User Documentation - CG2400

POSSIBILITIES START HERE 🌀 KONTPON



Table of Content

- User Documentation CG2400
 - Product description
 - <u>Overview</u>
 - Specifications
 - <u>Platform components</u>
 - <u>Product architecture</u>
 - <u>Description of system access methods</u>
 - <u>Recommended technical expertise</u>
 Getting started
 - <u>Getting started</u>
 <u>Application installation and performance benchmarking</u>
 - <u>Planning</u>
 - Environmental considerations
 - Power consumption and power budget
 - <u>Network architecture</u>
 - <u>MAC addresses</u>
 - <u>PCI mapping</u>
 - <u>Platform, modules and accessories</u>
 - Material, information and software required
 - Hardware compatibility list
 - <u>Validated operating systems</u>
 - <u>Security</u>
 - Installing
 - Mechanical installation and precautions
 - ESD protections
 - Unboxing
 - <u>Components installation and assembly</u>
 - Airflow
 - <u>Rack installation</u>
 - Cabling
 - <u>Software installation and deployment</u>
 - <u>Preparing for installation</u>
 - Installing an operating system on a server
 - <u>Verifying installation</u>
 - <u>Platform installation for high availability</u>
 <u>Common software installation</u>
 - <u>Configuring</u>
 - <u>Configuration of system access methods</u>
 - Configuring and managing users
 - Baseboard management controller BMC
 - <u>Configuring the network time protocol NTP</u>
 - Basic BIOS option configuration
 - <u>Customizing platform data</u>
 - <u>Network infrastructure integration</u>
 - Configuring the BMC when in non-redundant PSU configuration
 - <u>Operating</u>
 - Default user names and passwords
 - Accessing platform components
 - Accessing the operating system of a server
 - Accessing the BIOS
 - Accessing a BMC
 - <u>Platform power management</u>
 - Monitoring
 - Monitoring sensors
 - Sensor list
 - Interpreting sensor data
 - <u>Configuring and using SNMP traps</u>
 - System Inventory
 - Configuring and using SNMP traps in WebUI
 - <u>Telco Alarm Manager</u>
 - <u>Maintenance</u>
 - System event log
 - <u>Components replacement</u>
 - BIOS backup and restore
 - Upgrading
 - <u>Platform cooling and thermal management</u>
 - Managing customer-specific sensors
 - Minimum Fan Speed Override
 - Troubleshooting
 - Collecting diagnostics
 - Recovering corrupted BIOS
 - <u>Factory default</u>
 - Support information
 - Knowledge base
 - Scripting KVM and Network Manager cause SSH session to hang for couple of seconds
 - Raid Controller SNMP
 - <u>Application notes</u>
 - Secure Erase
 - StorCLI utility
 - Software RAID (VRoC)
 - <u>CG2400 in 10/100Mbps infrastructure</u>

- <u>Provisioning custom secure boot keys</u>
- <u>Generating custom secure boot keys</u>
- <u>Reference guides</u>
 - Supported IPMI commands
 - Supported Redfish commands
 - SNMP OID list
 - Parallel configuration

 - <u>CG2400 SNMP BMC User guide</u>
 <u>BIOS configuration of CG2300 compared to CG2400</u>
 - mcelog Identifying a faulty DIMM from error log
- Document symbols and acronyms
- Safety and regulatory information
- Warranty and support

Product description

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

- <u>CG2400 Carrier Grade Server</u>
 - Main applications
 - <u>Main features</u>

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

- <u>Specifications</u>
 <u>Platform components</u>
- 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

- <u>CG2400 key hardware features</u>
- <u>CG2400 key software features</u>
- <u>CG2400 physical dimensions</u>
- <u>CG2400 packaging physical dimensions</u>
- <u>CG2400 shipping weights</u>
- <u>CG2400 environmental specifications</u>

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/offSystem resetChassis 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 <u>Hardware compatibility list</u> Various third-party HW SAS/RAID controllers supported Refer to the <u>Hardware compatibility list</u> Internal flash storage supported - M.2 SATA or NVMe (2280) Refer to the <u>Hardware compatibility list</u> 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 <u>Hardware compatibility list</u> 			
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. 			
1/0	 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) 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 <i>Right or left-side orientation as looking from the front of the chassis</i> 			
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 (supplementa) features that are not part of IPMI IPMI 20 feature support Firmware update and maintenance Fan monitoring Mot_swap fan support Integrated keyboard, video, and mouse (K/M) VKW 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) Enhancements to embedded Web server: Human-readable SEL Additional system configurability Additional system configurability Additional system configurabilities Power Mode Manager support Thermal management Power Mode Manager support Thermal management health monitoring E-mail alerting Integrated remote media redirection Ulghtweight Directory Access Protocol (LDAP) System globalty unique identifier (GUID) storage and retrieval IPMI 20 features IPMI 20 features IPMI 20 features IPMI 20 features Power Mode funding command bridging and user/session support Chassis device functionality, including power/reset control and BIOS boot flags support System Stolabelty unique identifier (GUID) storage and retrieval PMI 20 features IPMI 20 features IPMI 20 features IPMI 20 features IPMI 20 features IPMI watchdog timer Messaging support, including command bridging and user/session support System Event Log (SEL) device functionality, Access to system Simsor Data Records (SDRs) Sensor device management and polling to monitor and report system health Serial over LAW (SDL) ACPI state synchronization to state changes provided by the BIOS IPMI interfaces including system management software (SMS) with receive message queue support and server management mode (SMM) Intelligent Platform Management Bus (IPMB) interface LAW interfaces that supports the IPMI over LAW protocol (RMCP, RMCP+)
Operating system	Refer to <u>Validated operating systems</u>
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	Width (mm	Height (mm
[in])	[in])	[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	-5°C to +55°C (+23°F to +131°F)
Temperature, non-operating	-40°C to +70°C (-40°F to +158°F)
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) 40°C
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)

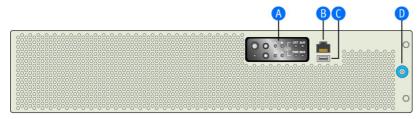
Platform components

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

Table of contents

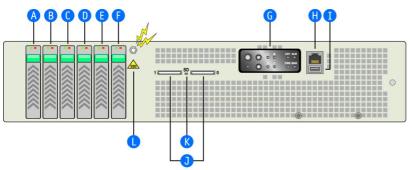
- Platform front panel
- Platform rear panel
- Platform fan module
- Power supply units
 - <u>AC power subsystem</u>
 - Voltage and current requirements
 - DC power subsystem
 Voltage and current requirements
- <u>Platform button and LED behavior</u>
 - Front panel
 - <u>Rear panel</u>
 - <u>incur punct</u>

Platform front panel



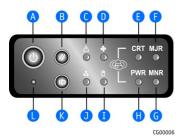
CG00004

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



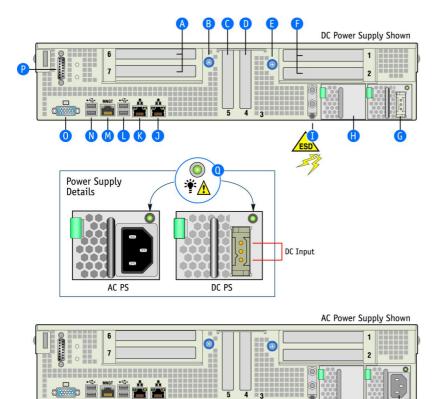
CG00005

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



Item	Description	Item	Description
А	Power button	G	Minor alarm (amber)
В	System reset button	н	Power alarm (amber)
С	System status LED	I	Drive activity LED
D	Fan status LED	J	NIC activity LED
E	Critical alarm (amber)	К	Chassis ID button
F	Major alarm (amber)	L	NMI button

Platform rear panel



4



Item	Description	Item	Description
A	Right ¹ 2-slot FL/FH PCIe assembly (slots 6 and 7)	J	GbE NIC2
В	Thumb screw to secure right PCIe assembly (A)	К	GbE NIC1
С	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)	М	Dedicated server management NIC
E	Thumb screw to secure left PCIe assembly (F)	Ν	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)	0	Video connector
G	Power supply 1 (shown with DC power supply installed)	Ρ	TAM dry relay connector
Н	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)

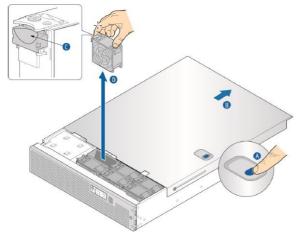
NOTES:

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 to replace the fans. Follow the instructions below to service a fan.



Step_1	Press the quick release button (A) located on the top cover.
Step_2	Slide the top cover (B) back to the support cross bar so the 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

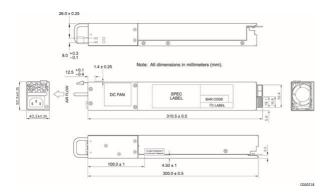
AC power subsystem

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.

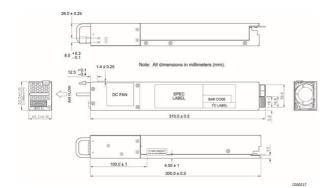
Line voltage		
Nominal 110 Vrms (low line)		
Minimum	90 V _{rms}	
Rated	100-127 V _{rms}	
Maximum	132 V _{rms}	
Nominal 220 Vrms (high line)		
Minimum	180 V _{rms}	
Rated	200-240 V _{rms}	
Maximum	264 V _{rms}	
Start-up voltage	85 Vrms ±5 Vrms	
Power off voltage	75 Vrms ±5 Vrms	
Line current		
Maximum	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

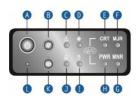
NOTE : The maximum current listed in the table below is the maximum current the system will draw from the power supply at -48 V input voltage.

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

 $^{1}\mbox{The}$ minimum steady-state DC input voltage at which the equipment remains fully operational is -40 VDC .

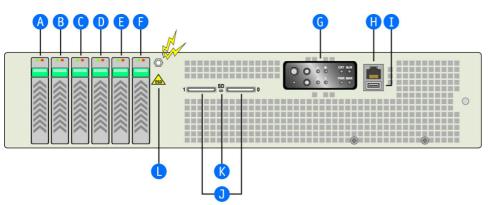
Platform button and LED behavior

Front panel



ltem	Button/LED description	Color	Condition	Description
А	Power/sleep (on	Green	On	Legacy power on / ACPI SO state
b	button)	Green	Blinking	Sleep / ACPI S1 state
		-	Off	Power off / ACPI S4 or S5 state
В	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	Amber	On	Critical level condition asserted
	NOTE : Supported from BMC 2.9.0955AB31	-	Off	No critical level condition or condition deasserted
F Major alarm	Amber	On	Major level condition asserted	
	NOTE : Supported from BMC 2.9.0955AB31	-	Off	No major level condition or condition deasserted
G	Minor alarm	Amber	On	Minor level condition asserted
	NOTE : Supported from BMC 2.9.0955AB31	-	Off	No minor level condition or condition deasserted
Н	Power alarm NOTE : Supported	Amber	On	Power sub-system condition asserted
	from BMC 2.9.0955AB31	-	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
К	Chassis ID (on button)	White	On	Chassis identification active via command or button
		-	Off	Chassis identification inactive
L	NMI button			Button only, no LED

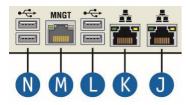
Item	Signal name	Description
A	Power button	Toggles the system power on/off, also functions as a sleep button if enabled by an ACPI-compliant operating system. A status LED is embedded in this button.
В	System reset button	Reboots and initializes the system.
к	Chassis ID button	Toggles the front panel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



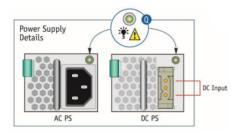
CG00005

ltem	LED description	Color	Condition	Description
A, B, C, D,	2.5-in HDD	Green	Solid	HDD present
E, F			Blinking	HDD activity
	2.5-in SSD	Amber	Solid	HDD fault
	2.3-111 220	Green	Off	SSD present
			Blinking	SSD activity
		Amber	Solid	SSD fault
Н	RJ45 serial port			No LED Serial over RJ45 port
к	SD flash Gree module	Green	Off	No SD card activity
			Blinking	SD card activity

Rear panel



ltem	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
М	Link activity (left) Dedicated management NIC	Green	Off	No link established
			Solid	Link is established
			Blinking	Link activity
	Link speed (right)	Green	Solid	1000 Mbps
Dedicated management NIC		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*

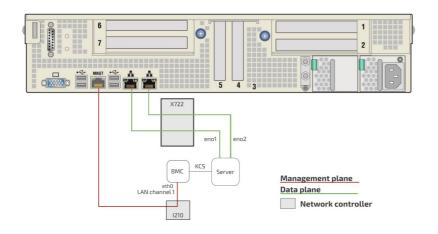
* Blinking frequency: 1 Hz (0.5 s red / 0.5 s green)

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
 - Block diagram

Internal connections



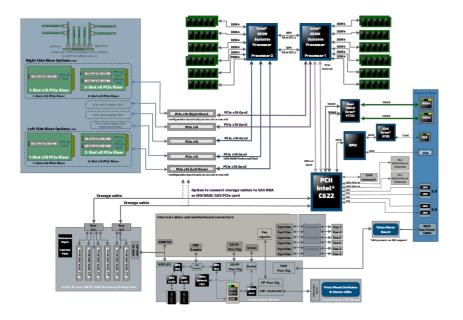
Network planes

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.



Description of system access methods

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

• Paths to the operating system

- Paths to the BIOS
- Paths to the management interface (BMC)
- To configure, monitor and troubleshoot the CG2400 platform and its components, several interfaces can be used:
- Operating system through the management plane, data plane, serial port or VGA connection of the platform
- $\bullet~$ 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 <u>Accessing the operating system of a server</u>.

Paths to the operating system	
Path description	Main reasons for use
KVM (Keyboard Video Mouse) <i>Fail-safe path to access the server if any elements (OS, BIOS, etc.) get misconfigured.</i> <i>Accessible from the management plane.</i>	 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 (05, 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 <u>Accessing the BIOS</u>.

Paths to the BIOS	
Path description	Main reasons for use
KVM (Keyboard Video Mouse) <i>Fail-safe path to access the server if any elements (OS, BIOS, etc.) get misconfigured.</i> <i>Accessible from the management plane.</i>	Initial BIOS configurationBIOS 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 (05, 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 <u>Accessing a BMC</u>.

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 monitoringOS video accessFirmware 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 monitoringFirmware 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 monitoringRemote 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 monitoringRemote 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

- <u>Getting started Application installation and performance benchmarking</u>
 [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

 Introduction
 - Assumptions
 - Unboxing the platform
 - <u>What's in the box</u>
 - Unboxing steps
 - <u>Planning</u>
 - Material and information required
 - Component installation and assembly
 - Power cables and tooling
 - <u>Rack installation material</u>
 - Network cables and modules
 - <u>Network infrastructure</u>
 - <u>Software required</u>
 - Installing components
 - Opening the enclosure
 - Removing the right riser card assembly
 - <u>Removing the left riser card assembly</u>
 - <u>Removing the processor air duct</u>
 - Installing the processors and heat sinks
 - Socket and processor handling and ESD precautions
 - Handling precautions
 - ESD precautions
 - <u>Processor location</u>
 - Adding a processor in a PHM
 - Preparing the processor for assembly with the PHM
 - Installing the processor
 - Installing a PHM in the platform
 - Installing memory DIMMs
 - Locating the DIMMs
 - DIMM population guidelines for optimal performance
 - Installing memory DIMMs
 - Installing a hardware RAID controller
 - Locating the SAS cables
 - Disconnecting the SAS cables
 - Installing the controller
 - Installing the SuperCap battery backup module
 - Installing a low-profile PCIe card in slot 4 or 5
 - Installing a full height card mounted on the left riser
 - <u>Assembling the PCIe riser card</u>
 - Installing the PCIe add-in card on the riser assembly
 - <u>Reinstalling the processor air duct</u>
 - <u>Reinstalling the left riser card assembly</u>
 - Reinstalling the right riser card assembly
 - <u>Closing the enclosure</u>
 - <u>Racking the platform</u>
 - <u>TMLPMOUNT51 rack mount kit</u>
 - Installing inner rails and mounting ears
 - Building the outer rail assembly
 - Attaching the outer rail assemblies to the rack posts
 - •
 - Securing the equipment
 - <u>DC earth-grounding</u>
 - <u>Connecting the network cables</u>
 - <u>Building and connecting a DC power cable</u>
 - DC power supply input connector
 - <u>Connector Description</u>
 - 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.
 - <u>Connector Assembly Proccess</u>
 - Building the power cables
 - DC power supply connection
 - <u>Confirming network links are established</u>
 - Discovering the platform management IP address
 - Discovering the management IP in the BIOS using the VGA display port
 - <u>Prerequisites</u>
 - Port location
 - Accessing the BMC network configuration menu
 - Preparing for operating system installation
 - Installing an operating system
 - <u>Prerequisites</u>
 - Browser considerations
 - <u>Connecting to the Web UI of the BMC</u>
 - Changing the user name and password
 - Launching the KVM
 - Mounting the operating system image via virtual media

- Accessing the BIOS setup menu
- Selecting the boot order from boot override
- <u>Completing operating system installation</u>
- Verifying operating system installation
- Benchmarking an application
- <u>Monitoring platform sensors</u>

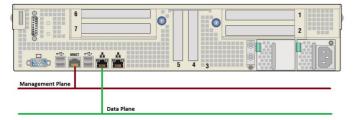
NOTICE

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 <u>Components installation and assembly</u> 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

ltem_1	#1 Phillips (cross-point) screwdrivers (or interchangeable tip screwdriver with #1 and #2 Phillips bits)
ltem_2	#2 Phillips (cross-point) screwdrivers (or interchangeable tip screwdriver with #1 and #2 Phillips bits)
Item_3 One T30 Torx screwdriver	
ltem_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.			
	ltem_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

ltem_1	Black stranded 12 AWG wire to build the power cable based on the length required
ltem_2	Red stranded 12 AWG wire to build the power cable based on the length required
ltem_3	One Positronic DC power supply input mating connector (includes a strain relief assembly)
ltem_4	Three Positronic gauge-16 crimp terminals
Item_5	Two strain relief screws
ltem_6	One strain relief plate
ltem_7	Two flat head Phillips screws
ltem_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)
ltem_12	10 mm wrench or equivalent tool
ltem_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.

ltem_1

TMLPMOUNT51

Network cables and modules

ltem_1	One RJ45 Ethernet management plane cable
ltem_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

	ltem_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 .		A hardware detection tool such as pciutils is installed on the local server to view information about devices connected to the server PCI buses.

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.



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.	

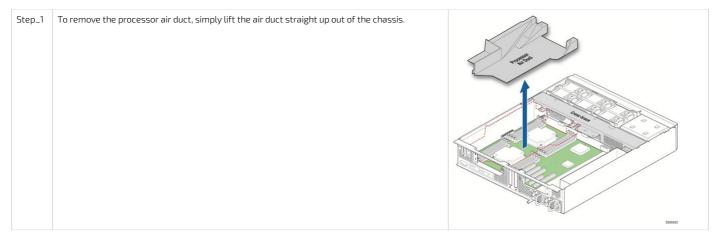
Removing the right riser card assembly

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).	Company and Company
itep_2	Using the two blue touch points (C), lift the riser card assembly out of the chassis (D).	

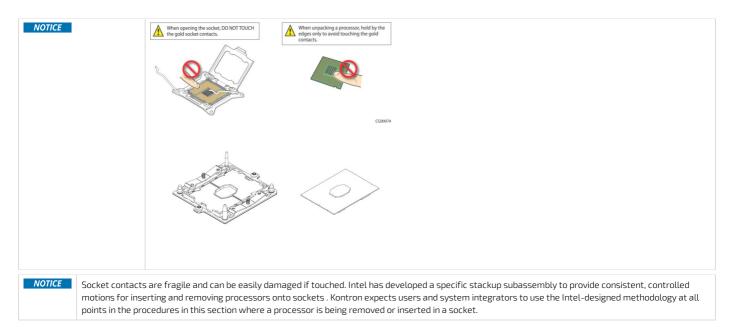
Removing the processor air duct



Installing the processors and heat sinks

Socket and processor handling and ESD precautions

Handling precautions



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.

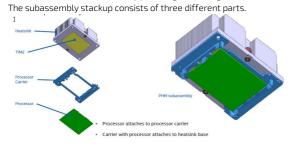


Image source: Intel Corporation

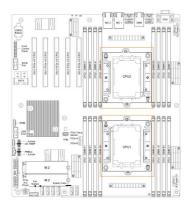
ESD precautions



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 <u>Hardware compatibility list</u> 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.

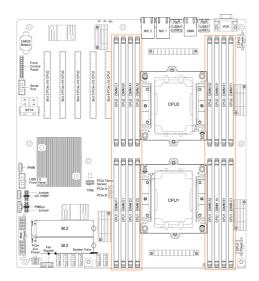
Installing the processor

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.	A AND AND AND AND AND AND AND AND AND AN
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).	

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

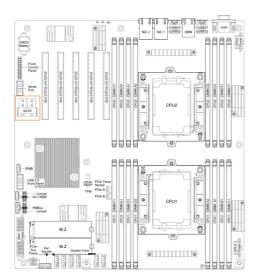
Installing memory DIMMs

Step_1	Open the levers of the DIMM slot. (A)	FT
Step_2	Note the location of the alignment notch on the DIMM edge. (B)	The The
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.	hat to
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). 	No. Contraction of the second
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

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

Motherboard PCIe slots available depends on the number of CPUs. For details, see <u>CG2400 PCIe mapping</u>. **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

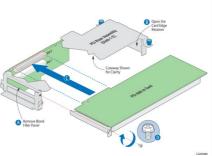
Assembling the PCIe riser card

Step_1	Fasten the left riser card to its bracket with the two 6/32 screws (8 lbf-in torque).	and a second
		C600210

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).	Remove Bla Filter Fanel



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.	
		C SUB

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).

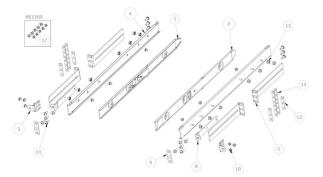
Closing the enclosure

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.	6
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

	Anchor the equipment rack – The equipment rack must be anchored to an unmovable support to prevent it from falling over when one or more server are extended in front of it on slide assemblies. The equipment rack must be installed according to the manufacturer's instructions. You must also consid 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).
in TI tv G w PP w ra A CC P	Hains 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 to 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 wo power cords 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 wo power cords must be removed. rounding the rack installation — To avoid the potential for an electrical shock hazard, for AC power you must include a third wire safety ground conducts 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 serve ower 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 an outlet that is part of the rack, then you must provide proper grounding for the server. You must provide additional, proper grounding for tak and other devices installed in it. C 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 ord 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 supplement rotection for the server. The overall current rating of a server configured with two power supplies is less than 6 amperes.
OTICE	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.

TMLPMOUNT51 rack mount kit



ltem	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.

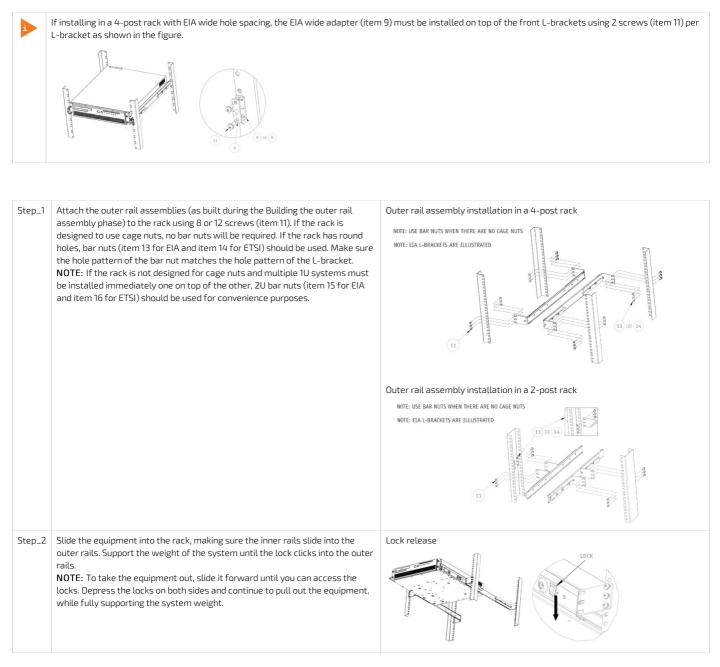
Installing inner rails and mounting ears

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

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.	S ON B ON T	

Attaching the outer rail assemblies to the rack posts



Securing the equipment

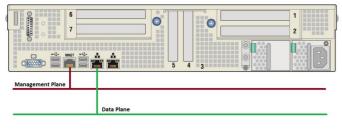
Step_1	Fasten each mounting ear (item 3) to a front L-bracket using a total of 2 screws (item 11) as shown in the figures.	Securing the equipment to a 4-post rack (EIA standard)
		Securing the equipment to a 4-post rack (EIA Wide)

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.	Nut Star Washer Crimp Here Crimp Lug

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

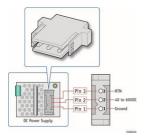
NOTE: For an AC PSU or for further information, refer to the <u>Cabling</u> section.

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.

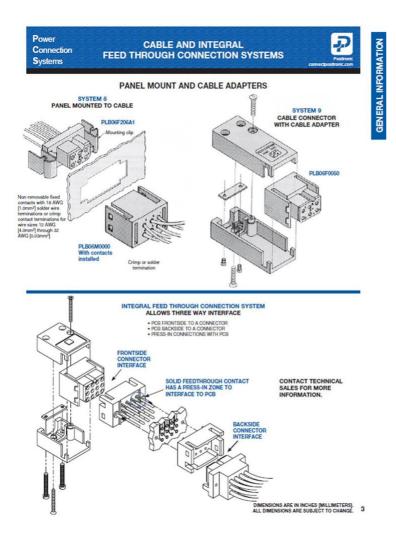
DC power supply input connector

• 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

AWARNING 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.

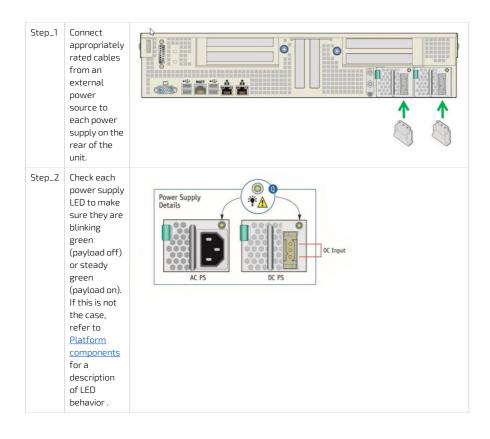
NOTE: The other ends of the cables will need to be built according to national wiring codes and conform to local regulations in addition to your data center power installation requirements.

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	 <u>DMC hand crimp tool catalog</u> <u>DMC AF8 data sheet</u>
Manual extraction tool	1	<u>9081-0-0-0</u>	Molex extraction tool catalog Application tooling specification sheet

Refer to the <u>Cabling</u> 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



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 <u>Platform components</u> 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

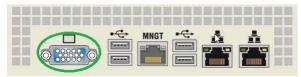
The platform management IP address can be discovered in the BIOS u sing the VGA display port (physical connection).

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 .	Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Hain Advanced IntelRCSetup Server Mame Security Boot Event Logs	>
		SIOS Information IChoose the system SIOS Vendor American Regatends Core Version 5.14 Compliancy UEF1 2.6; PI 1.4 Project Version 1	
		Build Date and Time 06/26/2019 09:12:28 Access Level Administrator	
		FPGA Version 2.02.0800AD12 ><1 Select Screen Memory Information 1^v: Select Item Total Memory 32768 MB Enter: Select	
		4/-: Change Opt. System Language (English) [P1: General Help [P1: Fervious Values System Date [Ued 07/10/2019] [P3: 9 trained Defaults System Time [13:47:54] [P4: Save & Exit [P5: Fart	
		Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.	/ AB
Step_2	Select BMC network configuration .	Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Main Advanced IntelECSetup Server Mumi Security Boot Event Logs	,
		/	
		Vai: For EMC [Disabled] +[configuration.] FR8-2 Timer [Enabled] +[FR8-2 Timer timeout [6 minutes] *[FR8-2 Timer Folicy [Power Cycle] *[
		08 Watchdog Timer [Disabled] * 08 Wdd Timer Timeout [10 minutes] * 08 Wdd Timer Policy [Reset] * 9 Serial Sux [Disabled] *	
		System Event Log System Event Log Very FBU information Very FBU information Very FBU information Very System Event Log	
		Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.	/ AB
Step_3	The BMC network configuration menu is displayed.	Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc.	
	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 .	5K metoork configurelom- 5K metoork configurelom- Configure IV4 support 5K metoork configurelom- 5K me	
		Version 2.20.1271. Copyright (C) 2019 American Regatrends, Inc.	AB

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 <u>Validated operating systems</u> .		
For information on components, refer to the <u>PCI mapping</u> .		

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 er NOTE: The HTTPS prefix is mandatory. https://[BMC MNGMT_IP]	iter the IP address discovered for the BMC.
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.	<section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>
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.	Image: Section 1.1 I
Step_4	Log in to the BMC Web UI using the appropriate credentials. NOTE: Default Web UI user name and password is admin/admin.	Literane Passend Signein Erget my passend
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	August Augu

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 .	Image: Stand
Step_2	Select the user to manage. NOTE: The first and second users are reserved fields, therefore, their usernames can't be modified.	Image: Section of the sec
Step_3	Change field Username if required.	Username operator change Password Cange Password second Size Confirm Password Confirm Password
Step_4	Check the Change Password box.	Username operator Change Password Size 1 b bres Password Confirm Password Confirm Password
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.	Username operator Change Password Password Size Password Confirm Password
Step_6	Confirm the password.	Username operator Change Password Password Size Stotytes Ostrom Password Confirm Password U U U U U U U U U U U U U U U U U U U
Step_7	Press Save .	Email Format Mit Format Email ID Existing SSH Kay Not Available Upload SSH Key Criters Criters

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 .	Interference in
Step_2	From the Remote Control menu, click on the Launch KVM button.	Import of the second secon
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.	Control of the state of the

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 .	<complex-block><complex-block><complex-block><complex-block><complex-block><complex-block><complex-block><complex-block><complex-block></complex-block></complex-block></complex-block></complex-block></complex-block></complex-block></complex-block></complex-block></complex-block>
		61
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.	Suge finit Optimizer: CentoS-Fatti, Ed-Monard-110falaer Vider - Mouse - Optimizer: Keybeard - Send Keys - HertKeys - Vides Record - Power - Active Users - Help - Vider - Mouse - Optimizer: Keybeard - Send Keys - HertKeys - Vides Record - Power - Active Users - Help Vider - Mouse - Optimizer: Keybeard - Send Keys - HertKeys - Vides Record - Power - Active Users - Help Vider - Mouse - Optimizer: Keybeard - Send Keys - HertKeys - Vides Record - Power - Active Users - Help Vider - Mouse - Optimizer: Keybeard - Send Keys - HertKeys - Vides Record - Power - Active Users - Help Vider - Mouse - Optimizer: Keybeard - Send Keys - HertKeys - Vides Record - Power - Active Users - Help Vider - Mouse - Optimizer: Keybeard - Send Keys - HertKeys - Vides Record - Power - Active Users - Help Vider - Mouse - Optimizer: Keybeard - Send Keys - HertKeys - Vides Record - Power - Active Users - Help Vider - Mouse - Optimizer: Keybeard - Send Keys - HertKeys - Vides Record - Power - Active Users - Help Vider - Mouse - Optimizer: Keybeard - Send Keys - HertKeys - Vides Record - Power - Active Users - Help

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.	The second product of perform a server power control operation. The addron you have higgered will be performed on the server. Do you want to perform Power Reset operation? Mark addron you have higgered will be performed on the server. Do you want to perform Power Reset operation? Mark addron you have higgered will be performed on the server. Do you want to perform Power Reset operation? Mark addron you have higgered will be performed on the server. Do you want to perform Power Reset operation? Mark addron you have higgered will be performed on the server. Do you want to perform Power Reset operation? Mark addron you have higgered will be performed on the server. Do you want to perform Power Reset operation?
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.	<page-header></page-header>

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 CDROMO 1.00 and press Enter. The server will reboot and the media installation process will	Samp NM Others - Keybeard - Send Keys - Not Keys - Video Actio Setup Utility - Copyright (C) Save & Exit	A Zoom 100 % 🖵 🕈
	start.	UET: PME IP4 Intel(R) Ethernet Connecti XSS 10 DDF Backplane VEX 20 DDF Backplane UET: PME IP4 Ereadons DDF7422 Metthem IODF RMM Ethernet Controller UET: PME IP4 Ereadons DDF7422 Metthem IODF RMM Ethernet Controller UET: PME IP4 Ereadons DDF7422 Metthem IODF RMM Ethernet Controller Met Virusi ECKOM0 1.00 Met Virusi ECKOM0 1.00 Met Virusi CORME 1.00 M	n E E E

> 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

1	All the results and commands may vary depending on the operating system and the devices added.	
Step_1 Step_2	Reboot the OS as recommended, then access the OS command prompt. 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 [root@localhost -]# free -h free shared buff/cache available detected. 155 460M 146 18M 273M 146 LocalServer_OSPrompt:~# free -h 7.76 08 7.76	
Step_4	Verify that all the storage devices are detected. LocalServer_OSPrompt:-# lsblk[root@localhost ~]# lsblk MAE MAB_MIN_RM_SIZE_RO_TYPE_MOUNTPOINT nvme0n1p1_259:10200M 00 part part /boot/efi nvme0n1p3_259:30200M 0 part /boot0part /bootIsblk-nvme0n1p3_259:30200M 00 part part0part (boot-nvme0n1p3_259:30200M 00 part part-nvme0n1p4_259:40237.16 00 part (boot-nvme0n1p3_259:30200M 00 part (boot-nvme0n1p4_259:40237.16 00 lvm 	
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 IcotalSecure for the state of the state and the state of the state	
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	
Step_9	NOTE: Updating the packages may take a few minutes. (Optional) If PCIe add-in cards or other hardware components are installed, verify that they are detected. Irection cards the properties of the proper	
	NOTE: The keyword is a unique word helping to identify the hardware component. The product PCI mapping may help with this validation.	
	www.kontron.com	

Step_10	Verify communication between the operating system and the BMC. LocalServer_OSPrompt:~# ipmitool mc info	LocalServer_OSPrompt:~# ipmitool mc inf Device ID : 32 Device Revision : 1 Firmware Revision : 0.01 IPMI Version : 2.0 Manufacturer ID : 15000 Manufacturer Name : Kontron Product ID : 1100 (0x04 Product Name : Unknown (O Device Available : yes Provides Device SDRs : no Additional Device Support : Sensor Device SDR Repository Device SEL Device FRU Inventory Device IPMB Event Generator Chassis Device Aux Firmware Rev Info 0x09 0x33 0x9b 0xf8	ic)

Benchmarking an application

Install your application and proceed with benchmarking.

Monitoring platform sensors

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

ep.2 From the left-side menu, click on Sensor , Image: constraint of the left-side menu, click on Sensor , ep.3 The sensor list will be displayed. Image: constraint of the left-side menu, click on Sensor , ep.4 Scroll down to see the list of sensors, Image: constraint of the left-side menu of t
ep.4 Scroll down to see the list of sensors. ep.4 Cluck on a sensor to see more details.
ep. 5. Click on a sensor to see more details. ep. 5. Click on a sensor to see more details.
ep. 5. Click on a sensor to see more details. ep. 5. Click on a sensor to see more details.
ep.4 Circle down to see the list of sensors. ep.4 Circle down to see the list of sensors. Circle down to see the list of sensors. ep.4 Circle down to see the list of sensors. Circle down to see the list of sensors. ep.4 Circle down to see the list of sensors. Circle down to see the list of sensors. ep.4 Circle down to see the list of sensors. Circle down to see the list of sensors. ep.4 Circle down to see the list of sensors. Circle down to see the list of sensors. ep.4 Circle down to see the list of sensors. Circle down to see the list of sensors. ep.4 Circle down to see the list of sensors. Circle down to see the list of sensors. ep.5 Circle down to see more details. Circle down to see more details. ep.5 Circle non a sensor to see more details. Circle down to see the dist of sensors.
ep.4 Click on a sensor to see more details. ep.5 Click on a sensor to see more details. Sensor to see more details. Sensor to see more details.
ep.4 Scroll down to see the list of sensors. Image: manual sensor to see more details. Image: manual sensor to see more details. Image: manual sensor to see more details.
ep.4 Scroll down to see the list of sensors. p.4. Scroll down to see the list of sensors. Image: manual sensor () manual sensor () Image: manual sensor () Image: manual sensor () manual sensor () Image: manual sensor () Image: manual sensor () manual sensor () Image: manual sensor () Image: manual sensor () manual sensor () Image: manual sensor () Image: manual sensor () manual sensor () Image: manual sensor () Image: manual sensor () manual sensor () Image: manual sensor () Image: manual sensor () manual sensor () Image: manual sensor () Image: manual sensor () manual sensor () Image: manual sensor () Image: manual sensor () manual sensor () Image: manual sensor () Image: manual sensor () manual sensor () Image: manual sensor () Image: manual sensor () manual sensor () Image: manual sensor () Image: manual sensor () manual sensor () Image: manual sensor () Image: manual sensor () manual sensor () Image: manual sensor () Image: manual sensor () manual sensor () Image: manual sensor () Image: manual sensor () manual sensor ()
ep_4 Scroll down to see the list of sensors. $ep_5 \\ Click on a sensor to see more details. ep_5 \\ Click on a sensor to see more details. ep_5 \\ Click on a sensor to see more details. ep_5 \\ Click on a sensor to see more details. ep_5 \\ Click on a sensor to see more details. ep_6 \\ Click on a sens$
ep_4 Scroll down to see the list of sensors. Image: manual sensor to see more details. Image: manual sensor to see more details. ep_5 Click on a sensor to see more details. Sected and sensor to see more details. Sected and sensor to see more details. Sected and sensor to see more details.
ep_4 Scroll down to see the list of sensors. p_4 Scroll down to see the list of sensors. Image: manual sensor to see more details. p_5 Click on a sensor to see more details. Second till down to see the list of sensors.
ep_4 Scroll down to see the list of sensors. Binding and the sensor to see more details. Binding and the sensor to see more details.
ep_4 Scroll down to see the list of sensors. $\left \begin{array}{cccccccccccccccccccccccccccccccccccc$
ep_4 Sroll down to see the list of sensors. Page 5 Click on a sensor to see more details. Page 5 Click 0 C
ep_4 Scroll down to see the list of sensors. Particul down to see more details. Particul down to see more details. Particul down to see more details. Particul down to see the list of sensor to see more details. Particul down to see the list of sensor to see more details. Particul down to see the list of sensor to see more details. Particul down to see the list of sensor to see more details. Particul down to see the list of sensor to see more details. Particul down to see the list of sensor to see more details. Particul down to see the list of sensor to see more details. Particul down to see the list of sensor to see more details. Particul down to see the list of sensor to see more details. Particul down to see the list of sensor to see more details. Particul down to see the list of sensor to see more details. Particul down to see the list of sensor to see more details. Particul down to see the list of sensor to see more details. Particul down to see the list of sensor to see more details. Particul down to see the list of sensor to see more details. Particul down to see the list of sensor to see more details. Particul down to see the list of sensor to s
eps. Click on a sensor to see more details. eps.5 Click on a sensor to see more details. eps.1 eps.1 eps.1
eps Click on a sensor to see more details. eps 5 Click on a sensor to see more details.
ep 5 Click on a sensor to see more details.
ep_5 Click on a sensor to see more details. $since to the sensor to see more details. since to the sensor to the sensor to see more details. since to the sensor to the sensor to see more details. since to the sensor to the sens$
eps Click on a sensor to see more details. eps 5. Click on a sensor to see more details. ensor detail Adverses to the matter of the content of
ep_5 Click on a sensor to see more details. $1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 +$
ep.5 Click on a sensor to see more details. Sensor detail at information Sensor detail at information ep.5 Click on a sensor to see more details. Sensor detail at information Sensor detail at information ep.5 Click on a sensor to see more details. Sensor detail at information Sensor detail at information ep.5 Click on a sensor to see more details. Sensor detail at information Sensor detail at information ep.5 Click on a sensor to see more details. Sensor detail at information Sensor detail at information ep.5 Click on a sensor to see more details. Sensor detail at information Sensor detail at information ep.5 Click on a sensor to see more details. Sensor detail at information Sensor detail at information ep.6 Click on a sensor to see more details. Sensor detail at information Sensor detail at information exert weak Sensor detail at information Sensor detail at information Sensor detail at information exert weak Sensor detail at information Sensor detail at information Sensor detail at information exert weak Sensor detail at information Sensor detail at information Sensor detail at information Sensor detail Sensor
eps.5 Click on a sensor to see more details. Sensor detail is information 1000000000000000000000000000000000000
eps.5 Click on a sensor to see more details. Sensor detail 1 identication doubtharms Sensor detail 1 identication doubtharms Sensor detail 1 identication doubtharms eps.5 Click on a sensor to see more details. Sensor detail 1 identication doubtharms Sensor detail 1 identication doubtharms Sensor detail 1 identication doubtharms eps.5 Click on a sensor to see more details. Sensor detail 1 identication doubtharms Sensor detail 1 identication doubtharms Sensor detail 1 identication doubtharms exercises Sensor detail 1 identication doubtharms Sensor detail 1 identication doubtharms Sensor detail 1 identication doubtharms exercises Sensor detail 1 identication doubtharms Sensor detail 1 identication doubtharms Sensor detail 1 identication doubtharms exercises Sensor detail 1 identication doubtharms Sensor detail 1 identication doubtharms Sensor detail 1 identication doubtharms exercises Sensor features Sensor features Sensor features Sensor features exercises Sensor features Sensor features Sensor features Sensor features exercises Sensor features Sensor features Sensor features Sensor features exercises Sensor features Sensor features Sensor features
ep_5 Click on a sensor to see more details. Per_5 Click on a sensor to see more details.
ep_5 Click on a sensor to see more details. ep_5 Click on a sensor to see more details.
eps Click on a sensor to see more details. eps Sensor detail A reference shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future shot fits server Image: Sensor future sho
e 4.900,080,08 14.9496
eps.5 Click on a sensor to see more details. Person <td< td=""></td<>
ep_5 Click on a sensor to see more details. Intervention of the sensor of the
ep_5 Click on a sensor to see more details. Image: Click on a sensor to see more details. Sensor detail at downore doubt to sensor. Image: Click on a sensor to see more details. Sensor detail at downore doubt to sensor. Image: Click on a sensor to see more details. Sensor detail at downore doubt to sensor. Image: Click on a sensor to see more details. Sensor detail at downore doubt to sensor. Image: Click on a sensor to see more details. Sensor detail at downore doubt to sensor. Image: Click on a sensor to see more details. Sensor detail at downore doubt to sensor. Image: Click on a sensor to see more details. Sensor detail at downore doubt to sensor. Image: Click on a sensor to see more details. Sensor detail at downore doubt to sensor. Image: Click on a sensor. Sensor detail at downore doubt to sensor. Image: Click on a sensor. Sensor detail at downore doubt to sensor. Image: Click on a sensor. Sensor formstor. Image: Click on a sensor. Sensor formstor.
ep_5 Click on a sensor to see more details.
ep_5 Click on a sensor to see more details.
Temp BMC Sensor Information
1000 1000 <td< td=""></td<>
1 1
1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000
1917 tope this - Calified 152 9 508 Low 100 child 67 9 308 Low 100 child 67 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100
6034 Lower Orisout 41 % 2637- 6030 article Accessed are 2 There (excessed) There (excessed)
253- 000
este intervents
Sensor Events
R Sensor Events
۲

For a list of all the sensors, refer to <u>Sensor list</u>.

For more monitoring methods refer to <u>Monitoring sensors</u>.

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
- <u>Network architecture</u>
- <u>MAC addresses</u>
- PCI mapping
- Platform, modules and accessories
- Material, information and software required
- <u>Hardware compatibility list</u>
 [Content under creation] Deployment infrastructure
- Validated operating systems
- <u>Security</u>

Environmental considerations

{This article provides environmental guidelines in order to ensure the proper functioning of the platform.}

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

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

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

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

This equipment should not be exposed directly to the elements (sun, rain, wind, dust).

Power consumption and power budget

[This article provides power supply electrical specifications and explains how to estimate power consumption based on various use cases.] Table of contents

Power budget

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

General power information

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

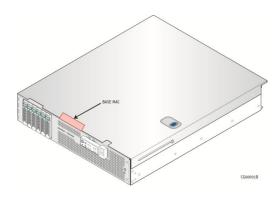
MAC addresses

[This article provides information on the product MAC addresses and on means of discovering them.] Table of contents

- <u>CG2400 MAC addresses</u>
- <u>Discovering the platform MAC addresses</u>
- Discovering a MAC address using IPMI
 - <u>Prerequisite</u>
 - Procedure via ipmitool lan print
 - Procedure via ipmitool fru print
 - Discovering a MAC address using the BIOS
 - <u>Accessing the BIOS using the VGA display port (physical connection)</u>
 - <u>Accessing the BIOS using a serial console (physical connection)</u>

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 <u>IPMI</u>
- 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:
- <u>lan print</u>
- 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	\$ ipnitool +H 172.16.192.125 -I lanplus -U admin -P admin lan print Set in Progress : Set Complete Auth Type Support : Auth Type Enable : Callback : : User : : Operator : : Admin :
		IP Address Source : DHCP Address IP Address Source : DHCP Address IP Address : 172.16.192.125 Subnet Mask : 255.255.0.0 MAC Address : 00:a0:a3:da9:e88 IP Header : TTL=0440 Flags=0x40 Precedence=0x00 TO5=0x10
		BMC ARP Control : ARP Responses Enabled, Gratuitous ARP Disabled Gratituous ARP Intrvl : 1.0 seconds Default Gateway MAC : 07.2.6.9.1 Default Gateway MAC : 00:05:64:2f:10:5f Backup Gateway NP : 0.0.0 Backup Gateway IP : 0.0.00:00:00:00:00
		802.1q VLAN ID : Disabled 802.1q VLAN Priority : 0 RMCP+ Cipher Suite : 0,1.2,3,6,7,8,11,12,15,16,17 Cipher Suite Priv Max : CaaaaaaaaaaaXXX : X=Cipher Suite Unused : c=CALLBACK
		- C-TALEONCH - U-USER - O-DFEATOR - a-AMMIN - 0-0EM Bad Password Threshold : 0
		Invalid password disable: no Attempt Count Reset Int.: 0 User Lockout Interval : 0

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.	<pre>ipmitool -H 172.16.192.125 -I lanplus -U admin -P admin fru print FRU Device Description : Builtin FRU Device (ID 0) Chassis Type : Main Server Chassis Chassis Part Number : KNB-TXS100-00 Chassis Serial : 000000000 Chassis Extra : KNB-TXS100 Board Mfg Date : Mon Aug 12 11:55:00 2019 Board Mfg : Kontron Canada Inc. Board Product : KNB-TXS100 Board Serial : 000000000 Board Serial : 000000000 Board Part Number : 1065-6288 Board Extra : MKAC-60:a0:a5:da:90:88 Read FRU Area length 264 too large, Adjusting to 95 Product Manufacturer : Kontron Canada Inc. Product Manufacturer : KNB-TXS100 Product Version : Product Version : KNB-TXS100 Product Version : FRU Device Description : Power Supply 1 (ID 1) Product Part Number : YA572851AM Product Part Number : YA572851AM Product Serial : 26070871837602973 Product Asset Tag : 126018 Product Asset Tag : 26018 Product Asset Tag : Adjusting Product Serial : A01R Product Serial : A01R Product Serial : A01R Product Asset Tag : 126018 Product Asset Tag : 126018 Product Asset Tag : 27275 Product Serial : 7406A319192800020 Product Serial : 7406A319192800020 Product Extra : A</pre>

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

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

		+
BIOS Information		Choose the system
IOS Vendor	American Negatrends	default language
Core Version	5.14	I
lompliancy	UEFI 2.6; PI 1.4	1
Project Version		1
Build Date and Time	06/26/2019 09:12:28	

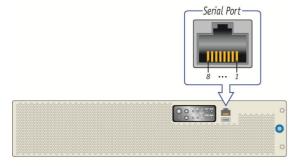
	Access Level	Administrator	
	FPGA Version	2.02.0800AD12	
	Nemory Information		<pre>><: Select Screen ^v: Select Item</pre>
	Total Nemory	32768 MB	Enter: Select
	l i i i i i i i i i i i i i i i i i i i		+/-: Change Opt.
	System Language		F1: General Help F2: Previous Values
	System Date	[Wed 07/10/2019]	F3: Optimized Defaults
	System Time	[13:47:54]	F4: Save & Exit ESC: Exit
	\		1550: 5X10
	Version 2.20.1271.	Copyright (C) 2019 Amer	ican Megatrends, Inc. AB
Select BMC network configuration .	Aptio Setup Utility Main Advanced Intels	- Copyright (C) 2019 Am CSetup Server Mgmt Sec	erican Megatrends, Inc. urity Boot Event Logs
	BMC Interface(s)	KCS, USB	<pre>^ Press <enter> to enable + or disable Serial Mux</enter></pre>
	Wait For BMC	[Disabled]	+ configuration.
			+1
	FRB-2 Timer Policy	[Power Cycle]	- Million - Charles - Char
	 OS Natchdog Timer	(Direbled)	* *
	OS Wtd Timer Timeout	[10 minutes]	
	OS Wtd Timer Policy	[Reset]	*1
	Serial Mux		* ><: Select Screen * ^v: Select Item
	> System Event Log		* Enter: Select
		07	* +/-: Change Opt. * F1: General Help
	> View System Event Log	on	* F2: Previous Values
	> BMC User Settings		* F3: Optimized Defaults
	BMC Warm Reset		<pre>v F4: Save & Exit ESC: Exit</pre>
	Version 2.20.1271.	Copyright (C) 2019 Amer	ican Megatrends, Inc. AB
The BMC network configuration menu is displayed.	Aptio Setup Utility	r - Copyright (C) 2019 Am Server Ngmt	erican Megatrends, Inc.
NOTE: When the platform is powered up after being shut off, the UEFI/BIOS may load before the BMC		tion	^ Select to configure LAN
has respired its ID address. In this sace the UEEL/DIOS menu information will need to be refreshed by			* channel parameters
restarting the server and re-entering the UEFI/BIOS .	******************		* statically or * dynamically(by BIOS or * BHC). Unspecified
	Lan channel 1		+ option will not modify
	Configuration Address		+ any BMC network + parameters during BIOS
	Source Current Configuration	DynamicAddressBmcDhcp	+1
	Address source		+i
		172.16.205.245	+ + + ><: Select Screen + ^v: Select Item
	Address source Station IP address Subnet mask Station MAC address	172.16.205.245 255.255.0.0 00-&0-&5-D6-33-2&	+ + ><: Select Screen + ^v: Select Item + Enter: Select
	Address source Station IP address Subnet mask	172.16.205.245 255.255.0.0 00-&0-&5-D6-33-2& 172.16.0.1	+ + + ><: Select Screen + >v: Select Item + Enter: Select + Enter: Select
	Address source Station IP address Subnet mask Station MAC address Router IP address Router MAC address	172.16.205.245 255.255.0.0 00-&0-&5-D6-33-2&	+ + >: Select Screen + ^v: Select Item + Enter: Select + +1-: Change Opt. + F1: General Help + F2: Previous Values
	Address source Station IP address Subnet mask Station MAC address Router IP address	172.16.205.245 255.255.0.0 00-&0-&5-D6-33-2& 172.16.0.1	+ + >:: Select Screen + ^v: Select Icem + Enter: Select + /-: Change Opt. + /1: General Help + 72: Previous Values + 73: Optimized Defaults
	Address source Station IP address Subnet mask Station MAC address Router IP address Router MAC address	172.16.205.245 255.255.0.0 00-&0-&5-D6-33-2& 172.16.0.1	+ + >: Select Screen + ^v: Select Item + Enter: Select + +1-: Change Opt. + F1: General Help + F2: Previous Values
	Address source Station IP address Subnet mosk Station MAC address Fouter IP address Fouter IAC address Lan channel 2	172.16.205.245 255.255.0.0 00-&0-&5-D6-33-2& 172.16.0.1	 + ×: Select Screen + ×: Select Iem + Enter: Select + F1: General Help + F1: General Help + F3: Provide Values + F3: Quinized Defaults + F4: Quinized Defaults + F4: Screek Exit + E3C: Exit
		Select BMC network configuration . April Strugg PCLIDS File 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 her prevent is [P address. In this case the UEFI/BIOS menu information will need to be refressed by	Select BMC network configuration .

