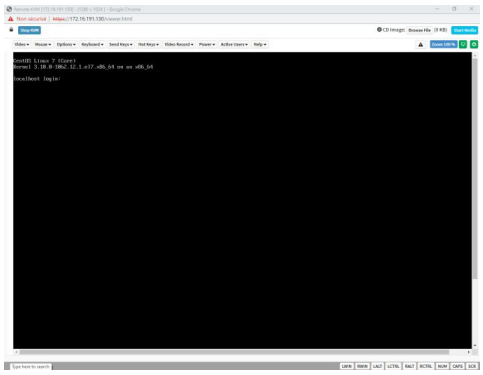
Access procedure

Accessing the BMC of the server for which you want to access the BIOS

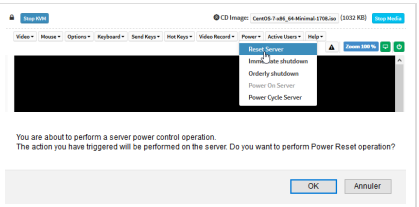
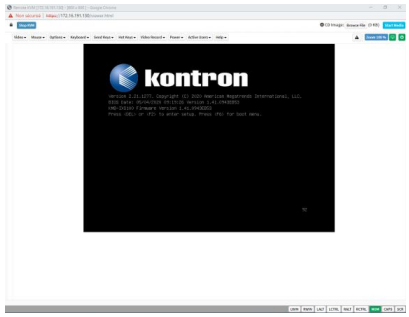
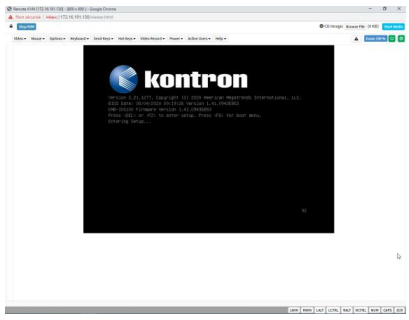
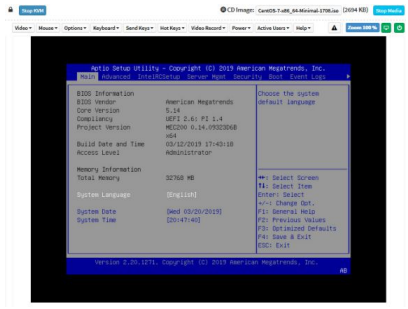
To obtain the list of default user names and passwords, refer to Default user names and passwords .

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 s tart 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

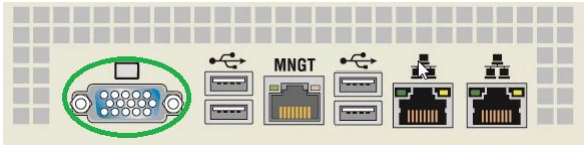
Step_1	From the **Power** drop-down menu, select **Reset Server** to access the BIOS menu. Click on **OK** to confirm the operation. **NOTE:** When a reset server command is launched, it may take a few seconds for the BIOS sign on screen to display.	
Step_2	When the BIOS sign on screen is displayed, 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. 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.	

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

Step_1	Connect the VGA cable to the monitor and the platform.
Step_2	Reset the platform.
Step_3	The BIOS screen should be displayed on the monitor.

Accessing the BIOS using Serial over LAN (SOL)

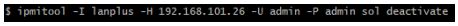
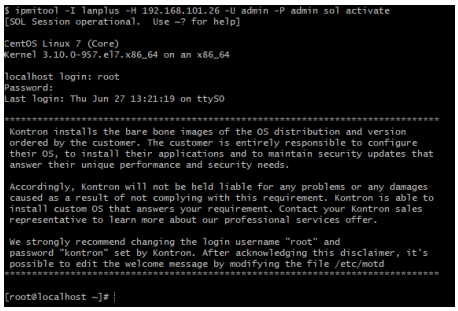
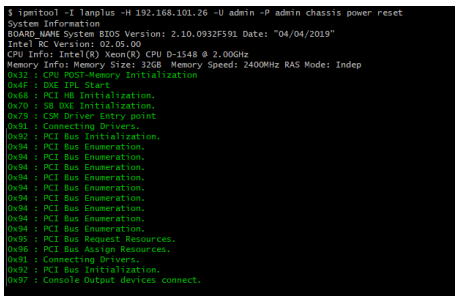
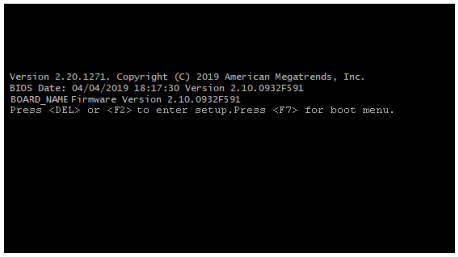
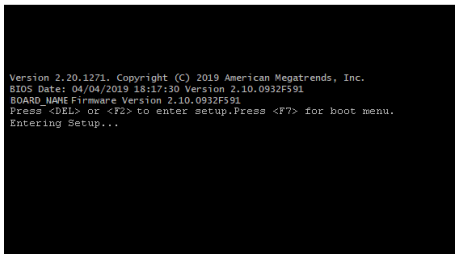
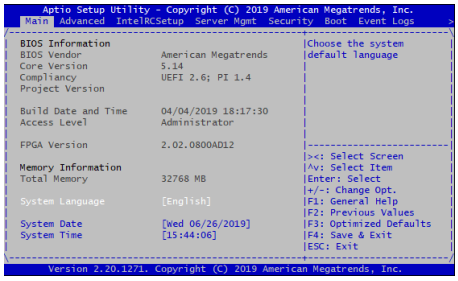
Prerequisites

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 .

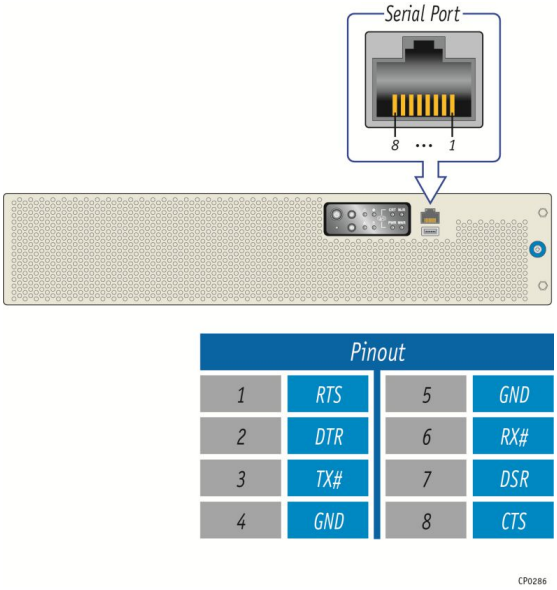
Step_1	From a remote computer that has access to the management network subnet, open the OS command prompt and deactivate any previous SOL session. RemoteComputer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] sol deactivate**	
Step_2	Activate an SOL session. RemoteComputer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] sol activate** **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. RemoteComputer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI p assword] chassis power 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)

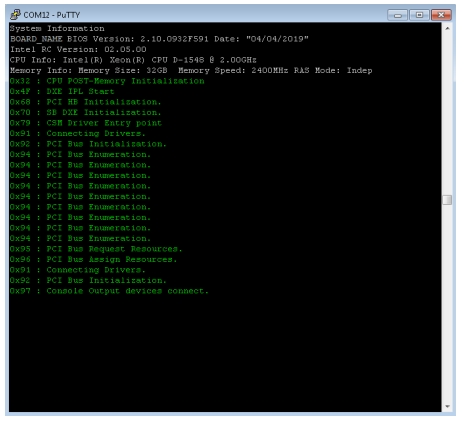
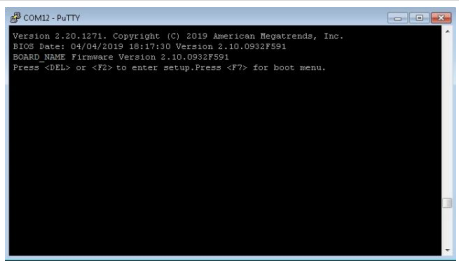
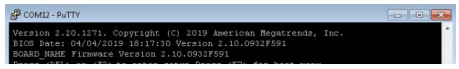
Prerequisites

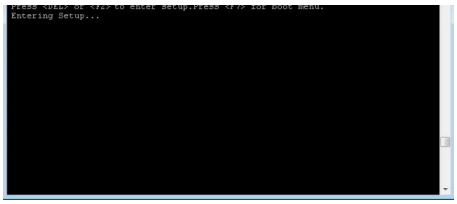
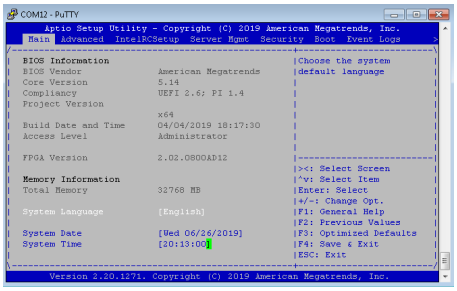
1	A physical connection to the device is required. **NOTE:** The serial console port is compatible with Cisco 72-3383-01 cable.
2	A serial console tool is installed on the remote computer. • Speed (Baud): 115200 • Data bits: 8 • Stop bits: 1 • Parity: None • Flow Control: None • Recommended emulation 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

A BMC can be accessed through various methods:

- Using the [Content under creation] Web UI – this is the recommended path for first time out-of-the-box system configuration
- Using [Content under creation] IPMI over LAN (IOL)
- Using [Content under creation] IPMI via KCS
- Using [Content under creation] SNMP
- Using [Content under creation] 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

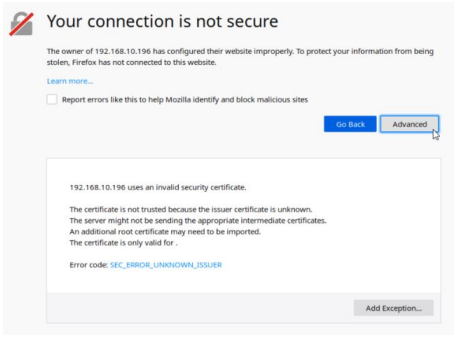
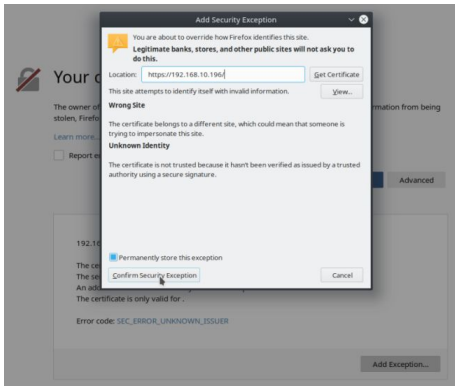
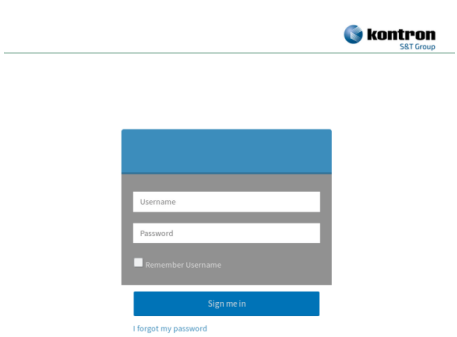
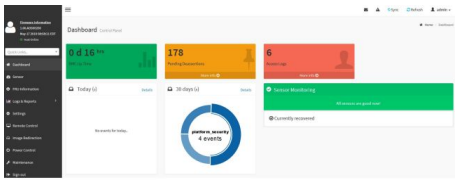
Browser considerations

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

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 s tart 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.	

Accessing a BMC using IPMI over LAN (IOL)

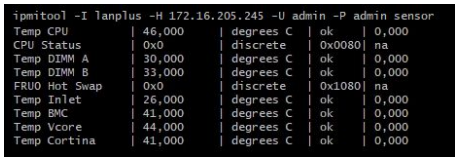
Prerequisites

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, e nter 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 .

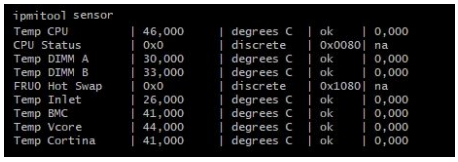
Accessing a BMC using IPMI via KCS

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 the server OS through SSH, RDP or the platform serial port, e nter 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:

- [Content under creation] BMC SNMP
- The [Content under creation] Kontron linux snmp-agent

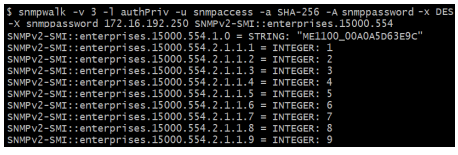
Accessing a BMC using BMC SNMP

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, e nter the desired command. RemoteComputer_OSPrompt:~# **snmpwalk -v 3 -l [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [PASSWORD] [BMC MNGMT_IP] [OID]**	

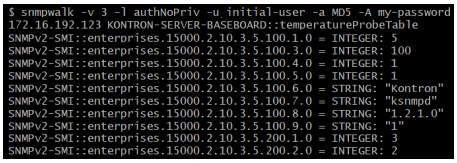
Accessing a BMC using the Kontron linux snmp-agent

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, e nter the desired command. RemoteComputer_OSPrompt:~# **snmpwalk -v3 -l [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [PASSWORD] [SERVER_IP] [ODI]**	

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 parsor 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. RemoteComputer_OSPrompt:~$ **curl -k -s [ROOT_URL] Managers/Self | jq**	

Platform power management

{This article provides instructions to safely power on, power off or reboot a component.}

Table of contents

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:

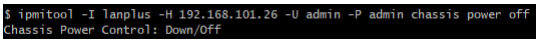
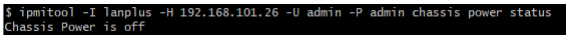
- [Content under creation] Power off : Immediately powers off the platform. **WARNING** : This command does not initiate a clean shutdown of the operating system prior to powering down the system.
- [Content under creation] Power on : Powers on the platform. **NOTE** : Due to the electrical setup of the system, there is a 30 seconds delay for the system to start.
- [Content under creation] 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.
- [Content under creation] 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.
- [Content under creation] 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 [Content under creation] Web UI
- Using [Content under creation] IPMI (IOL)
- Using [Content under creation] IPMI (KCS)
- Using [Content under creation] Redfish

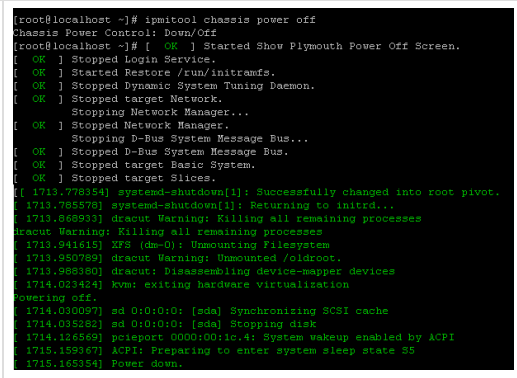
Power off using IPMI (IOL)

Refer to [Content under creation] 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 power off the platform. RemoteComputer_OSPrompt:~$ **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power off**	
Step_2	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**	

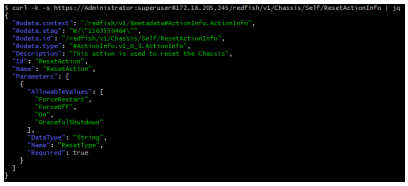
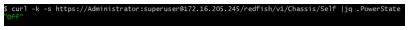
Power off using IPMI (KCS)

Refer to [Content under creation] 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, power off the platform. LocalServer_OSPrompt:~# **ipmitool chassis power off**	

Power off using Redfish

Refer to [Content under creation] Accessing a BMC using Redfish for access instructions.

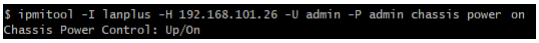
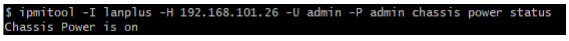
Step_1	Print the list of available power actions. RemoteComputer_OSPrompt:~$ **curl -k -s [ROOT_URL]Chassis/Self/ResetActionInfo | jq**	
Step_2	Power off the platform. RemoteComputer_OSPrompt:~$ **curl -k -s [ROOT_URL]Chassis/Self/Actions/Chassis.Reset -X POST -d '{"ResetType":"ForceOff"}' -H "Content-Type: application/json"**	
Step_3	Verify the power status. RemoteComputer_OSPrompt:~$ **curl -k -s [ROOT_URL]Chassis/Self | jq .PowerState**	

Power on

- Using the [Content under creation] Web UI
- Using [Content under creation] IPMI (IOL)
- Using [Content under creation] Redfish

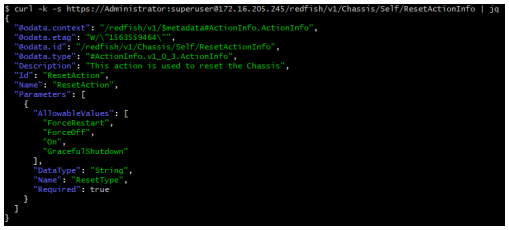
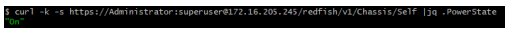
Power on using IPMI (IOL)

Refer to [Content under creation] 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 power on the platform. RemoteComputer_OSPrompt:~$ **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power on**	
Step_2	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**	

Power on using Redfish

Refer to [Content under creation] Accessing a BMC using Redfish for access instructions.

Step_1	Print the list of available power actions. RemoteComputer_OSPrompt:~$ **curl -k -s [ROOT_URL] Chassis/Self/ResetActionInfo | jq**	
Step_2	Power on the platform. RemoteComputer_OSPrompt:~$ **curl -k -s [ROOT_URL]Chassis/Self/Actions/Chassis.Reset -X POST -d '{"ResetType":"On"}' -H "Content-Type: application/json"**	
Step_3	Verify the power status. RemoteComputer_OSPrompt:~$ **curl -k -s [ROOT_URL]Chassis/Self | jq .PowerState**	

Reset (warm boot)

- Using the [Content under creation] Web UI
- Using [Content under creation] IPMI (IOL)
- Using [Content under creation] IPMI (KCS)
- Using [Content under creation] Redfish

Reset (warm boot) using IPMI (IOL)

Refer to [Content under creation] 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. RemoteComputer_OSPrompt:~$ **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power reset**	`$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power reset` `Chassis Power Control: Reset`
Step_2	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** **NOTE:** It may take a moment for the OS to reboot.	`$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power status` `Chassis Power is on`

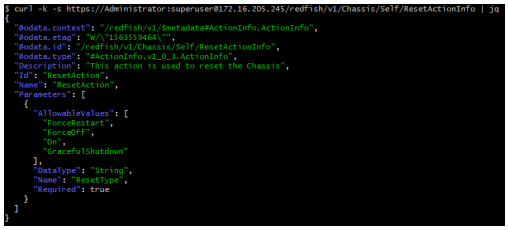
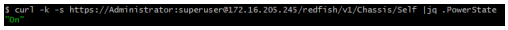
Reset (warm boot) using IPMI (KCS)

Refer to [Content under creation] 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, reset the platform. LocalServer_OSPrompt:~# **ipmitool chassis power reset** **NOTE:** It may take a moment for the OS to reboot.	`[root@localhost ~]# ipmitool chassis power reset` `Chassis Power Control: Reset`

Reset (warm boot) using Redfish

Refer to [Content under creation] Accessing a BMC using Redfish for access instructions.

Step_1	Print the list of available power actions. RemoteComputer_OSPrompt:~$ **curl -k -s [ROOT_URL] Chassis/Self/ResetActionInfo | jq**	
Step_2	Reset the platform. RemoteComputer_OSPrompt:~$ **curl -k -s [ROOT_URL]Chassis/Self/Actions/Chassis.Reset -X POST -d '{"ResetType":"ForceRestart"}' -H "Content-Type: application/json"**	
Step_3	Verify the power status. RemoteComputer_OSPrompt:~$ **curl -k -s [ROOT_URL]Chassis/Self | jq .PowerState**	

Power cycle (cold boot)

- Using the [Content under creation] Web UI
- Using [Content under creation] IPMI (IOL)
- Using [Content under creation] IPMI (KCS)

Power cycle (cold boot) using IPMI (IOL)

Refer to [Content under creation] 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 perform a power cycle. RemoteComputer_OSPrompt:~$ **ipmitool -I lanplus -H [BMC MNGMT_IP] - -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power cycle**	`$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power cycle` `Chassis Power Control: Cycle`
Step_2	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** **NOTE:** It may take a moment for the OS to reboot.	`$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power status` `Chassis Power is on`

Power cycle (cold boot) using IPMI (KCS)

Refer to [Content under creation] 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 a power cycle. LocalServer_OSPrompt:~# **ipmitool chassis power cycle** **NOTE:** It may take a moment for the OS to reboot.	`[root@localhost ~]# ipmitool chassis power cycle` `Chassis Power Control: Cycle`

ACPI shutdown (clean shutdown)

- Using the [Content under creation] Web UI
- Using [Content under creation] IPMI (IOL)
- Using [Content under creation] IPMI (KCS)
- Using [Content under creation] Redfish

ACPI shutdown using IPMI (IOL)

Refer to [Content under creation] 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 perform an ACPI shutdown. RemoteComputer_OSPrompt:~$ **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power soft**	`$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power soft` `Chassis Power Control: Soft`
Step_2	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**	`$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power status` `Chassis Power is off`

ACPI shutdown using IPMI (KCS)

Refer to [Content under creation] 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**
		`[root@localhost ~]# ipmitool chassis power soft`
		`Chassis Power Control: Soft`
		`[root@localhost ~]# [  OK  ] Started Show Plymouth Power Off Screen.`
		`[  OK  ] Stopped Network Manager.`
		`Stopping D-Bus System Message Bus...`
		`[  OK  ] Stopped D-Bus System Message Bus.`
		`[  OK  ] Stopped Login Service.`
		`[  OK  ] Stopped target Basic System.`

ACPI shutdown using Redfish

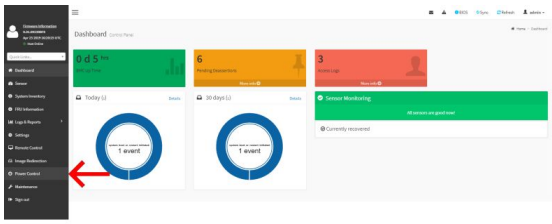
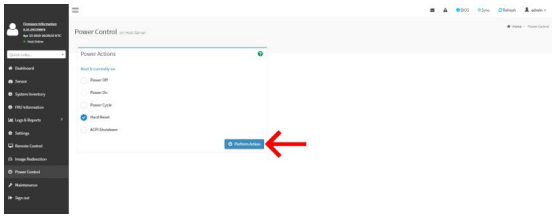
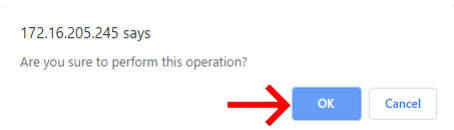
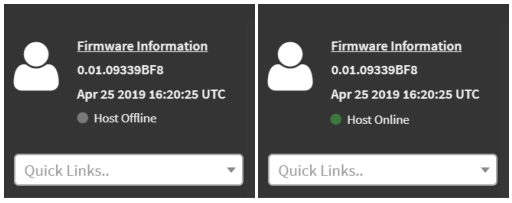
Refer to [Content under creation] Accessing a BMC using Redfish for access instructions.

Step_1	Print the list of available power actions.
	RemoteComputer_OSPrompt:~$ **curl -k -s [ROOT_URL] Chassis/Self/ResetActionInfo | jq**
		`$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Chassis/Self/ResetActionInfo | jq`
		`{`
		`"@odata.context": "/redfish/v1/$metadata#ActionInfo.ActionInfo",`
		`"@odata.etag": "W/\"1563559464\"",`
		`"@odata.id": "/redfish/v1/Chassis/Self/ResetActionInfo",`
		`"@odata.type": "#ActionInfo.v1_0_3.ActionInfo",`
		`"Description": "This action is used to reset the Chassis",`
		`"Id": "ResetAction",`
		`"Name": "ResetAction",`
		`"Parameters": [`
		`{`
		`"AllowableValues": [`
		`"ForceRestart",`
		`"ForceOff",`
		`"On",`
		`"GracefulShutdown"`
		`],`
		`"DataType": "String",`
		`"Name": "ResetType",`
		`"Required": true`
		`}`
		`]`
		`}`

Step_2	Perform the power action on the platform. RemoteComputer_OSPrompt:~$ **curl -k -s [ROOT_URL]Chassis/Self/Actions/Chassis.Reset -X POST -d '{"ResetType":"GracefulShutdown"}' -H "Content-Type: application/json"**	
Step_3	Verify the power status. RemoteComputer_OSPrompt:~$ **curl -k -s [ROOT_URL]Chassis/Self | jq .PowerState**	`$ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/v1/Chassis/Self |jq .PowerState` `"On"`

Sending a power command using the Web UI

Refer to [Content under creation] 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.

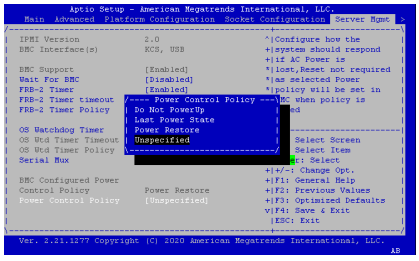
IPMI	BIOS menu	Note
always-on	Power Restore	Platform powers up when power is restored
previous	Last Power State	Platform returns to previous state (before the power outage) when power is restored
always-off	Do Not Power Up	Platform stays unpowered even though input power is back

Using IPMI

Step_1	Using the **ipmitool chassis policy** command, set the power control policy. L ocalServer_OSPrompt:~# **ipmitool chassis power policy [POLICY]**	`$ ipmitool chassis policy always-on` `Set chassis power restore policy to always-on`

Using the BIOS menu

Refer to Accessing the BIOS for access instructions.

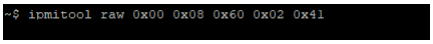
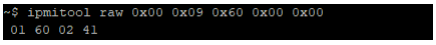
Step_1	From the **Server Mgmt** menu, select the **Power Control Policy** value.	

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 support:

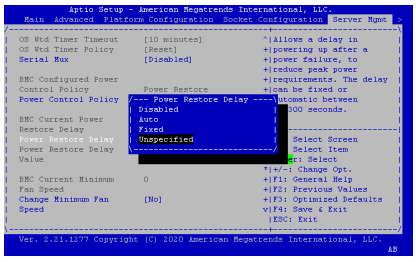
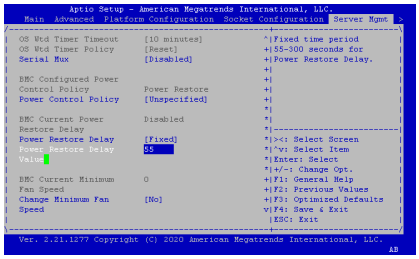
BIOS value	Note
Disabled	No Power Restore Delay will be set, platform starts automatically after power outage (default value)
Auto	Random value (between 55-300 sec) will be set, platform starts after this delay is elapsed
Fixed	Selected value (between 55-300 sec) will be set, platform starts after this delay is elapsed

Using IPMI

Step_1	Using this **ipmitool raw OEM** command, set the Power Restore Delay parameters. L ocalServer_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. L ocalServer_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

Children

- Monitoring sensors
- Sensor list
- Interpreting sensor data
- Configuring and using SNMP traps
- System Inventory
- Configuring and using SNMP traps in WebUI
- Telco Alarm Manager

Monitoring sensors

{This article details all available monitoring agents of the platform.}

Table of contents

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

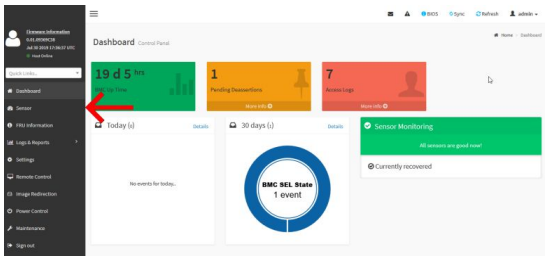
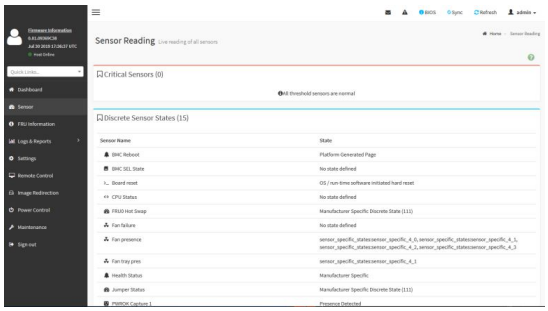
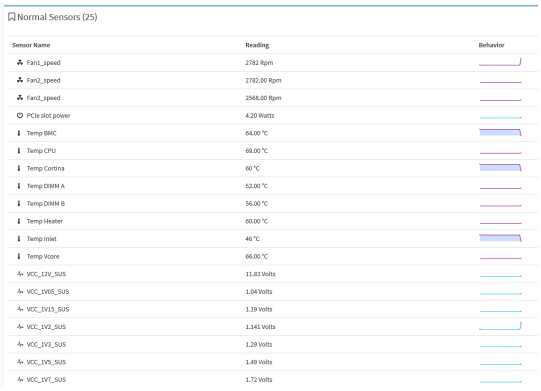
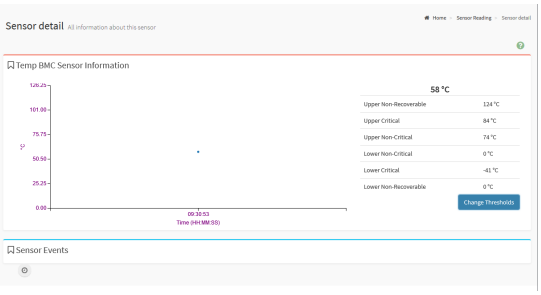
For sensor data interpretation instructions, refer to Interpreting sensor data .

