User Documentation - ME1210

POSSIBILITIES START HERE 💽 KONTPON



Table of contents

- User Documentation ME1210
 - Product description
 - <u>Revision history</u>
 - Warranty and support
 - <u>Safety and regulatory information</u>
 - <u>Overview</u>
 - Specifications
 - <u>Platform components</u>
 - <u>Product architecture</u>
 - <u>Description of system access methods</u>
 - Recommended technical expertise
 - <u>Planning</u>
 - Environmental considerations
 - Power consumption and power budget
 - MAC addresses
 - PCI mapping
 - <u>Connector pinouts and electrical characteristics</u>
 - Material, information and software required
 - Platform, modules and accessories
 - Hardware compatibility list
 - <u>Validated operating systems</u>
 - Security
 - <u>Getting started</u>
 - Getting started Application installation and performance benchmarking
 - <u>Mechanical installation and precautions</u>
 - ESD protections
 - Unboxing
 - <u>Components installation and assembly</u>
 - Airflow
 - <u>Rack installation</u>
 - Cabling
 - Accessing platform components
 - Accessing a BMC
 - Accessing the operating system of a server
 - Accessing the UEFI or BIOS
 - Accessing the switch NOS
 - Discovering platform IP addresses
 - Default user names and passwords
 - Software installation and deployment
 - Preparing for operating system installation
 - Installing an operating system on a server
 - Verifying operating system installation
 - Platform resources for customer application
 - Common software installation
 - <u>Configuring</u>
 - <u>Configuring system access methods</u>
 - <u>Configuring date and time</u>
 - <u>Configuring BMC date and time</u>
 - Configuring switch NOS date and time
 - Configuring networking
 - Configuring the BMC networking
 - Configuring UEFI network boot
 - <u>Configuring switch NOS networking</u>
 - Configuring the switch
 - <u>Configuring synchronization</u>
 - <u>Configuring UEFI/BIOS options</u>
 - Configuring and managing users
 - <u>Configuring and managing BMC users</u>
 - <u>Configuring and managing switch NOS users</u>
 - <u>Configuring sensors and thermal parameters</u>
 - Operating
 - Platform power management
 - Monitoring
 - Monitoring sensors
 - <u>Sensor list</u>
 - <u>Maintenance</u>
 - System event log

- Interpreting sensor data
- <u>Component replacement</u>
- Backup and restore
- Upgrading
- Platform cooling and thermal management
- <u>Troubleshooting</u>
 - <u>Collecting diagnostics</u>
 - Factory default
 - Support information
- Knowledge base
 - Sending a BREAK signal over a serial connection
 - <u>Disabling sleep states in Linux</u>
- <u>Application notes</u>
 - <u>Generating custom secure boot keys</u>
 - Provisioning custom secure boot keys
- <u>Reference guides</u>
 - Supported Redfish commands
 - <u>Supported IPMI commands</u>
- Document symbols and acronyms

Product description

Table of contents

- <u>ME1210 High Performance RAN/MEC Platform</u>
 - <u>Main applications</u>
 - <u>Main features</u>

ME1210 High Performance RAN/MEC Platform



The Kontron ME1210 high performance 1U edge server is a d istributed unit for wide temperature ranges . The ME1210 is used for RAN or multiaccess edge computing (MEC). This platform has more cores, more memory and an increased density.

Main applications

- Solve restricted space and power challenges to enable complex applications closer to the network edge
- Decrease network congestion and improve the performance of applications by getting task processing closer to the user
- Enable applications such as Radio Access Network (RAN), artificial intelligence, data caching, ultra-low latency, and high-bandwidth edge applications

Main features

- Intel® Xeon® D-2100 processor (code-named Skylake-D)
- Two PCIe expansion slots for hardware acceleration
- Optional on-board Ethernet network switch with PTP/SyncE and OCXO holdover
- Long product lifecycle
- Daisy chain configuration to connect multiple distributed units together
- Support for major open RAN software solutions
- DC power (AC as an option)
- Eight DDR4 DIMM sockets, 4 channels @ 2667 MHz support up to 512GB
- Two M.2-2230/2280/22110, up to 1TB each (SATA or NVMe)

Revision history

Revision	Brief description of changes	Date of issue
1.0	First product release	July 2021
2.0	 Adjustments made mainly to sections under Configuring and Operating Modifications for BMC firmware version 2.x (procedures using IPMI IOL, Redfish and the Web UI) Modification of sensor definitions and information Modification of the network synchronization configuration page with new parameter recommendations Modification of the position of the following sections, which were inserted between the mechanical and software installation sections Accessing platform components (previously under Operating) Discovering platform IP addresses (previously under Operating) Default user names and passwords (previously under Operating) 	June 2022

Warranty and support

Table of contents

- <u>Limited warranty</u>
- <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 <u>www.kontron.com/support-and-services</u>.

Safety and regulatory information

Table of contents

- <u>General safety warnings and cautions</u>
 - <u>Elevated operating ambient temperature</u>
 - <u>Reduced air flow</u>
 - Mechanical loading
 - <u>CE mark</u>
 - Waste electrical and electronic equipment directive
- <u>General power safety warnings and cautions</u>
 - <u>Circuit overloading</u>
 - DC power supply safety
 - Reliable earth-grounding
- <u>Regulatory specifications</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

A CAUTION	Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.
AWARNINGTo prevent a fire or shock hazard, do not expose this product to rain or moisture. The chassis should not be expose splashing liquids and no objects filled with liquids should be placed on the chassis cover.	

ESD sensitive device!

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

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.

Reduced air flow

Do not compromise on the amount of air flow required for safe operation when installing this product in a rack. Side clearances must be respected.

Mechanical loading

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

CE mark

The CE marking on this product indicates that it is in compliance with the applicable European Union Directives: Low Voltage, EMC, Radio Equipment and RoHS requirements.

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.



General power safety warnings and cautions



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

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.

DC power supply safety

Platforms equipped with a DC power supply must be installed in a restricted access area. When powered by DC supply, this equipment must be protected by a listed branch circuit protector with a maximum 20 A rating. The DC source must be electrically isolated from any hazardous AC source by double or reinforced insulation.

The DC power supply is protected from reverse polarity by internal diodes and will not operate at all if wired incorrectly.

ACAUTION 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).

All of the following conditions must be met:

- 1. This equipment shall be connected directly to the d.c. supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus to which the d.c. supply system earthing electrode conductor is connected.
- 2. This equipment shall be located in the same immediate area (such as adjacent cabinets) as any other equipment that has a connection between the earthed conductor of the same d.c. supply circuit and the earthing conductor, and also the point of earthing of the d.c. system. The d.c. system shall not be earthed elsewhere.
- 3. The d.c. supply source shall be located within the same premises as this equipment.
- 4. Switching or disconnecting devices shall not be in the earthed circuit conductor between the d.c. source and the point of the connection of the earthing electrode conductor.

Reliable earth-grounding

Always maintain reliable grounding of rack-mounted equipment.

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.
Europe	This 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 Part 15/ICES-003 Class A. It is designed to meet GR-1089 and GR-63.			
Europe	This product complies with the Electromagnetic Compatibility Directive 2014/30/EU and EN 300 386. The GPS version complies with Radio Equipment Directive 2014/53/EU, EN 301 489-1 and EN 303 413.			
International	This product complies with CISPR 32 Class A and CISPR 35.			
Japan	This product complies with VCCI Class A. Note for Japan AC input rating is 90-130 VAC.			
この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害				

を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう

要求されることがあります。

VCCI – A

Overview

- <u>Specifications</u>
- Platform components
- <u>Product architecture</u>
- <u>Description of system access methods</u>
- <u>Recommended technical expertise</u>

Specifications

Table of contents

- ME1210 key hardware features
- <u>ME1210 key software features</u>
- <u>ME1210 physical dimensions</u>
- ME1210 packaging physical dimensions
- ME1210 shipping weights
- ME1210 environmental specifications

ME1210 key hardware features

Feature	Description
Hardware platform	 High-performance server for radio access network (RAN) and multi-access edge computing (MEC) Rackmount, 1U height, 13.5 inches deep, 19 inches wide Front access only (motherboard I/O, PSU, PCIe add-in card I/O)
1/0	 Two USB 3.0 One RJ45 10/100/1000Base-T management port One RJ45 serial port One RJ45 alarm input port IO module options with: Four 10 GbE SFP+ One 12 port Ethernet switch (8x SFP+, 4x SFP28)
Timing	With Ethernet switch IO module option:One SMA GNSS antenna inputOne SMA PPS Sync Signal Output
PCIe add-in card	 Two optional FHHL or FH¾L PCIe x16 add-in card supported (power and thermal restrictions may apply) Maximum power consumption supported is 75 W per card PCIe 3.0 (8GT/s) Refer to the <u>Hardware compatibility list</u>
CPU	 Intel® Xeon® D-2100 family processors are supported, including the following processors: Xeon® D-2187NT, 16 Cores @ 2.00GHz with QAT, 110 W Xeon® D-2183IT, 16 Cores @ 2.20GHz, 100 W
Drive	Two M.2 SSDs: • SATA or NVMe • Supported types: 2230, 2280 and 22110 Refer to the <u>Hardware compatibility list</u>
Memory	DDR4 DIMM with ECC Bandwidth up to 2666 MT/s Four memory channels Two DIMM socket per channel Refer to the <u>Hardware compatibility list</u>
Power inlet	One -57 VDC to -40 VDC dual input feed or 90 VAC to 264 VAC 47/63 Hz single input
Power consumption	Refer to Power consumption and power budget
Fans	Eight fans in N+1 configurationAutomatic fan speed control
Rack mounting brackets	Front mount in a 19-in wide rack

ME1210 key software features

Feature	Description		
Platform management	BMC powered by OpenBMCUEFI based on AMI AptioV		
Connectivity	 Dedicated or shared (NC-SI) LAN interface USB LAN host interface (for Redfish) IPMI host interface (thru KCS) Remote management Redfish 1.9 + 2020.1 Schema IPMI 2.0 RMCP+ Web UI Remote Access KVM/VM Serial interface over IPMI and SSH 		
Monitoring and power control	 Power control Power control Status Boot device override Cooling and heating Monitoring Thermal Power Humidity Board/device monitoring Telco alarm Logging and alerting (logs and events) 		
Configuration	 User management (internal, LDAP) Firmware management Version Update Signature validation Failsafe thru dual bank (available thru Redfish and Web UI) Network management (DHCP and static, VLAN) 		
Security	 Encryption (password encryption, TLS, IPMI Cipher 17) Authentication (LDAP / Active Directory) Firmware signature Secure boot CSM/legacy (available, but disabled by default) 		
Kontron Secure Edge	Management Redfish/Web UI enabledAgent pre-provisioned		
Operating system	Refer to the <u>Validated operating systems</u>		
Thermal management	 Platform Environment Control Interface (PECI) for thermal management support Memory and CPU thermal management 		

ME1210 physical dimensions

Chassis	Measurements (mm [in])	Notes
Depth	343 [13.5]	Body
Width	449 [17.6] max.	Body
	483 [19] max.	Overall width: front mounting brackets included (2 times 17.2 mm [0.7 in])
	465 [18.3]	Between rack mounting points
Height	43.5 [1.7] max.	Body
Side clearance	None	
Front clearance	100 [4]	Recommended
Rear clearance	70 [2.8]	

ME1210 packaging physical dimensions

Depth (mm [in])	Width (mm [in])	Height (mm [in])
489 [19.25]	571.5 [22.5]	190.5 [7.5]

ME1210 shipping weights

Component	Weight (kg [lb])
AC PSU system weight – with four DIMMs and one M.2-2280 SATA SSD	6.95 [15.3]
DC PSU system weight – with four DIMMs and one M.2-2280 SATA SSD	6.85 [15.1]
Packaging (box + foam + bag)	1.4 [3.1]

ME1210 environmental specifications

Environment	Specification
Temperature, operating	DC power supply: -40°C to +65°C (-40°F to +149°F) AC power supply: -5°C to +50°C (23°F to +122°F) The failure of one fan will not impact operation for at least 4 hours at 65 ° C. Certain limitations may apply. These limitations could be the result of the operating temperature range of installed configurable components (e.g., SFP+ module, SSD and PCIe add-in card). Kontron only supports using SFP+ and SSD modules rated for an industrial operating temperature range (-40 ° C to +85 ° C).
Temperature, non-operating	-40°C to +70°C (-40°F to +158°F)
Humidity, operating	5% to 95%, non-condensing
Altitude/pressure, operating	-60 m to 1,800 m altitude without temperature de-rating Up to 4,000 m altitude with temperature de-rating of 1 degree Celsius per 300 m above 1,800 m
Altitude/pressure, non-operating	Up to 4,570 m
Vibration, operating	 This product meets operational random vibration standards. Test profile based on ETSI EN 300 019-2-3 class 3.2 5 Hz to 10 Hz at +12 dB/octave (slope up) 10 Hz to 50 Hz at 0.02 m2/s3 (0.0002 g²/Hz) (flat) 50 Hz to 100 Hz at -12 dB/octave (slope down) 30 minutes for each of the three axes
Vibration, non- operating	 This product meets transportation and storage random vibration standards. Test profile based on GR-63 clause 5.4.3, and ETSI EN 300 019-2-2 class 2.3 5 Hz to 20 Hz at 1 m2/s3 (0.01 g²/Hz) (flat) 20 Hz to 200 Hz at -3 dB/octave (slope down) 30 minutes for each of the three axes
Shock, operating	 This product meets operational shock standards. Test profile based on ETSI EN 300 019-2-3 class 3.2 11 ms half sine, 3 g, three shocks in each direction
Drop/free fall	This product meets Bellcore GR-63 section 5.3. Packaged = 1,000 mm, six surfaces, three edges and four corners Unpackaged = 100 mm, two sides and two bottom corners
Electrostatic discharge	This product meets 8 kV contact, 15 kV air discharge using IEC 61000-4-2 test method.
RoHS and WEEE	This product is designed to meet China RoHS Phase 1 (self-declaration and labeling). This product complies with EU directive 2012/19/EU (WEEE). This product complies with RoHS directive 2011/65/EU as modified by EU 2015/863.

Platform components

Table of contents

- Platform front panel
 - <u>Ethernet switch IO module option</u>
 - <u>Pass-through IO module option</u>
- <u>Platform LEDs</u>
 - <u>General platform LEDs</u>
 - <u>Network port Srv 5 LEDs</u>
 - 10 module network port LEDs
 - <u>Pass-through module</u>
 - Ethernet switch module
 - Power supply LEDs
 - <u>DC power supply</u>
 - <u>AC power supply</u>
- Platform fans
- Platform label

Platform front panel

The ME1210 platform is available in two IO module options as shown below. The platform is also available with a DC or AC power supply. To simplify documentation, only the DC version is shown here.

For information on component pinouts, refer to <u>Connector pinouts and electrical characteristics</u>. For information on cabling, refer to <u>Cabling</u>.

Ethernet switch IO module option



Pass-through IO module option



Platform LEDs

General platform LEDs



Status LED Amber/Red Power LED Green ID/Preheat Indicator LED Blue

CP0294

Status (amber/red)		State		
Off		No active error notification (normal operation)		
Amber On		Major alarm a	Major alarm active	
Red On		Critical alarm active (service/maintenance is required)		
ID/preheat Indicator (blue)	Power	(green)	State	
Off	Off		Both power inputs DOWN or out of range for normal operation	
On	Off		One or both power inputs UP – ACPI Software off state (S5)	
Slow blink	Off		Platform preheating prior to server activation	
Normal blink	Any		BMC is executing an identification request	
Off	Rapid b	olink	Server processor activation complete and executing – ACPI Working state (S0)	
Off	Norma	l blink	UEFI/BIOS started POST	
Off	Norma	l blink or On ¹	UEFI/BIOS hand over to OS boot loader	
Off	0n ¹		Application started/running OK	

¹ By default, the Power LED will "normal blink" until customer application confirms it is running by setting an I/O register bit. Via a UEFI/BIOS setting, the Power LED can be set to steady on after POST (before starting the OS/application), but the default UEFI/BIOS setting leaves that task to the application. Refer to Configuring option Application Ready LED in section <u>Configuring UEFI/BIOS options</u> to configure the appropriate UEFI/BIOS option and to <u>Platform resources for customer application</u> to view an example of a script to integrate into the application.