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



	Pin	out	
1	RTS	5	GND
2	DTR	6	RX#
3	TX#	7	DSR
4	GND	8	CTS

CP0286

Step_1	From a computer with a physical connection to the serial port, open a serial console tool and start the which the device is connected.	communication between the console and the port to
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".	COM12-PuTY Comparison 3.20.1371, Sopyright (0) 2019 American Repartends, Inc. Eros Pares 00/04/2019 E017:10 Version 2.10.0937591 Possa (JIL) or <f2> to enter actup.Press (JT> for boot menu.</f2>
Step_4	The BIOS sign on screen displays "Entering Setup". NOTE: It will take several seconds to display and enter the BIOS setup menu.	COM21-PuTV Version 3.20.1271. Copyright (C) 2019 American Repartends, Inc. RoAdd, NAME Jriewase Version 2.10.09317931 ROAdd, NAME Jriewase Version 2.10.09317931 ROAdd, NAME Jriewase Version 2.10.09317934 Roadd, NAME Jriewase Version 2.10.0931793 Roadd, NAME Jriewase Version 2.10.0931794 Roadd, NAME Jriewase Version 2.100017 Roadd, NAME Jrie
Step_5	The BIOS setup menu is displayed.	COMPLANTY Comparing the constraint of the cons

Accessing the BMC network configuration menu

ep_1	From the UEFI/BIOS menu, navigate to tab Server Mgmt .	Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Main Advanced IntelRCSetup Server Mgmt Security Boot Event
		BIG Information Choose the syst Comp Version S.14 Compliancy UEF1 2.6; FI 1.4 Project Version 06/26/2019 09:12:20 Access Level Administrator FOG Version 2.02.0800AD12 FF03 Version 2.02.0800AD12 Fog Version 2.02.0800AD12 Version 2.02.0800AD12 System Language [Inglimh] System Language [Inglimh] System Tame [13:47:54] Version 2.100:1271. Copyright (C) 2019 American Regetrends, Tr
ep_2	Select BMC network configuration .	Aptio Setup Utility - Copyright (C) 2019 American Megatrands, Main Advanced intelSCOStup Devector Security Noot Event
		BRC Interface(s) KCE, USB */Press <future> Vait For BWC [Dismbled] + configuration. FRB-2 Timer Incourt [Canabled] + FRB-2 Timer Follow [6 minutes] + FRB-2 Timer Follow [7 Page Follow] + </future>

		Version 2.20.1271	. Copyright (C) 2019 Ame:	rican Megatrends, Inc.
Step_3 The	e BMC network configuration menu is displayed.	Aptio Setup Utilit	y - Copyright (C) 2019 As Server Ngmt	merican Negatrends, Inc.
has	DTE : When the platform is powered up after being shut off, the UEFI/BIOS may load before the BMC is received its IP address. In this case, the UEFI/BIOS menu information will need to be refreshed by starting the server and re-entering the UEFI/BIOS .	-BRC network configur Configure 1974 support Configure 1974 support Configure 1974 support Configure 1974 support Configure 1974 support Station 19 address Station 19 address Station 19 address Router HAC address Lan channel 2 Version 2.400.1271		<pre>ident to configure LNN identically or identicaly or identically or identical</pre>

<u>۱</u>----

PCI mapping

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

The KMB-IX5100 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) \rightarrow Slot 5 (chassis) Slot 6 (motherboard) \rightarrow 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) \rightarrow Slot 5 (chassis) Slot 6 (motherboard) \rightarrow 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) \rightarrow Slots 1 and 2 (chassis) Slot 3 (motherboard) \rightarrow Slot 3 (chassis) Slot 4 (motherboard) \rightarrow 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	alec	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	alaf	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 m	apped as bu	s 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.6	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
17:0e.7 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)

17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 19:03.0 8 19:03.0 8 19:03.0 8 19:03.0 8 19:03.0 8 19:03.0 8 19:03.0 8 19:03.0 8 19:03.0 8 10:00.0 8 10:00.0 8 10:00.0 8 10:00.0 8 10:00.0 8 10:00.0 8 10:00.0 8 10:00.0 8 10:00.0 8 10:00.0 8 10:00.0 8 10:00.0 8 10:00.0 8 10:00.0 8 10:00.0 8 <t< th=""><th>8086 8086 8086 8086 8086 8086 8086 8086</th><th>37c0 37c5 37d2 37d2</th><th>System peripheralSystem peripheralPCI bridgeSif onty 1 CPU is installedPCI bridgePCI bridgePCI bridgePCI bridgeSystem peripheralPCI bridgeSystem peripheralSystem peripheral<</th><th>Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Sky Lake-E PCU Registers (rev 04)</th><th></th></t<>	8086 8086 8086 8086 8086 8086 8086 8086	37c0 37c5 37d2 37d2	System peripheralSystem peripheralPCI bridgeSif onty 1 CPU is installedPCI bridgePCI bridgePCI bridgePCI bridgeSystem peripheralPCI bridgeSystem peripheralSystem peripheral<	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Sky Lake-E PCU Registers (rev 04)	
17.1d.1 4 17.1d.2 4 17.1d.3 4 17.1d.0 4 17.1e.0 4 17.1e.1 4 17.1e.2 4 17.1e.3 4 17.1e.3 4 17.1e.3 4 17.1e.4 4 17.1e.5 4 17.1e.5 4 17.1e.5 4 19.03.0 4 <t< td=""><td>80.86 80.86</td><td>2080 2081 2082 2083 2084 2085 2085 2085 2085 2085 3702</td><td>System peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralPCI bridgeBrony 1 CPU is installedBroly 1 CPU is installedPCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgeSystem peripheralPCI bridgePCI bridgeSystem peripheralSystem periphe</td><td>Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04) Intel Corporation Sky Lake-E PCI Express Root Port A (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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4x4x4) and a card in the</td><td></td></t<>	80.86 80.86	2080 2081 2082 2083 2084 2085 2085 2085 2085 2085 3702	System peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralPCI bridgeBrony 1 CPU is installedBroly 1 CPU is installedPCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgeSystem peripheralPCI bridgePCI bridgeSystem peripheralSystem periphe	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04) Intel Corporation Sky Lake-E PCI Express Root Port A (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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4x4x4) and a card in the	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 19:03.0 8 19:03.0 8 19:03.0 8 13:00.0 9 13:00.0 8 <t< td=""><td>80.86 80.86</td><td>2080 2081 2082 2083 2084 2085 2086 2086 37c0 37c0 37c2 37c2 37d2 37d2 37d2 2030 2030 2030 2032 203 20 20 20 20 20 20 20 20 20 20</td><td>System peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralPCI bridgeEthernet controllerBi fonly 1 CPU is installedPCI bridgePCI bridgeBi fonly 1 CPU is installedPCI bridgePCI bridgeSystem peripheralPCI bridgeSystem peripheralSystem peripheral</td></t<> <td>Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04) NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 4th slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 4th slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 4th slot. Intel Corporation Sky Lake-E PCI Express Root Port D (rev 04) NOTE: Will be present if there is a neared of type (x4x</td> <td></td>	80.86 80.86	2080 2081 2082 2083 2084 2085 2086 2086 37c0 37c0 37c2 37c2 37d2 37d2 37d2 2030 2030 2030 2032 203 20 20 20 20 20 20 20 20 20 20	System peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralPCI bridgeEthernet controllerBi fonly 1 CPU is installedPCI bridgePCI bridgeBi fonly 1 CPU is installedPCI bridgePCI bridgeSystem peripheralPCI bridgeSystem peripheralSystem peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04) NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 4th slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 4th slot. NOTE: Will be present if there is a riser of type (x4x4xk4) and a card in the 4th slot. Intel Corporation Sky Lake-E PCI Express Root Port D (rev 04) NOTE: Will be present if there is a neared of type (x4x	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.4 8 17:1e.5 8 17:1e.6 8 17:1e.7 8 17:1e.3 8 17:1e.4 8 17:1e.5 8 19:03.0 8 19:03.0 8 19:03.0 8 19:03.0 8 19:03.0 8 19:03.0 8 19:03.0 8 19:03.0 8 19:03.0 8 19:03.0 8 19:03.0 8 10:03.0 8 10:03.0 8 10:03.0 8 10:03.0 8 10:03.0 8 10:03.0 9 10:03.0 9 10:03.0 19 10:03.0 10 10:03.0 10 10:03.0 10 10:03.0 10 10:03.0 10 10:03.0 10 10:03.0 10 </td <td>8086 8086 8086 8086</td> <td>2080 2081 2082 2083 2084 2085 2086 2086 3702</td> <td>System peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralPCI bridgeChorageBCI bridgePCI bridgeSystem peripheralPCI bridgeSystem peripheralSystem peripheral<trt< td=""><td>Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04) NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if t</td><td></td></trt<></td>	8086 8086 8086 8086	2080 2081 2082 2083 2084 2085 2086 2086 3702	System peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralPCI bridgeChorageBCI bridgePCI bridgeSystem peripheralPCI bridgeSystem peripheralSystem peripheral <trt< td=""><td>Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04) NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if t</td><td></td></trt<>	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04) NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (vk4x4x4A) and a card in the 2nd slot. NOTE: Will be present if t	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.1 8 17:1e.1 8 17:1e.3 8 19:03.0 8 19:03.0 8 19:03.0 8 19:03.0 8 10:00.1 9 10:00.3 8 10:00.3 8 10:00.3 8 10:00.3 8 10:00.3 8 10:00.3 8 10:00.3 8 10:00.3 8 10:00.3 8 10:00.3 8 10:00.3 8 10:00.3 8 10:00.3 8 10:00.3 8 10:00.3 8 10:00.3 8 10:00.3 8 10:00.3 8 10:00.3 8 <t< td=""><td>8086 8086 </td><td>2080 2081 2082 2083 2084 2085 2086 2086 37c0 37c0 37c2 37d2</td><td>System peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralPCI bridgeEthernet controllerBFCI bridgePCI bridgePCI bridgePCI bridgeBPCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgeSystem peripheralSystem peripheral<</td><td>Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04) NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a nexpansion card of type (v4x4x4x4x4) and a card</td><td></td></t<>	8086 8086	2080 2081 2082 2083 2084 2085 2086 2086 37c0 37c0 37c2 37d2	System peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralPCI bridgeEthernet controllerBFCI bridgePCI bridgePCI bridgePCI bridgeBPCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgeSystem peripheralSystem peripheral<	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04) NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a nexpansion card of type (v4x4x4x4x4) and a card	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.3 8 17:1e.3 8 17:1e.3 8 17:1e.4 8 17:1e.5 8 13:00.0 8 13:00.1 8 13:00.1 8 13:00.0 8 13:00.0 8 13:00.0 8 13:00.0 8 13:00.0 8 13:00.0 8 13:00.0 8 13:00.0 8 13:00.0 8 13:00.0 8 13:00.0 8 13:00.0 8 13:00.0 8 13:00.0 8 13:00.0 8 13:00.0 9 13:00.0 10 14:00.0 10 15:00.0 10 16:00.0 10 17:00.0 10 18:00.0 10 19:00.0 10 10:00.0 10 10:00.0 10 <	8086 8086 8086 8086	2080 2081 2082 2083 2084 2085 2086 2086 37c0 37c0 37c2 37d2 37d2 2030 2030 2031 2032 2032 2032 2033 2033 2033 2033 2034 2035 2036 2036 2036 2036 2036 2036 2036 2036 2036 2036 2036 2036 2036 2036 2037 20 20 20 20 20 20 20 20 20 20	System peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralPCI bridgeChrenet controllerBi fonly 1 CPU is installedPCI bridgePCI bridgeSystem peripheralSystem peripheral <trt< td=""><td>Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04) NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. N</td><td></td></trt<>	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04) NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (v4x4x4x4) and a card in the 2nd slot. N	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.3 8 17:1e.3 8 17:1e.3 8 17:1e.5 8 17:1e.6 8 17:1e.7 8 17:1e.3 8 17:1e.5 8 19:03.0 8 1a:00.1 8 1a:00.1 8 3a:01.0 8 3a:02.0 8 3a:03.0 8 <t< td=""><td>8086 8086</td><td>2080 2081 2082 2083 2084 2085 2086 2086 3700 3700 3702</td><td>System peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralPCI bridgeEthernet controllerBi fonly 1 CPU is installedPCI bridgePCI bridg</td><td>Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4x4x4) and a card in the 4th slot. Intel Corporation Sky Lake-E PCI Express Root Port D (rev 04) Intel Corporation Sky Lake-E NT-d (rev 04) Intel Corporation Sky Lake-E N</td><td></td></t<>	8086 8086	2080 2081 2082 2083 2084 2085 2086 2086 3700 3700 3702	System peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralPCI bridgeEthernet controllerBi fonly 1 CPU is installedPCI bridgePCI bridg	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4x4x4) and a card in the 4th slot. Intel Corporation Sky Lake-E PCI Express Root Port D (rev 04) Intel Corporation Sky Lake-E NT-d (rev 04) Intel Corporation Sky Lake-E N	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.3 8 17:1e.3 8 17:1e.3 8 17:1e.5 8 13:00.0 8 13:00.1 8 13:00.1 8 13:00.1 8 13:00.0 8 3a:00.0 8 3a:01.0 8 3a:02.0 8 3a:03.0 8 <t< td=""><td>8086 8086 8086 8086 8086 8086 8086 8086</td><td>2080 2081 2082 2083 2084 2085 2086 2086 37c0 37c0 37c2 37d2 37d2 2030 2030 2031 2032 2032 2032 2033 2033 2033 2033 2034 2035 2036 2037 20 20 20 20 20 20 20 20 20 20</td><td>System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral Cl bridge Cl bridge Cl</td><td>Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4x4x4) and a card in the 4th slot. Intel Corp</td><td></td></t<>	8086 8086 8086 8086 8086 8086 8086 8086	2080 2081 2082 2083 2084 2085 2086 2086 37c0 37c0 37c2 37d2 37d2 2030 2030 2031 2032 2032 2032 2033 2033 2033 2033 2034 2035 2036 2037 20 20 20 20 20 20 20 20 20 20	System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral Cl bridge Cl	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4x4x4) and a card in the 4th slot. Intel Corp	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.4 8 17:1e.5 8 17:1e.6 8 17:1e.5 8 13:00.0 8 13:00.1 8 13:00.1 8 13:00.1 8 13:00.1 8 3a:00.0 8 <t< td=""><td>8086 8086 8086 8086 8086 8086 8086 8086</td><td>2080 2081 2082 2083 2084 2085 2086 2086 3702</td><td>System peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralPCI bridgeEthernet controllerBi fonly 1 CPU is installedPCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgeSystem peripheralPCI bridgePCI bridgePC</td><td>Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a nexpansion card of type (x4x4x4x4) and a card in the 2nd slot.</td><td></td></t<>	8086 8086 8086 8086 8086 8086 8086 8086	2080 2081 2082 2083 2084 2085 2086 2086 3702	System peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralSystem peripheralPCI bridgeEthernet controllerBi fonly 1 CPU is installedPCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgePCI bridgeSystem peripheralPCI bridgePCI bridgePC	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a nexpansion card of type (x4x4x4x4) and a card in the 2nd slot.	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.3 8 17:1e.3 8 17:1e.3 8 17:1e.5 8 13:00.0 8 14:00.1 8 13:00.0 8 13:00.1 8 13:00.1 8 13:00.1 8 13:00.1 8 13:00.1 9 14:00.1 9 <t< td=""><td>8086 8086 8086 8086 8086 8086 8086 8086</td><td>2080 2081 2082 2083 2084 2085 2086 2086 37c0 37c0 37c2 37d2 2030 2030 2031 2032 2032 2033 2033 2034 2034 2035</td><td>System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral CPCI bridge CPCI b</td><td>Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present</td><td></td></t<>	8086 8086 8086 8086 8086 8086 8086 8086	2080 2081 2082 2083 2084 2085 2086 2086 37c0 37c0 37c2 37d2 2030 2030 2031 2032 2032 2033 2033 2034 2034 2035	System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral CPCI bridge CPCI b	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.4 8 17:1e.5 8 17:1e.6 8 17:1e.5 8 13:00.0 8 13:00.1 8 13:00.1 8 13:00.1 8 13:00.0 8 13:00.0 8 13:00.1 8 13:00.0 8 13:00.1 9 13:00.1 9 13:00.0 9 13:00.1 9 13:00.1 9 13:00.0 9 13:00.0 9 13:00.0 9 13:00.0 9 13:00.0 9 13:00.0 9 13:00.0 9 13:00.0 9 13:00.0 9 13:00.0 9 13:00.0 9 13:00.0 9 13:00.0 9 13:00.0 9 13:00.0 9 14:00.0 9 <t< td=""><td>8086 8086 8086 8086 8086 8086 8086 8086</td><td>2080 2081 2082 2083 2084 2085 2085 2085 2085 3702 3702 3702 3702 3702 3702 2030 2031 2031 2032 2033 2033 2034</td><td>System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral Cl bridge Cl bridge System peripheral</td><td>Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) an</td><td></td></t<>	8086 8086 8086 8086 8086 8086 8086 8086	2080 2081 2082 2083 2084 2085 2085 2085 2085 3702 3702 3702 3702 3702 3702 2030 2031 2031 2032 2033 2033 2034	System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral Cl bridge Cl bridge System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) an	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.3 8 17:1e.3 8 17:1e.5 8 17:1e.5 8 19:03.0 8 13:00.1 8 13:00.1 8 13:00.1 8 13:00.1 8 13:00.1 8 13:00.1 8 13:00.1 9 13:00.1 9 13:00.1 9 13:00.1 9 13:00.1 9 13:00.1 9 13:00.1 9 13:00.1 9 13:00.1 9 13:00.1 9 13:00.1 9 13:00.1 9 13:00.1 9 13:00.1 9 13:00.1 9 13:00.1 9 14:00.1 9 15:00.1 9 15:00.1 9 16:00.1 9 17:00.1 9 18:00.1 9 <t< td=""><td>8086 8086 8086 8086 8086 8086 8086 8086</td><td>2080 2081 2082 2083 2084 2085 2086 2086 37c0 37c5 37d2 37d2 2030 2031 2031 2032</td><td>System peripheral System perip</td><td>Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4x4x4) and a card in the 2nd slot. NOTE: Will</td><td></td></t<>	8086 8086 8086 8086 8086 8086 8086 8086	2080 2081 2082 2083 2084 2085 2086 2086 37c0 37c5 37d2 37d2 2030 2031 2031 2032	System peripheral System perip	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. NOTE: Will be present if there is a riser of type (x4x4x4x4) and a card in the 2nd slot. NOTE: Will	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.4 8 17:1e.5 8 17:1e.6 8 17:1e.5 8 19:03.0 8 1a:00.1 8 1a:00.1 8 3a:01.0 8 3a:02.0 8 3a:05.6 8 3a:02.0 8 3a:02.0 8 3a:02.0 8 3a:03.0 8	8086 8086 8086 8086 8086 8086 8086 8086	2080 2081 2082 2083 2084 2085 2086 306 37c0 37c2 37d2 2030 2031 2032	System peripheral System perip	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 3rd slot. 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 (x4x4x4x4) and a card in the 3rd slot. 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 (x8x4x4x4) and a card in the 3rd slot. NOTE: Will be present if there is a riser of type (x8x4x4x4) and a card in the 3rd slot. NOTE: Will be present if there is a riser of type (x8x4x4x4) and a card in the 3rd slot. NOTE: Will be present if there is a riser of type (x8x4x4x4) and a card in the 3rd slot. NOTE: Will be present if there is a riser of type (x8x4x4x4) and a card in the 3rd slot. NOTE: Will be present if there is a riser of type (x8x4x4x4) and a card in the 3rd slot. NOTE: Will	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.4 8 17:1e.5 8 17:1e.5 8 17:1e.6 8 17:1e.7 8 17:1e.6 8 17:1e.7 8 18:00.0 8 19:03.0 8 19:03.0 8 10:00.1 8 10:00.2 8 10:00.3 8 10:00.4 8 10:00.0 8 10:00.0 8 10:00.0 8 10:00.0 8 10:00.0 8 10:00.0 8 10:00.0 9 10:00.0 9 10:00.0 9 10:00.0 9 10:00.0 9 10:00.0 9 10:00.0 9 10:00.0 9 10:00.0 9 10:00.0 9 10:00.0 9 10:00.0 9 10:00.0 9 <t< td=""><td>8086 8086 8086 8086 8086 8086 8086 8086</td><td>2080 2081 2082 2083 2084 2085 2086 306 37c0 37c2 37d2 37d2 2030 2031</td><td>System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral Sustr, 18 and 19 if only 1 CPU is PCI bridge CI bridge CI bridge PCI bridge PCI bridge PCI bridge</td><td>Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x8) and a card in</td><td></td></t<>	8086 8086 8086 8086 8086 8086 8086 8086	2080 2081 2082 2083 2084 2085 2086 306 37c0 37c2 37d2 37d2 2030 2031	System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral Sustr, 18 and 19 if only 1 CPU is PCI bridge CI bridge CI bridge PCI bridge PCI bridge PCI bridge	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x4) and a card in the 2nd slot. 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 (x4x4x4x8) and a card in	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.4 8 17:1e.5 8 17:1e.5 8 17:1e.6 8 17:1e.5 8 19:03.0 8 1a:00.1 9 1a:00.1 9 <t< td=""><td>8086 8086 8086 8086 8086 8086 8086 8086</td><td>2080 2081 2082 2083 2084 2085 2086 306 37c0 37c2 37d2 37d2 2030 2031</td><td>System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral Sustr, 18 and 19 if only 1 CPU is PCI bridge CI bridge CI bridge PCI bridge PCI bridge PCI bridge</td><td>Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04) 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 (x4x4x48) and a card in the 2nd slot.</td><td></td></t<>	8086 8086 8086 8086 8086 8086 8086 8086	2080 2081 2082 2083 2084 2085 2086 306 37c0 37c2 37d2 37d2 2030 2031	System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral Sustr, 18 and 19 if only 1 CPU is PCI bridge CI bridge CI bridge PCI bridge PCI bridge PCI bridge	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04) 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 (x4x4x48) and a card in the 2nd slot.	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.4 8 17:1e.5 8 17:1e.5 8 17:1e.6 8 17:1e.5 8 19:03.0 8 19:03.0 8 1a:00.1 8 Bus 3a-3ce.v 8 3a:00.0 8	8086 8086 8086 8086 8086 8086 8086 8086	2080 2081 2082 2083 2084 2085 2086 2086 37c0 37c0 37c2 37d2 37d2 37d2	System peripheral System perip	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09) Intel Corporation Ethernet Connection X722 for 10GBASE-T (rev 09)	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.4 8 17:1e.5 8 17:1e.6 8 17:1e.7 8 17:1e.3 8 17:1e.4 8 19:03.0 8 19:03.0 8 1a:00.1 8	8086 8086 8086 8086 8086 8086 8086 8086	2080 2081 2082 2083 2084 2085 2086 2086 3705 37c5 37c5 37d2	System peripheral System perip	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode])	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.4 8 17:1e.5 8 17:1e.5 8 17:1e.6 8 17:1e.5 8 18:00.0 8 19:03.0 8 19:03.0 8	8086 8086 8086 8086 8086 8086 8086 8086	2080 2081 2082 2083 2084 2085 2086 2086 37c0 37c0 37c5	System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral Is 17, 18 and 19 if only 1 CPU is PCI bridge PCI bridge Ethernet controller	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode])	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.4 8 17:1e.5 8 17:1e.6 8 17:1e.7 8 17:1e.3 8 17:1e.4 8 17:1e.5 8 18:00.0 8 19:03.0 8	8086 8086 8086 8086 8086 8086 8086 1 1a are ma 8086 8086	2080 2081 2082 2083 2084 2085 2085 2086 2086 37c0 37c5	System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral Is 17, 18 and 19 if only 1 CPU is PCI bridge PCI bridge	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode]) Intel Corporation Device (rev 09) (prog-if 00 [Normal decode])	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.5 8 17:1e.5 8 17:1e.6 8 17:1e.5 8 18:00.0 8	8086 8086 8086 8086 8086 8086 8086 1 1a are ma 8086	2080 2081 2082 2083 2084 2085 2086 2086 2086 37c0	System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral system peripheral Is 17, 18 and 19 if only 1 CPU is PCI bridge	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Sky Lake-E PCU Registers (rev 04)	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.4 8 17:1e.5 8 17:1e.6 8 17:1e.7 8 17:1e.5 8 17:1e.6 8	8086 8086 8086 8086 8086 8086 8086 8086	2080 2081 2082 2083 2084 2085 2085 2086	System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral system peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Sky Lake-E PCU Registers (rev 04)	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.4 8 17:1e.5 8	8086 8086 8086 8086 8086 8086 8086	2080 2081 2082 2083 2084 2085 2085	System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Sky Lake-E PCU Registers (rev 04)	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.4 8 17:1e.5 8	8086 8086 8086 8086 8086 8086	2080 2081 2082 2083 2084 2085	System peripheral System peripheral System peripheral System peripheral System peripheral System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Sky Lake-E PCU Registers (rev 04)	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8 17:1e.4 8	8086 8086 8086 8086 8086	2080 2081 2082 2083 2083	System peripheral System peripheral System peripheral System peripheral System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8 17:1e.3 8	8086 8086 8086 8086	2080 2081 2082 2083	System peripheral System peripheral System peripheral System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)	
17:1d.1 8 17:1d.2 8 17:1d.3 8 17:1e.0 8 17:1e.1 8 17:1e.2 8	8086 8086 8086	2080 2081 2082	System peripheral System peripheral System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Sky Lake-E PCU Registers (rev 04)	
17:1d.1 & 8 17:1d.2 & 8 17:1d.3 & 8 17:1e.0 & 8 17:1e.1 & 8	8086 8086	2080 2081	System peripheral System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04) Intel Corporation Sky Lake-E PCU Registers (rev 04)	
17:1d.1 & £ 17:1d.2 & £ 17:1d.3 & £ 17:1e.0 & £	8086	2080	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)	
17:1d.1 & E 17:1d.2 & E 17:1d.3 & E					
17:1d.1 &	0000	2057	System peripheral	Inter corporation sky Lake-L CHA Registers (160 04)	
17:1d.1 8	8086			Intel Corporation Sky Lake-E CHA Registers (rev 04)	
	8086	2056	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
17:1d.0 8	8086	2055	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
	8086	2054	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
17:11.3 8	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
	8086	200e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
	8086	200e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
	8086	200e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
	8086	200e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
17:0f.6 8	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	

3a:0a.7	8086	2047	System peripheral	Intel Corporation Sky Lake-E LMDP Channel 1 (rev 04)
3a:0b.0	8086	2047	System peripheral	Intel Corporation Sky Lake-E DECS Channel 2 (rev 04)
3a:0b.1	8086	2040	System peripheral	Intel Corporation Sky Lake-E LM Channel 2 (rev 04)
3a:0b.2	8086	2045 204a	System peripheral	Intel Corporation Sky Lake-E LMS Channel 2 (rev 04)
3a:0b.3	8086	2040 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	2040	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
3a:0c.2	8086	2041		Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
	_		System peripheral	
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	Cardin 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	l 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 ($x4x4x4$) 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 (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)
5d:05.0				NOTE : Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot.
50.05.0	8086	2034	System peripheral	NOTE: Will be present if there is an expansion card of type (x4x4x4x4) and a card in the 4th slot. Intel Corporation Sky Lake-E VT-d (rev 04)
5d:05.2	8086 8086	2034 2035	System peripheral System peripheral	
				Intel Corporation Sky Lake-E VT-d (rev 04)
5d:05.2	8086	2035	System peripheral	Intel Corporation Sky Lake-E VT-d (rev 04) Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04)
5d:05.2 5d:05.4	8086 8086	2035 2036	System peripheral PIC	Intel Corporation Sky Lake-E VT-d (rev 04) Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04) Intel Corporation Sky Lake-E IOxAPIC Configuration Registers (rev 04) (prog-if 20 [IO(X)-APIC])
5d:05.2 5d:05.4 5d:0e.0	8086 8086 8086	2035 2036 2058	System peripheral PIC Performance counters	Intel Corporation Sky Lake-E VT-d (rev 04) Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04) Intel Corporation Sky Lake-E IOxAPIC Configuration Registers (rev 04) (prog-if 20 [IO(X)-APIC]) Intel Corporation Sky Lake-E KTI 0 (rev 04)
5d:05.2 5d:05.4 5d:0e.0 5d:0e.1	8086 8086 8086 8086	2035 2036 2058 2059	System peripheral PIC Performance counters System peripheral	Intel Corporation Sky Lake-E VT-d (rev 04) Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04) Intel Corporation Sky Lake-E IOxAPIC Configuration Registers (rev 04) (prog-if 20 [IO(X)-APIC]) Intel Corporation Sky Lake-E KTI 0 (rev 04) Intel Corporation Sky Lake-E UPI Registers (rev 04)
5d:05.2 5d:05.4 5d:0e.0 5d:0e.1 5d:0f.0	8086 8086 8086 8086 8086 8086	2035 2036 2058 2059 2058	System peripheral PIC Performance counters System peripheral Performance counters	Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04) Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04) Intel Corporation Sky Lake-E IOxAPIC Configuration Registers (rev 04) (prog-if 20 [IO(X)-APIC]) Intel Corporation Sky Lake-E KTI 0 (rev 04)
5d:05.2 5d:05.4 5d:0e.0 5d:0e.1 5d:0f.0 5d:0f.1	8086 8086 8086 8086 8086 8086 8086	2035 2036 2058 2059 2058 2059	System peripheral PIC Performance counters System peripheral Performance counters System peripheral	Intel Corporation Sky Lake-E VT-d (rev 04) Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04) Intel Corporation Sky Lake-E IOxAPIC Configuration Registers (rev 04) (prog-if 20 [IO(X)-APIC]) Intel Corporation Sky Lake-E KTI 0 (rev 04) Intel Corporation Sky Lake-E UPI Registers (rev 04)
5d:05.2 5d:05.4 5d:0e.0 5d:0e.1 5d:0f.0 5d:0f.1 5d:10.0	8086 8086 8086 8086 8086 8086 8086	2035 2036 2058 2059 2059 2058 2059 2058	System peripheral PIC Performance counters System peripheral Performance counters System peripheral Performance counters	Intel Corporation Sky Lake-E VT-d (rev 04) Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04) Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04) (prog-if 20 [I0(X)-APIC]) Intel Corporation Sky Lake-E KTI 0 (rev 04)
5d:05.2 5d:05.4 5d:0e.0 5d:0e.1 5d:0f.0 5d:0f.1 5d:10.0 5d:10.1	8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086	2035 2036 2058 2059 2058 2059 2058 2058	System peripheral PIC Performance counters System peripheral Performance counters System peripheral Performance counters System peripheral	Intel Corporation Sky Lake-E VT-d (rev 04) Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04) Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04) (prog-if 20 [I0(X)-APIC]) Intel Corporation Sky Lake-E KTI 0 (rev 04) Intel Corporation Sky Lake-E KTI 0 (rev 04) Intel Corporation Sky Lake-E UPI Registers (rev 04) Intel Corporation Sky Lake-E KTI 0 (rev 04) Intel Corporation Sky Lake-E KTI 0 (rev 04) Intel Corporation Sky Lake-E UPI Registers (rev 04)
5d:05.2 5d:05.4 5d:0e.0 5d:0e.1 5d:0f.0 5d:0f.1 5d:10.0 5d:10.1 5d:12.0	8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086	2035 2058 2059 2059 2059 2059 2058 2059 2059 204c	System peripheral PIC Performance counters System peripheral Performance counters System peripheral Performance counters System peripheral Performance counters System peripheral Performance counters Performance counters Performance counters Performance counters	Intel Corporation Sky Lake-E VT-d (rev 04) Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04) Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04) (prog-if 20 [I0(X)-APIC]) Intel Corporation Sky Lake-E KTI 0 (rev 04) Intel Corporation Sky Lake-E UPI Registers (rev 04) Intel Corporation Sky Lake-E KTI 0 (rev 04) Intel Corporation Sky Lake-E KTI 0 (rev 04) Intel Corporation Sky Lake-E KTI 0 (rev 04) Intel Corporation Sky Lake-E MIR Registers (rev 04) Intel Corporation Sky Lake-E MIR Registers (rev 04) Intel Corporation Sky Lake-E MIR Registers (rev 04)
5d:05.2 5d:05.4 5d:0e.0 5d:0e.1 5d:0f.0 5d:0f.1 5d:10.0 5d:10.1 5d:12.0 5d:12.2	8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086	2035 2036 2058 2059 2058 2059 2058 2059 204c 204c	System peripheral PIC Performance counters System peripheral	Intel Corporation Sky Lake-E VT-d (rev 04)Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04)Intel Corporation Sky Lake-E IOxAPIC Configuration Registers (rev 04) (prog-if 20 [IO(X)-APIC])Intel Corporation Sky Lake-E KTI 0 (rev 04)Intel Corporation Sky Lake-E KTI 0 (rev 04)Intel Corporation Sky Lake-E UPI Registers (rev 04)Intel Corporation Sky Lake-E KTI 0 (rev 04)Intel Corporation Sky Lake-E KTI 0 (rev 04)Intel Corporation Sky Lake-E UPI Registers (rev 04)Intel Corporation Sky Lake-E UPI Registers (rev 04)Intel Corporation Sky Lake-E KTI 0 (rev 04)Intel Corporation Sky Lake-E KTI 0 (rev 04)Intel Corporation Sky Lake-E MIR Registers (rev 04)
5d:05.2 5d:05.4 5d:0e.0 5d:0f.0 5d:0f.0 5d:10.0 5d:10.1 5d:12.0 5d:12.1 5d:12.2 5d:12.2	8086 8086	 2035 2036 2058 2059 2059 2058 2059 2058 2059 204c 204c 204c 	System peripheral PIC Performance counters System peripheral Performance counters Performance counters System peripheral Performance counters System peripheral Performance counters	Intel Corporation Sky Lake-E VT-d (rev 04)Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04)Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04) (prog-if 20 [I0(X)-APIC])Intel Corporation Sky Lake-E KTI 0 (rev 04)Intel Corporation Sky Lake-E MJRTI Registers (rev 04)
5d:05.2 5d:0e.0 5d:0e.1 5d:0f.0 5d:0f.1 5d:10.0 5d:10.1 5d:12.0 5d:12.1 5d:12.2	8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086 8086	2035 2036 2058 2059 2058 2059 2058 2059 204c 204c	System peripheral PIC Performance counters System peripheral	Intel Corporation Sky Lake-E VT-d (rev 04)Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04)Intel Corporation Sky Lake-E IOxAPIC Configuration Registers (rev 04) (prog-if 20 [IO(X)-APIC])Intel Corporation Sky Lake-E KTI 0 (rev 04)Intel Corporation Sky Lake-E KTI 0 (rev 04)Intel Corporation Sky Lake-E UPI Registers (rev 04)Intel Corporation Sky Lake-E KTI 0 (rev 04)Intel Corporation Sky Lake-E KTI 0 (rev 04)Intel Corporation Sky Lake-E UPI Registers (rev 04)Intel Corporation Sky Lake-E UPI Registers (rev 04)Intel Corporation Sky Lake-E KTI 0 (rev 04)Intel Corporation Sky Lake-E KTI 0 (rev 04)Intel Corporation Sky Lake-E MIR Registers (rev 04)

www.kontron.com

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	Cardin expansion "Slot 5 "or "Slot 5 + Riser 1 st Slot "	depending on PCIe expansion card –	
5f:00.x ^{Slot} 5	ХХХХ	XXXX	Card in expansion "Slot 5 + Riser 2 nd Slot	depending on PCIe expansion card -	
50:00.x 5lot 5	ХХХХ	XXXX	" Card in expansion "Slot 5 + Riser 3 rd Slot "	depending on PCIe expansion card -	
51:00.x Slot	XXXX	XXXX	Card in expansion "Slot 5 + Riser 4 th Slot "	depending on PCIe expansion card –	
Next buses	are only a	vailable 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)	
30:04.2	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)	
30:04.5	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)	
30:04.7	8086	2021	System peripheral	Intel Corporation Sky Lake-E CBDMA Registers (rev 04)	
30:05.0	8086	2024	System peripheral	Intel Corporation Sky Lake-E MM/Vt-d Configuration Registers (rev 04)	
30:05.2	8086	2025	System peripheral	Intel Corporation Sky Lake-E RAS (rev 04)	
30:05.4	8086	2026	PIC	Intel Corporation Sky Lake-E IOAPIC (rev 04) (prog-if 20 [IO(X)-APIC])	
30:08.0	8086	2014	System peripheral	Intel Corporation Sky Lake-E Ubox Registers (rev 04)	
30:08.1	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)	
35:00.0 5lot 2	8086	2030	PCI bridge	Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04)	
85:01.0 5lot 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 (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 5lot 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)	
35:05.2	8086	2035	System peripheral	Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04)	
35:05.4	8086	2036	PIC	Intel Corporation Sky Lake-E IOxAPIC Configuration Registers (rev 04) (prog-if 20 [IO(X)-APIC])	
35:08.0	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
35:08.1	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
35:08.2	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
35:08.3	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
35:08.4	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
5:08.5	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
35:08.6	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
35:08.7	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
35:09.0	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)	
35:09.1	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)	
35:09.2	8086	2080 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			
85:10.0	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04) Intel Corporation Sky Lake-E CHA Registers (rev 04)	
			System peripheral		
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)	
	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	Cardin expansion "Slot 2 "or"Slot 2 + Riser 1 st Slot "	depending on PCIe expansion card –	
87:00.x Slot 2	XXXX	XXXX	Cardin expansion "Slot 2 + Riser 2 nd Slot	depending on PCIe expansion card -	
88:00.x Slot 2	ХХХХ	XXXX	Cardin expansion "Slot 2 + Riser 3 rd Slot	depending on PCIe expansion card -	
89:00.x Slot 2	XXXX	XXXX	" Cardin 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	2045	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)	
ae:0a.5	8086	2044	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)	
47∙0£1	2026	7059	Suctom norinhoral	Intel Corneration Sky Lake_F LIPI Registers (rev 0/1) WWWW kontron com	

u	0000	2000	system periprierat	Inter corporation any care is or mediaters (revion)
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 <code>Slot n</code> .

 $^{\sf NVMe}$: 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
 - <u>Serviceable items (spare)</u>
 - <u>Fans</u>
 - HDD/SSD carrier
 - Front bezel
 - <u>Top cover</u>
 - Power supply units
 - <u>PCIe configurations and PCIe risers</u>
 - PCIe slots
 - PCIe riser slots
 - <u>PCIe risers</u>
 - <u>Rackmount kits</u>
 - <u>Accessories</u>

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	
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 (iaca)) s
1	GND	Black	
2	GND	Black	4 00 8
3	GND	Black	FRONT VIEW
4	GND	Black	PCIe AUX POWER
5	+12V	Yellow	
6	+12V	Yellow	
7	+12V	Yellow	
8	+12V	Yellow	

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	N/A	1
The second secon	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.		
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
 - <u>Component installation and assembly</u>
 - Power cables and tooling
 - <u>Rack installation material</u>
 - Network cables and modules
 - <u>Network infrastructure</u>
- <u>Software required</u>

Material and information required

Optional adapter



Component installation and assembly

Relevant section:

Components installation and assembly

ltem_1	#1 Phillips (cross-point) screwdrivers (or interchangeable tip screwdriver with #1 and #2 Phillips bits)			
ltem_2	2 Phillips (cross-point) screwdrivers (or interchangeable tip screwdriver with #1 and #2 Phillips bits)			
ltem_3	One T30 Torx screwdriver			
ltem_4	One 5 -mm flat-head screwdriver			
ltem_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_1Back stranded 12 AWG wire to build the power cable based on the length requiredItem_2Red stranded 12 AWG wire to build the power cable based on the length requiredItem_3One Positronic DC power supply input mating connector (includes a strain relief assembly)Item_4Three Positronic gauge-16 crimp terminalsItem_5Two strain relief screwsItem_6One strain relief screwsItem_7One strain relief plateItem_9Two flat head Phillips screwsItem_9One hand crimp tool, DMC AF8Item_10One strain cloud cable based on the length requiredItem_11One ground Lag BAWG (Kontron P/N 1064-4226)Item_12One more capital et al.Item_13One hand crimp tool, Panduit CT-1700		
Item_3One Positronic DC power supply input mating connector (includes a strain relief assembly)Item_4Three Positronic gauge-16 crimp terminalsItem_5Two strain relief screwsItem_6One strain relief plateItem_7Two flat head Phillips screwsItem_8One hand crimp tool, DMC AF8Item_10One strain toolItem_11One ground cable based on the length requiredItem_12One ground lug right angle, 8 AWG (Kontron P/N 1064-4226)	ltem_1	Black stranded 12 AWG wire to build the power cable based on the length required
Item_4Three Positronic gauge-16 crimp terminalsItem_5Two strain relief screwsItem_6One strain relief plateItem_7Two flat head Phillips screwsItem_8One hand crimp tool, DMC AF8Item_9One manual extraction toolItem_10One ground Lable based on the length requiredItem_11One ground lug right angle, 8 AWG (Kontron P/N 1064-4226)Item_12Internet on tool	ltem_2	Red stranded 12 AWG wire to build the power cable based on the length required
Item_5Two strain relief screwsItem_6One strain relief plateItem_7Two flat head Phillips screwsItem_8One hand crimp tool, DMC AF8Item_9One manual extraction toolItem_10One 8 AWG ground cable based on the length requireditem_11One ground lug right angle, 8 AWG (Kontron P/N 1064-4226)Item_12Un myrench or equivalent tool	ltem_3	
Item_6One strain relief plateItem_7Two flat head Phillips screwsItem_8One hand crimp tool, DMC AF8Item_9One manual extraction toolItem_10One 8 AWG ground cable based on the length requireditem_11One ground lug right angle, 8 AWG (Kontron P/N 1064-4226)Item_12In mwrench or equivalent tool	ltem_4	Three Positronic gauge-16 crimp terminals
Item_7Two flat head Phillips screwsItem_8One hand crimp tool, DMC AF8Item_9One manual extraction toolItem_10One 8 AWG ground cable based on the length requireditem_11One ground lug right angle, 8 AWG (Kontron P/N 1064-4226)Item_12In mwrench or equivalent tool	ltem_5	Two strain relief 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 0 mm wrench or equivalent tool	ltem_6	One strain relief plate
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	ltem_7	Two flat head Phillips screws
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	ltem_8	One hand crimp tool, DMC AF8
item_11 One ground lug right angle, 8 AWG (Kontron P/N 1064-4226) Item_12 10 mm wrench or equivalent tool	Item_9	One manual extraction tool
Item_12 10 mm wrench or equivalent 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_13 One hand crimp tool, Panduit CT-1700	Item_12	10 mm wrench or equivalent tool
	Item_13	One hand crimp tool, Panduit CT-1700

Rack installation material

Relevant section: Rack installation

Network cables and modules

ltem_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

ltem_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.
ltem_2	A terminal emulator such as puTTY is installed on a remote computer.
ltem_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

- Memory RDIMM ECC module
- <u>M.2 SSD (SATA or NVMe)</u>
- <u>SSD 2.5 in (SATA)</u>
- <u>SSD 2.5 in (SAS)</u>
- HDD SAS 2.5 in (SAS)
- SAS and RAID PCIe cards
- PCle NIC cards
- <u>FCIE NIC Calus</u>

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	Туре	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	Туре	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	Туре	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	Туре	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

- <u>Status description</u>
 <u>OS certification status</u>

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 <u>Configuring and managing users</u>.
- Determine the access paths that are to be closed or open. Refer to <u>Configuration of system access methods</u>.
- The platform features a Trusted Platform Module (TPM). Determine your requirement with regards to hardware-based, security-related functions. Refer to <u>Configuring TPM</u>.

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
 - <u>Unboxing</u>
 - Components installation and assembly
 - <u>Airflow</u>
 - Rack installation
 - <u>Cabling</u>
- Software installation and deployment
 - Preparing for installation
 - Installing an operating system on a server
 - <u>Verifying installation</u>
 - Platform installation for high availability
 - <u>Common software installation</u>

Mechanical installation and precautions

[This section details the steps and safety precautions required for the physical installation of the product.]

- Children
 - ESD protections
 - <u>Unboxing</u>
 - <u>Components installation and assembly</u>
 - <u>Airflow</u>
 - <u>Rack installation</u>
 - <u>Cabling</u>

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

• What's in the box <u>Unboxing steps</u>

At.A	

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 <u>Components installation and assembly</u> 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

- <u>Tools and supplies needed</u>
- <u>Compatible parts and components</u>
- Cable management
- Front bezel
 - <u>Removing the front bezel</u>
 - <u>Reinstalling the front bezel</u>
- <u>Chassis top cover</u>
 - <u>Removing the chassis top cover</u>
 - <u>Reinstalling the chassis cover</u>
- <u>Drives</u>
 - <u>Removing a drive carrier from the chassis</u>
- Installing a drive in a carrier
- <u>System fans</u>
- Replacing a fan
- Power supply unit
- Inserting or replacing a power supply unit
- <u>Riser card assemblies</u>
 - <u>Removing a riser card assembly</u>
 - <u>Removing the left riser card assembly</u>
 - <u>Removing the right riser card assembly</u>
 - <u>Reinstalling a riser card assembly</u>
 - <u>Reinstalling the left riser card assembly</u>
 <u>Reinstalling the right riser card assembly</u>
- <u>Processor air duct</u>
 - <u>Removing the processor air duct</u>
 - Reinstalling the processor air duct
- SuperCap battery backup
 - <u>Removing the SuperCap battery backup</u>
 - <u>Reinstalling the SuperCap battery backup</u>
- Support cross-brace
- <u>Removing the support cross-brace</u>
 - <u>Reinstalling the support cross-brace</u>
- <u>SAS hot-swap backplane (HSBP) board</u>
 - <u>Removing the SAS hot-swap backplane (HSBP) board</u>
 - <u>Reinstalling the SAS hot-swap backplane (HSBP) board</u>
- <u>Memory DIMMs</u>
 - Locating the DIMMs
 - <u>DIMM population guidelines for optimal performance</u>
 - <u>Removing memory DIMMs</u>
 - Installing memory DIMMs
- Processor and heat sink
 - Socket and processor handling and ESD precautions
 - <u>Handling precautions</u>
 - ESD precautions
 - <u>Processor location</u>
 - Disassembling the processor heat sink module (PHM)
 - Adding or replacing a processor in a PHM
 - Preparing the processor for assembly with the PHM
 - Installing the processor (new heat sink and processor carrier)
- Installing a PHM in the platform
- <u>Raid controller</u>
 - <u>Disconnecting the two SAS cables from the motherboard</u>
 - Locating the SAS cables
 - Disconnecting the SAS cables
 - Installing a hardware RAID controller
- Installing the SuperCap battery backup module
- PCle add-in cards and riser cards
 - PCIe add-in cards in slots 4 and 5
 - Installing a PCIe add-in card
 - <u>Removing a PCIe card</u>
 - PCIe riser cards
 - Assembling the PCIe riser cards
 - PCIe add-in cards on riser assemblies
 - Removing a PCIe add-in card
 - Installing PCIe add-in cards
- <u>M.2 storage</u>
 - Locating the M.2 storage
 - <u>Removing an M.2 storage</u>
 - Installing an M.2 storage



ESD sensitive device!

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

4	Disc	connect 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 <u>ESD protections</u> .
A WAR	NING	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 re	eferences 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).	
		(1949)89

Chassis top cover

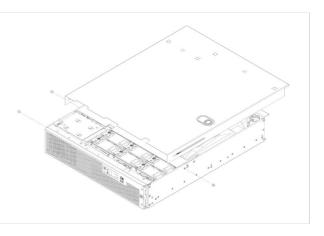
A	Standby power is present inside the chassis whenever the power supply module(s) are connected to a power source. Before removing the top cover, always power down the server and unplug all peripheral devices and the power cable(s).			
ΝΟΤΙΟ	CE	The CG2400 server must be operated with the top cover in 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.	n
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 $bf \cdot in$.
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

ΝΟΤΙΟ	CE	Drives must be installed in the proper orientation in the carrier. Failure to do so may damage the equipment.	
Step_1	attach i OR If a driv	ive carrier is empty (first time installation), remove the black plastic filler panel by unfastening the four screws that t to the carrier (A). Set the screws aside for use with the new drive. e is already installed (drive replacement), remove it by unfastening the four screws that attach the drive to the drive A). Set the screws aside for use with the new drive.	
Step_2	Lift the	drive (or filler panel) out of the carrier (B).	Protest
Step_3	NOTE: positior	he new drive in the drive carrier (A) and secure the drive with the four screws (with 4 lbf-in torque, max) (B). Ensure proper drive orientation. The SATA connector must be exposed in the back of the carrier. When the carrier is in the shown on the image, the SATA connector located in the back of the drive must not be visible. It should be in contact with k surface.	
Step_4	With th	e 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 th	ne locking lever until it snaps shut and secures the drive in the slot (B).	CCOORE

System fans

Fans are hot-swappable .