For instructions on how to access the BMC, refer to Accessing a BMC .

Monitoring using the BMC Web UI

Accessing sensor details

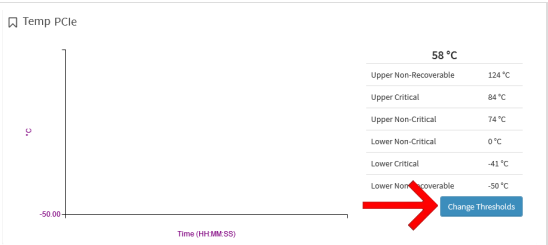
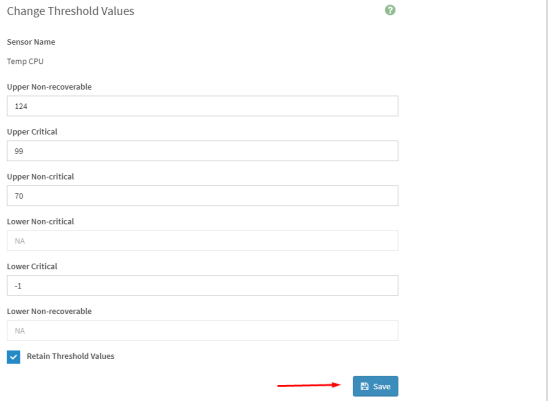
Refer to Accessing a BMC using the Web UI for access instructions.

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.

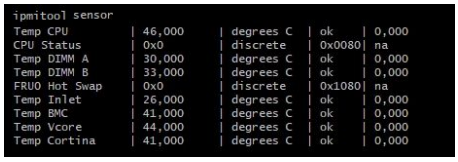
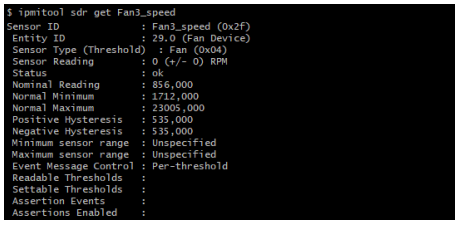
NOTICE	Default platform sensor thresholds should not be changed. They have been set to ensure proper operation. Should you decide to change them, use caution as inappropriate settings could cause a property damage.

Step_1	From the sensor detail page, click on **Change Thresholds** .	
Step_2	Set the thresholds as desired and click on **S ave** . 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]** .

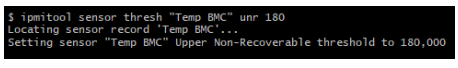
Viewing sensor details

Step_1	From a remote computer that has access to the server OS through SSH, RDP or the platform serial port , e nter 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.

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	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:

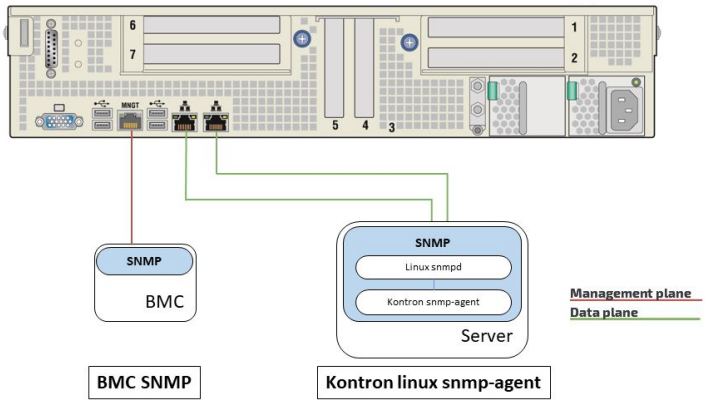
- Using BMC SNMP
- Using the Kontron linux snmp-agent

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 Kontron linux snmp-agent me thod .
- 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.

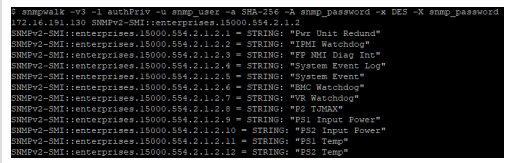
- The linux snmp-agent is accessible from the two 10GbE LAN ports on the data plane.



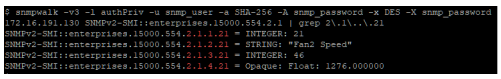
Monitoring using BMC SNMP

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. RemoteComputer_OSPrompt:~# **snmpwalk -v3 -l [AUTH_LEVEL] -u [USER_NAME]-a [AUTH_PROTOCOL] -A [PASSWORD] -x [ENC_PROTOCOL] -X " [PASSWORD]" [MGMNT_IP] [OID]**	

Viewing sensor details

Step_1	Use the following command to view sensor details. RemoteComputer_OSPrompt:~# **snmpwalk -v3 -l [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [PASSWORD] -x [ENC_PROTOCOL] -X " [PASSWORD]" [MGMNT_IP] [OID] | grep "\.[TABLE_ENTRY_NUMBER] "** **NOTE:** The space between the [TABLE_ENTRY_NUMBER] attribute and the quotes is required for the grep command to work properly.	

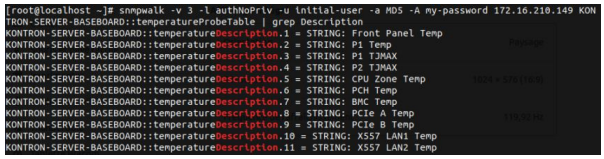
Monitoring using the Kontron linux snmp-agent

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

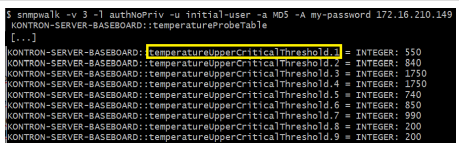
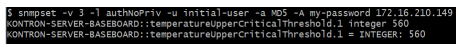
Group	Group OID	Sub-group	Sub-group OID | Numerical OID
Power	powerGroup	Power unit	powerUnitTable | 1.3.6.1.4.1.15000.2.10.3.5.400.10
		Power supply	powerSupplyTable | 1.3.6.1.4.1.15000.2.10.3.5.400.20
		Voltages	voltageProbeTable | 1.3.6.1.4.1.15000.2.10.3.5.400.30
		Discrete voltage	discreteVoltageProbeTable | 1.3.6.1.4.1.15000.2.10.3.5.400.40
Thermal	thermalGroup	Cooling unit	coolingUnitTable | 1.3.6.1.4.1.15000.2.10.3.5.600.10
		Cooling device	coolingDeviceTable | 1.3.6.1.4.1.15000.2.10.3.5.600.20
		Discrete cooling device	discreteCoolingTable | 1.3.6.1.4.1.15000.2.10.3.5.600.30
		Temperature	temperatureProbeTable | 1.3.6.1.4.1.15000.2.10.3.5.600.40

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). RemoteComputer_OSPrompt:~# **snmpwalk -v3 -l [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [PASSWORD] [SERVER_IP] KONTRON-SERVER-BASEBOARD:: [OID_SUB_GROUP] | grep Description**	
Step_2	View sensor details for a specific sensor. RemoteComputer_OSPrompt:~# **snmpwalk -v3 -l [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [PASSWORD] [SERVER_IP] KONTRON-SERVER-BASEBOARD:: [OID_SUB_GROUP] | grep "\.[TABLE_ENTRY_NUMBER] "** **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. RemoteComputer_OSPrompt:~# **snmpwalk -v3 -l [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [PASSWORD] [SERVER_IP] KONTRON-SERVER-BASEBOARD:: [OID_SUB_GROUP] | grep "[SENSOR_NAME]"**	
Step_2	Set the value of the desired threshold. RemoteComputer_OSPrompt:~# **snmpset -v3 -l [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [PASSWORD] [SERVER_IP] KONTRON-SERVER-BASEBOARD:: [THRESHOLD_OID].[SENSOR_ID_NUMBER] integer [NEW_VALUE]**	

Monitoring using Redfish

Refer to Accessing a BMC using Redfish for access instructions.

Creating URL extensions

Type	Sensors	URL extensions
Power sensor	• All sensors of type 02h (Voltage)	Chassis/Self/Power | jq
Thermal	• All sensors of type 01h (Temperature)	Chassis/Self/Thermal | jq ".Temperatures"
	• Fan1_speed • Fan2_speed • Fan3_speed • Fan4_speed	Chassis/Self/Thermal | jq ".Fans"
Health	• CPU Status	Managers/Self/HostInterfaces/Self | jq ".Status"
	• Health Status	Chassis/Self | jq ".Status"

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_EXTENTION]**	

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 .

Sensor name [Sensor_ID]	SNMP sensor number [Sensor_ID_number]	IPMI sensor number [Sensor_ID_number]	Sensor type code	Event / Reading type code	Description
PCI Error		23h	13h	6Fh	Various PCI/PCIe errors detected by BIOS (GenId:21)
Memory Error		24h	0Ch	6Fh	Various Memory errors detected by BIOS (GenId:21)
Processor Error		25h	07h	6Fh	Various Processor errors detected by BIOS (GenId:21)
Direct Memory Access (DMA) Error		26h	07h	6Fh	Various DMA errors detected by BIOS (GenId:21)
OutBound Traffic Controller (OTC) Error		27h	07h	6Fh	Various OTC errors detected by BIOS (GenId:21)
InBound Traffic Controller (ITC) Error		28h	07h	6Fh	Various ITC errors detected by BIOS (GenId:21)
Intel VT-d Error		29h	07h	6Fh	Various VT-d errors detected by BIOS (GenId:21)
FP NMI Diag Int	3	05h	13h	6Fh	
IPMI Watchdog	2	03h	23h	6Fh	IPMI Watchdog sensor
BMC Watchdog	6	0Ah	28h	03h	Management health watchdog
VR Watchdog	7	0Bh	02h	03h	
System Event Log	5	07h	10h	6Fh	
System Event	5	08h	12h	6Fh	
Front Panel Temp		21h	01h	01h	Temperature of front panel
P1 Temp	64	C7h	01h	01h	Processor 1 Temperature
P2 Temp	74	D2h	01h	01h	Processor 2 Temperature
P1 TJMAX	18	20h	01h	01h	Processor 1 Temperature: maximum temperature before thermal trip
P2 TJMAX	8	0Fh	01h	01h	Processor 2 Temperature: maximum temperature before thermal trip.
CPU Zone Temp	57	B5h	01h	01h	Temperature of CPU Zone
PCH Temp	17	1Eh	01h	01h	Temperature of PCH
BMC Temp	61	BAh	01h	01h	BMC Temperature
PCIe A Temp	59	B7h	01h	01h	PCIe A Temperature (J33 Extension cable) Managing extension probe
PCIe B Temp	60	B9h	01h	01h	PCIe B Temperature (J37 Extension cable) Managing extension probe
X557 LAN1 Temp	62	BBh	01h	01h	Temperature of X557 LAN 1
X557 LAN2 Temp	63	BCh	01h	01h	Temperature of X557 LAN 2
M.2 Temp	56	B4h	01h	01h	M.2 zone Temperature
Battery Temp	58	B6h	01h	01h	Temperature of Battery
P1 DIMMA1 Temp	65	C8h	01h	01h	Temp CPU1 DIMM Channel
P1 DIMMA2 Temp	66	C9h	01h	01h	Temp CPU1 DIMM Channel
P1 DIMMB1 Temp	67	CAh	01h	01h	Temp CPU1 DIMM Channel
P1 DIMMC1 Temp	68	CBh	01h	01h	Temp CPU1 DIMM Channel
P1 DIMMD1 Temp	69	CCh	01h	01h	Temp CPU1 DIMM Channel
P1 DIMMD2 Temp	70	CDh	01h	01h	Temp CPU1 DIMM Channel
P1 DIMME1 Temp	71	CEh	01h	01h	Temp CPU1 DIMM Channel
P1 DIMMF1 Temp	72	CFh	01h	01h	Temp CPU1 DIMM Channel
P2 DIMMA1 Temp	75	D3h	01h	01h	Temp CPU2 DIMM Channel

P2 DIMMA1 Temp	75	D3h	01h	01h	Temp CPU2 DIMM Channel
P2 DIMMA2 Temp	76	D4h	01h	01h	Temp CPU2 DIMM Channel
P2 DIMMB1 Temp	77	D5h	01h	01h	Temp CPU2 DIMM Channel
P2 DIMMC1 Temp	78	D6h	01h	01h	Temp CPU2 DIMM Channel
P2 DIMMD1 Temp	79	D7h	01h	01h	Temp CPU2 DIMM Channel
P2 DIMMD2 Temp	80	D8h	01h	01h	Temp CPU2 DIMM Channel
P2 DIMME1 Temp	81	D9h	01h	01h	Temp CPU2 DIMM Channel
P2 DIMMF1 Temp	82	DAh	01h	01h	Temp CPU2 DIMM Channel
P1 DIMMA1 T Mrgn		F0h	01h	01h	Temp Margening CPU1 DIMM Channel
P1 DIMMA2 T Mrgn		F1h	01h	01h	Temp Margening CPU1 DIMM Channel
P1 DIMMB1 T Mrgn		F2h	01h	01h	Temp Margening CPU1 DIMM Channel
P1 DIMMC1 T Mrgn		F3h	01h	01h	Temp Margening CPU1 DIMM Channel
P1 DIMMD1 T Mrgn		F4h	01h	01h	Temp Margening CPU1 DIMM Channel
P1 DIMMD2 T Mrgn		F5h	01h	01h	Temp Margening CPU1 DIMM Channel
P1 DIMME1 T Mrgn		F6h	01h	01h	Temp Margening CPU1 DIMM Channel
P1 DIMMF1 T Mrgn		F7h	01h	01h	Temp Margening CPU1 DIMM Channel
P2 DIMMA1 T Mrgn		AAh	01h	01h	Temp Margening CPU2 DIMM Channel
P2 DIMMA2 T Mrgn		ABh	01h	01h	Temp Margening CPU2 DIMM Channel
P2 DIMMB1 T Mrgn		ACh	01h	01h	Temp Margening CPU2 DIMM Channel
P2 DIMMC1 T Mrgn		ADh	01h	01h	Temp Margening CPU2 DIMM Channel
P2 DIMMD1 T Mrgn		AEh	01h	01h	Temp Margening CPU2 DIMM Channel
P2 DIMMD2 T Mrgn		AFh	01h	01h	Temp Margening CPU2 DIMM Channel
P2 DIMME1 T Mrgn		B0h	01h	01h	Temp Margening CPU2 DIMM Channel
P2 DIMMF1 T Mrgn		B1h	01h	01h	Temp Margening CPU2 DIMM Channel
Fan Failure	26	34h	04h	6Fh	Indicates a defective fan
Fan1 Speed	20	2Dh	04h	01h	Speed of fan #1 (RPM)
Fan2 Speed	21	2Eh	04h	01h	Speed of fan #2 (RPM)
Fan3 Speed	22	2Fh	04h	01h	Speed of fan #3 (RPM)
Fan4 Speed	23	30h	04h	01h	Speed of fan #4 (RPM)
Fan5 Speed	24	31h	04h	01h	Speed of fan #5 (RPM)
Fan6 Speed	25	32h	04h	01h	Speed of fan #6 (RPM)
Fan1 Present	33	61h	04h	08h	FAN1 presence state
Fan2 Present	34	62h	04h	08h	FAN2 presence state
Fan3 Present	35	63h	04h	08h	FAN3 presence state
Fan4 Present	36	64h	04h	08h	FAN4 presence state
Fan5 Present	37	65h	04h	08h	FAN5 presence state
Fan6 Present	38	66h	04h	08h	FAN6 presence state
Pwr Unit Redund	1	02h	09h	0Bh	Redundancy states of Power units
PS1 Status	13	1Ah	08h	6Fh	Status of Power supply 1
PS2 Status	14	1Bh	08h	6Fh	Status of Power supply 2
PS1 Input Power	9	16h	08h	01h	Input power of Power supply 1
PS2 Input Power	10	17h	08h	01h	Input power of Power supply 2
PS1 Output Power	15	1Ch	08h	01h	Output power of Power supply 1

PS2 Output Power	16	1Dh	08h	01h	Output power of Power supply 2
PS1 Temp	11	18h	01h	01h	Temperature of Power supply 1
PS2 Temp	12	19h	01h	01h	Temperature of Power supply 2
CPU ERR2	39	7Ch	07h	03h	Catastrophic error sensor
CATERR	40	80h	07h	03h	Catastrophic error sensor
CPU Missing	41	82h	07h	03h	Processor presence state
P1 Status	86	EDh	07h	6Fh	Processor 1 status
P2 Status	87	EEh	07h	6Fh	Processor 2 status
P1 DTS Thrm Mrgn	83	DBh	01h	01h	Thermal margin before Processor 1 Thermal trip
P2 DTS Thrm Mrgn	84	DCh	01h	01h	Thermal margin before Processor 2 Thermal trip
Voltage Fault	73	D1h	02h	01h	Voltage fault status
V_2V5_AUX_X557	42	91h	02h	01h	2.5V AUX Voltage
V_2V1_AUX_X557	43	92h	02h	01h	2.1V AUX Voltage
V_1V2_AUX_X557	44	93h	02h	01h	1.2V AUX Voltage
V_0V83_AUX_X557	45	94h	02h	01h	0.83V AUX Voltage
V_VNN_PCH_AUX	46	95h	02h	01h	VNN PCH AUX Voltage
V_1V05_PCH_AUX	47	96h	02h	01h	1.05V PCH AUX Voltage
V_1V8_PCH_AUX	48	97h	02h	01h	1.8V PCH AUX Voltage
V_1V18_AUX	49	98h	02h	01h	1.18V AUX Voltage
V_2V5_AUX	50	99h	02h	01h	2.5V AUX Voltage
V_3V3_AUX	51	9Ah	02h	01h	3.3V AUX Voltage
V_5V_AUX	52	9Bh	02h	01h	5V AUX Voltage
V_3V3	53	9Ch	02h	01h	3.3V Voltage
V_5V	54	9Dh	02h	01h	5V Voltage
V_12V	55	9Eh	02h	01h	12V Voltage
V_3V_BAT	85	DEh	02h	01h	3V battery voltage
HDD0 Status	27	50h	0Dh	6Fh	HDD0 Presence status
HDD1 Status	28	51h	0Dh	6Fh	HDD1 Presence status
HDD2 Status	29	52h	0Dh	6Fh	HDD2 Presence status
HDD3 Status	30	53h	0Dh	6Fh	HDD3 Presence status
HDD4 Status	31	54h	0Dh	6Fh	HDD4 Presence status
HDD5 Status	32	55h	0Dh	6Fh	HDD5 Presence status
CPU Error		EFh	07h	6Fh	IERR and MCE
Board Status		0Ch	C4h	6Fh	Board reset type and sources
Power State		0Dh	D1h	6Fh	Actual chassis power state
PWROK Capture 1		12h	08h	6Fh	Latched power rail status
PWROK Capture 2		13h	08h	6Fh	Latched power rail status
Ver Change FPGA		25h	2Bh	6Fh	FPGA Firmware Change Detection
Ver Change BMC		27h	2Bh	6Fh	BMC Firmware Change Detection

Interpreting sensor data

{This article describes how to interpret sensor data.}

Table of contents

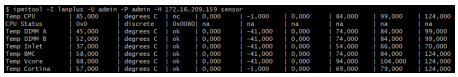
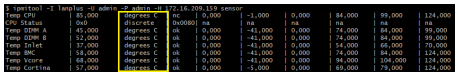
Interpretation procedure

Before beginning the interpretation procedure, make sure to collect the following event information:

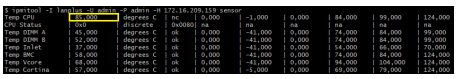
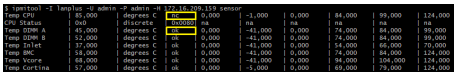
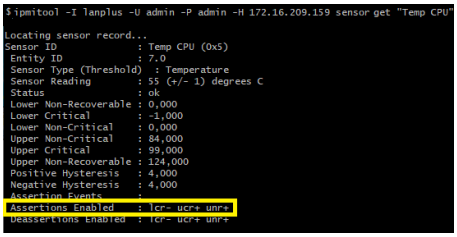
- Event ID
- Associated sensor
- Description

Refer for System event log for instructions.

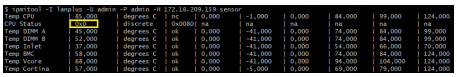
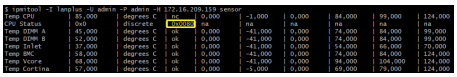
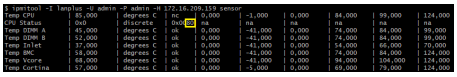
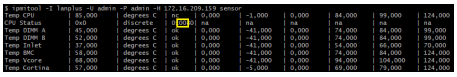
NOTE: IOL and IPMI/KCS are the preferred methods for interpretation.

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 [Content under creation] Interpreting non-discrete sensor data or [Content under creation] 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 [Content under creation] 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. RemoteComputer_OSPrompt:~$ **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] sensor get [Sensor_ID]**	

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 [Content under creation] 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 [Content under creation] Accessing event data byte 2 for additional information.	

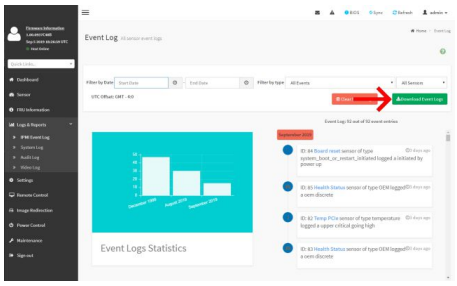
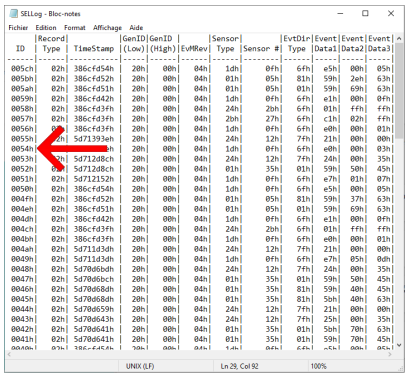
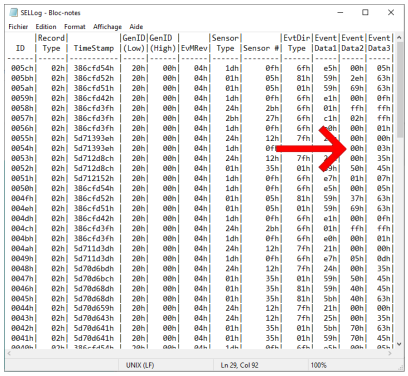
Accessing event data byte 2 and 3 (optional)

NOTE: This part of the procedure is needed only if the sensor concerned specifies it. Refer to [Content under creation] Sensor event/reading type .
Even data can be obtained:

- Using the [Content under creation] BMC Web UI
- Using [Content under creation] IPMI

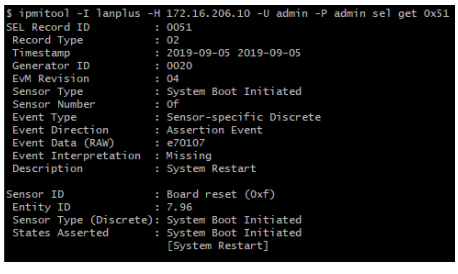
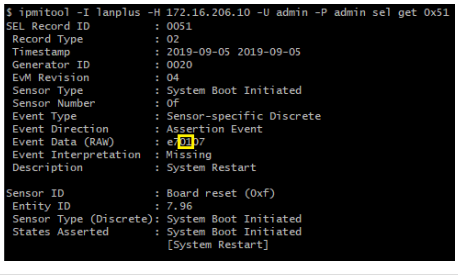
A ccessing event data byte 2 using the BMC Web UI

Refer to [Content under creation] Accessing a BMC using the Web UI 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 [Content under creation] Event data byte 2 to interpret the event data byte.	

Accessing event data byte 2 using IPMI

The following procedures will be executed using the [Content under creation] Accessing a BMC using IPMI over LAN (IOL) method, but some tasks can also be performed using KCS ([Content under creation] Accessing a BMC using IPMI via KCS). 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_2	Print the event's detailed information using the hexadecimal conversion of the ID. RemoteServer_OSPrompt:~$ **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] sel get [Event_ID]**	
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 [Content under creation] Event data byte 2 to interpret the event data byte.	

Interpretation information

Each sensor has a [Content under creation] Sensor type attribute and a [Content under creation] Sensor event/reading type attribute. When a sensor created an event

specified, more data about the event can be found in [Content under creation] 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.

Sensor type	Description
01h (Temperature)	General information about temperatures of different components.
02h (Voltage)	General information about voltages either on the board or the power supply.
04h (Fan)	General information about the fan(s) of the platform (e.g. speed, presence, failure).
07h (Processor)	General information about the processor (e.g. presence, failure, health status).
08h (Power supply)	General information about the power supply (e.g. presence, failure, health status).
09h (Power Unit)	General information about the power unit.
0Ch (Memory)	General information about the memory (error).
0Dh (Drive Slot/Bay)	General information about storage devices slots and bay.
10h (Event logging disabled)	General information about the platform disabled system event log.
12h (System Event)	General information about the system events.
13h (Critical Interrupt)	General information about the critical interrupts on the system.
23h (Watchdog2)	General information about the IPMI watchdog.
28h (Management Subsys Health)	General information about the management subsystem health (BMC).
2Bh (Version Change)	Detection of firmware change (FPGA and BMC).
C4h (OEM board reset)	Kontron custom board reset type and sources sensor.
D1h (OEM Power State)	Kontron custom power state sensor.

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.

Event/reading type	7-bit event type code	Description	Offset
Threshold based	01h	Non-discrete, meaning it has a numerical reading and event triggers.	Offsets are standard and defined in the [Content under creation] Threshold based event/reading type table.
Sensor-specific	6Fh	Discrete, meaning it has no numerical values, but it has event triggers.	Offsets are specific to the sensor's type and defined in the [Content under creation] Sensor-specific event/reading type 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.

Event offset	Event trigger	State
00h	Lower noncritical - going low	nc
01h	Lower noncritical - going high	
02h	Lower critical - going low	cr
03h	Lower critical - going high	
04h	Lower non-recoverable - going low	nr
05h	Lower non-recoverable - going high	
06h	Upper noncritical - going low	nc
07h	Upper noncritical - going high	
08h	Upper critical - going low	cr
09h	Upper critical - going high	
0Ah	Upper non-recoverable - going low	nr
0Bh	Upper non-recoverable - going high	

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.