- Slow blink: 1 short pulse every 2 seconds
- Normal blink: 1 pulse every second
- Rapid blink: 2 pulses every second

Network port Srv 5 LEDs



CP0301

Link (left – green/yellow)	Activity (right – green)	State
Off	Off	No link
Off	On (no activity) Blinking (activity)	10Base-T link established
Yellow On	On (no activity) Blinking (activity)	100Base-TX link established
Green On	On (no activity) Blinking (activity)	1000Base-T link established

IO module network port LEDs

Pass-through module



СР0300

Network link/activity (green)	State
On	Link established, no activity
Blinking	Activity
Off	No link

Ethernet switch module



Network Link/Activity LED (Port 2) Green/Amber Network Link/Activity LED (Port 1) Green/Amber

CP0299

Network link/activity (green/amber)	State
Green On	Link established at maximum port speed (10 or 25Gbps), no activity
Amber On	Link established at below maximum port speed (e.g. link is at 1Gbps on a 10Gpbs port) , no activity
Blinking (green or amber based on port speed)	Activity
Off	No link

Power supply LEDs

DC power supply



Output status/operation (amber/green)	State
Off	Hot-swap controller Off or FPGA not loaded
Amber On	Hold-up not ready or voltage too low for start-up
Green On	Hold-up ready
Input status/operation (amber/green)	State
Off	No 48V
Amber On	Hot-swap controller Off (low input voltage or fault)
Green On	Hot-swap controller On

AC power supply



Input status/operation (green)	State
On	Input voltage operating within normal specified range
Blinking	Input voltage operating in: 1) overvoltage warning, or 2) undervoltage warning
Off	Input voltage operating: 1) above overvoltage range, or 2) below undervoltage range, or 3) not present
Output status/operation (amber/green)	State
Green On	Power good mode: Main output and standby output enabled with no power supply warning or fault detected
Blinking Green	Standby mode: Standby output enabled with no power supply warning or fault detected
Blinking Amber	Warning mode: Power supply warning detected as per PMBus STATUS_X reporting bytes
Amber On	Fault mode: Power supply fault detected as per PMBus STATUS_X reporting

Platform fans

There are 8 fans inside the platform. Refer to <u>Components installation and assembly</u> for instructions on how to replace a fan.

Platform label

The platform has a manufacturing label and a QR code label. The manufacturing label provides:

- The part number
- A description of the product including configurable options

• The manufacturing batch number Here is an example of the information that could be displayed: Kontron part # = 1069-1291 Kontron product name = ME1210BX-BCDDBXX ZZXX1234HH (XX) = 01A0001100



Relevant section:

MAC addresses (for QR code results, which include the serial number)

Product architecture

Table of contents

- <u>Block diagram</u>
 - Block diagram with the Ethernet switch IO module option
 - Block diagram with the pass-through IO module option
- <u>Network planes</u>
- Internal connections
 - Internal connections with the Ethernet switch IO module option
 - Internal connections with the pass-through IO module option

Block diagram

Block diagram with the Ethernet switch IO module option



Block diagram with the pass-through IO module option



Network planes

The ME1210 platform provides:

• 3 network planes (management plane, control plane, data plane)

Network planes	Description	Speed (GbE)	Component access
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
Control plane	The control plane carries customer application signaling traffic. This plane is used to control customer applications.	1	Server
Data plane	The data plane carries customer data application traffic. This plane is used to deliver service to end users.	1/10/25	Server, BMC, switch NOS

Internal connections

Internal connections with the Ethernet switch IO module option



Internal connections with the p ass-through IO module option



Description of system access methods

Table of contents

- Paths to the management interface (BMC)
- <u>Paths to the operating system</u>
- Paths to the UEFI/BIOS options
- Paths to the switch network operating system (NOS)

To configure, monitor and troubleshoot the ME1210 platform and its components, several interfaces can be used:

- Operating system through the management plane, control plane, data plane or the serial port of the platform
- UEFI/BIOS through the management plane or the serial port of the platform
- Management interface (BMC) through the management plane and the data plane of the platform
- Switch network operating system (NOS) (on platforms equipped with the Ethernet switch IO module option) through the management plane and the data plane

Paths to the management interface (BMC)

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

Paths to the management interface (BML)	
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, and locally from the server operating system via the Redfish host interface.	 Remote server control and monitoring OS video access Firmware upgrades
Redfish <i>This is the ideal path for automated monitoring/control script once the platform has been configured for the first time.</i> <i>Accessible from the management plane, and locally from the server operating system via the Redfish host interface.</i>	Remote server monitoringRemote server controlFirmware upgrades
IPMI over LAN (IOL) <i>This is a good path for automated monitoring/control script once the platform has been configured for the first time.</i> <i>Accessible from the management plane</i> .	Remote server control and monitoring
IPMI via KCS Accessible locally from the server operating system.	 Local access to the BMC from the operating system for server monitoring Initial BMC configuration

Paths to the operating system

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 <i>This is the recommended path for first time out-of-the-box system</i> <i>configuration.</i> <i>Fail-safe path to access the server if any elements (OS, UEFI/BIOS, etc.) get</i> <i>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 a network session to the OS 	
Serial over LAN using the Web UI Fail-safe path to access the server if any elements (OS, UEFI/BIOS, etc.) get misconfigured. Accessible from the management plane.	 OS network interface configuration Unable to establish a network session to the OS OS serial console access 	
Serial over LAN using SSH from a remote computer Accessible from the management plane.	 OS network interface configuration Unable to establish a network session to the OS OS serial console access 	
Serial ov er LAN using IPMI from a remote computer Accessible from the management plane.	OS network interface configurationUnable to establish a network session to the OS	

SSH/RDP/Customer application protocols•Ideal path once OS installation and OS network interface configurations have been•performed.•Accessible from the control plane and the data plane.•	 Operating the platform under normal operation Remote access to the OS
Serial console (physical connection)•Fail-safe path to access all server components when elements (OS, BMC, UEFI/BIOS, etc.) get misconfigured.•Accessible from the physical port.•	 Initial OS network interface configuration No configuration performed on BMC Troubleshooting

Paths to the UEFI/BIOS options

To access the UEFI/BIOS options through one of the paths, refer to <u>Accessing the UEFI or BIOS</u>.

Paths to the UEFI/BIOS options		
Path description	Main reasons for use	
Serial over LAN using the Web UI This is the recommended path for first time out-of-the-box system configuration. Fail-safe path to access the server if any elements (OS, UEFI/BIOS, etc.) get misconfigured. Accessible from the management plane.	 Initial UEFI/BIOS configuration UEFI/BIOS video access 	
KVM Fail-safe path to access the server if any elements (OS, UEFI/BIOS , etc.) get misconfigured. Accessible from the management plane.	Initial UEFI/BIOS configurationUEFI/BIOS video access	
Serial over LAN using SSH from a remote computer Accessible from the management plane.	 Initial UEFI/BIOS configuration UEFI/BIOS serial console access OS network interfaces not configured, but BMC network access is available 	
Serial over LAN using IPMI from a remote computer Accessible from the management plane.	 Initial UEFI/BIOS configuration UEFI/BIOS serial console access OS network interfaces not configured, but BMC network access is available 	
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, and locally from the server operating system via the Redfish host interface.	Basic UEFI/BIOS configuration	
Serial console (physical connection) Fail-safe path to access all server components when elements (OS, BMC, UEFI/BIOS, etc.) get misconfigured. Accessible from the physical port.	 Initial UEFI/BIOS configuration No configuration performed on BMC Troubleshooting 	

Paths to the switch network operating system (NOS)

To access the switch network operating system through one of the paths, refer to Accessing the switch NOS.

Paths to the switch network operating system (NOS)	
Path description	Main reasons for use
Switch Web UI This is the recommended path for first time out-of-the-box system configuration. Accessible from the data plane.	Switch NOS control and monitoringFirmware upgrades
Serial over LAN using the BMC Web UI Accessible from the management plane.	NOS network interface configurationInitial switch NOS configuration
Serial over LAN using SSH from a remote computer Accessible from the management plane.	NOS network interface configurationInitial switch NOS configuration

SSH from a remote computer	 Switch NOS control and monitoring
This is a good path for automated monitoring/control script once the platform has	Firmware upgrades
been configured for the first time.	
Accessible from the data plane.	
SSH from the integrated server	• Local access to the s witch NOS for control and
Accessible locally from the server operating system.	monitoring

Recommended technical expertise

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.

Planning

- Environmental considerations
- Power consumption and power budget
- MAC addresses
- PCI mapping
- <u>Connector pinouts and electrical characteristics</u>
- <u>Material, information and software required</u>
- Platform, modules and accessories
- <u>Hardware compatibility list</u>
- <u>Validated operating systems</u>
- <u>Security</u>

Environmental considerations

The ME1210 platform has been designed to work over the extended temperature range of -40° C to $+65^{\circ}$ C (-40° F to $+149^{\circ}$ F) when using a DC power supply or -5° C to $+50^{\circ}$ C (23° F to $+122^{\circ}$ F) when using an AC power supply and to withstand non-condensing humidity levels up to 95%. This equipment should not be exposed directly to the elements (sun, rain, wind, dust). For installations in outdoor or other harsh, uncontrolled environments, appropriate housing must be used.

If components that do not support the ME1210 temperature range are installed, the customer is responsible to configure sensor thresholds and thermal management accordingly. Refer to <u>Configuring sensors and thermal parameters</u> and <u>Platform cooling and thermal management</u>.

When powering up the ME1210 at the lower end of the extended temperature range, it is normal for the system to take some time for preheating before completing the initial boot sequence. Once powered up and in operation, the system will dissipate enough power to stay warm. The warm-up delay of the deep cold start is a rare event that could occur only at the initial power-up or after a power outage in a cold environment. Special considerations must be taken if you are exposing the ME1210 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.

If you are installing the ME1210 in a hot environment, it is recommended to take additional measures to maximize the cooling and air circulation as constant exposure to high temperatures reduces the life expectancy of electronic equipment.

The ME1210 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.

Power consumption and power budget

Table of contents

- <u>DC power supply input voltage and current requirements</u>
- <u>AC power supply input voltage and current requirements</u>
- Power consumption examples
 - System power consumption
 - <u>Component power consumption examples</u>

DC power supply input voltage and current requirements

DC input voltage	
-54 VDC	
-40 VDC	
-57 VDC	
17 A at -40 VDC; 12 A at -57 VDC	
660 W	

AC power supply input voltage and current requirements

AC input voltage			
Nominal	115/230 VAC		
Minimum	90 VAC		
Maximum	264 VAC		
AC input current			
Maximum	8.5 Arms at 90 VAC		
Power input			
Maximum	700 W		

Power consumption examples



This section provides power consumption values obtained in a test environment. Actual values highly depend on the application that will be used. The values provided must therefore only be used as a general reference and tests need to be performed with the actual hardware configuration and application that will be used.

System power consumption

The following ME1210 configuration was used to obtain the typical power consumption values shown in the table below:

- Xeon[®] D-2187NT processor
- Ethernet switch IO module with standard OCXO
- Eight 64 GB LRDIMM
- One 128 GB M.2 SATA module
- Two 25GBASE-LR SFP28 modules
- Two 10GBASE-SR SFP+ modules
- Two PCIe add-in cards: 75 W power test jigs
- DC PSU
- Standard 8 fans

Status	Typical consumption (W)	Notes
Idle	76	Idle power consumption was measured in CentOS 7 once it had finished booting
Maximum application	380	Maximum power was measured in CentOS 7 running "mprime -t" as a stress application
Maximum application and fan	525	Maximum power was measured in CentOS 7 running "mprime $\mbox{-t"}$ as a stress application with fans at maximum speed

NOTE:

- DC power supply input is at 48 VDC.
- Test was performed at ambient temperature.
- Power consumption varied during the test.
- Power consumption was measured at the DC power supply input.

Component power consumption examples

Power figures given per component in the table were measured at the DC power supply output (12 V side). They therefore do not include the PSU efficiency.

Power at the DC power supply input (48 V side) is typically 5% higher.

Components	Typical consumption (W)	Notes
Intel ® Xeon ® D-2187NT	110	TDP
Intel ® Xeon ® D-2183IT	100	TDP
Ethernet switch IO module with standard OCXO	23	Ethernet switch has 4 SFP interfaces with link up
Fans	23	At maximum speed
64 GB LRDIMM	6	Under active use
16 GB RDIMM	3.5	Under active use
SATA 128 GB M.2 SSD	3	Under active use. Idle power is 0.5 W.
NVMe 960 GB M.2 SSD	7	Under active use. Idle power is 4 W.
25GBASE -LR SFP28	1	Connection is link up with partner device
10GBASE-SR SFP+	1	Connection is link up with partner device

NOTICE

If all the optional components are used and operate at maximum power, the system could exceed its maximum power consumption.

MAC addresses

Table of contents

- MAC addresses
 - <u>Ethernet switch IO module option</u>
 - Pass-through IO module option
- Discovering the platform MAC addresses
 - Discovering a MAC address using the QR code
 - Discovering a MAC address using the UEFI/BIOS

Relevant section:

Product architecture

MAC addresses

Ethernet switch IO module option

MAC address	Interface description	Device	Note
MAC_BASE	Front panel Srv 5	ВМС	Shared connector with server
MAC_BASE + 1	Server internal port 4	ВМС	Internal to switch interface 1/13 . Shared connection with server.
MAC_BASE + 2	Server internal port 1	Server	Internal to switch interface 1/13
MAC_BASE + 3	Server internal port 2	Server	Internal to switch interface 1/14
MAC_BASE + 4	Server internal port 3	Server	Internal to switch interface 1/15
MAC_BASE + 5	Server internal port 4	Server	Internal to switch interface 1/16. Shared connection with BMC.
MAC_BASE + 6	Front panel Srv 5	Server	Server control plane. Shared connection with BMC
SW_MAC_BASE	Any switch interface	Switch NOS	MAC used by the switch network operating system for configuration/monitoring access
SW_MAC_BASE + 63	Reserved	Switch NOS	Reserved MAC for switch network operating system

Pass-through IO module option

MAC address	Interface description	Device	Note
MAC_BASE	Front panel Srv 5	BMC	Shared connection with server
MAC_BASE + 1	Front panel Srv 4	BMC	Shared connection with server
MAC_BASE + 2	Front panel Srv 1	Server	Server data plane
MAC_BASE + 3	Front panel Srv 2	Server	Server data plane
MAC_BASE + 4	Front panel Srv 3	Server	Server data plane
MAC_BASE + 5	Front panel Srv 4	Server	Server data plane . Shared connection with BMC.
MAC_BASE + 6	Front panel Srv 5	Server	Server control plane. Shared connection with BMC.

Discovering the platform MAC addresses

The platform MAC addresses can be discovered:

- Using the <u>QR code</u>
- Using the <u>UEFI/BIOS</u>

Discovering a MAC address using the QR code

Step_1 Using a QR code application, scan the QR code. Record the information obtained in your device (e.g. by taking a s/ screen shot).

S/N:901702000 P/N:1065-2823 BATCH:0A00000 MAC: 00A0A5D6402A in the table above 00A0A5E1B934 replace SW_MAC switch module.	 Platform serial number Platform part number 0001 = Platform production lot number A = First MAC address attributed to the BMC/server. Value to be used to replace MAC_fe = First MAC address attributed to the integrated Ethernet switch. Value to be used to C_BASE in the table above. This is only present for an ME1210 configured with the IO Eth 	MAC: 00A0A5D6402A 00A0A5E1B934 BASE hernet
---------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------

Discovering a MAC address using the UEFI/BIOS

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.

Accessing the BMC network configuration menu

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

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 Mgmt Security Boot Event Logs >			
		BIOS Information Choose the system BIOS Vendor American Megatrends Idefault language Core Version 5.14 Idefault language Compliancy UEFI 2.6; PI 1.4 Idefault language			
		Build Date and Time 06/26/2019 09:12:28 Access Level Administrator	1		
		FPGA Version 2.02.0800AD12			
		Memory Information ^v: Select Item Total Memory 32768 MB Enter: Select +/-: Change Opt. +/-: Change Opt.	1		
		System Language (English) (F1: General Help (F2: Previous Values System Date (Ved 07/10/2019) (F3: Optimized Defaults	 		
		System Time [13:47:54] F4: Save & Exit ESC: Exit	1		
		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 IntelRCSetup Server Mgmt Security Boot Event Logs	>		
		BHC Interface(s) KCS, USB ^ Press <enter> to enabl + or disable Serial Mux</enter>	le t		
		Wait For BMC [Disabled] + configuration. FRB-2 Timer [Enabled] +			
		FRD-2 limer timeout [6 minutes] * FRB-2 Timer Folicy [Power Cycle] *			
		OS Watchdog Timer [Disabled] * OS Wtd Timer Timeout [10 minutes] *			
		OS Wtd Timer Policy [Reset] * Serial Mux [Disabled] * Select Screen			
		<pre>> System Event Log * ""' Select Item > System Event Log * Enter: Select > View FPU information # !+/-: Change Out</pre>			
		> BHC network configuration * F1: General Help > View System Event Log * F2: Previous Values			
		> BRC User Settings * F3: Optimized Defaults BRC Warm Reset V F4: Save & Exit ESC: Exit	.s 		
		Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.	λB		
Step_3	The BMC network configuration menu is displayed.	Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Server Mgmt			
	NOTE: When the platform is powered up after being shut off, the		AN		
	UEFI/BIOS may load before the BMC has received its IP address. In this	Configure IPV4 support * statically or * statically (by BIOS or * dynamically (by BIOS or *)	r		
	case, the UEFI/BIOS menu information will need to be refreshed by	* BHC). Unspecified Lan channel 1 + option will not modify	y I		
	restarting the server and re-entering the UEFI/BIOS .	Configuration Address [Unspecified] + any BHC network source + parameters during BIOS	s		
		Current Configuration DynamicAddresssmcDucp + Address source + + Station IP address 172.16.205.245 + ><: Select Screen			
		Subnet mask 255.255.0.0 + ^v: Select Item Station MAC address 00-A0-A5-D6-33-2A + Enter: Select	i		
		Router IP address 172.16.0.1 + +/-: Change Opt. Router MAC address 00-05-64-2F-10-5F + F1: General Help			
		+ F2: Previous Values Lan channel 2 + F3: Optimized Defaults V F4: Save & Exit	.s		
		ESC: Exit	/		
		Version 2.20.1271. Copyright (C) 2019 $kmerican$ Megatrends, Inc.	ÅB		

PCI mapping

Table of contents

- Platform PCI mapping
- Feature-dependent entries
 - Entries when Intel® QuickAssist Technology (QAT) enabled CPUs are present
 - Entries when Intel® QuickAssist Technology (QAT) enabled CPUs are not present

To obtain the platform PCI mapping, use command lspci -nn . The lspci description database may have to be updated with command updatepciids .