ACAUTIONBecause 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).	Image: series of the series
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).	
		(6003

Removing the right riser card assembly

Step_2 Using the two blue touch points (C), lift the riser card assembly out of the chassis (D). 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.	2
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. 	and the second s
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.	Astrony of the second s
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).	

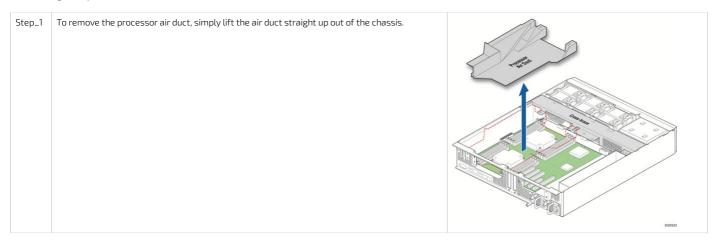
Processor air duct

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.	
ΝΟΤΙΟ	E 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



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.

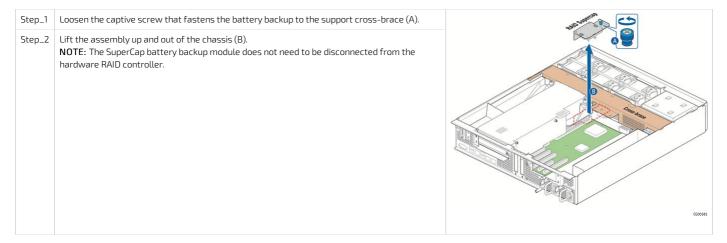
SuperCap battery backup

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



Reinstalling the SuperCap battery backup

	Position the SuperCap backup battery assembly over the support cross-brace (A).
(B).	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 	<image/>
Step_2	Remove the three small flat screws that fasten the cross-brace to the sides of the chassis:One on the left sideTwo on the right side	ann tan III
Step_3	Remove the support cross-brace from the chassis.	Procession of the second

Reinstalling the support cross-brace

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).	الله الله الله الله الله الله الله الله
Step_3	Lift the cover plate off of the HDD bay assembly (C).	Note: Chassis and Front Panel NOT shown for daity.
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 I² C/HDD LED cable 	Back View
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 Re-install the SAS backplane board and air duct (B).	Image: selection of the se
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).	الله الله الله الله الله الله الله الله
Step_4	Re-fasten the screw that holds the cover plate in place (C).	Note: Chassis and Front Panel NOT shown for clarity.
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

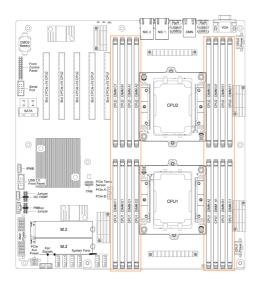


To reduce the risk of electrostatic discharge (ESD) damage to the processor or the DIMMs, be sure to follow these procedures:

- 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 <u>Hardware compatibility list</u>.

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).	F
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)	F
Step_2	Note the location of the alignment notch on the DIMM edge. (B)	The The American State
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) \ensuremath{E}	

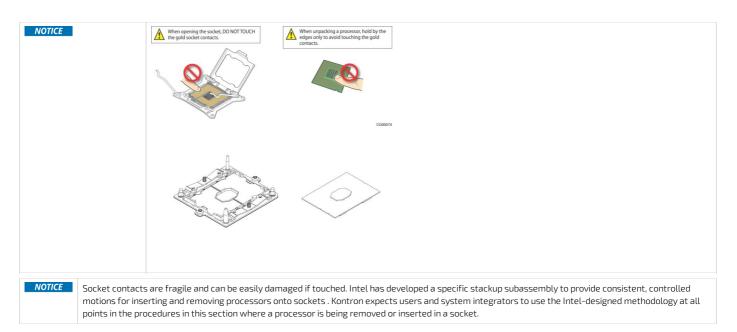
Processor and heat sink

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



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.

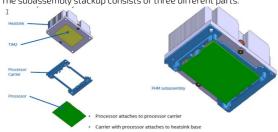
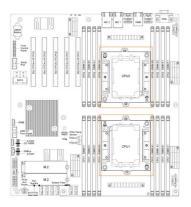


Image source: Intel Corporation

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.	1/4" WIDE #1 FLATHEAD SCREW DRIVER
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 <u>Hardware compatibility list</u> 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.	ALL AND STREET
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.

1

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

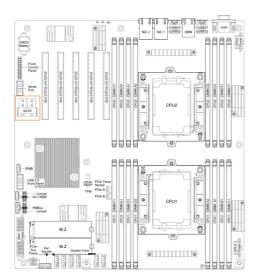
Before you can install or remove the hardware RAID controller board and the SuperCap battery backup module, you must first remove (and afterwards put back in place):

• the [Content under creation] chassis top cover

• the left side [Content under creation] riser card assembly

Disconnecting the two SAS cables from the motherboard

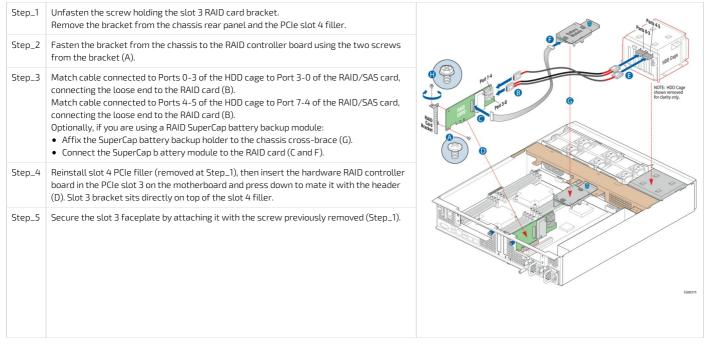
Locating the SAS cables



Disconnecting the SAS cables

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

Installing a hardware RAID controller



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 <u>Platform, modules and accessories</u>.

- ·		
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).	and the second s
Step_3	Slide the module/tray assembly towards the back (side with the connector) of the bracket until it locks into place.	CON12
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).	0 the second second
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.	

PCle add-in cards and riser cards

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

ACAUTION 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

Step_1	Fasten each riser card to its bracket with the two 6/32 screws (8 lbf-in torque) .	Communities of the second seco
		C600210

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):

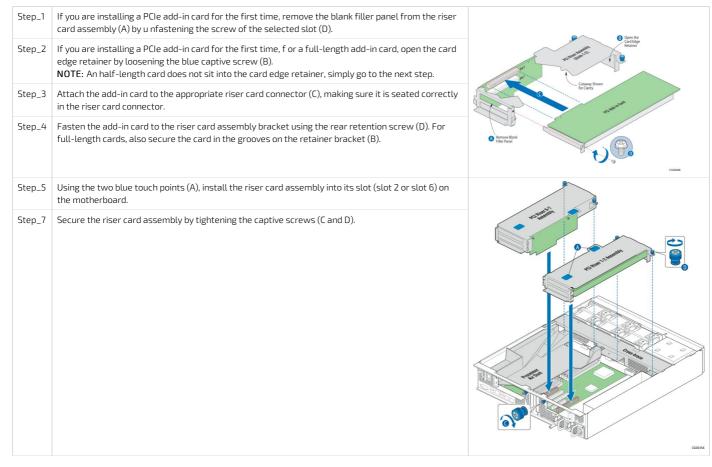
the [Content under creation] chassis top cover

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. 	Contraction of the last the la
Step_2	Unfasten and remove the rear retention screw (D).	Gutanay Shown
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).	D Prove Bala
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.	Ссеема

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).



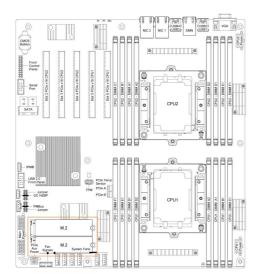
M.2 storage

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

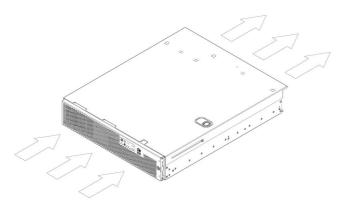
Step_1	Remove the clip from the post. NOTE: When only one M.2 storage is added, it is recommended to use the slot located near the fans.	
Step_2	Insert one end of the M.2 card in the connector and seat the other end around the post on the motherboard.	
Step_3	Secure the M.2 storage by inserting the clip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

Airflow

(This article provides guidelines to ensure proper airflow to the platform.) Table of contents

- <u>Airflow direction</u>
- <u>Considerations for proper airflow</u>

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
 - <u>Rack mount kits</u>
 - TMLCMOUNT21
 - TMLPMOUNT51
 - <u>TMLPMOUNT52</u>
 - <u>Bracket and extender kits</u>
 - <u>1059-8187 extender kit</u>
 - <u>1061-2890 extender kit</u>
- Installing the server in a rack
 - Using TMLPMOUNT51 or TMLPMOUNT52
 - Installing inner rails and mounting ears
 - Building the outer rail assembly
 - Four-post installation racks under 24-inches deep
 - Four-post installation racks 24- to 31%-inches deep
 - Four-post installation racks 3014- to 343%-inches deep
 - <u>Two-post installation</u>
 - <u>Attaching the outer rail assemblies to the rack posts</u>
 - <u>Securing the equipment</u>
 - Securing the equipment to a 4-post rack
 - Securing the equipment to a 2-post rack
 - Using TMLPMOUNT21
- Earth grounding

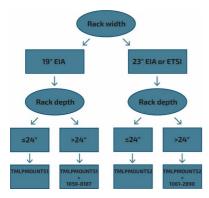
Selecting a rail kit

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

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

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

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



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
TMLPMOUNTS1	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.

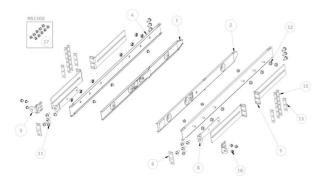
- EIA Wide spacing doesn't have the interstitial hole that is present in EIA Universal spacing. TMLPMOUNT51 contains an EIA Wide Adapter to overcome issue.

Rack mount kits

TMLCMOUNT21

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

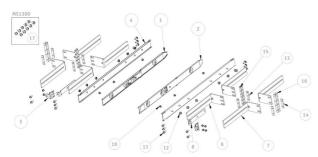
TMLPMOUNT51



Item	Qty	Description
1	1	LEFT INNER RAIL
2	1	RIGHT INNER RAIL
З	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.

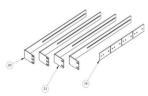
Bracket and extender kits

1059-8187 extender kit

0 G (19)

ltem	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

	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).
<u>/1</u>	 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 an outlet that is part of the rack, then you must provide 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.
NOTIC	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 rac	к.

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 31% deep, go to [Content under creation] Four-post installation racks 24- to 31%-inches deep
- For a 4-post installation for racks 30¼" to 34%" deep, go to [Content under creation] Four-post installation racks 30¼- to 34%-inches deep

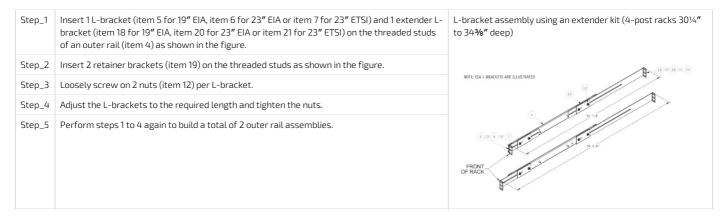
Four-post installation – racks under 24-inches deep

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 31%-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 31‰″ deep)
Step_2	Insert 2 retainer brackets (item 19) on the threaded studs as shown in the figure.	NOTE: EIA L-BRACKETS ARE ILLUSTRATED
Step_3	Loosely screw on 2 nuts (item 12) per L-bracket.	10 The A
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.	FRONT OF RACK

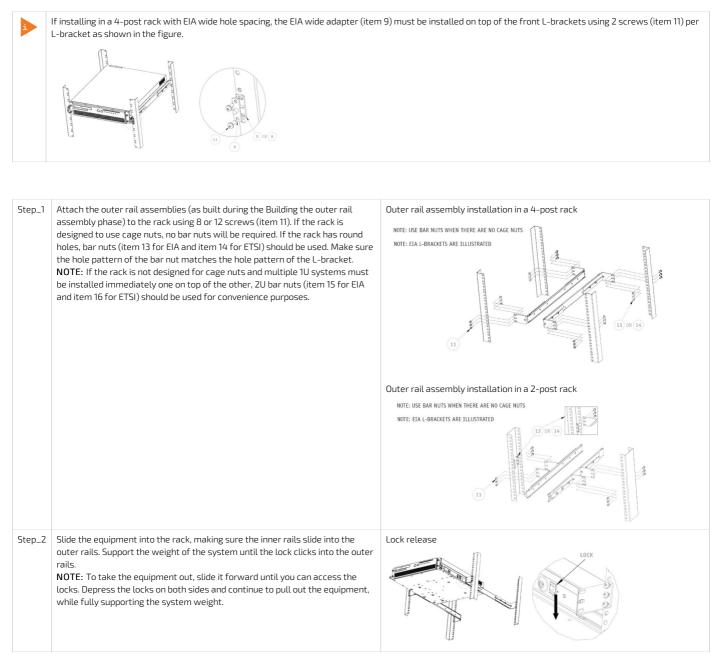
Four-post installation - racks 30¼- to 343/8-inches deep



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.	NOTE: EIA L-BRACKETS ARE ILLUSTRATED
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.	9 (5) OR (6) OR (7)
Step_5	Perform steps 1 to 4 again to build a total of 2 outer rail assemblies.	8 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6

Attaching the outer rail assemblies to the rack posts



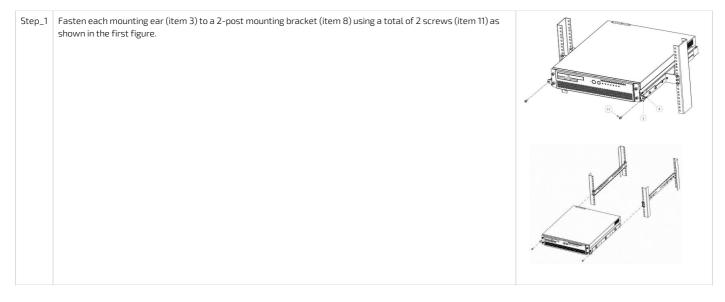
Securing the equipment

- 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



Using TMLPMOUNT21

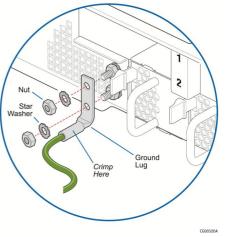
Step_1	Fasten each mounting bracket to the platform using a total of 3 screws as shown in the figure.	
Step_2	Fasten each mounting bracket to the rack using a total of 2 screws as shown in the figure.	

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.	(v



Cabling

[This article provides all necessary details to safely connect the platform: connection types, required cables, prerequisites, connection sequences.] Table of contents

<u>AC power supply</u>

- <u>Power cord usage guidelines</u>
- <u>AC power supply connection</u>
- DC power supply
- DC power sup
 - <u>DC power supply input connector</u>
 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
 - DC power supply connection

AC power supply

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

AWARNING 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.

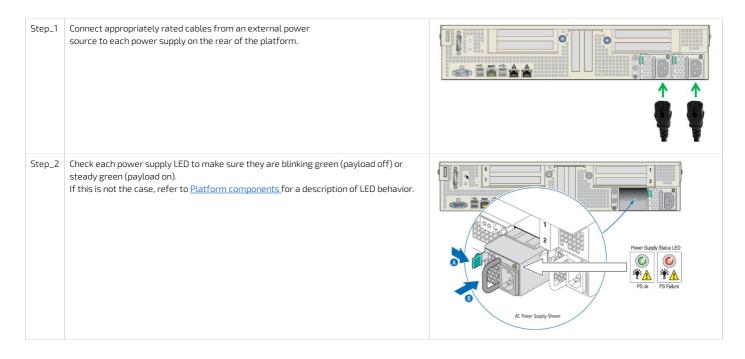
Power cord usage guidelines

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



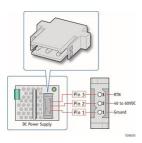
DC power supply

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.

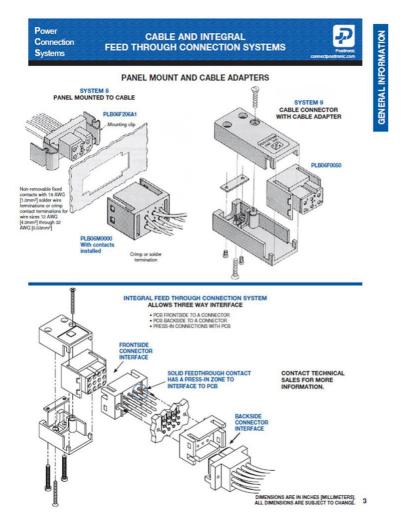
DC power supply input connector

• 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

AWARNING 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.

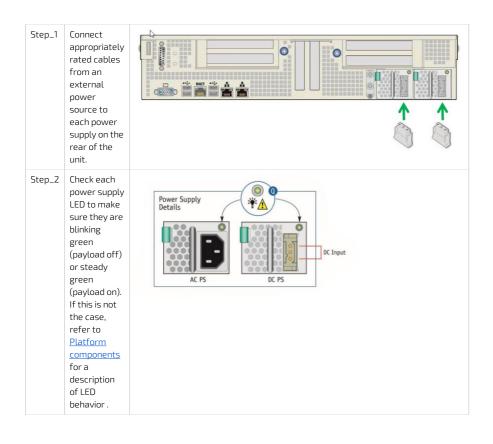
NOTE: The other ends of the cables will need to be built according to national wiring codes and conform to local regulations in addition to your data center power installation requirements.

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	<u>Positronic catalog</u>
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	 <u>DMC hand crimp tool catalog</u> <u>DMC AF8 data sheet</u>
Manual extraction tool	1	<u>9081-0-0-0</u>	 <u>Molex extraction tool catalog</u> <u>Application tooling</u> <u>specification sheet</u>

Below is a link to a <u>video showing how to crimp pins</u> 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



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
 - <u>Common software installation</u>

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 <u>Validated operating systems</u>. For information on components, refer to the <u>PCI mapping</u>.

Installing an operating system on a server

[This article provides step-by-step OS installation instructions for all access paths.] Table of contents

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

<u>Accessing a BMC</u>

Prerequisites

2 The remote computer has access to the management network subnet.	
2 merende compater has access to the management network subject.	

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 er NOTE: The HTTPS prefix is mandatory. https://[BMC MNGMT_IP]	iter the IP address discovered for the BMC.
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.	<section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>
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.	Image: Section 1.1 I
Step_4	Log in to the BMC Web UI using the appropriate credentials. NOTE: Default Web UI user name and password is admin/admin.	Literane Passend Signein Erget my passend
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	Arristic Arritory Arrito

Changing the user name and password

i

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 .	Image: Control of the control of t
Step_2	Select the user to manage. NOTE: The first and second users are reserved fields, therefore, their usernames can't be modified.	Image: Constraint of the constr
Step_3	Change field Username if required.	Username operator Change Password Assword Size A bytes Password Confirm Password Confirm Password
Step_4	Check the Change Password box.	Username operator Change Password Password Size I blytes Password Confirm Password Confirm Password
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.	Username operator Change Password Password Size Sobytes Password Confirm Password
Step_6	Confirm the password.	Username operator Change Password Password Size Password Confirm Password Confirm Password
Step_7	Press Save .	Email Format AMB-Format Email ID Existing SSH Key Not Available Upload SSH Key Codeer

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.	

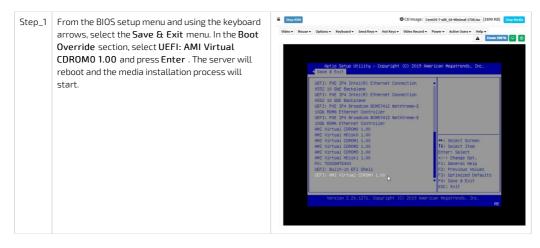
Mounting the operating system image via virtual media

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 .	Contract: (normality (normality)) (normality) Contract: (normal
		84
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.	Burg XXX C Dhinge: Cando Falls, 6446-inal 1210/av (0 K8) Burg XXX Videx + Kouse* Options* Keybaard* Send Keys* Het Keys* Vides Bacrif* Prese* Active Lises* Heig* Dem Staffs Company Company Company Keybaard* Send Keys* Het Keys* Vides Bacrif* Prese* Active Lises* Heig* Vides + Kouse* Options* Keybaard* Send Keys* Het Keys* Vides Bacrif* Prese* Active Lises* Heig* Vides + Kouse* Options* Keybaard* Send Keys* Het Keys* Vides Bacrif* Prese* Active Lises* Heig* Vides + Kouse* Options* Keybaard* Send Keys* Het Keys* Vides Bacrif* Prese* Active Lises* Heig*

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.	Det many: (see 16 and and and and the second the s
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.	<page-header></page-header>

Selecting the boot order from boot override



> 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.

<u>Accessing the BIOS</u>

NOTE: Using Boot from LAN requires a PXE server architecture.

Step_1	Access the BIOS menu. Refer to Accessing the		
Step_2	Select the Advanced tab and then the Network Stack Configuration submenu.	Aptio Setup Utility - Copyright (C) 2019 Aum Rain Advanced Intel®EStup Server How Secu > Trusted Computing > Redish Host Interface Settings > Setial Port Console Redirection > D CSB Configuration > DSB Configuration > Task the Configuration > KAK Disk Configuration > KAK 12839FE2E607-IFv4 Network Configuration Acti2839FE2E607-IFv6 Network Configuration	<pre>team Megatrends, Inc. tivy Boot Yeam Logs Network Stack Settings </pre>
Step_3	Enable Network Stack .	Version 2.20.1271. Copyright (c) 2019 Ameri Aptio Setup Utility - Copyright (c) 2019 Ameri Advanced Persons Stack (Enabled) Ipv4 FME Support (Disabled) Ipv6 FME Support (<pre>can Megatrends, Inc. ican Megatrends, Inc. Enable/Disable UEFI Network Stack Enable/Disable UEFI Network Stack iv: Select Stack iv: Select Ican Enter: Sele</pre>
Step_4	Enable IPv4 PXE Support or IPv6 PXE Support, depending on the application.	Aprio Setup Utility - Copyright (C) 2019 Ame Advanced Network Stack [Enabled] Try By Support [Disabled] Try BYTP Support [Disabled] Try BYTP Support [Disabled] PYE Boot wait time 0 Hedia detect count 1 Statute 2 20 221 Computed (C) 2010 Ame	Enable/Disable IPv4 FXE boot support. If disabled, IPv4 FXE boot swallable. vvs1buble. vvs1buble. vvs1buble. vvs1buble. vvs1buble. vvs1buble. fv1buble. fv1bu
Step_5	Reboot the system and access the BIOS setup	menu once again.	can megacrenus, inc.
Step_6	Navigate to the Save & Exit menu and then to the Boot Override section.	Aptio Setuo - American Megatrends Inte ▲ Security Ecot Save a Exit Restare User Defaults Boot Override Centos (P4: SaMSUNG M27N0480HA8H-00003) UEFI: Fatriat Memory PMAP, Partition 1 UEFI: Patriat Memory PMAP, Partition 1 UEFI: Built-in EFI Shell MFI Virtual CBCNO 1.00 SATAO P4: SAMSUNG M27N0480HA8H SATAO P5: INTEL SSOC2082408B Generic Ultra HS-SD 1 Patriat Memory PMAP AMI Virtual HDIskO 1.00 Generic Ultra HS-SD 1 UEFI: PKE IP4 Intel(R) Ethernet Connection X722 for 106BASE-T UEFI: FKE IP4 Intel(R) Ethernet Connection X722 for 106BASE-T Ver. 2,21.1277 Copyright (C) 2020 American Megat	+*: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F2: Previous Values F2: Previous Values F4: Save a Exlt ESC: Exlt
Step_7	Choose the PXE option desired.	Aptio Setup - American Megathends Inte < Security Boot Save & Exit Restore User Defaults Boot Overnide CentOS (P4: SANSUNG NZTMOABDHARM-00003) UEFI: Pariot Memory PMAP, Fartition 1 UEFI: Built-in FFI Shell AMI Virtual CORONO 1.00 SATAO P5: INTEL SSDSCkR24008 Generic UITRA HS-SD 1 Patriot Memory PMAP AMI Virtual HOjsko 1.00 Generic UITRA HS-SD 0 UEFI: PKE IP4 Intel(R) Ethernet Connection WZ22 for 10GBASE-T Ver. 2.21.1277 Copyright (0) 2020 American Megat	++: Select Screen 1: Select Item Enter: Select 4/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Soptimized Defaults F4: Select Exit

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

Completing operating system installation

Installing an OS on a server using a USB storage device

Relevant sections:

- <u>Accessing the BIOS</u>
- Platform power management

Preparing the USB storage device

Step_1	Create a bootable USB key using the app	propriate 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/E	e 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: serialspeed=115200 terminal_input serial terminal_output serial	<pre>serialspeed=15200 terminal_input serial terminal_output serial set default="1" function load_video { insmod efi_gop insmod vide_bochs insmod vide_bochs insmod vide_bochs insmod vide_cirrus insmod vide_lirus insmod vide_dirus insmod vide_lirus insmod vide_lirus </pre>	
Step_6	In the " <i>Test this media & install</i> <i>CentOS 7</i> " entry replace the " <i>quiet</i> " argument with " <i>console=ttyS0,115200n81</i> ".	<pre>// ## MEDIF /etc/grah.d/12_line# ### // ## MEDIF /etc/grah.d/12_line# ### // ## MEDIF /etc/grah.d/12_line# ### // ##############################</pre>	
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_2	Access the BIOS setup menu. Refer to Accessing the BIOS.	Aptio Setup Utili Main Advanced Intel 7 BIOS Information DIOS Vendor Core Version Core Version Project Version Build Date and Time Access Level FFOA Version Hemory Information Total Memory System Language System Date System Time	y - Copyright (c) 2019 Am ECSetup Server Numt Sec American Regatrends 5.14 UEFT 2.6; FT 1.4 Hill00 2.10.0932F591 x64 04/04/2019 16:17:30 Administrator 2.02.0800AD12 32768 MB [Reglash] [Ved 06/26/2019] [20:13:00]	cfican Negatrends, Inc. uity Boot Event Logs : (Choose the system [default language])) ><: Select Screen [Inter: Select Item [Inter: Select Item]
Step_4	Navigate to the Save & Exit menu and then to the Boot Override section.	Save & Exit Default Options Restore Defaults Sove as User Defaults Sove as User Defaults Sove as User Defaults Restore User Defaults NIT Witches MIT Witches MIT Witches MIT Vitches Door Overlide Door Overlide MIT MIT Store Overlide	0 0 0 0 11	<pre></pre>
Step_5	Choose your USB storage device. NOTE: The USB storage device should be named like this: " <i>UEFI: myUSBname, Partition X</i> ".	Save & Exit Save as User Defaults Restore User Defaults Restore User Defaults ANTFNUdate ANTFNUdate ANT Virtual CORMX 1.0 ANT Virtual CORMX 1.0 ANT Virtual CORMX 1.0 ANT Virtual CORMX 1.0 PO: TS32VSAMMOSTKO UEFI: Built-in EFI She IBA KE SID: 0400 v358 IBA KE SI	0 0 0 11 11 eler 3.0PMAP eler 3.0PMAP. Partition 2	A + + + + + + + + + + + + + + + + + + +

Completing operating system installation

step_r complete the installation by rollowing the on selectific on the specific oscillation.	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 <u>Accessing the BIOS</u> 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 .	Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Advanced
		USB Configuration Enables L/O port 607/54h emulation USB Module Version 21 USB Controllers: USB Controllers: 1 XHCI USB Devices: 4 Drives, 1 Keyboard, 1 Mouse, 3 Hubs
		Legacy USB Support [Enabled] XHOI Hand-off [Enabled] USB Mass Storage Enabled] T1: Select Trem Port 50%E Building Enabled Port 50%E Building Port 50
Step_2	Press F4 to save and exit.	Use transfer time-out [20 sec] Version 2.20.1276. Copyright (C) 2019 American Megstrends, Inc.

Installing RHEL/CentOS 7.3 and preparing for AST driver installation

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	Install CentOS 7 Test this modul & install CentOS 7 Troubleshooting> Use the ★ and ▼ keys to change the selection. Fress 'a' to edit the selected item, or 'c' for a command prompt.	
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.	setparams 'install Cent08 7' linuefi /images/pxeboot/wilinuz inst.stage2=hd:LABEL=CENT0S\x207\x20X\ 0 modprob.blacklist=ast uplet initrdefi /images/pxeboot/initrd.img Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to discard edits and return to the menu. Pressing Tab lists possible completions.	
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.	CentOS Linux (3.10.0-514.25.2.e17.X85_64) 7 (Core) CentOS Linux (3.10.0-514.e17.X85_64) 7 (Core) CentOS Linux (0-rescue-594207ba9f214ae59450cd7a8f5f46e6) 7 (Core)	
		Use the \star and \bullet keys to change the selection. Press 'e' to edit the selected item, or 'c' for a command prompt.	
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.	<pre>load_video set gropuloadsteep insmod gelo insmod gelo insmod part_got insmod ys if [xsfeaturs_Dlafform_search_hint = xy]: then search =-no-floppyfs-uuldseteroot 74cb8a8d-1917-4496-b8e0-e374 eccf2a8d else eccf2a8d eccf2a9d search =-no-floppyfs-uuldseteroot 74cb8a8d-1917-4496-b8e0-e374 linuxef1 /vmlinuz-5.10.0-514.26.2.e17.x86.54 roots/dev/mapper/c1-root linuxef1 /vmlinuz-5.10.0-514.26.2.e17.x86.54 roots/dev/mapper/c1-root Noisen_US.UTF-8 2 Press Ctrl=x to start, Ctrl=c for a command prompt or Escape to dicard edits and return to the menu. Pressing Tab lists possible completions.</pre>	
Step_7	Press CTRL+X or F10 to boot the OS.		

Installing the AST driver

Relevant links:

The driver package can be downloaded from: <u>https://www.aspeedtech.com/support.php</u>

The AST driver package version used in this procedure is: <u>http://upload.aspeedtech.com/BIOS/v11003_linux.zip</u>

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 <u>https://downloadmirror.intel.com/29072/eng/ASPEED_v11003_linux.zip</u>	
Step_2	LocalServer_OSPrompt:~# unzip ASPEED_v11003_linux.zip	
Step_3		
Step_4	Extract the content. LocalServer_OSPrompt:~# tar xvzf lxdrm.tar.gz	
Step_5	Install the driver. LocalServer_OSPrompt:~#./auto-update.sh The architecture is xd6 (4) Check Frevious Installation Package Install Rackage Ready and Please Recot System!	
Step_6	Reboot the platform. LocalServer_OSPrompt:~# reboot	
Step_7	<pre>(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</pre>	
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 -ncrandom-file /root/.bashrccontent-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 CoalServer_OSPrompt:-#make install CoalServer_OSPr
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</eot>
	[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, t	then access the OS command prompt.
Step_2	LocalServer_OSPrompt:~# dmesg LocalServer_OSPrompt:~# dmesg LocalServer_OSPrompt:~# dmesg LocalServer_OSPrompt:~# dmesg	g grep -i Error g grep -i Warning
Step_3	Verify that the DIMMs are detected. LocalServer_OSPrompt:~# free -h	[root@localhost -]# free -h total used free shared-buff/cache-available Mem: 156 460M 14G 18M 273M 14G Swap: 7.7G 08 7.7G
Step_4	Verify that all the storage devices are detected. LocalServer_OSPrompt:~# lsblk	<pre>[root@localhost ~]# lsblk NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT nvmeOn1 259:0 0 238.56 0 disk -nvmeOnlp1 259:1 0 200M 0 part /boot/efi -nvmeOnlp2 259:2 0 1G 0 part -nvmeOnlp3 259:3 0 200M 0 part /boot -nvmeOnlp4 259:4 0 237.1G 0 part -centos00-root 253:0 0 50G 0 lvm / -centos00-swap 253:1 0 7.7G 0 lvm [SwAP] -centos00-swap 253:2 0 179.4G 0 lvm /home nvmeInlp1 259:5 0 477G 0 disk -nvmeInlp2 259:7 0 476G 0 part -centos-swap 253:3 0 7.7G 0 lvm -centos-swap 253:3 0 7.7G 0 lvm -centos-swap 253:3 0 7.7G 0 lvm</pre>
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.	1895259.7762431 [40e 0000:1a:00.0 end]: NIC Link is Up. 10 Gbps Fall Duplex, Flow Control: None 195359.7762021 [40e 0000:1a:00.1 end2: NIC Link is Up. 10 Gbps Fall Duplex, Flow Control: None
Step_6	Confirm that all the network interfaces are detected. LocalServer_OSPrompt:~# ip address NOTE: You should see two NIC interfaces.	<pre>[fcocklocklock-if ip defress 11 lot (LOCMENC, UP_LOWER, UP ment 45334 gpiint nogene state DWENOME group default gien 1000 11 met 127.00 //4 scope host 10 http://output/score/ imet 127.00 //4 scope host 10 http://output/score/ imet 127.00 //4 scope host 10 http://output/score/ imed 127.01 scope host 10 http://output/score/ imed 127.01 scope host 10 http://output/score/ imed 127.01 http://output/score/ tem/score/score/score/score/ imed/score/score/score/score/ imed/score/score/score/score/ imed/score/score/score/score/ imed/score/score/score/ imed/score/score/score/score/ wild iff forewer preferred iff forewer wild iff forewer preferred iff forewer score/score/score/score/score/ wild iff forewer preferred iff forewer score/score/score/score/score/ wild iff forewer preferred iff forewer score/score/score/score/score/score/ wild iff forewer preferred iff forewer score/score/score/score/score/score/ wild iff forewer preferred iff forewer score/score/score/score/score/score/score/score/score/ score/s</pre>
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.	Image: Control of the second secon
Step_8	Install ipmitool and pciutils usin ipmitool version recommended is Example: LocalServer_OSPrompt:~ # yum u LocalServer_OSPrompt:~ # yum ir LocalServer_OSPrompt:~ # yum ir	pdate Istall ipmitool
	NOTE: Updating the packages ma	ıy take a few minutes.
Step_9	(Optional) If PCIe add-in cards or other hardware components are installed, verify that they	[rootBlocalhost -]# lspci 00:00.0 Host bridge: Intel Corporation Sky Lake-E DMI3 Registers (rev 06) 00:04.0 System peripheral: Intel Corporation Sky Lake-E CBDMA Registers (rev 06) 00:04.1 System peripheral: Intel Corporation Sky Lake-E CBDMA Registers (rev 06) 00:04.2 System peripheral: Intel Corporation Sky Lake-E CBDMA Registers (rev 06) 00:04.3 System peripheral: Intel Corporation Sky Lake-E CBDMA Registers (rev 06) 00:04.3 System peripheral: Intel Corporation Sky Lake-E CBDMA Registers (rev 06) 00:04.4 System peripheral: Intel Corporation Sky Lake-E CBDMA Registers (rev 06) 00:04.5 System peripheral: Intel Corporation Sky Lake-E CBDMA Registers (rev 06)
		www.kontron.com

	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.	00:04.7 system peripheral: riflet curporation sky Lake-E camba Register's (rev 06) 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 SEL Device FRU Inventory Device 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

- <u>Required software tools</u>
- Recommended software tools
- Product specific software tools



Commands may vary depending on the OS and the package manager.

Some tools may not be required depending on the functionalities supported for the platform.

Required software tools

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:	
ksnmpd	Kontron Linux sub-agent.	LocalServer_OSPrompt:~# yum install ./ kontron-snmp-agent- 1.2.2-1.x86_64.rpm NOTE: This software is provided by Kontron.	
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 <u>StorCLI utility</u>
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

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

Configuration of system access methods

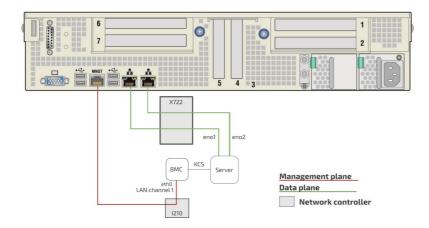
(This article provides detailed setup instructions to enable system access for all available methods.) Table of contents

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

General considerations and warnings about network configuration

The architecture of the CG2400 platform offers many entry points, including one LAN channel to the BMC.

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



Disabling IOL on a LAN channel

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

Using [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 langlus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password].

Step_1	Disable the LAN access. LocalServer_OSPrompt:~# ipmitool lan set [LAN_CHANNEL] access off	[root@localhost ~]# ipmitool lan set 1 access off Set Channel Access for channel 1 was successful.
--------	---	---

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 langlus -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	[root0localhost ~]# ipmitool lan set 1 access on Set Channel Access for channel 1 was successful.
--------	---	--

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 langlus -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	\$ ipnitedl sol info Set in progress : set-complete Enabled : true Force Encryption : full Force Encryption : full Force Encryption : full Force Encryption : AMPLIERTROTE Character Accumulate Level (ms) : 60 Character Send Threshold : 96 Retry Interval Ret : 150 Retry Interval Ret (bps) : 115.2 Non-Volatile Bit Rate (bps) : 115.2 Non-Volatile Bit Rate (bps) : 115.2 Payload Port : 623
Step_2	Display SOL parameters available for configuration. LocalServer_OSPrompt:~# ipmitool sol set	I ipritor loo set 50. set parameters and values: set-in-progress set-complete set-in-progress commit-write enabled true false force-encryption rel false privilge-level very label character-acomplete/set character-acomplete/set character-acomplete/set character-acomplete/set character-acomplete/set character-acomplete/set character-acomplete/set character-acomplete/set character-acomplete/set set and set and set and set and set and set and menoralistic-set a serial 36 (15:2 36:4 57:6 115:2 menoralistic-set a serial 36 (15:2 36:4 57:6 115:2 36:4 57:6 115:2 menoralistic-set a serial 36 (15:2 36:4 57:6 115:2 36:4 57:6 115:2 menoralistic-set a serial 36 (15:2 36:4 57:6 115:2 57:6 115:2 57:6 115:2 57:6 115:2 57:6 115:2 57:6 115:2 57:6 115:2 57:6 115:2 57:6 115:2 57:6 115:2 57:6 115:2 57:6 115:2 57:6 115:2 57:6 115:2 57:6 115:2 57:6 115:2 57:6 115:2 57:6 115:2
Step_3	Set the desired parameters. LocalServer_OSPrompt:~# ipmitool sol set [PARAMETER] [PARAMETER_VALUE] [LAN_CHANNEL]	\$ ipmitool solset non-volatile-bit-rate 115.2 1

Creating the Redfish root URL

Prerequisites

Default user names and passwords

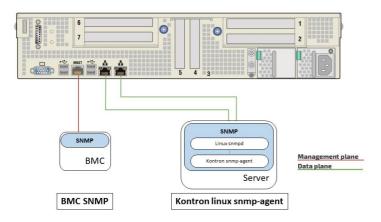
1	The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).	
2	An HTTP client tool is installed on the remote computer.	
3	A JSON parsor command-line tool such as jq is installed.	
Relevant sections: Baseboard management controller - BMC Common software installation		

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 $\underline{\mathbf{e}}$ 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.	<pre>\$ curl -k -s https://Administrator:superus%er&172.16.205.245/redfish/v1/ {"Godata.context":*/redfish/v1/setadataServiceRoot", "Godata.teg": `W/~15536478(", "Godata.id":/redfish/v1/~redfish/v1/AccountService", "Chass is:{"Godata.id":/redfish/v1/Setasis", "CompositionService";{"Godata.teg": `h/v1/CompositionService", "Boata.id":/redfish/v1/AccountService", "Chass is:{"Godata.id":/redfish/v1/Setasis", "CompositionService", "Chass is:{"Godata.id":/redfish/v1/Setasis", "CompositionService", "Chass is:{"Godata.id":/redfish/v1/Setasis", "CompositionService", "Chass is:{"Godata.id":/redfish/v1/Setasis", "CompositionService", "Chass is:", "SonSchemas", "Boata.id":/redfish/v1/SonSchemas", "Links", "Se ssions" '[Godata.id":/redfish/v1/SetasionService", "Godata .id"://redfish/v1/Managers", "Name": "Koot Service", "Gom::{"Mai":!"Godata.id":/redfish/v1 /Configurations', "RtpVersion":1.2.1", "Der::{"Godata.id":/redfish/v1/Jona micExtension"}], "RtpVersion":1.2.1", "Registries", "Godata.id":/redfish/v1/Jona st["Godata.id":/redfish/v1/Systems'], "Tasks";["Godata.id":/redfish/v1/Jona micExtension"]], "RedfishVersion":1.2.1", "Registries", "Godata.id":/redfish/v1/Jona micExtension", "Systems', "Tasks";["Godata.id":/redfish/v1/Jona micExtensionScience:", "Godata.id":/redfish/v1/Jona micExtensionScience:", "Godata.id":/redfish/v1/Jona micExtensionScience:", "Godata.id":/redfish/v1/Jona micExtensionScience:", "Godata.id":/redfish/v1/Jona micExtensionScience:", "Systems', "Tasks":["Godata.id":/redfish/v1/Taskse rvice:", "TelemetryService:", "Godata.id":/redfish/v1/Taskse rvice:", "TelemetryService:", "Godata.id":/redfish/v1/TelemetryService:", "Godata.id":", "redfish/v1</pre>

*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 <u>Accessing a BMC using the Web UI</u> for access instructions.

Step_1	From the left menu, click on Settings and then User Management.	Image: State
Step_2	Select the user.	User Management # Home - Meeting - User Homegment Channel 1 Image: Channel 1 1 and provide a statistic of the provide a statistic of th
Step_3	Click on the SNMP Access checkbox to give the user an SNMP access.	Privilege(Channel 1) Administrator Privilege(Channel 2) Administrator Privilege(Channel 8) Administrator
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.	VMM Access VMedia Access SIMIP Access SIMIP Access SIMIP Access level Read Write SIMIP Access level SIMIP Authentication Protocol SIMIP Privacy Protocol DES
Step_5	Choose the SNMP Authentification Protocol .	
Step_6	Choose the SNMP Privacy Protocol .	
Step_7	Click on Save .	Uplead SSH Key

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: <pre>/etc/snmp/snmp.conf [-H] 0 L: [+ 0 1/ 1] * (0 / 510b) 35 0x023 <pre># 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 # rousing them by commenting out the following line. # 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/ietf</pre></pre>

Verifying SNMP communication for a user



Disabling an SNMP access

Refer to <u>Accessing a BMC using the Web UI</u> for access instructions.

Step_1	Access the BMC	WebIII	
Step_2	From the left menu, click on Settings and then User Management.		Image: Section of the section of t
Step_3	Select the user.	User Management Tanent Tanent Tanent Tanent Tanent Tanent Channel 1 Control Channel	Image: String:
Step_4	Click on the SNMP Access checkbox to disable the SNMP access of the user selected.	KVM Access VMedia Access SMMP Access SMMP Access SMMP Access SMMP Access SMMP Authentication Protocol SMA SMMP Privacy Protocol DES	
Step_5	Click on Save .	Upload SSH Key	Bi 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 <u>Accessing the operating system of a server</u> 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



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.con	f.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-configcreate-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 <u>Configuring and</u> managing users for more instructions.	<pre>[rost9localhost -]# /usr/bin/net-snmp-configcreate-snmpv3-user adding the following line to /usr/lib/net-snmp/snmpd.conf: createdom initial-user boots "my-onservation" (B.S. adding the following line to /utc/snmp/snmpd.conf; maker initial-user</pre>

Running the Kontron linux snmp-agent and verifying installation and configuration

Step_1	Run snmpd. LocalServer_OSPrompt:~# service snmpd start	[root@localhost ~]# service snmpd start Redirecting to /bin/ <u>s</u> ystemctl start snmpd.service
Step_2	Verify that snmpd is running properly. LocalServer_OSPrompt:~# service snmpd status	FordetBlock Hunch - THE screenfor sample fichting Boltrecht 196 (or Alsongerhert Leikan: sample screenfor sample screenfor - Simple Returk Knospennet Protocol (3092) Baeson. Londef: Londef Converliveyscreensing the symple screenfor (linkbid: vendor preset: disabled) facture: active (remain) since The 2019-10-17 15:31:29 (6T: 5min app http://doi.org/10.1000/000000000000000000000000000000
Step_3	(Optional) If there are some issues with one mechanism. Refer to [Content under creation	or both services, it might be due to the SELinux security n] Disabling SELinux for further instructions.
Step_4	Run ksnmpd. LocalServer_OSPrompt:~# service ksnmpd start	[root@localhost ~]# service ksnmpd start Redirecting to /bin/ <u>s</u> ystemctl start ksnmpd.service
Step_5	Verify that ksnmpd is running properly. LocalServer_OSPrompt:~# service ksnmpd status	[rostBlocalboxt "]H service knowed status Beiresting to Ahrwyteneti status benepiservice Isaderi isadei (victo-zyntechnychetekwise) archivice mablet; ventor preset; disabled) Active: active framing) since The 2019-18-75 JS:13177 ACT: Sain ago Process: 202 ExeCitart-curv.rol.knowed/ahrwide/ahrwide/aktivempagent (Brung). // Unsequent) Ghrung // Active framing archive active active active active active Ghrung // Active framing archive active active active Laboration active framing archive active active active active active Ghrung // Active framing archive active active active active active Laborative active active active active active active active active active active Laborative active ac
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]	<pre>codgeneteror/# compatite * 1 < pails = A (cord local locge/shift).Compd will include enterprise:15000 contino-istrute.indlobation systemmagementind/orseitstanulatin = A = HTGBE: include complete include include includ</pre>
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]	<pre>6 mmovallop 1 mvsHodpire -= initial_user -= http://parsword 172.16.150.216 WorThous Structs-AddEndabits temps nature to deve hale WorThous Structs-AddEndabits temps nature to deve hale WorThous Structs-AddEndabits temps nature to deve in the INTEGRE 1 WorThous Structs-AddEndabits temps nature to deve in the INTEGRE 2 WorThous Structs-AddEndabits temps nature to deve in the INTEGRE 3 WorThous Structs-AddEndabits temps nature to deve in the INTEGRE 4 WorThous Structs-AddEndabits temps nature to deve in the INTEGRE 4 WorThous Structs-AddEndabits temps nature index, = INTEGRE 4 WorThous Structs-AddEndabits temps nature index, = INTEGRE 7 WorThous Structs-AddEndabits temps nature index, = INTEGRE 7 WorThous Structs-AddEndabits temps nature index, = INTEGRE 10 WorThous-Structs-AddEndabits temps nature index, = INTEGRE 10 WorThous-Structs-AddEndabits temps nature index, = INTEGRE 10 WorThous-Structs-AddEndabits temps nature index, 12 = INTEGRE 10 WorThous-Structs-AddEndabits temps nature index, 12 = INTEGRE 12</pre>

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.

<i>.</i>		GNU nano 2.3.1 File: /etc/selinux/config Modified
Step_1	Open the SELinux configuration file with any text editor. LocalServer_OSPrompt:~# nano /etc/selinux/config	This file controls the state of SELinux on the system. SELINUX- can take one of these three values: SELINUX-can take one of these three values: permission - SELinux points warnings instead of enforcing. # disable - ho SELinux points userings instead of enforcing. SELINUX-File an take one of three taw values: targeted - Targeted processes are protected, m sign = Nill Lacel Security protection. SELINUX-File targeted protection. SELINUX-File targeted protection.
Step_2	Modify the file by changing the SELINUX parameter to disabled.	Cold many 2014 Files Selection control (p) Description # This file controls the state of SELinox on the system. # SELINGY can take now of these three values: # SELINGY can take now of these three values: # SELINGY can be state of selection (selection) # SELINGY can be state of selection (selection) # SELINGY can selection (selection) # selection (selection) # SELINGY can be selected of selection (selection) # SELINGY can be selected (selection) # SELINGY can be selected - Targeted processes are protected, # selected - Targeted (selection). # selected processes are protected. # selection - Full (selection) (selection). # selected selection. # selection (selection).
Step_3	Save the changes and reboot the operating system. LocalServer_OSPrompt:~# reboot	froot@localhost "J# 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 -v1 -c public -m /usr/local/ksnmpd/mibs/ksnmpd.mib localhost [MIBS]	<pre>Froot@localhost "lm samparlk -v 1 -c public -m .vsr/local/ksimpd.mibs/ksimpd.mib localhost enterprize.joB00 MarTankerStateLandStateL</pre>
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 - I [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [PASSWORD] [SERVER_IP] [ODI]	<pre>\$ snmpwalk -v 3 -l authNoPriv -u_initial-user -a MD5 -A my-password 172.16.192.123 KONTRON-SERVER-BASEBOARD::temperatureProbeTable SNMPV2-SMI::enterprises.15000.2.10, 3.5,100.1.0 = INTEGER: 1 SNMPV2-SMI::enterprises.15000.2.10, 3.5,100.4.0 = INTEGER: 1 SNMPV2-SMI::enterprises.15000.2.10, 3.5,100.6.0 = INTEGER: 1 SNMPV2-SMI::enterprises.15000.2.10, 3.5,100.6.0 = STRING: "Work" SNMPV2-SMI::enterprises.15000.2.10, 3.5,100.6.0 = STRING: "Work" SNMPV2-SMI::enterprises.15000.2.10, 3.5,100.6.0 = STRING: "Nortroof" SNMPV2-SMI::enterprises.15000.2.10, 3.5,100.8.0 = STRING: "1,2.1,0" SNMPV2-SMI::enterprises.15000.2.10, 3.5,100.8.0 = STRING: "1,2.1,0" SNMPV2-SMI::enterprises.15000.2.10, 3.5,100.8.0 = STRING: "1,2.1,0" SNMPV2-SMI::enterprises.15000.2.10, 3.5,100.8.0 = STRING: "1,2.1,0" SNMPV2-SMI::enterprises.15000.2.10, 3.5,200.8.0 = STRING: "1,2.1,0" SNMPV2-SMI::enterprises.15000.2.10, 3.5,200.8.0 = INTEGER: 3 SNMPV2-SMI::enterprises.15000.2.10, 3.5,200.8.0 = INTEGER: 3</pre>

Configuring and managing users

[This article provides detailed configuration instructions for platform users.] Table of contents

- <u>Configuring BMC users</u>
 - Configuring BMC user names and passwords
 - <u>Adding a BMC user</u>
 - Deleting or disabling a BMC user
 - <u>Configuring privilege level for BMC users</u>
- <u>Configuring SNMP users</u>
 - <u>Configuring SNMP users using BMC SNMP</u>
 - <u>Configuring SNMP users using the Kontron linux snmp-agent</u>
- Managing Redfish users
 - <u>Configuring Redfish user names and passwords</u>
 - Adding a Redfish user
 - Deleting a Redfish user
 - <u>Configuring Redfish privilege level</u>
- <u>Configuring OS users</u>

Configuring BMC users

i

Administrator rights are required to manage users.