ID	Sensor name	Sensor type	Specific offset	Event trigger/state
23h	PCI Error **NOTE:** See SMI Handler generated event data table below for more information.	13h (Critical Interrupt)	04h	PCI PERR
			05h	PCI SERR
			07h	Bus Correctable Error
			08h	Bus Uncorrectable Error
			0Ah	Bus Fatal Error
			0Fh	LastBoot PCIe Error
24h	Memory Error **NOTE:** See SMI Handler generated event data table below for more information.	0Ch (Memory)	00h	Correctable ECC / Other correctable memory error
			01h	Uncorrectable ECC / other uncorrectable memory error
			02h	Parity
			05h	Correctable ECC / other correctable memory error logging limit reached
25h	Processor Error **NOTE:** See SMI Handler generated event data table below for more information.	07h (Processor)	05h	Configuration Error
26h	Direct Memory Access (DMA) Error **NOTE:** See SMI Handler generated event data table below for more information.	07h (Processor)	05h	Configuration Error
27h	OutBound Traffic Controller (OTC) Error **NOTE:** See SMI Handler generated event data table below for more information .	07h (Processor)	05h	Configuration Error
28h	InBound Traffic Controller (OTC) Error **NOTE:** See SMI Handler generated event data table below for more information.	07h (Processor)	05h	Configuration Error
29h	Intel VT-d Error **NOTE:** See SMI Handler generated event data table below for more	07h (Processor)	05h	Configuration Error

	for more information.			
05h	FP NMI Diag Int	13h (Critical Interrupt)	00h	07h (Processor)
34h	Fan Failure	04h (Fan)	00h	Failure reported on fan #1
			...	
			05h	Failure reported on fan #6
03h	IPMI Watchdog **NOTE:** See BIOS generated event data table below for more information.	23h(Watchdog2)	00h	Timer expired
			01h	Hard reset
			02h	Power down
			03h	Power Cycle
			08h	Timer interrupt
07h	System Event Log	10h(Event Logging Disabled)	02h	System event log cleared
			04h	System event log full
			05h	System event log almost full
08h	System Event **NOTE:** See event data table below for more information.	12h(System Event)	04h	[PEF Action
			05h	Timestamp Clock Sync
18h	P1 Status	07h (Processor)	01h	Thermal trip
19h	P2 Status		0Ah	Throttled
50h	HDD0 Status	0Dh(Drive Slot / Bay)	00h	Drive Presence
51h	HDD1 Status			
52h	HDD2 Status			
53h	HDD3 Status			
54h	HDD4 Status			
55h	HDD5 Status			
0Ch	Board Status **NOTE:** See event data table below for more information.	C4h (OEM board reset)	00h	Push Button
			02h	Unknown
			06h	Cold Reset
			07h	IPMI Command
			09h	Power Up Reset
			0Ah	Power Down
0Dh	Power State	D1h (OEM Power State)	00h	Power ON
			01h	Power OFF
			02h	Power ON Request
			03h	Power OFF Request
			04h	Full Reset In Progress
12h	PWROK Capture 1	08h (Power supply)	00h	Power supply presence detected
13h	PWROK Capture 2		01h	Power supply failure detected
25h	Ver Change FPGA	2Bh (Version Change)	01h	Firmware change detected
27h	Ver Change BMC			

EFh	CPU Error	07h (Processor)	00h	IERR
			0Bh	Machine Check Exception

Other event/reading types

ID	Sensor name	Sensor type	Specific offset	Event trigger/state
0Ah	BMC Watchdog	03h ('digital' Discrete - Assert/Deassert)	01h	State asserted
0Bh	VR Watchdog			
7Ch	CPU ERR2			
80h	CATERR			
82h	CPU Missing			
61h	Fan1 Present	08h ('digital' Discrete - Present/Absent)	00h	Device absent
62h	Fan2 Present			
63h	Fan3 Present			
64h	Fan4 Present		01h	Device present
65h	Fan5 Present			
66h	Fan6 Present			
02h	Pwr Unit Redund	0Bh (Discrete)	00h	Fully Redundant
			01h	Redundancy Lost
			03h	Non-Redundant: Sufficient from Redundant
			04h	Non-Redundant: Sufficient from Insufficient
			05h	Non-Redundant: Insufficient Resources

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.

ID	Sensor	Specific offset	Event data 2
03h	IPMI Watchdog	• 00h • 01h • 02h • 03h • 08h	[7:4] - Interrupt type: • 0x00 = None • 0x10 = SMI • 0x20 = NMI • 0x30 = Messaging interrupt • 0xF0 = Unspecified [3:0] - Timer use at expiration: • 0x00 = Reserved • 0x01 = BIOS/FRB2 • 0x02 = BIOS/POST • 0x03 = OS load • 0x04 = SMS/OS • 0x05 = OEM • 0x0F = Unspecified
08h	System Event	• 04h PEF Action	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. [7:6] - reserved [5] - 1b = Diagnostic Interrupt (NMI) [4] - 1b = OEM action [3] - 1b = power cycle [2] - 1b = reset [1] - 1b = power off [0] - 1b = Alert
		• 05h Timestamp Clock Synch.	This event can be used to record when changes are made to the timestamp clock(s) so that relative time differences between SEL entries can be determined. [7] - first/second • 0x0 = event is first of pair. • 0x1 = event is second of pair. [6:4] - reserved [3:0] - Timestamp Clock Type • 0x0 = SEL Timestamp Clock updated. (Also used when both SEL and SDR Timestamp clocks are linked together.) • 0x1 = SDR Timestamp Clock updated.
0Ch	Board Status	• 00h • 02h • 06h • 07h	Report additional information about the reset type: Specific offset 00h: • 0x02 = Push button reset Specific offset 02h: • 0x04 = Straight to S5 condition • 0x0d = Serial port reset • All others = Unknown reset cause Specific offset 06h: • 0x05 = Cold reset without power cycle • 0x0F = Cold reset with power cycle Specific offset 07h: • 0x01 = Power reset IPMI command
25h	Ver Change FPGA	• 01h	• 0x11 Version change type is FPGA.
27h	Ver Change BMC	• 01h	• 0x02 Version change type is BMC.

SMI Handler generated event data bytes 2 and 3 description

This table defines the event data bytes 2 and 3 for OEM-defined sensors generated from the BIOS SMI Handler (Generator ID = 0x21).

ID	Sensor	Sensor type	Specific offset	Event data 2	Event data 3
23h	PCI Error	13h (Critical Interrupt)	• 04h • 05h • 07h • 08h • 0Ah	[7:0] - PCI bus number for failed device	[7:3] - PCI device number for failed device [2:0] - PCI function number for failed device
24h	Memory Error	0Ch (Memory)	• 00h • 01h • 02h • 05h	[2:1] - Memory Controller Number: • 0x0 = Memory Controller 0 for channels A, B, C • 0x1 = Memory Controller 1 for channels D, E, F [0] - Current/Last Boot Error: • 0x0 = Current Boot • 0x1 = Last Boot	[7:6] - CPU Socket Number: • 0x0 = CPU1 • 0x1 = CPU2 [5:4] - Channel Number: • 0x0 = Channel A if Memory Controller 0 Channel D if Memory Controller 1 • 0x1 = Channel B if Memory Controller 0 Channel E if Memory Controller 1 • 0x2 = Channel C if Memory Controller 0 Channel F if Memory Controller 1 [3:0] - DIMM Number: • 0x0 = DIMM 1 • 0x1 = DIMM 2
25h	Processor Error	07h (Processor)	• 05h	[7:4] - CPU Socket Number: • 0x0 = CPU1	[7:4] - Processor Error Type: • 0x0 = UNKNOWN • 0x1 = Cache

				• 0x0 = CPU1 • 0x1 = CPU2 [3:0] = Bank Type: • 0x0 = None • 0x1 = IFU • 0x2 = DCU • 0x3 = DTLB • 0x4 = MLC • 0x5 = PCU • 0x6 = IIO • 0x7 = CHA • 0x8 = UPI	• 0x1 = Cache • 0x2 = TLB (Translation Look aside Buffer) • 0x4 = Bus • 0x8 = Micro Architecture [3:1] = Error Severity: • 00 = Correctable Error • 01 = Fatal Error • 02 = Corrected Error [0] - Current/Last Boot Error: • 0x0 = Current Boot • 0x1 = Last Boot
26h	Direct Memory Access (DMA) Error	07h (Processor)	• 05h	[7:4] - CPU Socket Number: • 0x0 = CPU1 • 0x1 = CPU2 [3:1] - CPU Stack Number [0] - Current/Last Boot Error: • 0x0 = Current Boot • 0x1 = Last Boot	[7:0] - Direct Memory Access Error codes as per Skylake-EP EDS Specification: • 40h = Received_Poisoned_Data_from_DP_status 41h = DMA_internal_HW_parity_error_status 42h = Cfg_Reg_Parity_Error_status 43h = RD_Cmpl_Header_Error_status 44h = Read_address_decode_error_status 45h = Multiple errors 46h = DMA Transfer Source Address Error. 47h = DMA Transfer Destination Address Error. 48h = Next Descriptor Address Error. 49h = Error when reading a DMA descriptor 4Ah = Chain Address Value Error. 4Bh = CHANCMD Error 4Ch = Data Parity Error 4Dh = DMA Data Parity Error. 4Eh = Read Data Error. 4Fh = Write Data Error. 50h = Descriptor Control Error. 51h = Descriptor Length Error. 52h = Completion Address Error. 53h = Interrupt Configuration Error. 54h = CRC or XOR P Error 55h = XOR Q Error 56h = Descriptor Count Error 57h = DIF All F Detect Error 58h = DIF Guard Tag Error 59h = DIF Application Tag Error 5Ah = DIF Reference Tag Error 5Bh = DIF Bundle Error
27h	OutBound Traffic Controller (OTC) Error	07h (Processor)	• 05h	[7:4] - CPU Socket Number: • 0x0 = CPU1 • 0x1 = CPU2 [3:1] - CPU Stack Number [0] - Current/Last Boot Error: • 0x0 = Current Boot • 0x1 = Last Boot	[7:0] - Outbound Traffic Controller Error codes as per Skylake-EP EDS Specification: • 60h = OTC OB credit underflow 61h = OTC OB credit overflow 62h = Parity error in the OTC hdr_q RF 63h = Parity error in the OTC addr_q RF 64h = ECC uncorrected error in the OTC dat_dword RF 65h = Completer abort 66h = Master abort 67h = Multicast target error for ITC 68h = ECC corrected error in the OTC dat_dword RF 69h = Misc block request overflow 6Ah = IOAPIC RTE parity error 6Bh = Parity error on incoming data from IRP 6Ch = Parity error on incoming addr from IRP
28h	Inbound Traffic Controller (ITC) Error	07h (Processor)	• 05h	[7:4] - CPU Socket Number: • 0x0 = CPU1 • 0x1 = CPU2 [3:1] - CPU Stack Number [0] - Current/Last Boot Error: • 0x0 = Current Boot • 0x1 = Last Boot	[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
29h	Intel VT-d Error	07h (Processor)	• 05h	[7:4] - CPU Socket Number: • 0x0 = CPU1 • 0x1 = CPU2 [3:1] - CPU Stack	[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

				Number [0] - Current/Last Boot Error: • 0x0 = Current Boot • 0x1 = Last Boot	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

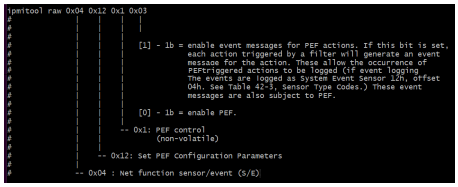
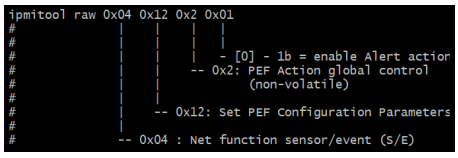
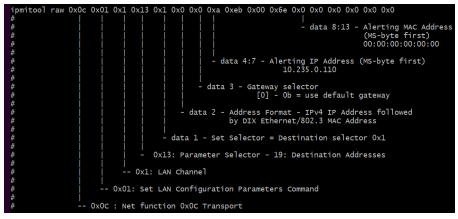
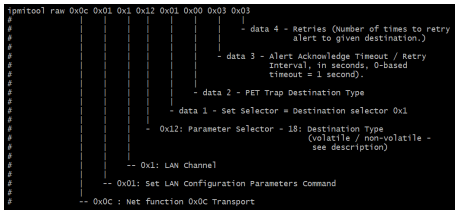
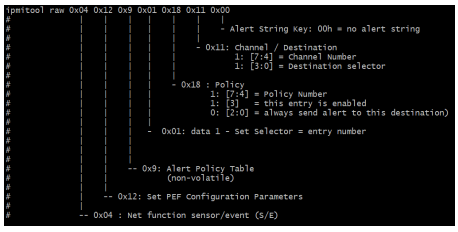
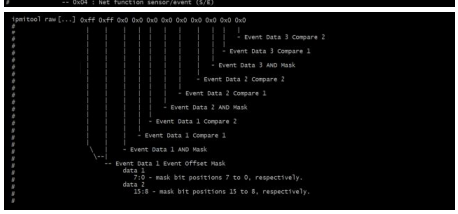
Setting up SNMP alarms using IPMI

The following procedures will be executed using the Accessing a BMC using IPMI (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]** .

NOTE: It is stronly 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 additionnal 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** **NOTE:** A maximum of 16 event filter can be configured.	 

Alarm setup examples

Detecting an HDD removal

- Event filter: 15

- Alert policy: 1
- Severity: informational

```
LocalServer_OSPrompt:~# ipmitool raw 0x04 0x12 0x6 0x0f 0x80 0x1 0x1 0x02 0xff 0xff 0xd 0xff 0xff 0x1 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
```

Detecting a fan removal

- Event filter: 14
- Alert policy: 1
- Severity: critical

```
LocalServer_OSPrompt:~# i pmitool raw 0x04 0x12 0x6 0x0e 0x80 0x1 0x1 0x10 0xff 0xff 0x4 0xff 0x8 0x1 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
```

Detecting an AC or DC power lost

- Event filter: 13
- Alert policy: 2
- Severity: critical

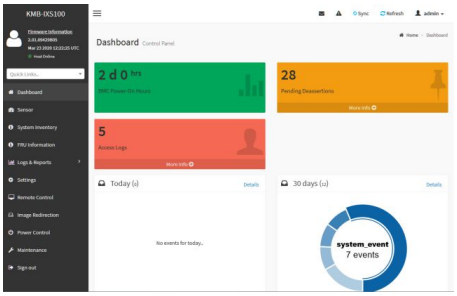
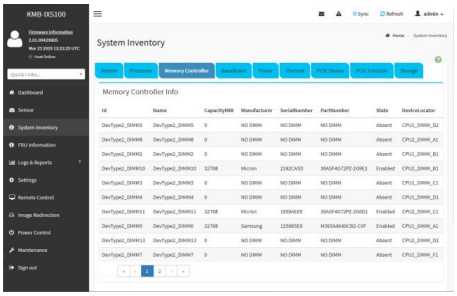
```
LocalServer_OSPrompt:~# ipmitool raw 0x04 0x12 0x6 0x0d 0x80 0x1 0x1 0x10 0xff 0xff 0x9 0xff 0xb 0xff 0xff 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
```

System Inventory

The System Inventory provides information about the CPUs, memory DIMMS, storage, sensors, etc.

Accessing Inventory

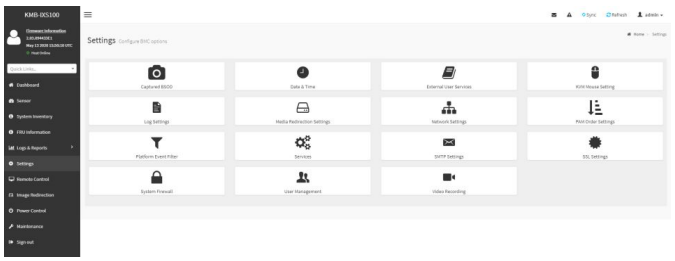
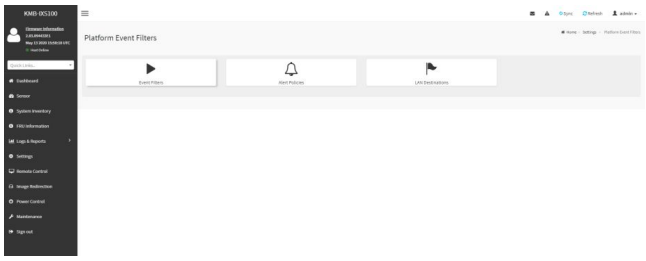
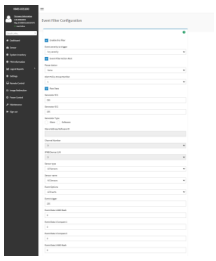
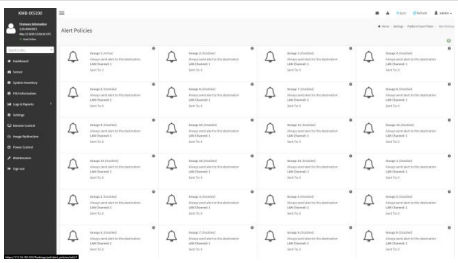
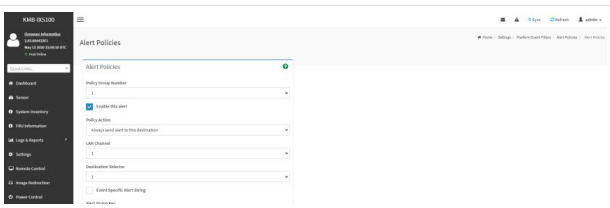
Refer to [Content under creation] Accessing a BMC using the Web UI for access instructions.

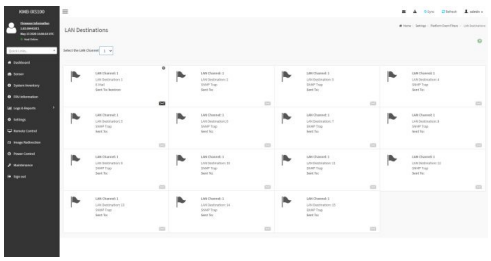
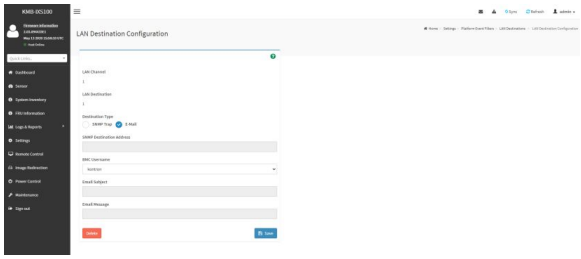
Step_1	Access the BMC Web UI.	
Step_2	From the left-side menu, click on **System Inventory** .	
Step_3	The system inventory will be displayed.	

Configuring and using SNMP traps in WebUI

Setting up SNMP traps in WebUI

The following procedures will be executed using the WebUI method.

Step_1	Go to Settings→ Platform Event Filter	
Step_2	Go to Event Filters	
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 Poilcies under Settings → Platform Envent 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_8	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 independant Power alarm indicator.

CG00100

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.

```
# ipmitool raw 0x3c 0x0B 0x00 0x00
                  |  ---------  |
                  |      |      -- Get TAM configuration
                  |      |
                  |      -- TAM command
                  |
                  -- Network Function (netfn): OEM command
```

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 0x01 [TAM Parameter]
                  |  ---------  |        |
                  |      |      |        -- Configuration byte
                  |      |      |
                  |      |      -- Set TAM configuration
                  |      |
                  |      -- TAM command
                  |
                  -- Network Function (netfn): OEM command
```

Configuration Byte

Bit position	Description	Values
[0]	Enable/Disable	0: The Telco Alarm Manager feature is **disabled** . The four indicators can be controlled by the user with a dedicated IPMI command. 1: The Telco Alarm Manager feature is **enabled** (default).
[1]	Telco Alarm Model	0: **'All Severities Only'** model. 1: **'Most Severe Only'** model (default).
[2-7]	Unused	

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

{This article explains how to view system logs, how to replace, backup and restore components, and how to upgrade and scale the platform. }

Children

- System event log
- Components replacement
- BIOS backup and restore
- Upgrading
- [Content under creation] Scaling

System event log

{This article gives step-by-step instructions to view and manage system event logs.}

Table of contents

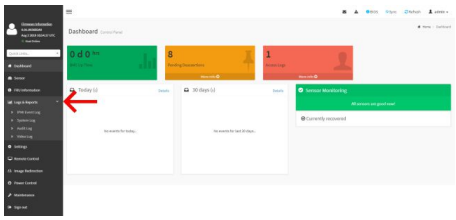
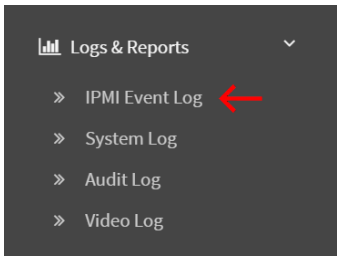
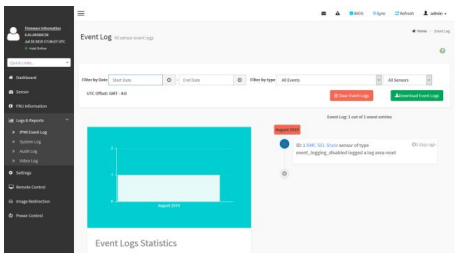
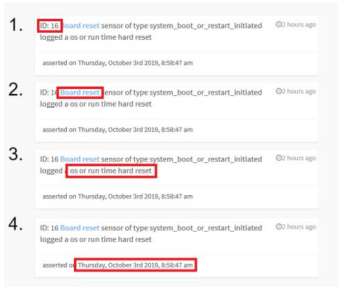
The system event log can be accessed:

- Using the [Content under creation] BMC Web UI
- Using [Content under creation] IPMI
- Using Redfish

Accessing the SEL using the BMC Web UI

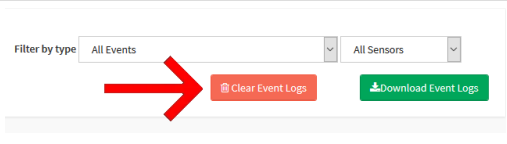
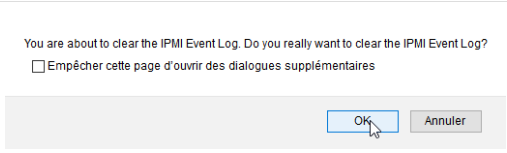
Accessing the system event log

Refer to Accessing a BMC using the Web UI for access instructions.

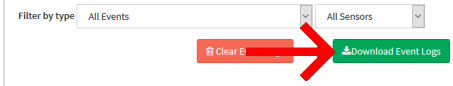
Step_1	Access the BMC Web UI of the server.	
Step_2	Select **Logs & Reports** from the left side menu.	
Step_3	Select **IPMI Event Log** from the dropdown menu.	
Step_4	The system event log is displayed.	
Step_5	Click on an event and collect the following information: 1. Event ID 2. Associated sensor 3. Description 4. Time asserted	

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** .	

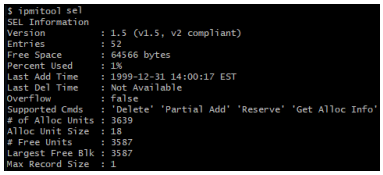
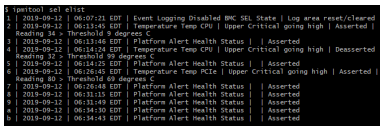
Downloading the system event log

Step_1	In the **Event Log** menu, select **Download Event Logs** .	

Accessing the SEL using IPMI via KCS

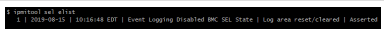
The following procedures will be executed using the Accessing a BMC using IPMI (KCS) method, but some configurations can also be performed using IOL (Accessing a BMC using IPMI over LAN (IOL)). To use IOL, add the IOL parameters to the command: **-I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI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

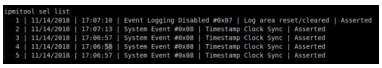
Step_1	From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, c lear the system event log. LocalServer_OSPrompt:~# **ipmitool sel clear**	
Step_2	Verify that the system event log was properly cleared. LocalServer_OSPrompt:~# **ipmitool sel elist**	

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.



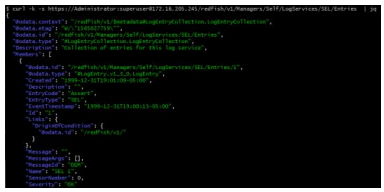
This behavior has been observed with the latest version of ipmitool (1.8.18) released to date. However, the latest unreleased version fixes the issue.
To get latest unreleased version:

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

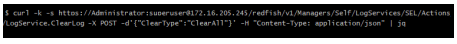
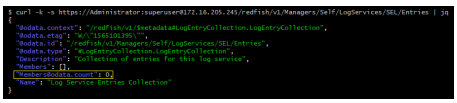
Accessing the system event log

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 a ccess 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 c lear the system event log. RemoteComputer_OSPrompt:~# **curl -k -s [ROOT_URL]Managers/Self/LogServices/SEL/Actions/LogService.ClearLog -X POST -d'{"ClearType":"ClearAll"}' -H "Content-Type: application/json" | jq**
	
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.}

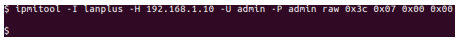
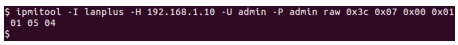
To replace a component on a CG2400 platform, refer to Components installation and assembly .

BIOS backup and restore

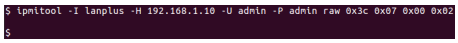
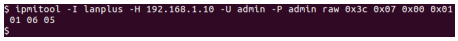
Table of contents

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 [Content under creation] 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.

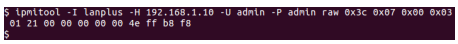
Backing up the BIOS

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 [Content under creation] 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 [Content under creation] 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-BYTE5] version: • [1B] Major • [1B] Minor • [4B] Aux [BYTE6] Status [BYTE7-BYTE10] Unix timestamp In the image, the version is **1.33.00000000** , the status is **0x00** and the timestamp is **1325381880** .	

Description of creation and restoration steps

Step description	Step value (BYTE1)	Details
Snapshot validation	0x00	Check if the saved snapshot is valid for restoration.
Check BIOS end of POST	0x01	Check if BIOS is valid and booted before creating a snapshot.
MTD partition detect	0x02	Check if the Flash device and partition are detected.
Server Power Off	0x03	Set server to Power Off state.
Force Intel ME Recovery mode	0x04	Force Intel ME to recovery mode.
Snapshot MTD Flash erase	0x05	Erasing of the snapshot flash. Erase progress in percent (%) available in [BYTE2] of get status command (0x01).
Snapshot MTD Flash write	0x06	Writing of the snapshot flash. Writing progress in percent (%) available in [BYTE2] of get status command (0x01).
Snapshot MTD Flash verify	0x07	Verifying of the snapshot flash. Verifying progress in percent (%) available in [BYTE2] of get status command (0x01).
Reset Intel ME to Normal mode	0x08	Reset Intel ME to return to normal mode.

Upgrading

{This article provides detailed instructions to safely upgrade the platform's components. }
Table of contents

General considerations

You may have been informed by Kontron that your running system would benefit from the latest firmware upgrades. Furthermore, n ewer 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 [Content under creation] BMC and the FPGA using ipmitool – recommended
- Upgrading the [Content under creation] BIOS and 10GbE LAN

Upgrading the BMC and the FPGA using ipmitool

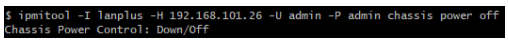
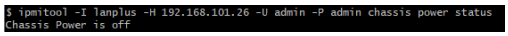
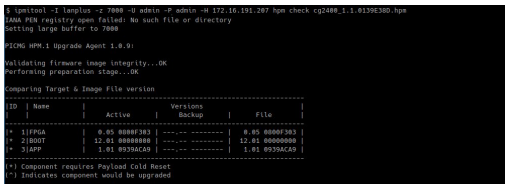
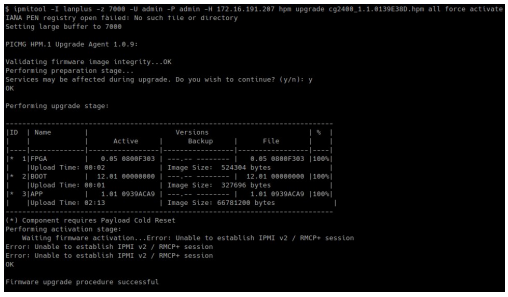
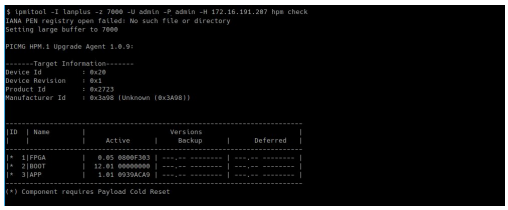
The following procedure will upgrade the BMC and FPGA at the same time.

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, e nter the desired command. RemoteComputer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power off** **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. RemoteComputer_OSPrompt:~# **ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] chassis power status**	
Step_3	Verify that the upgrade version is adequate. RemoteComputer_OSPrompt:~# **ipmitool -z 7000 -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] hpm check <HPM bundle(HPM file)>**	
Step_4	Proceed with firmware upgrade. RemoteComputer_OSPrompt:~# **ipmitool -z 7000 -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] hpm upgrade <HPM bundle(HPM file) > all activate** **NOTE:** W ait 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. RemoteComputer_OSPrompt:~# **ipmitool -z 7000 -I lanplus -H [BMC MNGMT_IP] -U [IPMI_USER_NAME] -P [IPMI_PASSWORD] hpm check**	

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 cyle 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 [Content under creation] BIOS
- Upgrading the [Content under creation] 10GbE LAN

Upgrading the BIOS

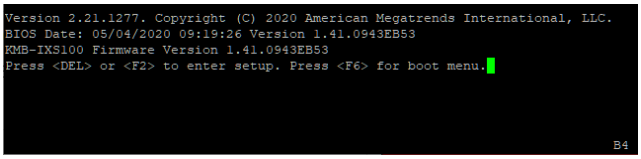
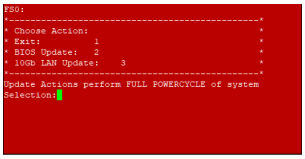
Step_1	From an OS command prompt, start the upgrade process. **sudo bash ./bios-update.sh**
Step_2	Follow the instructions on screen until the upgrade process is finished. Note that the system will reboot a few times.

Upgrading the 10GbE LAN

Step_1	From an OS command prompt, start the upgrade process. **sudo bash ./lan-update.sh**
Step_2	Follow the instructions on screen until the upgrade process is finished.

USB key method

This method requires a physical access to the system.

Step_1	Uncompress and copy files to the root of a USB key formatted as FAT32.	
Step_2	Insert the USB key in the CG2400, using the front or rear USB port of the CG2400 platform.	
Step_3	Reset the system. See Platform power management for reset methods.	
Step_4	When the system has restarted, press F6 to activate the boot menu and select USB key. **NOTE:** You can also press F2 or DEL, enter the BIOS menu, go to the **Save & Exit** tab and select the USB key under Boot Override. Do not press <ESC>. This will bring you in the EFI shell, thus requiring to reboot the CG2400 again to boot from the USB key.	
Step_5	A menu will appear. Select what you want to do: • Exit (press 1) • Update BIOS (press 2) • Update 10Gb LAN (press 3) **NOTE:** The system will perform a full power cycle after updating the BIOS or the 10Gb LAN.	

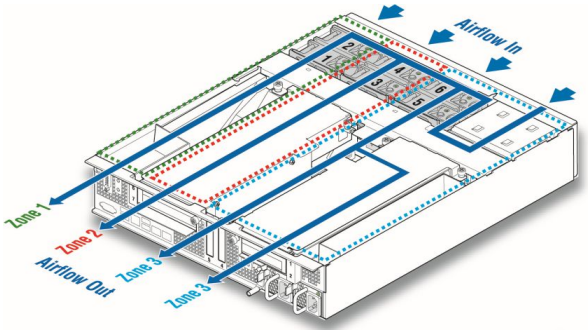
Platform cooling and thermal management

{This article provides informations about platform cooling and thermal management mechanism and describes specific behavior across platform operating temperature range.}

Table of contents

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.



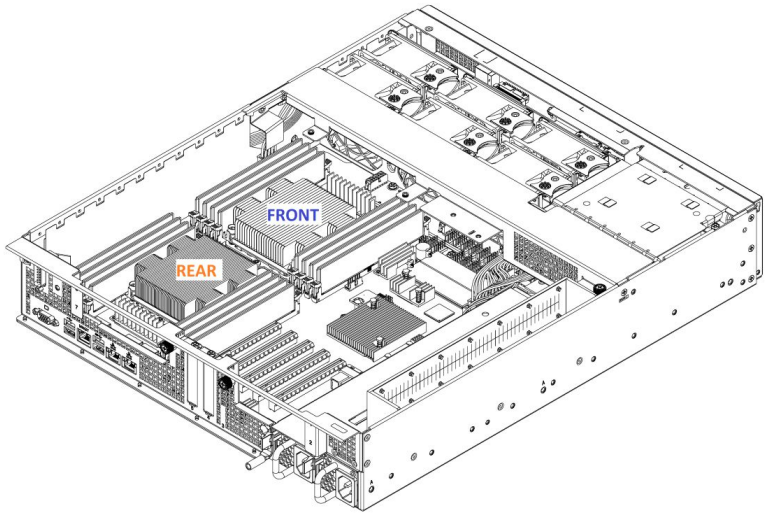
The CG2400 platform has six 80 mm x 38 mm fans, configured as three redundant pairs. There are three cooling zones delimited by the colored dotted lines in the figure above.

- 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

ID(hex)	Sensor	Description	Sensor type	Event/reading type code
21h	Front Panel Temp	Temperature of front panel	Temperature (0x01)	0x01 (Threshold Based)
C7h	P1 Temp	Processor 1 Temperature	Temperature (0x01)	0x01 (Threshold Based)
D2h	P2 Temp	Processor 2 Temperature	Temperature (0x01)	0x01 (Threshold Based)
20h	P1 TJMAX	Processor 1 Temperature maximum temperature/thermal trip (throttling) point.	Temperature (0x01)	0x01 (Threshold Based)
0Fh	P2 TJMAX	Processor 2 Temperature maximum temperature/thermal trip (throttling) point.	Temperature (0x01)	0x01 (Threshold Based)
B5h	CPU Zone Temp	Temperature of CPU Zone	Temperature (0x01)	0x01 (Threshold Based)
1Eh	PCH Temp	Temperature of PCH	Temperature (0x01)	0x01 (Threshold Based)
BAh	BMC Temp	Temperature of BMC	Temperature (0x01)	0x01 (Threshold Based)
B7h	PCIe A Temp	Temperature of PCIe A (optional Thermal Probe cable*)	Temperature (0x01)	0x01 (Threshold Based)
B9h	PCIe B Temp	Temperature of PCIe B (optional Thermal Probe cable*)	Temperature (0x01)	0x01 (Threshold Based)
BBh	X557 LAN1 Temp	Temperature of X557 LAN 1	Temperature (0x01)	0x01 (Threshold Based)
BCh	X557 LAN2 Temp	Temperature of X557 LAN 1	Temperature (0x01)	0x01 (Threshold Based)
B4h	M.2 Temp	Temperature of M.2 Zone	Temperature (0x01)	0x01 (Threshold Based)
B6h	Battery Temp	Temperature of Battery	Temperature (0x01)	0x01 (Threshold Based)
C8h	P1 DIMMA1 Temp	Temperature of Processor 1 DIMM Channel	Temperature (0x01)	0x01 (Threshold Based)
C9h	P1 DIMMA2 Temp	Temperature of Processor 1 DIMM Channel	Temperature (0x01)	0x01 (Threshold Based)
CAh	P1 DIMMB1 Temp	Temperature of Processor 1 DIMM Channel	Temperature (0x01)	0x01 (Threshold Based)
CBh	P1 DIMMC1 Temp	Temperature of Processor 1 DIMM Channel	Temperature (0x01)	0x01 (Threshold Based)
CCh	P1 DIMMD1 Temp	Temperature of Processor 1 DIMM Channel	Temperature (0x01)	0x01 (Threshold Based)
CDh	P1 DIMMD2 Temp	Temperature of Processor 1 DIMM Channel	Temperature (0x01)	0x01 (Threshold Based)
CEh	P1 DIMME1 Temp	Temperature of Processor 1 DIMM Channel	Temperature (0x01)	0x01 (Threshold Based)
CFh	P1 DIMMF1 Temp	Temperature of Processor 1 DIMM Channel	Temperature (0x01)	0x01 (Threshold Based)
D3h	P2 DIMMA1 Temp	Temperature of Processor 2 DIMM Channel	Temperature (0x01)	0x01 (Threshold Based)
D4h	P2 DIMMA2 Temp	Temperature of Processor 2 DIMM Channel	Temperature (0x01)	0x01 (Threshold Based)
D5h	P2 DIMMB1 Temp	Temperature of Processor 2 DIMM Channel	Temperature (0x01)	0x01 (Threshold Based)
D6h	P2 DIMMC1 Temp	Temperature of Processor 2 DIMM Channel	Temperature (0x01)	0x01 (Threshold Based)
D7h	P2 DIMMD1 Temp	Temperature of Processor 2 DIMM Channel	Temperature (0x01)	0x01 (Threshold Based)
D8h	P2 DIMMD2 Temp	Temperature of Processor 2 DIMM Channel	Temperature (0x01)	0x01 (Threshold Based)
D9h	P2 DIMME1 Temp	Temperature of Processor 2 DIMM Channel	Temperature (0x01)	0x01 (Threshold Based)
DAh	P2 DIMMF1 Temp	Temperature of Processor 2 DIMM Channel	Temperature (0x01)	0x01 (Threshold Based)
34h	Fan Failure	Current FANs Failure status	Fan (0x04)	0x4
2Dh	Fan1 Speed	Current FAN 1 Speed (RPM)	Fan (0x04)	0x01 (Threshold Based)
2Eh	Fan2 Speed	Current FAN 2 Speed (RPM)	Fan (0x04)	0x01 (Threshold Based)
2Fh	Fan3 Speed	Current FAN 3 Speed (RPM)	Fan (0x04)	0x01 (Threshold Based)
30h	Fan4 Speed	Current FAN 4 Speed (RPM)	Fan (0x04)	0x01 (Threshold Based)
31h	Fan5 Speed	Current FAN 5 Speed (RPM)	Fan (0x04)	0x01 (Threshold Based)
32h	Fan6 Speed	Current FAN 6 Speed (RPM)	Fan (0x04)	0x01 (Threshold Based)
61h	Fan1 Present	Presence state of FAN1	Fan (0x04)	0x8
62h	Fan2 Present	Presence state of FAN2	Fan (0x04)	0x8
63h	Fan3 Present	Presence state of FAN3	Fan (0x04)	0x8
64h	Fan4 Present	Presence state of FAN4	Fan (0x04)	0x8

65h	Fan5 Present	Presence state of FAN5	Fan (0x04)	0x8
66h	Fan6 Present	Presence state of FAN6	Fan (0x04)	0x8
18h	PS1 Temp	Temperature of Power supply 1	Temperature (0x01)	0x01 (Threshold Based)
19h	PS2 Temp	Temperature of Power supply 2	Temperature (0x01)	0x01 (Threshold Based)
DBh	P1 DTS Thrm Mrgn	Thermal margin before Processor 1 Thermal trip	Temperature (0x01)	0x01 (Threshold Based)
DCh	P2 DTS Thrm Mrgn	Thermal margin before Processor 1 Thermal trip	Temperature (0x01)	0x01 (Threshold Based)

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 informations and instructions to monitor and integrate customer-specific sensors in the cooling mechanism of the platform}

Table of contents

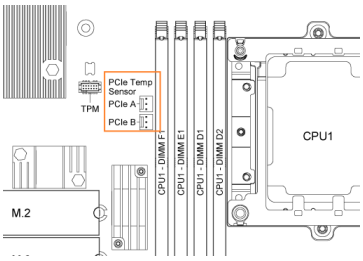
Thermal probe

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.



Probe installation

For each probe:

Step_1	Connect the probe's 3-pin connector to the motherboard. **NOTE:** The connector is keyed to ensure proper connection of the thermal probe to the motherboard.
Step_2	Affix the thermal probe's endpoint/transistor to the element to be monitored (e.g. chip). **NOTE:** Kapton tape, hot glue, RTV silicone or any other suitable binding material can be used.
Step_3	Route the cable in the platform making sure it does not interfere with other components.

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.