Platform PCI mapping

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 04)
00:11.5	8086	a1d2	SATA controller	SATA controller: Intel Corporation C620 Series Chipset Family SSATA Controller [AHCI mode] (rev 04)
00:14.0	8086	alaf	USB controller	Intel Corporation C620 Series Chipset Family USB 3.0 xHCI Controller (rev 04)
00:14.2	8086	a1b1	Signal processing controller	Intel Corporation C620 Series Chipset Family Thermal Subsystem (rev 04)
00:16.0	8086	a1ba	Communication controller	Intel Corporation C620 Series Chipset Family MEI Controller #1 (rev 04)
00:16.1	8086	a1bb	Communication controller	Intel Corporation C620 Series Chipset Family MEI Controller #2 (rev 04)
00:16.4	8086	albe	Communication controller	Intel Corporation C620 Series Chipset Family MEI Controller #3 (rev 04)
00:1c.0	8086	a190	PCI bridge	Intel Corporation C620 Series Chipset Family PCI Express Root Port #1 (rev f4)
00:1c.2	8086	a192	PCI bridge	Intel Corporation C620 Series Chipset Family PCI Express Root Port #3 (rev f4)
00:1c.3	8086	a193	PCI bridge	Intel Corporation C620 Series Chipset Family PCI Express Root Port #4 (rev f4)
00:1c.4	8086	a194	PCI bridge	Intel Corporation C620 Series Chipset Family PCI Express Root Port #5 (rev f4)
00:1f.0	8086	a1c8	ISA bridge	Intel Corporation Device a1c8 (rev 04)
00:1f.2	8086	a1a1	Memory controller	Intel Corporation C620 Series Chipset Family Power Management Controller (rev 04)
00.15 /	,0000	1 7		

Version 2.0 (June 2022)

www.kontron.com

UU: I†.4	8086	ala⊰	SMBus	Intel Corporation Cb2U Series Chipset Family SMBus (rev U4)
00:1f.5	8086	a1a4	Serial bus controller	Intel Corporation C620 Series Chipset Family SPI Controller (rev 04)
02:00.0	1a03	1150	PCI bridge	ASPEED Technology, Inc. AST1150 PCI-to-PCI Bridge (rev 04)
03:00.0	1a03	2000	VGA compatible controller	ASPEED Technology, Inc. ASPEED Graphics Family (rev 41)
04:00.0	8086	1533	Ethernet controller	Intel Corporation I210 Gigabit Network Connection (rev 03)
05:00.0	XXXX	XXXX	Module in left M.2 slot (J8)	depends on M.2 module
06:00.0	XXXX	XXXX	Module in right M.2 slot (J9)	depends on M.2 module
16:05.0	8086	2034	System peripheral	Intel Corporation Sky Lake-E VT-d (rev 04)
16:05.2	8086	2035	System peripheral	Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04)
16:05.4	8086	2036	PIC	Intel Corporation Sky Lake-E IOxAPIC Configuration Registers (rev 04)
16:08.0	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:08.1	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:08.2	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:08.3	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:08.4	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:08.5	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:08.6	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:08.7	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:09.0	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:09.1	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:09.2	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:09.3	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:09.4	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:09.5	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:09.6	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:09.7	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0a.0	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0a.1	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0a.2	8086	208d	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0e.0	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0e.1	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0e.2	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0e.3	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0e.4	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0e.5	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0e.6	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0e.7	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0f.0	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0f.1	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0f.2	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0f.3	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0f.4	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0f.5	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
		·		

Version 2.0 (June 2022)

www.kontron.com

16:0f.6	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:0f.7	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:10.0	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:10.1	8086	208e	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:1d.0	8086	2054	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:1d.1	8086	2055	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:1d.2	8086	2056	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:1d.3	8086	2057	System peripheral	Intel Corporation Sky Lake-E CHA Registers (rev 04)
16:1e.0	8086	2080	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
16:1e.1	8086	2081	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
16:1e.2	8086	2082	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
16:1e.3	8086	2083	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
16:1e.4	8086	2084	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
16:1e.5	8086	2085	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
16:1e.6	8086	2086	System peripheral	Intel Corporation Sky Lake-E PCU Registers (rev 04)
17:0.0	XXXX	XXXX	Card in expansion " Slot 1 "	depends on PCIe expansion card
64:05.0	8086	2024	System peripheral	Intel Corporation Sky Lake-E VT-d (rev 04)
64:05.2	8086	2025	System peripheral	Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04)
64:05.4	8086	2026	PIC	Intel Corporation Sky Lake-E IOxAPIC Configuration Registers (rev 04)
64:08.0	8086	2066	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
64:09.0	8086	2066	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
64:0a.0	8086	2040	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
64:0a.1	8086	2041	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
64:0a.2	8086	2042	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
64:0a.3	8086	2043	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
64:0a.4	8086	2044	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
64:0a.5	8086	2045	System peripheral	Intel Corporation Sky Lake-E LM Channel 1 (rev 04)
64:0a.6	8086	2046	System peripheral	Intel Corporation Sky Lake-E LMS Channel 1 (rev 04)
64:0a.7	8086	2047	System peripheral	Intel Corporation Sky Lake-E LMDP Channel 1 (rev 04)
64:0b.0	8086	2048	System peripheral	Intel Corporation Sky Lake-E DECS Channel 2 (rev 04)
64:0b.1	8086	2049	System peripheral	Intel Corporation Sky Lake-E LM Channel 2 (rev 04)
64:0b.2	8086	204a	System peripheral	Intel Corporation Sky Lake-E LMS Channel 2 (rev 04)
64:0b.3	8086	204b	System peripheral	Intel Corporation Sky Lake-E LMDP Channel 2 (rev 04)
64:0c.0	8086	2040	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
64:0c.1	8086	2041	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
64:0c.2	8086	2042	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
64:0c.3	8086	2043	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
64:0c.4	8086	2044	System peripheral	Intel Corporation Sky Lake-E Integrated Memory Controller (rev 04)
64:0c.5	8086	2045	System peripheral	Intel Corporation Sky Lake-E LM Channel 1 (rev 04)
64:0c.6	8086	2046	System peripheral	Intel Corporation Sky Lake-E LMS Channel 1 (rev 04)
64:0c.7	8086	2047	System peripheral	Intel Corporation Sky Lake-E LMDP Channel 1 (rev 04)
64:0d.0	8086	2048	System peripheral	Intel Corporation Sky Lake-E DECS Channel 2 (rev 04)
64:0d.1	8086	2049	System peripheral	Intel Corporation Sky Lake-E LM Channel 2 (rev 04)
64:0d.2	8086	204a	System peripheral	Intel Corporation Sky Lake-E LMS Channel 2 (rev 04)

Version 2.0 (June 2022)

www.kontron.com

64:0d.3	8086	204b	System peripheral	Intel Corporation Sky Lake-E LMDP Channel 2 (rev 04)
65:0.0	XXXX	XXXX	Card in expansion " Slot 2 "	depends on PCIe expansion card
b2:00.0	8086	2030	PCI bridge	Intel Corporation Sky Lake-E PCI Express Root Port A (rev 04)
b2:05.0	8086	2034	System peripheral	Intel Corporation Sky Lake-E VT-d (rev 04)
b2:05.2	8086	2035	System peripheral	Intel Corporation Sky Lake-E RAS Configuration Registers (rev 04)
b2:05.4	8086	2036	PIC	Intel Corporation Sky Lake-E IOxAPIC Configuration Registers (rev 04) (prog-if 20 [IO(X)-APIC])
b2:12.0	8086	204c	Performance counters	Intel Corporation Sky Lake-E M3KTI Registers (rev 04)
b2:12.1	8086	204d	Performance counters	Intel Corporation Sky Lake-E M3KTI Registers (rev 04)
b2:12.2	8086	204e	System peripheral	Intel Corporation Sky Lake-E M3KTI Registers (rev 04)
b2:15.0	8086	2018	System peripheral	Intel Corporation Sky Lake-E M2PCI Registers (rev 04)
b2:16.0	8086	2018	System peripheral	Intel Corporation Sky Lake-E M2PCI Registers (rev 04)
b2:16.4	8086	2018	System peripheral	Intel Corporation Sky Lake-E M2PCI Registers (rev 04)
b2:17.0	8086	2018	System peripheral	Intel Corporation Sky Lake-E M2PCI Registers (rev 04)
b3:00.0	8086	37c0	PCI bridge	Intel Corporation Device 37c0 (rev 04)
b4:00.0	8086	37c2	PCI bridge	Intel Corporation Device 37c2 (rev 04)
b4:01.0	8086	37c3	PCI bridge	Intel Corporation Device 37c3 (rev 04)
b4:02.0	8086	37c4	PCI bridge	Intel Corporation Device 37c4 (rev 04)
b4:03.0	8086	37c5	PCI bridge	Intel Corporation Device 37c5 (rev 04)

Feature-dependent entries

Entries when Intel [®] QuickAssist Technology (QAT) enabled CPUs are present

b5:00.0	8086	37c8	Co-processor	Intel Corporation C62x Chipset QuickAssist Technology (rev 04)
b6:00.0	8086	37c8	Co-processor	Intel Corporation C62x Chipset QuickAssist Technology (rev 04)
b7:00.0	8086	37c8	Co-processor	Intel Corporation C62x Chipset QuickAssist Technology (rev 04)
b8:00.0	8086	37d3	Ethernet controller (pass- through)	Intel Corporation Ethernet Connection X722 for 10GbE SFP+ (rev 04)
	8086	37cE	Ethernet controller (switch)	Intel Corporation Ethernet Connection X722 for 10GbE backplane (rev 04)
b8:00.1	8086	37d3	Ethernet controller (pass- through)	Intel Corporation Ethernet Connection X722 for 10GbE SFP+ (rev 04)
	8086	37cE	Ethernet controller (switch)	Intel Corporation Ethernet Connection X722 for 10GbE backplane (rev 04)
b8:00.2	8086	37d3	Ethernet controller (pass- through)	Intel Corporation Ethernet Connection X722 for 10GbE SFP+ (rev 04)
	8086	37cE	Ethernet controller (switch)	Intel Corporation Ethernet Connection X722 for 10GbE backplane (rev 04)
b8:00.3	8086	37d3	Ethernet controller (pass- through)	Intel Corporation Ethernet Connection X722 for 10GbE SFP+ (rev 04)
	8086	37cE	Ethernet controller (switch)	Intel Corporation Ethernet Connection X722 for 10GbE backplane (rev 04)

Entries when Intel [®] QuickAssist Technology (QAT) enabled CPUs are not present

b5:00.0	8086	37d3	Ethernet controller (pass- through)	Intel Corporation Ethernet Connection X722 for 10GbE SFP+ (rev 04)
	8086	37cE	Ethernet controller (switch)	Intel Corporation Ethernet Connection X722 for 10GbE backplane (rev 04)
b5:00.1	8086	37d3	Ethernet controller (pass- through)	Intel Corporation Ethernet Connection X722 for 10GbE SFP+ (rev 04)
	8086	37cE	Ethernet controller (switch)	Intel Corporation Ethernet Connection X722 for 10GbE backplane (rev 04)
b5:00.2	8086	37d3	Ethernet controller (pass- through)	Intel Corporation Ethernet Connection X722 for 10GbE SFP+ (rev 04)
	8086	37cE	Ethernet controller (switch)	Intel Corporation Ethernet Connection X722 for 10GbE backplane (rev 04)
b5:00.3	8086	37d3	Ethernet controller (pass- through)	Intel Corporation Ethernet Connection X722 for 10GbE SFP+ (rev 04)
	8086	37cE	Ethernet controller (switch)	Intel Corporation Ethernet Connection X722 for 10GbE backplane (rev 04)
Connector pinouts and electrical characteristics

Table of contents

- <u>Platform external connectors</u>
 - Ethernet switch IO module option
 - <u>Pass-through IO module option</u>
- Description, pinout and electrical characteristics of external connectors
 - <u>SMA GNSS RF input</u>
 - SMA PPS output
 - RJ45 alarm port
 - RJ45 serial port
 - <u>SFP+ and SFP28</u>
 - <u>Ethernet switch IO module option</u>
 - Pass-through 10 module option
 - RJ45 Ethernet management port
 - USB interfaces
 - •
- <u>DC power supply input connector</u>
- AC power supply input connector

Customers can build custom cables based on the information provided in this section.

Relevant sections:

Platform components

Cabling



All connectors and interfaces are ESD protected (IEC 61000-4-2, 15kV (air), 8kV (discharge)), unless otherwise specified.



All connectors and interfaces are intended for a short connection (less 6 meters) within the same cabinet, unless otherwise specified.

Platform external connectors

Ethernet switch IO module option



Pass-through IO module option



Description, pinout and electrical characteristics of external connectors

This section describes the following connectors and lists their pinouts and electrical characteristics: Version 2.0 (June 2022) www.kontron.com

- SMA GNSS RF input available only on platforms with the Ethernet switch IO module
- SMA PPS output available only on platforms with the Ethernet switch IO module
- RJ45 alarm port
- RJ45 serial port
- SFP+ and SFP28 ports
- RJ45 Ethernet management port
- USB interfaces
- DC power supply input connector
- AC power supply input connector

SMA GNSS RF input



Mating connector: SMA Male

Description:

- Interface with a link to a NEO-M9N module from <u>u-blox</u>
- Can be used with passive and active antennas (the antenna must be matched to the requisite 50 ohms)
- Suitable for connection to external outdoor antennas
- RF input
 - Maximum input power is < 0 dBm
 - Good antenna with > 4 dBic gain recommended
 - Good low noise amplifier (LNA) with a noise figure of less than 2 dB recommended
 - Active antenna gain of 15 dB to 35 dB (maximum) recommended
- DC bias output
 - ∘ 5V±5%
 - Up to 150 mA
 - Over-current protected (< 350 mA)
 - Thermally protected
- Includes surge protection (IEC 61000-4-5 class 2, 1 kV)

Relevant section:

<u>Cabling</u>

SMA PPS output



Mating connector: SMA Male

Description:

- Compliant with ITU-G.703, section 19.2
- Output is 3.3 V source terminated (50 ohms)
- Output duty cycle is 10% (100 ms)
- Suitable for use with unterminated loads:
 - \circ V _{OH} > 2.6 V at I _{OH} = -12 mA
 - $\circ~$ V $_{OL}$ < 0.7 V at I $_{OH}$ = 12 mA
- Suitable for use with 50 ohms to ground terminated loads:
 - V _{OH} > 1.2 V
 - V_{OL} < 0.3 V
- PPS rising edge (at SMA) aligned within ± 5 ns from internal time of day (ToD) counter

RJ45 alarm port



Description:

The alarm port is intended for use with normally closed dry contacts only. It uses an RS-232 buffer for its electrical interface and is therefore fully protected against shorts.



Open circuit voltage:

- ALARM_CM: 5 V to 7 V, current limited to < 60 mA
- ALARM_IN[4:1]: -7 V to -5 V, 10 kiloohms impedance

External connector pinout:

Pin	Signal description	Pin	Signal description
1	ALARM_IN[1]	5	ALARM_IN[4]
2	ALARM_IN[2]	6	NC
3	NC	7	NC
4	ALARM_IN[3]	8	ALARM_CM

Relevant sections: Discrete sensors monitoring procedure

Interpreting sensor data

RJ45 serial port



Description:

The serial port is electrically compatible to standard RS-232.

|--|

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

SFP+ and SFP28

Ethernet switch IO module option



The port map will determine whether the port is an SFP+ or SFP28 port. Refer to <u>Configuring the switch</u> for information on how to configure the port map.

Mating connector: SFP+ or SFP28 modules

Pass-through IO module option



Mating connector: SFP+ modules

Description:

The SFP+ and SFP28 interfaces are standardized and are compliant to the following (non exhaustive):

- SFF-8431, SFF-8432 (SFP+)
- SFF-8402 (SFP28)
- 1000BASE-LX/SX, SFP-MSA, SFF INF-8074i (pass-through IO module and Ethernet switch IO module)
- 10GBASE-CR/LR/SR, IEEE802.3 clause 52 (pass-through IO module and Ethernet switch IO module)
- 25GBASE-CR/LR/SR, IEEE802.3 clause 110 and 112 (Ethernet switch IO module)

NOTICE Always use optical modules with optical fiber for long (> 6 meters) or outdoor connections.