Configu ring BMC user names and passwords

For default user names and passwords, refer to <u>Default user names and passwords</u>.

- 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	E & Olios Osyrc Diatrata 1.	admin +
Drep_1	click on User Management .	transition Transition Transition	- Settings
		Storer System howstery Capital SSO D Data Sites Deter Deter Deter Sites Deter Sites Deter Deter S	4
		PT012honuske Ing Strings Holds hefrevise Strings Holds hefrevise Strings Holds hefrevise Strings Holds hefrevise Strings	51
		Suttings Control Result Control Partices Event Filter Instance Suff Suttings Suff Suttings Suff Suttings Suff Suttings	
		A man format Management	
Step_2	Select the user to manage.	E B & 9805 Sign Dinnis Las	imin +
	NOTE: The first and second users are reserved	Branna Marsine Branna Bran	(prosent)
	fields, therefore, their usernames can't be modified.	Possilain. • Cheerel 1 •	0
		Sonar Careel: Convert Sonar Sonar	
		Mit tegek Reports * O conset1 O con	
		Bit Integrations (Cannot) O Prever Cantod	
Step_3	Change field Username if required.	Usename	
		operator	
		Change Password Password Size	
		16 bytes •	
		Password	
		Confirm Password	
Step_4	Check the Change Password box.	Username	
		operator	
		Change Password	
		16 bytes •	

		Password Confirm Password
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.	Username coparator Change Password Password Size 16 bytes Password Confirm Password Confirm Password
Step_6	Confirm the password.	Username operator Change Password Password Size 10 bytes Password Confirm Password
Step_7	Press Save .	Email Format All-Format Email ID Existing SSH Key Not Available Upload SSH Key Device Device Ssev

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 <u>Accessing a BMC using IPMI over LAN</u> 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	\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin user list ID Name Callin Link Auth IPMI Msg Channel Priv Limit 1 false false 2 admin 3 operator 4 true 5 true 6 true 6 true 6 true 6 true 7 true 7 true 7 true 7 true 6 true 6 true 7 true
Step_2	Identify the ID number of the user to be changed.	[_coetBlocalhost -]# ipmited H 192,168,101.26-U admin → P admin user list [TD Name Callin Link Arch IPH Mag Channel Friv Lint Link Arch IPH Mag Channel Friv Lint a dmin false false true AUMINISTRATOR USER true false false NO ACCESS 5 true false false NO ACCESS 6 true false false NO ACCESS 7 true false false NO ACCESS 8 true false false NO ACCESS 9 true false false NO ACCESS
Step_3	Change the user name. RemoteComputer_OSPrompt:~\$ ipmitool -I lanplus -H [name] -P [administrator IPMI password] user set na NOTE: The first and second user names of the user list are	me [IPMI user ID] [new IPMI user name]
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	\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin user list ID Name Callin Link Auth IPMI Msg Channel Priv Limit 1 false false true AdMINISTRATOR 2 admin false false true AdMINISTRATOR 3 operator true false false 4 true false false 5 true false false 6 true false false 7 true false false MOXINSTRATOR 8 true false false NO ACCESS 9 true false false NO ACCESS 10 true false false NO ACCESS
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.	5 ipnttool -I lanplus -H 192.166.101.26 -U admin -P admin user set password 3 newpassword Set User Password command successful (user 3)
		www.kontron.com

	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 [MI user ID]		
Step_7	Configure privilege level. RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H name] -P [administrator IPMI password] channel se [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]	\$ ipmitool -I lamplus -H 19 ID Name Callin 1 false 2 admin false 3 operator false 4 true 6 true 7 true 8 true 9 true 9 true 10 true	2.168.101.2 Link Auth false false false false false false false false false false false	or -P newpassword user list Channel Priv Limit ADMINISTRATOR ADMINISTRATOR NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS
	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]	[rost@localhost ~]# ID Name 1 2 admin 3 user 4 5 6 7 8 9 9 10		l user list Link Auth false false true false false false false false false false		Channel Priv Limit ADMINISTRATOR ADMINISTRATOR ADMINISTRATOR NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS
Step_2	Identify the ID number of the user to be changed.	<pre>(root@localhost ~)# TD Name 1 2 admin 3 user 4 5 6 7 8 9 9 10</pre>	ipmitool Callin false false true true true true true true true tru	l user list Link Auth false false true false false false false false false false false	1 IPHI Msg true true true false false false false false false false	Channel Priv Limit ADMINISTRATOR ADMINISTRATOR ADMINISTRATOR NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS
Step_3	Change the user name. LocalServer_OSPrompt: ~# ipmitool user set NOTE: The first and second user names of the modified.	-	-	-		-
Step_4	Verify that the user name has updated correctly by printing the user list. LocalServer_OSPrompt:~# ipmitool user list [LAN_CHANNEL]	[root@iocalhost -]# 10 Name 2 admin 3 operator 4 5 6 7 0 9 10	Callin false false true true true true true true true tru	Link Auth I false t false t true t false f false f false f false f false f false f	rue à rue à rue à alse N alse N alse N alse N alse N alse N	Thannel Priv Limit DHINISTRATOR UMINISTRATOR DHINISTRATOR DHINISTRATOR DHINISTRATOR DHINISTRATOR DO ACCESS DO ACCESS DO ACCESS DO ACCESS DO ACCESS
Step_5	Change the password. LocalServer_OSPrompt: ~# ipmitool user set password [IPMI user ID] [new IPMI password]	[root@localhost Set User Passwor				sword 3 newpassword ; 3)
Step_6	Verify that the credentials updated correctly b NOTE: Other parameters could limit the acces Refer to ipmitool documentation.	, 0				0

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

1

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.	Set
Step_2	Click on Settings in the left side menu and click on User Management .	A and a field of the series A and a field of the ser
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.	Openel: Openel: <t< td=""></t<>
Step_4	Configure the user according to the application's requirements. NOTE: Refer to <u>Configuring privilege</u> <u>level for BMC users using the Web UI</u> for further instructions on privilege level.	User Management Configuration
Step_5	Enable the user on the desired channel(s).	Enable User Access Channel 1 Channel 2
Step_6	Press Save to exit.	Enail ID Existing SH Key NG Available Upload SSH Key

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	<pre># ignitool -I lanp ID Name 1 2 admin 3 4 5 6 7 8 9 10</pre>	Callin false false true true true true true true true	Link Auth false false false false false false false false false false	-U admin IPMI Msg true true false false false false false false false false	P admin user list Channel Pirv Limit ADMINISTRATOR ADMINISTRATOR NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS
Step_2	Create a user name. RemoteServer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGM" [administrator IPMI password] user set name [IPMI user ID] [NOTE: The first and second user names of the user list are reserved	new IPMI user	name]			ne] -P
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]	[root@localhost ~]# ↓ Name 2 admin 3 4 5 6 7 8 9 10	ipmitool user 1: Calin Link A false false false false true false true false true false true false true false true false true false true false		Channel Priv Limit AbHINISTRATOR ADHINISTRATOR NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS		
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.	Ansatz de la construir de	A 20050 eesti	16 Arous Laga Merror Monitoring	
Step_2	Click on Settings in the left side menu and click on User Management .	Arrore Contraction Contr	Dest train Dest train Wate Networks Worky Units Dest Train Dest Train De	Deve de transit Deve de transit Martin Alerge Ser França	A BOX SOM ALMONICATION
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.	Dravel: Language Language Language Mill: Statistics	Carrel 1 2 Jamin (2) Arrist Stress (2) Arrist Stress (2) Arrist Stress (2) Arrist Stress (2) Arrist Arrist Stress (2) Arrist Arrist Arrist Browned	-	Daniel chined viniel

Existing SSH Key	
Not Available	
Upload SSH Key	
	b
Delete	🖺 Save

Disabling a BMC user using IPMI over LAN (IOL)

Users can't be deleted using **ipmitool** . However, they can disabled. Refer to <u>Accessing a BMC using IPMI over LAN</u> 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	ID Na 1	imin		user list Link Auth false false false false false false false false false false false	1 IPMI Msg true false false false false false false false false false	Channel Priv Limit ADMINISTRATOR ADMINISTRATOR NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS		
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 <u>Accessing a BMC using IPMI (KCS)</u> 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]	[root@iocalhost ~]# TD Name 1 2 admin 3 4 5 6 7 8 9 10	user list Link Auth false false false false false false false false false false	Channel Priv Limit ADMINISTRATOR ADMINISTRATOR NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS
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	e 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 <u>Accessing a BMC using the Web UI</u> for access instructions.

Step_1	Access the BMC Web UI of the server.		A Oracle Street Charles A
Step_2	Click on Settings in the left side menu and click on User Management .	Image: Second	A A BOO TOP DATA AND
Step_3	Select the ID of the user to manage.	A Constitution Merror and Constitution Merro	Ovaval 1 4,00actived

	NOTE: The first and second users are reserved fields and therefore can't be overwritten.	Internation Description Operation Op
Step_4	Configure the privilege level for each channel according to the application's requirements.	Privilege(Channel 1) Administrator Privilege(Channel 2) Administrator
Step_5	Press on Save to exit.	Email ID Existing SSH Key Not Available Upload SSH Key

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	[root[]localhost -]# 10 Name 2 admin 3 admin 4 6 6 7 8 9 10 10 10 10 10 10 10 10 10 10		user list Link Auth false false false false false false false false false false		Channel Priv Limit ADMINISTRATOR ADMINISTRATOR NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS		
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	<pre>Shannel Commands: setting: cohamel number; mar privileged setting:</pre>						
	Step_3	Set privilege level for each channel. RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC [administrator IPMI password] channel setaccess [LAN_ NOTE: The first and second user names of the user list are rese	CHANNEL] [USER	_ID] pr	ivilege=	[PRIVILE	-		

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]	[root@localhost -]. TD Name 2 achin 3 4 5 6 8 9 10		user list Link Auth false false false false false false false false false false false		Channel Priv Limit ADMINISTRATOR ADMINISTRATOR NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS NO ACCESS	
Step_2	List the privilege levels available. LocalServer_OSPrompt:~# ipmitool channel help	<pre>damasi Command : esthong command in markers and the status indexes (intro [intro [intro</pre>					
Step_3	ep_3 Set the privilege level for each channel. LocalServer_OSPrompt:~# ipmitool channel setaccess [LAN_CHANNEL] [USER_ID] privilege=[PRIVILEGE_LEVEL NOTE: The first and second user names of the user list are reserved fields and therefore can't be modified.						

Configuring SNMP users

Relevant sections: Accessing a BMC using SNMP BMC Accessing a BMC using the Kontron linux snmp-agent

Configuring SNMP users using BMC SNMP

BMC SNMP users are shared with BMC users.

- To configure a user, refer to [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 <u>Accessing a BMC using the Kontron linux snmp-agent</u> 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]	\$ snmusm -v3 -l authNoPriv -u initial-user -a ND5 -A my-password -x DES 172.16.210.149 passwd my-password new-password operator SMMPv3 Key(s) successfully changed.
--------	---	--

Adding an SNMP user

Refer to <u>Accessing a BMC using the Kontron linux snmp-agent</u> 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]	\$ snmpusm -v3 -1 authNoPriv -u initial-user -a MD5 -A my-password 172.16.210.149 create operator User successfully created.
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]	S snmpusm -v3 -l authNoPriv -u initial-user -a MD5 -A my-password 172.16.210.149 cloneFrom operator initial-user User successfully cloned.

Deleting an SNMP user

Refer to <u>Accessing a BMC using the Kontron linux snmp-agent</u> 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	<pre>col 1 = 4 MINING/Addition/Development/PL/11/2014/ord/Addition/MARCHARMENTER/ENDERLE 1 34 Mining contexty 1 = 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,</pre>
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	<pre>set1 - 4 - 9 Mutah://doi.not.org/comments/13.13.33.43/methab/std/standstorid/Research/1 j1 "Additional additional additionadditional additional additional additional additional add</pre>
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	3 см ⁻¹ - к - к Нтда //Амтіпістатог ізареникенії 12.16.206.346/redfish/v4/AccountService/ AccountS/A - х НбЗО - і егер ГТад
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.	1, eu-h 4-s Miter//Aministrator inproved12.12,122,223,237,241,547,1657,1650,2457,47 Constrat, 7, 97,167,167 ("Deptember ModerBack") - 4"Tf-Antoi W"13130977" - 4 "Content-type: application/jum" j
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	f orl -i -s https://weitsetweetspervaet027.16.205.245/reifftsh/d/AccountServier/ counts/1_2_KEGO-i grop Elag Elag: M/156494139*
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.	3 col-3, -1 http://doinistratoringenue817.16.30.30/reffish/s/Acoustiervice/ Content-toper.apyletics/file/1/acoustiervice/ Content-toper.apyletics/file/1/a
Step_7	Verify that the credentials updated correctly by opening a r	new session in the Redfish API.

Adding a Redfish user

Refer to <u>Accessing a BMC using Redfish</u> for access instructions.

Step_1	Append the Root URL with the AccountService/Accounts suffix. RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts jq	<pre>1 cr 1 - 1 - 1 - 3 http://doi.org/1 / 2.1.200.2017.07 http://doi.org/10.1111/2017.07 http://doi.org/10.11111/2017.07 http://doi.org/10.111111/2017.07 http://doi.org/10.111111/2017.07 http://doi.org/10.11111111111111111111111111111111111</pre>
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.	<pre>Sign of Sign of S</pre>
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	<pre>\$ curl -k -s https://Administrator:superuse#3122.16.205.245/redFish/v1 /AccountService/Accounts/6 -X HEAD -i grep ETag ETag: W/"1564427308"</pre>
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	<pre>\$ curl -s -k https://Administrator:superuser8172.16.205.245/redfish/vL /AccountService/Accounts.6 -X PATCH -d "("Enabled":true)" +H 'If-Match: W/"1564427308" -H 'Content-type: application/json' jq</pre>
Step_5	Verify that the user was created correctly by connecting to Redfish using its credentials.	

Deleting a Redfish user

Refer to <u>Accessing a BMC using Redfish</u> 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	<pre>1 cm² = 4. http://doinitration.com/energine.lib/ord/lib/ord/com/fib/ord/com/fib/ord/com/fib//</pre>
Step_2	Delete the user. RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts/[USER_ID] -X DELETE jq	<pre>\$ curl -s -k https://Administrator:superuser0172.16.205.245/redfish/v1 /AccountService/Accounts/7 -X DELETE jq</pre>
Step_3	Verify that the user has been deleted properly. RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts jq	<pre>1 av1 - 1 http://doititr.twice.ispercentR02.14.305.304/reff.hbv1/AccountSorvice/Accounts] pt</pre>

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 <u>Accessing a BMC using Redfish</u> 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	<pre>1 expl vs A https://doinvist.ntr.superareRX7.11.107.145/redf/hdv/iAccountervie/Accountil] sp Profile control ", "control vs (red) from the superare accounts of the time memory accounts of the time", "books in the "profile", "control vs (red) from the superare accounts of the time", "books interview", "control vs (red) from the superare accounts of the time", "books interview", "control vs (red) from the superare accounts of the time", "books interview", "control vs (red) from the superare accounts of the time", "books interview", "control vs (red) from the superare accounts of the time", "books interview", "control vs (red) from the superare accounts of the time", "books interview", "control vs (red) from the superare accounts of the time", "books interview", "control vs (red) from the superare accounts of the time", "books interview", "control vs (red) from the superare accounts of the time", "books interview", "control vs (red) from the superare accounts of the time", "books interview", "control vs (red) from the superare accounts of the time", "books interview", "control vs (red) from the superare accounts of the time", "books interview", "control vs (red) from the superare accounts of the time", "books interview", "control vs (red) from the superare accounts of the time", "books interview", "control vs (red) from the superare accounts of the time", "books interview", "control vs (red) from the superare accounts of the time", "books interview", "books interview,</pre>
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	S curl -k -s https://Administrator:superuser0172.16.205.245/redfish/v1 /AccountSevvice/Accounts/8 -X HEAD -i grep ETag ETag: W/"1564431523"
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	<pre>\$ curl -k -s https://Administratorisuperuse#3172.16.205.245/redfjsh/v1 /AccountService/Accounts/8 -X PATCH -d '("RoleId":"Administrator")' -H 'IF-Match: W/'IS64431523'' -H 'Content-type: application/json' jq</pre>
Step_4	Verify that the RoleID has updated properly. RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]AccountService/Accounts/[USER_ID] jq	<pre>set '1' - 1 Migs://doi/sit/set/ar/set/a</pre>

Configuring OS users

Refer to <u>Accessing the operating system of a server</u> 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.

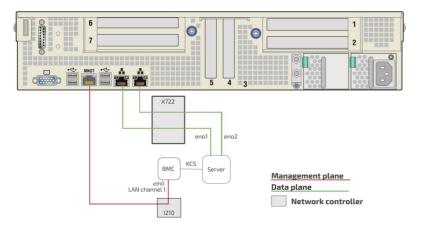
Baseboard management controller - BMC

[This article provides detailed setup instructions for all BMC configuration methods.] Table of contents

<u>BMC architecture</u>

- Selecting an access method
- Discovering the platform management IP address
 - Discovering the platform management IP address with DHCP Dynamic DNS update
 - <u>Discovering the platform management IP address using the BIOS</u>
 - Discovering the management IP address in the BIOS using the VGA display port
 - Discovering the management IP address in the BIOS using a serial console (physical connection)
 - Discovering the platform management IP address using DHCP server logs
- <u>Configuring a static IP address</u>
 - <u>Configuring a static IP address using the BIOS setup menu</u>
 - <u>Accessing the BIOS setup menu</u>
 - <u>Accessing the BMC network configuration menu</u>
 - <u>Configuring a static IP address</u>
 - <u>Configuring a static IP address using IPMI</u>
 - <u>Accessing the BMC</u>
 - <u>Configuring a static IP address</u>
- <u>Configuring a dynamic IP address using DHCP</u>
 - <u>Configuring a dynamic IP address using the BIOS setup menu</u>
 - <u>Accessing the BIOS setup menu</u>
 - <u>Accessing the BMC network configuration menu</u>
 - <u>Configuring a dynamic IP address using DHCP</u>
 - <u>Configuring a dynamic IP address using IPMI</u>
 - <u>Accessing the BMC</u>
 - Configuring a dynamic IP address

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 <u>Product architecture</u> 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-IX5100_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_00A0ASD2E90A[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:

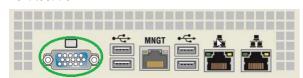
- Using the [Content under creation] VGA display port (physical connection)
- Using a serial console (physical connection)

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

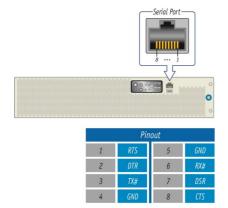
Step_1	From the UEFI/BIOS menu, navigate to tab Server Mgmt .	Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Main Advanced IntelRCSetup Server Mumt Security Boot Zvent Logs
		BIOS Information Ichoose the system BIOS Mendor American Repartends Ichoose the system Core Version 5.14 Ichoose the system Core Version 5.14 Ichoose the system Project Version 0.12.65 Pl 1.4 Ichoose the system Project Version 06/28/2019 09:12:28 Ichoose the system Build base and Tume 06/28/2019 09:12:28 Ichoose the system
		FPGA Version 2.02.0800AD12 Memory Information 1 << sheet Stream Total Remory 32766 HB Total Remory 1 /< : Change Opt. System Language (English) System The [104 07/10/2019] System The [134774] System The [134774] Version 2.20.4271. Copyright (5) 2019 American Megatiends, Inc.
Step_2	Select BMC network configuration .	Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Main Advanced IncelRCSetup Server Nyme Security Soot Event Logs
		BKC Interface(s) KCS, USB / Frees Chiter> to enable Wait For ENC [Dismbled] + configuration. FRB-2 Timer Inter [Family [Four Cycle] + FRB-2 Timer Timer [Dismbled] + CO Watchdog Timer [Dismbled] + System Event Log + > Vise System Event Log + > Vise System Event Log + > Watch System Event Log +
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.	Aptic Setup Utility - Copyright (c) 2018 American Megatrends, Inc. Server Name BRC network configuration ***********************************

Discovering the management IP address in the BIOS using a s erial console (physical connection)

Prerequisites

	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.	Description Optimizer Local State State Local State	
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".	COM12-PuTTY Version 3.20.203. Copyright (c) 2019 American Reportends, Inc. EroS are: cp404/2019 18137:10 Version 2.10.09317531 BOARD_NAME Firmware Version 2.10.09317591 Fress (BLL) or <f2> to enter setup.Fress <f7> for boot menu.</f7></f2>	
Step_4	The BIOS sign on screen displays "Entering Setup". NOTE: It will take several seconds to display and enter the BIOS setup menu.	COMUL-PUTY Version 3.20.1273. Copyright (C) 2019 American MagArtenda, Inc. BIOG baris (VA/2420) 213(37:30 Version 2.10.093)27531 BOADD JANE Firework Version 2.10.09317531 Prefer (VB) Of (F2) to enter setup.Frees (F7) for boot menu. Entering Servey	
Step_5	The BIOS setup menu is displayed.	CONCIDENTY INCOMESTING BIOD Satury Dilley - Conversion Repairs and Ampairs	

Accessing the BMC network configuration menu

		incio Secun Unilica	- Compright (C) 2018 hm	arigan Magatrande Ing
Step_1	From the UEFI/BIOS menu, navigate to tab Server Mgmt .	Rain Advanced Drac 19 200 Honoreton 200 Vendor Core Version Core Version Core Version Suid Date and Time Access Level FPGA Version Menory Information Total Remory System Language System Time	- Copyright (c) 2019 Au - Copyright (c) 2019 Au American Regatrends 5.14 UFT 2.62 F1 1.4 06/26/2019 09:12:28 Administrator 2.02.0800AD13 32766 RB (Logitan)) (Logitan)) (Ded 07/10/2019) (13:47:54) Copyright (c) 2019 Ameri	<pre>itity Boot Event Loogs ></pre>
Step_2	Select BMC network configuration .	Pain Advanced IntelP DRC Interface(s) URLI Por INNC FPB-2 Timer Inter Timeout FPB-2 Timer Follow CS Watching Timer OS Wid Timer Follow SWID Timer Policy serial Nur S WStem Frent Log > UNC wire FRU Information > UNC wire Struct Society > DEC unterview Configuret: >	KCS, USB (Dismbled) [Pambled] [Power Cycle] [Dismbled] [10 minutes] [Peret] [Peret]	<pre>urity Boot Event.Loge > Press (free> to enable Hears (free> to enable) Hears (free to enable) Hears (free=to enable) Hears (free to enable)</pre>
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 .	Aptio Setup Vility BK metock configure Configure IVM support Lan channel 1 Address source Station IP address Subpt mach Subpt mach Station RLC address Router IAC address Router IAC address Lan channel 2 	- Copyright (C) 2019 Am Server Nome (Despective) (Despective) Dynamic AddreasterDhop 172.16.205.245 255.255.04 07.045.55 00-05-64-27-10-57 Copyright (C) 2019 Ameri	<pre> Bainct to configure LAW Tatatically or Idynamically[by BIOS Idynamically[by Idynam</pre>

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:		

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 .	Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Hain Advanced IntelRCSetup Server Mgmt Security Boot Event Logs >>
		BIOS Information IChoose the system BIOS Vendor American Megatrends Idefault language Core Version 5.14 Image: Core Version Project Version Build Date and Time 06/26/2019 09:12:20 Image: Core Version
		Access Level Administrator I FFOA Version 2.02.000AD12 > Memory Information Yolkics Intern Total Memory 32768 HB Interi Select System Language [Hglish] If Change Opt. System Language [Hglish] If Control Melles System Language [Uest 07/10/2019] If Firevious Values System Time [13:47:54] If Series Internet Version 2.200.1271. Copyright (C) 2019 American Regatrents, Inc. AD
Step_2	Select BMC network configuration .	Aprio Setup Urility - Copyright (6) 2012 Meerican Megatinnas, Inc. Nain Advanced IntelEXetup Server Kame Security Boot Youth Loop > 2 INC Interface(s) KCS, UNB - (Press Christy to enable INC Interface(s) KCS, UNB - (Press Christy to enable Wast For ENC [Disabled] + (configuration, Interf FRB-2 Timer (Inshied) + (FRB-2 Timer Charles) (FRB-2 Timer Charles) (FRB-2 Timer Charles) (FRB-2 Timer Charles) (CG Unchdag Timer [Disabled] + (CG Unchdag T
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 .	Aptio Setup Utility - Copyright (6) 2019 American Megatrends, Inc. Earver Manc DK metoork configuration

Configuring a static IP address

Step_1	From the BMC network configuration menu, select the	Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Server Ngmt
	Configuration Address source option for the LAN interface to configure (LAN channel 1 in this example).	BEC settoric configuration
Step_2	Select Static.	/ Configuration &ddress source\ Unspecified <mark>Static</mark> DynamicBmcDhcp DynamicBmcNonDhcp \/
Step_3	Change the Station IP address . NOTE: This is the management IP address (BMC MNGMT_IP).	Lan channel 1 Configuration Address source Station IP address Subnet mask Station HAC address Router IP address 00-00-00-00-00-00
Step_4	Change the Subnet mask .	Lan channel 1 Configuration Address [Static] source [25.255.0.0] Subnet mask [25.255.0.0] Station MAC address 00- Router IP address 0.0.0.0 Router MAC address 00-00-00-00-00
C+ F		Lan channel 1

Steb ² 2	(Optional) change the Router IP address .	Configuration Address source Station IP address Subnet mask Station MAC address Router IP address Router MAC address	[Static] /Router IP address 172.16.0.1 / 00 0.0.0.0 00-00-00-00-00-00
Step_6	Confirm the configuration has changed and exit BMC network configuration using the ESC key.	Lan channel 1 Configuration Address source Station IP address Subnet mask Station MAC address Router IP address Router MAC address	[Static] 172.16.205.245 255.255.0.0 00-A0-A5-D6-33-2A 172.16.0.1 00-05-64-2F-10-5F

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	I_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.	{root#localhost -}# ipmitool lan set 1 ipaddr 172.16.205.245 Setting LAN IP Addregs to 172.16.205.245
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.	[root@localhost ~]# ipmitool lan set 1 netmask 255.255.0.0 Setting LAN Subnet Mask to 255.255.0.0 T
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.	[rootBlocalhost -]# ipmitool lan set 1 defgu ipaddr 172.16.0.1 Setting LAN Default Gateway IP to 172.16.0.1
Step_5	Set the default gateway MAC address. LocalServer_OSPrompt:~#ipmitool lan set [LAN_CHANNEL] defgw macaddress [ROUTER_MAC]	[rootBlocalNost -]# spmito3 lan set 1 defgw macaddress 00:05:64:2f;10:5f Betting LMI Befault oxtrway MLC to 00:05:64:2f;10:5f
Step_6	Verify that the configuration has changed. LocalServer_OSPrompt:~# ipmitool lan print [LAN_CHANNEL]	<pre>[root@iocalhost -]# ipmitcol lan print 1 Set in Progress : Set Complete Auth Type Enable : NONE PASSWORD Auth Type Enable : Callback :</pre>

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 <u>Accessing the BIOS</u> to choose an access method.

Accessing the BMC network configuration menu

		Jurio Corus Briling	Comminder (C) 2010 Jul	riger Megetrende Tre
Step_1	From the UEFI/BIOS menu, navigate to tab Server Mgmt .	Aptio Setup Utility Main Advanced Intelf 	CSetup Server Mgmt Secu American Hegatrends 5.14 UEFI 2.6; PI 1.4	riosn Megatrends, Inc. mitty Boot Kvent Logg > (Choose the system default language
		Build Date and Time Access Level FPGA Version Memory Information Total Hemory System Language System Date System Date System Call	06/26/2019 09:12:28 Administrator 2.02.0800AD12 32766 MB (English) (Vget 07/10/2019) [13:47:54] Copyright (C) 2019 Ameri)-4: Belect Screen /Y: Select Item Enter: Select I+/: Change Opt. /F1: General Help /F2: Previous Values /F4: Bave Exit LSC: Exit LSC: Exit LSC: Act
Step_2	Select BMC network configuration .	Aptio Setup Utility Nain AtVanced Intel DRC Interface(s) Usit For BRC FRB-2 Timer Timeout FRB-2 Timer Policy OS Wid Timer Policy Setup Have The Timeout OS Wid Timer Policy Bersin Max > System Event Log > Utav YEW Information > Visw YEV Information	CCREATE Server Mane Sect RCS.USS [Simbled] [Enabled] [Fower Cycle] [Dismbled] [Reset] [Id minutes] [Reset] [idminutes]	rican Megatrends, Inc. wiky Root Event Logs / Press (Entry) to enable / or disable Serial Hux + or disable Serial Hux + or disable Serial Hux + or disable Serial Hux + or disable Serial + or
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 .	DEC merusche configure Configure IFV4 support Len channel 1 Unterent Configuration Address source Station IP address Schott and Address Router IR Address Router IR Address Lan channel 2	- Copyright (C) 2019 Jac Server Home tion (Unspecified) DynamicAddreasEmeDhop 172.16.205.245 255.255.0-0 00-Ab-De-33-2A 00-05-64-27-10-57 Copyright (C) 2019 Ameri	<pre> 'sheat to configure LAN 'channel parameters 'channel parameters 'latarcally or 'la</pre>

Configuring a dynamic IP address using DHCP

Step_1	From the BMC network configuration menu, select	Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Server Mamt
	the Configuration Address source option of the LAN interface to configure (LAN channel 1 in this example).	BMC metwork configuration
Step_2	Select DynamicBmcDhcp.	/ Configuration Address source\ Unspecified Static DynamicEmeDhop DynamicEmeDhop \/
Step_3	Navigate to Save & Exit .	Lytis decay Utility - Copyright (C) 2019 American Heystrends, Inc. Towns # Not Amage and Reset Paramet Changes and Reset Bare Changes For Changes For Change For
Step_4	Select Save Changes and Exit , this will perform a server reset.	Actio Setup Utility - Copyright (C) 2013 American Megatrends, Inc. - Save & Sitt - Save of Sitt - Save of Sitt - Save of Sitt system setup after - Save of Changes and Sitt - Save Changes and Sitt - Save Changes and Sitt - Save Changes - Save Changes <t< td=""></t<>
Step_5		pecified key to enter the BIOS setup menu. Then, access the uration . T he address displayed is your management 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 langlus -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).	[rootBlocalhost -)# ip set in Progress Auch Type Support Auch Type Support Auch Type Tanble IP Address Subnet Mark Mark Access Buther & Control Graditous AFP Intrv1 Default Gateway IP Backup Gateway IP Sackup Gateway IP Sackup Gateway INC Sackup Gateway INC	<pre>1 Set Complete 1 MORE PASSUDD 1 MORE PASSUDD 0 Dec : NORE PLSSUDD 0 pertaon: NORE PLSSUDD 1 Operator: NASSUDD 1 Operator: NASSUDD 1 T73.16.2013.43 1 T73.16.2014 1 Obseconds 1 T73.16.0.1 1 T73.16.0.1 1 Obseconds 1 Obseconds 1 T73.16.0.1 1 Obseconds 1 T7</pre>

Configuring the network time protocol - NTP

[This article describes how to configure the NTP using different methods.] Table of contents

- Configuring the NTP using the Web UI
 - <u>Prerequisites</u>
 - <u>Procedure</u>
- <u>Configuring the NTP using IPMI (IOL or KCS)</u>
 - Prerequisites (IOL)
 - Prerequisites (KCS)
 - <u>Getting the BMC time and date</u>
 - <u>Setting the BMC time and date</u>
 - <u>Confirming configuration</u>
 - Decoding NTP raw configuration data
- The network time protocol (NTP) can be configured:
- Using the Web UI
- Using IPMI (IOL or KCS)

NOTE: The system time is not set after powering up the unit. Resetting the server is sufficient to set it automatically once the BMC NTP server is configured.

Configuring the NTP using the Web UI

Prerequisites

1 The BMC IP address is known (refer to section Configuring/Baseboard management controller - BMC to obtain the BMC MNGMT_IP).

2 The remote computer has access to the management network subnet.

Relevant sections: Baseboard management controller - BMC

Accessing a BMC

Procedure

Step_1	From a remote computer that has access to the management network subnet, access the BMC Web UI using the BMC IP address.	A and do
Step_2	Click on Settings from the left side menu. Then, click on Date & Time .	Image: Specific of the speci
Step_3	In the Primary NTP Server field, enter the desired NTP server address.	Ident True Low
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.	 word Configure Date & Time Configur

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:			
Base	eboard 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).	
З	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.	[root0localhost ~]# ipmitool sel time get 07/16/2019 23:14:24 _	
	LocalServer_OSPrompt:~# ipmitool sel time get		

Setting the BMC time and date

Relevant section: Decoding NTP raw configuration data

Step_1	Enable the NTP service. LocalServer_OSPrompt:~# ipmitool raw 0x32 0xA8 3 1		
Step_2	Get the NTP configuration data to recover the current NTP server address. LocalServer_OSPrompt:~# ipmitool raw 0x32 0xA7	$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	
Step_3	Decode the raw data table. Refer to Decoding NTP raw configuration data.	Decoded data for this example: NTP Status: $0x01 \leftrightarrow Enabled$ Primary ntp: 70 6f 6f 6c 2e 6e 74 70 2e 6f 72 67 \leftrightarrow " <u>pool.ntp.org</u> ." Secondary ntp: 74 69 6d 65 2e 6e 69 73 74 2e 67 6f 76 \leftrightarrow " <u>time.nist.gov</u> ."	
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 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	
Step_5	Restart NTP service in order to save the NTP configuration. LocalServer_OSPrompt:~# ipmitool -H [BMC MNGMT_IP] -U [USER_NAME] -P [PASSWORD] -I lanplus raw 0x32 0xA8 4		

Confirming configuration

Step_1	Get the BMC time and date. LocalServer_OSPrompt:~# ipmitool sel time get	[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

0.



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

Basic BIOS option configuration

[This section details the most common configuration options related to the BIOS.] Table of contents

- <u>Changing the boot order</u>
- Overriding the boot order
- Overriding the boot order using IPMI
- Enter the BIOS menu on the next boot using IPMI
- Enabling Retry Boot Order when CSM is disabled
- <u>Configuring Secure Erase</u>
- Enabling Secure Boot
- <u>Configuring the TPM</u>

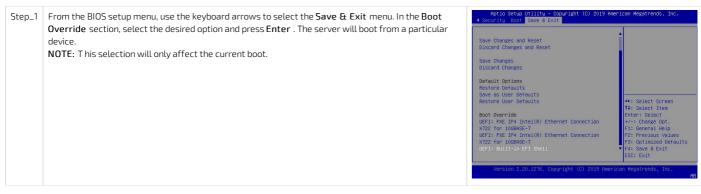
Changing the boot order

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	Aptio Setup Utility – Copyright (C) 2019 American Megatrends, Inc. ◀ Security Boot Save & Exit
	order as desired.	Boot Configuration Setup Fromo: Timeout i Setup Fromo: Timeout i Setup Fromo: Timeout i Boot Option Priorities Ioniality Ioniality Setup Fromo: Timeout i Boot Option Priorities Domestion X22 for ionian Priorities Setup Fromo: Timeout i H+: Select Screen Boot Option #2 IOEFI: PRE IF4 Intel(R) Ethernet Connection X22 for ioniant in Connection X22 for ioniant in Connection X22 for ionic Connection X22 for ioniant in Connection X22 for ioniant in Connection X22 for ioniant is Shellj H+: Select Screen Boot Option #3 IDEFI: Built-in EFI Stellin File Shell F1: General Hein Boot Option #3 IDEFI: Built-in EFI F3: Optimized Default F3: Optimized Default Version 2:20:1276, Copymight (C) 2019 American Megatrends, Inc. Version 2:20:1276, Copymight (C) 2019 American Megatrends, Inc.
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.	Antio Setup Ufility - Copyright (C) 2019 American Megatrends, Inc. Security Boot Save 8 Exit Save Changes and Exit Sav

Overriding the boot order

Refer to <u>Accessing the BIOS</u> for access instructions.



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.	<pre>\$ ipmitool chassis bootdev help bootdev <device> [clear-cmoseyes]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 Diagnostic Partition bios :: Force boot from CoV/VD bios :: Force boot from Floppy/primary removable media</device></device></pre>
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 <u>Accessing the BIOS</u> for access instructions.

o be able to retry the boot sequence indefinitely the EFI shell must be disabled in the list of boot options.	< Security Boot Save 4	Exit	
	Boot Option Priorities Boot Option #1	[CentOS (P4: SAMSUNG	^ Sets the system boot + order
	Boot Option #2	[UEFI: PXE IP4	
		Connection X722 for 10GBASE-T]	4
	Boot Option #3 	[UEFI: FXE IP4 Intel(R) Ethernet	- 11
	Burn Constant At	1000000 21	* * ><: Select Screen * ^v: Select Item
	1	Shell]	* Enter: Select
		(Disabled)	* +/-: Change Opt. * F1: General Help
	Boot Option #7	[Disabled]	* F2: Previous Values * F3: Optimized Defaul v F4: Save & Exit ESC: Exit
T	To be able to retry the boot sequence indefinitely the EFI shell must be disabled in the list of boot options.	To be able to retry the boot sequence indefinitely the EFI shell must be disabled in the list of boot options.	Boc Option Fioritie Boc Op

Configuring Secure Erase

Refer to <u>Accessing the BIOS</u> for access instructions.

Step_1	From the BIOS setup menu, select the Security menu and	Aptio Setup - American Megatrends International, LLC.
	disable the HDD Security Freeze Lock option.	I COLLY the Decr's personned is not, then this boot or enter Setup. In Setup the User will have Administrator rights. The paraword length must be in the following reget History length 3 Administrator Paraword User Paraword User Paraword Db Security Freese [Display] HDD Securi
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.	Actio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Security Boot Save & Exit: Save Changes and Reset Discard Changes and Reset Discard Changes Discard Discard Discard Discard Discard Discard Discard Discard Discard Discard Discard Dis
Step_3	Use the following application note to Secure Erase the applicable drive.	Secure Erase

Enabling Secure Boot

Refer to <u>Accessing the BIOS</u> for access instructions.

Step_1	Access the Secure Boot submenu from the Security tab.	Aptio Setup - American Megatrends In < Security Boot Save & Exit	ternational, LLC.
		The password length must be in the following range: Naximum length 20 Administrator Password User Fassword HDD Security Freeze (Enabled) Lock HDD Security Freeze (Enabled) Dock HDD Security Freeze (Enabled) Dock HDD Security Freeze (Enabled) Lock HDD Security Freeze (Enabled) Dock HDD Security Freeze (Enabled)	<pre> / Secure Boot</pre>
Step_2	Select the Secure Boot option and change it to Enabled .	Aptio Setup - American Megatrends In Security System Mode Deer System Fode International Source Secure Boot Mode I Secure Boot Mode [Standard] D Restore Factory Rey D Rest To Setup Mode > Key Management	<pre>ternational, LLC. iscure Boot feature is Active if Source Boot IPLaform Hey(FF) is ienrolled and the System is in User mode. IThe mode change Irequires platform reset</pre>
Step_3	Use the following application notes to generate and configure secure boot keys.	Generating custom secure boot ke Provisioning custom secure boot k	
Step_4	Using the keyboard arrows, select the Save & Exit menu, go to Save Changes and Exit and press Enter to confirm.	Aptio Setup Utility - Coowright (C) 2019 A 4 Security Noot Save 6 Exit Save Charges and Exit Discard Charges and Exit Discard Charges and Reset Discard Charges Discard Ch	 Exit system setup after saving the changes. **: Select Screen 11: Select Item Enter: Select 4/-: Change Oot. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save BixIt ESC: Exit

Configuring the TPM

Refer to <u>Accessing the BIOS</u> 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.	Aptio Setup - American Megatrends International, LLC. Advanced THM20 Device Found Firmater Version: 7.62 Vendor: IRX Security Device Found Advined Security Security Device Transform Advined Device Found Advined Device Transform Security Device Transform Advined Device Transform Security Device Transform
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.	Actio Setup - American Megatrends International, LIC. Avanced Active PCR banks SHA-1, SHA256 Available PCR banks SHA-1, SHA256 SHA-1 PCR Bank [Enabled] SHA-1 PCR Bank [Enabled] SHA-1 PCR Bank [Enabled] Platform Herarchy [Enabled] Total Metarchy
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 / <u>Auto</u>] NOTE: TPM has to be inserted to see the menu.	Aptio Setup - Aserican Megarrends International, 112. Advanced Active FCR banks SHA-1,5H2356 (ITM 1.3 will restrict (SH2) SHA-1 FCR Bank (Enabled) (ITM 1.2 will restrict (SH2) SHA-1 FCR Bank (Enabled) (ICM 2.2 will restrict support to TH 1.2 (ITM 1.2 will restrict support to TH 1.2 (ITM 2.2 will restrict support to TH 1.2 will restrict support to TH 1.2 (ITM 2.2 will restrict support to TH 1.2 will restrict support to TH 1.2 (ITM 2.2 will restrict support to TH 1.2 will restrict support to TH 1.2 (ITM 2.2 will restrict support to TH 1.2 will restrict support to TH 1.2 (ITM 2.2 will restrict support to TH 1.2 will restrict support to TH 1.2 (ITM 2.2 will restrict support to TH 1.2 will restrict support to TH 1.2 (ITM 2.2 will restrict support to TH 1.2 will restrict support to TH 1.2 (ITM 2.2 will restrict support to TH 1.2 will
Step_4	Using the keyboard arrows, select the Save & Exit menu, go to Save Changes and Exit and press Enter to confirm.	Actio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. 4 Security Boot Save & Exit Save Colones Save Colones Discard Changes and Reset Discard Changes Discard Changes Discard Changes Discard Changes Default Options Restore Defaults Restore Defaults Restore Defaults Boot Override UEFI: FX14 Thts[/K] Ethernet Connection XT22 for 100BASE-T Sto: Exit Version 2,20,1276. Copyright (C) 2019 American Megatrends, Inc.

Customizing platform data

{This article describes how to customize field replaceable unit data.} Table of contents

- <u>Customizing platform FRU data using IPMI</u>
- <u>FRU customizing commands</u>
 - <u>Customizing product related informations</u>
 - <u>Customizing chassis related informations</u>
- <u>Customizing logos</u>

Customizing platform FRU data using IPMI

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

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 langlus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password].

	not yield the desired results.	ocrecommended (1.8.18) witt	
Step_1	Display current FRU information. LocalServer_OSPrompt:~# i pmitool fru print	Chassis Type Chassis Fart Number Chassis Serial Chassis Extra Board Mfg Date Board Mfg Date Board Product Board Product Board Part Number Board Extra Product Manufacturer Product Manufacturer Product Part Number Product Part Number Product Serial Product Serial	: Main Server Chassis : CG2400-00 : CG24924004 : CG2400 : Mon Aug 12 15:55:00 2019 : Kontron Canada Inc. : KNB-TXS100 : 9016311783 : 1066-6560 : MAC=00:A0:A5:DA:9E:1E/05 : Kontron Canada Inc. : CG2400 : CG2400-00 : : CG24924004 :
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.	<pre>\$ ipmitool fru edit 0 field p 0 vAST28 String size are not equal, resizing fre Fre size Fre size And the second second second second Second second second second second NumByte Change: a9 NumByte Change: a9 Start Section : 1 End Section : 15 End Section : 15 End Section : 15 End Section : 15 Land Section : 15 New Fadding Length: 4 Change_size_by28: -1 heade-nofset_board: 7 Change multi offset from 0 to -1 Change multi offset from 0 to -1 Change multi of sections: 16 Calculate New Checkum: fffff19 writing new FRU. Bone.</pre>	148 1 to fit new string 5), from 248 to 240 with 'VAS1283148' (Length from '211' to '202')
Step_3	Confirm changes were properly applied. LocalServer_OSPrompt:~# ipmitool fru print	Chassis Type Chassis Fart Number Chassis Serial Chassis Extra Board Mfg Date Board Product Board Product Board Part Number Board Extra Product Manufacturer Product Manufacturer Product Part Number Product Part Number Product Serial Product Asset Tag	<pre>: Main Server Chassis : CG2400-00 : CG24924004 : CG2400 : Mon Aug 12 15:55:00 2019 : Kontron Canada Inc. : KMB-IXS100 : 9016311783 : 1066-6560 : MAC=00:A0:A5:DA:9E:1E/05 : Kontron Canada Inc. : CG2400 : CG2400-00 : : CG24924004 :</pre>

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
р 0	Product Manufacturer	LocalServer_OSPrompt:~# ipmitool fru edit 0 field p 0 [VALUE]
р1	Product Name	
р 2	Product Part Number	
р 3	Product Version	
р4	Product Serial Number	
р 5	Product Asset Tag	

Customizing chassis related informations

Comm	nand	FRU data	Example
c 0		Chassis Part Number	LocalServer_OSPrompt:~# ipmitool fru edit 0 field c 0 [VALUE]
с1		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

<u>Configuring VLANs</u>

- <u>Enabling the UEFI Network Stack and configuring CSM</u>
- <u>Creating VLANs</u>
- <u>Removing VLANs</u>
- <u>Removing VLANS</u>

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.	Aptio Setup – American Megatrends International, LLC. Advanced
	Enable Network Stack .	Network Stack LEmabled Enable/OSable UEF1 Ipv4 PXE Support [Enabled] Network Stack Ipv6 PXE Support [Disabled] Network Stack Ipv6 PXE Support [Disabled] Network Stack Ipv6 PXE Support [Disabled] Ipv6 PXE Support [Disabled] IPv6 PXE Support [Disabled] IPSE Certificate [Enabled] PXE Doct wait time 0 Nedia detect count 1
		+: Select Screen 11: Select Item Enter: Select +-: Change Oot, F1: General Help F2: Previous Volues F3: Optimized Defaults F4: Save & Rtut ESC: Exit Ver. 2,21.1277 Copyright (C) 2020 American Megatrends International, LLC. Ab
Step_2	From the Advanced menu, go to the Compatibility Support Module Configuration section.	Aptio Setup – American Megatrends International, LLC. Advanced
	If CSM Support is set to Disabled, go to Step_4. If CSM Support is set to Enabled, go to Step_3.	Compatibility Support Module Configuration CGM Support [Disabled] +: Select Screen 11: Select Ttem Enter: Select +-: Change Opt. Fil: General Help
		Ver. 2.21.1277 Copyright (C) 2020 American Megatrends International, LLC.
Step_3	Under Option ROM execution , set Network to UEFI, if not already done.	Aptio Setup – American Megatrends International, LLC. Advanced
	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).	Compatibility Support Module Configuration of UEF1 and Legacy Controls the execution of UEF1 and Legacy CSM 5 Module Version 07.84 CSM 5 Module Version 07.84 GateR20 Active [Upon Request] INT19 Trap Response [Upon Request] INT19 Trap Response Boot option filter [UEF1 and Legacy] 4+: Select Screen 14: Select Item Enter: Select Option ROM execution
		Video [UEFI] F3: Optimized Defaults Other PGI devices [UEFI] F4: Save 8 Exit ESC: Exit Ver. 2.21.1277 Copyright (C) 2020 American Megatrends International, LLC. AB
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:xxxxxxxxxxx) section.	Aptio Setup - American Megotrends International, LLC. Main <u>edwannesi</u> Platinem Configuration Socket Configuration Server Ment ▶
	Select Enter Configuration Menu . NOTE : The MAC address will be the one of the X722 10GbE port for which you want to configure VLANs.	 SESSI Configuration All Gui Information VLNN Configuration (Mec2n0928816607) Mec2n0928816617-Envs Neture: Configuration Intel(%) Ethernet Connection X722 for 1006862-T - 004704550076159 VHN Configuration (Mec2n09080765) VHN Configuration (Mec2n09080766) VHA Configuration (Mec2n09080766)
Step_2	Create a new VLAN as needed by setting its VLAN ID and Priority: • VLAN ID: value between 0 and 4094	Aptio Setup - American Megatrends International, LLC. Indvanced
	 Priority: value between 0 and 7 The example in the image shows a VLAN ID of 1001, with 802.1Q Priority 2. 	Create new VLAN 802.12 Priority, valid VLAN 10 1001 value is 0"7 Add VLAN 2000 Configured VLAN List Remove VLAN
		++: Select Screen 14: Select Item Enter: Select +/ Change Opt. F1: General Help F2: Previous Volues F3: Optimized Defaults F4: Save & Exit ESC: Exit
		Ver. 2.21.1277 Copyright (C) 2020 American Megatrends International, LLC. AB
Step_3	Select Add VLAN to create the VLAN. NOTE : You can also update an existing VLAN ID using steps 2 and 3.	Aptio Setup - American Megatrends International, LLC. Advanced Create new VLAN VLAN ID 0 Priority 0 Add VLAN Configured VLAN List VLAN ID:001, [Disabled] Prioritys2 Remove VLAN
		+: Select Screen 11: Select Item Enter: Select +-: Change Oot. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save 8 Exit ESC: Exit Ver. 2.21.1277 Copyright (c) 2020 American Megatrends International, LLC. #8
Step_4	Add other VLANs as required, using steps 2 and 3.	Aptio Setup – American Megatrends International, LLC. Advanced
	 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. 	Create new VLAN VLAN ID of new VLAN or existing VLAN or existing VLAN or existing VLAN yould related to the second value is 0°4094 value is 0°
		Priority:4 Remove VLAN He: Select Screen 11: Select Item Enter: Select + Change Opt. FI: General HeID F2: Previous Values F3: Optimized Defaults F4: Save 8 Exit ESC: Exit Ver. 2.21.1277 Copyright (C) 2020 American Magatends International, LLC. AB
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:xxxxxxxxxx) section. Select Enter Configuration Menu . NOTE: The MAC address will be the one of the X722 10GbE port for which you want to remove VLANs.	Rdvanced Create new VLAN VLAN 10 Priority Add VLAN Configured VLAN List VLAN 10:001, Priority22 VLAN 10:2002, Priority24 Remove VLAN	 American Megatrends Intel 0 0 (Enabled) [Disabled] nt (C) 2020 American Megat 	Select for remove ++: Select Screen 11: Select Item Enter: Select +/-: Change Gol. F2: Previous Valees F3: GotImized Defaults F4: Save Brit ESC: Exit
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.	Advanced Create new VLAN VLAN ID Priority Add VLAN Configured VLAN List VLAN ID:1001, Priority:2 VLAN ID:2002, Priority:4 Remove VLAN	- American Megatnends Inte 0 0 (Disabled] [Enabled] ht (C) 2020 American Megat	Remove selected VLANS ++: Select Screen 11: Select Item Enter: Select +-: Change Opt. F2: Providous Values F3: Optimized Defaults F3: Solutilized Defaults F3: Solutilized Defaults F3: Solutilized Schut ESD: Exit
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 name LED indicating alarm conditions (System Status LED)

- 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 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 langlus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password].