```
[root@localhost ~]# ipmitool sdr elist | grep PCIe
PCIe A Temp      | B7h | ns  |  7.1 | No Reading
PCIe B Temp      | B9h | ns  |  7.1 | No Reading
[root@localhost ~]#
```

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 Minimal 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. Details about the OEM commands can be found here: [Content under creation] Kontron IPMI OEM commands
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:

```
$ # Get current minimal speed (returns 0x0A = 10%)
$ ipmitool -H 192.168.1.10 -I lanplus -U admin -P admin raw 0x3c 0x0A 0x00 0x00 0x01
 0A
$
$ # 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

{This section provides instructions to detect issues and to identify their root causes in order to resolve them.}
Children

- Collecting diagnostics
- [Content under creation] Working with logs
- [Content under creation] Working with error messages
- [Content under creation] Networking issues
- Recovering corrupted BIOS
- Factory default
- Support information

Collecting diagnostics

{This article explains how to generate system logs.}
Table of contents

When the support team is contacted, the following data is required to make the proper board health diagnostics:

- [Content under creation] FRU information
- [Content under creation] Firmware version
- [Content under creation] System event log

Collecting all this data beforehand can accelerate the process.

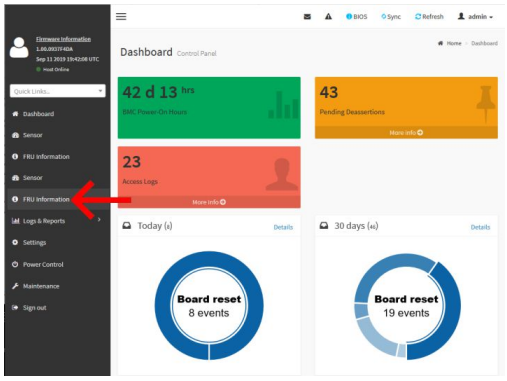
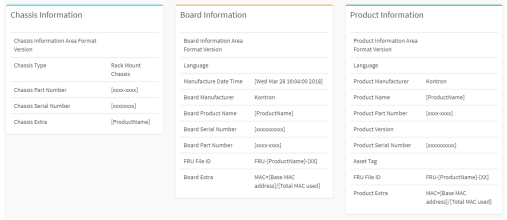
Collecting FRU information

FRU information can be collected:

- Using the BMC [Content under creation] Web UI
- Using [Content under creation] IPMI

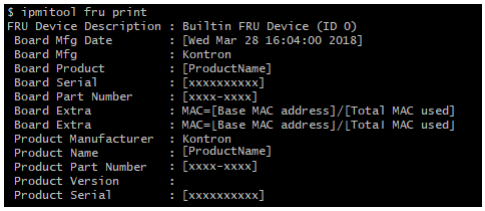
Collecting FRU information using the BMC Web UI

Refer to Accessing a BMC using the Web UI for access instructions.

Step_1	Access the BMC Web UI of the server.	
Step_2	Select **FRU Information** from the left side menu.	
Step_3	The FRU information is displayed.	

Collecting FRU information 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 FRU information. LocalServer_OSPrompt:~$ **ipmitool fru print**	

Collecting the firmware version

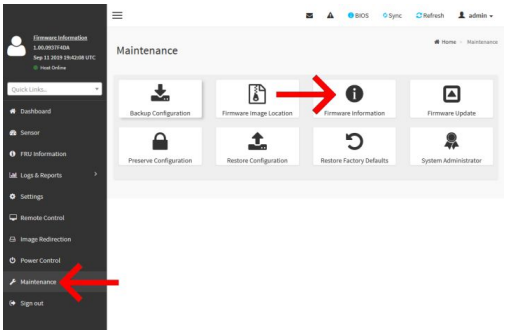
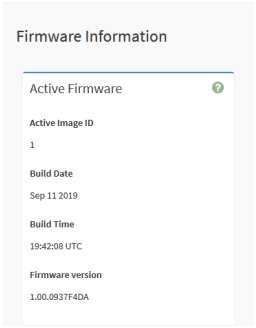
The firmware version can be collected:

- Using the BMC [Content under creation] Web UI

- Using [Content under creation] IPMI

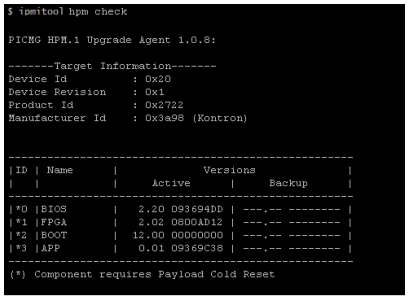
Collecting the firmware version using the BMC Web UI

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

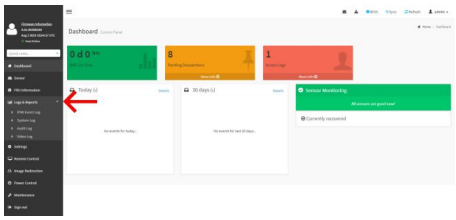
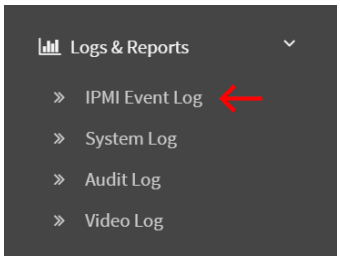
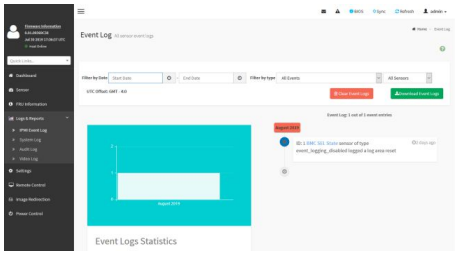
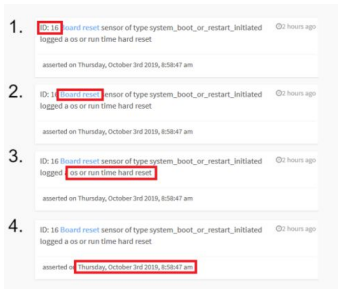
System event logs can be collected:

- Using the BMC [Content under creation] Web UI
- Using [Content under creation] 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.

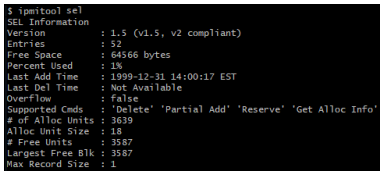
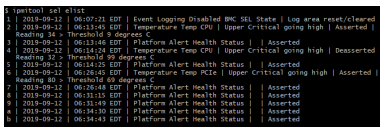
Step_1	Access the BMC Web UI of the server.	
Step_2	Select **Logs & Reports** from the left side menu.	
Step_3	Select **IPMI Event Log** from the dropdown menu.	
Step_4	The system event log is displayed.	
Step_5	Click on an event and collect the following information: 1. Event ID 2. Associated sensor 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	

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

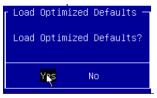
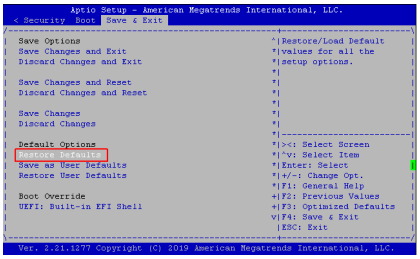
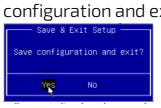
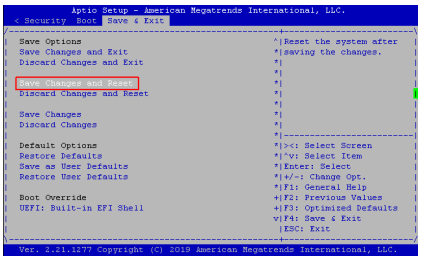
Restoring default BIOS settings

The BIOS settings can be reset to factory default:

- Using the [Content under creation] BIOS menu
- Using [Content under creation] IPMI
- Using a [Content under creation] 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**	`$ ipmitool chassis bootdev none clear-cmos=yes` `Set Boot Device to none`
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.	`$ ipmitool chassis power reset` `Chassis Power Control: Reset`

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.

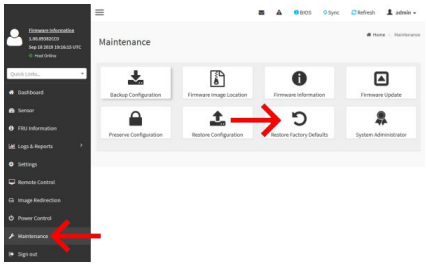
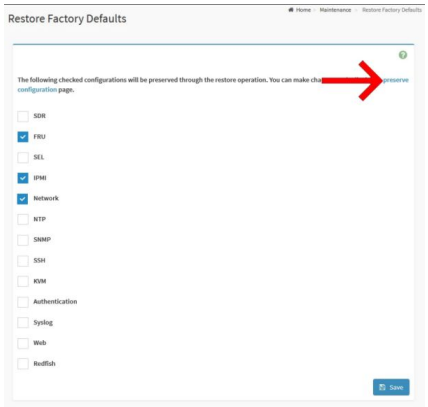
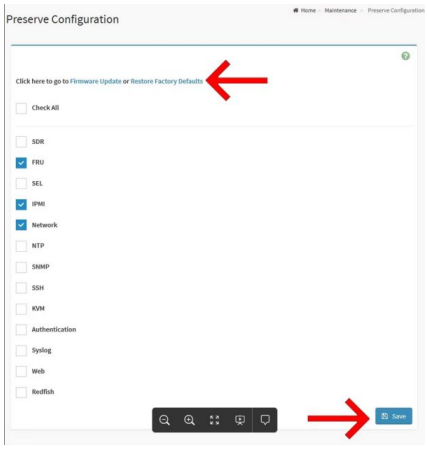
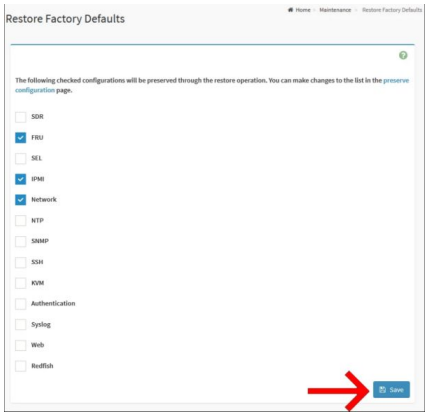
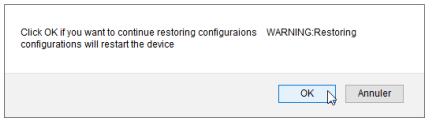
Restoring default BMC settings

Default BMC settings can be reset to factory default:

- Using the [Content under creation] Web UI
- Using [Content under creation] Redfish

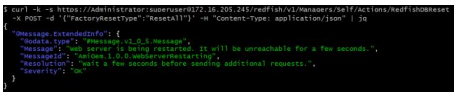
Restoring default BMC settings using the BMC Web UI

Refer to Accessing a BMC for access instructions.

Step_1	Access the BMC Web UI of the server.	
Step_2	From the left side menu, select **Maintenance** and then **Restore Factory Defaults** .	
Step_3	If necessary, click on **preserve configuration** to change the list of unaffected configurations.	
Step_4	Modify the list of preserved configurations, as required. Click on **Save** and then **Restore Factory Defaults** to return to the previous menu.	
Step_5	Click on **Save** .	
Step_6	Confirm the factory default restoration by clicking on **OK**. **NOTE:** The platform will reset.	

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** . RemoteComputer_OSPrompt:~$ **curl -k -s [ROOT_URL]Chassis/Self | jq .PowerState**	
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:

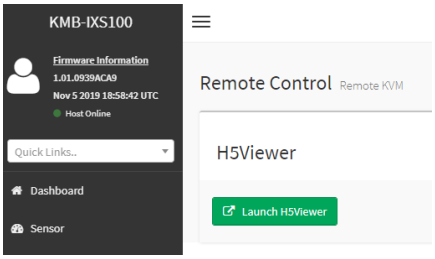
- By phone: 1-888-835-6676
- By email: support-na@kontron.com
- Via the website: www.kontron.com

Knowledge base

{ Self-service library of informative & descriptive content .}

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.

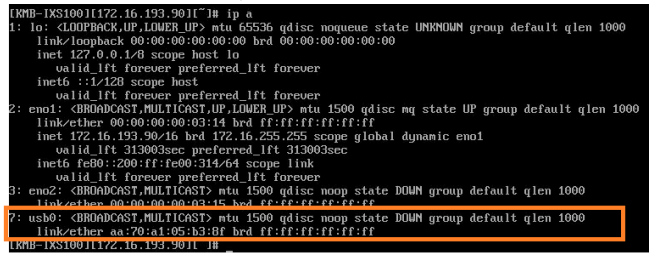


Konton observed that an automated routine rebooting the payload and then waiting for the host to ping back again may fail if KVM is opened.
Same routine executes correctly when no KVM is opened.

When a KVM is opened
In the Centos 7.3 console/SSH you can do "ip a" command :

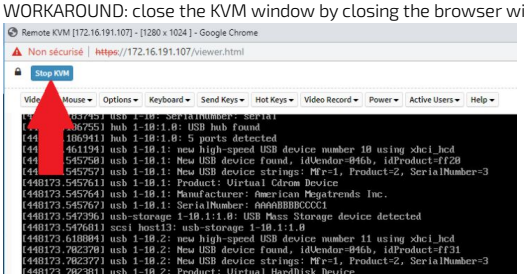
```
1 ip a
```

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

	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.

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

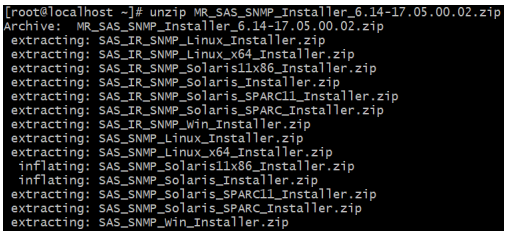
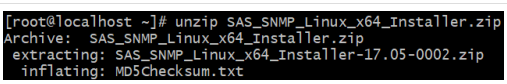
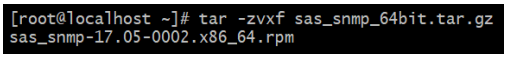
Downloading SNMP Installer

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]**

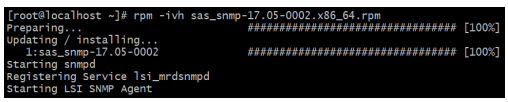
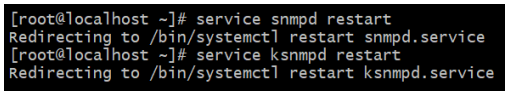
Extracting the content

NOTE: For example purposes, the operating system is Centos 7.3. Please note that commands may vary depending on the operating system installed.

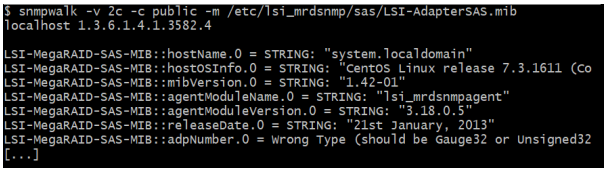
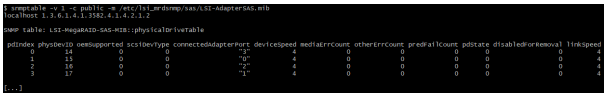
Step_1	Extract the content from the archive. LocalServer_OSPrompt:~# **unzip MR_SAS_SNMP_Installer_6.14-17.05.00.02.zip**	
Step_2	From the decompressed files, extract the content from the generated archive matching the operating system of the platform. LocalServer_OSPrompt:~# **unzip [ARCHIVE_NAME]**	
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

Step_1	Using the mib file and the command below, you should get all the information about your controller, LocalServer_OSPrompt:~# **snmpwalk -v 2c -c public -m /etc/lsi_mrdsnmp/sas/LSI-AdapterSAS.mib localhost 1.3.6.1.4.1.3582.4**	
Step_2	Use this command to see the physical devices table. 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**	

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.**
If the **SAS-IR** version is installed, this OID needs to be used to get the data: **1.3.6.1.5.1.3582.**

Application notes

Step-by-step procedures to execute specific use cases

Secure Erase

Table of contents

	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

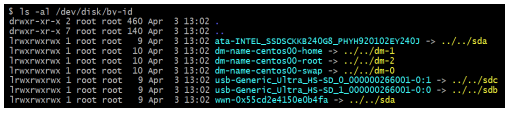
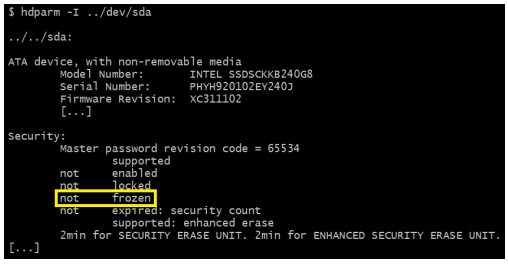
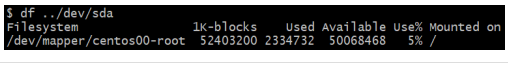
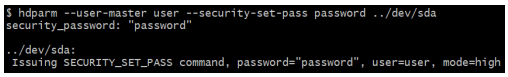
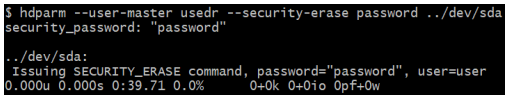
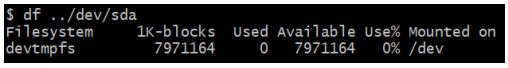
Prerequisites

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

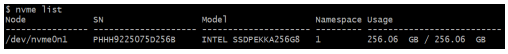
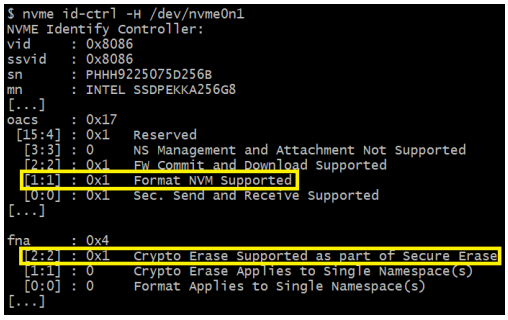
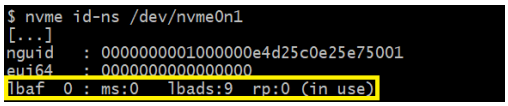
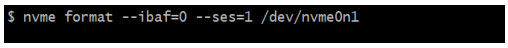
Prerequisites

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

Procedure

Refer to Accessing the operating system of a server for access instructions.