Relevant section:

Hardware compatibility list

RJ45 Ethernet management port



Description:

This interface is a standard 10/100/1000 Base-T port and is compliant to the following (non exhaustive):

• IEEE 802.3 clause 40



USB interfaces



Mating connector: USB

Description:

The USB interfaces are standard type A host connectors and comply with USB 3.1 and USB 2.0 specifications, available from the <u>USB Implementers</u> Forum.

DC power supply input connector



Mating connector: Refer to Cabling to build appropriate cables.

Description :

The DC power input is designed in accordance with Telcordia GR-1089 and ATIS-0600315 and has the following characteristics:

- Redundant feeds (using active OR-ing diodes)
- -40.0 V to -56.7 V continuous operating voltage
- Internal fuses (30 A on RTN_A and RTN_B; 25 A on -48V_A, -48V_B)
- Inrush and over-current protection with active hot-swap controller
- Includes surge protection (IEC 61000-4-5 class 2, 1kV)

NOTICE The DC power interface is surge protected and cable length is not restricted to 6 meters. This interface is adequate for connection to local DC power systems (GR-1089 type 8) and intra-cell site DC power limited outdoor exposure (type 8b).

AC power supply input connector



Mating connector: IEC C13

Description:

The AC power input has the following basic characteristics (refer to Murata documentation for component D1U54P-W-650-12-HB4C for more details):

- 90 to 264 VAC, 47 to 63 Hz
- Inrush limited (25 Apk)
- 80 plus platinum efficiency
- Includes surge protection (IEC 61000-4-5 class 3, 2kV)

Material, information and software required

Table of contents

- <u>Material and information required</u>
 - Optional adapter
 - <u>Component installation and assembly</u>
 - PCle add-in card
 - Power cables and tooling
 - For a DC PSU
 - For an AC PSU
 - <u>Rack installation material</u>
 - <u>Network cables and modules</u>
 - Ethernet switch IO module option
 - <u>Pass-through IO module option</u>
- <u>Software required</u>

Material and information required

For a list of compatible components, refer to the Hardware compatibility list.

Optional adapter



Component installation and assembly

PCle add-in card

Refer to Platform resources for customer application to view examples of script to integrate into the application to manage customer-specific temperature sensors.

ltem_1	One T10 Torx screwdriver
ltem_2	(Optional) One thermal probe for temperature monitoring (if physical temperature monitoring is chosen)
ltem_3	(Optional) Glue that can withstand the temperature generated by the PCIe add-in card and that has appropriate properties for the application (e.g. Loctite adhesive 444 and Loctite activator SF 7452)

Power cables and tooling

For a DC PSU

ltem_1	 Crimp lugs: Two or four Molex insulated spade crimp lugs for 14-16 wire gauge (19131-0023) OR Two or four Panduit insulated ring crimp lugs for 10-12 wire gauge (EV10-6RB-Q)
ltem_2	 Black stranded wire to build the power cable based on the length required: Proper wire gauge for application based on cable specification and local electrical code Maximum insulation diameter: 4.40 mm [0.175 in] for Molex crimp lugs OR Maximum insulation diameter : 5.8 mm [0.23 in] for Panduit crimp lugs
ltem_3	 Red stranded wire to build the power cable based on the length required: Proper wire gauge for application based on cable specification and local electrical code Maximum insulation diameter : 4.40 mm [0.175 in] for Molex crimp lug OR Maximum insulation diameter : 5.8 mm [0.23 in] for Panduit crimp lug
ltem_4	One hand crimp tool: • Molex Premium Grade Hand Crimp Tool (640010100) OR • Panduit Hand Crimp Tool (638130400)
Item_5	One 8 AWG ground cable based on the length required
ltem_6	One ground lug right angle, 8 AWG (Kontron P/N 1064-4226)
ltem_6 ltem_7	One ground lug right angle, 8 AWG (Kontron P/N 1064-4226) One hand crimp tool, Panduit CT-1700

For an AC PSU

ltem_1	C13 to CEE 7/7 European AC power cord, 10A/250 VAC, 1.8 m long
	OR
	C13 to NEMA 5-15P AC power cord, 10A/125 VAC, 2 m long

Rack installation material

ltem_1	Racking fasteners (rack specific)

Network cables and modules

Ethernet switch IO module option

ltem_1	One SFP optical module (SX, LX, SR, LR) with compatible optical cable
ltem_2	One RJ45 Ethernet management/control plane cable
ltem_3	One RJ45 serial connection cable

Pass-through IO module option

ltem_1	One SFP optical module (SX, LX, SR, LR) with compatible optical cable
ltem_2	One RJ45 Ethernet management/control plane cable
ltem_3	One RJ45 serial connection cable

Software required

ltem_1	An HTTP client such as cURL or Postman is recommended for using the ME1210 Redfish interface. Throughout the documentation, cURL will be used.
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 .
ltem_4	A community version of ipmitool is installed on a remote computer and on the local server to enable remote monitoring —it is recommended to use ipmitool version 1.8.18.

Platform, modules and accessories

Description Kontron Illustration P/N RJ45 to DB9 serial adapter 1015-9404 ... **HILLI** 1061-0410 C13 to CEE 7/7 European AC power cord, 10A/250 VAC, 1.8 m long C13 to NEMA 5-15P AC power cord, 10A/125 VAC, 2 m 1-340000-0 long Ground lug right angle, 8 AWG 1064-4226 Thermal probe for PCIe add-in card 1065-9296 Connector NTC thermistor

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

Hardware compatibility list

Table of contents

- <u>M.2 industrial SSD (-40°C to 85°C)</u>
- <u>Memory RDIMM ECC industrial modules (-40°C to 85°C)</u>
- <u>SFP and SFP+ industrial modules (-40°C to 85°C)</u>

M.2 industrial SSD (-40°C to 85°C)

Vendor	Vendor P/N	Туре	Size	Dimension	Status	Kontron P/N
Innodisk	DEM28-32GM41BW1DC-U48	SATA	32 GB	2280	Active	1065-5798
Transcend	TS32GMTS800I				Active	
Innodisk	DEM28-A28M41BW1DC-U48	SATA	128 GB	2280	Active	1065-7669
ATP	AF128GSMIC-VABIP				Active	
Transcend	TS128GMTS800I				Active	
Innodisk	DGM28-C12D81BWBQC-U48	SATA	512 GB	2280	Active	1065-7935
ATP	AF512GSMIC-VABIP				Active	
Transcend	TS512GMTS800I			Active		
ATP	AF1TSMIC-VABIP	SATA	1 TB	2280	Active	1065-8190
Transcend	TS1TMTS800I				Active	
Innodisk	DGM28-01TD81BWBQC-U48				Active	
Greenliant	GL588BP960G3-I-CD300	NVMe	960GB	2280	Active	1066-5026

Memory RDIMM ECC industrial modules (-40°C to 85°C)

Vendor	Vendor P/N	Туре	Size	Status	Kontron P/N
Micron Technology	MTA18ASF2G72PDBZ-3G2E1	DDR4-3200*	16GB	Active	1067-0181
Virtium Technology	VL38A8K67B-N8SC-S1	DDR4-2666	64GB	Active	1067-0159

*ME1210 supports DDR4 speeds of 2666 (one DIMM per channel) or 2400 (two DIMMs per channel).

SFP and SFP+ industrial modules (-40°C to 85°C)

Modules shall be tested:

- With the pass-through IO module running CentOS 7.8 on the server
- With the Ethernet switch IO module in ports configured to support the module speed grade

Vendor	Vendor P/N	Туре	Description	Status	Kontron P/N
II-VI (Finisar)	FTLF8519P3BTL	1000BASE-SX	500m, 850nm, -40°C to 85°C, SFP optical transceiver	Active	1064-5770
II-VI (Finisar)	FTLX8573D3BTL	10GBASE-SR	400m, 850nm, -40°C to 85°C, SFP+ optical transceiver	EOL	1064-5765
FormericaOE	TAS-A2NH1-P11	10GBASE-SR	300m, 850nm, -40°C to 85°C, SFP+ optical transceiver	Active	
FormericaOE	TSD-S2CA1-F11	1000BASE-LX	10Km, 1310nm, -40°C to 85°C, SFP optical transceiver	Active	1065-3758
II-VI (Finisar)	FTLF1318P3BTL	1000BASE-LX	10Km, 1310nm, -40°C to 85°C, SFP optical transceiver	Active	
Avago	AFCT-5715ALZ	1000BASE-LX	10Km, 1310nm, -40°C to 85°C, SFP optical transceiver	Active	
FS	SFP-10GLR-31-I	10GBASE-LR	10Km, 1310nm, -40°C to 85°C, SFP+ optical transceiver	Active	1065-6804
II-VI (Finisar)	FTLX1475D3BTL	10GBASE-LR	10Km, 1310nm, -40°C to 85°C, SFP+ optical transceiver	Active	
FS	SFP28-25GSR-85-I	25GBASE-SR	100m, 850nm, -40°C to 85°C, SFP28 optical transceiver	Active	1068-5031
II-VI (Finisar)	FTLF8536W4BTV	25GBASE-SR	100m, 850nm, -40°C to 85°C, SFP28 optical transceiver	Active	
FS	SFP28-25GLR-31-I	25GBASE-LR	10Km, 1310nm, -40°C to 85°C, SFP28 optical transceiver	Active	1068-5037
II-VI (Finisar)	FTLF1436W4BTV	25GBASE-LR	10Km, 1310nm, -40°C to 85°C, SFP28 optical transceiver	Active	

Validated operating systems

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 has started.

OS certification status

Note: Contact <u>Customer support</u> for additional operating system certification or validation.

Operating system	Status
CentOS 7.8	VALIDATED
RHEL 7.8	CERTIFIED Kontron ME1210 - Certified Server - Red Hat Ecosystem Catalog
Ubuntu 20.04	VALIDATED
VMWare ESXi 7.0	IN PROCESS

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>Configuring system access methods</u>.
- The platform supports Secure Boot. Refer to <u>Configuring UEFI/BIOS options</u>.
- The platform features a Trusted Platform Module (TPM). Determine your requirement with regards to hardware-based, security-related functions. Refer to Configuring the TPM in section <u>Configuring UEFI/BIOS options</u>.

For more information on security features, contact Kontron.

Getting started

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

Getting started - Application installation and performance benchmarking

Table of contents

- <u>Safety and regulatory information</u>
- Introduction
 - <u>Ethernet switch IO module option</u>
 - <u>Pass-through IO module option</u>
- <u>Unboxing the platform</u>
- What's in the box
- <u>Planning</u>
 - <u>Material and information required</u>
 - Software required
- Installing one or two PCIe add-in cards and thermal probes in an ME1210
 - <u>Opening the chassis</u>
 - Installing one or two thermal probes for the PCIe add-in cards
 - <u>Connecting one or two PCIe add-in cards</u>
 - <u>Closing the chassis</u>
- <u>Racking the platform</u>
- <u>Connecting the network cables</u>
 - <u>Ethernet switch IO module option</u>
 - <u>Pass-through IO module option</u>
- Preparing and connecting the DC power supply cables
 - Procedure
- <u>Discovering the BMC IP address</u>
 - <u>Accessing the UEFI/BIOS using a serial console (physical connection)</u>
 - <u>Accessing the BMC network configuration menu</u>
- Discovering the switch NOS IP address
 - Discovering the switch NOS IP address through the switch NOS serial console CLI
- Preparing for operating system installation
- Installing an operating system using the KVM
 - <u>Prerequisites</u>
 - <u>Browser considerations</u>
 - <u>Connecting to the Web UI of the BMC</u>
 - Launching the KVM
 - Mounting the operating system image via virtual media
 - <u>Accessing the UEFI/BIOS setup menu</u>
 - <u>Selecting the boot order from boot override</u>
 - <u>Completing operating system installation</u>
- Verifying operating system installation
- Benchmarking an application
- Monitoring platform sensors
 - Monitoring platform sensors using the Web UI

Safety and regulatory information

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

The ME1210 platform is available in two IO module options. Refer to the appropriate introduction section to read the associated use case:

- Ethernet switch IO module
- Pass-through IO module

Ethernet switch IO module option

This getting started section describes the network integration, platform access and operating system installation steps required to start operating an ME1210 platf orm equipped with one or two PCIe add-in cards provided by the customer and o ne 128GB M.2 SATA drive, and used to leverage two segregated network links (one for the management/control plane and one for the data plane). This use case is based on a simplified architecture with one management plane, one control plane and one data plane.

Assumptions

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

- The network connections of the system are as follows:
 - \circ One management plane (red line) and one control plane (green line) via the RJ45 management port 5 (Srv 5)
 - $\circ~$ One data plane (purple line) via SFP switch port 1 ($Sw\,1$)
 - $\circ~$ One serial connection via the RJ45 serial port of the platform
- The IPv4 scheme is DHCP for the management plane
- The preferred method to obtain or configure the BMC IP address is through the DHCP server
- The preferred method to obtain or configure the switch NOS IP address is through the DHCP server
- The preferred access method for the BMC and the operating system is through the Web UI
- PCIe add-in card temperature is monitored using a thermal probe installed in the platform

Network integration summary



Pass-through IO module option

This getting started section describes the network integration, platform access and operating system installation steps required to start operating an ME1210 platform equipped with one or two PCIe add-in cards provided by the customer and one 128GB M.2 SATA drive, and used to leverage two segregated network links (one for the management/control plane and one for the data plane). This use case is based on a simplified architecture with one management plane, one control plane and one data plane.

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) and one control plane (green line) via the RJ45 management port 5 (Srv 5)
 - One data plane (purple line) via SFP port 1 (Srv 1)
 - One serial connection via the RJ45 serial port of the platform
- The IPv4 scheme is DHCP for the management plane
- The preferred method to obtain or configure the BMC IP address is through the DHCP server
- The preferred access method for the BMC and the operating system is through the Web UI
- PCIe add-in card temperature is monitored using a thermal probe installed in the platform

Network integration summary



Unboxing the platform

What's in the box

The box includes one ME1210 multi-access edge computing 1U platform .



Step_1	Carefully remove the platform from its packaging.		
Step_2	Remove the plastic film from the platform. Failure to do so may affect platform airflow efficiency, thus resulting in poor cooling capabilities.		

NOTE: Additional material may be required to proceed with installation and configuration (refer to <u>Material and information required</u> for more information).

Planning

Material and information required

For a list of compatible components, refer to the <u>Hardware compatibility list</u>.

PCle add-in card

NOTE: One thermal probe is required per PCIe add-in card.

ltem_1	One T10 Torx screwdriver
ltem_2	(Optional) One thermal probe for temperature monitoring (if physical temperature monitoring is chosen)
Item_3	(Optional) Glue that can withstand the temperature generated by the PCIe add-in card and that has appropriate properties for the application (e.g. Loctite adhesive 444 and Loctite activator SF 7452)

Power cables and tooling

ltem_1	 Crimp lugs: Two or four Molex insulated spade crimp lugs for 14-16 wire gauge (19131-0023) OR Two or four Panduit insulated ring crimp lugs for 10-12 wire gauge (EV10-6RB-Q)
ltem_2	 Black stranded wire to build the power cable based on the length required: Proper wire gauge for application based on cable specification and local electrical code Maximum insulation diameter: 4.40 mm [0.175 in] for Molex crimp lugs OR Maximum insulation diameter: 5.8 mm [0.23 in] for Panduit crimp lugs
Item_3	 Red stranded wire to build the power cable based on the length required: Proper wire gauge for application based on cable specification and local electrical code Maximum insulation diameter : 4.40 mm [0.175 in] for Molex crimp lug OR Maximum insulation diameter : 5.8 mm [0.23 in] for Panduit crimp lug
ltem_4	One hand crimp tool: • Molex Premium Grade Hand Crimp Tool (640010100) OR • Panduit Hand Crimp Tool (638130400)
ltem_5	One 8 AWG ground cable based on the length required
ltem_6	One ground lug right angle, 8 AWG (Kontron P/N 1064-4226)
ltem_7	One hand crimp tool, Panduit CT-1700
ltem_8	7 mm wrench or equivalent tool

Rack installation material

Network ca bles and module s

ltem_1	One SFP optical module (SX, LX, SR, LR) with compatible optical cable
ltem_2	One RJ45 Ethernet management/control plane cable
Item_3	One RJ45 serial connection cable

Network infrastructure

- The following IP addresses may be required:
 - One management/control plane IP address for the BMC
 - Control plane and data plane IP addresses for the server
 - One data plane IP address for the switch NOS in the case of an ME1210 with the Ethernet switch IO module option

Software required

Relevant section:

Common software installation

ltem_1	An HTTP client such as cURL or Postman is recommended for using the ME1210 Redfish interface. Throughout the documentation, cURL will be used.
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 .
ltem_4	A community version of ipmitool is installed on a remote computer and on the local server to enable remote monitoring —it is recommended to use ipmitool version 1.8.18.