S	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
S	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
- <u>Accessing platform components</u>
- Platform power management
- <u>Monitoring</u>
- <u>Maintenance</u>
- 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
- <u>BIOS</u>
- <u>Management interface (BMC)</u>

Operating system

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

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

- <u>Accessing the operating system of a server</u>
- <u>Accessing the BIOS</u>
- <u>Accessing a BMC</u>

Accessing the operating system of a server

Table of contents

- Accessing an OS using the KVM
 - <u>Prerequisites</u>
 - <u>Browser considerations</u>
 - <u>Access procedure</u>
 - Accessing the BMC of the server for which you want to access the OS
 - Launching the KVM
- <u>Accessing an OS using the display port (VGA)</u>
 - <u>Prerequisites</u>
 - Port location
 - <u>Access procedure</u>
- <u>Accessing an OS using SSH, RDP or customer application protocols</u>
 - <u>Prerequisites</u>
 - <u>Access procedure</u>
- Accessing an OS using Serial over LAN (SOL)
 - <u>Prerequisites</u>
 - <u>Access procedure</u>
- <u>Accessing an OS using a serial console (physical connection)</u>
 - Prerequisites
 - Port location
 - <u>Access procedure</u>

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).		
З	The remote computer has access to the management network subnet.		
Relevant section:			
-	and the second		

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 <u>Default user names and passwords</u>.

Step_1	From a remote computer that has access to the management network, open a browser window and en NOTE: The HTTPS prefix is mandatory. <i>https://[BMC MNGMT_IP]</i>	iter the IP address discovered for the BMC.
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.	<section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>
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.	Image: Series of the series
Step_4	Log in to the BMC Web UI using the appropriate credentials. NOTE: Default Web UI user name and password is admin/admin.	Control of the second s
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	Image: state

Launching the KVM

Step_1	From the left menu, click on Remote Control .	Image: Section of the section of
Step_2	From the Remote Control menu, click on the Launch KVM button.	Image: Control of the control of
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.	

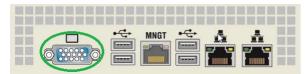
If the OS is not displayed, perform a server reset as described in <u>Sending a power command using the Web UI</u>. Then relaunch the KVM.

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.
З	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.
З	The remote computer has access to the OS subnet.

Access procedure

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).
З	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 <u>Default user names and passwords</u>.

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	\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin 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	i ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin sol activate [305 Ession operational. Use -> for help] CentOS linux 7 (Core) Kernel 3.10.0-957.el7.886.64 on an x86.64 localhost login: root Massaurdi: Last Togin: Thu Jun 27 13:21:19 on tty50 Kontron installs the bare bone images of the 05 distribution and version ordered by the customer. The customer is a threly responsible to configure their 50, to install their applications and contrain security updates that answer there, unique porformance and security needs. Accordingly, Kontron will not be held liable for any problems or any damages cused as a result of not complying with this requirement. Kontron is able to install custom 65 that answer your requirement. Contact your Kontron sales representitive to learn more about our professional services sifter. We strongly recommend changing the login username "root" and password "Kontron" set by Kontron. After acknowledging this disclamer, it's possible to dit the welcome essage by modifying the file jetC/motd Troot@localhost -]#
Step_3	The OS start screen will be displayed.	

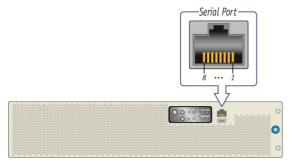
NOTE : If the OS is not displayed, perform a server reset. Refer to <u>Platform power management</u>.

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.

Baseboard management controller - BMC



Pinout			
1	RTS	5	GND
2	DTR	6	RX#
3	TX#	7	DSR
4	GND	8	CTS

CP0286

Access procedure

To obtain the list of default user names and passwords, refer to <u>Default user names and passwords</u>.

Step_1	Iter with a physical connection to the serial port, open a tool and start the communication between the console o which the device is connected.	
Step_2	The OS start screen will be displayed.	Control Linux 7 (Core) Rereal 3.18.0-877.617.806.46 on an 366_64 Localhoot Jophin F core Passeroni Last login: Thu Jun 77 14:46:36 on tryB0 Last login: Thu Jun 77 14:46:36 on tryB0 Last login: Thu Jun 77 14:46:36 on tryB0 Recordingly, forceron will not be held labeled for any probleme or any damages reduced as a result of and complying with this requirement. Four forcers in sells requested as a result of and complying with this requirement. Four four nells requested as a result of and complying with this requirement. Four four nells requested as a result of and complying with this requirement. Four four nells requested as a result of and complying with this requirement. Four four nells requested of the and complying with this requirement. Four four nells requested of the and complying the login werease "cord" and passered "Monteon" act by Fources. After acknowledging this disclinater, 1, * resultion exits the active active restrict restrict recorder.

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

Accessing the BIOS

Table of contents

- Accessing the BIOS using the KVM
 - <u>Prerequisites</u>
 - <u>Browser considerations</u>
 - <u>Access procedure</u>
 - Accessing the BMC of the server for which you want to access the BIOS
 - Launching the KVM
 - <u>Accessing the BIOS setup menu</u>
- <u>Accessing the BIOS using the display port (VGA)</u>
 - <u>Prerequisites</u>
 - Port location
 - <u>Access procedure</u>
- <u>Accessing the BIOS using Serial over LAN (SOL)</u>
 - Prerequisites
 - <u>Access procedure</u>
- <u>Accessing the BIOS using a serial console (physical connection)</u>
 - <u>Prerequisites</u>
 - Port location
 - <u>Access procedure</u>

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 <u>Default user names and passwords</u>.

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.	<section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>
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.	Image: A starting for a starting fo
Step_4	Log in to the BMC Web UI using the appropriate credentials. NOTE: Default Web UI user name and password is admin/admin.	Contraction of the contraction o
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	Image: state

Launching the KVM

Step_1	From the left menu, click on Remote Control .	=	🖗 🛦 🛛 Ballys Organic Zhanhanin 🕹 adminis
7.6471		A marked second se	Image: Section of the sectio
Step_2	From the Remote Control menu, click on the Launch KVM button.		₽ 4 800 to 2000 Aunt Ann 1990
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.	■ Anticipation of the first field in the product of the first field in the product of the first field of	

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.	* **** • C3 Image: Gends 146 (Add Add context (Mich 20) • ************************
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.	<page-header><page-header><text></text></page-header></page-header>

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

•~	MNGT	•~	4	

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 <u>Default user names and passwords</u>.

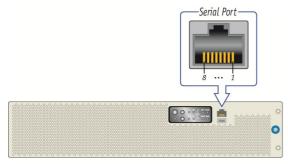
Step_1	From a remote computer that has access to the management network subnet, open the OS command prompt and deactivate any previous SOL session. RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] sol deactivate	\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin 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.	<pre>§ ipmitool -I lanplus -H 192:168:101.26 -U admin -P admin sol activate [S00: Session operational. Use -7 for help] Cent05 Linux 7 (Core) Kernel 3:10.0-957.el7.x86_64 on an x86_64 localhost login: root Password? Last login: Thu Jun 27 13:21:19 on tty50 Terment of the customer. The customer is entirely responsible to configure their 05, to install their applications and to maintain security updates that answer their unique performance and security needs. Accordingly, Kontron will not be held liable for any problems or any damages caused as negul of no complying with this requirement. Kontron sables representive to learn more about our professional services offer. We strongly recommend changing the login username "root" and password Kontron". Stri by Kontron. Kitre acknowledging this disclaimer, it's possible to edit the welcome message by modifying the file /etc/wotd [root8localhost -]# </pre>
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.	<pre>\$ ignitool -1 lamplus +# 192.168.101.26 -U admin -P admin chassis power reset System Information BOARD_MME System EDOS Version: 2.10.0932598. Date: "04/04/2013" Intel RC Version: 20.05.00 CPU Info: Intel(R) Xenn(R) CPU D-1548 & 2.000Hz Not Info: Reset Not Info: Reset Dos Intel(R) Xenn(R) CPU D-1548 & 2.000Hz Not Info: Reset Dos Info: Reset Dos Intel(R) Xenn(R) CPU D-1548 & 2.000Hz Not Info: Reset Dos Info: Reset Dos Intel(R) Xenn(R) CPU D-1548 & 2.000Hz Not Info: Reset Dos Info: Reset</pre>
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".	Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc. BIOS Date: 04/04/2019 18:17:30 Version 2.10.0932F591 BOARD MANE Firmware Version 2.10.0932F591 Press (DEL> or (F2> to enter setup.Press (F7> for boot menu.
Step_5	The BIOS sign on screen displays "Entering Setup". NOTE: It will take several seconds to display and enter the BIOS setup menu.	Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc. BIOS Date: 04/04/2019 18:17:30 Version 2.10.0932F591 BOARD_WARE Fireware Version 2.10.0932F591 Press <f7> for boot menu. Entering Setup</f7>
Step_6	The BIOS setup menu is displayed.	Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Mann Advance IntelRCSetup Server Must Security Boot Event Logs BIOS Information BIOS Vendor Compliancy American Megatrends USF 2.6, PT 1.4 Choose the system default language Gompliancy UEF 2.6, PT 1.4 Choose the system default language Build Dust and Time Project Version 04/04/2019 18:17:30 Access Level Access Level Administrator >:< Select Screen Administrator FPOA Version 2.768 MB -:< Select Screen Advised Screen File Compliance System Language English] File General Help File General Help File System Time System Time [15:144:06] File Save & Exit [ESC Exit Version 2.20.1271. Copyright (C) 2019 American Hegatrends, Inc. Notest Complexity Screen Heip

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



Pinout				
1	RTS	5	GND	
2	DTR	б	RX#	
3	TX#	7	DSR	
4	GND	8	CTS	

CP0286

Access procedure

Step_1	From a computer with a physical connection to the serial port, open a serial console tool and start the which the device is connected.	communication between the console and the port to
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.	Description Control (1) System 10.09327591 bace: "04/04/2019" Honds Dank Honds Honds Value (1) 0.09327591 bace: "04/04/2019" Marcy Info: training Value (1) 0.0912 World (1) 0.011 World (1) 0.0111
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".	COMUL-PATTY Conversion 2.10.009/restore Regetered, Inc. Blob Date: 04/04/2019 18:17:30 Version 2.10.009/r591 polad Date: Fireware Version 2.10.009/r591 Frond Otab. of (F2) of more setup.Provide of the Regutered Version (F2) of the Regitered Vers
Step_4	The BIOS sign on screen displays "Entering Setup".	PCM12-PuTTY Version 3.20.1271. Copyright (C) 2019 American Regarrends, Inc.
	NOTE: It will take several seconds to display and enter the BIOS setup menu.	BIOS Date: 04/04/2019 18:17:30 Version 2.10.0932F591 BOARD_NAME Firmware Version 2.10.0932F591
	have kontron com	//1

		P+d35 Enter	⟨ν£µ> of √Ja> to ant	et Betuy, freds (fr)> 10f D	2001 Melau -
Step_5	The BIOS setup menu is displayed.	fm BIO BIO BIO Com Pro Bui Arec FPG Mem Tot	in Advanced Intell	- Copyright (C) 2019 Am Coput Server Munic Yes American Regartends 5.14 WEFI 2.45 FI 1.4 X64 04/04/2019 18:17:30 Administrator 2.02.0800AB12 32766 HB [English] (Med 06/25/2019]	
		I Sys	tem Time	[20:13:00 <mark>]</mark>	F4: Save 6 Exit ESC: Exit

Accessing a BMC

Table of contents

- Accessing a BMC using the Web UI
 - <u>Prerequisites</u>
 - Browser considerations
 - <u>Access procedure</u>
- Accessing a BMC using IPMI over LAN (IOL)
 - <u>Prerequisites</u>
 - <u>Access procedure</u>
- <u>Accessing a BMC using IPMI via KCS</u>
 - Prerequisites
 - <u>Access procedure</u>
- Accessing a BMC using SNMP
 - Accessing a BMC using BMC SNMP
 - <u>Prerequisites</u>
 - <u>Access procedure</u>
 - <u>Accessing a BMC using the Kontron linux snmp-agent</u>
 - Prerequisites
 - <u>Access procedure</u>
- <u>Accessing a BMC using Redfish</u>
 - <u>Prerequisites</u>
 - <u>Access procedure</u>

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.	
Rele	levant section:	
Base	aseboard 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 <u>Default user names and passwords</u>.

Step_1	From a remote computer that has access to the management network, open a browser window and er NOTE: The HTTPS prefix is mandatory. <i>https://[BMC MNGMT_IP]</i>	iter the IP address discovered for the BMC.
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.	Source on the stand of the
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.	Image: Section 1.1 Image: Se
Step_4	Log in to the BMC Web UI using the appropriate credentials. NOTE: Default Web UI user name and password is admin/admin.	Linger my password
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	A train from the second

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.				
Rel	Relevant sections:				
<u>Bas</u>	Baseboard management controller - BMC				
<u>Con</u>	Common software installation				

Access procedure

To obtain the list of default user names and passwords, refer to <u>Default user names and passwords</u>.

Step_1	From a remote computer that has access to the management network subnet, e nter the desired	ipmitool -I lang	olus -H 172.1	5.205.245 -U ad	min -P ac	min sensor
· ·		Temp CPU	46,000	degrees C	ok	0,000
	command.	CPU Status	0x0	discrete	0x0080	na
	Deserve Computer OCDurrent Hismitteel Handline H [DMC MNCMT ID] H [IDMI week men al	Temp DIMM A	30,000	degrees C	ok	0,000
	RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] - P [IPMI password] [IPMI command]	Temp DIMM B	33,000	degrees C	ok	0,000
		FRUO Hot Swap	0x0	discrete	0x1080	na
	r [irmi password] [irmi command]	Temp Inlet	26,000	degrees C	ok	0,000
		Temp BMC	41,000	degrees C	ok	0,000
		Temp Vcore	44,000	degrees C	ok	0,000
		Temp Cortina	41,000	degrees C	ok	0,000

For a list of supported IPMI commands, refer to <u>Supported IPMI commands</u>. For a list of all the sensors, refer to <u>Sensor list</u>.

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).		
З	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.		
Rel	Relevant section:		
<u>Cor</u>	Common software installation		

Access procedure

<pre>tep_1 From a remote computer that has access the server OS through SSH, RDP or the platform serial p e nter the desired command. LocalServer_OSPrompt:~# ipmitool [IPMI command]</pre>	Temp CPU CPU Status Temp DIMM A Temp DIMM B FRUO Hat Swap Temp Inlet Temp BMC Temp Vcore Temp Cortina	46,000 0x0 30,000 33,000 0x0 26,000 41,000 41,000	degrees C discrete degrees C degrees C discrete degrees C degrees C degrees C degrees C	0x0080 ok ok 0x1080 ok ok ok	0,000 0,000
---	---	--	---	--	----------------

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]	\$ snmpynalk v 3 -1 authoriv -us snmpacess -4 SMA-256 -4 snmppassword -X D X snmpassword 1Z.7.6 192.20 SNMPV-SMT:entervise.1500.54 SNMPV2-EMT:enterprises.1500.554.1.0 - STRING: "WELLOD_00A0A5063E9C" SNMPV2-SMT:enterprises.1500.554.2.1.1.1 = HTTGGR: SNMPV2-SMT:enterprises.1500.554.2.1.1.3 = INTEGGR: 3 SNMPV2-SMT:enterprises.1500.554.2.1.1.3 = INTEGGR: 3 SNMPV2-SMT:enterprises.1500.554.2.1.1.5 = INTEGGR: 3 SNMPV2-SMT:enterprises.1500.554.2.1.1.5 = INTEGGR: 3 SNMPV2-SMT:enterprises.1500.554.2.1.1.5 = INTEGGR: 3 SNMPV2-SMT:enterprises.1500.554.2.1.1.5 = INTEGGR: 5 SNMPV2-SMT:enterprises.1500.554.2.1.1.7 = INTEGGR: 6 SNMPV2-SMT:enterprises.1500.554.2.1.1.7 = INTEGGR: 7 SNMPV2-SMT:enterprises.1500.554.2.1.1.7 = INTEGGR: 7 SNMPV2-SMT:enterprises.1500.554.2.1.1.8 = INTEGGR: 8 SNMPV2-SMT:enterprises.1500.554.2.1.1.8 = INTEGGR: 8 SNMPV2-SMT:enterprises.1500.554.2.1.1.8 = INTEGGR: 8 SNMPV2-SMT:enterprises.1500.554.2.1.1.8 = INTEGGR: 8
--------	--	---

Accessing a BMC using the Kontron linux snmp-agent

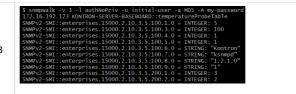
Prerequisites

1	An OS is installed.
2	The OS IP address is known.
З	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	<pre>{ curl -k -s https://Administrator:superuser@172.16.205.245/redfish/vl/ jq { "@odata.context": "/redfish/vl/Smetadata#ServiceRoot.ServiceRoot", "Madata.td": "/redfish/vl/Smetadata#ServiceRoot", "Madata.td": "/redfish/vl/Lossi "@odata.id": "/redfish/vl/CompositionService" "@odata.id": "/redfish/vl/Chassis" "@odata.id": "/redfish/vl/Chassis" "@odata.id": "/redfish/vl/CompositionService" "@odata.id": "/redfish/vl/CompositionService" "@odata.id": "/redfish/vl/CompositionService" "@odata.id": "/redfish/vl/CompositionService" "@odata.id": "/redfish/vl/CompositionService" "@odata.id": "/redfish/vl/Smetaervice" "@odata.id": "/redfish/vl/Smetaervice"</pre>
Step_2	Add the Managers/Self extension. RemoteComputer_OSPrompt:-\$curl -k -s [ROOT_URL] Managers/Self jq	<pre>{ curl -k -s https://Administrator:superuser#172.16.205.245/redfish/v1/Managers/Self jq "@ddta.cutext": "/redfish/v1/Sestadata@Manager.Manager", "Modta.type": "Manager.vL3.3.Manager", "Actions": { "Modta.type": "Manager.vL3.3.Manager", "Actions": { "Modta.type": "Manager.vL3.3.Manager", "Actions": { "Modta.type": "Manager.sest"; "incredestart" "incredestart"; "modta.type"; "Manager.sest"; "incredestart"; "in</pre>

Platform power management

[This article provides instructions to safely power on, power off or reboot a component.]

- Table of contents
 - Available power commands
 - <u>Power off</u> Power on
 - <u>Reset (warm boot)</u>
 - Power cycle (cold boot)
 - ACPI shutdown (clean shutdown)
 - Sending a power command using the Web UI.
 - Power control policy on power outage
 - Power Restore Delay on power outage

Available power commands

The power states of the CG2400 platform can be managed using various commands sent through the platform Web UI or an IPMI client (IOL or KCS). It is recommended to use the Web UI, and automation of power management tasks requires an IPMI access.

- The power commands are:
 - [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.



Power off using IPMI (KCS)

Refer to [Content under creation] Accessing a BMC using IPMI via KCS for access instructions.



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. If the late integration interacting and 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	\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power on Chassis Power Control: Up/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	S ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power status Chassis Power is on

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	<pre>t curl -k -s https://definistratorisuperuse4122.16.205.245/redfis/vi/Chassis/sdef/ResetActionInfo jq "Boditat.comtett" = //redfis/vi/SectadataSctionInfo.ActionInfo", "Boditat.comtett" = //redfis/vi/SectadataSctionInfo.ActionInfo", "Boditat.sppe" = //redistribution/", "Boditat.sppe" = //redistributio</pre>
Step_2	Power on the platform. RemoteComputer_OSPrompt:~\$ curl - POST -d '{"ResetType":"On"}' -H "Co	k -s [ROOT_URL]Chassis/Self/Actions/Chassis.Reset -X ntent-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:superuser0172.16.205.245/redfish/v1/Chassis/Self []g .PowerState Curl

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 -T 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

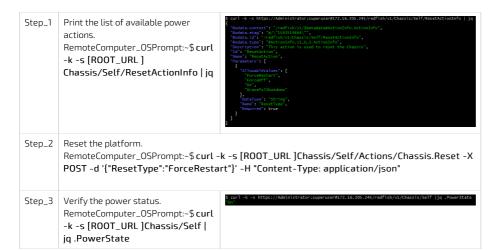
Reset (warm boot) using IPMI (KCS)

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.	[root@localhost ~]# ipmitool chassis power reset Chassis Power Control: Reset
	LocalServer_OSPrompt:~# ipmitool chassis power reset NOTE: It may take a moment for the OS to reboot.	

Reset (warm boot) using Redfish

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



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.

 From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, perform a power cycle.	[root0localhost ~]# ipmitool chassis power cycle Chassis Power Control: Cycle
LocalServer_OSPrompt:-# ipmitool chassis power cycle NOTE: It may take a moment for the OS to reboot.	

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	<pre>[root@localhost ~]# ipmitool chassis power soft Chassis Power Control: Soft [root@localhost ~]# [OK] Started Show Plymouth Power Off Screen.</pre>
--------	--	---

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	<pre>g corl =k =s https://Addinistrator:superusers172.16.205/245/redfib/oJrChassis/Self/RestActionInfo []q "Bookta.comtett = 7/redfib/oJrChassis/Self/RestActionInfo .comtended", "Bookta.comtett = 7/redfib/oJrChassis/Self/RestActionInfo .comtended", "Bookta.type: Self/RestActionInfo .comtended", "Bookta.type: Self/RestActionInf</pre>
Step_2		orm. k -s [ROOT_URL]Chassis/Self/Actions/Chassis.Reset -X utdown"}' -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:superuser0172.16.205.245/redfish/v1/Chassis/Self jg .PowerState Curl

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.	Control
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.	172.16.205.245 says Are you sure to perform this operation? OK Cancel
Step_5	Verify the power status by looking at the power status in the left side menu.	Firmware Information 0.01.09339BF8 Apr 25 2019 16:20:25 UTC 0.01.09339BF8 Host Offline Host Online Quick Links Quick Links

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 <u>Accessing the BIOS</u> for access instructions.



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	-\$ inmitool raw 0x00 0x08 0x60 0x02 0x41
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]	~\$ ipmitool raw 0x00 0x09 0x60 0x00 0x00 01 60 02 41

Using the BIOS menu

Refer to <u>Accessing the BIOS</u> for access instructions.

Step_1	From the Server Mgmt menu, select the Power Restore Delay	Aptio Setup - American Regatrends International, LLC. Main Advanced Platform Configuration Socket Configuration Server Nume -
	parameter.	02 Wed Tamer Timeout [10 minutes] ^ [Alines a delay in 10 Wed Timer Folloy [40:1] + invering up distr a 10 Serial Nux [2:smbled] + power failure, to + prover failure, to
	NOTE: when entering menu, default value will always be [unspecified] . It is imperative to select the desired value to trigger the change.	BBC Configured Power +icsuitesquitessets. The delay Control Policy
Step_2	If parameter Fixed is selected, enter a value between 55 and 300	Aptio Setup - American Megatrends International, LLC, Bain Advanced Platform Configuration Socket Configuration Server Number >
	seconds in the numerical box Power Restore Delay Value .	00 Wd Timer Timeout [10 mixuord] ''Fised time period 00 Wd Timer Tollory Hesti +55-00 decodad for 10 Betting Hesti Hesti 10 Betting Hesting Hesting 10 Betti

Monitoring

Children

- Monitoring sensors
 Sensor list
- Interpreting sensor data
- <u>Configuring and using SNMP traps</u>
 <u>System Inventory</u>
- 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

- Monitoring using the BMC Web UI
 - <u>Accessing sensor details</u>
- <u>Configuring sensors</u>
- Monitoring using IPMI
 - <u>Viewing sensor details</u>
 - <u>Configuring sensors</u>
- Monitoring using SNMP
 - Monitoring using BMC SNMP
 - Monitoring using the Kontron linux snmp-agent
- <u>Monitoring using Redfish</u>
 - <u>Creating URL extensions</u>
 - <u>Viewing sensor details</u>

The platform has many sensors, you can refer to the <u>Sensor list</u> for details and to determine the sensor ID. There are several methods to monitor platform sensors, including:

- Using the <u>BMC Web UI</u>
- Using <u>IPMI</u>
- Using <u>SNMP</u>
- Using <u>Redfish</u>

For sensor data interpretation instructions, refer to <u>Interpreting sensor data</u>. For instructions on how to access the BMC, refer to <u>Accessing a BMC</u>.

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 .	Contract control of the second control of th	1 Vaday hamafan marata	A end type Dates Leave- ener-teater
		transversence fordary (c) fordary	5.00 (20, 20, 20, 20, 20, 20, 20, 20, 20, 20,	moor Noorkoving All annexes are good new encently recovered
Step_3	The sensor list will be displayed.			a A O BOS O Sync C Retrech 1 admin -
		Entere Librardon All and Constraining All and Constraining Sensor Reading Uver reading	of all sensors	a surve - lessor-bandrer
		Calcitumia. * Critical Sensors (0)	Onlit threshold sensors are normal	
		Bonsor Discrete Sensor States (15) FIU Information		
		lat Logi & Reports > Secon Rame	State	
		Suttings Suttings Suttings Suttings Suttings	Platform Generated Page No state defined	
		Kernote Centrel A_ Doard reset	OS / run-time software init	ated hard reset
		Di Image Redirection di CPU Status Divere Control Resto Hot Swap	No state defined Manufacturer Specific Disc	who State (111)
		≱ Maintenance ♣ Fan failure	No state defined	
		Se Signified Article	sensor_specific_statessen sensor_specific_statessen	or_specific_4_0, sensor_specific_statessensor_specific_4_3, or_specific_4_3, sensor_specific_statessensor_specific_4_3
		🕹 Fan tray pres	sensor_specific_states.sen	
		Health Status Dumper Status	Manufacturer Specific Manufacturer Specific Disc	ete State (113)
		Generation Generation	Preserves Defected	
Step_4	Scroll down to see the list of sensors.	Normal Sensors (25)		
		Sensor Name	Reading	Behavior
		Fant_speed	2782 Rpm]
		♣ Fan2_speed ♣ Fan2_speed	2782.00 Rpm 2568.00 Rpm	
		C PCle slot power	2368.00 Rpm 4.20 Watts	
		1 Temp BNC	64.00 °C	
		I Temp CPU	69.00 °C	
		Temp Cortina	60 °C	
		I Temp DINM A	52.00 °C	
		Temp DINM B	56.00 °C	
		I Temp Heater	60.00 °C 46 °C	
			46 °C 66.00 °C	
		Temp Voore 4- VCC_12V_SUS		
		Temp Vcore 4- VCC_12V_SUS 4- VCC_1V05_SUS	11.83 Volts 1.04 Volts	
		4- VCC_12V_SUS	11.83 Volts	
		4 VCC_12V_505 4 VCC_1V05_505 4 VCC_1V13_505 4 VCC_1V13_505 4 VCC_1V2_505	11.81 Volts 1.04 Volts 1.19 Volts 1.19 Volts	
		 № 102, 170, 503 № 02, 170, 505 № 02, 173, 505 № 02, 172, 505 	11.02 Volts 1.04 Volts 1.19 Volts 1.14 Volts 1.29 Volts	
		 № 005_107_005 № 005_108_005 № 005_107_3,505 № 005_107_2,505 № 005_107_5,505 № 005_107_5,505 	11.42 Welts 1.64 Welts 1.34 Welts 1.34 Welts 2.40 Welts 1.60 Welts	
		 № 102, 170, 503 № 02, 170, 505 № 02, 173, 505 № 02, 172, 505 	11.02 Volts 1.04 Volts 1.19 Volts 1.14 Volts 1.29 Volts	
Step 5	Click on a sensor to see more details.	 405,127,035 405,268,035 405,272,035 405,272,035 405,272,035 405,272,035 405,272,035 	11.42 Welts 1.64 Welts 1.34 Welts 1.34 Welts 2.40 Welts 1.60 Welts	 Nov Sear-Rada - Sear-Additioned
Step_5	Click on a sensor to see more details.	 № 005_107_005 № 005_108_005 № 005_107_3,505 № 005_107_2,505 № 005_107_5,505 № 005_107_5,505 	11.42 Welts 1.64 Welts 1.34 Welts 1.34 Welts 2.40 Welts 1.60 Welts	
Step_5	Click on a sensor to see more details.	4 (95,179,98) 4 (95,179,98) 4 (95,179,98) 4 (95,179,98) 4 (95,179,98) 4 (95,179,98) 4 (95,179,98) 4 (95,179,98) 5ensor detail Al information about the same	11.42 Welts 1.64 Welts 1.34 Welts 1.34 Welts 2.40 Welts 1.60 Welts	d tree - Severhales - Severhale
Step_5	Click on a sensor to see more details.		11.42 Welts 1.64 Welts 1.34 Welts 1.34 Welts 2.40 Welts 1.60 Welts	Ø
5tep_5	Click on a sensor to see more details.	4 (95,179,98) 4 (95,179,98) 4 (95,179,98) 4 (95,179,98) 4 (95,179,98) 4 (95,179,98) 4 (95,179,98) 4 (95,179,98) 5ensor detail Al information about the same	11.01bbh 144bb 144bb 144bb 133bb 133bb 133bb 133bb	9 58 °C
Step_5	Click on a sensor to see more details.		11.01bbh 144bb 144bb 144bb 133bb 133bb 133bb 133bb	S8 °C ret lion Recoverable 124 °C
Step_5	Click on a sensor to see more details.		11.01bbh 144bb 144bb 144bb 133bb 133bb 133bb 133bb	58 °C ter Kinn Recoverable 124 °C eer Criticaal 84 °C
Step_5	Click on a sensor to see more details.		11.01bbh 144bb 144bb 144bb 133bb 133bb 133bb 133bb	
Step_5	Click on a sensor to see more details.	4 VEC_177_005 4 VEC_170_005 4 VEC_170_005 4 VEC_170_005 4 VEC_170_005 4 VEC_170_005 5 Sensor detail 1 Interp BMC Sensor Information 1 VEC_170_05 9 908	11.01bbh 144bb 144bb 144bb 133bb 133bb 133bb 133bb	58 °C ter Kinn Recoverable 124 °C eer Criticaal 84 °C
Step_5	Click on a sensor to see more details.		11.01bbh 144bb 144bb 144bb 133bb 133bb 133bb 133bb	58°C 131°C er Non Receivedé 131°C er Non Stock 41°C er Non Ottobal 71°C Mr Non Ottobal 0°C
Step_5	Click on a sensor to see more details.		11.01bbh 140bb 140bb 140bb 1.41bb 1.41bb 1.23bb 1.23bb	58°C 50°C 60°C
Step_5	Click on a sensor to see more details.		11.01bbh 144bb 144bb 144bb 133bb 133bb 133bb 133bb	58°C 50°C 60°C
5tep_5	Click on a sensor to see more details.		11.01bbh 140bb 140bb 140bb 1.41bb 1.41bb 1.23bb 1.23bb	58°C 50°C 60°C
ōtep_5	Click on a sensor to see more details.		11.01bbh 140bb 140bb 140bb 1.41bb 1.41bb 1.23bb 1.23bb	58°C 50°C 60°C
ep_5	Click on a sensor to see more details.		11.01bbh 140bb 140bb 140bb 1.41bb 1.41bb 1.23bb 1.23bb	58°C 50°C 60°C

Configuring sensors

NOTE: Sensor thresholds are set to factory default when resetting the platform.



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 .	2 Temp PCIe	58 °C Upper Nor-Receiverable Upper Nor-Critical Lower Non-Critical Lower Critical Lower Critical Lower Non-Critical	124 °C 84 °C 74 °C 0 °C -41 °C -50 °C e 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	Change Threshold Values Senso Name Temp CPU Upper Non-recoverable 224 Upper Critical 99 Upper Non-critical 70 Cover Ortical 70 Cover Critical 1 Lower Critical 1 Lower Critical 1 Cover Critical	©	

Monitoring using IPMI

The following procedures will be executed using the <u>Accessing a BMC using IPMI (KCS)</u> method, but some configurations can also be performed using IOL (<u>Accessing a BMC using IPMI over LAN (IOL)</u>). 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	ipmitool sensor Temp CPU 46,000 degrees C ok 0,000 CPU Status 0x0 discrete 0x0080 na Temp DDMM A 33,000 degrees C ok 0,000 Temp DDMM B 33,000 degrees C ok 0,000 FRU0 Hot Swap 0x0 discrete 0x1080 na Temp Inlet 26,000 degrees C ok 0,000 Temp BVC 41,000 degrees C ok 0,000 Temp Vcore 44,000 degrees C ok 0,000 Temp Cortina 41,000 degrees C ok 0,000
Step_2	Use the sdr command to see more details about a specific sensor. LocalServer_OSPrompt:-# ipmitool sdr get [SENSOR_ID]	<pre>\$ ipmitool sdr get Fan3_speed Sensor ID : Fan3_speed (0x2f) Entity ID : 29.0 (Fan Device) Sensor Reading : 0 (cr/ 0) RPM Somor Reading : 0 (cr/ 0) RPM Normal Maximum : 1712,000 Normal Maximum : 23005,000 Positive Hysteresis : 335,000 Minimum messor Ange : Unspecified Event Message Control : Marchard Entities Event Message Control : Marchard Entities Settable Thresholds : Settable Thresholds : Assertions Enabled ;</pre>

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]	<pre>\$ ipmitool sensor thresh "Temp BMC" unr 180 Locating sensor record 'Temp BMC' Setting sensor "Temp BMC" Upper Non-Recoverable threshold to 180,000</pre>

Monitoring using SNMP

The platform can be remotely monitored with the SNMP protocol:

- Using <u>BMC SNMP</u>
- Using the Kontron linux snmp-agent

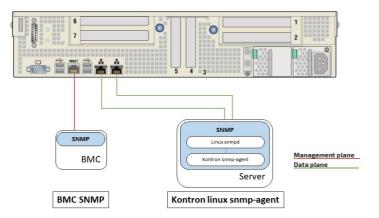
Each method is independent.

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 <u>Default user names and passwords</u> 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 <u>Accessing a BMC using BMC SNMP</u> 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]	<pre>\$ snmpwalk -v3 -1 auth 172.16.191.130 SNMPv2- SNMPv2-SMI:enterprise SNMPv2-SMI:enterprise SNMPv2-SMI:enterprise SNMPv2-SMI:enterprise SNMPv2-SMI:enterprise</pre>
		SNMPv2-SMI::enterprise SNMPv2-SMI::enterprise SNMPv2-SMI::enterprise

	authPriv -u snmp_user -			DES -X snmp_passwor
172.16.191.130 SNM	Pv2-SMI::enterprises.15			
SNMPv2-SMI::enterp	rises.15000.554.2.1.2.1	- STRING:	"Pwr Unit Redund"	
SNMPv2-SMI::enterp			"IPMI Watchdog"	
SNMPv2-SMI::enterp	rises.15000.554.2.1.2.3	B = STRING:	"FP NMI Diag Int"	
SNMPv2-SMI::enterp	rises.15000.554.2.1.2.4	= STRING:	"System Event Log"	
SNMPv2-SMI::enterp			"System Event"	
SNMPv2-SMI::enterp			"BHC Watchdog"	
SNMPv2-SMI::enterp			"VR Watchdog"	
SNMPv2-SMI::enterp	rises.15000.554.2.1.2.8	B = STRING:	"P2 TJMAX"	
SNMPv2-SMI::enterr	rises.15000.554.2.1.2.9		"PS1 Input Power"	
SNMPv2-SMI::enterp			"PS2 Input Power"	
SNMPv2-SMI::enterp			"PS1 Temp"	
SNMD92_SMT · · entern	riege 15000 554 2 1 2 1	0 = 0707MC	HDG2 Town	

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] "	§ snapkelk -v3 -1 authFriv -u snap_user -a SHA-256 -A snap_password -k DES -X snap_password 172.16.59.130 SMMFVD-SMT:renterprises_15000.584.2.1.31 SMMFVD-SMT:renterprises_15000.584.2.1.32 = INTERNE 10 SMMFVD-SMT:renterprises_15000.584.2.1.34.21 = INTERNE 46 SMMFV2-SMT:renterprises_15000.584.2.1.4.21 = Opaque: Float: 1276.000000
	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 <u>Configuring Kontron linux snmp-agent on the platform</u> for configuration instructions. See also <u>Configuring SNMP users using the Kontron linux snmp-agent</u> 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 - I [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [PASSWORD] [SERVER_IP] KONTRON-SERVER- BASEBOARD:: [OID_SUB_GROUP] grep Description	<pre>[root@localhost -]# snmpwalk -v 3 -t authNoPriv -u initial-user -a R05 -A my-password 172.16.210.149 KON TRON-SERVER-BASEBOADD::temperaturePerception.a = STRIKC: Front Panel Temp KONITON:SERVER-BASEBOADD::temperaturePerception.a = STRIKC: Front Panel Temp KONITON:SERVER-BASEBOADD::temperaturePerception.a = STRIKC: Pitters KONITON:SERVER-BASEBOADD::temperaturePerception.a = STRIKC: STRIK</pre>
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.	<pre>Transfit Continues - JP sequent -v 3 -1 aurtMarket's u stitle - uner - + RDS -A my-passerd 322.16.218.108 KOM TOW-STURMER-RESIDENCE - the person store in the result</pre>

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]"	\$ snppkalk ~v 3 ~l authkoPriv ~u initial-user ~a M05 ~A my-password 172.16.210.149 KONTRON-SERVER-ASEBADD::temparatureroberTable [] MONTRON-SERVER-ASEBADD::temparatureroberTable MONTRON-SERVER-ASEBADD::temparaturepoperCriticalThreshold: = INTEGER: 550 MONTRON-SERVER-ASEBADD::temparaturepoperCriticalThreshold: = INTEGER: 1750 KONTRON-SERVER-ASEBADD::temparaturepoperCriticalThreshold: = INTEGER: 200 KONTRON-SERVER-ASEBADD::temparaturepoperCriticalThreshold: = INTEGER: 200
Step_2	Set the value of the desired threshold. RemoteComputer_OSPrompt:~# snmpset -v3 - I [AUTH_LEVEL] -u [USER_NAME] -a [AUTH_PROTOCOL] -A [PASSWORD] [SERVER_IP] KONTRON-SERVER- BASEBOARD:: [THRESHOLD_OID]. [SENSOR_ID_NUMBER] integer [NEW_VALUE]	§ snmpset -v 3 -l authoPriv -u initial-user -a M95 -A my-password 172.16.210.149 KONTRON-SEVER-BASEDOAD::temperatureUpperCriticalThreshold.1 integer 560 KONTRON-SEVER-BASEDOAD::temperatureUpperCriticalThreshold.1 = 10FEGEN: 560

Monitoring using Redfish

Refer to <u>Accessing a BMC using Redfish</u> for access instructions.

Creating URL extensions

Туре	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



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 detecte 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) <u>Managing extension probe</u>
PCIe B Temp	60	B9h	01h	01h	PCIe B Temperature (J37 Extension cable) <u>Managing extension probe</u>
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
	72		01b	01b	

ו ב טוויזיוט וכוווין	L I	ווכט	UIII	UIII	ו כוווף כו טב טוויוויו כומווווכנ
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
		www.kontron.			// 20

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
 - Interpreting non-discrete sensor data
 - Interpreting discrete sensor data
 - Accessing event data byte 2 and 3 (optional)
 - Accessing event data byte 2 using the BMC Web UI
 - <u>Accessing event data byte 2 using IPMI</u>
- Interpretation information
 - <u>Sensor type</u>
 - <u>Sensor event/reading type</u>
 - <u>Threshold based event/reading type</u>
 - <u>Sensor-specific event/reading type</u>
 - Other event/reading types
 - Event data byte 2
 - SMI Handler generated event data bytes 2 and 3 description

Interpretation procedure

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

- Event ID
- Associated sensor
- Description

Refer for <u>System event log</u> for instructions.

 $\label{eq:NOTE:IOL} \textbf{NOTE: IOL} and \text{IPMI/KCS} are the preferred methods for interpretation.}$

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	1 Grant Carl - 7 Januar - 8 Grant Trav CTU - 1 - 8 Grant Cross Data - 1 - 8 Grant Cross Data - 1 - 1 - 2 Grant Trave Bar - 1 - 1 - 2 Grant Trave Bar - 1 - 1 - 2 Grant Trave Bar - 2 Gran	= 7 doing 10 22.04.000 10 0 dorres C = 10 doing 10 00 0 doing		44,000 99,000 99,000 99,000 99,000 99,000 94,000 9	1 124,000 1 99.000 1 99.000 1 124,000 1 124,000 1 124,000 1 124,000
Step_2	Refer to the third column of the table or the platform <u>Sensor list</u> 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.	1 Jan 2014 - Jan 2014	- Julin 1177,44,601 HT Grigore C Historie D Grigore C D Grigore C Grigore C G Grigore C Grigore C G Grigore C Grigore C Grigore C	8500° 1.000 0.000 6.000	\$4,000 \$9,000 84,000 84,000 84,000 84,000 84,000 84,000 84,000 84,000 84,000 84,000 104,00	124,000 n6 99,000 79,000 70,000 124,000 124,000 124,000
Step_3	Refer to [Content under creation] creation] Interpreting discrete ser					

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.	μ (march -1) (march -1) (march -2) (march
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.	1 (mittal) -11 (mittal) -21 (mittal) - 2 (mittal) - 2 (mittal) - 2 (mittal) - 2 (mittal) -2 (mitta) -2 (mitta) -2 (mitta) -2
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]	\$ ipmitool -I lanplus -U admin -P admin -H 172.16.209.159 sensor get "Temp CPU" Locating sensor record Sensor TD Sensor TD Sensor TD Sensor TD Sensor TD Sensor TP Upper Critical : 90,000 Upper Critical : 24,000 Positive Hystersis : 4,000 Assertions Enabled : 1cr- ucr+ unr+ Upassertions Enabled : 1cr- ucr+ unr+

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 .	1 1 0.00 4 0.00 1 0.00
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.	1 1
Step_3	As for byte 3, all values should be 0x80, meaning all event messages are enabled for this sensor.	$ \begin{array}{llllllllllllllllllllllllllllllllllll$
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.	1 emption 3 family 0 effects 0 effects 0 for 0.0 10 mms ⁻¹ mm ⁻¹ effects 0 effects 0 effects 0 for 0.0 10 mms ⁻¹ mm ⁻¹ effects 0
Step_5	If specified in the event/reading type desc Accessing event data byte 2 for additional	ription of the sensor, refer to [Content under creation] 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.	Image: Strategy of the strategy of
Step_4	In the SELLog file, find the event using its ID.	Billing-tile.com C X Fall Gamma Allfalage <
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.	Pitug-shows − × Amily Shows The state for an analysis of the state st

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 langlus -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]	<pre>\$ ipmitool -I lamplus -H 172.16.206.10 -U admin -P admin sel get 0x51 SEL Record ID : 0051 Record Type : 02 Timestamp : 2019-09-05 2019-09-05 Generator ID : 0020 EWH Revision : 04 Sensor Number : 07 Event Type : Sensor-specific Discrete Event Direction : Assertion Event Event Direction : Assertion Event Event Direction : System Boot Initiated Sensor ID : Board reset (0xf) Entity ID (Discrete): System Boot Initiated States Asserted : System Boot Initiated States Asserted : System Boot Initiated Event System Restart</pre>
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.	<pre>\$ ipmitool -I lanplus -H 172.16.206.10 -U admin -P admin sel get 0x51 SEL Record ID : 0051 Record Type : 02 Timestamp : 2019-09-05 2019-09-05 Generator ID : 0020 EvM Revision : 04 Sensor Type : Sensor-specific Discrete Event Direction : Assertion Event Event Direction : Assertion Event Event Direction : System Restart Sensor ID : Board reset (0xf) Entity ID (Discrete): System Boot Initiated States Asserted :: System Boot Initiated Event Direction : System Boot Initiated States Asserted :: System Boot Initiated States Asserted :: System Boot Initiated Event System Restart </pre>
Step_4	Refer to [Content under creation] Eve	ent 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 <u>Sensor list</u>.

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	

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	13h (Critical	04h	PCI PERR
NOTE: See SMI Handler		05h	PCI SERR	
	generated		07h	Bus Correctable Error
	event data table below		08h	Bus Uncorrectable Error
	for more information.		0Ah	Bus Fatal Error
	an ormation.		0Fh	LastBoot PCIe Error
24h	Memory Error NOTE: See	0Ch (Memory)	00h	Correctable ECC / Other correctable memory error
	SMI Handler generated event data table below		01h	Uncorrectable ECC / other uncorrectable memory error
	for more		02h	Parity
	information.		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	07h (Processor)	05h	Configuration Error

)5h	information. FP NMI Diag	13h (Critical	00h	07h (Processor)
	Int	Interrupt)	5511	
34h	Fan Failure	04h (Fan)	00h	Failure reported on fan #1
			05h	Failure reported on fan #6
)3h	IPMI	23h(Watchdog2)	00h	Timer expired
	Watchdog NOTE: See		01h	Hard reset
	BIOS generated		02h	Power down
	event data		03h	Power Cycle
	table below for more information.		08h	Timer interrupt
)7h	System	10h(Event	02h	System event log cleared
	Event Log	Logging Disabled)	04h	System event log full
			05h	System event log almost full
)8h	System	12h(System	04h	[PEF Action
	Event NOTE: See	Event)	05h	Timestamp Clock Sync
	event data table below for more information.			
8h	P1 Status	07h (Processor)	01h	Thermal trip
9h	P2 Status		0Ah	Throttled
50h	HDD0 Status	0Dh(Drive Slot / Bay)	00h	Drive Presence
51h	HDD1 Status			
52h	HDD2 Status			
i3h	HDD3 Status			
54h	HDD4 Status			
5h	HDD5 Status			
)Ch	Board	C4h (OEM board	00h	Push Button
	Status	reset)	02h	Unknown
	NOTE: See event data		06h	Cold Reset
	table below		07h	IPMI Command
	for more information.		09h	Power Up Reset
			0Ah	Power Down
)Dh	Power	D1h (OEM Power	00h	Power ON
	State	State)	01h	Power OFF
			02h	Power ON Request
			03h	Power OFF Request
			04h	Full Reset In Progress
2h	PWROK Capture 1	08h (Power supply)	00h	Power supply presence detected
3h	PWROK Capture 2		01h	Power supply failure detected
		2Bh (Version	01h	Firmware change
25h	Ver Change FPGA	Change)		detected

EFF	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 -	01h	State asserted
0Bh	VR Watchdog	Assert/Deassert)		
7Ch	CPU ERR2			
80h	CATERR			
82h	CPU Missing			
61h	Fan1 Present	08h ('digital' Discrete -	00h	Device absent
62h	Fan2 Present	Present/Absent)		
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	Ox11 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: 0x1 = DIMM 1 0x1 = DIMM 2
25h	Processor Error	07h (Processor)	• 05h	[7:4] - CPU Socket Number:	 [7:4] - Processor Error Type: 0x0 = UNKNOWN 0x1 Content www.kontron.com

				 UXU = CPU1 0x1 = CPU2 [3:0] = Bank Type: 0x0 = None 0x1 = IFU 0x2 = DCU 0x3 = DTLB 0x4 = MLC 0x5 = PCU 0x6 = II0 0x7 = CHA 0x8 = UPI 	 UX1 = LaCTIE 0X2 = TLB (Translation Look aside Buffer) 0X4 = Bus 0X8 = Micro Architecture [3:1] = Error Severity: 00 = Correctable Error 01 = Fatal Error 02 = Corrected Error 02 = Corrected Error 03 = 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 43h = RD_Cmpl_Header_Error_status 43h = RD_Cmpl_Header_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. 48h = CHANCMD Error 40h = DMA Data Parity Error. 4Eh = Read Data Error. 50h = Descriptor Control Error. 51h = Descriptor Length Error. 52h = Completion Address Error. 53h = Interrupt Configuration Error. 53h = Interrupt Configuration Error. 53h = Descriptor Count Error 55h = XOR Q Error 56h = Descriptor Count Error 57h = DIF All F Detect Error 58h = DIF Aul F Detect Error 58h = DIF Application Tag Error 58h = 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

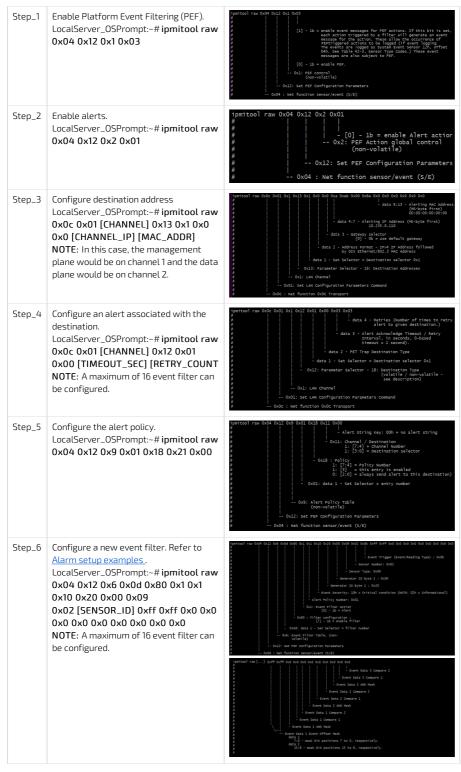
Setting up SNMP alarms using IPMI

The following procedures will be executed using the <u>Accessing a BMC using IPMI (KCS)</u> method, but some configurations can also be performed using IOL (<u>Accessing a BMC using IPMI over LAN (IOL</u>)). To use IOL, add the IOL parameters to the command: -I langlus -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.