Step_1	List NVME devices and get device name. LocalServer_OSPrompt:~# **nvme list**	
Step_2	Get NVME device properties. Formatting and secure erase need to be supported. LocalServer_OSPrompt:~# **nvme id-ctrl -H [DEVICE_NAME]**	
Step_3	Get IBAF format type. LocalServer_OSPrompt:~# **nvme id-ns [DEVICE_NAME]**	
Step_4	Perform Secure Erase on the NVME disk. LocalServer_OSPrompt:~# **nvme format --ibaf=[IBAF] --ses=1 [DEVICE_NAME]**	

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

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

Term	Meaning
/cx	Controller specific commands
/ex	Enclosure specific commands
/sx	Slot/PD specific commands
/vx	Virtual drive specific commands
/dx	Disk group specific commands
/fall	Foreign configuration specific commands
/px	Phy specific commands
/bbu or /cv	Battery Backup Unit or Cachevault commands
/jbodx	JBOD drive specific commands

NOTE: The **x** in an argument represents the ID of a specific element.

Abbreviations

Term	Meaning
EID	Enclosure ID
Slt	Slot Number
VD	Virutal Drive
DID	Device ID
DG	Drive Group
DHS	Dedicated Hot Spare
UGood	Unconfigured Good
GHS	Global Hot Spare
UBad	Unconfigured Bad
Onln	Online
Offln	Offline
Intf	Interface
Med	Media Type
SED	Self Encryptive Drive
PI	Protection Info
SeSz	Sector Size
Sp	Spun
U	Up
D	Down/PowerSave
T	Transition
F	Foreign
UGUnsp	Unsupported
UGShld	UnConfigured Shielded
HSPShld	Hotspare Shielded
CFShld	Configured Shielded
Cpybck	Copyback
CBShld	Copyback Shieled

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

Vendor	Manufacturer P/N and description	Kontron P/N
Intel	RS3DC080 SCM x8 PCIe 3.0 LSI SAS3108 RAID-On-Chip	1061-7348
Intel	RS3DC040 RAID-CTRL_RS3DC040_PCIe_4x-SAS/SATA	1062-0561
LSI/Broadcom	MegaRAID SAS 9341-8i (Support up to 8 HDD/SSD)	1065-7734
LSI/Broadcom	MegaRAID SAS 9341-4i (Support up to 4 HDD/SSD)	1065-7736
LSI/Broadcom	MegaRAID SAS 9361-8i (8-port)	1065-5999
LSI/Broadcom	MegaRAID SAS 9361-4i (4-port)	1065-7726

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.

Step_1	Download the package from the following URL. LocalServer_OSPrompt:~# **wget** https://downloadmirror.intel.com/27654/eng/StorCLI_MR7.4p1.zip
Step_2	Unzip the archive downloaded from the Intel website. LocalServer_OSPrompt:~# **unzip StorCLI_MR7.4p1.zip**
Step_3	Navigate to **StorCLI_MR7.4p1/Linux** and execute the following commands. LocalServer_OSPrompt:~# **rpm -Uvh storcli-007.0415.0000.0000-1.noarch.rpm** LocalServer_OSPrompt:~# **ln -s /opt/MegaRAID/storcli/storcli64 /bin/storcli**
Step_4	Reboot the operating system. LocalServer_OSPrompt:~# **reboot**
Step_5	Test the StorCLI installation by displaying the version number. LocalServer_OSPrompt:~# **storcli -v**

Installing StorCLI on Debian / Ubuntu

NOTE: To perform the following instructions, root privileges are required.

Step_1	Download the package from the following URL. LocalServer_OSPrompt:~# **wget** https://downloadmirror.intel.com/27654/eng/StorCLI_MR7.4p1.zip
Step_2	Unzip the archive downloaded from the Intel website. LocalServer_OSPrompt:~# **unzip StorCLI_MR7.4p1.zip**
Step_3	Navigate to **StorCLI_MR7.4p1/Ubuntu** and execute the following commands. LocalServer_OSPrompt:~# **dpkg -i storcli_007.0415.0000.0000_all.deb** LocalServer_OSPrompt:~# **ln -s /opt/MegaRAID/storcli/storcli64 /bin/storcli**
Step_4	Reboot the operating system. LocalServer_OSPrompt:~# **reboot**
Step_5	Test the StorCLI installation by displaying the version number. LocalServer_OSPrompt:~# **storcli -v**

Installing StorCLI on Windows

NOTE: To perform the following instructions, administrator privileges are required.

Step_1	Download the **.zip** file from the Software download URL and extract the content from it.
Step_2	Open a command prompt with administrator privileges and navigate to the extracted folder. LocalServer_OSPrompt:~# **dir StorCLI_MR7.4p1**
Step_3	Execute the **storcli64.exe** file. LocalServer_OSPrompt:~# **start storcli64.exe**

Using the StorCLI utility

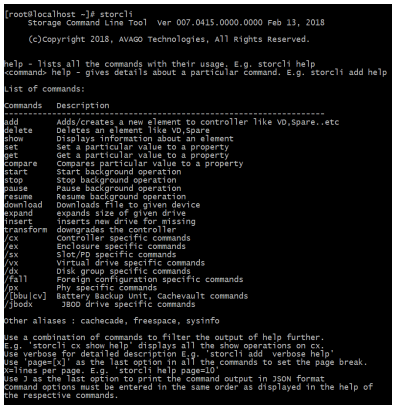
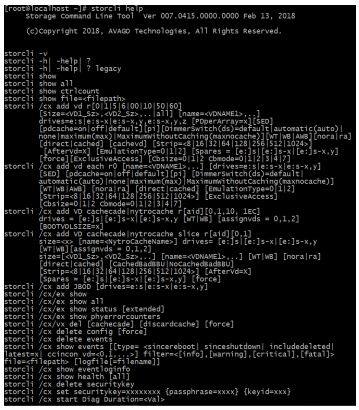
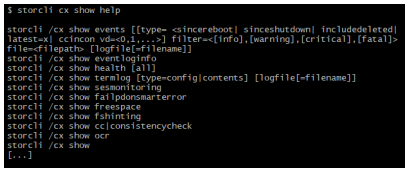
Commands

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**	

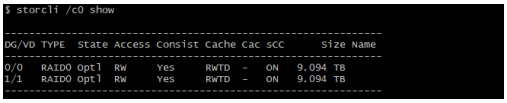
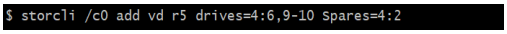
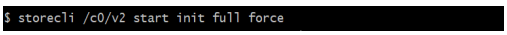
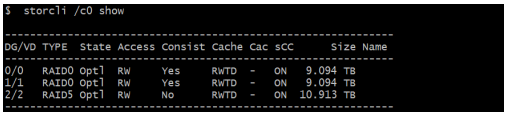
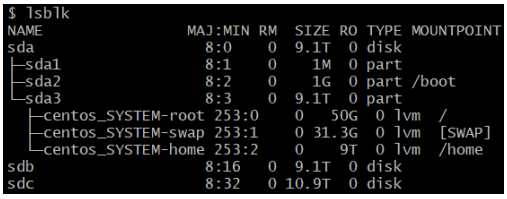
Show

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:

Command	Purpose
LocalServer_OSPrompt:~# **storcli /c0 show**	Shows details about the first controller.
LocalServer_OSPrompt:~# **storcli /c0 /p0 show**	Shows details about the first physical drive of the first controller.
LocalServer_OSPrompt:~# **storcli /c0 /v0 show**	Shows details about the first virtual drive of the first controller.
LocalServer_OSPrompt:~# **storcli /c0 show all**	Shows all details about the first controller.
LocalServer_OSPrompt:~# **storcli /c0 /v0 show all**	Shows all details about the first virtual drive of the first controller.

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. LocalServer _OSPrompt:~# **storcli /[CX] add [DRIVE_TYPE] r[RAID_TYPE] drives= [DRIVES] Spares=[SPARES_DRIVES]**	
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 avalaible in the operating system of the platform. LocalServer_OSPrompt:~# **lsblk**	

Delete

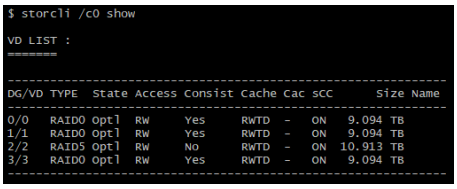
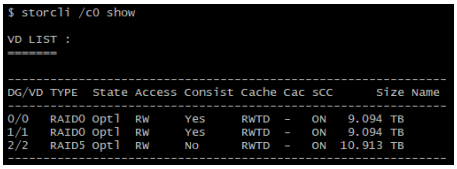
NOTE: For detailed explanations, refer to the StorCLI documentation - Chapter 2.6.4.2, pages 40 and 41.

The delete commands described in this section are:

- Deleting a virtual drive
- Deleting a hot spare drive from a virtual drive

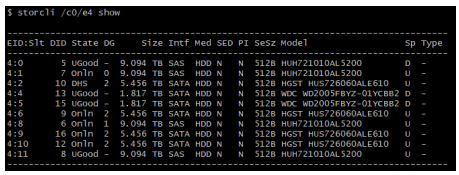
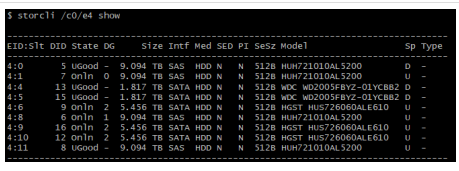
Deleting a virtual drive

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**	

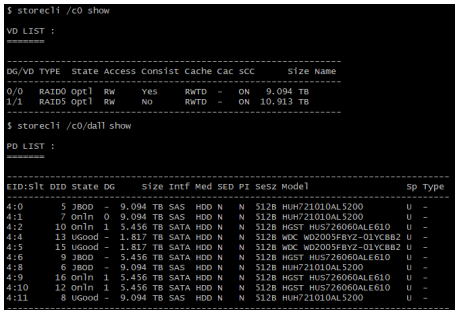
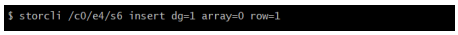
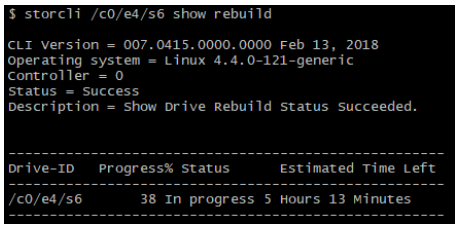
Deleting a hot spare drive from a virtual drive

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 - 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**	

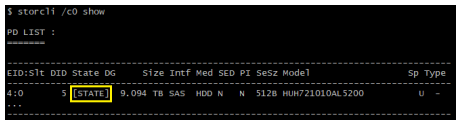
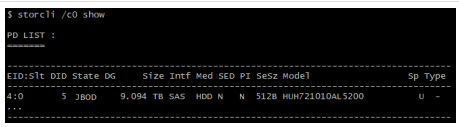
Set

NOTE: For detailed explanations, refer to the StorCLI documentation - 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 - 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 force) • 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

Step_1	Enable or disable an alarm on critical errors. The option silence silences the alarm. LocalServer_OSPrompt:~# **storcli /[CX] set alarm=[VALUE]** Possible values: • on • off • silence	`$ storcli /c0 set alarm=on`

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.

Step_1	Set the EGHS configuration . LocalServer_OSPrompt:~# **storcli /[CX] set eghs state=[VALUE] smarter=[VALUE] eug= [VALUE]** Possible values for state | smarter | eug: • on • off	`$ storcli /c0 set eghs state=on smarter=off eug=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

Step_1	Display all the drives considered as foreign configured. LocalServer_OSPrompt:~# **storcli /[CX]/fall show all**	`$ storcli /c0/fall show all`

Delete foreign configuration

Step_1	Delete the foreign configuration . LocalServer_OSPrompt:~# **storcli /[CX]/fall del**	`[root@localhost ~]# storcli /c0/fall del`

Import foreign configuration

Step_1	Import a foreign configuration . LocalServer_OSPrompt:~# **storcli /[CX]/fall import**	`[root@localhost ~]# storcli /c0/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

Step_1	Add a drive to an existing drive group. LocalServer_OSPrompt:~# **storcli /[CX]/[VX] start migrate type=[RAID_TYPE] option=add drives=[DRIVES]**	`$ storcli /c0/v2 start migrate type=raid0 option=add drives=4:0,4:1,4:2`

Removing a drive from a RAID

Step_1	Remove a drive from a RAID. LocalServer_OSPrompt:~# **storcli /[CX]/[VX] start migrate type=[RAID_TYPE] option=remove drives=[DRIVES]**	`$ storcli /c0/v2 start migrate type=raid0 option=remove drives=4:2`

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 - 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**	`$ storcli /c0/e4/s4 add hotsparedrive`

Delete a Global Hot Spare drive

Step_1	Delete a Global Hot Spare drive. LocalServer_OSPrompt:~# **storcli /[CX]/[VX]/[SX] delete hotsparedrive**	`$ storcli /c0/e4/s4 delete hotsparedrive`

Software RAID (VRoC)

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

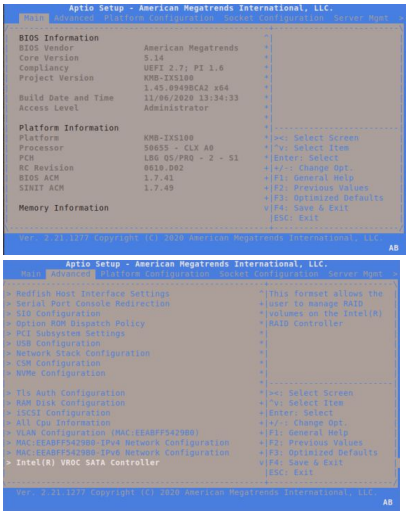
1. Go into the BIOS Setup Utility, Platform Configuration → PCH Configuration → PCH SATA Configuration → Configure SATA as → *RAID*
2. Other options are necessary to make it works, but are different depending on if you will be using UEFI or Legacy setup
3. Save and reset (F4)

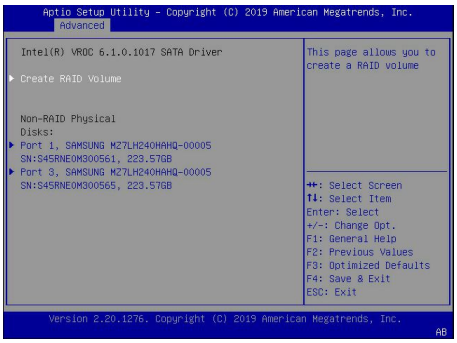
Install at least 1 drive in the front drive array (in order to see the menu)
Go into the BIOS Setup Utility, Advanced will have an entry called "Intel(R) VROC SATA Controller"

UEFI

VROC SATA Driver

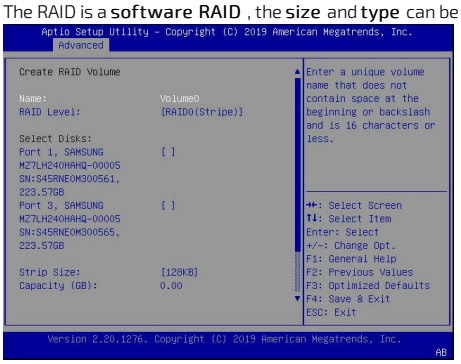
Main Menu



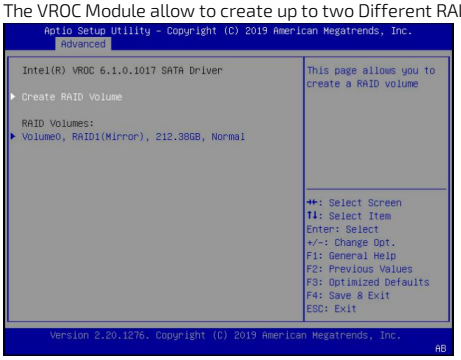


Create RAID

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.

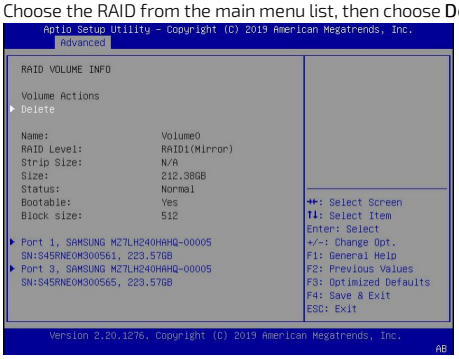


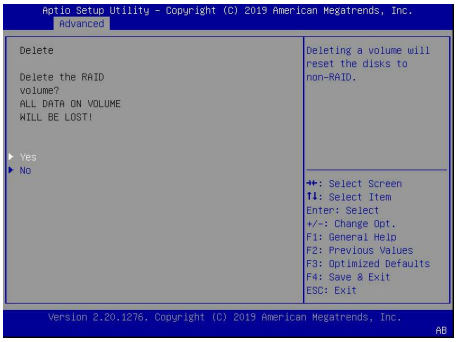
The VROC Module allow to create up to two Different RAID using the same Drives.



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

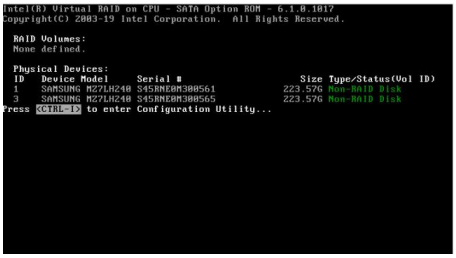
1. Go into the BIOS Setup Utility, Platform Configuration → PCH Configuration → PCH SATA Configuration → Configure SATA as → ***RAID***
2. Go to Advanced → CSM Cinfiguration → CSM Support → ***Enabled***
3. Put the Option ROM execution → Storage → ***Legacy***
4. Put the Option ROM execution → Video → ***Legacy***
5. Then, Put the Option ROM Messages → ***Force BIOS***
6. Save and Reset (F4)

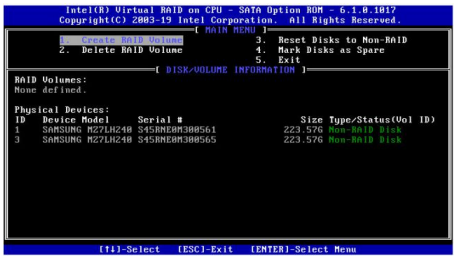
To access the Management console, during the boot, press ***CTRL+I***
WARNING : CTRL+I only works via the Serial Console Redirection

Hardware Specification

The CG2400M system is limited to six drives connected in the front bay.

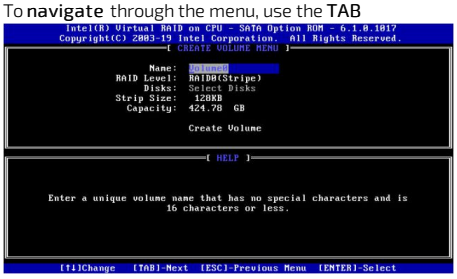
VRoC Option ROM & Dashboard





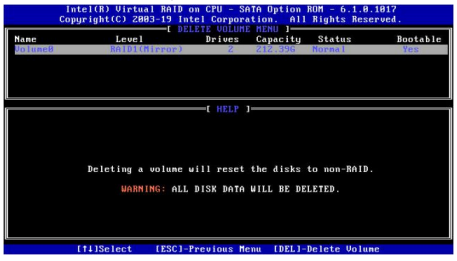
Raid Creation

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**



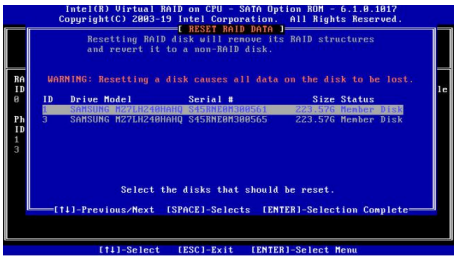
Raid Deletion

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**.



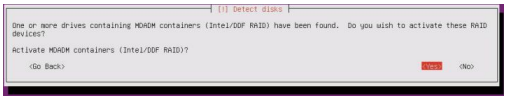
How the OS manage the RAID ?

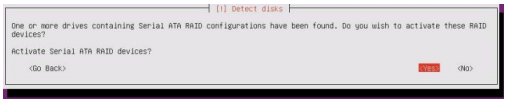
The Linux see a mdadm RAID.

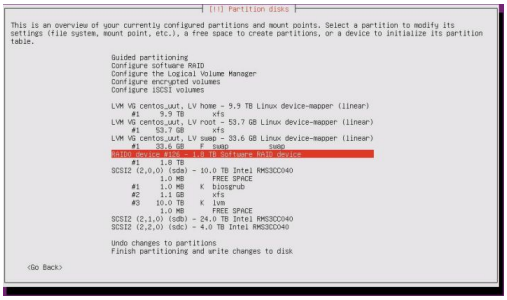
```
[root @SYSTEM ~]# lsblk
...
sdd 8 : 48 0 894 .3G 0 disk
└─md126 9 : 126 0 1 .7T 0 raid0
sde 8 : 64 0 894 .3G 0 disk
└─md126 9 : 126 0 1 .7T 0 raid0
```

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)

```
ubuntu@ubuntu:~$ sudo lsblk
NAME    MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
sda       8:0    0   9.1T  0 disk
sdb       8:16   0  21.8T  0 disk
sdc       8:32   0   3.7T  0 disk
sdd       8:48   0 894.3G  0 disk
└─md126   9:126  0   1.7T  0 raid0 /
sde       8:64   0 894.3G  0 disk
└─md126   9:126  0   1.7T  0 raid0 /
ubuntu@ubuntu:~$
```

Centos 7.4

Using a kickstart installation script, the process go through automatically and the installation work successfully.

```
[root@localhost ~]# lsblk
NAME              MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
sda                 8:0    0 447.1G  0 disk
└─md126             9:126  0 424.8G  0 raid1
  ├─md126p1       259:0    0     1G  0 md    /boot
  └─md126p2       259:1    0 423.8G  0 md
    ├─centos-root 253:0    0    50G  0 lvm   /
    ├─centos-swap 253:1    0  31.3G  0 lvm   [SWAP]
    └─centos-home 253:2    0 342.5G  0 lvm   /home
sdb                 8:16   0 447.1G  0 disk
└─md126             9:126  0 424.8G  0 raid1
  ├─md126p1       259:0    0     1G  0 md    /boot
  └─md126p2       259:1    0 423.8G  0 md
    ├─centos-root 253:0    0    50G  0 lvm   /
    ├─centos-swap 253:1    0  31.3G  0 lvm   [SWAP]
    └─centos-home 253:2    0 342.5G  0 lvm   /home
sdc                 8:32   0   9.1T  0 disk
sdd                 8:48   0  21.8T  0 disk
sde                 8:64   0   3.7T  0 disk
[root@localhost ~]# _
```

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

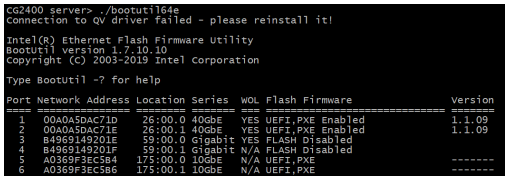
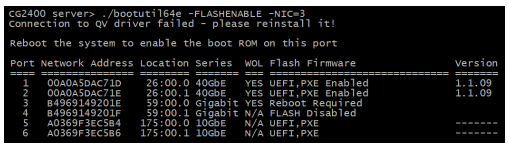
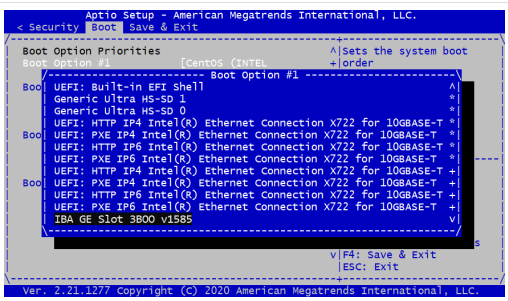
Links

Download center link	https://downloadcenter.intel.com/download/29137?v=t
Bootutil documentation	https://downloadmirror.intel.com/29137/eng/bootutil.txt
Tool for Linux	https://downloadmirror.intel.com/29137/eng/Preboot.tar.gz

Installation procedure

Step_1	Get the archive from the following link. LocalServer_OSPrompt:~# **wget https://downloadmirror.intel.com/29137/eng/Preboot.tar.gz**
Step_2	Extract the content of the archive. LocalServer_OSPrompt:~# **tar xvzf Preboot.tar.gz**
Step_3	Change directory. LocalServer_OSPrompt:~# **cd APPS/BootUtil/Linux_x64/**
Step_4	Make the file executable. LocalServer_OSPrompt:~# **chmod +x bootutil64e**

Interface configuration

Step_1	List the current settings LocalServer_OSPrompt:~# **./bootutil64e**	
Step_2	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. LocalServer_OSPrompt:~# **./bootutil64e -FLASHENABLE NIC=[PORT_NUMBER]**	
Step_3	To apply the modifications, reboot the system. LocalServer_OSPrompt:~# **reboot**	
Step_4	Access the BIOS menu. Refer to Accessing the BIOS for access instructions.	
Step_5	From the **Boot** menu, navigate to **Boot Option Priorities** . You should be able to configure the network interfaces as a boot option.	

Provisioning custom secure boot keys

Table of contents

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

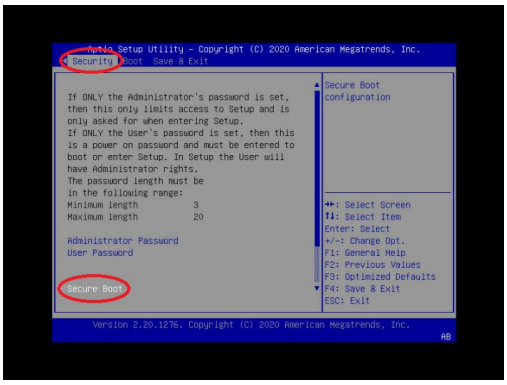
Prerequisites

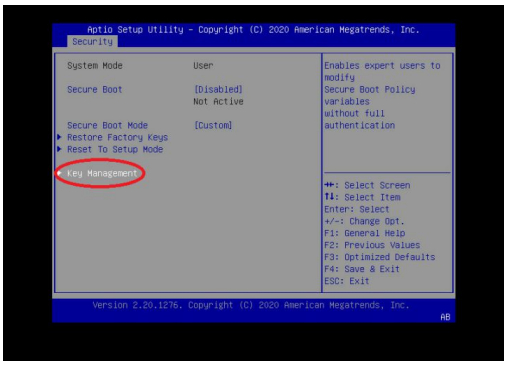
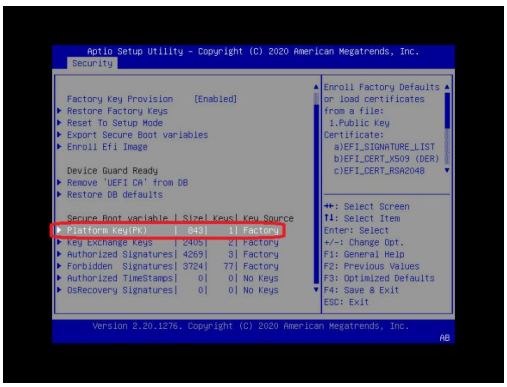
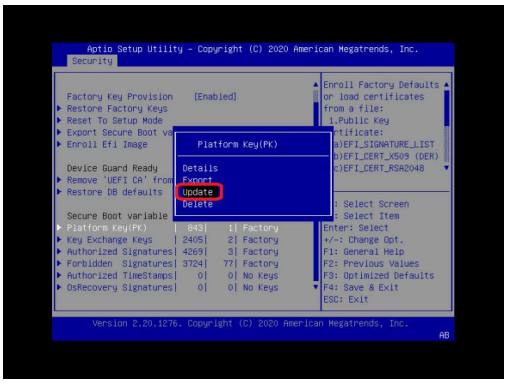
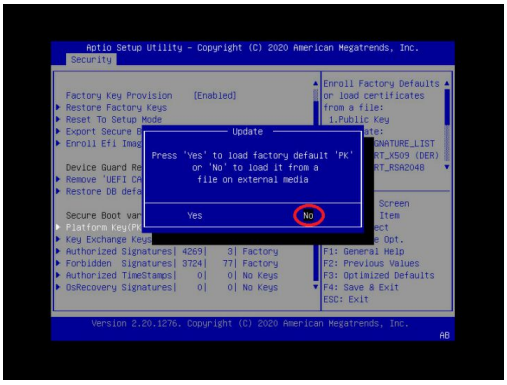
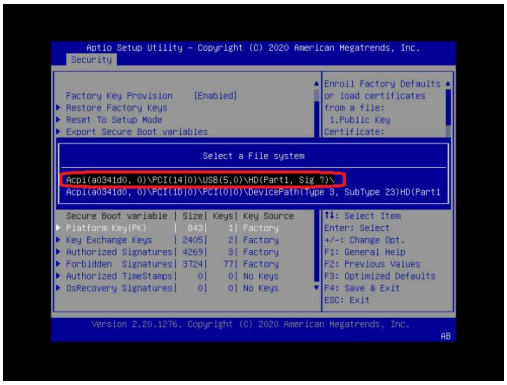
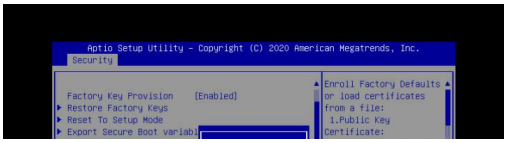
1	A set of Secure Boot keys has been created (PK, KEK and db).
2	Public Key certificates that are to be provisioned are in DER format.
3	Public Key certificates are present on a FAT-partitioned USB drive, which is connected to the board. If Virtual Media redirection is available, it is also possible to use a corresponding ISO image instead.