> You now have the material and software required. Proceed with the installation of the PCIe add-in card(s).

Installing one or two PCIe add-in cards and thermal probes in an ME1210



ESD sensitive device!

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



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

Opening the chassis

Step_1	Remove the 5 screws from the top using a T10 Torx screwdriver.	
Step_2	Remove the 16 screws from the sides (8 per side) using a T10 Torx screwdriver.	
Step_3	Remove the 7 screws from the back using a T10 Torx screwdriver .	
Step_4	Lift the cover up to remove it.	

Installing one or two thermal probes for the PCIe add-in cards

Locating the thermal probe connections

There are three thermal probe connectors on an ME1210.

Location	Reference designator	Connector
Back	J19	PCIe slot 1
Middle	JZO	PCIe slot 2
Front	J21	Chassis



I nstalling the thermal prob es



Step_1	Install the thermal probe in the connector as prescribed in the thermal probe specifications. Use the proper connector based on the PCIe add-in card location in the assembly.
Step_2	Affix the NTC thermistor to the PCIe card. Please ensure the thermistor is located as close as possible to the heat generating components to obtain a relevant temperature reading. Any non-thermally conductive elements should be avoided. Typically, thermistors are installed between the fins of the PCIe card heatsink. Do not forget to use glue that can withstand the temperature and that has appropriate properties for the application. Examples of glues that could be used include: Loctite adhesive 444 and Loctite activator SF 7452. NOTE: Configuration will be performed once the platform is operational (thresholds, specific software configurations, etc.).
Step_3	Repeat steps 1 and 2 if two thermal probes must be installed.

Refer to Configuring sensors and thermal parameters to configure thermal parameters.

Connecting one or two PCIe add-in cards

The maximum form factor of the optional PCIe add-in cards is full-height, three-quarter length (FH3/4L).

Step_1	Using a T10 Torx screwdriver, unfasten the two thumbscrews located in the front of the chassis a nd on the main board . Disconnect the intrusion detection switch wire near the front of the chassis. Lift the PCIe assembly out of the chassis.	
Step_2	Using a T10 Torx screwdriver, remove one PCIe blank L-bracket if you are installing one PCIe add-in card or remove the two PCIe blank L- brackets if you are installing two PCIe add-in cards. Using the T10 Torx screwdriver, remove the PCIe rear holder from the assembly. NOTE: If you are installing only one PCIe add-in card, it can be installed in slot 1 or slot 2. The system has no electrical preference. NOTE: PCIe slot 1 is the lower slot and PCIe slot 2 is the upper slot.	
Step_3	Install the PCIe add-in card(s) onto the PCIe riser(s). Using a T10 Torx screwdriver, f asten the blank L-bracket(s) to the PCIe holder (6 lbf·in torque). Mount the PCIe rear holder onto the assembly and tighten the M3 screws with a T10 Torx screwdriver (6 lbf·in torque). NOTE: If the PCIe add-in cards do not comply with PCIe Electromechanical Specifications for rear keepouts, discard the PCIe rear holder.	
Step_4	Carefully insert the PCIe assembly into the unit and fasten the two thumbscrews (6 lbf-in torque). Connect the intrusion detection switch wire near the front of the chassis.	

Closing the chassis



Racking the platform

Relevant section:

<u>Airflow</u>

Ensure there is no physical obstruction that would hinder proper airflow when choosing a location for the platform in the rack.

Step_1	Choose a location for the platform in the rack.	
Step_2	Insert the platform in the rack.	
Step_3	Fasten the platform to the rack using the appropriate fasteners.	
Step_4	If a ground lug is installed, remove the 2 nuts and washers from the ground lug studs. Take out the ground lug.	
Step_5	Strip 19 mm (0.75 in) of the 8 AWG ground cable.	
Step_6	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).	Contraction of the second seco
Step_7	Install the ground lug on the studs, fastening with the 2 nuts and washers. NOTE: The thread of the two chassis ground lugs is M4x0.7.	

> You are now ready to connect the network and power cables and start platform configuration.

Connecting the network cables

Ethernet switch IO module option

Connect the network cables according to the image below.

Step_1	Connect one RJ45 cable to port 5 for the management and the control planes ($ m Srv~5$).
Step_2	Connect one SFP or SFP+ cable to switch port 1 for the data plane ($Sw 1$).



Pass-through IO module option

Connect the network cables according to the image below.

Step_1	Connect one RJ45 cable to port 5 for the management and the control planes ($ m Srv~5$).
Step_2	Connect one SFP or SFP+ cable to port 1 for the data plane (Srv 1).



Preparing and connecting the DC power supply cables

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.
AWARNING	Installation of this product must be performed in accordance with national wiring codes and conform to local regulations.
	Pliers may be used to bend the crimp lugs.

Procedure

Step_1	Strip 6 mm [0.236 in] from the end of a black stranded 14 AWG wire (for Molex crimp lu of a black stranded 12 AWG wire (for Panduit crimp lug EV10-6RB-Q).	g 19131-0023) or 8 mm [0.315 in] from the end
Step_2	Strip 6 mm [0.236 in] from the end of a red stranded 14 AWG wire (for Molex crimp lug 7 a red stranded 12 AWG wire (for Panduit crimp lug EV10-6RB-Q).	19131-0023) or 8 mm [0.315 in] from the end of
Step_3	Insert each wire in a crimp lug. Follow the crimp lug manufacturer's procedure, using the Application tooling specification sheet of the tool.	ne appropriate hand crimp tool as specified in
Step_4	Bend the crimp lugs to a 45° angle as shown in the image.	
Step_5	Remove the screw from the terminal block RTN "B" location.	
Step_6	Insert the crimped red wire in the RTN "B" location as shown in the image.	
Step_7	Screw the crimp lug in place.	
Step_8	Remove the screw from the terminal block -48V DC "B" location.	CO De Gent Lug
Step_9	Insert the crimped black wire in the -48V DC "B" location as shown in the image.	Correct Bend Configuration
Step_10	Screw the crimp lug in place.	45%
Step_11	(Optional) If redundancy is required, repeat steps 1 to 10 for a second set of cables. They are to be installed in the -48V DC and RTN "A" locations.	Bend starts here
Step_12	Put the plastic terminal cover back in place once all the cables are screwed in place. NOTE: The power supply is reverse polarity protected. The unit will power on as soon as external power is applied (green power LED).	Plastic Terminal Cover
		Correct Installation

> You are now ready to discover IP addresses.

Discovering the BMC IP address

The BMC IP address is the minimum required to access the Web UI and the monitoring interface. The BMC IP address can be discovered using various methods. The UEFI/BIOS method will be used in this getting started section.

Relevant section: Discovering platform IP addresses

Accessing the UEFI/BIOS using a s erial console (physical connection)

Prerequisites

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

Sending a BREAK signal over a serial connection

Port location



Accessing the UEFI/BIOS setup menu

Step_1	From a computer with a physical connection to the serial port, open a serial console and the port to which the device is connected.	console tool and start the communication between the
Step_2	 Perform a server reset using one of the following options: If the server is currently running an installed operating system, log in and issue the appropriate reboot command. If the server is currently running the integrated UEFI shell, issue the "reset" command. Send a "BREAK" signal over the serial connection using the method provided in the terminal emulator. Disconnect all the input power connections for 30 seconds and reconnect them. NOTE: If an operating system is installed on the device, a method based on a 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 UEFI/BIOS sign on screen to display. 	<pre>WEI210 System starting System information WEI210 System BIOS version: 0.08.0146552F Date: "07/20/2020" Intal RC Version: 06051, CPU Info: Intal(R) Xeon(R) D-2187NT CPU 0 2.00GHz processors: 1, CORS: 16, Stepping: M0 WeDPY Info: Memory Size: 16G, Memory Speed: 2666WHz, RAS Mode: Indep 0.056 ; FCI H Initialization. 0x70 : SE DXE Initialization.</pre>
Step_3	When the UEFI/BIOS sign on screen is displayed, press the specified key to enter the UEFI/BIOS setup menu. NOTE : It may take a few seconds for the UEFI/BIOS sign on screen to display confirmation message "Entering Setup".	Version 2.20,1271. Copyright (C) 2020 American Megatrends, Inc. BIOS Date: 07/20/2020 16:46:55 Version 0.08.0146552F MEL220/RS1210 Firmware Version 0.08.0146552F Press or <f2> to enter setup. Press <f7> for boot menu.</f7></f2>
Step_4	The UEFI/BIOS sign on screen displays "Entering Setup". NOTE: It will take several seconds to display and enter the UEFI/BIOS setup menu.	Version 2.20.1271. Copyright (C) 2020 American Megatrends, Inc. BIOS Date: 07/20/2020 16:46:53 Version 0.08 0246552P Press Media Unremune Version 0.08 0246552P Press Media Unremune Version 0.08 024652P Press Media Unremune Version 0.08 024652P Press Media Unremune Version 0.08 024552P Press Media Unremune Version 0.09 024552P Press Media Unremune Version 0.08 0245
Step_5	The UEFI/BIOS setup menu is displayed.	Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc. Main Advanced Platform Configuration Socket Configuration Server Mgmt > BIOS Information BIOS Vendor Compliancy Orge Version Suid Date and Time Processor Platform Information McCess Level Memory Information McR Revision Sock PCA (S/RQ - 82-0) Protessor Sock PCA (S/RQ - 82-0) Memory Information Total Memory Memory Information Yet Sock PCA (S/RQ - 82-0) Version Version Version Version Version Memory Information Yet Sock PCA (S/RQ - 82-0) Version

Accessing the BMC network configuration menu

NOTE: In an ME1210 platform, LAN channel 1 corresponds to port Srv 5, the RJ45 connector.

Step 1	From the LIFEL/BLOS menu, pavigate to tab Server Mgmt	Aptio Setup Utility	7 - Copyright (C) 2019 Am	erican Megatrends, Inc.
Step_1		BIOS Information BIOS Vendor Core Version Compliancy Project Version Build Date and Time Access Level	American Megatrends 5.14 UEFI 2.6; PI 1.4 06/26/2019 09:12:28 Administrator	Choose the system Choose the system default language
		FPGA Version Hemoty Information Total Hemoty System Language System Date System Time Version 2.20.1371	2.02.0900AD12 32768 MB [English] [Ved 07/10/2019] [13:47:54]	<pre>><: Select Screen 'v: Select Icem Enter: Select 4/:-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save 4 Exit [ESC: Exit Can Regatrends, Inc. AB</pre>
Step_2	Select BMC network configuration .	Aptio Setup Otilits Main Advanced Intel DRC Interface(s) Wait For BRC FRB-2 Timer Dimer FRB-2 Timer Policy OS Watchdog Timer OS Watchdog Timer OS Watchdog Timer OS Watchdog Timer OS Watchdog Timer S Watchdog Timer OS Watchdog Timer OS Watchdog Timer OS Watchdog Timer OS Watchdog Timer S Watchdog Timer View Setting DRC Ware Setting DRC Ware Setting	<pre>Copyright (C) 2019 Am CCetup Server Numt Sec NCS, USB [Disabled] [Enabled] [Fower Cycle] [Disabled] [10 minutes] [Reset] [Neset] (Disabled] (Disabled) (Disabled)</pre>	Arican Megatrends, Inc. Mrity Root Event Leges A Press CEnter> to enable +lor disable Serial Mux +lordinable Serial Mux +lordinable Serial Mux +lordinable Serial Mux +lordinable Serial +lordinable Series +lordinable S
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 Utilit BRC metwork configure BRC metwork configure Configure IP04 support 	<pre>y - Copyright (C) 2019 Am Server Ngmt Ation [Unspecified] DynamicAddressBmcDhep 172.16.205.245 255.255.0.0 00-AD-X5-D6-33-2Å 172.16.0.1 00-05-64-2F-10-SF . Copyright (C) 2019 Amer</pre>	<pre>rican Megatrends, Inc. '[Select to configure LN '[chancel parameters !statically or !chancel parameters !statically (by BIOS or !BMO). Unapecified !option will not moduly !any BNC network !parameters during BIOS ! !otics Select Screen !hore: Select Screen !hore: Select Tem !hore: Select Tem</pre>

Discovering the switch NOS IP address

The switch NOS IP address is the minimum required to access the switch NOS Web UI and the monitoring interface.

Discovering the switch NOS IP address through the switch NOS serial console CLI

Prerequisites

	1	The BMC IP address is known.
	2	An SSH client tool is installed on the remote computer. NOTE: PuTTY is recommended for Windows environments and SSH is recommended for Linux environments.
	3	The remote computer has access to the management network subnet.
Relevant sections:		

Default user names and passwords Accessing the switch NOS

Procedure

NOTE: When using Serial over SSH, to quit the session press ${\it Enter}$ followed by ~ .

Step_1	 Using an SSH client tool, open an SSH session with the following parameters: BMC IP address Port number: 2201 (the BMC will automatically redirect communication to the switch NOS serial console) 	login as: admin admin@172.16.220.94's password:
Step_2	Log in the BMC using the appropriate credentials. Upon successful login, press Enter to get a response from the switch NOS CLI.	IStax - Kontron 1.02.014833d3 2021-09-18T11:19:13-4:00 Press ENTER to get started #
Step_3	Use the following command to discover the switch NOS IP address. LocalSwitchNOS_OSPrompt:~# show ip interface brief	<pre># show ip interface brief Interface Address Method Status VLAN 1 172.16.220.68/16 DHCP UP</pre>

> With the IP addresses, you are now ready to start the OS installation.

Preparing for operating system installation

Step_1	Choose the operating system needed based on the requirements of your application. It is recommended to choose one from the list of validated operating systems.
Step_2	Confirm the OS version to be installed includes or has divers supporting the platform components listed in the PCI mapping.
Step_3	If applicable, download the ISO file of the OS to be installed.

Installing an operating system using the KVM

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

Prerequisites

1	The BMC IP address is known.
2	The remote computer has access to the management network subnet.

Browser considerations

HTML5	To connect to the Web UI, a Web browser supporting HTML5 is required.
HTTPS self- signed certificate	Upon connection to the Web UI, it is mandatory to accept the HTTPS self-signed certificate. For further information about accepting HTTPS self-signed certificates, please refer to your Web browser's documentation.
File download permission	File download from the site needs to be permitted. For further information about file download permission, please refer to your Web browser's documentation.
Cookies	Cookies must be enabled in order to access the website. For further information about enabling cookies, please refer to your Web browser's documentation.

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

Connecting to the Web UI of the BMC

Step_1	 From a remote computer that has access to the management network, open a browser window and enter the IP address discovered for the BMC. NOTE: The HTTPS prefix is mandatory. https://[BMC MNGMT_IP] 				
Step_2	Click on Advanced in order to s tart the HTTPS self-signed certificate acceptance process . Information on the error message will be displayed.	Your connection is not secure. The more of 12: 13: 13: 13: 13: 13: 13: 13: 13: 13: 13			
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.	Verify Particular discrete d			
Step_4	Log in to the BMC Web UI using the appropriate credentials.	Utername			
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	Overvice Overvice Legs Connect Connect Legs Connect Connect Legs Connect Connect Legs Connect Connect Legs Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Connect Conneconnect Connect Connecon Connect Connect Conneconnect Connect Conn			

i

It is recommended to change the administrator password immediately after accessing the Web UI.