Alarm setup examples

Detecting an HDD removal

• Event filter: 15

- Alert policy: 1
- Severity: informational

Detecting a fan removal

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

Detecting an AC or DC power lost

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

System Inventory

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

Accessing Inventory

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

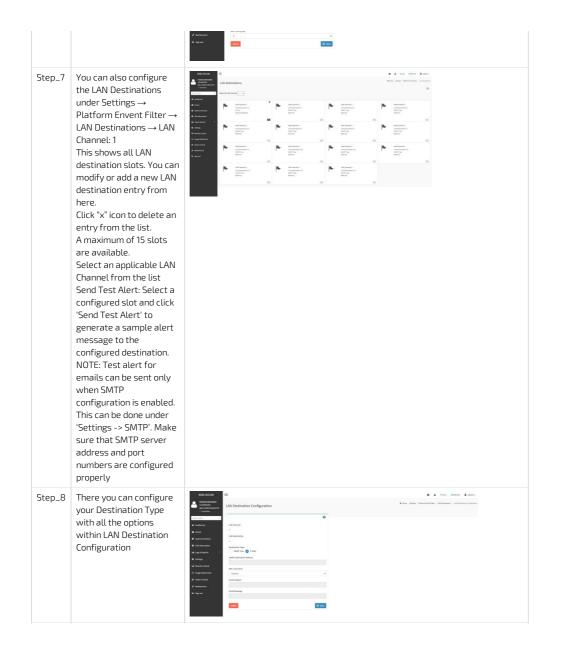
Step_1	Access the BMC Web UI									
Step_2	From the left-side menu, click on System Inventory .	AME ODUM Proceedings of the observation Proceedings of the observation Procedings of the observation Proceedings of the ob	Electronic constraints of the second constra	netroi Panel More and O	×-	Desis	28 Pending Dees	wertions More veto	o	a Luder-
Step_3	The system inventory will be displayed.	Alter Sector	DevType2_08MM3 DevType2_08MM4 DevType2_08MM0 DevType2_08MM0 DevType2_08MM2 DevType2_08MM7	Memory Control Ottler Info Name Dev/type2_08865 Dev/type2_08865 Dev/type2_08865 Dev/type2_08865 Dev/type2_08865 Dev/type2_08865 Dev/type2_08865 Dev/type2_08865 Dev/type2_08865 Dev/type2_08865	Capacity408 0 0 32258 0 32258 32258 32258 0	Manufacturer NG Denk NG Denk NG Denk NG Denk NG Denk NG Denk NG Denk NG Denk	SorialHeamber Aio Delmin Aio Delmin	A O Spec Control Contro Control Control Control Control	Absent Absent Enabled Enabled Absent	A 1 store- at base-sources at base-sou

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	KMB-DX5100	E Settings Configur BHC options			5	A Objec District 1 admits -
		Charbeles QuickLinks. • A Carboard A Sensor	Captrar Bloo	Date à Time	Esterni User	Services	KOR Weeks Setting
		Dyslem Investory FIU Information Idd Logs & Reports	Ling serings	Netta Patricito Settings		(1-1)	Fine Data Sattings
		tettings Fitnets Cantrol El Image/Indirection	System Freesal	Le Uter Management	Sala Sec	l dag	Disc Lettings
		© PowerControl → Hainberance In Sign out					
Step_2	Go to Event Filters	KMB-0/S100	Platform Event Filters				Diger Ditelest & admin -
		Neg 13 200 15 del 16 480 © Inset (Mass Queste Linis. * Combined		And Trailors	(AN Sections)		
		System Investory System Investory D FRUmburgation History					
		● Settings □ Innuts Cartral □ Seage Subjective					
		 Power Cardrel Mantenaren Sign out 					
Step_3	Choose PEF ID: #	RMB-05300				B & Olym Distant Laters -	
	You can modify or add new event filters from	ELEMENT RECENTIONS	Event Filters Cat: Configured Concentiguest PDT II. Linuking	WEDDING *	REALDING .	0 PTF TE + (Dasking)	
	here. By default, 15 event filter entries are	 Brease System Inventory ED/ Information Edl Laga & Reports 	Adv.All server sub-All (1) & karses sub-All (2) & karses Adv.All (2) & karses Adv.All (2) & karses	Werk 15 Kanness werkken 15 Kanness Mer 15 Kanness Mer 15 Kanness	velent II Season anthonic are strendty resided (2) & volue PAR de 2 (Season where al Season	when AS demants (and AS) is a ly summity rear direct (H) A roome FAS Site As/Decoded when AS location	
	configured among the 40 available slots.	 Satingi Investor Control Fauge-Technologie Prover Control 	bothistic bay seeing nat Ake(5) (seeing control contro control control control control control c	PCT-IN-16-19 average PCT-IN-16-20 average white-ind portion white-ind portion white-ind white-ind portion white-ind porti	And Charles any servery rescaled (1) & room PCF 00: 11 (Dearbed) which all Servery and Ref (1) & room	MICRAE I AN INVESTIG	
	Choose All option to view available Configured and	 Maldecare Signad 	PCF 40: 52.05 streed adva.33 Server satisfer (3) 6.5 server	PD 10.14.20x00x0 adva.14.50x00y autotes to any servedy conducts to any servedy conducts (30.4.xxxx	POP 00.13 (Seation) where all Seatory autobasis a way served can kited (13) is some		
	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	Markan M	elan •				
	options within the Event Filter Configuration	training and the second s					
	section	E Marcinel (n) → Marcent (n) →					
		Pilline III in dram dram dram dram dram Langes Langes	-				
		an Lenine (Marine Racinate Graphic Racinate Graphic Racinate Graphic Racinate (Marine)					
Step_5	You can also configure	ANRA-ESSIXE = Alienteense Alienteense Alienteense	Policies		 A Day Date: Later- A set and relationship and and and and and and and and and and		
	the Alert Poilcies under Settings \rightarrow Platform	Andrew Constraints	Imper 1 nmer Mener 2 nmer Mener Mener 2 nmer Mener 2 nmer Mener 2 nmer Mener 2	Annual Annual (Statistic) Annual (Statistic) Manual (Statistic) Manua	August Daniel August		
	Envent Filter \rightarrow Alert policies \rightarrow Group: 1	a top top to top to top top top top top t	An interpret data to be particular in the particular interpret and interpret in the particular interpret in the particular interpret in the particular interpret	Andrew	Analog of all the definition Analog of all the definition Analog of all the definition Analog of Analog Analog Analog of Analog A		
	It shows all configured Alert policies and available slots.	tractored	Anapat a pusating Anapat a pusating Anapat a for the transmission Meditional 1 Medition Organizational Anapat	Annuter	the set of the se		
	You can modify or add new alert policy entry	L.	Usepi Listedi American Strength Usepi Listedi American Strength Usepi Listedi American Strength Dimensional American American Strength	Annual Annual Section 2014 Sect	Annual Stranding Constants Annual A		
	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	KMB 05100 See finance Monster 24134-029	≡ Alert Policies			B ▲ Otyre Offe ♦ Trains - Satisgie - Factore Sect75ace - A	drach 🚹 adrein u urfrädens - Alectrices
	options within Alert Policies section	Constraint, *	Alort Policies Polity Gray Number 1 State this silent	•			
		System Insertory Set enformation intel Legi & Reports Settings	Policy Action Along's and alert to this destination LAN Channel 1	v v			
		 Russels Cardral da image Redection Four Control 	Destinative Salvator	v			
				WWW	.kontron.c	om	



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

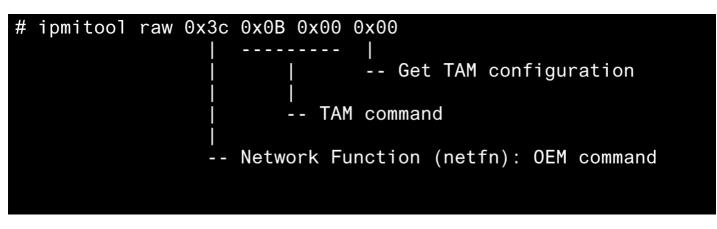
In this model, only the Telco Alarm Panel indicators that correspond to all asserted alarms are set. The Telco Alarm Panel state may indicate any combination of the three alarm severities. If any alarm is power-related, then the "Power" indicator is set; otherwise it is reset. The power alarm does not 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.

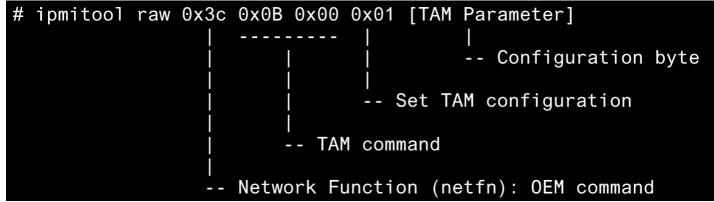
Retrieving the Telco Alarm Manager Configuration

The following IPMI command will return the actual TAM configuration byte.



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.



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 logComponents replacement
- BIOS backup and restore
- <u>Upgrading</u>
- [Content under creation] Scaling

System event log

[This article gives step-by-step instructions to view and manage system event logs.] Table of contents

- <u>Accessing the SEL using the BMC Web UI</u>
 - Accessing the system event log
 - <u>Clearing the system event log</u>
 - Downloading the system event log
- Accessing the SEL using IPMI via KCS
 - Accessing the system event log
 - <u>Clearing the system event log</u>
 - <u>Setting system event log time</u>
 - <u>Known limitation</u>
- <u>Accessing the SEL using Redfish</u>
 - <u>Accessing the system event log</u>
 - <u>Clearing the system event log</u>

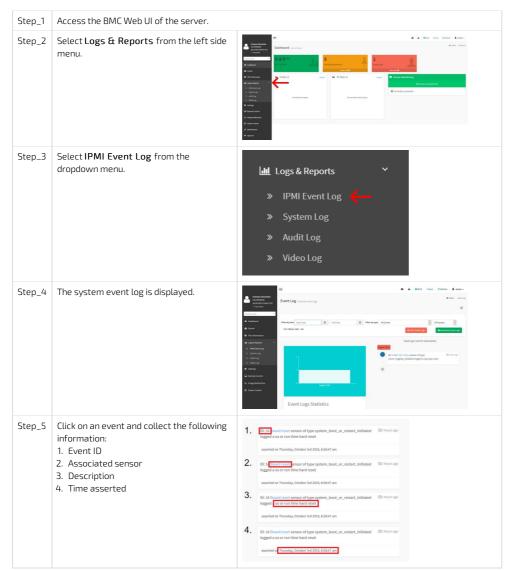
The system event log can be accessed:

- Using the [Content under creation] BMC Web UI
- Using [Content under creation] IPMI
- Using <u>Redfish</u>

Accessing the SEL using the BMC Web UI

Accessing the system event log

Refer to <u>Accessing a BMC using the Web UI</u> for access instructions.



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.

Step_1	In the Event Log menu, select Clear Event Logs .	Filter by type All Events All Sensors All Sensors Clear Event Logs
Step_2	Confirm the action by clicking on OK .	You are about to clear the IPMI Event Log. Do you really want to clear the IPMI Event Log? Empêcher cette page d'ouvrir des dialogues supplémentaires OK

Downloading the system event log

Step_1	In the Event Log menu, select Download Event Logs .	Filter by type All Events All Sensors
--------	---	---------------------------------------

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	\$ ipniteol sel \$ Information Version : 1.5 (V1.5, v2 compliant) Entries : 52 Free Space : 64566 bytes Percent User : 18 Last Del Time : Not Available Overflow : false Supported Cmds : 'Delete' 'Partial Add' 'Reserve' 'Get Alloc Info' # of Alloc Units : 3639 Alloc Unit Size : 18 # Free Units : 3557 Largest Free Blk : 3557 Max Record Size : 1
Step_2	Access the system event log list. LocalServer_OSPrompt:~\$ ipmitool sel elist	I ipritual sel elist I ipritual sel elist I 2010-9-31 00:0712 General Faunt Logeng Draabled MC SEL Seate Log area reast/cleared Databel 1 2010-9-31 00:0712 General Faunt Logeng Draabled MC SEL Seate Log area reast/cleared Databel 1 2010-9-31 00:1146 EUT Platform Aler tamb Status Asserted Databel 1 2010-9-31 00:1146 EUT Platform Aler tamb Status Asserted Databel 1 2010-9-31 00:1146 EUT Platform Aler tamb Status Asserted Databel 1 2010-9-31 00:1146 EUT Platform Aler tambs Status Asserted Databel 1 2010-9-31 00:1146 EUT Platform Aler tambs Status Asserted Asserted Asserted Asserted Asserted Databel 2 00:1146 EUT Platform Aler tambs Status Asserted Databel 2 00:1146 EUT Platform Aler tambs Status Asserted Databel 2 00:1146 EUT Platform Aler tambs Status Asserted Databel 2 00:1146 EUT Platform Aler tambs Status Asserted Databel 2 00:1146 EUT Platform Aler tambs Status Asserted Databel 2 00:1146 EUT Platform Aler tambs Status Asserted Databel 2 00:1146 EUT Platform Aler tambs Status Asserted Databel 2 00:1146 EUT Platform Aler tambs Status Asserted Databel 2 00:146 EUT Platform Aler tambs Status Asserted Databel 2 00:146 EUT Platform Aler tambs Status Asserted Databel 2 00:146 EUT Platform Aler tambs Status Asserted Databel 2 00:146 EUT Platform Aler tambs Status Asserted Databel 2 00:146 EUT Platform Aler tambs Status Asserted Databel 2 00:146 EUT Platform Aler tambs Status Asserted Databel 2 00:146 EUT Platform Aler tambs Status Asserted Databel 2 00:146 EUT Platform Aler tambs Status Asserted Databel 2 00:146 EUT Platform Aler tambs Status Asserted Databel 2 00:146 EUT Platform Aler tambs Status Asserted Databel 2 00:146 EUT Platform Aler tambs Status Asserted Databel 2 00:146 EUT Platform Aler tambs Status Asserted Databel 2 00:146 EUT Platform Aler tambs Status Asserted Databel 2 0:146 EUT Platform Aler tambs Statu
Step_3	Collect the following information for the specified e • Event ID - 1st column • Time asserted - 2nd and 3rd column • Associated sensor - 4th column (optional) • Description - 5th column	vent:

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	\$ ipeitool sel clear. Clearing SEL. Please allow a few seconds to erase.
Step_2	Verify that the system event log was properly cleared. LocalServer_OSPrompt:~# ipmitool sel elist	Experiment and affinit 1. 2019-00-21 2010-04 EBT Event cogging Disabled BKC SEL State Log www.reset/claved Accented 1. 2019-00-21 2010-04 EBT Event cogging Disabled BKC SEL State Log www.reset/claved Accented

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]"	\$ ipsitool sel time set "11/14/2018 17:06:57" 11/14/2018 17:06:58
Step_2	Verify that the sel time was properly set. LocalServer_OSPrompt:~# ipmitool sel time get	ipmitool sel time get 11/14/2018 17:07:38

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 <u>https://github.com/ipmitool.jpmitool.git</u> 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</bmc>

Accessing the SEL using Redfish

Accessing the system event log

Refer to <u>Accessing a BMC using Redfish</u> 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	<pre>[#1 4. * http://bainstader.squerame/2.11.00.30//mark/bb/2.Mangers/16/1/Agdersing/01/20/Asterner [] #</pre>
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) 	<pre>"Members": [</pre>

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
	f corl 4. a https://doinititraturisueroureB27.16.26.26.26/veBrah/u/Amougers/B1/LogBervices/SE/Actions LogBervice.Ctearcog -X PDF -d [CclearType: clearItr]- +n "Content-Type: sepification/jbas" 5g
Step_2	Verify that the system event log was properly cleared. RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL]Managers/Self/LogServices/SEL/Entries jq
	<pre>1 corl & a https://doinite.ter.source.edu/c.do.200.100/cofficient/JARAger/Sel/Address je </pre>

Components replacement

{This article gives detailed instructions to safely replace components.}

To replace a component on a CG2400 platform, refer to <u>Components installation and assembly</u>.

BIOS backup and restore

Table of contents

- Backing up the BIOS
- <u>Restoring the BIOS</u>

<u>Getting information on latest BIOS snapshot</u>

<u>Description of creation and restoration steps</u>

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	§ tpritool -l lanplus -H 192.148.1.10 -U admin -P admin raw 0x3c 0x07 0x00 0x00 S
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.	§ ipmitsol -I lampius -H 192.168.1.10 -U admin -P admin raw 0x3C 0x07 0x00 0x01 01 05 04 5

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	Ş ipnitool -I lanplus -H 192.108.1.10 -U admin -P admin raw 0x3c 0x07 0x00 0x02 Ş
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.	5 ipnitool -I lanplus -H 192.168.1.10 -U admin -P admin raw 0x3c 0x07 0x00 0x01 os 05 p

Getting information on latest BIOS snapshot

Step_1 Get backed up BIOS information. RemoteServer_OSPrompt :~# ipmitool -1 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 [BYTE7-BYTE10] Unix timestamp In the image, the version is 1.33.00000000, the status is 0x00 and the timestamp is 1325381880 .	ίπ -Ρ ad∩in raw 0x3c 0x07 0x00 0x03
---	-------------------------------------

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	0×01	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	0×07	Verifying of the snapshot flash. Verifying progress in percent (%) available in [BYTE2] of get status command (0x01).
Reset Intel ME to Normal mode	0×08	Reset Intel ME to return to normal mode.

Upgrading

[This article provides detailed instructions to safely upgrade the platform's components.]

- Table of contents
 - <u>General considerations</u>
 - Downloading the latest firmware versions
 - Upgrading the BMC and the FPGA using ipmitool
 - Prerequisite
 - Procedure
 - Upgrading the BIOS and 10GbE LAN
 - Linux method
 - <u>Transferring and uncompressing the package</u>
 - <u>Upgrading the BIOS</u>
 - Upgrading the 10GbE LAN
 - USB key method

General considerations

You may have been informed by Kontron that your running system would benefit from the latest firmware upgrades. Furthermore, 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 <u>https://www.kontron.com/products/systems/telecom-systems/cg2400-carrier-grade-server.html</u> 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.	\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power off Chassis Power Control: Down/Off
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	\$ ipmitool -I lanplus -H 192.168.101.26 -U admin -P admin chassis power status Chassis Power is off
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)=""></hpm>	A particul -1 haplet - 2 MMR -3 data -4 223 (132.247 has check cp244.1.1.4335230.has Data FFF cs124.000 -4 200.000 -4 223.000 Count FFF cs124.000 -4 200.000 -4 200.000 Victor MFT. Digsta Aport 1.8.0
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.</hpm>	<pre>h Lipstitudi _1 Limples - 2 Toble -0, admin _0 422.16.191.207 hpm upgrade cg0448.1-1.41396380.hpm all force activate Disting Urgs buffer to 7 bills The Urgs Urgs District The Urgs Urgs District to 2 bills The Urgs Urgs District The Urg</pre>
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	9 EpstEnd: -1 Supplie: -2 2000 -02 Addrs -07 Markit -41 227-14 121.207 Mpm Check Jank 197 registry pane Tailout No Nuch Tile or diractory Setting Large Markit - 10 2000 - 200

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 b="" package="" tar.gz<="">> OR unzip <update .zip="" package=""></update></update>
Step_3	Select the proper directory. cd bios-bundle- <version></version>

Select the upgrade to perform:

Upgrading the [Content under creation] BIOSUpgrading 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 <u>Platform power management</u> 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.</esc>	Version 2.21.1277. Copyright (C) 2020 American Megatrends International, LLC. BIOS Date: 05/04/2020 09:19:26 Version 1.41.0943EB53 KMB-LXS100 Firmware Version 1.41.0943EB53 Press or <f2> to enter setup. Press <f6> for boot menu. B4</f6></f2>			
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.	FSO: * Choose Aution: * Erics: 1 * SGO LaN Quedact: 3 * Come LaN Quedact: 3 * Opdate Actions perform FULL FOWERCYCLE of system Selection:			

Platform cooling and thermal management

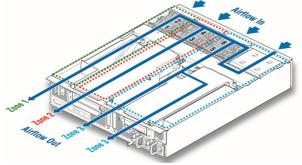
[This article provides informations about platform cooling and thermal management mechanism and describes specific behavior across platform operating temperature range.]

Table of contents

- Platform cooling subsystem
 - <u>CPU heatsinks</u>
 - AC and DC power supply airflow
- Platform thermal management
 - <u>CG2400 aggregated temperature sensors</u>
 - AC and DC power supply thermal protection

Platform cooling subsystem

The CG2400 is equipped with three sets of paired fans ensuring appropriate cooling of basic to complex component arrangements. All system components, except the power distribution board and power supply modules, are cooled by the six fans mounted near the front of the chassis behind the front panel board, as shown in the figure below.



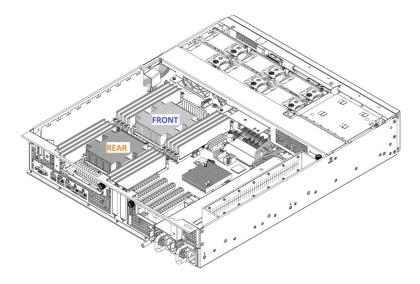
The CG2400 platform has six 80 mm x 38 mm fans, configured as three redundant pairs. There are three cooling zones delimited by the colored dotted lines in the figure above.

- Zone 1 (green dotted lines) contains fans 1 and 2, which cool both CPUs, half of the DIMMs and all the other components in this zone. Air flows through the front bezel to the rear of the chassis (zone 1 arrow).
- Zone 2 (red dotted lines) contains fans 3 and 4, which cool the other half of the DIMMs, the right-side PCI riser assembly, and all the other components in this zone. Air flows through the front bezel to the rear of the chassis (zone 2 arrow).
- Zone 3 (blue dotted lines) contains fans 5 and 6, which cool the six HDDs, the two LP PCI adapters in baseboard slots 3 and 4, the left-side PCI riser assembly and all the other components in this area. Air flows from the front bezel over the drive bay to the fans and then takes two routes for this zone: straight back to the rear of the chassis (left zone 3 arrow) and back over the power supplies to the rear of the chassis (right zone 3 arrow).
- Internal power supply fans as well as system fans 5 and 6 cool the power distribution board (PDB) and power supply modules.

The right riser card assembly (right when facing the front of the platform) sits above the CPU/memory air duct in zone 2. The vertical baffles on the top surface of the CPU/memory air duct combined with the riser card assembly and its sheet metal housing form an air duct for the PCI adapters installed in the right riser card assembly. The left riser card assembly (left when facing the front of the platform) sits above the left-most portion of the baseboard and power supply module 2 in zone 3. The left riser card assembly, its sheet metal housing and the air baffle installed to the left of the riser card assembly form an air duct for the PCI adapters installed in the left riser card assembly. 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 <u>Optional thermal probe</u> 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 overtemperature 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

- <u>Description</u>
- Location
- Probe installation
- Probe reading
- Including thermal probes into the platform's cooling algorithm
 - Guidelines for setting thermal probe thresholds

Thermal probe

Description

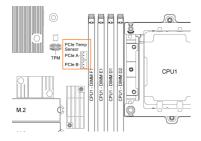
The CG2400 platform offers the flexibility to add up to two specific temperature measurement points by connecting optional temperature probes to the platform's motherboard

The probes have to be installed or affixed near thermal measurement points of interest. For example, a measurement point can be a specific chip or a known hot zone found on a PCIe card.

Such probes are included in the temperature sensor list of the fan cooling algorithm and influence the speed of the platform's fans. For the CG2400 thermal probe ordering part number, click <u>here</u>.

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. Iroot@localhost ~ J# ipmitool sdr elist + grep PCIe PCIe A Temp + B7h + ns + 7.1 + No Reading PCIe B Temp + B7h + ns + 7.1 + No Reading

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 <u>Configuring sensors</u> 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

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

Collecting diagnostics

{This article explains how to generate system logs.}

- Table of contents
 - <u>Collecting FRU information</u>
 - <u>Collecting FRU information using the BMC Web UI</u>
 - <u>Collecting FRU information using IPMI</u>
 - <u>Collecting the firmware version</u>
 - <u>Collecting the firmware version using the BMC Web UI</u>
 - <u>Collecting the firmware version using IPMI</u>
 - <u>Collecting the system event logs</u>
 - Collecting the system event logs using the BMC Web UI
 - <u>Accessing the system event log</u>
 - Downloading the system event log

<u>Collecting the system event logs using IPMI</u>

- 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 <u>Accessing a BMC using the Web UI</u> for access instructions.

Step_1	Access the BM	C Web UI of tl	ne serve	ŕ.				
Step_2	Select FRU Information from the left side menu.	Emmercialization 2.6.0007400 Sep 11.2003164024 UTC 0 wat Oxfore Quick Links.	Dashboard 42 d 1 MC Power-On M	3 hrs	du	43 Pending Deassertions	tyne C Refresh	1 admin - Horne - Dushboard
		 FIU Information Sentor TRU Information If Up Information Up Cogn Englishing Setting Prover Control Matintennos Sign out 	23 Access Logs Today (s	Board reset 8 events	Detalls		ard reset 9 events	Deteils
Step_3	The FRU information is displayed.	Chassis Information Classis Information Version Classis Type Chassis Part Number Chassis Serial Number Classis Editor	Rack Mount Chastis [store-occ] [store-occ] [ProductViene]	Board Information Board Information Area Format Version Language Manufacture Date Time Board Product Name Board Product Name Board Product Name Board Part Number	Wed Mar 28 16/0400 20 Kontron [ProductName] Jourswood] Jourswood]	Product Name Product Part I Product Versi Product Seria	nation Anua n facturer Kontron : (Produc ismber Doox-oo is	tName) IN

Collecting FRU information using IPMI

The following procedures will be executed using the <u>Accessing a BMC using IPMI (KCS)</u> method, but some configurations can also be performed using IOL (<u>Accessing a BMC using IPMI over LAN</u>). To use IOL, add the IOL parameters to the command: -I langlus -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	<pre>\$ ipmitool fru print FRU Device Description : Builtin FRU Device (ID 0) Board Mfg E [Wed Mar 28 16:04:00 2018] Board Mrg E [Nortron Board Product : [ProductName] Board Serial : [Xxxxxxxx] Board Extra : MAC=[Base MAC address]/[Total MAC used] Product Manufacturer : Kontron Product Mame : [ProductName] Product Name : [ProductName] Product Varsion : Product Serial : [XXXxxXXX]</pre>
--	--

Collecting the firmware version

The firmware version can be collected:

• Using the BMC [Content under creation] Web UI

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 .	I construction
Step_3	The firmware version is displayed.	Firmware Information Active Firmware Active Firmware Active timage ID I Build Date Sep 11 2019 Build Time 194208 UTC Firmware version L00.093TF4DA

Collecting the firmware version using IPMI

The following procedures will be executed using the <u>Accessing a BMC using IPMI (KCS)</u> method, but some configurations can also be performed using IOL (<u>Accessing a BMC using IPMI over LAN</u>). To use IOL, add the IOL parameters to the command: -I langlus -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	<pre>\$ immited hpm check PICMG HPM.1 Upgrade Agent 1.0.8:Target Information Device Id : 0x20 Device Revision :: 0x1 Product Id :: 0x2722 Manufacturer Id :: 0x3a98 (Kontron)</pre>	
		ID Name Versions Active Backup	
		1*0 [BIOS 2.20 093694DD 1*1 [FPGA 2.02 0800AD12 1 1 1 1 0.00 1 1 0.00 0.00000000 1 1 1 1 1 1 0.00 0.000000000 1 1 1 1 0.00 0.0000000000	
		(*) Component requires Payload Cold Reset	

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 <u>Accessing a BMC using the Web UI for access instructions</u>.

Step_1	Access the BMC Web UI of the server.		
Step_2	Select Logs & Reports from the left side menu.	Image: Section of the section of t	
Step_3	Select IPMI Event Log from the dropdown menu.	Logs & Reports ✓ ≫ IPMI Event Log ≫ System Log ≫ Audit Log ≫ Video Log	
Step_4	The system event log is displayed.	Control of the second of th	
Step_5	Click on an event and collect the following information: 1. Event ID 2. Associated sensor 3. Description 4. Time asserted	1. D1 must invest sensor of type system, boot, or , restart, bittated O2 hours age 1. D1 must age, conder int 2018, 55.647 am O2 hours age 2. D1 for an time baid reset. O2 hours age 3. D1 if board reset sensor of type system, boot, or , restart, bittated O2 hours age 3. D1 if board reset sensor of type system, boot, or , restart, bittated O2 hours age asorted on Thursday, conder int 2018, 55.647 am O2 hours age 3. D1 if board reset sensor of type system, boot, or , restart, bittated O2 hours age asorted on Thursday, Cotaber int 2018, 55.647 am O2 hours age asorted on Thursday, Cotaber 3d 2018, 55.647 am O2 hours age asorted on Thursday, Cotaber 3d 2018, 55.647 am O2 hours age asorted on Thursday, Cotaber 3d 2018, 55.647 am O2 hours age asorted on Thursday, Cotaber 3d 2018, 55.647 am O2 hours age bigged a or or not time hard reset. O2 hours age samering if the top system, boot, or, restart, bittated O2 hours age bigged a or or not time hard reset. O2 hours age samering if the top system, boot, or, restart, bittated O2 hours age bigged a or or time hard reset. O2 hours age same	

Downloading the system event log

Step_1	In the Event Log menu, select Download Event Logs .	Filter by type All Events All Sensors All Sensors All Sensors All Sensors All Sensors

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 langlus -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	<pre>\$ ipentool sel SL ipentool sel SL information Entries : 52 Free Space : 64566 bytes Percent User : 53 14:00:17 EST Last Add The : 10% Available Overflow : false Supported Cads : 'Delete' 'Partial Add' 'Reserve' 'Get Alloc Info' a of Alloc Linits : 363 Alloc Linits : 363 Largest Free Blk : 3587 Max Record Size : 1</pre>
Step_2	Access the system event log list. LocalServer_OSPrompt:~\$ ipmitool sel elist	b batton) 441 4154 1 7012-05-1 (607)71 457 tvent Logging Disabled MC 553 5444 Log area reset/cleared 1 7012-05-1 (607)71 457 Telform Aler Month State Log area reset/cleared 1 2012-05-1 (601346 457) Telform Aler Month State Log area 1 2012-05-1 (60146 457) Telform Aler Month State Log area 1 20
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 <u>BIOS backup and restore</u> for details.

Factory default

[This article provides detailed instructions to reset the platform to factory default.] Table of contents

- <u>Restoring default BIOS settings</u>
 - <u>Restoring default BIOS settings using the BIOS menu</u>
 - <u>Restoring default BIOS settings using IPMI</u>
 - <u>Restoring default BIOS settings using a jumper</u>
- <u>Restoring default BMC settings</u>
 - <u>Restoring default BMC settings using the BMC Web UI</u>
 - <u>Restoring default BMC settings using Redfish</u>

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".	Aprio Schup - Marinem Repartends 1 C Security Dec Save 2 Sol Save Options Discut Changes and Fut Save Changes and Fut Save Changes Discut Changes Discu	<pre>Partors/Load Pefault * setup options. * * * * * * * * * * * * * * * * * * *</pre>
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?"	Aptic Setup - American Regaternds) - Socurity Book State Fill Save Options Save Options Save Options Discard Changes and Ent Discard Changes and Henet Save Changes Discard Changes Dis	<pre>> Deset the system after > verying the changes. * * * * * * * * * * * * * * * * * * *</pre>

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 <u>Accessing a BMC using IPMI via KCS</u> method, operations could also be performed using IOL (<u>Accessing a BMC using IPMI over LAN (IOL</u>). To use IOL, add the IOL parameters to the command: -I langlus -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 <u>Accessing a BMC</u> 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 .	A and A
Step_3	If necessary, click on preserve configuration to change the list of unaffected configurations.	Restore Factory Defaults Restore Factory
	behautts to return to the previous menu.	Preserve Configuration
Step_5	Click on Save .	Restore Factory Defaults
Step_6	Confirm the factory default restoration by clicking on OK . NOTE: The platform will reset.	Click OK if you want to continue restoring configurations WARNING Restoring configurations will restart the device

Restoring default BMC settings using Redfish

Refer to <u>Accessing a BMC using Redfish</u> 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	<pre>f coll & sitter://Additionationstorecompensional additional interaction of Additional Comparison of and Additional Additional Comparison of a discrete state of the additional respects.", """""""""""""""""""""""""""""""""""</pre>
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	а дау и и и <u>Марли Аланиан андаландал и ни каканандал и ни какан</u> такана Так
Step_3	After reset, the BMC settings should have be	en restored to their default values.

Support information

{This article provides a list of additional support resources.}

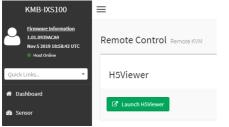
Kontron's technical support team can be reached through the following means:
By phone: 1-888-835-6676
By email: <u>support-na@kontron.com</u>
Via the website: <u>www.kontron.com</u>

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.

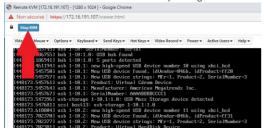
When a KVM is opened

In the Centos 7.3 console/SSH you can do "ip a" command :

і тра
to list the network interfaces, where USB0 can be seen.
(RMB-TXS10011172.16.193.901(⁻ 1# ip a 1: lo: <pre>cloopBaCK,UP,LDWER_UP> ntu 65536 qdisc noqueue state UNKNDWN group default qlen 1000 link/loopback 00:00:00:00:00 bod 00:00:00:00:00:00 inet 127.0.0.1/3 scope host lo uslid_lft forever preferred_lft forever inet6 ::1/120 scope host uslid lft forever preferred lft forever</pre>
2: encl: (BR0PAC6ST,MULTICAST,UP_LONDER_UP> mtu 1500 qdisc nq state UP group default qlen 1000 link/ether 00:00:00:00:03:14 brd ff:ff:ff:ff:ff:ff inet 172.16.193.90/16 brd 172.16.255.255 scope global dynamic encl valid_lft 313003scc preferred_lft 313003scc inet6 fcB0::200:ff:fe00:314/64 scope link valid_lft forever preferred_lft forever
3: eno2: <broadcast,multicast> ntu 1500 qdisc noop state DOWN group default qlen 1000 linkzether 00:00:00:00:03:15 brd ff:ff:ff:ff:ff:ff:ff:</broadcast,multicast>
7: usb0: <broadcast,multicast> ntu 1500 qdisc noop state DOWN group default qlen 1000 link/ether aa:70:a1:05:b3:8f brd ff:ff:ff:ff:ff:ff</broadcast,multicast>
LKMB-IXS100JL172.16.193.90JL J# _

Checking *dmesg* log, it is observable that USB0 interface causes problem with the Network Manager: Network Manager hangs, SSH service not being able to start for around 10 seconds.

WORKAROUND: close the KVM window by closing the browser window or using the Stop KVM button.



FIX: situation will be fixed within next CG2400 BMC release.

Raid Controller SNMP

[This section describes how to install and use the snmp agent for broadcom RAID cards] Table of contents

- Prerequisites
- Installing the RAID controller SNMP
- Downloading SNMP Installer
 - Extracting the content
- Using the RAID controller SNMP
- Where are the mibs ?
- What is the difference between SAS and SAS_IR?
 - <u>Meaning</u>

<u>Difference</u>



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

	Kontron linux snmp-agent is installed and running on the platform. Refer to <u>Configuring Kontron linux snmp-agent on the platform</u> .
2.	The net-snmp-utils package is installed. Refer to <u>Common software installation</u> .

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	<pre>[root@localhost -]# unzip MR_SAS_SNMP_Installer_6.14-17.05.00.02.zip Archive: MR_SAS_SNMP_Installer_6.14-17.05.00.02.zip extracting: SAS_IR_SNMP_Linux_Installer_zip extracting: SAS_IR_SNMP_Solaris_Installer_zip extracting: SAS_IR_SNMP_Solaris_Installer_zip extracting: SAS_IR_SNMP_Solaris_Installer_zip extracting: SAS_IR_SNMP_Solaris_SPARCL_Installer_zip extracting: SAS_IR_SNMP_Solaris_Installer_zip extracting: SAS_IR_SNMP_Linux_Installer_zip extracting: SAS_SNMP_Linux_Installer_zip inflating: SAS_SNMP_Solaris_Installer_zip inflating: SAS_SNMP_Solaris_SPARCL_Installer_zip extracting: SAS_SNMP_Solaris_STASLIP_INSTAller_zip extracting: SAS_SNMP_Solaris_SPARCL_Installer_zip inflating: SAS_SNMP_Solaris_SPARCI_Installer_zip extracting: SAS_SNMP_Solaris_SPARCI_Installer_zip extracting: SAS_SNMP_Solaris_SPARCI_Installer_zip extracting: SAS_SNMP_Solaris_SPARCI_Installer_zip extracting: SAS_SNMP_Solaris_SPARCI_Installer_zip extracting: SAS_SNMP_Solaris_SPARCI_Installer_zip</pre>
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]	<pre>[root@localhost ~]# unzip SAS_SNMP_Linux_x64_Installer.zip Archive: SAS_SNMP_Linux_x64_Installer.zip extracting: SAS_SNMP_Linux_x64_Installer-17.05-0002.zip inflating: MD5Checksum.txt</pre>
Step_3	Extract the file from the archive generated. LocalServer_OSPrompt:~# unzip [ARCHIVE_NAME]	[root@localhost ~]# unzip SAS_SNMP_Linux_x64_Installer-17.05-0002.zip Archive: SAS_SNMP_Linux_x64_Installer-17.05-0002.zip inflating: sas_smmp_G6bit.tar.gz inflating: sassnmp_linux_x64_readme.txt
Step_4	Extract the content from the following archive : LocalServer_OSPrompt:~# tar -zvxf sas_snmp_64bit.tar.gz	<pre>[root@localhost ~]# tar -zvxf sas_snmp_64bit.tar.gz sas_snmp-17.05-0002.x86_64.rpm</pre>

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]	<pre>[root0localhost -]# rpm -ivh sas_snmp-17.05-0002.x86_64.rpm Preparing ###################################</pre>
Step_2	Restart the snmpd and th ksnmpd service using the following commands: LocalServer_OSPrompt:~# service snmpd restart LocalServer_OSPrompt:~# service ksnmpd restart	<pre>[root@localhost ~]# service snmpd restart Redirecting to /bin/systemctl restart snmpd.service [root@localhost ~]# service ksnmpd restart Redirecting to /bin/systemctl restart ksnmpd.service</pre>

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	<pre>\$ snmpwalk -v 2c -c public -m /etc/lsi_mrdsnmp/sas/LSI-AdapterSAS.mib localhost 1.3.6.1.4.1.3582.4 LSI-MegaRAID-SAS-MIB::hostSInf0.0 = STRING: "system.localdomain" LSI-MegaRAID-SAS-MIB::hostSInf0.0 = STRING: "1.42-01" LSI-MegaRAID-SAS-MIB::molversion.0 = STRING: "1.42-01" LSI-MegaRAID-SAS-MIB::agentWoduleName.0 = STRING: "3.18.0.5" LSI-MegaRAID-SAS-MIB::agentWoduleName.0 = STRING: "3.18.0.5" LSI-MegaRAID-SAS-MIB::ralentWoduleName.0 = STRING: "3.18.0.5" LSI-MegaRAID-SAS-MIB::adentWoduleName.0 = STRING: "2.15 January, 2013" LSI-MegaRAID-SAS-MIB::adentWoduleName.0 = Wrong Type (should be Gauge32 or Unsigned32 []</pre>
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	I surgetable v_1 1 - (public u_1 /(t/) (1) informe / sat/(14) - dagter fab.mb Northow 1, 3, 1, 4, 1, 3/4, 1, 4, 2, 2, 2 core table. If a substrate interpretation of the sate of t

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

- Secure Erase on a SATA disk
 - <u>Prerequisites</u>
 - <u>Procedure</u>
- Secure Erase on an NVME disk
 - Prerequisites
- <u>Procedure</u>
- Known issues
 - <u>Command time-out during erase with larger drives</u>

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

2	Option HDD Security Freeze Lock BIOS is disabled.	
	The hdparm command line tool is installed on the local server — it is recommended to use hdparm version 9.58.	

Common software installation

Procedure

Refer to <u>Accessing the operating system of a server</u> for access instructions.

Step_1	Retrieve the disk device name. LocalServer_OSPrompt:~#ls -al /dev/disk/by-id	\$ 1s -a1 /dev/disk/bv-1d dmxx-x-x-2 frost root 100 Apr \$ 13:02 . dmxx-x-x-2 frost root 100 Apr \$ 13:02 . Invxrxmx 1 root root 30 Apr \$ 13:02 . Invxrxmx 1 root root 30 Apr \$ 13:02 dm-name-centrol0-home >/,/dm-1 Invxrxmx 1 root root 100 Apr \$ 13:02 dm-name-centrol0-home >/,/dm-1 Invxrxmx 1 root root 100 Apr \$ 13:02 dm-name-centrol0-home >/,/dm-1 Invxrxmx 1 root root 100 Apr \$ 13:02 dm-name-centrol0-sup >/,/dm-1 Invxrxmx 1 root root 10 Apr \$ 13:02 dm-name-centrol0-sup >/,/dm-1 Invxrxmx 1 root root 10 Apr \$ 13:02 dm-name-centrol0-sup >/,/dm-1 Invxrxmx 1 root root 9 Apr \$ 13:02 dm-name-centrol0-sup >/,/dm-1 Invxrxmx 1 root root 9 Apr \$ 13:02 dm-name-centrol0-sup >/,/dm-1 Invxrxmx 1 root root 9 Apr \$ 13:02 dm-name-centrol0-sup >/,/dm 1 Invxrxmx 1 root root 9 Apr \$ 13:02 dm-name-centrol0-sup >/,/dm 1 Invxrxmx 1 root root 9 Apr \$ 13:02 dm-name-centrol0-sup >/,/dm 1 Invxrxmx 1 root root 9 Apr \$ 13:02 dm-name-centrol0-sup >/,/dm 1 Invxrxmx 1 root root 9 Apr \$ 13:02 dm-name-centrol0-sup >/,/dm 1 Invxrxmx 1 root root 9 Apr \$ 13:02 dm-name-centrol0-sup >/,/dm 1 Invxrxmx 1 root root 9 Apr \$ 13:02 dm-name-centrol0-sup >/,/dm 1 Invxrxmx 1 root root 9 Apr \$ 13:02 dm-name-centrol0-sup >/,/dm 1 Invxrxmx 1 root root 9 Apr \$ 13:02 dm-name-centrol0-sup >/,/dm 1 Invxrxmx 1 root root 9 Apr \$ 13:02 dm-name-centrol0-sup >/,/dm 1 Invxrxmx 1 root root 9 Apr \$ 13:02 dm-name-centrol0-sup >/,/dm 1 Invxrxmx 1 root root 9 Apr \$ 13:02 dm-name-centrol0-sup >/,/dm 1 Invxrxmx 1 root root 9 Apr \$ 13:02 dm-name-centrol0-sup \$// sup \$/m 1 Invxrxmx 1 root root 9 Apr \$ 13:02 dm-name-centrol0-sup \$// sup \$// sup \$/m 1 Invxrxmx 1 root root 9 Apr \$/m 1 Invxrx
Step_2	Verify that the disk is not frozen. LocalServer_OSPrompt:-# hdparm -I [DEVICE_NAME]	<pre>\$ hdparm -I/dev/sda //sda: ATA device, with non-removable media Model Number: INTEL SDSCKW824008 Settal Number: INTEL SDSCKW824008 Settal Number: INTEL SDSCKW824008 Seturity: Security: Master password revision code = 65534 Master password revisio</pre>
Step_3	Verify that the disk contains data. LocalServer_OSPrompt:~# df [DEVICE_NAME]	\$ df/dev/sda Filesystem 1K-blocks Used Available Use% Mounted on /dev/mapper/centos00-root \$2403200 2334732 \$0068468 5% /
Step_4	Set disk password. LocalServer_OSPrompt:~# hdparmuser-master [USER]security-set-pass [PASSWORD] [DEVICE_NAME]	\$ hdparmuser-master usersecurity-set-pass password/dev/sda security_password: "password" /dev/sda: Issuing SECURITY_SET_PASS command, password="password", user=user, mode=high
Step_5	Perform Secure Erase on the disk. LocalServer_OSPrompt:~# hdparmuser-master [USER]security-erase [PASSWORD] [DEVICE_NAME]	<pre>\$ hdparmuser-master usedrsecurity-erase password/dev/sda security_password: "password" /dev/sda: Issuing SECURITY_ERASE command, password="password", user=user 0.000u 0.000s 0:39.71 0.0% 0+0k 0+0io 0pf+0w</pre>
Step_6	Verify that the data has been erased. LocalServer_OSPrompt:~# df [DEVICE_NAME]	\$ df/dev/sda Filesystem 1K-blocks Used Available Use% Mounted on devtmpfs 7971164 0 7971164 0% /dev

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:		
Rasic RIOS - Secure Frase		

Procedure

Refer to <u>Accessing the operating system of a server</u> for access instructions.

Step_1	List NVME devices and get device name. LocalServer_OSPrompt:~# nvme list	5 mwa 11st Node 5N Model Namespace Usage /dev/nwme0n1 PHHH922507502568 INTEL SSDPEKKA25668 1 256.06 G8 / 256.06 G8
Step_2	Get NVME device properties. Formatting and secure erase need to be supported. LocalServer_OSPrompt:~# nvme id-ctrl -H [DEVICE_NAME]	<pre>\$ nvme id-ctrl -H /dev/nvme0n1 NVME Identify Controller: vid : 0x8086 ssvid : 0x8086 sn : PHHH922507502568 mn : INTEL SSDPEKKA25668 [] oacs : 0x17 [J5:4] : 0x1 Reserved [3:3] : 0 NS Management and Attachment Not Supported [3:3] : 0 NS Management and Attachment Not Supported [1:1] : 0x1 FW Commit and Download Supported [1:1] : 0x1 Format NVM Supported] [0:0] : 0x1 Sec. Send and Receive Supported [] fna : 0x4 [2:2] : 0x1 Crypto Erase Supported as part of Secure Erase [1:1] : 0 Crypto Erase Applies to Single Namespace(s) [0:0] : 0 Format Applies to Single Namespace(s) []</pre>
Step_3	Get IBAF format type. LocalServer_OSPrompt:~# nvme id-ns [DEVICE_NAME]	<pre>\$ nvme id-ns /dev/nvme0n1 [] nguid : 000000001000000e4d25c0e25e75001 eui64 : 0000000000000 lbaf 0 : ms:0 lbads:9 rp:0 (in use)</pre>
Step_4	Perform Secure Erase on the NVME disk. LocalServer_OSPrompt:~# nvme formatibaf=[IBAF]ses=1 [DEVICE_NAME]	<pre>\$ nvme formatibaf=0ses=1 /dev/nvme0n1</pre>

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 IGB 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

<u>References</u>

- <u>StorCLI documentation</u>
- Software download URL
- <u>Vocabulary</u>
 - <u>Command arguments</u>
 - <u>Abbreviations</u>
- Installing StorCLI
 - <u>Prerequisites</u>
 - <u>Compatibility list</u>
 - Installation
 - Installing StorCLI on CentOS / RHEL
 - Installing StorCLI on Debian / Ubuntu
 - Installing StorCLI on Windows
- Using the StorCLI utility
 - <u>Commands</u>
 - <u>Help</u>
 - <u>Show</u>
 - <u>Add</u>
 - <u>Delete</u>
 - Insert
 - <u>Set</u>
 - Foreign configuration
 - Display foreign configuration
 - Delete foreign configuration
 - Import foreign configuration
 - <u>Migrate RAID configuration</u>
 - Adding a drive to an existing drive group
 - <u>Removing a drive from a RAID</u>
 - Possible RAID configurations
 - <u>Global Hot Spare</u>
 - Set a drive as Global Hot Spare
 - Delete a Global Hot Spare drive

The StorCLI utility lets users manage the RAID controller cards within the platform's operating system.

References

StorCLI documentation

This application note only covers the basic configuration and operation procedures. For further details, refer to Broadcom documentation at https://docs.broadcom.com/docs/MR-TM-StorCLI-UGI02. 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
/рх	Phy specific commands
/bbu or /cv	Battery Backup Unit or Cachevault commands
/jbodx	JBOD drive specific commands

NOTE: The ${\bf x}$ 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
Т	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 <u>Compatibility list</u> .	
3	The Intel StorCLI package has been downloaded from the <u>Software download URL</u> .	

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 <u>StorCLI documentation</u> - Chapter 2.5, pages 8 and 9.

StorCLI can be installed:

- On <u>CentOS / RHEL</u>
 On <u>Debian / Ubuntu</u>

• On <u>Windows</u>

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 <u>https://downloadmirror.intel.com/27654/eng/StorCLI_MR7.4p1.zip</u>	
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 <u>https://downloadmirror.intel.com/27654/eng/StorCLI_MR7.4p1.zip</u>	
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 <u>Software download URL</u> 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:

- <u>Help</u>
- <u>Show</u>
- <u>Add</u>
- <u>Delete</u>
- <u>Insert</u>
 <u>Set</u>
- <u>bet</u>

Help NOTE: For detailed explanations, refer to the <u>StorCLI documentation</u> - Chapter 2.5, pages 9 to 11.