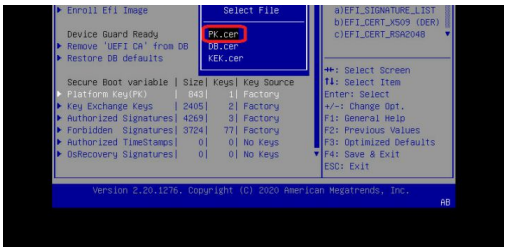
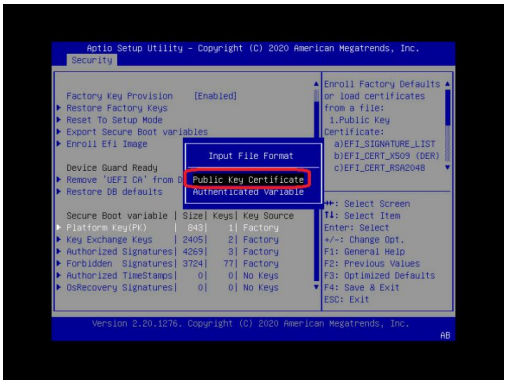
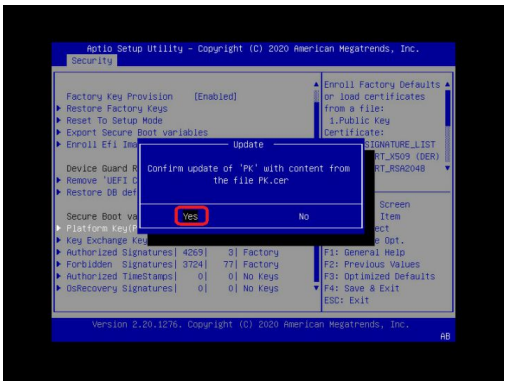
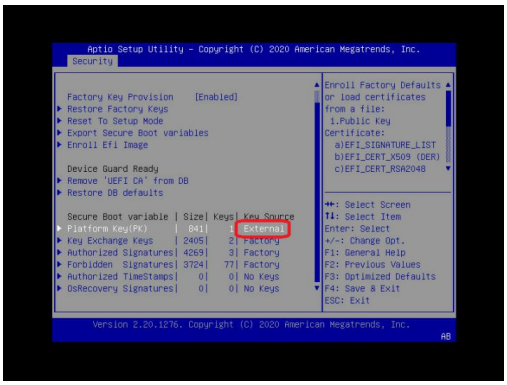
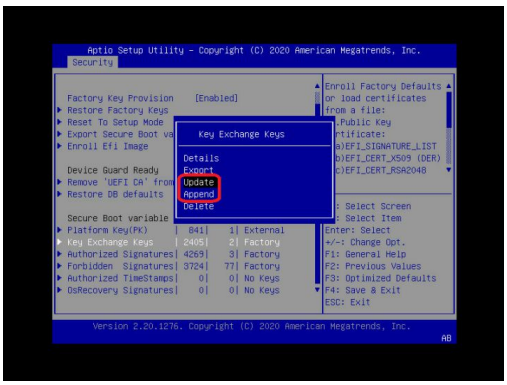
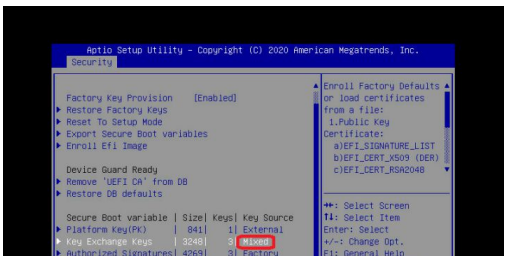
Relevant section:
Generating custom secure boot keys

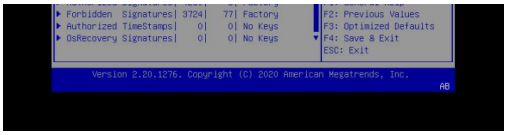
i	As the current time is verified against certificate timestamps as a security measure, make sure the system time is valid prior to manipulating Secure Boot variables. Otherwise, a Security Violation error will be obtained and no change will be possible.

Procedure

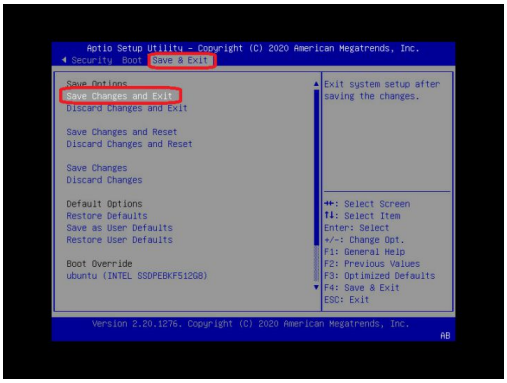
Step_1	Access the UEFI Setup Utility by pressing F2 or DEL when the sign-on screen is displayed during boot.	
Step_2	Access the **Secure Boot** submenu from the **Security** tab.	
Step_3	Access the Key Management page by selecting the **Key Management** menu item.	

		
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).	

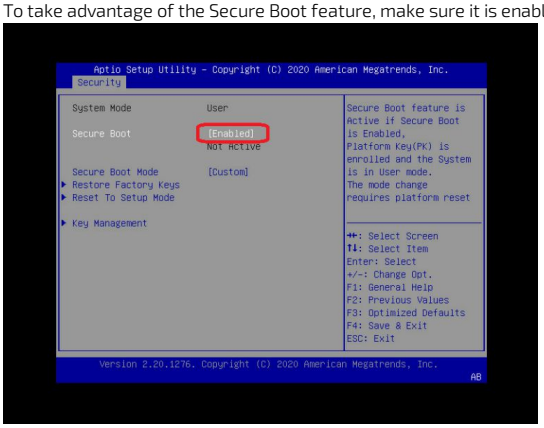
		
Step_9	Specify that the file format is **Public Key Certificate** .	
Step_10	Select **Yes** to confirm Platform Key update.	
Step_11	Confirm that the update completed successfully. The table should now show that a key was added from an "External" Key Source.	
Step_12	Select **Key Exchange Keys** to update 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

Relevant section:
Provisioning 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

1	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

{ Documents for system administrators, to configure and operate systems & solutions. Documents assume that the reader has basic knowledge of key system & solution concepts. }

Supported IPMI commands

Table of contents

Application commands

IPM device commands

Net function	Command	Command name	Supported / Unsupported	M/O
0x06	0x01	Get Device ID	Supported	M
0x06	0x02	Cold Reset	Supported	O
0x06	0x03	Warm Reset	Unsupported *	O
0x06	0x04	Get Self Test Results	Supported	M
0x06	0x05	Manufacturing Test On	Unsupported *	O
0x06	0x06	Set ACPI Power State	Supported	O
0x06	0x07	Get ACPI Power State	Supported	O
0x06	0x08	Get Device GUID	Supported	O
0x06	0x09	Get NetFn Support	Supported	O
0x06	0x0A	Get Command Support	Supported	O
0x06	0x0C	Get Configurable Commands	Supported	O
0x06	0x60	Set Command Enables	Supported	O
0x06	0x61	Get Command Enables	Supported	O
0x06	0x64	Get OEM NetFn IANA Support	Supported	O
0x06	0x0B	Get Command Sub-function Support	Supported	O
0x06	0x0D	Get Configurable Command Sub-functions	Supported	O
0x06	0x62	Set Command Sub-function Enables	Unsupported	O
0x06	0x63	Get Command Sub-function Enables	Unsupported	O
0x06	0x52	Master Write-Read	Supported	O

* Commands are not rejected and can cause unpredictable behavior.

Watchdog timer commands

Net function	Command	Command name	Supported / Unsupported	M/O
0x06	0x22	Reset Watchdog Timer	Supported	M
0x06	0x24	Set Watchdog Timer	Supported	M
0x06	0x25	Get Watchdog Timer	Supported	M

BMC device and messaging commands

Net function	Command	Command name	Supported / Unsupported	M/O
0x06	0x2E	Set BMC Global Enables	Supported	M
0x06	0x2F	Get BMC Global Enables	Supported	M
0x06	0x30	Clear Message Flags	Supported	M
0x06	0x31	Get Message Flags	Supported	M
0x06	0x32	Enable Message Channel Receive	Supported	O
0x06	0x33	Get Message	Supported	M
0x06	0x34	Send Message	Supported	M
0x06	0x35	Read Event Message Buffer	Supported	O
0x06	0x37	Get System GUID	Supported	O
0x06	0x38	Get Channel Authentication Capabilities	Supported	O
0x06	0x39	Get Session Challenge	Supported	O
0x06	0x3A	Activate Session	Supported	O
0x06	0x3B	Set Session Privilege Level	Supported	O
0x06	0x3C	Close Session	Supported	O
0x06	0x3D	Get Session Info	Supported	O
0x06	0x3F	Get AuthCode	Supported	O
0x06	0x40	Set Channel Access	Supported	O
0x06	0x41	Get Channel Access	Supported	O
0x06	0x42	Get Channel Info Command	Supported	O
0x06	0x43	Set User Access Command	Supported	O
0x06	0x44	Get User Access Command	Supported	O
0x06	0x45	Set User Name	Supported	O
0x06	0x46	Get User Name Command	Supported	O
0x06	0x47	Set User Password Command	Supported	O
0x06	0x52	Master Write-Read	Supported	M
0x06	0x58	Set System Info Parameters	Supported	O
0x06	0x59	Get System Info Parameters	Supported	O

IPMI 2.0 specific commands

Net function	Command	Command name	Supported / Unsupported	M/O
0x06	0x48	Activate Payload	Supported	O
0x06	0x49	Deactivate Payload	Supported	O
0x06	0x4A	Get Payload Activation Status	Supported	O
0x06	0x4B	Get Payload Instance Info	Supported	O
0x06	0x4C	Set User Payload Access	Supported	O
0x06	0x4D	Get User Payload Access	Supported	O
0x06	0x4E	Get Channel Payload Support	Supported	O
0x06	0x4F	Get Channel Payload Version	Supported	O
0x06	0x50	Get Channel OEM Payload Info	Supported	O
0x06	0x54	Get Channel Cipher Suites	Supported	O
0x06	0x55	Suspend/Resume Payload Encryption	Supported	O
0x06	0x56	Set Channel Security Keys	Supported	O
0x06	0x57	Get System Interface Capabilities	Supported	O

Chassis commands

Net function	Command	Command name	Supported / Unsupported	M/O
0x00	0x00	Get Chassis Capabilities	Supported	M
0x00	0x01	Get Chassis Status	Supported	M
0x00	0x02	Chassis Control	Supported	M
0x00	0x04	Chassis Identify	Supported	O
0x00	0x05	Set Chassis Capabilities	Supported	O
0x00	0x06	Set Power Restore Policy	Supported	O
0x00	0x07	Get System Restart Cause	Supported	O
0x00	0x08	Set System Boot Options	Supported	O
0x00	0x09	Get System Boot Options	Supported	O
0x00	0x0A	Set Front Panel Button Enables	Supported	O
0x00	0x0B	Set Power Cycle Interval	Supported	O
0x00	0x0F	Get POH Counter	Supported	O

Bridge commands

B ridge management commands

Net function	Command	Command name	Supported / Unsupported	M/O
0x02	0x00	Get Bridge State	Unsupported	O
0x02	0x01	Set Bridge State	Unsupported	O
0x02	0x02	Get ICMB Address	Unsupported	O
0x02	0x03	Set ICMB Address	Unsupported	O
0x02	0x04	SetBridgeProxyAddress	Unsupported	O
0x02	0x05	Get Bridge Statistics	Unsupported	O
0x02	0x06	Get ICMB Capabilities	Unsupported	O
0x02	0x08	Clear Bridge Statistics	Unsupported	O
0x02	0x09	GetBridge Proxy Address	Unsupported	O
0x02	0x0A	Get ICMB Connector Info	Unsupported	M

Bridge discovery commands

Net function	Command	Command name	Supported / Unsupported	M/O
0x02	0x10	Prepare For Discovery	Unsupported	O
0x02	0x11	Get Addresses	Unsupported	O
0x02	0x12	Set Discovered	Unsupported	O
0x02	0x13	Get Chassis Device Id	Unsupported	O
0x02	0x14	Set Chassis Device Id	Unsupported	O

Bridging commands

Net function	Command	Command name	Supported / Unsupported	M/O
0x02	0x20	Bridge Request	Unsupported	O
0x02	0x21	Bridge Message	Unsupported	O

Bridge event commands

Net function	Command	Command name	Supported / Unsupported	M/O
0x02	0x30	Get Event Count	Unsupported	O
0x02	0x31	Set Event Destination	Unsupported	O
0x02	0x32	Set Event Reception State	Unsupported	O
0x02	0x33	SendICMB Event Message	Unsupported	O
0x02	0x34	Get Event Destination	Unsupported	O
0x02	0x35	Get Event Reception State	Unsupported	O

Sensor event commands

Net function	Command	Command name	Supported / Unsupported	M/O
0x04	0x00	Set Event Receiver	Supported	M
0x04	0x01	Get Event Receiver	Supported	M
0x04	0x02	Platform Event	Supported	M
0x04	0x10	Get PEF Capabilities	Supported	M
0x04	0x11	Arm PEF Postpone Timer	Supported	M
0x04	0x12	Set PEF Configuration Parameters	Supported	M
0x04	0x13	Get PEF Configuration Parameters	Supported	M
0x04	0x14	Set Last Processed Event ID	Supported	M
0x04	0x15	Get Last Processed Event ID	Supported	M
0x04	0x16	Alert Immediate	Supported	O
0x04	0x17	PET Acknowledge	Supported	O
0x04	0x20	Get Device SDR Info	Supported	O
0x04	0x21	Get Device SDR	Supported	O
0x04	0x22	Reserve Device SDR Repository	Supported	O
0x04	0x23	Get Sensor Reading Factors	Supported	O
0x04	0x24	Set Sensor Hysteresis	Supported	O
0x04	0x25	Get Sensor Hysteresis	Supported	O
0x04	0x26	Set Sensor Threshold	Supported	O
0x04	0x27	Get Sensor Threshold	Supported	O
0x04	0x28	Set Sensor Event Enable	Supported	O
0x04	0x29	Get Sensor Event Enable	Supported	O
0x04	0x2A	Re-arm Sensor Events	Supported	O
0x04	0x2B	Get Sensor Event Status	Supported	O
0x04	0x2D	Get Sensor Reading	Supported	M
0x04	0x2E	Set Sensor Type	Supported	O
0x04	0x2F	Get Sensor Type	Supported	O
0x04	0x30	Set Sensor Reading And Event Status	Supported	O

Storage commands

FRU information commands

Net function	Command	Command name	Supported / Unsupported	M/O
0x0a	0x10	Get FRU Inventory Area Info	Supported	M
0x0a	0x11	Read FRU Data	Supported	M
0x0a	0x12	Write FRU Data	Supported	M

SDR repository commands

Net function	Command	Command name	Supported / Unsupported	M/O
0x0a	0x20	Get SDR Repository Info	Supported	M
0x0a	0x21	Get SDR Repository Allocation Info	Supported	O
0x0a	0x22	Reserve SDR Repository	Supported	M
0x0a	0x23	Get SDR	Supported	M
0x0a	0x24	Add SDR	Supported	M
0x0a	0x25	Partial Add SDR	Supported	M
0x0a	0x27	Clear SDR Repository	Supported	M
0x0a	0x28	Get SDR Repository Time	Supported	M
0x0a	0x2C	Run Initialization Agent	Supported	O
0x0a	0x26	Delete SDR Repository	Supported	M

SEL device commands

Net function	Command	Command name	Supported / Unsupported	M/O
0x0a	0x40	Get SEL Info	Supported	M
0x0a	0x41	Get SEL Allocation Info	Supported	O
0x0a	0x42	Reserve SEL	Supported	O
0x0a	0x43	Get SEL Entry	Supported	M
0x0a	0x44	Add SEL Entry	Supported	M
0x0a	0x45	Partial Add SEL Entry	Supported	M
0x0a	0x47	Clear SEL	Supported	M
0x0a	0x48	Get SEL Time	Supported	M
0x0a	0x49	Set SEL Time	Supported	M
0x0a	0x5C	Get SEL Time UTC OffSet	Supported	O
0x0a	0x5D	Set SEL Time UTC OffSet	Supported	O

Transport commands

IPM d evice commands

Net function	Command	Command name	Supported / Unsupported	M/O
0x0c	0x01	Set LAN Configuration Parameters	Supported	M
0x0c	0x02	Get LAN Configuration Parameters	Supported	M
0x0c	0x03	Suspend BMC ARPs	Supported	O

Serial over LAN commands

Net function	Command	Command name	Supported / Unsupported	M/O
0x0c	0x22	Get SOL Configuration Parameters	Supported	O
0x0c	0x21	Set SOL Configuration Parameters	Supported	O

AMI commands

AMI restore factory default settings command

Net function	Command	Command name	Supported / Unsupported	M/O
0x32	0x66	Restore Defaults	Supported	O

Kontron OEM commands

Net Function	Command	Command Name	Supported/Unsupported	M/O
0x3c	0x0A	Override Minimum Fan Speed	Supported	O

NOTE: M/O = Mandatory/Optional

Supported Redfish commands

Table of contents

The information is presented in the following format:

- Description | Method | URL

Miscellaneous URLs

- Root resource of the Redfish service | -GET | /redfish/v1/
- Collection of DynamicExtension types | -GET | /redfish/v1/DynamicExtension
- Collection of DynamicExtensions | -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 ResourceBlocks | -GET **or** -PATCH | /redfish/v1/CompositionService/ResourceBlocks
- Collection of ResourceZones | -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 JSON schemas and extensions | -GET | /redfish/v1/JsonSchemas
- Returns informations about a specified JSON schema | -GET | /redfish/v1/JsonSchemas/[JSON_SCHEMA_NAME]
- Collection of sessions | -GET **or** -POST | /redfish/v1/SessionService/Sessions
- Session service | -GET **or** -PATCH | /redfish/v1/SessionService
- Returns informations 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 informations 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 | -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/Systems/[SYSTEM_INSTANCE]/LogServices/BIOS
- Collection of entries for this log service | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/LogServices/BIOS/Entries
- Collection of network interfaces | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/NetworkInterfaces
- Collection of storage resource instances | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/Storage
- A reference to the UEFI SecureBoot resource associated with this system | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/SecureBoot
- Collection of memory domains | -GET | /redfish/v1/Systems/[SYSTEM_INSTANCE]/MemoryDomains
- Zone capabilities | -GET | /redfish/v1/Systems/Capabilities

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/[ETHERNET_INTERFACE_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/[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 informations | -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/[SERIAL_INTERFACE_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/[HOST_INTERFACE_INSTANCE]
- Collection of ethernet interfaces connected to this host interface on this manager | -GET | /redfish/v1/Managers/[MANAGER_INSTANCE]/HostInterfaces/[HOST_INTERFACE_INSTANCE]/HostEthernetInterfaces

- Configures the number of CD/DVD devices that are supported for virtual media redirection | -POST | /redfish/v1/Managers/[MANAGER_INSTANCE]/Actions/Oem/Ami/VirtualMedia.ConfigureCDInstance
- Enables/disables RMedia support | -POST | /redfish/v1/Managers/[MANAGER_INSTANCE]/Actions/Oem/Ami/VirtualMedia.EnableRMedia

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

SNMP OID list

Here's a table of the possible informations that can be found via SNMP.

OID	Description	Action
SNMPv2-MIB::sysObjectID.0		
DISMAN-EVENT-MIB::sysUpTimeInstance	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.	GET
SNMPv2-MIB::sysContact.0	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.	GET SET
SNMPv2-MIB::sysName.0	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.	GET SET
SNMPv2-MIB::sysLocation.0	The physical location of this node (e.g.,`telephone closet, 3rd floor').	GET SET
SNMPv2-MIB::sysORLastChange.0	The value of sysUpTime at the time of the most recent change in state or value of any instance of sysORID.	GET
SNMPv2-MIB::sysORTable	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.	GET TABLE
IF-MIB::ifNumber.0	The number of network interfaces (regardless of their current state) present on this system.	GET
IF-MIB::ifTable	A list of interface entries. The number of entries is given by the value of ifNumber. The entries consist of these fields. Index, Descr, Type, Mtu, Speed, PhysAddress, AdminStatus, OperStatus, LastChange, InOctets, InUcastPkts, InNUcastPkts, InDiscards, InErrors InUnknownProtos, OutOctets, OutUcastPkts, OutNUcastPkts, OutDiscards, OutErrors, OutQLen.	GET TABLE
1.3.6.1.2.1.3.1.1.1	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.	GET
1.3.6.1.2.1.3.1.1.2	The media-dependent `physical' address.	GET
1.3.6.1.2.1.3.1.1.3	The NetworkAddress (e.g., the IP address) corresponding to the media-dependent `physical' address.	GET
IP-MIB::ipForwarding	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).	GET
IP-MIB::ipDefaultTTL	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.	GET
IP-MIB::ipInReceives	The total number of input datagrams received from interfaces, including those received in error.	GET
IP-MIB::ipInAddrErrors	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.	GET
IP-MIB::ipForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source- Routed via this entity, and the Source- Route option processing was successful.	GET
IP-MIB::ipInUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.	GET
IP-MIB::ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.	GET
IP-MIB::ipInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).	GET
IP-MIB::ipOutRequests	The total 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 counted in ipForwDatagrams.	GET
IP-MIB::ipOutDiscards	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 ipForwDatagrams if any such packets met this (discretionary) discard criterion.	GET
IP-MIB::ipOutNoRoutes	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 ipForwDatagrams which meet this `no-route' criterion. Note that this includes any datagarms which a host cannot route because all of its default gateways are down.	GET
IP-MIB::ipReasmTimeout	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.	GET
IP-MIB::ipReasmReqds	Number of IP fragments received which needed to be reassembled at this entity.	GET

IP-MIB::ipReasmOKs	Number of IP datagrams successfully re-assembled.	GET
IP-MIB::ipReasmFails	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 815) can lose track of the number of fragments by combining them as they are received.	GET
IP-MIB::ipFragCreates	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.	GET
IP-MIB::ipFragFails	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.	GET
IP-MIB::ipFragOKs	Number of IP datagrams that have been successfully fragmented at this entity.	GET
IP-MIB::ipAddrTable	Table of addressing information relevant to this entity's IP addresses.	GET TABLE
1.3.6.1.2.1.4.21	IP Routing table.	GET
IP-MIB::ipNetToMediaTable	IP Address Translation table used for mapping from IP addresses to physical addresses.	GET TABLE
IP-MIB::ipRoutingDiscards	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.	GET
IP-FORWARD-MIB::ipCidrRouteTable	This entity's IP Routing table.	GET TABLE
IP-FORWARD-MIB::inetCidrRouteNumber	The number of current ipCidrRouteTable entries that are not invalid.	GET
IP-FORWARD-MIB::inetCidrRouteTable	This entity's IP Routing table.	GET 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.	GET
IP-MIB::ipv6IpDefaultHopLimit	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.	GET
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.	GET TABLE
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.	GET
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.	GET TABLE
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	GET TABLE
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	GET
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	GET TABLE
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.	GET TABLE
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.	GET TABLE
IP-MIB::ipDefaultRouterTable	The table used to describe the default routers known to this entity.	GET TABLE
IP-MIB::icmpInMsgs	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.	GET
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::icmpInParmProbs	Number of ICMP Parameter Problem messages received.	GET
IP-MIB::icmpInSrcQuenchs	Number of ICMP Source Quench messages received.	GET
IP-MIB::icmpInRedirects	Number of ICMP Redirect messages received.	GET

IP-MIB::icmpInEchos	Number of ICMP Echo (request) messages received.	GET
IP-MIB::icmpInEchoReps	Number of ICMP Echo Reply messages received.	GET
IP-MIB::icmpInTimestamps	Number of ICMP Timestamp (request) messages received.	GET
IP-MIB::icmpInTimestampReps	Number of ICMP Timestamp Reply messages received.	GET
IP-MIB::icmpInAddrMasks	Number of ICMP Address Mask Request messages received.	GET
IP-MIB::icmpInAddrMaskReps	Number of ICMP Address Mask Reply messages received.	GET
IP-MIB::icmpOutMsgs	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.	GET
IP-MIB::icmpOutErrors	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should notinclude errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.	GET
IP-MIB::icmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.	GET
IP-MIB::icmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.	GET
IP-MIB::icmpOutParmProbs	The number of ICMP Parameter Problem messages sent.	GET
IP-MIB::icmpOutSrcQuenchs	The number of ICMP Source Quench messages sent.	GET
IP-MIB::icmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.	GET
IP-MIB::icmpOutEchos	The number of ICMP Echo (request) messages sent.	GET
IP-MIB::icmpOutEchoReps	The number of ICMP Echo Reply messages sent.	GET
IP-MIB::icmpOutTimestamps	The number of ICMP Timestamp (request) messages sent.	GET
IP-MIB::icmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.	GET
IP-MIB::icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.	GET
IP-MIB::icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.	GET
IP-MIB::icmpStatsTable	The table of generic system-wide ICMP counters.	GET TABLE
IP-MIB::icmpMsgStatsTable	The table of system-wide per-version, per-message type ICMP counters.	GET TABLE
TCP-MIB::tcpRtoAlgorithm	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.	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.	
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::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::tcpActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.	GET
TCP-MIB::tcpPassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.	GET
TCP-MIB::tcpAttemptFails	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 TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.	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
TCP-MIB::tcpOutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.	GET
TCP-MIB::tcpRetransSegs	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.	GET
TCP-MIB::tcpConnTable	A table containing TCP connection-specific information.	GET TABLE
TCP-MIB::tcpInErrs	The total number of segments received in error (e.g., bad TCP checksums).	GET
TCP-MIB::tcpOutRsts	The number of TCP segments sent containing the RST flag.	GET

TCP-MIB::tcpConnectionState	The state of this TCP connection. More information can be found here https://oidref.com/1.3.6.1.2.1.6.12	GET
TCP-MIB::tcpConnectionProcess	The number of packets received on this connection. This count includes retransmitted data.	GET
TCP-MIB::tcpListenerTable	A table containing information about TCP listeners. More information can be found here https://oidref.com/1.3.6.1.2.1.6.20	GET TABLE
UDP-MIB::udpInDatagrams	The total number of UDP datagrams delivered to UDP users.	GET
UDP-MIB::udpNoPorts	The total number of received UDP datagrams for which there was no application at the destination port.	GET
UDP-MIB::udpInErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port	GET
UDP-MIB::udpOutDatagrams	The total number of UDP datagrams sent from this entity.	GET
UDP-MIB::udpTable	A table containing UDP listener information.	GET TABLE
UDP-MIB::udpEndpointTable	A table containing UDP listener information.	GET TABLE
SNMPv2-MIB::snmpInPkts	The total number of messages delivered to the SNMP entity from the transport service.	GET
SNMPv2-MIB::snmpOutPkts	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.	GET
SNMPv2-MIB::snmpInBadVersions	The total number of SNMP messages which were delivered to the SNMP entity and were for an unsupported SNMP version.	GET
SNMPv2-MIB::snmpInBadCommunityNames	The total number of SNMP Messages delivered to the SNMP protocol entity which used a SNMP community name not known to said entity.	GET
SNMPv2-MIB::snmpInBadCommunityUses	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.	GET
SNMPv2-MIB::snmpInASNParseErrs	The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.	GET
SNMPv2-MIB::snmpInTooBigs	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'.	GET
SNMPv2-MIB::snmpInNoSuchNames	The total numb er of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was `noSuchName'.	GET
SNMPv2-MIB::snmpInBadValues	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'.	GET
SNMPv2-MIB::snmpInReadOnlys	The total number valid SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was `readOnly'. It should be noted that it is a protocol error to generate an SNMP PDU which contains the value `readOnly' in the error-status field, as such this object is provided as a means of detecting incorrect implementations of the SNMP.	GET
SNMPv2-MIB::snmpInGenErrs	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 `genErr'.	GET
SNMPv2-MIB::snmpInTotalReqVars	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 and Get-Next PDUs.	GET
SNMPv2-MIB::snmpInTotalSetVars	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.	GET
SNMPv2-MIB::snmpInGetRequests	The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpInGetNexts	The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpInSetRequests	The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpInGetResponses	The total number of SNMP Get-Response PDUs which have been accepted and processed by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpInTraps	The total number of SNMP Trap PDUs which have been accepted and processed by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpOutTooBigs	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.'	GET
SNMPv2-MIB::snmpOutNoSuchNames	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status was `noSuchName'.	GET
SNMPv2-MIB::snmpOutBadValues	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 `badValue'.	GET
SNMPv2-MIB::snmpOutGenErrs	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 `genErr'.	GET
SNMPv2-MIB::snmpOutGetRequests	The total number of SNMP Get-Request PDUs which have been generated by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpOutGetNexts	The total number of SNMP Get-Next PDUs which have been generated by the SNMP protocol entity.	GET