Launching the KVM

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

Step_1	From the left-side menu of the BMC Web UI, click on Operations and then on KVM .	Image: Server III Image: Server IIII Image: Server IIII Image: Server IIIII Image: Server IIIII Image: Server IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
Step_2	A new browser window opens and displays the virtual server screen.	Send Open in new tab

Mounting the operating system image via virtual media

Step_1	From the Operations menu, select	🔇 kontron	🤗 Healt	th 🥝 Power 🖸	Refresh 🛞 admin 🗝
	Virtual media .	E Overview	Overview		
		Event logs POST code logs	BMC time 2021-11-23 17:24:00 UTC	Server LED	
		Hardware status	Edit network settings \rightarrow	SOL console	→
		Sensors	BMC information	Server infor	mation
		KVM	Firmware version 2.00.0159fce6	Model ME1210	Manufacturer Kontron
		Firmware Reboot RMC		Serial number 9017064072	UEFI version 1.02.09579455
		SOL console	Network information		
		Server power operations Virtual media	eth0 Hostname MAC address BMC00A0A5E10E20 00:a0:a5:e1:0e:20	Power consu	Power cap
		 Settings ~ Security and access ~ 	IP address 172.16.182.31	Not available	Disabled
		🖬 Resource management 🗸			
Step_2	Click on Add file to browse for the ISO				
	file.	Virtual med	lia		
		Load image from	web browser		
		Virtual media device	web browser		
		Start			
Step_3	Click on Start to access virtual media from the OS.	Virtual med	lia		
		Load image from	web browser		
		Virtual media device			
		OS.iso	×		
		Start			

Accessing the UEFI/BIOS setup menu

Step_1	From the BMC Web UI, click on the Power button.	🚱 kontron	Ø Health Ø Power C Refresh Ø admin -
ו_נשיב		Overview Logs √ Hardware status Hardware status Sensors Operations Settings Security and access	BMC time Server LED 2021-11-20 163553 UTC ● Off Edit network settings ● Off Edit network settings ● Off Server information Product information Model Manufacturer Meddel Kontron Manufacturing Data Serial number 2011-04-06 - \$9017064072 1733000 Anste How provide
			Part number UER version 1067-2338 1.02.09579455
Step_2	From the Reboot server section, select Orderly and then click on Reboot .	Operations Reboot server Orderly – operati Immediate – Sen shutting down; n Reboot	ing system shuts down, then server reboots ver reboots without operating system nay cause data corruption
Step_3	From the Operations menu, click on KVM.	Skontron	🥺 Health 🥥 Power 🗘 Refresh 🛞 admin 🕶
Stop (Overview Logs Verview Logs Verview Logs Verview Logs Verview Verview Verview Reboot BMC SOL console Server power operations Virtual media Settings Virtual media	Boot settings biosSetup bioSetup biosSetup bi
Step_4	When the UEFI/BIOS sign on screen is displayed, press the specified key to enter the UEFI/BIOS setup menu. NOTE: When a reset server command is launched, it may take a few seconds for the UEFI/BIOS sign on screen to display. NOTE: It may take a few seconds for the UEFI/BIOS sign on screen to display the confirmation message "Entering Setup".	Statu: Connected	<page-header><text><section-header><section-header></section-header></section-header></text></page-header>
Step_5	The UEFI/BIOS sign on screen displays "Entering Setup". NOTE: It may take several seconds to display and enter the UEFI/BIOS setup menu.	Statu: Connected	

Step_6 The UEFI/BIOS setup menu will be displayed.	<image/> <image/> <text><text><text></text></text></text>

Selecting the boot order from boot override

Step_1 From the UEFI/BIOS setup menu and using the keyboard arrows, select the Save & Exit menu. In the Boot Override section, select UEFI: Linux File-Stor Gadgetxxxx and press Enter . The server will reboot and the media installation process will start.		KV N Status: Ø	Connected Aptio Setup Utility - Copyright ≰Jecurity Boot [Save BiEQ1]	↓ Send Ctrl+Alt+Delet (C) 2021 American Hegat	e DzOpen in new tab rends, Inc.
			Bact Superial Description (Constitution) UEF1 DS (SOC PC DSCS SOPPLIA-SECS) UEF1 DS (SOC PC DSCS SOPPLIA-SECS) UEF1 PS ETV Inte(N) INTERNOT ECON XC2 for 1006E GPF- UEF1 PS ETV Inte(N) Ethernet Econ XC2 for 1006E GPF- UEF1 PSE INA Inte(N) Ethernet Econ XC2 for 1006E GPF- UEF1 INE INA INTE(N) (Social Second UEF1 INE INA INTE(N) Social UEF1 UEF1 INTE(N) Social VEF1 INTE(N) Social VEF1 UEF1 INTE(N) Social VEF1 IN	Nettors metion metion metion n 1 (7,5 ptr 7,5	st Screen et Tree Let Mark Sch mige Dolo Tiod Values miged Defailts a Four t T

> 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.

Verifying operating system installation

Refer to the Introduction section to review the architecture used in this getting started section. **Relevant section:**

Common software installation

All the results and commands may vary depending on the operating system and the devices added.

	Step_1	Reboot the OS as recommended, then access the	OS command prompt.	
	Step_2	Install ethtool , ipmitool and pciutils using the precommended is 1.8.18.	package manager, and update the operating system packages. The ipmitool vers	sion
		Example for CentOS:		
		LocalServer_OSPrompt:~# yum update		
		LocalServer_OSPrompt:~# yum install pciutils		
		LocalServer_OSPrompt:~# yum install ethtool		
ſ	ersion 7 () (lune 2022)	www.kontron.com	// 6

	LocalServer_OSPrompt:~# yum install ipmitool				
	NOTE: Updating the packages may take a few minutes.				
Step_3	.3 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_4	Verify that the DIMMs are detected. LocalServer_OSPrompt:~# free -h	[-]# free -h Mem: 15G 211M 14G shared buff/cache available Swap: 08 08 08 17M 191M 14G			
Step_5	Verify that all the storage devices are detected. LocalServer_OSPrompt:~# lsblk	[-]# Tsblk NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT sda 8:0 0.29.8G 0.disk -sda1 8:1 0 512M 0 part -sda2 8:2 0.29.3G 0 part sdb 8:16 0.29.8G 0 disk			
Step_6	Confirm the control plane network interface controller is loaded by the igb driver. LocalServer_OSPrompt:~# lspci -s 04:00 -v NOTE: You should discover one 1GbE NIC.	[-]Hispol - S del00 - or coller: Insel Composition III S Gigabit Hetwork Connection (rev 03) 00:00.3 Emergence control Devide (140) Flags the manter, fract devel, latency 0, IGO 16, NUMA node 0 Hesory at all0000 (12-bit, non-prefetchable) [size=118] 1/0 ports at 1.000 [size=13] Hesory at all0000 [size=13] Capabilities (140) Ports Management (size=148] Capabilities (140) Ports Management (size=148) Capabilities (140) Ports Management (size=148) Capabilities (140) Ports Management (size=148) Capabilities (140) Parents Management (size=148) Parent Management (size=140) Parents Management (size=140) Parents Management (size=140)			
Step_7	Confirm the data plane network interface controllers are loaded by the i40e driver. LocalServer_OSPrompt:~# lspci -s b8:00 -v NOTE: You should discover up to four 10GbE NIC.	[*] Hadde -s. hifd) -s. [*] Hadde -s. hifd) - s. [*] Hadde -s. </td			
Step_8	Confirm that all the network interfaces are detected and get the list of device names. The following script requires Bash shell. Enter the following block of commands at the LocalServer_OSPrompt:~# ETH_NAMES=\$(grep PCI_SLOT_NAME /sys/class/net/*/device/uevent cut -d '/' -f 5) for ETH_NAME in \$ETH_NAMES; \ do echo -e "\$ETH_NAME: \$(ethtool -i \$ETH_NAME grep -E 'driver bus-info')\n"; \ done NOTE: You should discover one 1GbE NIC and up to four 10GbE NIC.	<pre>[-]#ETH NAMES=% (grep FCI_SLOT_NAME /sys/class/net/*/device/uevent cut -d '/' -f 5) [-]#for ETH_NAME in %ETH_NAMES; \ > > do echo -e "%ETH_NAME: % (ethtool -1 %ETH_NAME) grep -E 'driver bus-info')\n"; \ > > done eth1: driver: 140e bus-info: 0000:b8:00.0 eth3: driver: 140e bus-info: 0000:b8:00.1 eth4: driver: 140e bus-info: 0000:b8:00.2 eth5: driver: 140e bus-info: 0000:b8:00.3</pre>			
Step_9	Configure network interface controllers based on your requirements a NOTE: Interface names may change depending on the OS installed. He interface regardless of the operating system.	and network topology. owever, parameters Bus:Device.Function stay the same for the			
Step_10	(Optional) If one or two PCIe add-in cards are installed, verify that the cards are detected. LocalServer_OSPrompt:~# lspci	Colf 1993 [0015] Bote bridger Intel Corporation News IT wi/News IS wi/News D NEID (rev 0) [0015] For Linger Intel Corporation News IT wi/News IS wi/News D NEID (rev 0) [0015] For Linger Intel Corporation News IT wi/News IS wi/News D NEID (rev 0) [0015] For Linger Intel Corporation News IT wi/News IS wi/News D NEID (rev 0) [0015] For Linger Intel Corporation News IT wi/News D Wi/News D NEID (rev 0) [0015] For Linger Intel Corporation News IT wi/News D Wi/News D NEID (rev 0) [0015] For Linger Intel Corporation News IT wi/News D Wi/News D NEID (rev 0) [0015] For Linger Intel Corporation News IT wi/News D Wi/News D Wi/News D NEID (rev 0) [0016] For Particle Intel Corporation News IT wi/News D Wi/News D NEID (rev 0) [0016] For Particle Intel Corporation News IT wi/News D Wi/News D NEID (rev 0) [0016] For Particle Intel Corporation News IT wi/News D Wi/News D NeiD For Particle Intel (rev 0) [0016] For Particle Intel Corporation News IT wi/News D Wi/News D NeiD For Particle Intel (rev 0) [0016] For Particle Intel Corporation News IT wi/News D Wi/News D NeiD For Particle Intel (rev 0) [0016] For Particle Intel Corporation News IT wi/News D Wi/News D News D News IT wi/News D Wi/News D News D N			
Step_11	Verify communication between the operating system and the BMC. LocalServer_OSPrompt:~# ipmitool mc info	<pre>[-]# ipmitool mc info Device ZO : 0 Evice Revision : 0 Firmware Revision : 0.00 IPMI version : 2.0 Manufacturer ID : 15000 Product ID : 10027 (0x272b) Product Nable : Unknown (0x272b) Device Available : yes Provides Device SDRs : yes Additional Device SUpport : Sensor Device SEL Device FRU Inventory Device Chassis Chassis Device Chassis Chassis Chassis Chassis Chassis Chassis Chassis Chas</pre>			

Benchmarking an application

Install your application and proceed with benchmarking.

Monitoring platform sensors

Platform sensors can be monitored using various methods, including t he BMC Web UI.

The key sensors to look at are the following:

- Temperature sensors
- Power sensors

Relevant sections:

Accessing a BMC Monitoring sensors

Monitoring platform sensors using the Web UI

Step_1	Access the BMC Web UI.			
Step_2	From the left-side menu, click on Hardware status and then Sensors .	Sverview Otropy iour	🤗 Health 🛛 🤗 Power	🕄 Refresh 🛛 🕲 admin 🕶
		Constraints Const	Server LD ● Off → SOL console Server in Model Mitizio Seria number 9017064072 n **********************************	formation Manufacturer Konfora UEFiversion 1.02.09579455
Step_3	The sensor list will be displayed. Scroll down to see the list of sensors or use the dedicated search bar to filter the sensors.	Security and access MICONARSETIC20 DOBAGS MICONARSETIC20 DOBAGS MICONARSETIC20 DOBAGS MICONARSETIC20 MICONARS	e 1:0e:20 Power consumpt Not available	ion Power cap Disabled
		Logs Logs Aardware status Inventory and LEDs C. Search for sensors Constaines Constaines Constaines Constaines	57 items Lower Lower Curre critical warning value	The second secon
		KVM DC PSU Firmware DC PSU	V V 14.777 V	
		Network EMC Fred 8 • OK SOL console • DC PSU • OK Server power operations • DC PSU • OK	VV V VV 75.703 V	VV
		Virtual media V 12V	11.04 V 12.091 V V	
		Security and every		

Mechanical installation and precautions

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

ESD protections

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

What's in the box

 $\label{eq:main-constraint} \underline{ \mbox{The box includes one ME1210 multi-access edge computing 1U platform} \ .$



Step_1	Carefully remove the platform from its packaging.
Step_2	Remove the plastic film from the platform. Failure to do so may affect platform airflow efficiency, thus resulting in poor cooling capabilities.

Components installation and assembly

Table of contents

- Opening the enclosure
- <u>Connecting one or two PCIe add-in cards</u>
 - (Optional) Installing a thermal probe for the PCIe add-in card
 - Installing a PCIe add-in card
 - (Optional) Software installation instructions
- Installing an M.2 storage
 - Locating the M.2 storage
 - Installing the M.2 storage
- Installing DIMMs
 - Locating the DIMMs
 - <u>DIMM population guidelines for optimal performance</u>
 - Installing a DIMM
- <u>Replacing fans</u>
 - Locating the fans
 - Replacing a fan
- <u>Closing the enclosure</u>



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.



When handling components, follow the precautions described in section $\underline{\mathsf{ESD}\ protections}$.



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

Opening the enclosure

Step_1	Remove the 5 screws from the top using a T10 Torx screwdriver.	
Step_2	Remove the 16 screws from the sides (8 per side) using a T10 Torx screwdriver.	
Step_3	Remove the 7 screws from the back using a T10 Torx screwdriver .	
Step_4	Lift the cover up to remove it.	

Connecting one or two PCIe add-in cards

The maximum form factor of the optional PCIe add-in card is full-height, three-quarter length (FH3/4L).

(Optional) Installing a thermal probe for the PCIe add-in card

For the thermal probe part number, refer to <u>Platform, modules and accessories</u>.

(Optional) Locating the thermal probe connection

There are three thermal probe connectors on an ME1210.

Location	Reference designator	Connector
Back	J19	PCIe slot 1
Middle	JZO	PCIe slot 2
Front	J21	Chassis



(Optional) Building a thermal probe

Component	P/N	Description
NTC thermistor	GA10K3A1IA	NTC thermistor 10 Kohm, 3976K Bead
Connector	XHP-2	Connector housing 2.5 mm, 2 position
Pins	SXH-001-P0.6	Socket contact, 22-28 awg, crimp stamped
5tep_1 Using the components described in the table above, build a thermal probe.		

(Optional) Installing the thermal probe



Step_1	Install the thermal probe in the connector as prescribed in the thermal probe specifications. Use the proper connector based on the PCIe add-in card location in the assembly.
Step_2	Affix the NTC thermistor to the PCIe card. Please ensure the thermistor is located as close as possible to the heat generating components to obtain a relevant temperature reading. Any non-thermally conductive elements should be avoided. Typically, thermistors are installed between the fins of the PCIe card heatsink. Do not forget to use glue that can withstand the temperature and that has appropriate properties for the application. Examples of glues that could be used include: Loctite adhesive 444 and Loctite activator SF 7452. NOTE: Configuration will be performed once the platform is operational (thresholds, specific software configurations, etc.).
Step_3	Repeat steps 1 and 2 if two thermal probes must be installed.

Refer to <u>Configuring sensors and thermal parameters</u> to configure thermal parameters.

Installing a PCIe add-in card

Step_1	Using a T10 Torx screwdriver, unfasten the two thumbscrews located in the front of the chassis a nd on the main board . Disconnect the intrusion detection switch wire near the front of the chassis. Lift the PCIe assembly out of the chassis.	
Step_2	Using a T10 Torx screwdriver, remove one PCIe blank L-bracket if you are installing one PCIe add-in card or remove the two PCIe blank L- brackets if you are installing two PCIe add-in cards. Using the T10 Torx screwdriver, remove the PCIe rear holder from the assembly. NOTE: If you are installing only one PCIe add-in card, it can be installed in slot 1 or slot 2. The system has no electrical preference. NOTE: PCIe slot 1 is the lower slot and PCIe slot 2 is the upper slot.	
Step_3	Install the PCIe add-in card(s) onto the PCIe riser(s). Using a T10 Torx screwdriver, f asten the blank L-bracket(s) to the PCIe holder (6 lbf·in torque). Mount the PCIe rear holder onto the assembly and tighten the M3 screws with a T10 Torx screwdriver (6 lbf·in torque). NOTE: If the PCIe add-in cards do not comply with PCIe Electromechanical Specifications for rear keepouts, discard the PCIe rear holder.	
Step_4	Carefully insert the PCIe assembly into the unit and fasten the two thumbscrews (6 lbf-in torque). Connect the intrusion detection switch wire near the front of the chassis.	

(Optional) Software installation instructions

Refer to <u>Hardware compatibility list</u> for specific supported PCIe add-in card software installation instructions.

Installing an M.2 storage

Up to two M.2 storage drives can be installed in an ME1210. For the list of tested M.2 storages, refer to <u>Hardware compatibility list</u>.

Locating the M.2 storage



Installing the M.2 storage

Step_1	Remove the screw and washer from the bottom section with a T6 Torx screwdriver.	
Step_2	Insert the M.2 storage into the connector as prescribed in the M.2 specifications.	
Step_3	Put the screw and washer back in place and tighten (2 lbf·in torque) .	

Installing DIMMs

Up to eight DIMMs can be installed in an ME1210. For the list of tested DIMMs, refer to <u>Hardware compatibility list</u>.

Locating the DIMMs



DIMM population guidelines for optimal performance

There are 8 DIMM slots, but only 4 channels – B1 and B2 are on the same channel, A1 and A2 are on the same channel, D1 and D2 are on the same channel, and E1 and E2 are on the same channel.

Therefore, do not populate A2, B2, D2 and E2 unless you have already populated all other DIMM slots.

Populate DIMMs in accordance with the following guidelines to ensure optimal performance.

- For configurations with 1 to 4 DIMMs populate slots A1, B1, D1 and E1 starting with A1.
- For a configuration with 6 DIMMs populate slots A1, A2, B1, D1, D2 and E1.
- For a configuration with 8 DIMMs populate all DIMM slots.
- Configurations with 5 and 7 DIMMs are not recommended as they are unbalanced and will produce a less optimal performance.

Installing a DIMM

Step_1	Open the levers of the DIMM slot. (A)	
Step_2	Note the location of the alignment notch on the DIMM edge. (B)	The The second sec
Step_3	Insert the DIMM, making sure the connector edge of the DIMM aligns correctly with the slot. (E) $% \left(E\right) =0$	
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) $$	

Replacing fans

There are eight fans in an ME1210.