Step_1	To retrieve possible commands use the storcli command . LocalServer_OSPrompt:~# storcli	<pre>[rootBlocsHest -]# store1 storage Command Line Tool yer 007.0415.0000.0000 reb 13, 2018 storage Command Line Tool yer 007.0415.0000.0000 reb 13, 2018 (c)Copyright 2018, AvacO Technologies, All Rights Reserved. While - first all The commands with their usage, E.g. store1: help commands help - gives details about a particular command. E.g. store1: add help Line of commands: Commands Enderstands the store of the st</pre>
Step_2	To retrieve all possible commands use the help command. LocalServer_OSPrompt:~# storcli help	<pre>(rootlocalmost - j6 store(1 hp)p</pre>
Step_3	Add the help keyword in order to access more precise information about the specified command. LocalServer_OSPrompt:~# storcli [COMMAND] help	<pre>\$ storcl1 cx show events [[type-sinceraboot] sinceshutdown] includedeleted] latestsx[crincon vds-0,1,] filter=(info)[karning],[critical],[fatal]> file=filepath[logfile][filterame]] storcl1/cx show eventlog[finto storcl1/cx show tearaing[roke=cnfil][contents] [logfile[-filename]] storcl1/cx show tearaing[roke=cnfil][contents] storcl1/cx show tearaing[roke=cnfil][contents] storcl1/cx show contents[roke=cnfil][contents] storcl1/cx show contents[roke=cnfil][contents][contents][contents][contents[roke=cnfil][contents][contents[roke=cnfil][contents][contents[roke=cnfil][contents][contents[roke=cnfil][con</pre>

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	S storcli /c0 show DG/VD TYPE State Access Consist Cache Cac sCC Size Name O/O RAIDO Optl RW Yes RWTD - ON 9.094 TB 1/L RAIDO Optl RW Yes RWTD - ON 9.094 TB
Step_2	Add and configure a virtual drive. LocalServer _OSPrompt:~# storcli /[CX] add [DRIVE_TYPE] r[RAID_TYPE] drives= [DRIVES] Spares=[SPARES_DRIVES]	<pre>\$ storcli /c0 add vd r5 drives=4:6,9-10 Spares=4:2</pre>
Step_3	Initialize the drive. LocalServer_OSPrompt:~# storcli /[CX]/[VX] start init full force	\$ storecli /c0/v2 start init full force
Step_4	Monitor initialization. LocalServer_OSPrompt:~# storcli / [CX]/[VX] show init	\$ storecli /c0/v2 show init
Step_5	Verify consistency after initialization has succeeded. LocalServer_OSPrompt:~# storcli / [CX]/[VX] start cc	\$ storcli /c0/v2 start cc
Step_6	Verify that the drive is added to the controller. LocalServer_OSPrompt:~# storcli /[CX] show	S storčli /c0 show DG/VD TYPE State Access Consist Cache Cac sCC Size Name O/O RAIDO Optl RW Yes RWTD - ON 9.094 TB 1/1 RAIDO Optl RW Yes RWTD - ON 9.094 TB 2/2 RAIDS Optl RW NO RWTD - ON 10.913 TB
Step_7	Verify that the drive is avalaible in the operating system of the platform. LocalServer_OSPrompt:~# lsblk	<pre>\$ lsblk NAME MAJ:MIN RM SIZE R0 TYPE MOUNTPOINT sda 8:0 0 9.1T 0 disk sda1 8:1 0 1M 0 part -sda2 8:2 0 1G 0 part /boot sda3 8:3 0 9.1T 0 part -centos_SYSTEM-root 253:0 0 50G 0 lvm / -centos_SYSTEM-swap 253:1 0 31.3G 0 lvm [SwAP] -centos_SYSTEM-home 253:2 0 9T 0 lvm /home sdb 8:16 0 9.1T 0 disk</pre>

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 <u>virtual drive</u>
 Deleting a <u>hot spare drive from a virtual drive</u>

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	<pre>\$ storcli /c0 show VD LIST :</pre>
		DG/VD TYPE State Access Consist Cache Cac sCC Size Name
		0/0 RAIDO OPTÌ RW YES RWTD - ON 9.094 TB 1/1 RAIDO OPTÌ RW YES RWTD - ON 9.094 TB 2/2 RAIDS OPTÌ RW NO RWTD - ON 10.913 TB 3/3 RAIDO OPTÌ RW YES RWTD - ON 9.094 TB
Step_2	Delete the virtual drive. LocalServer_OSPrompt:~# storcli /[CX]/[VX] del	\$ storcli /c0/v3 del
tep_3	Confirm suppression has succeeded. LocalServer_OSPrompt:~# storcli /[CX] show	<pre>\$ storcli /c0 show VD LIST :</pre>
		DG/VD TYPE State Access Consist Cache Cac sCC Size Name
		0/0 RAIDOOPTÌ RW YES RWTD - ON 9.094 TB 1/1 RAIDOOPTÌ RW YES RWTD - ON 9.094 TB 2/2 RAID5 OPTÌ RW NO RWTD - ON 10.913 TB

Deleting a hot spare drive from a virtual drive

NOTE: The hot spare drive is identified as $\ensuremath{\mathsf{DHS}}$ in the drive list.

Step_1	Display every element of the controller.	\$ storcli /c0/e4 show	
	LocalServer_OSPrompt:~# storcli /[CX]/[EX] show	EID:Slt DID State DG Size Intf Med SED PI SeSz Model Sp Type	
		4:0 5 Vicood -9.094 TB SAS HOB N N 128 HH1721010A15200 D - 4:1 7 0n1n 0 9.094 TB SAS HOB N N 128 HH3721010A15200 D - 4:2 10 DHS 2 3.458 TB SATA HOB N N 128 HH3721010A15200 D - 4:4 13 USOB 1.837 TB SATA HOB N N 1318 HK3701007-014788 D - 4:4 13 USOB 1.837 TB SATA HOB N N 1318 HK370107-014788 D - 4:6 9 Orl1 2 5.456 TB SATA HOB N N 3128 HS711043200 U - 4:9 16 Orl1 2 5.456 TB SATA HOB N N 3128 HS7110432000 U - 4:9 12 Orl1 2 5.456 TB SATA HOB N N 3128 HS7110432000 U <	
Step_2	Delete the hot spare drive. LocalServer_OSPrompt:~# storcli /[CX]/[EX]/[SX] delete hotsparedrive	\$ storcli /c0/e4/s2 delete hotsparedrive	
Step_3	Confirm suppression has succeeded.	\$ storcli /c0/e4 show	
	LocalServer_OSPrompt:~# storcli /[CX]/[EX] show	EID:Slt DID State DG Size Intf Med SED PI SeSz Model Sp Type	
		4:0 5 VERNOR 9:041 TB:SAS HOD N 3128 HHR721010843200 D - 4:1 7 0101 9:041 TB:SAS HOD N 3128 HKR721010843200 D - 4:4 13 VEGOD - 18.17 TB:SATA HOD N 3128 MKR20205792-01VCB82 D 4:5 13 VEGOD - 18.17 TB:SATA HOD N 3128 MKR20205792-01VCB82 D 4:6 9 0111 2 3.457 TB:SATA HOD N 3128 MKR20205792-01VCB82 D 4:6 9 0111 2 3.457 TB:SATA HOD N 3128 MKS710972-01VCB82 D 4:9 0111 2 3.457 TB:SATA HOD N 3128 MKS7110972050044610 U 4:9 16 011-0 2 5.456 TB:SATA HOD N 3128 HKS71105720500044610	

The **insert** command replaces the configured drive that is identified as missing. **NOTE**: For detailed explanations, refer to the <u>StorCLI documentation</u> - Chapter 2.6.3.2, pages 28 and 29.

Step_1	_1 Retrieve the drive group, array and row. LocalServer_OSPrompt:-# storcli / [CX] show LocalServer_OSPrompt:-# storcli /[CX]/dall show	\$ storecl1 /c0 show VD LIST : BG/VD TVME State Access consist Cache Cac SCC S12e Name O/O RAIDOOPT RW Ves RWTD - ON 30.094 TB 1/I RAIDS OPT RW NO RWTD - ON 10.913 TB \$ storecl1 /c0/dall show PD LIST :
		EID:Slt DID State DG Size Intf Med SED PI Sesz Model Sp Type 4:0 5 3000 - 0.004 TB SAS. FOD N N 3128 HH#721010A.5200 U - 4:1 7 0nin 0 9.004 TB SAS. FOD N N 3128 HH#721010A.5200 U - 4:1 10 0nin 1 3.438 TB SAR. FOD N N 3128 HH#721010A.5200 U - 4:2 10 0nin 1 3.438 TB SAR. FOD N N 3128 HH#721010A.5200 U - 4:3 10 0nin 1 1.847 B SAR. FOD N N 3128 HKCT HH\$72000A.5200 U - 4:4 10 0nin 1 1.847 B SAR. FOD N N 3128 HKCT HH\$72000A.5100 U - 4:5 13 0kcod - 1.847 TB SAR. FOD N N 3128 HKCT HH\$72000A.5100 U - 4:6 9 3000 - 5.456 TB SAR. FOD N N 3128 HKCT HH\$72000A.5100 U - 4:6 9 1000 - 5.456 TB SAR. FOD N N 3128 HKCT HH\$72000A.5100 U - 4:10 12 0nin 1 5.456 TB SAR. HDD N N 3128 HKCT HH\$72000A.5100 U - 4:11 8 0600d - 9.004 TB SAS HDD N N 3128 HKF71H\$72000A.5100 U - 4:11 8 0600d - 9.004 TB SAS HDD N N 3128 HKF71H\$72000A.5100 U -
Step_2 (Optional)	Set the drive to UGood. LocalServer_OSPrompt:~# storcli /[CX]/[EX]/[SX] set good force	\$ storcli /c0/e4/s6 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.	\$ storcli /c0/e4/s6 insert dg=1 array=0 row=1
Step_4	Set the drive state to online . LocalServer_OSPrompt:~# storcli /[CX]/[EX]/[SX] set online	\$ storcli /c0/e4/s6 set online
Step_5	Get the rebuild progress. LocalServer_OSPrompt:~# storcli /[CX]/[EX]/[SX] show rebuild	<pre>\$ storcli /c0/e4/s6 show rebuild cLI version = 007.0415.0000.0000 Feb 13, 2018 Operating system = Linux 4.4.0-121-generic Controller = 0 Status = Success Description = Show Drive Rebuild Status Succeeded. Drive-ID Progress% Status Estimated Time Left /c0/e4/s6 38 In progress 5 Hours 13 Minutes</pre>

Set

NOTE: For detailed explanations, refer to the <u>StorCLI documentation</u> - Chapter 2.6.2, pages 12 to 18. The set commands described in this section are:

- <u>Set drive state</u>
- <u>Set alarm actions</u>
- <u>Set EGHS configuration</u>

Set drive state

NOTE: For detailed explanations, refer to the <u>StorCLI documentation</u> - Chapter 2.6.3.3, pages 29 and 30.

Display all drives and identify the drive's state. Step_1 LocalServer_OSPrompt:~# storcli /[CX] show 9.094 TB SAS HDD N N 512B HUH721010AL52 Step_2 Set the drive state using one of the following states: \$ storcli /c0/e4/s0 set • 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] Display all drives using the following command to ensure the states updated successfully. Step_3 LocalServer_OSPrompt:~# storcli /[CX] show

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

Set EGHS configuration

This command is used to configure the emergency rebuild:

- State enables or disables the service.
- Smarter sets the service to replace predictive failed drive or not.
- EUG sets the EUG drive to be used automatically for rebuild or not.

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

Foreign configuration

When a drive already contains a configuration from another controller, the controller will identify it as a foreign configuration. **NOTE:** For detailed explanations, refer to the <u>StorCLI documentation</u> - 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

9	Step_1	Display all the drives considered as foreign configured.	\$ storcli /c0/fall show all
		LocalServer_OSPrompt:~# storcli /[CX]/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 .	[[root@localhost ~]# storcli /c0/fall import
	LocalServer_OSPrompt:~# storcli /[CX]/fall import	

Migrate RAID configuration

NOTE: For detailed explanations, refer to the StorCLI documentation - Chapter 2.6.4.8, pages 45 to 47.

This section describes the following:

- Adding a drive to an existing drive group
- <u>Removing a drive from a RAID</u>
- Possible RAID configurations

Adding a drive to an existing drive group

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

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	\$ storcli /c0/v2 start migrate type=raid0 option=remove drives=4:2
	drives=[DRIVES]	

Possible RAID configurations

Initial RAID level	Migrated RAID level
RAID 0	RAID 1
RAID 0	RAID 5
RAID 0	RAID 6
RAID 1	RAID 0
RAID 1	RAID 5
RAID 1	RAID 6
RAID 5	RAID 0
RAID 5	RAID 6
RAID 6	RAID 0
RAID 6	RAID 5

Global Hot Spare

NOTE: For detailed explanations, refer to the <u>StorCLI documentation</u> - 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.	\$ storcli /c0/e4/s4 add hotsparedrive
	LocalServer_OSPrompt:~# storcli /[CX]/[VX]/[SX] add hotsparedrive	

Delete a Global Hot Spare drive

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

Software RAID (VRoC)

- Introduction
- Supported RAID
- How to enable the RAID options
- <u>UEFI</u>
 - <u>VROC SATA Driver</u>
 - <u>Main Menu</u>
 - <u>Create RAID</u>
 - Delete RAID
- Legacy
 - VRoC Option ROM
 - <u>Acceding the Management Console</u>
 - Hardware Specification
 - VRoC Option ROM & Dashboard
 - <u>Raid Creation</u>
 - <u>Raid Deletion</u>
 - <u>Raid to Non-Raid</u>
 - How the OS manage the RAID ?
 - Can an OS be install on this volume ?
 - <u>Ubuntu 16.04</u>
 - <u>Centos 7.4</u>

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 \rightarrow PCH Configuration \rightarrow PCH SATA Configuration \rightarrow Configure SATA as \rightarrow *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

BIOS Information		
	American Megatrends	
	UEFI 2.7; PI 1.6	
	KMB-IX5100	
Access Level	Administrator	
Platform Information		
Platform	KM8-IX5100	
	50655 - CLX A0	
RC Revision		
SINIT ACM		
Memory Information		
Memory Informacion		
Aptio Setup	ght (C) 2020 American Me - American Megatrends In	[ESC: Exit patrends International, LLC ternational, LLC. t Configuration Server Nam
Ver. 2.21.1277 Copyri Aptio Setup Main Advanced Platf	ght (C) 2020 American Me - American Megatrends In orm Configuration Socke	gatrends International, LLC ternational, LLC. t Configuration - Server Mgm
Ver. 2.21.1277 Copyri Aptio Setup Hain Advanced Platf	ght (C) 2020 American Me - American Hegatrends In orm Configuration Socke - Settings	patrends international, ucc ternational, LLC. t Configuration Server Nym (This formset allows the
Ver. 2.21.1277 Copyri Aptio Setup Hain Advanced Platf Redfish Host Interface Serial Port Console Re	ght (C) 2020 American Me - American Hegatrends In orm Configuration Socke - Settings	ternational, LLC ternational, LLC. L Configuration Server Ngm This formset allows th + user to manage RAID
Ver. 2.21.1277 Copyri Aptio Setup Main Advanced Plata Redfish Host Interface serial Port Console Re 10 Configuration	ght (C) 2020 American Me - American Megatrends In orm Configuration Socke - Settings direction	patrends international, ULC ternational, LLC. E Configuration Server Nom Althis formset allows the Huser to manage RAID Volumes on the intel(R
Ver. 2.21.1277 Copyri Aptio Setup Hain Advanced Plate tedfish Host Interface terfal Port Console Re 10 Configuration ption ROM Dispatch Po	oht (C) 2020 American He - American Megatrends In Orm Configuration Socke Settings direction Licy	ternational, LLC ternational, LLC. L Configuration Server Ngm This formset allows th + user to manage RAID
Ver. 2.21.1277 Copyri Aptio Setup Main Advanced Plaif Redfish Host Interface Final Port Console Re FD Configuration Option ROM Dispatch Pe Ci Subsystem Settings	oht (C) 2020 American He - American Megatrends In Orm Configuration Socke Settings direction Licy	patrends international, ULC ternational, LLC. E Configuration Server Nom Althis formset allows the Huser to manage RAID Volumes on the intel(R
Ver. 2.21.1277 Copyri Aptio Setup Main Advanced Place tedfish Host Interface erial Port Console Re- 10 Configuration Pytion RON Dispatch Pe VCI Subsystem Settings 58 Configuration	9HE (0) 2020 American He - American Hegatrends In Orm Configuration Socke Settings direction licy	patrends international, ULC ternational, LLC. E Configuration Server Nom Althis formset allows the Huser to manage RAID Volumes on the intel(R
Aptio Setup Aptio Setup Hain Advanced Pleif Redfish Host Interface Hain Port Consile Re do Configuration Dition ROM Dispatch Po Ci Subsystem Settings 158 Configuration etwork Stack Configuration	9HE (0) 2020 American He - American Hegatrends In Orm Configuration Socke Settings direction licy	patrends international, ULC ternational, LLC. E Configuration Server Nom Althis formset allows the Huser to manage RAID Volumes on the intel(R
Aptio Setup Aptio Setup Main Advanced Plain Mediah Host Interface erial Port Console Re- rid Configuration Dition ROM Dispatch Port SE Configuration DES Configuration Network Stack Configur	9HE (0) 2020 American He - American Hegatrends In Orm Configuration Socke Settings direction licy	patrends international, ULC ternational, LLC. E Configuration Server Nom Althis formset allows the Huser to manage RAID Volumes on the intel(R
Aptio Setup Aptio Setup Main Advanced Plain Mediah Host Interface erial Port Console Re- rid Configuration Dition ROM Dispatch Port SE Configuration DES Configuration Network Stack Configur	9HE (0) 2020 American He - American Hegatrends In Orm Configuration Socke Settings direction licy	patrends international, ULC ternational, LLC. E Configuration Server Nom Althis formset allows the Huser to manage RAID Volumes on the intel(R
Aptio Setup Aptio Setup Hein Advanced Dise Kedlish Host Steriface In Configuration Diction RM Dispatch Pe CT Subsystem SetUngs Bis Configuration Network Stack Configur Ster Configuration Net Configuration	ght (c) 2020 Annakan ko c American Regatrends in Orn Controllington Sector Sattings direction licy. ation	parends unternationally it is termational, its. Itodafapuration Servers Paym This formet allows the Ithis formet allows the Italia contering and the NAID Controller
Aptio Setup Aptio Setup Haun Advanced State Heinia Port Canada in Harria Port Canada in Harria Port Canada in Harria Port Januari Davata in Harrian Canada in Harian Canada in Harrian Canada in	ght (c) 2020 American No - American Hegatrends In orn Configuration Socie Settings direction licy ation	partonds Unternational, LLC. ternational, LLC. Locality and a series to the series of the series o
Aptio Setup Aptio Setup Main Advanced Alors Main Advanced Alors Main Advanced Alors Main Mark Alors Main Mark Alors Mark	ght (c) 2020 American No - American Hegatrends In orn Configuration Socie Settings direction licy ation	parends Netternortenally LLC ternational, LLC, lConfiguration Server Allows the inter to respect to the inter to black Screen inter the
Aptio Setup Aptio Setup Hann Advanced Slove Heart Advanced Slove Heartal Port Conside re failed for Consider Re failed and Consider Re failed and Spatial State State State Heart State Configuration Whe Configuration Whe Configuration Configuration Sci Configuration	ght (c) 2020 American No - American Hegatrends In orn Configuration Socie Settings direction licy ation	ternational, it.C. ternational, it.C. Homispical waves of the second s
Actor 2423 1522 copyet Aptio Setup Main Advanced 2152 Main Advanced 2152 Main Mort Devices Main Mort Devices Main Mort Devices Main Mark Devices Main Mark Mark Mark Mark Devices Sciences Sciences Sciences Sciences Mark Devices Mark Devices	ght (cl.202) Annatan Mo - Aperican Appartends In an Lentinum School Settings diverien Licy atton	proved since a line and a line
Anto 2022 State 2022 Conjust Aptico State Anton Advanced 2 Jakas Median Not Thereface Herian Port Console Re I Consiguration Data Consiguration NMP Configuration NMP Configuration	<pre>c.ccccm/rss/version inc - Assrctan Registends In - Assrctan Registends In - Assrctant - Assrctant</pre>	percent contractions, suc terrational, LLC This former allow the - lacet is sample fail - lacet is sample fail - lacet contractor - in the contract of the - inter- - in
APTE Study of Congress APTE Study of Congress Aptendiate States and Congress Applications of Congress Applied States and Congress Applied Applied States Applied Applied States Applied	<pre>pht (ch2:0) Average for - Average for the second for - Control (ch2) average - Control (ch2) - Cont</pre>	Interesting of the state of the
Artso setup Artso setup artso activity and a setup and artsonal and a artsonal	<pre>c.compression c.compressi</pre>	percent discretion for the sur- ternational, the destination of the second percent of this format allows the subset of the final (in the second subset) of the final (in the subset) of the final (in the subset) of the second s
APTE Study of Congress APTE Study of Congress Aptendiate States and Congress Applications of Congress Applied States and Congress Applied Applied States Applied Applied States Applied	<pre>c.compression c.compressi</pre>	Interesting of the state of the



Create RAID

Choose the RAID Type (0 or 1)

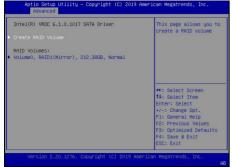
Choose which **drive** will be used.

Choose the **capacity** ,

The RAID is a software RAID , the size and type can be different using multiple partition with same drives.

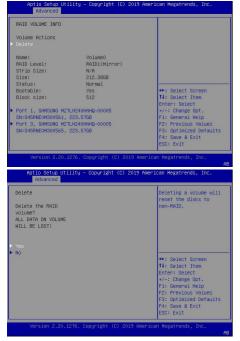


The VROC Module allow to create up to two Different RAID using the same Drives.



Delete RAID

Choose the RAID from the main menu list, then choose **Delete** and apply the change.



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

To access the Management console, during the boot, press *CTRL+1* 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 $\ensuremath{\mathsf{complete}}$ the process, Press $\ensuremath{\mathsf{ENTER}}$.



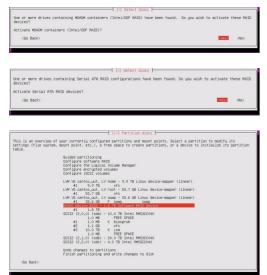
How the OS manage the RAID ?

The Linux see a mdadm RAID.

[root @SYSTEM ~]# lsblk ... sdd 8 : 48 0 894 .3G 0 disk └─mdl26 9 : 126 0 1 .7T 0 raid0 sde 8 : 64 0 894 .3G 0 disk └─mdl26 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)

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINT
sda	8:0		9.1T		disk	
sdb	8:16		21.8T		disk	
	8:32		3.7T		disk	
	8:48		894.3G		disk	
-md126	9:126		1.7T		raid0	
	8:64					
-md126	9:126		1.7T		raid0	

Centos 7.4

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

[root@localhost ~						
name	MAJ:MIN				TYPE	MOUNTPOINT
sda	8:0	0	447.1G		disk	
-md126	9:126	0	424.8G	0	raid1	
	259:0	0		0	md	/boot
_md126p2	259:1	0	423.8G	0	md	
-centos-root	253:0	0	50G	0	lum	
-centos-swap	253:1		31.3G	0	lum	[SWAP]
-centos-home	253:2	0	342.5G	8	lum	/home
sdb	8:16	0	447.1G	0	disk	
L_md126	9:126	8	424.8G	0	raid1	
-md126p1	259:0	0	1G	8	md	/boot
_md126p2	259:1	0	423.8G	0	md	
-centos-root	253:0	0	50G	0	lum	
-centos-swap	253:1	0	31.3G	8	lum	[SWAP]
-centos-home	253:2	0	342.5G	0	lum	/home
sdc	8:32	0	9.1T	0	disk	
sdd	8:48	0	21.8T	8	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 1350, 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	CG2400 server> ./bootutil64e Connection to QV driver failed - please reinstall it! Intel(Q) Element Flash Firmare Utility BootUtil version 1.7.10.10 Copyright (C) 2003-2019 Intel corporation Type BootUtil -7 for help Port Network Address Location Series WOL Flash Firmware Version 1 00A0ASDAC710 26:00.1 40Gbe YES UEFT,PXE Enabled 1.1.09 2 00A0ASDAC712 26:00.1 40Gbe YES UEFT,PXE Enabled 1.1.09 3 se4959.142001 59:00.0 Gigabit YES FLASH Disabled 4 se4959.945040 1.00.0 10Gbe YAS UEFT,PXE Enabled 5 se3059.945040 1.00.0 10Gbe YAS UEFT,PXE Enabled 5 se3059.945040 1.00.0 10Gbe YAS UEFT,PXE Enabled
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]	CG2400 server> /bootutil64e -FLASHENABLE -NICe3 Connection to QV driver failed - please reinstall it! Rebot the system to enable the boot ROM on this port Port Network Address Location series WOL Flash Firmware version
Step_3	To apply the modifications, r LocalServer_OSPrompt:~# r	,
Step_4	Access the BIOS menu. Refe	r to <u>Accessing the BIOS</u> 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.	Aprilo Setup - American Megatrends International, LLC. C Security Foot Save & Exit Boot Option Priorities A [Sets the system boot Boot Option Priorities A [Sets the system boot Horder C Utra NS-So 1 Generic Utra NS-So 1 Generic Utra NS-So 1 Generic Utra NS-So 1 Generic Trafisson (S) Ethernet Connection X722 for 1068ASE-T * UEFI: NPL TP4 Intel(8) Ethernet Connection X722 for 1068ASE-T * UEFI: NPL TP4 Intel(8) Ethernet Connection X722 for 1068ASE-T * UEFI: NPL TP4 Intel(8) Ethernet Connection X722 for 1068ASE-T * UEFI: NPL TP4 Intel(8) Ethernet Connection X722 for 1068ASE-T * UEFI: NPL TP4 Intel(8) Ethernet Connection X722 for 1068ASE-T * UEFI: NPL TP4 Intel(8) Ethernet Connection X722 for 1068ASE-T + UEFI: NPL TP4 Intel(8)

Provisioning custom secure boot keys

Table of contents

Introduction

- Updating secure boot keys from the UEFI setup utility
 - <u>Prerequisites</u>
 - Procedure

Introduction

This article describes how to provision a custom set of Secure Variables used as part of the Secure Boot feature.

Secure Boot is a UEFI-defined feature used to authenticate a UEFI executable, such as an OS loader, using digital signing mechanisms based on the Public Key Infrastructure process, reducing the risks of pre-boot malware attacks. The feature uses a database of authorized signatures to confirm the UEFI executable integrity prior to execution. Boards will typically have a pre-loaded set of Platform Key (PK), Key Exchange Keys (KEK), authorized signature database (db) and blacklisted / revoked signature database (dbx) as defined by the OEM, as well as some industry-standard certificates issued by Microsoft that allow booting Windows or well-known Linux distributions such as Ubuntu. It may be desirable for an end customer to update these keys with their own set for security reasons.

This document assumes the reader has some knowledge about the Secure Boot process, and that the required set of keys and certificates has been properly generated. The following link provides guidelines on creating and managing such keys and certificates:

https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/windows-secure-boot-key-creation-and-management-guidance

Updating secure boot keys from the UEFI setup utility

Prerequisites

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.				
Rel	Relevant section:				
Gen	enerating custom secure boot keys				

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.	<image/> <section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>
Step_2	Access the Secure Boot submenu from the Security tab.	Bound Setue Utility - Scopright (2) 2020 American Megatrends, Inc. Bound Setue Utility - Scopright (2) 2020 American Megatrends, Inc. F ONLY the Administrator's passand is set, then this only limits access to Setue and is set. If ONLY the User's passand as set. in but only limits access to Setue and is the other will the passand issent mass the interest to boot or enter Setue. In Setue to User will the passand issent mass the interest to Boot or enter Setue. In Setue to User will the passand issent mass the interest to Boot or enter Setue. The Setue to User will the Passand Issent mass the interest to Boot or enter Setue. In Setue 1000 The Passand Issent Mass to Boot or enter Setue. Administrator Passand User will the Passand Issent Boot or enterest to Boot or enter Setue. Maximum length 20 Administrator Passand User will the Passand Issent Boot Or Boot Devices Volume Setue to Setue 1000 The Se
Step 3	Access the Kev Management page by selecting the Kev Management menu item.	

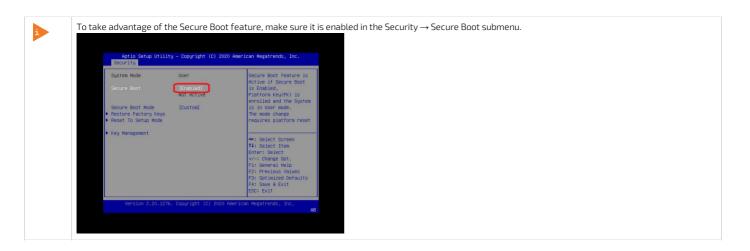
www.kontron.com

Step_4	Default Factory Keys should already be provisioned, as identified by the "Factory" attribute in	Aprilo Setup Utility - Copyright (C) 2020 American Hegatrends, Inc. Secure Boot Usen Not retry Combines expert users to modify Secure Boot Node Isetor Factory Keys Restor Factory Keys Factor Secure Boot Factory Merida Secure Boot Node Isetor Factory Keys Merida Secure Boot Factory Factor Secure Boot Factory Merida Secure Boot Rode Isetor Factory Keys Merida Secure Boot Factory Here Secure Factory Merida Secure Factory Keys Here Secure Factory Keys Merida Secure Factory Keys Here Secure Factory Keys </th
	the Key Source column in the Secure Boot variable table. To replace the default Platform Key with your own, select Platform Key(PK) .	Aprile Setup Utility - Copyright (c) 2020 American Megatrends, Inc. Becurity Factory Key Provision [Enabled] Martor Factory Key Martor Factory Key Boord Secure Boot vacables Brooll Effigure Device Guard Ready Restore Rod defaults Brools Efficience Boot devicibles Brools Efficience Boot devicibles Brools Efficience Boot devices Period Boot Secure Boot devices Broot Boot Boot devices Broot Boot Boot devices Broot devi
Step_5	Select Update from the pop-up window.	Antio Setup Utility - Copyright (C) 2020 American Hegatrends, Inc. Decoring Fractory Key Provision Enabled] Fractory Key Provision Enabled] Fractory Key Provision Bestor Board Board Key Platform Key(Pk) Benove Vier Finish Benove Vier Finish Benove Vier Finish Benove Vier Finish <tr< th=""></tr<>
Step_6	Select No to load a key from an external media.	Actio Setup Utility - Dopyright (C) 2020 American Hegatrends, Inc. Security Factory Key Provision (Enabled) Mestore Factory Keys Secure Bourd Be Perice Buard Be Secure Bourd Be Se
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.	Aprilo Setus Utility - Copyright (C) 2020 Ascrilan Hegatrends, Inc. Security Fractory key Provision [Enabled] Bestore Fractory keys Bestore Fractory keys Bestore Bestore Bestore Bestore Bestore Science
Step_8	From the list of files, select the Public Certificate file for the Platform Key (PK.cer in this example).	Actic Setup Utility - Copyright (C) 2020 American Hegatrends, Inc. Security Factory key Provision [Enabled] Factory key Factory keys Resort Factory keys Resort Secure Body Secure Body Control Liceta (Liceta) Control Liceta (Liceta) Contro

		 Encoll Eff Image Encoll Eff Image Recore Rectore De defaults Rectore De defaults Secure Boot variable Size keys key Source Rectore De defaults Rectore De defaults Rectore Boot variable Size keys key Source Rectore Boot variable Size keys key Source Rectore Boot variable Size keys key Source Rectore Boot variable Size keys Factory Retroited House Size Factory Retroited House Size Factory Retroited House O O No Keys General Network Keys Size Factory Retroited House O O No Keys General Network Size Copyright (c) 2020 American Heystrends, Inc.
Step_9	Specify that the file format is Public Key Certificate .	Actio Setup Utility - Copyright (c) 2020 American Hegatrands, inc. Excurs y Factory Key Provision (Enabled) Pactory Key Provision
Step_10	Select Yes to confirm Platform Key update.	Actio Setup Utility - Copyright (C) 2020 American Hegatrends, Inc. Executive Factory Key Provision (Enabled) Restore Factory Key Sectore Sectore Boat variables Device Guard R Option 161 Jan Secure Boat variables Device Guard R Option 161 Jan Secure Boat variables Device Guard R Option 161 Jan Nenove "UFF" C Secure Boat M Nenove "UFF" C Nethorized Tinseringes Cole
Step_11	Confirm that the update completed successfully. The table should now show that a key was added from an "External" Key Source.	Actio Setus Utility - Copyright (c) 2020 American Megatrends, Inc. Ecourity Fractory Kay Provision [Enabled] Prestor Factory Kay Provide Guard Gready Provide Guard
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. 	Actio Setus Utility - Cocyright (c) 2020 American Hegatrends, Inc. Ecourity Fractory Key Provision [Enabled] Fractory Key Provision [Enabled] Fractor
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".	Artio Setus Ufility - Copyright (C) 2020 American Megatrends, Inc. Security Factory Key Provision (Enabled) Pestore Factory Keys Pestore Factory variables Periodi Factory Variables Periodi Factory Variables Periodi Factory Keys Periodi Factory Keys Period

▶ OsRecovery Signatures 0 0 No Keys ▼ F4: Save & Exit		Signatures TimeStamps		ctory Keys	F2: Previous Values F3: Optimized Defaults
				2020 Hill	n Megatrends, Inc. A

Step_14	 Select Authorized Signatures to add an authorized Public Key certificate to the db. As f Selecting Update from the pop-up window will erase the pre-provisioned db entries a 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. 	and add a new certificate as a single entr	y;
Step_15	Select Save Changes and Exit from the Setup Utility.	Actio Setup Utility - Coopright (4 Security Sont Stats) See Danges and Fill Discard Changes and Fill Discard Changes and Reset Discard Changes) 2020 American Hegatrends, Inc. A Exit system serve after saving the changes.
		Discard Changes Default Options Restore Defaults Save as Usen Defaults Boot Override ubonts (INTEL SEGPEBRF51208) Version 2020,1876, Oppuright (c)	 **: Select Screen 4*: Select Screen 4: Select Tem 5: Change Obt, 7: General Heis 7: General Heis 7: General Heis 7: General Genults 7: General Constructs



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 <u>https://github.com/freshautomations/efitools-centos/releases/download/2019-05-12/efitools-v1.9.2-1.x86_64.rpm</u> wget <u>https://github.com/freshautomations/efitools-centos/releases/download/2019-05-12/sbsigntools-v0.9.2-1.x86_64.rpm</u> wget <u>https://www.rodsbooks.com/efi-bootloaders/mkkeys.sh</u> 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

- <u>Application commands</u>
 - IPM device commands
 - <u>Watchdog timer commands</u>
 - <u>BMC device and messaging commands</u>
 - IPMI 2.0 specific commands
 - Chassis commands
- Bridge commands
 - <u>Bridge management commands</u>
 - <u>Bridge discovery commands</u>
 - Bridging commands
 - Bridge event commands
- <u>Sensor event commands</u>
- <u>Storage commands</u>
 - FRU information commands
 - SDR repository commands
 - <u>SEL device commands</u>
- <u>Transport commands</u>
 - IPM device commands
 - Serial over LAN commands
- AMI commands
- AMI restore factory default settings command
- Kontron OEM commands

Application commands

IPM device commands

Net function	Command	Command name	Supported / Unsupported	M/0
0x06	0×01	Get Device ID	Supported	м
0x06	0x02	Cold Reset	Supported	0
0x06	0x03	Warm Reset	Unsupported *	0
0x06	0×04	Supported		м
0×06	0x05	Manufacturing Test On	Unsupported *	0
0×06	0×06	Set ACPI Power State	Supported	0
0x06	0×07	Get ACPI Power State	Supported	0
0×06	0×08	Get Device GUID	Supported	0
0×06	0×09	Get NetFn Support	Supported	0
0x06	0x0A	Get Command Support	Supported	0
0x06	0x0C	Get Configurable Commands	Supported	0
0×06	0x60	Set Command Enables	Supported	0
0×06	0x61	Get Command Enables	Supported	0
0x06	0x64	Get OEM NetFn IANA Support	Supported	0
0x06	0×0B	Get Command Sub-function Support	Supported	0
0x06	0x0D	Get Configurable Command Sub-functions	Supported	0
0x06	0x62	Set Command Sub-function Enables	Unsupported	0
0x06	0x63	Get Command Sub-function Enables	Unsupported	0
0×06	0×52	Master Write-Read	Supported	0

* Commands are not rejected and can cause unpredictable behavior.

Watchdog timer commands

Net function	Command	Command name	Supported / Unsupported	M/0
0x06	0x22	Reset Watchdog Timer	Supported	М
0×06	0x24	Set Watchdog Timer	Supported	М
0x06	0x25	Get Watchdog Timer	Supported	М

Net function	Command	Command name	Supported / Unsupported	M/0
0×06	0x2E	Set BMC Global Enables	Supported	м
0×06	0x2F	Get BMC Global Enables	Supported	М
0×06	0x30	Clear Message Flags	Supported	м
0×06	0x31	Get Message Flags	Supported	м
0×06	0x32	Enable Message Channel Receive	Supported	0
0×06	0x33	Get Message	Supported	м
0×06	0x34	Send Message	Supported	м
0×06	0x35	Read Event Message Buffer	Supported	0
0×06	0x37	Get System GUID	Supported	0
0×06	0x38	Get Channel Authentication Capabilities	Supported	0
0×06	0x39	Get Session Challenge	Supported	0
0×06	0x3A	Activate Session	Supported	0
0×06	0x3B	Set Session Privilege Level	Supported	0
0×06	0x3C	Close Session	Supported	0
0×06	0x3D	Get Session Info	Supported	0
0×06	0x3F	Get AuthCode	Supported	0
0×06	0x40	Set Channel Access	Supported	0
0×06	0x41	Get Channel Access	Supported	0
0×06	0x42	Get Channel Info Command	Supported	0
0×06	0x43	Set User Access Command	Supported	0
0×06	0x44	Get User Access Command	Supported	0
0×06	0x45	Set User Name	Supported	0
0x06	0x46	Get User Name Command	Supported	0
0x06	0x47	Set User Password Command	Supported	0
0x06	0x52	Master Write-Read	Supported	М
0x06	0x58	Set System Info Parameters	Supported	0
0x06	0×59	Get System Info Parameters	Supported	0

IPMI 2.0 specific commands

Net function	Command	Command name	Supported / Unsupported	M/0
0×06	0x48	Activate Payload	Supported	0
0×06	0x49	Deactivate Payload	Supported	0
0x06	0x4A	Get Payload Activation Status	Supported	0
0x06	0x4B	Get Payload Instance Info	Supported	0
0×06	0x4C	Set User Payload Access	Supported	0
0x06	0x4D	Get User Payload Access	Supported	0
0x06	0x4E	Get Channel Payload Support	Supported	0
0x06	0x4F	Get Channel Payload Version	Supported	0
0x06	0×50	Get Channel OEM Payload Info	Supported	0
0x06	0x54	Get Channel Cipher Suites	Supported	0
0x06	0x55	Suspend/Resume Payload Encryption	Supported	0
0x06	0x56	Set Channel Security Keys	Supported	0
0×06	0×57	Get System Interface Capabilities	Supported	0

Chassis commands

Net function	Command	Command name	Supported / Unsupported	M/0
0×00	0×00	Get Chassis Capabilities	Supported	Μ
0×00	0×01	Get Chassis Status	Supported	Μ
0×00	0x02	Chassis Control	Supported	Μ
0×00	0x04	Chassis Identify	Supported	0
0×00	0×05	Set Chassis Capabilities	Supported	0
0×00	0x06	Set Power Restore Policy	Supported	0
0×00	0×07	Get System Restart Cause	Supported	0
0×00	0x08	Set System Boot Options	Supported	0
0×00	0×09	Get System Boot Options	Supported	0
0×00	0x0A	Set Front Panel Button Enables	Supported	0
0×00	0×0B	Set Power Cycle Interval	Supported	0
0×00	0×0F	Get POH Counter	Supported	0

Bridge commands

B ridge management commands

Net function	Command	Command name	Supported / Unsupported	M/0
0x02	0×00	Get Bridge State	Unsupported	0
0x02	0×01	Set Bridge State	Unsupported	0
0x02	0x02	Get ICMB Address	Unsupported	0
0x02	0x03	Set ICMB Address	Unsupported	0
0x02	0x04	SetBridgeProxyAddress	Unsupported	0
0x02	0x05	Get Bridge Statistics	Unsupported	0
0x02	0x06	Get ICMB Capabilities	Unsupported	0
0x02	0x08	Clear Bridge Statistics	Unsupported	0
0x02	0×09	GetBridge Proxy Address	Unsupported	0
0x02	0×0A	Get ICMB Connector Info	Unsupported	М

Bridge discovery commands

Net function	Command	Command name	Supported / Unsupported	M/0
0x02	0×10	Prepare For Discovery	Unsupported	0
0x02	0x11	Get Addresses	Unsupported	0
0x02	0x12	Set Discovered	Unsupported	0
0x02	0x13	Get Chassis Device Id	Unsupported	0
0x02	0x14	Set Chassis Device Id	Unsupported	0

Bridging commands

Net function	Command	Command name	Supported / Unsupported	M/0
0x02	0×20	Bridge Request	Unsupported	0
0x02	0×21	Bridge Message	Unsupported	0

Bridge event commands

Net function	Command	Command name	Supported / Unsupported	M/0
0x02	0x30	Get Event Count	Unsupported	0
0x02	0x31	Set Event Destination	Unsupported	0
0x02	0x32	Set Event Reception State	Unsupported	0
0×02	0x33	SendICMB Event Message	Unsupported	0
0x02	0x34	Get Event Destination	Unsupported	0
0x02	0x35	Get Event Reception State	Unsupported	0

Sensor event commands

Net function	Command	Command name	Supported / Unsupported	M/0
0x04	0x00	Set Event Receiver	Supported	М
0x04	0x01	Get Event Receiver	Supported	М
0x04	0x02	Platform Event	Supported	М
0x04	0×10	Get PEF Capabilities	Supported	М
0x04	0x11	Arm PEF Postpone Timer	Supported	м
0x04	0x12	Set PEF Configuration Parameters	Supported	Μ
0x04	0x13	Get PEF Configuration Parameters	Supported	М
0x04	0x14	Set Last Processed Event ID	Supported	М
0x04	0x15	Get Last Processed Event ID	Supported	М
0x04	0x16	Alert Immediate	Supported	0
0x04	0x17	PET Acknowledge	Supported	0
0x04	0×20	Get Device SDR Info	Supported	0
0x04	0x21	Get Device SDR	Supported	0
0x04	0x22	Reserve Device SDR Repository	Supported	0
0x04	0x23	Get Sensor Reading Factors	Supported	0
0x04	0x24	Set Sensor Hysteresis	Supported	0
0x04	0x25	Get Sensor Hysteresis	Supported	0
0x04	0x26	Set Sensor Threshold	Supported	0
0x04	0x27	Get Sensor Threshold	Supported	0
0x04	0x28	Set Sensor Event Enable	Supported	0
0x04	0x29	Get Sensor Event Enable	Supported	0
0x04	0x2A	Re-arm Sensor Events	Supported	0
0x04	0x2B	Get Sensor Event Status	Supported	0
0x04	0x2D	Get Sensor Reading	Supported	М
0x04	0x2E	Set Sensor Type	Supported	0
0x04	0x2F	Get Sensor Type	Supported	0
0x04	0x30	Set Sensor Reading And Event Status	Supported	0

Storage commands

FRU information commands

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

SDR repository commands

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

SEL device commands

Net function	Command	Command name	Supported / Unsupported	M/0
0x0a	0x40	Get SEL Info	Supported	Μ
0x0a	0x41	Get SEL Allocation Info	Supported	0
0x0a	0x42	Reserve SEL	Supported	0
0x0a	0x43	Get SEL Entry	Supported	Μ
0x0a	0x44	Add SEL Entry	Supported	Μ
0x0a	0×45	Partial Add SEL Entry	Supported	Μ
0x0a	0x47	Clear SEL	Supported	Μ
0x0a	0x48	Get SEL Time	Supported	Μ
0x0a	0x49	Set SEL Time	Supported	Μ
0x0a	0x5C	Get SEL Time UTC OffSet	Supported	0
0x0a	0x5D	Set SEL Time UTC OffSet	Supported	0

Transport commands

IPM d evice commands

Net function	Command	Command name	Supported / Unsupported	M/0
0х0с	0×01	Set LAN Configuration Parameters	Supported	Μ
0х0с	0x02	Get LAN Configuration Parameters	Supported	Μ
0х0с	0x03	Suspend BMC ARPs	Supported	0

Serial over LAN commands

Net function	Command	Command name	Supported / Unsupported	M/0
0х0с	0x22	Get SOL Configuration Parameters	Supported	0
0х0с	0x21	Set SOL Configuration Parameters	Supported	0

AMI commands

Net function	Command	Command name	Supported / Unsupported	M/0
0×32	0×66	Restore Defaults	Supported	0

Kontron OEM commands

Net Function	Command	Command Name	Supported/Unsupported	M/0
ОхЗс	0×0A	Override Minimum Fan Speed	Supported	0
NOTE: M/O = Mandatory/Opt	ional			

Supported Redfish commands

Table of contents

- <u>Miscellaneous URLs</u>
- System URLs
- <u>Manager URLs</u>
- Telemetry URLs
- <u>Chassis URLs</u>

<u>Account service URLs</u>

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
P-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
P-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::ipReasmRegds	Number of IP fragments received which needed to be reassembled at this entity.	GET

www.kontron.com

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	GET
	deleted. If new objects are added to the ipIfStatsTable that require the ipIfStatsTableLastChange to be updated when they are modified, they must specify that requirement in their description clause.	
IP-MIB::ipIfStatsTable	The table containing per-interface traffic statistics. This table and the ipSystemStatsTable contain similar objects whose difference is in their granularity. Where this table contains per-interface statistics, the ipSystemStatsTable contains the same statistics, but counted on a system wide basis.	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 <u>http://oidref.com/1.3.6.1.2.1.4.33</u>	GET
IP-MIB::ipAddressTable	This table contains addressing information relevant to the entity's interfaces. More information can be found here <u>http://oidref.com/1.3.6.1.2.1.4.34</u>	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
P-MIB::ipDefaultRouterTable	The table used to describe the default routers known to this entity.	GET TABLE
P-MIB::icmpInMsgs	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.	GET
P-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
P-MIB::icmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.	GET
IP-MIB::icmpInTimeExcds	Number of ICMP Time Exceeded messages received.	GET
P-MIB::icmpInParmProbs	Number of ICMP Parameter Problem messages received.	GET
P-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. www.kontron.com	GET

www.kontron.com

P-MIB::icmpInEchos	Number of ICMP Echo (request) messages received.	GET
P-MIB::icmpInEchoReps	Number of ICMP Echo Reply messages received.	GET
P-MIB::icmpInTimestamps	Number of ICMP Timestamp (request) messages received.	GET
P-MIB::icmpInTimestampReps	Number of ICMP Timestamp Reply messages received.	GET
P-MIB::icmpInAddrMasks	Number of ICMP Address Mask Reguest messages received.	GET
P-MIB::icmpInAddrMaskReps	Number of ICMP Address Mask Reply messages received.	GET
P-MIB::icmpOutMsgs	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all	GET
P-MIB::icmpOutErrors	The route of ICMP messages which this entity did not send due to problems discovered within ICMP such as	GET
	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.	
P-MIB::icmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.	GET
P-MIB::icmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.	GET
P-MIB::icmpOutParmProbs	The number of ICMP Parameter Problem messages sent.	GET
P-MIB::icmpOutSrcQuenchs	The number of ICMP Source Quench messages sent.	GET
P-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
P-MIB::icmpOutEchos	The number of ICMP Echo (request) messages sent.	GET
P-MIB::icmpOutEchoReps	The number of ICMP Echo Reply messages sent.	GET
P-MIB::icmpOutTimestamps	The number of ICMP Timestamp (request) messages sent.	GET
P-MIB::icmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.	GET
P-MIB::icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.	GET
P-MIB::icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.	GET
-MIB::icmpStatsTable	The table of generic system-wide ICMP counters.	GET TAE
P-MIB::icmpMsgStatsTable	The table of system-wide per-version, per-message type ICMP counters.	GET TAE
CP-MIB::tcpRtoAlgorithm	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.	GET
CP-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.	
CP-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
CP-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
CP-MIB::tcpActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.	GET
CP-MIB::tcpPassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.	GET
CP-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
CP-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
CP-MIB::tcpCurrEstab	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.	GET
CP-MIB::tcpInSegs	The total number of segments received, including those received in error. This count includes segments	GET
	received on currently established connections.	
CP-MIB::tcpOutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.	GET
CP-MIB::tcpRetransSegs	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.	GET
CP-MIB::tcpConnTable	A table containing TCP connection-specific information.	GET TAE
CP-MIB::tcpInErrs	The total number of segments received in error (e.g., bad TCP checksums).	GET

ILP-MIB::tcpLonnectionState	The state of this TLP connection. More information can be found here <u>https://oidref.com/1.3.6.1.2.1.6.12</u>	uΕ Ι
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 <u>https://oidref.com/1.3.6.1.2.1.6.20</u>	GET TABLE
JDP-MIB::udpInDatagrams	The total number of UDP datagrams delivered to UDP users.	GET
JDP-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
JDP-MIB::udpOutDatagrams	The total number of UDP datagrams sent from this entity.	GET
JDP-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
5NMPv2-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
5NMPv2-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
5NMPv2-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
5NMPv2-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
5NMPv2-MIB::snmpInGetRequests	The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity.	GET
5NMPv2-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
5NMPv2-MIB::snmpInTraps	The total number of SNMP Trap PDUs which have been accepted and processed by the SNMP protocol entity.	GET
5NMPv2-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
5NMPv2-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
5NMPv2-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
5NMPv2-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. www.kontron.com	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
5NMPv2-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
5NMPv2-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 TABL
MTA-MIB::mtaGroupTable	The table holding information specific to each MTA group.	GET TABI
F-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 TABI
F-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
PV6-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 <u>https://oidref.com/1.3.6.1.2.1.55.1.1</u>	GET
PV6-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
PV6-MIB::ipv6Interfaces	The number of IPv6 interfaces (regardless of their current state) present on this system.	GET
PV6-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 TABI
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 <u>https://oidref.com/1.3.6.1.2.1.88.1.1.1</u>	GET
DISMAN-EVENT- MIB::mteResourceSampleInstanceMaximum	The maximum number of instance entries this system will support for sampling. More information can be found here <u>https://oidref.com/1.3.6.1.2.1.88.1.1.2</u>	GET
DISMAN-EVENT- AIB::mteResourceSampleInstances	The number of currently active instance entries as defined for mteResourceSampleInstanceMaximum.	GET
DISMAN-EVENT- NIB::mteResourceSampleInstancesHigh	The highest value of mteResourceSampleInstances that has occurred since initialization of the management system.	GET
DISMAN-EVENT- AlB::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 TAB
DISMAN-EVENT-MIB::mteEventTable	A table of management event action information.	GET TABI

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/1.3.6.1.2.1.92.1.11	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
5NMPv2-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

- <u>AMISCE download</u>
- BIOS default values
- <u>Tool name to use</u>
- Defining what values need to be configured
- Installing AMISCE
- UEFI Shell
- Operating the AMISCE tool use case 1 multiple changes
 - <u>Extracting all the BIOS options</u>
 - <u>Extracting only modified BIOS options</u>
 - Importing the modified set of BIOS options
- Operating the AMISCE tool use case 2 few changes
 - <u>Get all BIOS setup options</u>
 - Get one BIOS Setup option
 - <u>Getting one BIOS Setup option with Map String value</u>
 - <u>Getting one BIOS Setup option without Map String value</u>
 - Set one BIOS Setup option
 - Set one BIOS Setup option with a Map String value
 - <u>Set one BIOS setup option without a Map String value</u>
- Operating the AMISCE tool use case 3 changing the boot order
- Operating the AMISCE tool use case 4 passwords
 - <u>Setting a password</u>
 - Modifying a password

Introduction

The AMISCE command line tool is recommended for parallel and/or automated BIOS configuration. The AMISCE tool is mainly used to extract the modified BIOS Setup option values in a file. It can then be used to either modify these values or ultimately apply 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 <u>www.kontron.com</u>, 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 <u>Restoring default BIOS settings using the BIOS menu</u> 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:

05 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.

tep_1	p_1 (Optional) Access the BIOS. Go into the BIOS Setup menu. Navigate to Save & Exit \rightarrow Restore Defaults (or use F3: Optimized Defaults). N Changes and Reset.	
5tep_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 export and boot order controls in the generated script file. /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 CMD line option that produces a verbose script file. 	Output example: // Script File Name : MySet.txt // Created on 10/21/19 at 10:11:12 // Copyright (c) 1985-2019, American Megatrer 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 desire Option *[01]Enabled Setup Question = Ipv4 PXE Support Map String = NWSK001 []

NOTES:

- In the Setup script file generated (${\bf MySet.txt}$):

• 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 \rightarrow 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: Keep the header of original MySet.txt up to and including the HIICrc32 line. Add a comment in the header to describe the modifications. 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".
	<pre>// 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 []</pre>

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 cannot be used over different BIOS versions. Extracting in BIOS version X and importing in BIOS version Y is not possible nor recommended.
- There is an optional command /reboot to reboot/restart the system after any variable modification by AMISCE. Please close other processes in the OS before using this command.
- There is an optional command /shutdown to shut down the system after any variable modification by AMISCE. Please close other processes in the OS before using this command.