SNMPv2-MIB::snmpOutSetRequests	The total number of SNMP Set-Request PDUs which have been generated by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpOutGetResponses	The total number of SNMP Get-Response PDUs which have been generated by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpOutTraps	The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity.	GET
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.	GET
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 PDU (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.	GET
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 PDU (such as a Response-PDU) could be returned.	GET
HOST-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.	GET
HOST-RESOURCES-MIB::hrSystemDate	The host's notion of the local date and time of day.	GET
HOST-RESOURCES-MIB::hrSystemInitialLoadDevice	The index of the hrDeviceEntry for the device from which this host is configured to load its initial operating system configuration.	GET
HOST-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.	GET
MTA-MIB::mtaTable	The table holding information specific to an MTA.	GET TABLE
MTA-MIB::mtaGroupTable	The table holding information specific to each MTA group.	GET TABLE
IF-MIB::ifXTable	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.	GET 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 network management subsystem, then this object contains a zero value.	GET
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	GET
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.	GET
IPV6-MIB::ipv6Interfaces	The number of IPv6 interfaces (regardless of their current state) present on this system.	GET
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.	GET TABLE
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/1.3.6.1.2.1.88.1.1.1	GET
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/1.3.6.1.2.1.88.1.1.2	GET
DISMAN-EVENT-MIB::mteResourceSampleInstances	The number of currently active instance entries as defined for mteResourceSampleInstanceMaximum.	GET
DISMAN-EVENT-MIB::mteResourceSampleInstancesHigh	The highest value of mteResourceSampleInstances that has occurred since initialization of the management system.	GET
DISMAN-EVENT-MIB::mteResourceSampleInstanceLacks	The number of times this system could not take a new sample because that allocation would have exceeded the limit set by mteResourceSampleInstanceMaximum.	GET
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.	GET
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.	GET TABLE
DISMAN-EVENT-MIB::mteEventTable	A table of management event action information.	GET TABLE
DISMAN-EVENT-MIB::mteEventNotificationTable	A table of information about notifications to be sent as a consequence of management events.	GET TABLE

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/1.3.6.1.2.1.92.1.1.1	GET
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.	GET
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.	GET
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 iscarded due to the value of nlmConfigGlobalAgeOut.	GET
SNMPv2-SMI::enterprises.3582		GET
NET-SNMP-AGENT-MIB::nsModuleName	The module name that registered this OID.	GET
NET-SNMP-AGENT-MIB::nsModuleModes	The modes that the particular lower level handler can cope with directly.	GET
NET-SNMP-AGENT-MIB::nsModuleTimeout	The registered timeout. This is only meaningful for handlers that expect to return results at a later date (subagents, etc)	GET
NET-SNMP-EXTEND-MIB::nsExtendNumEntries	The number of rows in the nsExtendConfigTable.	GET
NET-SNMP-AGENT-MIB::nsCacheDefaultTimeout	Default cache timeout value (unless overridden for a particular cache entry).	GET
NET-SNMP-AGENT-MIB::nsCacheEnabled	Whether data caching is active overall.	GET
NET-SNMP-AGENT-MIB::nsCacheTimeout	The length of time (?in seconds) for which the data in this particular cache entry will remain valid.	GET
NET-SNMP-AGENT-MIB::nsCacheStatus	The current status of this particular cache entry. Acceptable values for Set requests are 'enabled(1)', 'disabled(2)' or 'empty(3)' (to clear all cached data). Requests to read the value of such an object will return 'disabled(2)' through to 'expired(5)'.	GET
NET-SNMP-AGENT-MIB::nsDebugEnabled	Whether the agent is configured to generate debugging output	GET
NET-SNMP-AGENT-MIB::nsDebugOutputAll	Whether the agent is configured to display all debugging output rather than filtering on individual debug tokens. Nothing willbe generated unless nsDebugEnabled is also true(1)	GET
NET-SNMP-AGENT-MIB::nsDebugDumpPdu	Whether the agent is configured to display raw packet dumps. This is unrelated to the nsDebugEnabled setting.	GET
NET-SNMP-AGENT-MIB::nsLogType	The (minimum) priority level for which this logging entry should be applied.	GET
NET-SNMP-AGENT-MIB::nsLogMaxLevel	The maximum priority level for which this logging entry should be applied.	GET
NET-SNMP-AGENT-MIB::nsLogStatus	Whether to generate logging output for this entry. Note that is valid for an instance to be left with the value notInService(2) indefinitely - i.e. the meaning of 'abnormally long' (see RFC 2579, RowStatus) for this table is infinite.	GET
NET-SNMP-VACM-MIB::nsVacmContextMatch	If the value of this object is exact(1), then all rows where the contextName exactly matches vacmAccessContextPrefix are selected. If the value of this object is prefix(2), then all rows where the contextName whose starting octets exactly match vacmAccessContextPrefix 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.	GET
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.	GET
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.	GET
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.	GET
SNMPv2-SMI::enterprises.20974.554.1	AMI SNMP Hostname Extension	GET
SNMPv2-SMI::enterprises.20974.554.2	AMI SNMP MIB library to return the system health status like power and sensor status.	GET
SNMPv2-SMI::enterprises.20974.554.3	AMI SNMP Platform Info Extension	GET

Parallel configuration

{This article details automation of platform configuration and application deployment use cases.}
Table of contents

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 those 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. Theses 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:

OS environment	64bits - application name
UEFI shell	SceEfi64.efi

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.

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 cases for using the AMISCE tool.

Extracting all the BIOS options

Refer to Accessing the BIOS for access instructions.

<table>
<tr><td>Step_1</td><td colspan="2">(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 .</td></tr>
<tr><td>Step_2</td><td>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.</td><td>Output example:
// Script File Name : MySet.txt
// Created on 10/21/19 at 10:11:12
// Copyright (c) 1985-2019, American Megatrends International LLC.
// All rights reserved. Subject to AMI licensing agreement.
// AMISCE Utility. Ver 5.03.1129
HIICrc32= 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
[...]</td></tr>
</table>

NOTES:

- In the Setup script file generated (**MySet.txt**):
  - D o 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 HIICrc32 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
	// Copyright (c) 1985-2019, American Megatrends International LLC.
	// All rights reserved. Subject to AMI licensing agreement.
	// AMISCE Utility. Ver 5.03.1129
	//Comment on change made
	HIICrc32= 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. **[AMISCE]** /i /s **MyFutureOptions.txt** /ds /b /lang **en-US** Command description: • **/i** - Indicates Import modified script file to the NVRAM (into the BIOS Setup). • **/s** - I ndicates 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 ca nnot 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

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.
		// All rights reserved. Subject to AMI licensing agreement.
		// AMISCE Utility. Ver 5.03.1129
		HIICrc32= 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**):
  - D o 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 Sting, 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 for 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:
		Setup Question = SR-IOV Support
		Map String = PCIS007
		Token =52
		// Do NOT change this line
		Offset =C9
		Width =01
		BIOS Default =[01]Enabled
		Options =[00]Disabled //
		Move "*" to the desired Option
		*[01]Enabled

Step_2	From the OS, use the following command to get one BIOS Setup option with Map String value. **[AMISCE]** /o /lang **en-US** /ms **[QUESTION_MAP_STRING]** [/q] [/d] /hb /ds Command description: • **/o** - Outputs content to the standard output (screen) • **/lang** - Enables mapping language mode (Lang Code = en-US and/or x-UEFI-AMI and/or nothing) • **/ms** - Indicates Map String of the Setup Question • **/q** - Indicates Quiet mode • **/d** - Skip checking for AptioV BIOS and behave normally • **/hb** - Hides tool information banner • **/ds** - Indicates BIOS Standard Default Value	**Example:** FS1:\> SceEfi64.efi /o /lang en-US /ms **PCIS007** /ds /hb BIOS Default =[01]Enabled Options =[00]Disabled *[01]Enabled
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

Step_1	(Optional) Search the Setup file extracted in the previous step (MySet.txt) to confirm the Setup Question of the BIOS Setup option. In the example, the Setup Question is "SR-IOV Support".	**Example:**
		Setup Question = SR-IOV Support
		Map String = PCIS007
		Token =52
		// Do NOT change this line
		Offset =C9
		Width =01
		BIOS Default =[01]Enabled
		Options =[00]Disabled // Move "*" to the desired Option
		*[01]Enabled

Step_2	(Optional) Note the BIOS Setup option and proceed to set it if required (see next section).	

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 /ms **[QUESTION_MAP_STRING]** /qv **[<QUESTION_VALUE>]** /lang **en-US** [/bt <device type>] [/q] [/d] /ds [/hb] [/ni] [/shutdown] [/reboot] Command description: **NOTE:** Values of type numeric will be taken as hex always (0x prefix optional). • **/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 • **/lang** - Enables mapping language mode (Lang Code = en-US and/or x-UEFI-AMI and/or nothing) • **/bt** - Indicates the device type for legacy boot device • **/q** - Indicates Quiet mode • **/d** - Skip checking for AptioV BIOS and behave normally • **/ds** - 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 /lang en-US /ds

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 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 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 /lang **en-US** /ms " **[SETUP_QUESTION]** " /qv **[<QUESTION_VALUE>]** /ds Command description: **NOTE:** Values of type numeric will be taken as hex always (0x prefix optional). • **/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 • **/lang** - Enables mapping language mode (Lang Code = en-US and/or x-UEFI-AMI and/or nothing) • **/bt** - Indicates the device type for legacy boot device • **/q** - Indicates Quiet mode • **/d** - Skip checking for AptioV BIOS and behave normally • **/ds** - 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 /lang en-US /ms "SR-IOV Support" /qv 01 /ds
Step_2	Validate the BIOS Setup value was changed. **[AMISCE]** /o /lang **en-US** /ms " **[SETUP_QUESTION]** " /ds	**Output example:** BIOS Default =[01]PCI Mode Options =[00]LPC Bus *[01]PCI Mode

Operating the AMISCE tool - use case 3 - changing the boot order

This section describes how to change the boot order using indexes in an option list. It p rovides 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. **[AMISCE]** /o /lang **en-US** /ms **SETUP006** /ds /hb 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** "<question value>" . **[AMISCE]** /i /lang **en-US** /ms **SETUP006** /qv " **index1,index2,index3,index4,index5,index6,index7** " /hb Question value imported successfully	**Example:** SceEfi64.efi /i /lang en-US /ms SETUP006 /qv "1,d,e,5,6,2,f" /hb 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	**[AMISCE]** /apwd **<new admin password>** /upwd **<new user password>** /lang **en-US** /hb OU **[AMISCE]** /apwdf **<file having new admin password>** /upwdf **<file having new user password>** /lang **en-US** /hb

Modifying a password

Step_1	**[AMISCE]** /cpwd **<current admin password>** /apwd **<new admin password>** /upwd **<new user password>** /lang **en-US** /hb Or **[AMISCE]** /cpwdf **<file having current admin password>** /apwdf **<file having new admin password>** /upwdf **<file having new user password>** /lang **en-US** /hb	**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.

Attribute	Description
[/cpwd]	Indicates the admin password of type Unicode.
[/cpwds]	Indicates the admin password of type scan code.
[/cpwde]	Indicates the admin password of type EFI key.
[/apwd]	Indicates the new admin password of type Unicode.
[/apwds]	Indicates new admin password of type scan code.
[/apwde]	Indicates new admin password of type EFI key.
[/upwd]	Indicates new user password of type Unicode.
[/upwds]	Indicates new user password of type scan code.
[/upwde]	Indicates new user password of type EFI key.
[/cpwdf]	Indicates file having admin password of type Unicode.
[/cpwdsf]	Indicates file having admin password of type scan code.
[/cpwdef]	Indicates file having admin password of type EFI key.
[/apwdf]	Indicates file having new admin password of type Unicode.
[/apwdsf]	Indicates file having new admin password of type scan code.
[/apwdef]	Indicates file having new admin password of type EFI key.
[/upwdf]	Indicates files having a new user password of type Unicode.
[/upwdsf]	Indicates file having a new user password of type scan code.
[/upwdef]	Indicates file having new user password of type EFI key.
[/hb]	Optional command-line option to hide the tool information banner.

CG2400 SNMP - BMC User guide

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

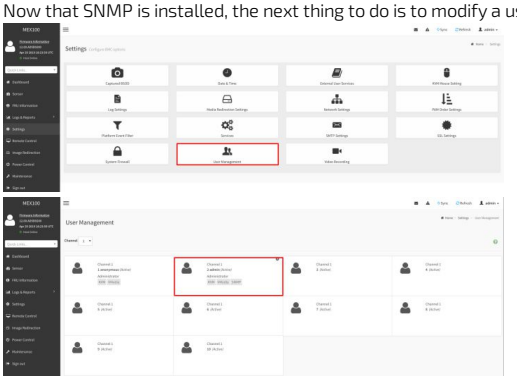
```
$ apt-get install snmp
```

To be able to see Human readable MIB (instead of seeing the OID), also install the following package

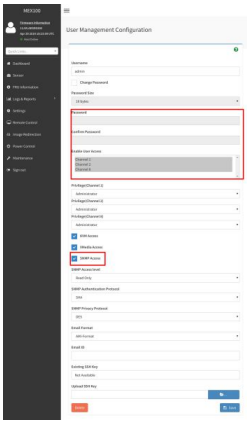
```
$ apt-get install snmp-mibs-downloader
```

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 commnad, using the user created at the previous step:

```
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:

```
$ 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:

```
$ 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
SNMPv2-SMI::enterprises.20974.554.2.1.1.21 = INTEGER: 21
SNMPv2-SMI::enterprises.20974.554.2.1.2.21 = STRING: "Fan1 Speed"
SNMPv2-SMI::enterprises.20974.554.2.1.3.21 = INTEGER: 45
SNMPv2-SMI::enterprises.20974.554.2.1.4.21 = Opaque: Float: 1640.00000
```

The following MIBs are supported on CG2400:

MIB	OID
SNMPv2-MIB	1.3.6.1.6.3.1
DISMAN-EVENT-MIB	1.3.6.1.2.1.88
IF-MIB	1.3.6.1.2.1.31
IP-FORWARD-MIB	1.3.6.1.2.1.4.24
SNMPv2-SMI	1.3.6.1.2.1
IP-MIB	1.3.6.1.2.1.48
TCP-MIB	1.3.6.1.2.1.49
MTA-MIB	1.3.6.1.2.1.28
IPV6-MIB	1.3.6.1.2.1.55
NOTIFICATION-LOG-MIB	1.3.6.1.2.1.92
NET-SNMP-VACM-MIB	1.3.6.1.4.1.8072.1.9.1.1
NET-SNMP-AGENT-MIB	1.3.6.1.4.1.8072.1.1
UDP-MIB	1.3.6.1.2.1.7

Here's a table of the possible informations that can be found via SNMP on the BMC.

OID	Description	Action
SNMPv2-MIB::sysObjectID.0		
DISMAN-EVENT-MIB::sysUpTimeInstance	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.	GET
SNMPv2-MIB::sysContact.0	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.	GET SET
SNMPv2-MIB::sysName.0	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.	GET SET
SNMPv2-MIB::sysLocation.0	The physical location of this node (e.g.,`telephone closet, 3rd floor').	GET SET
SNMPv2-MIB::sysORLastChange.0	The value of sysUpTime at the time of the most recent change in state or value of any instance of sysORID.	GET
SNMPv2-MIB::sysORTable	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.	GET TABLE
IF-MIB::ifNumber.0	The number of network interfaces (regardless of their current state) present on this system.	GET
IF-MIB::ifTable	A list of interface entries. The number of entries is given by the value of ifNumber. The entries consist of these fields. Index, Descr, Type, Mtu, Speed, PhysAddress, AdminStatus, OperStatus, LastChange, InOctets, InUcastPkts, InNUcastPkts, InDiscards, InErrors InUnknownProtos, OutOctets, OutUcastPkts, OutNUcastPkts, OutDiscards, OutErrors, OutQLen.	GET TABLE
1.3.6.1.2.1.3.1.1.1	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.	GET
1.3.6.1.2.1.3.1.1.2	The media-dependent `physical' address.	GET
1.3.6.1.2.1.3.1.1.3	The NetworkAddress (e.g., the IP address) corresponding to the media-dependent `physical' address.	GET
IP-MIB::ipForwarding	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).	GET
IP-MIB::ipDefaultTTL	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.	GET
IP-MIB::ipInReceives	The total number of input datagrams received from interfaces, including those received in error.	GET
IP-MIB::ipInAddrErrors	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.	GET
IP-MIB::ipForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source- Routed via this entity, and the Source- Route option processing was successful.	GET
IP-MIB::ipInUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.	GET
IP-MIB::ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.	GET
IP-MIB::ipInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).	GET
IP-MIB::ipOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for	GET

	transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.	
IP-MIB::ipOutDiscards	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 ipForwDatagrams if any such packets met this (discretionary) discard criterion.	GET
IP-MIB::ipOutNoRoutes	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 ipForwDatagrams which meet this `no-route' criterion. Note that this includes any datagarms which a host cannot route because all of its default gateways are down.	GET
IP-MIB::ipReasmTimeout	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.	GET
IP-MIB::ipReasmReqds	Number of IP fragments received which needed to be reassembled at this entity.	GET
IP-MIB::ipReasmOKs	Number of IP datagrams successfully re-assembled.	GET
IP-MIB::ipReasmFails	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 815) can lose track of the number of fragments by combining them as they are received.	GET
IP-MIB::ipFragCreates	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.	GET
IP-MIB::ipFragFails	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.	GET
IP-MIB::ipFragOKs	Number of IP datagrams that have been successfully fragmented at this entity.	GET
IP-MIB::ipAddrTable	Table of addressing information relevant to this entity's IP addresses.	GET TABLE
1.3.6.1.2.1.4.21	IP Routing table.	GET
IP-MIB::ipNetToMediaTable	IP Address Translation table used for mapping from IP addresses to physical addresses.	GET TABLE
IP-MIB::ipRoutingDiscards	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.	GET
IP-FORWARD-MIB::ipCidrRouteTable	This entity's IP Routing table.	GET TABLE
IP-FORWARD-MIB::inetCidrRouteNumber	The number of current ipCidrRouteTable entries that are not invalid.	GET
IP-FORWARD-MIB::inetCidrRouteTable	This entity's IP Routing table.	GET 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.	GET
IP-MIB::ipv6IpDefaultHopLimit	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.	GET
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.	GET TABLE
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.	GET
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.	GET TABLE
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	GET TABLE
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	GET
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	GET TABLE
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.	GET TABLE
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.	GET TABLE
IP-MIB::ipDefaultRouterTable	The table used to describe the default routers known to this entity.	GET TABLE

IP-MIB::icmpInMsgs	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.	GET
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::icmpInParmProbs	Number of ICMP Parameter Problem messages received.	GET
IP-MIB::icmpInSrcQuenchs	Number of ICMP Source Quench messages received.	GET
IP-MIB::icmpInRedirects	Number of ICMP Redirect messages received.	GET
IP-MIB::icmpInEchos	Number of ICMP Echo (request) messages received.	GET
IP-MIB::icmpInEchoReps	Number of ICMP Echo Reply messages received.	GET
IP-MIB::icmpInTimestamps	Number of ICMP Timestamp (request) messages received.	GET
IP-MIB::icmpInTimestampReps	Number of ICMP Timestamp Reply messages received.	GET
IP-MIB::icmpInAddrMasks	Number of ICMP Address Mask Request messages received.	GET
IP-MIB::icmpInAddrMaskReps	Number of ICMP Address Mask Reply messages received.	GET
IP-MIB::icmpOutMsgs	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.	GET
IP-MIB::icmpOutErrors	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should notinclude errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.	GET
IP-MIB::icmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.	GET
IP-MIB::icmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.	GET
IP-MIB::icmpOutParmProbs	The number of ICMP Parameter Problem messages sent.	GET
IP-MIB::icmpOutSrcQuenchs	The number of ICMP Source Quench messages sent.	GET
IP-MIB::icmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.	GET
IP-MIB::icmpOutEchos	The number of ICMP Echo (request) messages sent.	GET
IP-MIB::icmpOutEchoReps	The number of ICMP Echo Reply messages sent.	GET
IP-MIB::icmpOutTimestamps	The number of ICMP Timestamp (request) messages sent.	GET
IP-MIB::icmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.	GET
IP-MIB::icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.	GET
IP-MIB::icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.	GET
IP-MIB::icmpStatsTable	The table of generic system-wide ICMP counters.	GET TABLE
IP-MIB::icmpMsgStatsTable	The table of system-wide per-version, per-message type ICMP counters.	GET TABLE
TCP-MIB::tcpRtoAlgorithm	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.	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.	
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::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::tcpActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.	GET
TCP-MIB::tcpPassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.	GET
TCP-MIB::tcpAttemptFails	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 TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.	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
TCP-MIB::tcpOutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.	GET
TCP-MIB::tcpRetransSegs	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.	GET
TCP-MIB::tcpConnTable	A table containing TCP connection-specific information.	GET TABLE
TCP-MIB::tcpInErrs	The total number of segments received in error (e.g., bad TCP checksums).	GET
TCP-MIB::tcpOutRsts	The number of TCP segments sent containing the RST flag.	GET
TCP-MIB::tcpConnectionState	The state of this TCP connection. More information can be found here https://oidref.com/1.3.6.1.2.1.6.12	GET
TCP-MIB::tcpConnectionProcess	The number of packets received on this connection. This count includes retransmitted data.	GET
TCP-MIB::tcpListenerTable	A table containing information about TCP listeners. More information can be found here https://oidref.com/1.3.6.1.2.1.6.20	GET TABLE
UDP-MIB::udpInDatagrams	The total number of UDP datagrams delivered to UDP users.	GET
UDP-MIB::udpNoPorts	The total number of received UDP datagrams for which there was no application at the destination port.	GET
UDP-MIB::udpInErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port	GET
UDP-MIB::udpOutDatagrams	The total number of UDP datagrams sent from this entity.	GET
UDP-MIB::udpTable	A table containing UDP listener information.	GET TABLE
UDP-MIB::udpEndpointTable	A table containing UDP listener information.	GET TABLE
SNMPv2-MIB::snmpInPkts	The total number of messages delivered to the SNMP entity from the transport service.	GET
SNMPv2-MIB::snmpOutPkts	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.	GET
SNMPv2-MIB::snmpInBadVersions	The total number of SNMP messages which were delivered to the SNMP entity and were for an unsupported SNMP version.	GET
SNMPv2-MIB::snmpInBadCommunityNames	The total number of SNMP Messages delivered to the SNMP protocol entity which used a SNMP community name not known to said entity.	GET
SNMPv2-MIB::snmpInBadCommunityUses	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.	GET
SNMPv2-MIB::snmpInASNParseErrs	The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.	GET
SNMPv2-MIB::snmpInTooBigs	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'.	GET
SNMPv2-MIB::snmpInNoSuchNames	The total numb er of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was `noSuchName'.	GET
SNMPv2-MIB::snmpInBadValues	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'.	GET
SNMPv2-MIB::snmpInReadOnlys	The total number valid SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was `readOnly'. It should be noted that it is a protocol error to generate an SNMP PDU which contains the value `readOnly' in the error-status field, as such this object is provided as a means of detecting incorrect implementations of the SNMP.	GET
SNMPv2-MIB::snmpInGenErrs	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 `genErr'.	GET
SNMPv2-MIB::snmpInTotalReqVars	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 and Get-Next PDUs.	GET
SNMPv2-MIB::snmpInTotalSetVars	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.	GET
SNMPv2-MIB::snmpInGetRequests	The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpInGetNexts	The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpInSetRequests	The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpInGetResponses	The total number of SNMP Get-Response PDUs which have been accepted and processed by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpInTraps	The total number of SNMP Trap PDUs which have been accepted and processed by the SNMP protocol entity.	GET

SNMPv2-MIB::snmpInTraps	The total number of SNMP Trap PDUs which have been accepted and processed by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpOutTooBigs	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.'	GET
SNMPv2-MIB::snmpOutNoSuchNames	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status was `noSuchName'.	GET
SNMPv2-MIB::snmpOutBadValues	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 `badValue'.	GET
SNMPv2-MIB::snmpOutGenErrs	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 `genErr'.	GET
SNMPv2-MIB::snmpOutGetRequests	The total number of SNMP Get-Request PDUs which have been generated by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpOutGetNexts	The total number of SNMP Get-Next PDUs which have been generated by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpOutSetRequests	The total number of SNMP Set-Request PDUs which have been generated by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpOutGetResponses	The total number of SNMP Get-Response PDUs which have been generated by the SNMP protocol entity.	GET
SNMPv2-MIB::snmpOutTraps	The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity.	GET
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.	GET
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 PDU (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.	GET
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 PDU (such as a Response-PDU) could be returned.	GET
HOST-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.	GET
HOST-RESOURCES-MIB::hrSystemDate	The host's notion of the local date and time of day.	GET
HOST-RESOURCES-MIB::hrSystemInitialLoadDevice	The index of the hrDeviceEntry for the device from which this host is configured to load its initial operating system configuration.	GET
HOST-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.	GET
MTA-MIB::mtaTable	The table holding information specific to an MTA.	GET TABLE
MTA-MIB::mtaGroupTable	The table holding information specific to each MTA group.	GET TABLE
IF-MIB::ifXTable	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.	GET 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 network management subsystem, then this object contains a zero value.	GET
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	GET
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.	GET
IPV6-MIB::ipv6Interfaces	The number of IPv6 interfaces (regardless of their current state) present on this system.	GET
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.	GET TABLE
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/1.3.6.1.2.1.88.1.1.1	GET
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/1.3.6.1.2.1.88.1.1.2	GET
DISMAN-EVENT-MIB::mteResourceSampleInstances	The number of currently active instance entries as defined for mteResourceSampleInstanceMaximum.	GET
DISMAN-EVENT-MIB::mteResourceSampleInstancesHigh	The highest value of mteResourceSampleInstances that has occurred since initialization of the management system.	GET
DISMAN-EVENT-	The number of times this system could not take a new sample because that allocation would have exceeded	GET

MIB::mteResourceSampleInstanceLacks	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.	GET
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.	GET TABLE
DISMAN-EVENT-MIB::mteEventTable	A table of management event action information.	GET TABLE
DISMAN-EVENT-MIB::mteEventNotificationTable	A table of information about notifications to be sent as a consequence of management events.	GET TABLE
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/1.3.6.1.2.1.92.1.1.1	GET
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.	GET
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.	GET
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 iscarded due to the value of nlmConfigGlobalAgeOut.	GET
SNMPv2-SMI::enterprises.3582		GET
NET-SNMP-AGENT-MIB::nsModuleName	The module name that registered this OID.	GET
NET-SNMP-AGENT-MIB::nsModuleModes	The modes that the particular lower level handler can cope with directly.	GET
NET-SNMP-AGENT-MIB::nsModuleTimeout	The registered timeout. This is only meaningful for handlers that expect to return results at a later date (subagents, etc)	GET
NET-SNMP-EXTEND-MIB::nsExtendNumEntries	The number of rows in the nsExtendConfigTable.	GET
NET-SNMP-AGENT-MIB::nsCacheDefaultTimeout	Default cache timeout value (unless overridden for a particular cache entry).	GET
NET-SNMP-AGENT-MIB::nsCacheEnabled	Whether data caching is active overall.	GET
NET-SNMP-AGENT-MIB::nsCacheTimeout	The length of time (?in seconds) for which the data in this particular cache entry will remain valid.	GET
NET-SNMP-AGENT-MIB::nsCacheStatus	The current status of this particular cache entry. Acceptable values for Set requests are 'enabled(1)', 'disabled(2)' or 'empty(3)' (to clear all cached data). Requests to read the value of such an object will return 'disabled(2)' through to 'expired(5)'.	GET
NET-SNMP-AGENT-MIB::nsDebugEnabled	Whether the agent is configured to generate debugging output	GET
NET-SNMP-AGENT-MIB::nsDebugOutputAll	Whether the agent is configured to display all debugging output rather than filtering on individual debug tokens. Nothing willbe generated unless nsDebugEnabled is also true(1)	GET
NET-SNMP-AGENT-MIB::nsDebugDumpPdu	Whether the agent is configured to display raw packet dumps. This is unrelated to the nsDebugEnabled setting.	GET
NET-SNMP-AGENT-MIB::nsLogType	The (minimum) priority level for which this logging entry should be applied.	GET
NET-SNMP-AGENT-MIB::nsLogMaxLevel	The maximum priority level for which this logging entry should be applied.	GET
NET-SNMP-AGENT-MIB::nsLogStatus	Whether to generate logging output for this entry. Note that is valid for an instance to be left with the value notInService(2) indefinitely - i.e. the meaning of 'abnormally long' (see RFC 2579, RowStatus) for this table is infinite.	GET
NET-SNMP-VACM-MIB::nsVacmContextMatch	If the value of this object is exact(1), then all rows where the contextName exactly matches vacmAccessContextPrefix are selected. If the value of this object is prefix(2), then all rows where the contextName whose starting octets exactly match vacmAccessContextPrefix 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.	GET
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.	GET
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.	GET
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.	GET
SNMPv2-SMI::enterprises.20974.554.1	AMI SNMP Hostname Extension	GET
SNMPv2-SMI::enterprises.20974.554.2	AMI SNMP MIB library to return the system health status like power and sensor status.	GET
SNMPv2-SMI::enterprises.20974.554.3	AMI SNMP Platform Info Extension	GET

SNMPv2-SMI::enterprises.20974.994.3	AMI-SNMP-Platform-Info-Extension	GET

Tool

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

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

CG2300	CG2400	Notes
Menu → Boot Manager	Menu → Save & Exit → Section Boot Override	
Menu → Advanced → USB Configuration → Make USB Devices Non-Bootable [Enabled / **Disabled**]	Menu → Advanced → USB Configuration → USB Mass Storage Driver Support [**Enabled** / Disabled]	
Menu → Boot Maintenance Manager → Advanced Boot Options → Boot Option Retry [Enabled / **Disabled**]	Not present in AMI SETUP	Boot Option Retry is always enabled on the CG2400.
Menu → Boot Maintenance Manager → Advanced Boot Options → USB Boot Priority [**Enabled** / Disabled]	Not present in AMI SETUP	
Menu → Boot Maintenance Manager → Add EFI Boot Option → <Dynamic list of EFI Boot Options>	Menu → Boot → Section Boot Option Priorities	
Menu → Boot Maintenance Manager → Delete EFI Boot Option → <Dynamic list of EFI Boot Options>	Not present in AMI SETUP	
Menu → Boot Maintenance Manager → Change Boot Order → <Dynamic list of EFI Boot Options>	Not present in AMI SETUP	

Networking

Network interface availability

CG2300	CG2400	Notes
Menu → Advanced → PCI Configuration → NIC Configuration → Nic1 Controller [**Enabled** / Disabled]	Menu → Socket Configuration → IIO Configuration → Socket0 Configuration → Socket 0 PcieBr1D02F0 - Port 1C (PCIe Uplink) → PCI-E Port [**Auto** / Disable / Enable]	On the CG2400, both controllers are auto/enabled/disabled at the same time.
Menu → Advanced → PCI Configuration → NIC Configuration → Nic1 Port1 [**Enabled** / Disabled] Menu → Advanced → PCI Configuration → NIC Configuration → Nic1 Port2 [**Enabled** / Disabled]	Not present in AMI SETUP	On the CG2300, this option is only available if Nic1 Controller is enabled.