Locating the fans



Replacing a fan

Step_1	Disconnect the fan connector.
Step_2	Lift the fan up to take it out of the platform.
Step_3	Insert a new fan and connect the fan connector.

Closing the enclosure

Step_1	Place the cover onto the chassis.	
Step_2	Loosely fit all M3 flat head screws: • 5 on top • 8 per side (16 total) • 7 in the back Using a T10 Torx screwdriver, tighten all the screws (6 lbs-in torque).	

Airflow

The ME1210 platform features a front to back airflow system. To optimize heat transfer, refer to the <u>Specifications</u> section for the ideal clearances.



Rack installation

Installing an ME1210 platform in a 19-in rack

Ensure there is no physical obstruction that would hinder proper airflow when choosing a location for the platform in the rack.

Step_1	Choose a location for the platform in the rack.	
Step_2	Insert the platform in the rack.	
Step_3	Fasten the platform to the rack using the appropriate fasteners.	
Step_4	If a ground lug is installed, remove the 2 nuts and washers from the ground lug studs. Take out the ground lug.	
Step_5	Strip 19 mm (0.75 in) of the 8 AWG ground cable.	
Step_6	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).	C C C C C C C C C C C C C C C C C C C
Step_7	Install the ground lug on the studs, fastening with the 2 nuts and washers. NOTE : The thread of the two chassis ground lugs is M4x0.7.	

Cabling

Table of contents

- DC power supply inlet
- Preparing the DC power supply cables
 - <u>Material required</u>
 - Procedure
- <u>AC power supply inlet</u>
 - Power cord usage guidelines
 - AC power supply connection
- GNSS input
 - <u>Connecting to an RF splitter</u>
 - Connecting to an external antenna

DC power supply inlet

Description	Maximum input current	PSU receptacle model
600 W DC power supply module input connector	17 A	Amphenol (Anytek) YK6050423000G

Preparing the DC power supply cables

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



Pliers may be used to bend the crimp lugs.

Material required

Kontron suggests using crimp lugs (ring or spade crimp lug, straight, isolated, UL94V-0) on the power cables. Connect the appropriate cable to the appropriate polarity.

Use appropriate wire gauge for -48V DC and RTN based on cable specifications and local electrical code.

Description	Quantity	Manufacturer P/N	Link
Crimp lugs: • Molex insulated spade crimp lugs for 14-16 wire	2 (or 4 for redundancy)	19131-0023 or equivalent	<u>Molex product catalog</u><u>Part details</u>
 gauge Panduit insulated ring crimp lugs for 10-12 wire gauge 		EV10-6RB-Q or equivalent	 <u>Panduit product catalog</u> <u>Part drawing</u>
 Black stranded wire to build the power cable based on the length required: Maximum insulation diameter: 4.40 mm [0.175 in] for Molex crimp lugs Maximum insulation diameter : 5.8 mm [0.23 in] for Panduit crimp lugs 	Length required		
 Red stranded wire to build the power cable based on the length required: Maximum insulation diameter: 4.40 mm [0.175 in] for Molex crimp lugs Maximum insulation diameter : 5.8 mm [0.23 in] for Panduit crimp lugs 	Length required		
Hand crimp tool: Molex Premium Grade Hand Crimp Tool 	1	640010100 or equivalent	<u>Molex product catalog</u><u>Application tooling specification sheet</u>
Panduit Hand Crimp Tool		CT-460 or equivalent	<u>Panduit product catalog</u><u>Application tooling specification sheet</u>

Procedure

Step_1	Strip 6 mm [0.236 in] from the end of a black stranded 14 AWG wire (for Molex crimp lug of a black stranded 12 AWG wire (for Panduit crimp lug EV10-6RB-Q).	g 19131-0023) or 8 mm [0.315 in] from the end
Step_2	Strip 6 mm [0.236 in] from the end of a red stranded 14 AWG wire (for Molex crimp lug 1 a red stranded 12 AWG wire (for Panduit crimp lug EV10-6RB-Q).	19131-0023) or 8 mm [0.315 in] from the end of
Step_3	Insert each wire in a crimp lug. Follow the crimp lug manufacturer's procedure, using the the Application tooling specification sheet of the tool.	ne appropriate hand crimp tool as specified in
Step_4	Bend the crimp lugs to a 45° angle as shown in the image.	
Step_5	Remove the screw from the terminal block RTN "B" location.	
Step_6	Insert the crimped red wire in the RTN "B" location as shown in the image.	
Step_7	Screw the crimp lug in place.	
Step_8	Remove the screw from the terminal block -48V DC "B" location.	Bent Lug
Step_9	Insert the crimped black wire in the -48V DC "B" location as shown in the image.	Correct Bend Configuration
Step_10	Screw the crimp lug in place.	45%
Step_11	(Optional) If redundancy is required, repeat steps 1 to 10 for a second set of cables. They are to be installed in the -48V DC and RTN "A" locations.	Bend starts here
Step_12	Put the plastic terminal cover back in place once all the cables are screwed in place. NOTE: The power supply is reverse polarity protected. The unit will power on as soon as external power is applied (green power LED).	Plastic Terminal Cover
		Correct Installation

AC power supply inlet

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 <u>or equal to that of the electrical current rating marked on</u> the product.
 - The power cord must have a safety ground pin or contact that is suitable for the electrical outlet.
 - The power supply cord(s) are the main disconnect device to AC power. The socket outlet(s) must be near the equipment and readily accessible for disconnection.
 - The power supply cord(s) must be plugged into socket-outlet(s) that are provided with a suitable earth ground.

Power cord usage guidelines

The following guidelines may assist in determining the correct cord set. The power cord set used must meet local country electrical codes. For the U.S. and Canada, UL Listed and/or CSA Certified (UL is Underwriters' Laboratories, Inc., CSA is Canadian Standards Association). For outside of the U.S. and Canada, cords must be certified according to local country electrical codes, with three 0.75-mm conductors rated 250 VAC.

Wall outlet end connector:

- Cords must be terminated in a grounding-type male plug designed for use in your region.
- The connector must have certification marks showing certification by an agency acceptable in your region.

Platform end connectors are IEC 320 C13 type female connectors. Maximum cord length is 2 m.

AC power supply connection

Step_1 Connect an appropriately rated cable from an external power source to the power inlet in the front of the platform. Image: Step_2 The unit will power on as soon as external power is applied (green power LED).

For information on grounding, refer to <u>Rack installation</u>. For information on LED behavior, refer to <u>Platform components</u>.

GNSS input

Connecting to an RF splitter

Step_1	Connect a 50-ohm coaxial cable from the splitter to the ME1210. NOTE: The ME1210 requires the cable to be terminated with a female SMA connector. Cable type is not very critical if it is kept short between the splitter and the ME1210 and as long as a good antenna with low noise LNA is used.
Step_2	Follow the RF splitter documentation to connect the antenna.

Connecting to an external antenna



This is a general installation guideline and users are encouraged to read the GNSS antenna installation best practices of the antenna suppliers.



Step_1	Select a high quality antenna that includes a low noise amplifier with a 15 dB to 35 dB gain (depending on the distance from the antenna to the receiver).
Step_2	Install the antenna in a clear sky view area, ideally higher than any surrounding objects, buildings or trees. Use a sturdy support to minimize movement due to strong winds.
Step_3	Use a high quality, 50-ohm coaxial cable, such as LMR-400, to connect the antenna to the grounding bloc or surge protector. Type-N termination is a good choice for the antenna, cable and grounding bloc or surge protector.
Step_4	Install a grounding bloc and/or surge protector close to the coaxial cable entry in the building and connect to the building ground. Always refer to your local electrical code . The ME1210 includes surge protection for up to 1 kV.
Step_5	Use a high quality, 50-ohm coaxial cable, such as LMR-400, from the grounding bloc and surge protector to the ME1210. This cable needs an SMA connection on the ME1210 side.

Accessing platform components

- Accessing a BMC
- <u>Accessing the operating system of a server</u>
- Accessing the UEFI or BIOS
- Accessing the switch NOS

Accessing a BMC

Table of contents

- Accessing a BMC using the Web UI
 - <u>Prerequisites</u>
 - <u>Browser considerations</u>
 - <u>Access procedure</u>
- <u>Accessing a BMC using Redfish</u>
 - <u>Accessing a BMC using Redfish via an external network connection</u>
 - <u>Prerequisites</u>
 - <u>Creating the Redfish ROOT_URL</u>
 - <u>Access procedure</u>
 - <u>Accessing a BMC via the internal Redfish Host Interface</u>
 - <u>Access procedure</u>
- <u>Accessing a BMC using IPMI over LAN (IOL)</u>
 - <u>Prerequisites</u>
 - <u>Access procedure</u>
- <u>Accessing a BMC using IPMI via KCS</u>
 - <u>Prerequisites</u>
 - <u>Access procedure</u>

A BMC can be accessed through various methods:

- Using the Web UL this is the recommended path for first time out-of-the-box system configuration
- Using <u>Redfish</u>
- Using IPMI over LAN (IOL)
- Using <u>IPMI via KCS</u>

Refer to <u>Description of system access methods</u> for more information on the various paths.

Accessing a BMC using the Web UI

Prerequisites

2	The remote computer has access to the management network subnet.
1	The BMC IP address is known.

Discovering platform IP addresses

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, for the BMC. NOTE: The HTTPS prefix is mandatory. https://[BMC MNGMT_IP]	open a browser window and enter the IP address discovered
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>
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.	Add Scurpt Angelong Add Scurpt Angelong Angelong Angelong
Step_4	Log in to the BMC Web UI using the appropriate credentials.	Skontron Usename SkT Group Pasword Built on Image: Comparison of the second of the
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	Endet Over Cantered Operation Image: Construction of the second of the sec

Accessing a BMC using Redfish

There are two methods to access the BMC:

- Via an <u>external network connection</u>
- Via the internal Redfish Host Interface

Accessing a BMC using Redfish via an external network connection

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.
Polovant sostions	

Relevant sections:

Discovering platform IP addresses

<u>Configuring and managing users (if a password needs to be changed)</u>

Creating the Redfish ROOT_URL

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

Step_1	Begin the URL with the https prefix.	https://
Step_2	Add the BMC user name and password separated by a colon.	https:// [BMC_USERNAME] : [BMC_PASSWORD]
Step_3	Add @ to the URL followed by the BMC IP address.	https:// [BMC_USERNAME] : [BMC_PASSWORD] @ [BMC MNGMT_IP] In the documentation, this URL will be replaced by [ROOT_URL] in all Redfish commands.
Step_4	Access the API using an HTTP client and verify that the URL is valid.	RemoteComputer_OSPrompt:~# curl -k -s [ROOT_URL] /redfish/v1/ jq

Access procedure

Step_1	Access Redfish. RemoteComputer_OSPrompt:~# curl -k -s request GETurl [ROOT_URL] /redfish/v1/ jq	<pre>\$ curl -k -srequest GETurl https://admin:ready3go@172.16.182.31/redfish/vl jq "@odat.id*: */redfish/vl*. "@odat.id*: */redfish/vl/AccountService* }. CartificatsGervice*: { "@odat.id*: */redfish/vl/CartificateGervice" "@odat.id*: */redfish/vl/Chassis* }. WentService*: { "@odat.id*: */redfish/vl/EventService" "@odat.i</pre>
--------	------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Accessing a BMC via the internal Redfish Host Interface

BMC Redfish resources can be accessed locally by the integrated server using the internal, private, Redfish Host Interface. In the ME1210, this is implemented using a USB-LAN interface. Most modern Linux operating systems should have built-in support for this USB-LAN device.

Access procedure

Step_1	Find the USB interface name detected in Linux. This can be done by listing the net name from the sysfs folder.
	LocalServer_OSPrompt:~#ls /sys/bus/usb/drivers/rndis_host/1-3.2:1.0/net
	Example in CentOS 7:
	\$1s /sys/bus/usb/drivers/rndis_host/1-3.2:1.0/net enp8s20f0u3u2 e
	In this example the interface name discovered is enp0s20f0u3u2 .
	Sis /sys/bus/usb/drivers/rndis_host/1-3.2\:1.0/net/ enx00248c46642c
	In this example the interface name discovered is enx00248c46642c .
Step_2	Configure the static IP address of the USB-LAN interface. LocalServer_OSPrompt:~# ip addr add 169.254.0.1/24 dev [INTERFACE_NAME]
	<pre>\$ip addr add 169.254.0.1/24 dev emp8520F0u3u2 Sip addr show 1: loc .ULPER.UP> with 65536 qdisc monomene state UNRNOWN group default qlem 1000 1: loc .ULPER.UP> with 65536 qdisc monomene state UNRNOWN group default qlem 1000 1: wild 1ft forever welld.Ift forever inet6 ::://23 scope host </pre>
Step_3 You can now access the BMC Redfish interface using the internal Redfish Host Interface IP address. The BMC IP address is always 169.254.0.17 . LocalServer_OSPrompt:~# curl -k https://[USER_NAME]:[PASSWORD]@169.254.0.17/redfish/v1/[URL]	
	<pre>PScurl -k https://admin.readu2gu04169.254.8.17/redf1sh/v1/ "Bodata.dtps:" "readf1sh/v1/Smtadatat8ErviceRoot", "Bodata.idf": "rredf1sh/v1/Smtadatat8ErviceRoot", "Bodata.idf": "rredf1sh/v1/Corutf1cat8Ervice" "Bodata.idf": "rredf1sh/v1/Corutf1cat8Ervice" "Bodata.idf": "rredf1sh/v1/Corutf1cat8Ervice" "Bodata.idf": "rredf1sh/v1/Corutf1cat8Ervice" "Bodata.idf": "rredf1sh/v1/Corutf1cat8Ervice" "Bodata.idf": "rredf1sh/v1/Corutf1cat8Ervice" "Bodata.idf": "rredf1sh/v1/Corutf1cat8Ervice" "Bodata.idf": "rredf1sh/v1/SessionService/Sessions" "Inter": "MootService": ("Bodata.idf": "rredf1sh/v1/SessionService/Sessions" "Jobata.idf": "rredf1sh/v1/SessionService/Sessions" "Bodata.idf": "rredf1sh/v1/SessionService/Sessions" "Bodata.idf": "rredf1sh/v1/SessionService/Sessions" "Bodata.idf": "rredf1sh/v1/SessionService/Sessions" "Bodata.idf": "rredf1sh/v1/SessionService" "Bodata.idf": "r</pre>

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	evant section:
Disc	covering platform IP addresses

Access procedure

Step_1	From a remote computer that has access to the management network subnet, enter the desired command. RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -C 17 [IPMI command]	\$ ipmitcol -I Fan 1 Fan 2 Fan 3 Fan 4 Fan 5 Fan 6 Fan 6 Fan 7 Fan 8	lanplus -H 172.1 10282,000 10388,000 10706,000 10918,000 10600,000 10388,000 10600,000 10600,000	5.182.31 -U RPM RPM RPM RPM RPM RPM RPM RPM RPM	admin -P ok ok ok ok ok ok ok ok ok ok	ready2go - na na na na na na na na na	C 17 sensor na na na na na na na na na	list na na na na na na
--------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------	----------------------------------------------------------------------	------------------------------------------------------------------	-------------------------------------------------------------------	------------------------------------------

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.

Access procedure

Step_1	From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, enter the desired command.	\$ ipmitool senso Fan 1 Fan 2 Fan 3 Fan 4 Fan 5	pr 7252,000 7252,000 7742,000 7448,000 7448,000	RPM RPM RPM RPM RPM	ok ok ok ok	na na na na na	1666,000 1666,000 1666,000 1666,000 1666,000
	LocalServer_OSPrompt:~# ipmitool [IPMI command]	Fan 6 Fan 7 Fan 8 DIMM El CPU1 Die CPU1 Temp BMC Temp CPU Area Temp Chassis	7644,000 7742,000 7938,000 28,000 40,000 27,000 39,000 0,000	RPM RPM degrees C degrees C degrees C degrees C degrees C	ok ok ok ok ok ok ok	na na na na na na na	1666,000 1666,000 1666,000 0,000 na 0,000 0,000 0,000
		Temp FPGA	24,000	degrees C	ok	na	1,000

Accessing the operating system of a server

Table of contents

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

An operating system can be accessed through various methods:

- Using the <u>KVM</u> this is the recommended path for first time out-of-the-box system configuration
- Using the Web UI Serial over LAN console
- Using <u>Serial over LAN using SSH</u>
- Using IPMI Serial over LAN
- Using <u>SSH/RDP/Customer application protocols</u>
- Using a serial console (physical connection)
- Refer to Description of system access methods for more information on the various paths.

NOTE: This platform does not include a physical display port.

Accessing an OS using the KVM

NOTE: The KVM is not well suited for OS bootloader monitoring or configuration because of KVM boot time refresh issue. The KVM can still be used for operating system configuration. B ut, after the UEFI/BIOS execution, the KVM window will be resized, making bootloader output unavailable. Performing a full Web browser page refresh (use the browser refresh button or F5, which works in most browsers) may permit OS bootloader monitoring. An alternative method involves configuring the bootloader to output on the serial port. Refer to the documentation of the operating system to configure the output of the bootloader.