Operating the AMISCE tool - use case 2 - few changes

This section describes how to extract every BIOS option to apply them to another system when there are few changes. It provides one typical use cases for using the AMISCE tool.

The AMISCE tool provides many command-line options.

Get all BIOS setup options

Step_1	D_1 (Optional) Access the BIOS. Go into the BIOS Setup menu. Navigate to Save & Exit → Restore Defaults (or use F3: Optimized Defaults). Navig Changes and Reset.		
Step_2	 Changes and Reset . 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 export approximation of boot order controls in the generated script file. /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. 	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 \sf /sd option.
- AMISCE will not import commented out questions (generated mainly by /v). It will treat commented out questions as if they do not exist in the script. To import a commented out question, users have to remove the comment out symbols //. The comments will also show BIOS Setup menu titles, which may be useful to correctly identify setup questions and their map strings for when BIOS Setup sub-menus have similar options (e.g. for the PCIe Bridges).

Get one BIOS Setup option

- There are two cases when getting one BIOS Setup options:
 - When there is a Map String value
- When there is no Map String value

IMPORTANT: If a BIOS Setup option has a Map String it is highly recommended to use it to set the option as this is much faster. The AMISCE can read/modify such options without a Map String, but according to our tests, it takes a very long time (about 1 minute) to complete.

Getting one BIOS Setup option with Map String value

Step_1	To read the value of the BIOS Setup option, its Map String value is needed. Get the Map String value 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: F51:\> 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

p_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]</device></question_value>	Example: SceEfi64.efi /i /ms PCIS007 /qv 01 /lang en-US /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	

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 <u>Factory default</u> 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</question_value> 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 provides one typical use cases for using the AMISCE tool.

The Map String to define the Boot Order device list is "SETUP006".

Step_1	Get the current Boot Order.	Output example:
	[AMISCE] /o /lang en-US /ms SETUP006 /ds /hb	ListOrder =
		[000f] UEFI: Built-in EFI Shell
	That example returns a list with 7 boot devices, with indexes: [000f], [0001], [000d], etc.	[0001] CentOS
	NOTE: The index allocated to a boot device (for instance [000f] for the "UEFI: Built-in EFI Shell" in the above example) can	[000d] UEFI: PXE IP4 Intel(R)
	vary from system to system. This means that before changing the Boot Order of a particular system, its current device list	Ethernet Connection X722 for
	must be read first to be able to define and import a new boot order.	10GBASE-T
		[0006] UEFI: SanDisk, Partitio
		1
		[0005] UEFI: Memorex TD
		Classic 003B PMAP, Partition
		[000e] UEFI: PXE IP4 Intel(R)
		Ethernet Connection X722 for
		10GBASE-T
		[0002] UEFI: PXE IP4 America
		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="">".</question>	Example:
	[AMISCE] /i /lang en-US /ms SETUP006 /qv "index1,index2,index3,index4,index5,index5,index7 " /hb	SceEfi64.efi /i /lang en-US
	Question value imported successfully	/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 password="" user=""> /lang en-US /hb</new></new>
	OU
	[AMISCE] /apwdf <file admin="" having="" new="" password=""> /upwdf <file having="" new="" password="" user=""> /lang en-US /hb</file></file>

Modifying a password

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

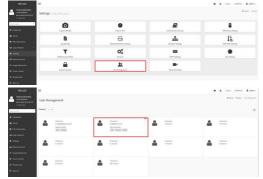
\$ apt-get install snmp

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.20974.554.2.1.21 = 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
5NMPv2-MIB::sysName.0	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.	GET SET
5NMPv2-MIB::sysLocation.0	The physical location of this node (e.g., `telephone closet, 3rd floor').	GET SET
5NMPv2-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 TABL
F-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 TABL
.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
P-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
P-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
P-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
P-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
P-MIB::ipInUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.	GET
P-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
P-MIB::ipInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).	GET
P-MIB::ipOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for	GET

www.kontron.com

	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
P-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
P-MIB::ipReasmReqds	Number of IP fragments received which needed to be reassembled at this entity.	GET
P-MIB::ipReasmOKs	Number of IP datagrams successfully re-assembled.	GET
P-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
P-MIB::ipFragCreates	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.	GET
P-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
P-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 TABL
1.3.6.1.2.1.4.21	IP Routing table.	GET
P-MIB::ipNetToMediaTable	IP Address Translation table used for mapping from IP addresses to physical addresses.	GET TABL
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
P-FORWARD-MIB::ipCidrRouteTable	This entity's IP Routing table.	GET TABL
P-FORWARD-MIB::inetCidrRouteNumber	The number of current ipCidrRouteTable entries that are not invalid.	GET
P-FORWARD-MIB::inetCidrRouteTable	This entity's IP Routing table.	
P-MIB::ipv6lpForwarding	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
P-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 iplfStatsTable contain similar objects whose difference is in their granularity. Where this table contains system wide traffic statistics, the iplfStatsTable contains the same statistics but counted on a per-interface basis.	GET TABL
IP-MIB::ipIfStatsTableLastChange	The value of sysUpTime on the most recent occasion at which a row in the ipIfStatsTable was added or	GET
	deleted. If new objects are added to the iplfStatsTable that require the iplfStatsTableLastChange to be updated when they are modified, they must specify that requirement in their description clause.	
IP-MIB::ipIfStatsTable	The table containing per-interface traffic statistics. This table and the ipSystemStatsTable contain similar objects whose difference is in their granularity. Where this table contains per-interface statistics, the ipSystemStatsTable contains the same statistics, but counted on a system wide basis.	GET TABL
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 <u>http://oidref.com/1.3.6.1.2.1.4.32</u>	GET TABL
P-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 <u>http://oidref.com/1.3.6.1.2.1.4.33</u>	GET
P-MIB::ipAddressTable	This table contains addressing information relevant to the entity's interfaces. More information can be found here <u>http://oidref.com/1.3.6.1.2.1.4.34</u>	GET TABL
P-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 TABL
P-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	GET TABL
	used in the IPv6 address architecture document.	

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	GET
IP-MIB::icmpOutErrors	those counted by icmpOutErrors. The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as	GET
	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.	
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	GET
	received on currently established connections.	_
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 <u>https://oidref.com/1.3.6.1.2.1.6.12</u>	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 <u>https://oidref.com/1.3.6.1.2.1.6.20</u>	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
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
CNIMD. 2 MID. completions	The total number of CNIMP Table DDI Is which have been accorded and processed by the CNIMP protocol optity.	сет //

aps וווואוויויא::מוואו-vz-וווא	דופ נטגמרחטוווטפו טר סואואר דומף רטטג איזונדווומצע טפטו מכנפענעו מווע ערטבאגעע טע נווע סואואר ערטנטנע פווענע.	UEI
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
5NMPv2-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
5NMPv2-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
NMPv2-MIB::snmpOutGetRequests	The total number of SNMP Get-Request PDUs which have been generated by the SNMP protocol entity.	GET
NMPv2-MIB::snmpOutGetNexts	The total number of SNMP Get-Next PDUs which have been generated by the SNMP protocol entity.	GET
NMPv2-MIB::snmpOutSetRequests	The total number of SNMP Set-Request PDUs which have been generated by the SNMP protocol entity.	GET
NMPv2-MIB::snmpOutGetResponses	The total number of SNMP Get-Response PDUs which have been generated by the SNMP protocol entity.	GET
NMPv2-MIB::snmpOutTraps	The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity.	GET
5NMPv2-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
5NMPv2-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
5NMPv2-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
IOST-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
IOST-RESOURCES-MIB::hrSystemDate	The host's notion of the local date and time of day.	GET
IOST-RESOURCES- /IB::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 TABL
MTA-MIB::mtaGroupTable	The table holding information specific to each MTA group.	GET TABL
F-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 TABL
F-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
PV6-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 <u>https://oidref.com/1.3.6.1.2.1.55.1.1</u>	GET
PV6-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
PV6-MIB::ipv6Interfaces	The number of IPv6 interfaces (regardless of their current state) present on this system.	GET
PV6-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 TABI
ISMAN-EVENT- IIB::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 <u>https://oidref.com/1.3.6.1.2.1.88.1.1.1</u>	GET
DISMAN-EVENT- AIB::mteResourceSampleInstanceMaximum	The maximum number of instance entries this system will support for sampling. More information can be found here <u>https://oidref.com/1.3.6.1.2.1.88.1.1.2</u>	GET
DISMAN-EVENT- AIB::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 www.kontron.com	GET

www.kontron.com

DISMAN-EVENT-MIB::mteTriggerFailures	The minimum mteTriggerFrequency this system will accept. A system may use the larger values of this	GET
	minimum to lessen the impact of constant sampling. For larger sampling intervals the system samples less often and suffers less overhead. This object provides a way to enforce such lower overhead for all triggers created after it is set.	
DISMAN-EVENT-MIB::mteObjectsTable	A table of objects that can be added to notifications based on the trigger, trigger test, or event, as pointed to by entries in those tables.	GET TABLE
ISMAN-EVENT-MIB::mteEventTable	A table of management event action information.	GET TABLE
ISMAN-EVENT- IIB::mteEventNotificationTable	A table of information about notifications to be sent as a consequence of management events.	GET TABLE
OTIFICATION-LOG- IIB::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/1.3.6.1.2.1.92.1.11	GET
IOTIFICATION-LOG- 11B::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
OTIFICATION-LOG- IIB::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
OTIFICATION-LOG- IIB::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
NMPv2-SMI::enterprises.3582		GET
ET-SNMP-AGENT-MIB::nsModuleName	The module name that registered this OID.	GET
ET-SNMP-AGENT-MIB::nsModuleModes	The modes that the particular lower level handler can cope with directly.	GET
ET-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
ET-SNMP-EXTEND- IB::nsExtendNumEntries	The number of rows in the nsExtendConfigTable.	GET
ET-SNMP-AGENT- IIB::nsCacheDefaultTimeout	Default cache timeout value (unless overridden for a particular cache entry).	GET
ET-SNMP-AGENT-MIB::nsCacheEnabled	Whether data caching is active overall.	GET
ET-SNMP-AGENT-MIB::nsCacheTimeout	The length of time (?in seconds) for which the data in this particular cache entry will remain valid.	GET
ET-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
ET-SNMP-AGENT-MIB::nsDebugEnabled	Whether the agent is configured to generate debugging output	GET
ET-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
ET-SNMP-AGENT-MIB::nsDebugDumpPdu	Whether the agent is configured to display raw packet dumps. This is unrelated to the nsDebugEnabled setting.	GET
ET-SNMP-AGENT-MIB::nsLogType	The (minimum) priority level for which this logging entry should be applied.	GET
ET-SNMP-AGENT-MIB::nsLogMaxLevel	The maximum priority level for which this logging entry should be applied.	GET
ET-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
IET-SNMP-VACM- /IB::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
IET-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
IET-SNMP-VACM- IIB::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
IET-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
NMPv2-SMI::enterprises.20974.554.1	AMI SNMP Hostname Extension	GET
NMPv2-SMI::enterprises.20974.554.2	AMI SNMP MIB library to return the system health status like power and sensor status.	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

- Boot configuration
- <u>Networking</u>
 - <u>Network interface availability</u>
 - Preboot Execution Environment (PXE)
 - <u>iSCSI</u>
 - <u>Network stack</u>
- BIOS password
- Power management
- <u>Virtualization</u>
- <u>Compatibility Support Module (CSM)</u>
- <u>Security</u>
 - Secure boot
 - <u>Trusted Platform Module (TPM)</u>
- <u>Trusted Execution Technology (TXT)</u>
 <u>Console redirection</u>
- Error logging

The following tables provide menu paths for the CG2300 and the CG2400. This is a partial list that includes the most common configuration parameters. Since the CG2300 uses the Intel EFI code base and the CG2400 uses the AMI EFI code base, the setup menus are referred to as the INTEL SETUP and the AMI SETUP. In the lists of possible values, the value in **bold**, **underline** is the default value.

Boot configuration

CG2300	CG2400	Notes
$Menu \to Boot\;Manager$	$\begin{array}{l} Menu \to Save \ \pounds \ Exit \to Section \ Boot \\ Override \end{array}$	
$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Advanced} \rightarrow \mbox{USB} \\ \mbox{Configuration} \rightarrow \mbox{Make USB} \\ \mbox{Devices Non-Bootable [Enabled / \\ \mbox{Disabled }] \end{array}$	Menu \rightarrow Advanced \rightarrow USB Configuration \rightarrow USB Mass Storage Driver Support [<u>Enabled</u> / Disabled]	
Menu \rightarrow Boot Maintenance Manager \rightarrow Advanced Boot Options \rightarrow Boot Option Retry [Enabled / <u>Disabled</u>]	Not present in AMI SETUP	Boot Option Retry is always enabled on the CG2400.
$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Boot Maintenance} \\ \mbox{Manager} \rightarrow \mbox{Advanced Boot} \\ \mbox{Options} \rightarrow \mbox{USB Boot Priority} \left[\\ \hline \mbox{Enabled} \right] \end{array}$	Not present in AMI SETUP	
$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Boot Maintenance} \\ \mbox{Manager} \rightarrow \mbox{Add EFI Boot} \\ \mbox{Option} \rightarrow < \mbox{Dynamic list of EFI} \\ \mbox{Boot Options} > \end{array}$	$\begin{array}{l} \text{Menu} \rightarrow \text{Boot} \rightarrow \text{Section Boot Option} \\ \text{Priorities} \end{array}$	
Menu \rightarrow Boot Maintenance Manager \rightarrow Delete EFI Boot Option \rightarrow <dynamic efi<br="" list="" of="">Boot Options></dynamic>	Not present in AMI SETUP	
Menu \rightarrow Boot Maintenance Manager \rightarrow Change Boot Order \rightarrow <dynamic efi<br="" list="" of="">Boot Options></dynamic>	Not present in AMI SETUP	

Networking

Network interface availability

CG2300	CG2400	Notes
$\begin{array}{l} Menu \to Advanced \to PCI \\ Configuration \to NIC \\ Configuration \to Nic1 \\ Controller \left[\underline{Enabled} \right] \\ Disabled \end{array}$	$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Socket Configuration} \rightarrow \mbox{IIO} \\ \mbox{Configuration} \rightarrow \mbox{SocketO} \\ \mbox{Configuration} \rightarrow \mbox{SocketO} \\ \mbox{Port 1C (PCle Uplink)} \rightarrow \mbox{Pcl-E Port [} \\ \mbox{Auto} \slashed{auto} \slashed{autom} $	On the CG2400, both controllers are auto/enabled/disabled at the same time.
$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Advanced} \rightarrow \mbox{PCl} \\ \mbox{Configuration} \rightarrow \mbox{NiC} \\ \mbox{Configuration} \rightarrow \mbox{Nic1 Port1} [\\ \hline \mbox{Enabled} \slash \mbox{Disabled}] \\ \mbox{Menu} \rightarrow \mbox{Advanced} \rightarrow \mbox{PCl} \\ \mbox{Configuration} \rightarrow \mbox{NiC} \\ \mbox{Configuration} \rightarrow \mbox{Nic1 Port2} [\\ \hline \mbox{Enabled} \slash \mbox{Disabled}] \\ \mbox{Menu} \slash \mbox{Disabled}] \end{array}$	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
$\begin{array}{l} Menu \to Advanced \to PCI \\ Configuration \to NIC \\ Configuration \to Nic1 Port1 PXE \left[\\ \underline{Enabled} \slash Disabled \right] \end{array}$	Menu \rightarrow Advanced \rightarrow Option ROM Dispatch Policy \rightarrow On Board Network Controller [Enabled / Disabled]	On the CG2300, this option is only available if Nic1 Controller is enabled.

iSCSI

CG2300	CG2400	Notes
$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Advanced} \rightarrow \mbox{PCI} \\ \mbox{Configuration} \rightarrow \mbox{UEFI} \mbox{Option} \\ \mbox{ROM Control} \rightarrow \mbox{iSCSI} \\ \mbox{Configuration} \end{array}$	Menu \rightarrow Advanced \rightarrow iSCSI Configuration \rightarrow *	

Network stack

CG2300	CG2400	Notes
Menu \rightarrow Advanced \rightarrow PCI Configuration \rightarrow UEFI Network Stack \rightarrow UEFI Network Stack [<u>Enabled</u> /Disabled]	Menu → Advanced → Network Stack Configuration → Network Stack [<u>Enabled</u> / Disabled]	
Menu \rightarrow Advanced \rightarrow PCI Configuration \rightarrow UEFI Network Stack \rightarrow IPv4 PXE Support [<u>Enabled</u> / Disabled]	$\begin{array}{l} Menu \to Advanced \to Network Stack \\ Configuration \to Ipv4 PXE Support \left[\\ \underline{Enabled} \ / \ Disabled \right] \\ Menu \to Advanced \to Network Stack \\ Configuration \to Ipv4 \ HTTP Support \\ [Enabled \ / \ \underline{Disabled} \] \end{array}$	On the CG2400, t his option is only available if UEFI Network Stack is enabled.
$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Advanced} \rightarrow \mbox{PCI} \\ \mbox{Configuration} \rightarrow \mbox{UEFI} \mbox{Network} \\ \mbox{Stack} \rightarrow \mbox{IPv6} \mbox{PXE} \mbox{Support} \mbox{[} \\ \mbox{Enabled} \mbox{/ Disabled} \mbox{]} \end{array}$	$\begin{array}{l} Menu \to Advanced \to Network Stack \\ Configuration \to Ipv6 PXE Support \\ [Enabled / \underline{Disabled}] \\ Menu \to Advanced \to Network Stack \\ Configuration \to Ipv6 HTTP Support \\ [Enabled / \underline{Disabled}] \end{array}$	On the CG2400, t his option is only available if UEFI Network Stack is enabled.
$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Advanced} \rightarrow \mbox{PCI} \\ \mbox{Configuration} \rightarrow \mbox{UEFI} \mbox{Option} \\ \mbox{ROM Control} \rightarrow \mbox{Intel}(\mbox{R}) \mbox{1350} \\ \mbox{Gigabit Network Connection} \\ \mbox{$	Menu → Advanced → Intel(R) Ethernet Connection X722 for 10GBASE-T - $-ADDRESS-I> → Nic Configuration →Link Speed [Auto Negotiated]$	On the CG2400, this option is read only.
$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Advanced} \rightarrow \mbox{PCI} \\ \mbox{Configuration} \rightarrow \mbox{UEFI} \mbox{Option} \\ \mbox{ROM Control} \rightarrow \mbox{Intel}(\mbox{Rom}) \mbox{1350} \\ \mbox{Gigabit Network Connection} \mbox{-} \\ \mbox{-} \mbox{Address of NIC1} \rightarrow \mbox{Blink} \\ \mbox{LEDs [} \mbox{Q} \mbox{/} \mbox{-} \mbox{Numbers} \mbox{]} \end{array}$	Menu → Advanced → Intel(R) Ethernet Connection X722 for 10GBASE-T - $\langle MAC - ADDRESS-1 \rangle$ → Blink LEDs [<u>0</u> / <0-15>]	
$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Advanced} \rightarrow \mbox{PCI} \\ \mbox{Configuration} \rightarrow \mbox{UEFI} \mbox{Option} \\ \mbox{ROM Control} \rightarrow \mbox{Intel}(\mbox{R}) \mbox{1350} \\ \mbox{Gigabit Network Connection} \\ \mbox{-} \mbox{Address of NIC1> - VLAN} \\ \mbox{Configuration} \rightarrow \mbox{Enter} \\ \mbox{Configuration} \mbox{Menu} \rightarrow \mbox{*} \end{array}$	Menu \rightarrow Advanced \rightarrow VLAN Configuration (MAC: <i>ADDRESS-1</i> >) \rightarrow Enter Configuration Menu \rightarrow *	
$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Advanced} \rightarrow \mbox{PCI} \\ \mbox{Configuration} \rightarrow \mbox{UEFI} \mbox{Option} \\ \mbox{ROM Control} \rightarrow \mbox{Intel}(\mbox{R}) \mbox{1350} \\ \mbox{Gigabit Network Connection} \\ \mbox{ - IPv4} \\ \mbox{Current settings} \rightarrow \end{tabular}$	Menu \rightarrow Advanced \rightarrow MAC: <i>«MAC-</i> <i>ADDRESS-1»</i> -IPv4 Network Configuration \rightarrow Enter Configuration Menu \rightarrow *	
$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Advanced} \rightarrow \mbox{PCI} \\ \mbox{Configuration} \rightarrow \mbox{UEFI} \mbox{Option} \\ \mbox{ROM Control} \rightarrow \mbox{Intel}(\mbox{R}) \mbox{1350} \\ \mbox{Gigabit Network Connection} \\ \mbox{ - IPv6} \\ \mbox{Current settings} \rightarrow \mbox{Enter} \\ \mbox{Configuration Menu} \rightarrow \mbox{*} \end{array}$	Menu \rightarrow Advanced \rightarrow MAC: <i>MAC</i> - <i>ADDRESS</i>-1> -IPv6 Network Configuration \rightarrow Enter Configuration Menu \rightarrow *	

BIOS password

CG2300	CG2400	Notes
$\begin{array}{l} Menu \rightarrow Security \rightarrow Set \\ Administrator \ Password \end{array}$	$Menu \rightarrow Security \rightarrow Administrator \\ Password$	
$Menu \rightarrow Security \rightarrow Set User$ Password	$Menu \to Security \to User\ Password$	
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 \rightarrow Advanced \rightarrow Power & Performance \rightarrow CPU Power and Performance Policy [Performance / <u>Balanced</u>	Not present in AMI SETUP	

/ Power]		
Menu → Advanced → Power & Performance → Workload Configuration [<u>Balanced</u> /1/0 Sensitive]	Menu \rightarrow Socket Configuration \rightarrow Advanced Power Management Configuration \rightarrow CPU - Advanced PM Tuning \rightarrow Energy Perf BIAS \rightarrow Workload Configuration [<u>Balanced</u> /I/O Sensitive]	
Menu \rightarrow Advanced \rightarrow Power & Performance \rightarrow Uncore Power Management \rightarrow Uncore Frequency Scaling [<u>Enabled</u> / Disabled]	Menu \rightarrow Socket Configuration \rightarrow Advanced Power Management Configuration \rightarrow CPU P State Control \rightarrow Uncore Freq Scaling (UFS) [<u>Enable</u> / Disable]	
Menu → Advanced → Power & Performance → Uncore Power Management → Performance P- .imit [<u>Enabled</u> / Disabled]	$\begin{array}{l} {\sf Menu} \to {\sf Socket \ Configuration} \to \\ {\sf Advanced \ Power \ Management} \\ {\sf Configuration} \to {\sf CPU \ P \ State \ Control} \to \\ {\sf Perf \ P-Limit} \to * \end{array}$	
Menu → Advanced → Power & Performance → CPU P State Control → Enhanced Intel SpeedStep(R) Tech [<u>Enabled</u> / Disabled]	Menu \rightarrow Socket Configuration \rightarrow Advanced Power Management Configuration \rightarrow CPU P State Control \rightarrow SpeedStep (Pstates) [Disable / <u>Enable</u>]	
Menu → Advanced → Power & Performance → CPU P State Control → Intel Configurable TDP [Enabled / Disabled]	$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Socket Configuration} \rightarrow \\ \mbox{Advanced Power Management} \\ \mbox{Configuration} \rightarrow \mbox{CPU P State Control} \rightarrow \\ \mbox{Config TDP [Normal / Level 1 / Level 2]} \end{array}$	
Menu \rightarrow Advanced \rightarrow Power & Performance \rightarrow CPU P State Control \rightarrow Intel(R) Turbo Boost Technology [<u>Enabled</u> / Disabled]	Menu \rightarrow Socket Configuration \rightarrow Advanced Power Management Configuration \rightarrow CPU P State Control \rightarrow Turbo Mode [<u>Enable</u> /Disable]	
Menu → Advanced → Power & Performance → CPU P State Control → Energy Efficient Turbo [Enabled / Disabled]	Menu \rightarrow Socket Configuration \rightarrow Advanced Power Management Configuration \rightarrow CPU P State Control \rightarrow Energy Efficient Turbo [<u>Enable</u> / Disable]	
Menu → Advanced → Power & Performance → CPU HWPM State Control → Enable CPU HWPM [Enabled / <u>Disabled]</u>	$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Socket Configuration} \rightarrow \mbox{Advanced Power Management} \\ \mbox{Configuration} \rightarrow \mbox{Hardware PM State} \\ \mbox{Control} \rightarrow \mbox{Hardware P-States} \mbox{[Disable / $Mative Mode} / $Out of Band Mode / $Native Mode with No Legacy Support]} \end{array}$	
Menu → Advanced → Power & Performance → CPU HWPM State Control → Enable CPU Autonomous Cstate [Enabled / <u>Disabled</u>]	$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Socket Configuration} \rightarrow \\ \mbox{Advanced Power Management} \\ \mbox{Configuration} \rightarrow \mbox{CPU C State Control} \rightarrow \\ \mbox{Autonomous Core C-State [Enable / \\ \hline \mbox{Disable]} \end{array}$	
Menu → Advanced → Power & Performance → CPU C State Control → CPU C-State [<u>Enabled</u> / Disabled]	Not present in AMI SETUP	
Menu → Advanced → Power & Performance → CPU C State Control → C1E Autopromote [Enabled / Disabled]	Menu \rightarrow Socket Configuration \rightarrow Advanced Power Management Configuration \rightarrow CPU C State Control \rightarrow Enhanced Halt State (C1E) [<u>Enable</u> / 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 \rightarrow Socket Configuration \rightarrow Advanced Power Management Configuration \rightarrow CPU C State Control \rightarrow CPU C6 report [Disable / Enable / <u>Auto</u>]	
Menu → Server Management → Resume on AC Power Loss [<u>Stay</u> <u>off</u> / 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 the previous line.
$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Server Management} \rightarrow \\ \mbox{Power Restore Delay} \left[\mbox{Disabled} \\ \mbox{/ Auto / Fixed} \right] \end{array}$	Not present in AMI SETUP	
Menu → Server Management → Power Restore Delay Value [<u>55</u> /<55-300>]	Not present in AMI SETUP	

Virtualization

CG2300	CG2400	Notes
$\begin{array}{l} Menu \to Advanced \to Processor\\ Configuration \to Intel(R)\\ Virtualization\\ Technology\left[Enabled / \underline{Disabled}\\ \right] \end{array}$	Menu \rightarrow Socket Configuration \rightarrow Processor Configuration \rightarrow VMX [<u>Enable</u> / Disable]	
Menu — Advanced — Integrated IO Configuration> Intel(R) VT for Directed I/O [Enabled / Disabled]	$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Socket Configuration} \rightarrow \mbox{II0} \\ \mbox{Configuration} \rightarrow \mbox{Intel. VT for Directed I/0} \\ \mbox{(VT-d)} \rightarrow \mbox{Intel. VT for Directed I/0 (VT-d)} \\ \mbox{[Enable / Disable]} \end{array}$	
Menu — Advanced — PCI Configuration — ARI Forwarding [Enabled / <u>Disabled</u>]	$\begin{array}{l} Menu \to Platform \ Configuration \to ARI \\ Miscellaneous \ Configuration \to ARI \\ Support \ [\ \underline{Enable} \ / \ Disable] \\ Menu \to Platform \ Configuration \to \\ Miscellaneous \ Configuration \to \\ ARI \\ Forward \ [Enable \ / \ \underline{Disable} \] \end{array}$	

Compatibility Support Module (CSM)

CG2300	CG2400	Notes
Not present in INTEL SETUP	$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Advanced} \rightarrow \mbox{CSM Configuration} \\ \rightarrow \mbox{CSM Support [Enabled / \underline{\mbox{Disabled }]} \end{array}$	
$\begin{array}{l} Menu \to Boot \ Maintenance \\ Manager \to Advanced \ Boot \\ Options \to Boot \ Mode \ [UEFI \ / \\ \underline{Legacy} \end{array}$	$\begin{array}{l} Menu \to Advanced \to CSM \ Configuration \\ \to Boot \ option \ filter \ [\ \underline{UEFI} \ and \ \underline{Legacy} \ / \\ Legacy \ only \ / \ UEFI \ only] \end{array}$	On CG2400, this option is only available if CSM Support is enabled.
$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Boot Maintenance} \\ \mbox{Manager} \rightarrow \mbox{Advanced Boot} \\ \mbox{Options} \rightarrow \mbox{Video BIOS [} \underline{\textbf{UEFI}} \\ \mbox{/ Legacy]} \end{array}$	Menu \rightarrow Advanced \rightarrow CSM Configuration \rightarrow Video [<u>UEFI</u> /Legacy]	On CG2400, this option is only available if CSM Support is enabled.

Security

Secure boot

CG2300	CG2400	Notes
$\begin{array}{l} {\sf Menu} \to {\sf Boot} \ {\sf Maintenance} \\ {\sf Manager} \to {\sf Advance} \ {\sf Boot} \\ {\sf Options} \to {\sf Secure} \ {\sf Boot} \\ {\sf Configuration} \to {\sf Attempt} \ {\sf Secure} \\ {\sf Boot} \ [{\sf Enabled} \ / \ \underline{{\sf Disabled}} \] \end{array}$	Menu \rightarrow Security \rightarrow Secure Boot \rightarrow Secure Boot [Enabled / <u>Disabled</u>]	

Trusted Platform Module (TPM)

CG2300	CG2400	Notes
$\begin{array}{l} Menu \rightarrow Security \rightarrow TPM \\ Administrative Control [\underline{No} \\ \underline{Operation} / Turn On / Turn Off \\ / Clear Ownership] \end{array}$	$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Advanced} \rightarrow \mbox{Trusted} \\ \mbox{Computing} \rightarrow \mbox{Security Device Support} \left[\\ \underline{\mbox{Enable}} \slash \right] \end{array}$	
Menu \rightarrow Security \rightarrow TPM2 Operation [<u>No Action</u> / TPM2 ClearControl(NO) + Clear]	Menu \rightarrow Advanced \rightarrow Trusted Computing \rightarrow TPM2.0 UEFI Spec Version [TCG_1_2 / TCG_2]	On both platforms, TPM has to be inserted to see the menu.
Menu \rightarrow Security \rightarrow TPM FW Update [Enabled / <u>Disabled</u>]	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.
$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Advanced} \rightarrow \mbox{PCI} \\ \mbox{Configuration} \rightarrow \mbox{UEFI} \mbox{Option} \\ \mbox{ROM Control} \mbox{(Dynamic Menu)} \rightarrow \\ \mbox{TrEE Configuration} \rightarrow \mbox{Attempt} \\ \mbox{TPM Device} \mbox{[Disable} / \mbox{TPM 1.2} / \\ \mbox{TPM 2.0 (DTPM)]} \end{array}$	Menu \rightarrow Advanced \rightarrow Trusted Computing \rightarrow Device Select [TPM 1.2 / TPM 2.0 / <u>Auto</u>]	On both platforms, TPM has to be inserted to see the menu.

Trusted Execution Technology (TXT)

CG2300	CG2400	Notes
$\begin{array}{l} {\sf Menu} \to {\sf Advanced} \to {\sf Processor} \\ {\sf Configuration} \to {\sf Intel}({\sf R}) \\ {\sf TXT} [{\sf Enabled} \ / \ \underline{{\sf Disabled}} \] \end{array}$	Menu → Socket Configuration → Processor Configuration → Enable Intel(R) TXT [Enable / <u>Disable</u>]	

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 \rightarrow Server Management \rightarrow Console Redirection \rightarrow Console Redirection [Disabled / Serial Port A / Serial Port B]	$\begin{array}{l} Menu \to Advanced \to Serial \; Port \; Console \\ Redirection \to Console \; Redirection \; [\\ \underline{Enabled} \; / \; Disabled] \\ Menu \to Advanced \to Serial \; Port \; Console \\ Redirection \to Legacy \; Console \\ Redirection \; Settings \to Redirection \; COM \\ Port \; [\; \underline{COMO} \;] \end{array}$	
Menu → Server Management → Console Redirection → Flow Control [None / RTS/CTS]	Menu → Advanced → Serial Port Console Redirection → Console Redirection Settings → Flow Control [<u>None</u> / 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 \rightarrow Advanced \rightarrow Serial Port Console Redirection \rightarrow Console Redirection Settings \rightarrow Bits per second [9600 / 19200 / 38400 / 57600 / <u>115200</u>]	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]	$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Advanced} \rightarrow \mbox{Serial Port Console} \\ \mbox{Redirection} \rightarrow \mbox{Console Redirection} \\ \mbox{Settings} \rightarrow Terminal Type [VT100 / $$$ $$ $$ $$ $$ $$ $$ $$ $$ $$ $$ $$ $	On the CG2300, the option is only shown if Console Redirection is enabled.
Menu \rightarrow Server Management \rightarrow Console Redirection \rightarrow Legacy OS Redirection [Enabled / Disabled]	$\begin{array}{l} Menu \to Advanced \to Serial \; Port \; Console \\ Redirection \to Legacy \; Console \\ Redirection \; Settings \to Redirect \; After \\ POST \; [\\ \underline{Always \; Enable} \; / \; BootLoader] \end{array}$	On the CG2300, the option is only shown if Console Redirection is enabled.
Menu → Server Management → Console Redirection → Terminal Resolution [80x24 / 100x31]	$\begin{array}{l} Menu \to Advanced \to Serial \; Port \; Console \\ Redirection \to Legacy \; Console \\ Redirection \; Settings \to Resolution \; [\\ \underline{\mathbf{80x24}} \; / \; 80x25] \\ Menu \to Advanced \to Serial \; Port \; Console \\ Redirection \to Console \; Redirection \\ Settings \to Resolution \; 100x31 \; [Enabled \; / \\ \underline{Disabled} \;] \end{array}$	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 <i><enter></enter></i>	$\begin{array}{l} Menu \to Server\;Mgmt \to System\;Event\\ Log \to Erase\;SEL \to [\underline{No}/Yes,On\;next\\ reset/Yes,On\;every\;reset]\\ Menu \to Server\;Mgmt \to System\;Event\\ Log \to When\;SEL\;is\;Full\;[\underline{Do\;Nothing}/Erase\;Immediately/Delete\;Oldest\\ Record]\\ Menu \to Server\;Mgmt \to System\;Event\\ Log \to Log\;EFI\;Status\;Codes\;[Disabled/Both/\underline{Error\;code}/Progress\;code]\\ \end{array}$	
Menu → Advanced → Memory Configuration → Memory RAS and Performance Configuration → Select Memory RAS Configuration [Maximum Performance / Mirroring / Rank Sparing / Lockstep]	$\begin{array}{l} {\sf Menu} \rightarrow {\sf Socket Configuration} \rightarrow {\sf Memory RAS} \\ {\sf Configuration} \rightarrow {\sf Static Virtual Lockstep} \\ {\sf Mode [Enable / Disable_]} \\ {\sf Menu} \rightarrow {\sf Socket Configuration} \rightarrow {\sf Memory RAS} \\ {\sf Configuration} \rightarrow {\sf Memory RAS} \\ {\sf Configuration} \rightarrow {\sf Mirror mode [Enable / Disable_]} \\ {\sf Menu} \rightarrow {\sf Socket Configuration} \rightarrow {\sf Memory RAS} \\ {\sf Configuration} \rightarrow {\sf Memory RAS} \\ {\sf Configuration} \rightarrow {\sf Memory RAS} \\ {\sf Configuration} \rightarrow {\sf UEFI} {\sf ARM Mirror} \\ \\ [Enable / Disable_] \\ \\ {\sf Menu} \rightarrow {\sf Socket Configuration} \rightarrow {\sf Memory RAS} \\ {\sf Configuration} \rightarrow {\sf Memory RAS} \\ \\ {\sf Configuration} \rightarrow {\sf Memory Rank Sparing} \\ \\ \\ \\ [{\sf Enable / Disable_]} \\ \end{array}$	On the CG2400, the option shown varies according to the type of memory installed in the system.
$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Advanced} \rightarrow \mbox{Memory} \\ \mbox{Configuration} \rightarrow \mbox{Memory} \mbox{RAS} \\ \mbox{and} \mbox{Performance} \mbox{Configuration} \end{array}$	Menu \rightarrow Socket Configuration \rightarrow Memory Configuration \rightarrow Memory RAS Configuration \rightarrow Patrol Scrub [<u>Enable</u> /	w kontron com

\rightarrow Patrol Scrub [<u>Enabled</u> / Disabled] Menu \rightarrow Advanced \rightarrow Memory Configuration \rightarrow Memory RAS and Performance Configuration \rightarrow Demand Scrub [<u>Enabled</u> / Disabled]	Disable] Menu \rightarrow Socket Configuration \rightarrow Memory Configuration \rightarrow Memory RAS Configuration \rightarrow Patrol Scrub Interval [24./ <1-24>] Menu \rightarrow Socket Configuration \rightarrow Memory Configuration \rightarrow Memory RAS Configuration \rightarrow Patrol Scrub Address Mode [Reverse Address / System Physical Address.]	
Menu \rightarrow Advanced \rightarrow Memory Configuration \rightarrow Memory RAS and Performance Configuration \rightarrow Correctable Error Threshold [20 / <u>10</u> / 5 / All / None]	Menu \rightarrow Socket Configuration \rightarrow Memory Configuration \rightarrow Memory RAS Configuration \rightarrow Correctable Error Threshold [<u>2fff</u> / <0-7ffff>]	
Menu \rightarrow Advanced \rightarrow Memory Configuration \rightarrow Memory RAS and Performance Configuration \rightarrow Memory Correctable Error Enabling [<u>Enabled</u> /Disabled]	Menu \rightarrow Socket Configuration \rightarrow Memory Configuration \rightarrow Memory Dfx Configuration \rightarrow ECC Checking [<u>Auto</u> / Enable / Disable]	
Menu \rightarrow Server Management \rightarrow Assert NMI on SERR [<u>Enabled</u> / Disabled]	Not present in AMI SETUP	
Menu \rightarrow Server Management \rightarrow Assert NMI on PERR [<u>Enabled</u> / Disabled]	Not present in AMI SETUP	
Menu → Server Management → PCIe AER Support [<u>Enabled</u> / Disabled]	$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Platform Configuration} \rightarrow \\ \mbox{Runtime Error Logging} \rightarrow \mbox{II0 Error} \\ \mbox{Enabling} \rightarrow \mbox{II0 PCIE AER Spec} \\ \mbox{Compliant [Enable / Disable]} \end{array}$	
Menu \rightarrow Server Management \rightarrow Log Correctable Errors [Enabled / Disabled]	Not present in AMI SETUP	
Menu \rightarrow Server Management \rightarrow WHEA Support [<u>Enabled</u> / Disabled]	Not present in AMI SETUP	
Menu \rightarrow Server Management \rightarrow Enable Cloaking [Enabled / Disabled]	Not present in AMI SETUP	
Menu \rightarrow Server Management \rightarrow PCIe Correctable Error Threshold [20 / All / 5 / <u>10</u>]	Not present in AMI SETUP	
Menu → Server Management → Reset on CATERR [<u>Enabled</u> / Disabled]	Not present in AMI SETUP	
$\begin{array}{l} \mbox{Menu} \rightarrow \mbox{Server Management} \rightarrow \\ \mbox{Reset on ERR2 [} \underline{Enabled} / \\ \mbox{Disabled]} \end{array}$	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:

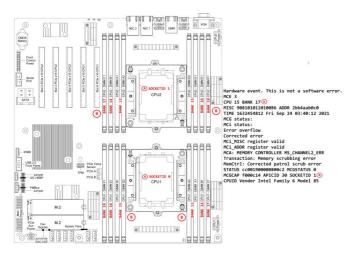
Hardware event. This is not a software error. MCE 0 CPU 0 BANK 18 MISC 90840080008228c ADDR 9ce494000 TIME 1499161840 Tue Jul 4 09:50:40 2021 MCG status: MCi status: Corrected error MCi_MISC register valid MCi_ADDR register valid MCA: MEMORY CONTROLLER MS_CHANNEL2_ERR Transaction: Memory scrubbing error 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.

ADANGER	DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.
AWARNING	WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.
	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.

i

This symbol indicates general information about the product and the documentation. This symbol also indicates detailed information about the specific product configuration.

Ø

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	
1/0	Input/Output	
1 ² C	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	Maximum Amberia remperature 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	
OCX0	Oven-Controlled Crystal Oscillator	
05	Operating System	
OTP	Over-Temperature Protection	

OVP		Over Veltage Brotestion
		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 l	Jnit
PTP	Precision Time	Protocol
PXE	Preboot eXecu	tion Environment
RAID	Redundant Arra	ay of Independent Disks
RAN	Radio Access N	letwork
RAS	Reliability, Avai	ilability, and Serviceability
RDIMM	Registered Dua	al In-Line Memory Module
RDP	Remote Deskto	qc
RMM	Remote Manag	gement Module
RoHS	Restriction of H	Hazardous Substances
SAS	Serial Attached	d SCSI (Small Computer System Interface)
SATA	Serial Advance	d Technology Attachment
SCSI	Small Compute	er Systems Interface
SDRAM	Synchronous D	ynamic RAM
SEL	System Event l	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 Ch	nip
SOL	Serial over LAN	I
SSD	Solid State Driv	/e
SSH	Secure Shell	
THOL	Tested Hardwa	are and Operating System List
TPM	Trusted Platfo	rm Module
TUV	Technischer Ut	perwachungs-Verein (A safety testing laboratory with headquarters in Germany)
UART		chronous Receiver Transmitter
UEFI		ible Firmware Interface
UL	Underwriter's l	
USB	Universal Seria	
UV	Under-Voltage	
V	Volt	
VA		volts multiplied by amps)
Vac	Volts Alternati	
Vdc	Volts Direct Cu	
VDE		cher Electrotechniker (German Institute of Electrical Engineers)
VGA	Video Graphics	
vua		Array Jio Access Network
VSB		
	Voltage Standt	y ,
W	Watt	al and Electronic Fouriement
WEEE	vvaste clectific	al and Electronic Equipment

Ω	Ohm		

Safety and regulatory information

Table of contents

- <u>General safety warnings and cautions</u>
 - <u>Elevated operating ambient temperature</u>
 - Mechanical loading
 - <u>Circuit overloading</u>
 - <u>AC power supply safety</u>
 - <u>Main AC power disconnect</u>
 - <u>Reliable earth-grounding</u>
 - Overcurrent protection
 - <u>DC power supply safety</u>
 - Main DC power disconnect
 - Overcurrent protection
 - <u>Reliable earth-grounding</u>
- <u>Regulatory specifications</u>
 - <u>RoHS</u>
 - Waste electrical and electronic equipment directive
 - <u>Air Filter</u>

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

AWARNING 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 liquid objects filled with liquids should be placed on the chassis cover.		iquids and no	
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.			
	ON	The equipment rack must provide sufficient airflow to the front of the server to maintain proper cooling.	

Elevated operating ambient temperature

If this product is installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, be careful to install the product in an environment that is compatible with the maximum operating temperature specified by the manufacturer in the specifications.

Mechanical loading



Do not load the equipment unevenly when mounting this product in a rack as it may create hazardous conditions.

	The power supply in this product contains no user-serviceable parts. There may be more than one supply in this product. Refer servicing only to qualified personnel.
	Do not attempt to modify or use the supplied AC power cord if it is not the exact type required. A product with more than one power supply will have a separate AC power cord for each supply.
	The power button on the system does not turn off system AC power. To remove AC power from the system, always unplug each AC power cord from the wall outlet or power supply. The power cord(s) is considered the disconnect device to the main (AC) power. The socket outlet that the system plugs into must be installed near the equipment and must be easily accessible.
	 SAFETY STEPS: Before removing the chassis covers to access the inside of the system, follow these steps: 1. Turn off all peripheral devices connected to the system. 2. Turn off the system by pressing the power button. 3. Unplug all AC power cords from the system or from wall outlets. 4. Label and disconnect all cables connected to I/O connectors or ports on the back of the system. 5. Provide electrostatic discharge (ESD) protection by wearing an antistatic wrist strap attached to chassis ground of the system—any unpainted metal surface—when handling components. After completing the six SAFETY STEPS above, you can remove the system covers. To do this: 1. Unlock and remove the padlock from the back of the system if a padlock has been installed. 2. Remove and save all screws from the covers. 3. Remove the covers. 4. Do not operate the system with the chassis covers removed.
	 For proper cooling and airflow, always reinstall the chassis covers before turning on the system. Operating the system without the covers in place can damage system parts. To install the covers: 1. Check first to make sure no loose tools or parts were left inside the system. 2. Check that cables, add-in boards, and other components are properly installed. 3. Attach the covers to the chassis with the screws removed earlier, and tighten them firmly. 4. Insert and lock the padlock to the system to prevent unauthorized access inside the system. 5. Connect all external cables and the AC power cord(s) to the system.
	A microprocessor and heat sink may be hot if the system has been running. Also, there may be sharp pins and edges on some board and chassis parts. Contact should be made with care. Consider wearing protective gloves.
SA AN	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.

AWARNING 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 disconnection 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.

AWARNING	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</har>
	3x 0.75 mm conductors rated 250 VAC.
	Connector, wall outlet end
	Cords must be terminated in a grounding - type male plug designed for use in your region. The connector must have certification marks showing
	certification by an agency acceptable in your region and for U.S. must be listed and rated for 125% of the overall current rating of the server.
	Connector, server end
	The connectors that plug into the AC receptacle on the server must be an approved IEC (International Electrotechnical Commission) 320, sheet C13, type
	female connector.
	Cord length and flexibility
	Cords must be less than 4.5 meters (14.8 feet) long.

DC power supply safety

Platforms equipped with a DC power supply must be installed in a restricted access area in accordance with articles 110 - 26 and 110 - 27 of the National Electric Code, ANSI/NFPA 70. When powered by DC supply, this equipment must be protected by a listed branch circuit protector with a maximum 25 A rating. The DC source must be electrically isolated from any hazardous AC source by double or reinforced insulation. The DC source must be capable of providing up to 1000 watts of continuous power per feed pair.

i	The DC power supply is protected from reverse polarity by internal diodes and will not operate at all if wired incorrectly.	
A CAUTIO	This equipment is designed for the earth grounded conductor (return) in the DC supply circuit to be connected to the earth grounding conductor on the equipment (ground lug).	

Main DC power disconnect

A properly rated DC power disconnect must be installed for the server system. This main disconnect must be readily accessible, and it must be labeled as controlling power to the server. The UL listed circuit breaker of a centralized DC power system may be used as a disconnect device when easily accessible.

Overcurrent protection

Overcurrent protection UL Listed circuit breakers must be provided as part of each host equipment rack and must be incorporated in the field wiring between the DC source and the server. The branch circuit protection shall be rated minimum 75 VDC, maximum 2 5 A per feed pair.

Reliable earth-grounding

This server is intended for installation with an isolated DC return (DC - I per NEBS GR - 1089, Issue 3). To avoid the potential for an electrical shock hazard, you must reliably connect an earth grounding conductor to the server. The earth grounding conductor must be a minimum 10AWG connected to the earth ground stud(s) on the rear of the server. The safety ground conductor should be connected to the chassis stud with a listed closed two - hole crimp terminal having 5/8 - inch pitch. The nuts on the chassis earth ground studs should be installed with a torque of 10 in - lbs. The safety ground conductor provides proper grounding only for the server. You must provide additional, proper grounding for the rack and other devices installed in it.

Earth ground lug location



Regulatory specifications

The platform meets the requirements of the following regulatory tests and standards:

Safety compliance

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: ENS5032, Class A Limit, Radiated & Conducted Emissions ENS5035 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.

Warranty and support

Table of contents

- Limited warranty
- <u>Disclaimer</u>
- <u>Customer support</u>
- <u>Customer service</u>

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.

This manual is protected by copyright. All rights are reserved by Kontron. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the express written permission of Kontron. Kontron points out that the information contained in this manual is constantly being updated in line with the technical alterations and improvements made by Kontron to the products and thus this manual only reflects the technical status of the products by Kontron at the time of publishing. Brand and product names are trademarks or registered trademarks of their respective owners. ©2022 by Kontron

Customer support

Kontron's technical support team can be reached through the following means:

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

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.