Preboot Execution Environment (PXE)

CG2300	CG2400	Notes
Menu → Advanced → PCI Configuration → NIC Configuration → Nic1 Port1 PXE [**Enabled** / Disabled]	Menu → Advanced → Option ROM Dispatch Policy → On Board Network Controller [**Enabled** / Disabled]	On the CG2300, this option is only available if Nic1 Controller is enabled.

iSCSI

CG2300	CG2400	Notes
Menu → Advanced → PCI Configuration → UEFI Option ROM Control → iSCSI Configuration	Menu → Advanced → iSCSI Configuration → *	

Network stack

CG2300	CG2400	Notes
Menu → Advanced → PCI Configuration → UEFI Network Stack → UEFI Network Stack [**Enabled** / Disabled]	Menu → Advanced → Network Stack Configuration → Network Stack [**Enabled** / Disabled]	
Menu → Advanced → PCI Configuration → UEFI Network Stack → IPv4 PXE Support [**Enabled** / Disabled]	Menu → Advanced → Network Stack Configuration → Ipv4 PXE Support [**Enabled** / Disabled] Menu → Advanced → Network Stack Configuration → Ipv4 HTTP Support [Enabled / **Disabled**]	On the CG2400, t his option is only available if UEFI Network Stack is enabled.
Menu → Advanced → PCI Configuration → UEFI Network Stack → IPv6 PXE Support [**Enabled** / Disabled]	Menu → Advanced → Network Stack Configuration → Ipv6 PXE Support [Enabled / **Disabled**] Menu → Advanced → Network Stack Configuration → Ipv6 HTTP Support [Enabled / **Disabled**]	On the CG2400, t his option is only available if UEFI Network Stack is enabled.
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]	Menu → Advanced → Intel(R) Ethernet Connection X722 for 10GBASE-T - ***<MAC-ADDRESS-1>*** → Nic Configuration → Link Speed [**Auto Negotiated**]	On the CG2400, this option is read only.
Menu → Advanced → PCI Configuration → UEFI Option ROM Control → Intel(R) I350 Gigabit Network Connection - <MAC Address of NIC1> → Blink LEDs [**0** / <Number>]	Menu → Advanced → Intel(R) Ethernet Connection X722 for 10GBASE-T - ***<MAC-ADDRESS-1>*** → Blink LEDs [**0** / <0-15>]	
Menu → Advanced → PCI Configuration → UEFI Option ROM Control → Intel(R) I350 Gigabit Network Connection - <MAC Address of NIC1> - VLAN Configuration → Enter Configuration Menu → *	Menu → Advanced → VLAN Configuration (MAC: ***<MAC-ADDRESS-1>***) → Enter Configuration Menu → *	
Menu → Advanced → PCI Configuration → UEFI Option ROM Control → Intel(R) I350 Gigabit Network Connection - <MAC Address of NIC1> - IPv4 Current settings → *	Menu → Advanced → MAC: ***<MAC-ADDRESS-1>*** -IPv4 Network Configuration → Enter Configuration Menu → *	
Menu → Advanced → PCI Configuration → UEFI Option ROM Control → Intel(R) I350 Gigabit Network Connection - <MAC Address of NIC1> - IPv6 Current settings → Enter Configuration Menu → *	Menu → Advanced → MAC: ***<MAC-ADDRESS-1>*** -IPv6 Network Configuration → Enter Configuration Menu → *	

BIOS password

CG2300	CG2400	Notes
Menu → Security → Set Administrator Password	Menu → Security → Administrator Password	
Menu → Security → Set User Password	Menu → Security → User Password	
Menu → Security → Power On Password	Not present in AMI SETUP	On the CG2400, User Password serves as the Power On Password.

Power management

CG2300	CG2400	Notes
Menu → Advanced → Power & Performance → CPU Power and Performance Policy [Performance / **Balanced**	Not present in AMI SETUP	

Performance / Balanced Power / Power]		
Menu → Advanced → Power & Performance → Workload Configuration [**Balanced** / I/O Sensitive]	Menu → Socket Configuration → Advanced Power Management Configuration → CPU - Advanced PM Tuning → Energy Perf BIAS → Workload Configuration [**Balanced** / I/O Sensitive]	
Menu → Advanced → Power & Performance → Uncore Power Management → Uncore Frequency Scaling [**Enabled** / Disabled]	Menu → Socket Configuration → Advanced Power Management Configuration → CPU P State Control → Uncore Freq Scaling (UFS) [**Enable** / Disable]	
Menu → Advanced → Power & Performance → Uncore Power Management → Performance P-limit [**Enabled** / Disabled]	Menu → Socket Configuration → Advanced Power Management Configuration → CPU P State Control → Perf P-Limit → *	
Menu → Advanced → Power & Performance → CPU P State Control → Enhanced Intel SpeedStep(R) Tech [**Enabled** / Disabled]	Menu → Socket Configuration → Advanced Power Management Configuration → CPU P State Control → SpeedStep (Pstates) [Disable / **Enable**]	
Menu → Advanced → Power & Performance → CPU P State Control → Intel Configurable TDP [Enabled / **Disabled**]	Menu → Socket Configuration → Advanced Power Management Configuration → CPU P State Control → Config TDP [**Normal** / Level 1 / Level 2]	
Menu → Advanced → Power & Performance → CPU P State Control → Intel(R) Turbo Boost Technology [**Enabled** / Disabled]	Menu → Socket Configuration → Advanced Power Management Configuration → CPU P State Control → Turbo Mode [**Enable** / Disable]	
Menu → Advanced → Power & Performance → CPU P State Control → Energy Efficient Turbo [**Enabled** / Disabled]	Menu → Socket Configuration → Advanced Power Management Configuration → CPU P State Control → Energy Efficient Turbo [**Enable** / Disable]	
Menu → Advanced → Power & Performance → CPU HWPM State Control → Enable CPU HWPM [Enabled / **Disabled**]	Menu → Socket Configuration → Advanced Power Management Configuration → Hardware PM State Control → Hardware P-States [Disable / **Native Mode** / Out of Band Mode / Native Mode with No Legacy Support]	
Menu → Advanced → Power & Performance → CPU HWPM State Control → Enable CPU Autonomous Cstate [Enabled / **Disabled**]	Menu → Socket Configuration → Advanced Power Management Configuration → CPU C State Control → Autonomous Core C-State [Enable / **Disable**]	
Menu → Advanced → Power & Performance → CPU C State Control → CPU C-State [**Enabled** / Disabled]	Not present in AMI SETUP	
Menu → Advanced → Power & Performance → CPU C State Control → C1E Autopromote [**Enabled** / Disabled]	Menu → Socket Configuration → Advanced Power Management Configuration → CPU C State Control → Enhanced Halt State (C1E) [**Enable** / Disable]	
Menu → Advanced → Power & Performance → CPU C State Control → Processor C3 [Enabled / **Disabled**]	Not present in AMI SETUP	
Menu → Advanced → Power & Performance → CPU C State Control → Processor C6 [**Enabled** / Disabled]	Menu → Socket Configuration → Advanced Power Management Configuration → CPU C State Control → CPU C6 report [Disable / Enable / **Auto**]	
Menu → Server Management → Resume on AC Power Loss [**Stay off** / Last State / Power On]	Menu →Server Mgmt → Power Control Policy [Do Not PowerUp / Last Power State / Power Restore / **Unspecified**]	Stay Off = Do Not PowerUp Last State = Last Power State Power On = Power Restore On CG2400, the Unspecified value means that the policy stays as it was. The current value can be seen on

		value can be seen on the previous line.
Menu → Server Management → Power Restore Delay [**Disabled** / Auto / Fixed]	Not present in AMI SETUP	
Menu → Server Management → Power Restore Delay Value [**55** / <55-300>]	Not present in AMI SETUP	

Virtualization

CG2300	CG2400	Notes
Menu → Advanced → Processor Configuration → Intel(R) Virtualization Technology [Enabled/ **Disabled**]	Menu → Socket Configuration → Processor Configuration → VMX [**Enable** / Disable]	
Menu → Advanced → Integrated IO Configuration --> Intel(R) VT for Directed I/O [Enabled / **Disabled**]	Menu → Socket Configuration → IIO Configuration → Intel. VT for Directed I/O (VT-d) → Intel. VT for Directed I/O (VT-d) [Enable / **Disable**]	
Menu → Advanced → PCI Configuration → ARI Forwarding [Enabled / **Disabled**]	Menu → Platform Configuration → Miscellaneous Configuration → ARI Support [**Enable** / Disable] Menu → Platform Configuration → Miscellaneous Configuration → ARI Forward [Enable / **Disable**]	

Compatibility Support Module (CSM)

CG2300	CG2400	Notes
Not present in INTEL SETUP	Menu → Advanced → CSM Configuration → CSM Support [Enabled / **Disabled**]	
Menu → Boot Maintenance Manager → Advanced Boot Options → Boot Mode [UEFI / **Legacy**]	Menu → Advanced → CSM Configuration → Boot option filter [**UEFI and Legacy** / Legacy only / UEFI only]	On CG2400, this option is only available if CSM Support is enabled.
Menu → Boot Maintenance Manager → Advanced Boot Options → Video BIOS [**UEFI** / Legacy]	Menu → Advanced → CSM Configuration → Video [**UEFI** / Legacy]	On CG2400, this option is only available if CSM Support is enabled.

Security

Secure boot

CG2300	CG2400	Notes
Menu → Boot Maintenance Manager → Advance Boot Options → Secure Boot Configuration → Attempt Secure Boot [Enabled / **Disabled**]	Menu → Security → Secure Boot → Secure Boot [Enabled / **Disabled**]	

Trusted Platform Module (TPM)

CG2300	CG2400	Notes
Menu → Security → TPM Administrative Control [**No Operation** / Turn On / Turn Off / Clear Ownership]	Menu → Advanced → Trusted Computing → Security Device Support [**Enable** / Disable]	
Menu → Security → TPM2 Operation [**No Action** / TPM2 ClearControl(NO) + Clear]	Menu → Advanced → Trusted Computing → TPM2.0 UEFI Spec Version [TCG_1_2 / **TCG_2**]	On both platforms, TPM has to be inserted to see the menu.
Menu → Security → TPM FW Update [Enabled / **Disabled**]	Not present in AMI SETUP	On both platforms, TPM has to be inserted to see the menu. On CG2400, only the current firmware version is shown.
Menu → Advanced → PCI Configuration → UEFI Option ROM Control *(Dynamic Menu)*→ TrEE Configuration → Attempt TPM Device [Disable / **TPM 1.2** / TPM 2.0 (DTPM)]	Menu → Advanced → Trusted Computing → Device Select [TPM 1.2 / TPM 2.0 / **Auto**]	On both platforms, TPM has to be inserted to see the menu.

Trusted Execution Technology (TXT)

CG2300	CG2400	Notes
Menu → Advanced → Processor Configuration → Intel(R) TXT [Enabled / **Disabled**]	Menu → Socket Configuration → Processor Configuration → Enable Intel(R) TXT [Enable / **Disable**]	

Console redirection

CG2300	CG2400	Notes
Menu → Server Management → Console Redirection → SOL for Baseboard Mgmt [Enabled / **Disabled**]	Not present in AMI SETUP	On CG2400, when SOL is activated with IPMI, serial console redirection is deactivated on the front panel serial connector.
Menu → Server Management → Console Redirection → Console Redirection [**Disabled** / Serial Port A / Serial Port B]	Menu → Advanced → Serial Port Console Redirection → Console Redirection [**Enabled** / Disabled] Menu → Advanced → Serial Port Console Redirection → **Legacy** Console Redirection Settings → Redirection COM Port [**COM0**]	
Menu → Server Management → Console Redirection → Flow Control [None / **RTS/CTS**]	Menu → Advanced → Serial Port Console Redirection → Console Redirection Settings → Flow Control [**None** / Hardware RTS/CTS]	On the CG2300, the option is only shown if Console Redirection is enabled.
Menu → Server Management → Console Redirection → Baud Rate [9.6k / 19.2k / 38.4k / 57.6k / **115.2k**]	Menu → Advanced → Serial Port Console Redirection → Console Redirection Settings → Bits per second [9600 / 19200 / 38400 / 57600 / **115200**]	On the CG2300, the option is only shown if Console Redirection is enabled.
Menu → Server Management → Console Redirection → Terminal Type [PC-ANSI / **VT100** / VT100+ / VT-UTF8]	Menu → Advanced → Serial Port Console Redirection → Console Redirection Settings → Terminal Type [VT100 / **VT100+** / VT-UTF8 / ANSI]	On the CG2300, the option is only shown if Console Redirection is enabled.
Menu → Server Management → Console Redirection → Legacy OS Redirection [Enabled / **Disabled**]	Menu → Advanced → Serial Port Console Redirection → **Legacy** Console Redirection Settings → Redirect After POST [**Always Enable** / BootLoader]	On the CG2300, the option is only shown if Console Redirection is enabled.
Menu → Server Management → Console Redirection → Terminal Resolution [**80x24** / 100x31]	Menu → Advanced → Serial Port Console Redirection → **Legacy** Console Redirection Settings → Resolution [**80x24** / 80x25] Menu → Advanced → Serial Port Console Redirection → Console Redirection Settings → Resolution 100x31 [Enabled / **Disabled**]	On the CG2300, the option is only shown if Console Redirection is enabled.

Error logging

CG2300	CG2400	Notes
Menu → Server Management → Clear System Event Log *<ENTER>*	Menu → Server Mgmt → System Event Log → Erase SEL → [**No** / Yes, On next reset / Yes, On every reset] Menu → Server Mgmt → System Event Log → When SEL is Full [**Do Nothing** / Erase Immediately / Delete Oldest Record] Menu → Server Mgmt → System Event Log → Log EFI Status Codes [Disabled / Both / **Error code** / Progress code]	
Menu → Advanced → Memory Configuration → Memory RAS and Performance Configuration → Select Memory RAS Configuration [**Maximum Performance** / Mirroring / Rank Sparing / Lockstep]	Menu → Socket Configuration → Memory Configuration → Memory RAS Configuration → Static Virtual Lockstep Mode [Enable / **Disable**] Menu → Socket Configuration → Memory Configuration → Memory RAS Configuration → Mirror mode [Enable / **Disable**] Menu → Socket Configuration → Memory Configuration → Memory RAS Configuration → UEFI ARM Mirror [Enable / **Disable**] Menu → Socket Configuration → Memory Configuration → Memory RAS Configuration → Memory Rank Sparing [Enable / **Disable**]	On the CG2400, the option shown varies according to the type of memory installed in the system.
Menu → Advanced → Memory Configuration → Memory RAS and Performance Configuration	Menu → Socket Configuration → Memory Configuration → Memory RAS Configuration → Patrol Scrub [**Enable** /	

→ Patrol Scrub [**Enabled** / Disabled] Menu → Advanced → Memory Configuration → Memory RAS and Performance Configuration → Demand Scrub [**Enabled** / Disabled]	Disable] Menu → Socket Configuration → Memory Configuration → Memory RAS Configuration → Patrol Scrub Interval [**24** / <1-24>] Menu → Socket Configuration → Memory Configuration → Memory RAS Configuration → Patrol Scrub Address Mode [Reverse Address / **System Physical Address**]	
Menu → Advanced → Memory Configuration → Memory RAS and Performance Configuration → Correctable Error Threshold [20 / **10** / 5 / All / None]	Menu → Socket Configuration → Memory Configuration → Memory RAS Configuration → Correctable Error Threshold [**7fff** / <0-7ffff>]	
Menu → Advanced → Memory Configuration → Memory RAS and Performance Configuration → Memory Correctable Error Enabling [**Enabled** / Disabled]	Menu → Socket Configuration → Memory Configuration → Memory Dfx Configuration → ECC Checking [**Auto** / Enable / Disable]	
Menu → Server Management → Assert NMI on SERR [**Enabled** / Disabled]	Not present in AMI SETUP	
Menu → Server Management → Assert NMI on PERR [**Enabled** / Disabled]	Not present in AMI SETUP	
Menu → Server Management → PCIe AER Support [**Enabled** / Disabled]	Menu → Platform Configuration → Runtime Error Logging → IIO Error Enabling → IIO PCIE AER Spec Compliant [Enable / **Disable**]	
Menu → Server Management → Log Correctable Errors [Enabled / **Disabled**]	Not present in AMI SETUP	
Menu → Server Management → WHEA Support [**Enabled** / Disabled]	Not present in AMI SETUP	
Menu → Server Management → Enable Cloaking [Enabled / **Disabled**]	Not present in AMI SETUP	
Menu → Server Management → PCIe Correctable Error Threshold [20 / All / 5 / **10**]	Not present in AMI SETUP	
Menu → Server Management → Reset on CATERR [**Enabled** / Disabled]	Not present in AMI SETUP	
Menu → Server Management → Reset on ERR2 [**Enabled** / Disabled]	Not present in AMI SETUP	

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:

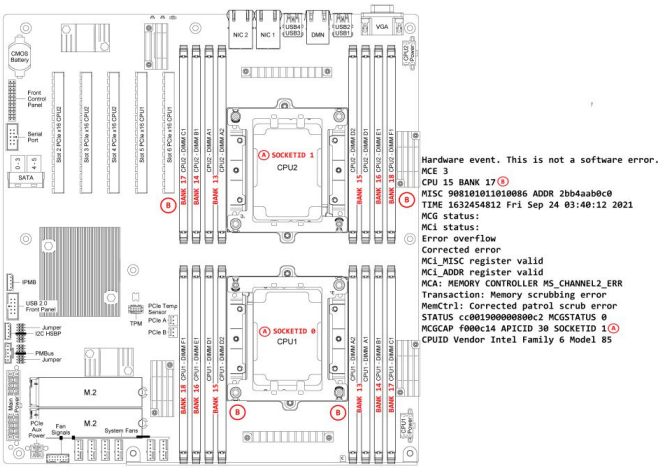
```
Hardware event. This is not a software error.
MCE 0
CPU 0 BANK 18
MISC 90840080008228c ADDR 9ce494000
TIME 1499161840 Tue Jul 4 09:50:40 2021
MCG status:
MCi status:
Corrected error
MCi_MISC register valid
MCi_ADDR register valid
MCA: MEMORY CONTROLLER MS_CHANNEL2_ERR
Transaction: Memory scrubbing error
MemCtrl: Corrected patrol scrub error
STATUS 8c000051000800c2 MCGSTATUS 0
MCGCAP 7000c16 APICID 0 SOCKETID 0
CPUID Vendor Intel Family 6 Model 85
```

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).

Machine Bank Number	Processor Module
7	IMC 0, Main
8	IMC 1, Main
13	IMC 0, channel 0
14	IMC 0, channel 1
15	IMC 1, channel 0
16	IMC 1, channel 1
17	IMC 0, channel 2
18	IMC 1, channel 2

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.

DANGER	DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.
WARNING	WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.
CAUTION	CAUTION indicates a hazardous situation which, if not avoided, may result in minor or moderate injury.
NOTICE	NOTICE indicates a property damage message.

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

ACPI	Advanced Configuration and Power Interface
AI	Artificial Intelligence
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
BIOS	Basic Input/Output System
BMC	Baseboard Management Controller
BSP	Board Support Package
CBIT	Continuous Built-In Test
CE	Community European (EU mark)
CLI	Command-Line Interface
CPU	Central Processing Unit
CRMS	Communications Rack Mount Servers
CSA	Canadian Standards Association
DC	Direct Current
DDR4	Double Data Rate Fourth Generation
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual Inline Memory Module
DRAM	Dynamic Random Access Memory
DU	Distributed Unit
ECC	Error Checking and Correcting
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
ETSI	European Telecommunications Standards Institute
ETSI	European Telecommunications Standards Institute

eUSB	Embedded Universal Serial Bus
FCC	Federal Communications Commission
FH/FL	Full Height/Full Length
FPGA	Field Programmable Gate Array
FRAU	Field Replaceable Unit
FRU	Field Replaceable Unit
Gb, Gbit	Gigabit
GB, Gbyte	Gigabyte – 1024 MB
GbE	Gigabit Ethernet
GND	Ground
GPI	General Purpose Input
GPIO	General Purpose Input/Output
GPO	General Purpose Output
GPS	Global Positioning System
GPU	Graphics Processing Unit
GUI	Graphical User Interface
HDD	Hard Disk Drive
Hz	Hertz – 1 cycle/second
I/O	Input/Output
I^2C	Inter-Integrated Circuit Bus
iBMC	Integrated Baseboard Management Controller
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMU	Inertial Measurement Unit
IOL	IPMI over LAN
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface
IRQ	Interrupt Request Line
KB, Kbyte	Kilobyte – 1024 bytes
KCS	Keyboard Controller Style
KEAPI	Kontron Embedded Application Programming Interface
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
LED	Light-Emitting Diode
LP	Low Profile
LPC	Low Pin Count
LVDS	Low Voltage Differential SCSI
MAT	Maximum Ambient Temperature
MB, Mbyte	Megabyte – 1024 KB
MCU	Microcontroller
MEC	Multi-Access Edge Computing
MXM	Mobile PCI Express Module
NCSI	Network Communications Services Interface
NEBS	Network Equipment-Building System
NIC	Network Interface Card, or Network Interface Controller, or Network Interface Controller port
NMI	Non-Maskable interrupt
NOS	Network Operating System
NVMe	Non-Volatile Memory Express
OCXO	Oven-Controlled Crystal Oscillator
OS	Operating System
OTP	Over-Temperature Protection

OVP	Over-Voltage Protection
PBIT	Power On Built-In Test
PCH	Platform Controller Hub
PCI	Peripheral Component Interconnect
PCIe	Peripheral Component Interconnect Express
PECI	Platform Environment Control Interface
PIRQ	PCI Interrupt Request Line
PMbus	Power Management Bus
PMM	POST Memory Manager
PnP	Plug and Play
POST	Power-On Self Test
PSU	Power Supply Unit
PTP	Precision Time Protocol
PXE	Preboot eXecution Environment
RAID	Redundant Array of Independent Disks
RAN	Radio Access Network
RAS	Reliability, Availability, and Serviceability
RDIMM	Registered Dual In-Line Memory Module
RDP	Remote Desktop
RMM	Remote Management Module
RoHS	Restriction of Hazardous Substances
SAS	Serial Attached SCSI (Small Computer System Interface)
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer Systems Interface
SDRAM	Synchronous Dynamic RAM
SEL	System Event Log
SFP+	Small Form-factor Pluggable that supports data rates up to 10.0 Gbps
SMBus	System Management Bus
SMS	Server Management Software
SNMP	Simple Network Management Protocol
SOC	System on a Chip
SOL	Serial over LAN
SSD	Solid State Drive
SSH	Secure Shell
THOL	Tested Hardware and Operating System List
TPM	Trusted Platform Module
TUV	Technischer Uberwachungs-Verein (A safety testing laboratory with headquarters in Germany)
UART	Universal Asynchronous Receiver Transmitter
UEFI	Unified Extensible Firmware Interface
UL	Underwriter's Laboratory
USB	Universal Serial Bus
UV	Under-Voltage
V	Volt
VA	Volt-Ampere (volts multiplied by amps)
Vac	Volts Alternating Current
Vdc	Volts Direct Current
VDE	Verband Deutscher Electrotechniker (German Institute of Electrical Engineers)
VGA	Video Graphics Array
vRAN	Virtualized Radio Access Network
VSB	Voltage Standby
W	Watt
WEEE	Waste Electrical and Electronic Equipment

Ω	Ohm

Safety and regulatory information

Table of contents

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

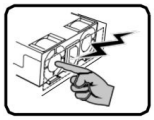
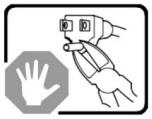
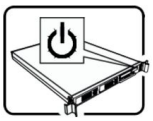
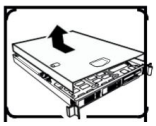
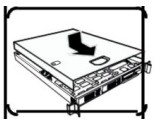
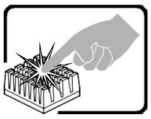
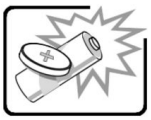
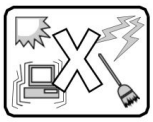
⚠WARNING	To prevent a fire or shock hazard, do not expose this product to rain or moisture. The chassis should not be exposed to dripping or splashing liquids and no objects filled with liquids should be placed on the chassis cover.
	**ESD sensitive device!** This equipment is sensitive to static electricity. 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 o f 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

	This product usually has more than one power supply cord. Disconnect all power supply cords before servicing to avoid electric shock.

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

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 disconnectio n then you must install an AC power disconnect for the entire rack unit. This main disconnect must be readily accessible, and it must be labe led 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.

⚠WARNING	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 Electrotechniker, 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 th e 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. Th e 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.
⚠CAUTION	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.

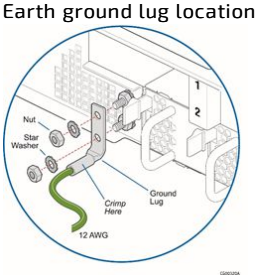
Overcurrent protection

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 fo r an electrical shock hazard, you must reliably connect an earth grounding conductor to the server. The earth grounding conductor must be a minimum 10AWG c onnected to the earth ground stud(s) on the rear of the server. The safety ground conductor should b e 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 th e 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

USA/Canada	This product is marked cCSAus. This product complies with UL 60950-1 2nd Edition and CSA C22.2 No. 60950-1-07 2nd Edition.
Europe	This CE marked product complies with the Low Voltage Directive 2014/35/EU and EN 62368-1.
International	This product has a CB report and certificate to IEC 62368-1.

Electromagnetic compatibility

USA/Canada	This product meets FCC Title 47 Part 15/ICES-003 Class A.
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 produc t 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.

WEEE directive logo

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 . 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

Please refer to the full terms and conditions of the Standard Warranty on Kontron's website at:
https://www.kontron.com/support-and-services/rma/canada/standard_warranty_policy_canada.pdf .

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.

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 .