Prerequisites

1	An OS is installed.		
2	The BMC IP address is known.		
З	The remote computer has access to the management network subnet.		
Releva	Relevant sections:		

Accessing a BMC Discovering platform IP addresses Platform power management

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, for the BMC. NOTE: The HTTPS prefix is mandatory. https://[BMC MNGMT_IP]	open a browser window and enter the IP address discovered
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 connection is not secure. The non-connection is not secure. The non-connection is not subset. The non-connection is not built we bails. The non-connection is not built be not an investigate and built be not connected to this website. The non-connection is not built be not be not built be not buil
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.	Ald Security Exception Image: Security Exception Image: Security Exception
Step_4	Log in to the BMC Web UI using the appropriate credentials.	S&T Group Deername Built on Passnord OpenBMC tog in
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	Construer Overview Overview <t< td=""></t<>

Launching the KVM

NOTE: The KVM sometimes loses connection. Simply refresh the Web browser page to establish the connection.



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

Accessing an OS using the Web UI Serial over LAN console

Prerequisites

-	1	An OS is installed.
-	2	The BMC IP address is known.
-	3	The remote computer has access to the management network subnet.
l	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.
R	elev	ant sections:
<u>A</u>	cces	sing a BMC
D		

Discovering platform IP addresses Platform power management

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, for the BMC. NOTE: The HTTPS prefix is mandatory. https://[BMC MNGMT_IP]	open a browser window and enter the IP address discovered
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>
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.	Add Scurpt Angelong Add Scurpt Angelong Angelong Angelong
Step_4	Log in to the BMC Web UI using the appropriate credentials.	Skontron Usename SkT Group Pasword Built on Image: Comparison of the second of the
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	Endet Over Cantered Operation Image: Construction of the second of the sec

Launching the Web UI SOL console

Step_1	From the BMC Web UI, click on the Operations menu and then on the SOL console button.	Executive Coverview Logs Hardware status Coperations KVM Firmware Rebott BMC Spir crussian Spir crussian	 ♥ Health Overview BMC time 2021-11-23 16:14:31 UTC Edit network settings → Server information 	Power € Refresh ® admin * Server LED ● Off SOL console → Product information
		Server power operations Virtual media Settings v Security and access v Resource management v	Model Manufacturer [PRODUCT_NAME] Kontron Manufacturing Data Serial number 2021-04-06 - 9017064072 1730:00 Part number UEFI version 1.02.09579455	Name Manufacturer [PRODUCT_NAME] Kontron Serial number Part number 9017064072 1067-2338 Asset Tag Venion
Step_2	The OS screen should be displayed. NOTE: If the screen is not displayed, make sure that the dropdown menu is set to Host Console .	Serial over LA SOL console redirects the server Status: Connected Cent05 Linux 7 (Core) Kernel 3.10.0-1127.e17.x86_64	AN (SOL) CONSO : serial port output to this window. Host Console on an x86_64	∙e €

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

Accessing an OS using Serial over SSH

Prerequisites

Г	Dediverties to the seriel part is configured in the OC
5	Redirection to the serial port is configured in the OS
5	Redirection to the serial nort is configured in the OS
-	
	NUTE: PUTTY is recommended for Windows environments and SSH is recommended for Linux environments.
4	AN SSH client tool is installed on the remote computer.
1	An CCI I client tool is installed on the remarks commuter
5	The remote computer has access to the management network subhet.
5	The remote computer has access to the management network subnet
2	The BMC IP address is known.
2	The RMC ID address is known
1	An OS is installed.

```
Discovering platform IP addresses
Common software installation
Accessing a BMC
```

Access procedure

NOTE: When using Serial over SSH, to quit the session press **Enter** followed by ~ . To obtain the list of default user names and passwords, refer to <u>Default user names and passwords</u>.

Step_1	 Using an SSH client tool, open an SSH session with the following parameter BMC IP address Server port number: 2200 	S:
Step_2	Log in the BMC using the appropriate credentials. Upon successful login, press Enter to get a response from the OS serial console.	CentOS Linux 7 (Core) Kernel 3.10.0-693.21.1.e17.x86_64 on an x86_64 localhost login:

Accessing an OS using IPMI Serial over LAN

Prerequisites

1	An OS is installed.
2	The BMC IP address is known.
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.
Rel	evant sections:

Discovering platform IP addresses Platform power management

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] -C 17 sol deactivate	\$ ipmitool -I lanplus -H 172.16.182.31 -U admin -P ready2go -C 17 sol deactivate
Step_2	Activate an SOL session. RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name]-P [IPMI password] -C 17 sol activate	\$ ipmitool -I lanplus -H 172.16.182.31 -U admin -P ready2go -C 17 sol activate [SOL Session operational. Use -? for help] [-]#
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 SSH, RDP or customer application protocols

Prerequisites

1	An OS is installed.	
2	The OS IP address is known.	
3	The remote computer has access to the OS subnet.	
Relevant section:		
<u>Platform power management</u>		

Access procedure

Step_1	Using the OS IP address, proceed with your preferred remote access method.

Accessing an OS using a serial 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.

Port location



Access procedure

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

Step_1	Physically connect a computer to the platform serial port.	
Step_2	Using a serial console tool, establish communication using the parameters provided. Press Enter .	
Step_3	The OS start screen will be displayed.	CentOS Linux 7 (Core) Kernel 3.10.0-593.21.1.e17.x86_64 on an x86_64 localhost login:

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

Accessing the UEFI or BIOS

Table of contents

- <u>Accessing the UEFI or BIOS using Serial Over LAN using the Web UI</u>
 - <u>Prerequisites</u>
 - Browser considerations
 - <u>Access procedure</u>
 - Accessing the BMC Web UI
 - <u>Accessing the UEFI/BIOS setup menu using SOL using the Web UI</u>
- <u>Accessing the UEFI or BIOS using the KVM</u>
 - <u>Prerequisites</u>
 - <u>Browser considerations</u>
 - <u>Access procedure</u>
 - Accessing the BMC Web UI
 - Accessing the UEFI/BIOS setup menu using the KVM
- <u>Accessing the UEFI or BIOS using Serial over SSH</u>
 - <u>Prerequisites</u>
 - <u>Access procedure</u>
- <u>Accessing the UEFI or BIOS using Serial over LAN using IPMI</u>
 - <u>Prerequisites</u>
 - <u>Access procedure</u>
- <u>Accessing the UEFI or BIOS using Redfish</u>
- Accessing the UEFI or BIOS using a serial console through a physical connection
 - Prerequisites
 - Port location
 - <u>Access procedure</u>
- UEFI/BIOS can be accessed through various methods :
 - Serial over LAN (SOL) using the Web UL this is the recommended path for first time out-of-the-box system configuration
 - <u>KVM</u>
 - Serial over SSH
 - Serial over LAN (SOL) using IPMI
 - <u>Redfish</u>
 - <u>Serial console (physical connection)</u>

Refer to **Description of system access methods** for more information on the various paths.

Accessing the UEFI or BIOS using Serial Over LAN using the Web UI

Prerequisites

7	The BMC IP address is known. The remote computer has access to the management network subnet
- Releva	ant section:

Discovering platform IP addresses

Browser considerations

HTML5	To connect to the Web UI, a Web browser supporting HTML5 is required.
HTTPS self- signed certificate	Upon connection to the Web UI, it is mandatory to accept the HTTPS self-signed certificate. For further information about accepting HTTPS self-signed certificates, please refer to your Web browser's documentation.
File download permission	File download from the site needs to be permitted. For further information about file download permission, please refer to your Web browser's documentation.
Cookies	Cookies must be enabled in order to access the website. For further information about enabling cookies, please refer to your Web browser's documentation.

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

Access procedure

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

Accessing the BMC Web UI

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. <i>https://[BMC MNGMT_IP]</i>		
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.	Your connection is not secure Advanced Department Report errors like this to help Mozilla identify and block malicious sites Department Department	
		The certificate is not trusted because the issuer certificate is unknown. The server might note be sending the appropriate intermediate certificates. An additional root certificate rays need to be imported. The certificate is only valid for. Error code: site_EIRCR_UNING/OWN_ISSUER Add Exception	
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.	Vertice Vertice Vertice	
Step_4	Log in to the BMC Web UI using the appropriate credentials.	S&T Group Built on OpenBMC	
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	Event logs Over Control Street (D) POST code logs But time Street (D) Street (D) Resource management Model Antonne Street (D) Street (D) Resource management Workshow Model Antonne Name Mandature Resource management With under time Street (D) Street (D) Street (D) Phr number Model Antonne Model Antonne Model Antonne Model Antonne Immutaturing Date Set in maker Street (D) Street (D) Street (D) Phr number Model Antonne Model Antonne Model Antonne Model Antonne Product Information Model Antonne Street Antonne Model Antonne Model Antonne Phr number Model Antonne Street Antonne Model Antonne Model Antonne Phr number UEP (PST) Street Antonne Model Antonne Model Antonne Phr number UEP (PST) Model Antonne Model Antonne Model Antonne Phr number UEP (PST) Model Antonne Model Antonne Model Antonne Phr number UEP (PST) Model	

Accessing the UEFI/BIOS setup menu using SOL using the Web UI

- - --

Step_1 From the BMC Web UI, click on the Operations menu and then on	😵 Kontron 🛛 😵 Health 🔮 Power 🕃 Refresh 🛞 admin -
the SOL console button.	Cverview Overview
	Hardware status > BMC time Server LED ☎ Operations ▲ 2021-11-23 16:14:31 UTC ● Off
	KVM Edit network settings → SOL console → Firmware →
	Reboot BMC SOL console
	Virtual media Manufacturing Date Serial number Serial number Part number 2021-04-06 - 9017064072 9017064072 9017064072 1067-2338 Settings 17:30:00 Asset Tag Version
	Security and access Part number UEF version 1067-2338 1.02.09579455

Step_2	Press an arrow on the keyboard to refresh the console. The OS screen should be displayed.	Serial over LAN (SOL) console		
	NOTE : If the screen is not displayed, make sure that the dropdown menu is set to Host Console .	SUL console redirects the server's senal port output to this window. Status: Connected Host Console		
		CentOS Linux 7 (Core) Kernel 3.10.0-1127.e17.x86_64 on an x86_64 localhost login:		
Step_3	If the system is already powered on, perform a server reset. Otherwise	e, power on the server.		
Step_4	When the UEFI/BIOS sign on screen is displayed, press the specified key to enter the UEFI/BIOS setup menu.	Serial over LAN (SOL) console SOL console redirects the server's serial port output to this window.		
	seconds for the UEFI/BIOS sign on screen to display. NOTE : It may take a few seconds for the UEFI/BIOS sign on screen to display the confirmation message "Entering Setup"	Status: Connected Host Console Acceleration (C) 2021 American Megatrends, Inc. BIOS Date: 08/30/2021 13:21:37 Version 1.02.09579455 ME1310 Firmmare Version 1.02.09579455 Press or <f2> to enter setup. Press <f7> for boot menu.</f7></f2>		
Step_5	The UEFI/BIOS sign on screen displays "Entering Setup". NOTE: It may take several seconds to display and enter the UEFI/BIOS	setup menu.		
Step_6	The UEFI/BIOS setup menu will be displayed.	Serial over LAN (SOL) console SOL console redirects the server's serial port output to this window. Status: Console	•	
		Aptio Setup Utility - Copyrapht (C) 2021 American Megatrends, Inc. Main Advanced Platform Configuration Socket Configuration Server Mgmt BIOS Information ^ Choose the system BIOS Vendor American Megatrends default language Core Version 5.14 * Compliancy UBFT 2.6; PT 1.4 * Project Version MEI310 1.02.09579455 * Access Level Administrator * Platform Information * * Processor 50654 - SIX M0 */v: Select Item PCH Soc CPCH QS/PRQ - B2-0 * * RC Revision 65536 M8 */r: Change Opt. * Memory Information * * * Total Memory 65536 M8 */F3: Optimized Defaults V/F4 Save & Exit Version 2.20.1271. Copyright (C) 2021 American Megatrends, Inc. * *		

Accessing the UEFI or BIOS using the KVM

NOTE: The KVM is not well suited for UEFI/BIOS configuration because of KVM refresh issues at UEFI/BIOS boot. The KVM can still be used for UEFI/BIOS configuration but, when the UEFI/BIOS is booting, the KVM window will be resized and rendered unusable until a full Web browser page refresh is performed (use the browser refresh button or F5, which works in most browsers). After the refresh, the KVM should remain stable and functional until the next UEFI/BIOS reboot.

Prerequisites

1	The BMC IP address is known.		
2	The remote computer has access to the management network subnet.		
Releva	Relevant section:		
Discov	viscovering platform IP addresses		

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>. **NOTE:** The KVM sometimes loses connection. Simply refresh the Web browser page to establish the connection.

Accessing the BMC Web UI

Step_1	From a remote computer that has access to the management network, or for the BMC. NOTE: The HTTPS prefix is mandatory. https://[BMC MNGMT_IP]	pen a browser window and enter the IP address discovered
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.	Your connection is not secure Means of 192.168.10.196 has configured their website improperly. To protect your information from being stoler, Firefox has not connected to this website. Learn more. Report errors like this to help Mozilla identity and block malicious sites Con Back Advanced
		192.108.10.196 uses an invalid security certificate. The certificate is not trusted because the issuer certificate is unknown. The server might not be sending the appropriate intermediate certificates. An additional root certificate may need to be imported. The certificate is only valid for . Error code: stc_ERROR_UNANCOVE_ISSUER Add Exception
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.	Algending and algending
Step_4	Log in to the BMC Web UI using the appropriate credentials.	Username S&T Group Built on OpenBMC

Step_5	You now have access to the management Web UI of the BMC. You can		🚱 kontron 👔			🥺 Health	🥝 Power 🛛 🔾 Ret	iresh 🛞 admin 🗝
	use the interface.	e U	🗟 Overview	^	Overvie	W		
			Event logs POST code logs		BMC time 2021-11-20 16:35:50	витс	Server LED	
		1	B Hardware status	~	Edit network setti	ngs →	SOL console	\rightarrow
		-	Coperations	×	Server inform	nation	Product info	rmation
		0	Security and access	~	Model [PRODUCT_NAME]	Manufacturer Kontron	Name [PRODUCT_NAME]	Manufacturer Kontron
		6	Resource management	~	Manufacturing Date 2021-04-06 -	Serial number 9017064072	Serial number 9017064072	Part number 1067-2338
					17:30:00		Asset Tag	Version
					Part number 1067-2338	UEFI version 1.02.09579455	Address	, same

Accessing the UEFI/BIOS setup menu using the KVM

Step_1	From the BMC Web UI, click on the Power button.	S kontron	⊗ Health 🔮 Power 🖏 Refresh 🛞 admin →
		⊡ Overview Image: Second S	Server LED Off SOL console Product information rer Name Manufacturer [RODUCT_NAME] Konton Serui Joundary 1067-238 9017064072 1067-238 0072 Asst Tag Version on
Step_2	From the Reboot server section, select Orderly and then click on Reboot .	Operations Reboot server Orderly – operating system shuts of Immediate – Server reboots withou shutting down; may cause data co Reboot	lown, then server reboots ut operating system rruption
Step_3	From the Operations menu, click on KVM .	Image: Second section s	Health Power Refresh admin -
Step_4	When the UEFI/BIOS sign on screen is displayed, press the specified key to enter the UEFI/BIOS setup menu. NOTE: When a reset server command is launched, it may take a few seconds for the UEFI/BIOS sign on screen to display. NOTE: It may take a few seconds for the UEFI/BIOS sign on screen to display the confirmation message "Entering Setup".	KVM strux:	rl+Alt+Delete COpen in new tab manual states and the states and t
Step_5	The UEFI/BIOS sign on screen displays "Entering Setup". NOTE: It may take several seconds to display and enter the	KVM	//1

Version 2.0 (June 2022)

www.kontron.com

	UEFI/BIOS setup menu.	Status: 🥝 Connected	↓ Send Ctrl	+Alt+Delete 📑 Open in new ta	ıb
		Virtual and a second and a seco	DINTEPO Listi (1) 2009 American Nego Heris version (0) disess ersion 0:00 Ottesser inter setue, Press (7), for	trends, Inc. 5 boot menu.	
Step_6	The UEFI/BIOS setup menu will be displayed.	KVM			
		Status: 📀 Connected			
		Connected	↓ Send Ctrl	+Alt+Delete 📑 Open in new ta	b
		Aptio Setup Utili Main Advanced Plat	↓ Send Ctrl 19 - Copyright (C) 2020 Amer Form Configuration Socket C	+Alt+Delete C Open in new ta	b
		Aptio Setup VIIII Noin Advanced Fist BIOS Information DOPE Version OPPE Version Project Version	↓ Send Ctri- vy - Copyright (C) 2020 Awer Gree Configuration Socket (C American Megatrends 5.14 UEFI 2.6: PT 1.4 MEIZIO/RSIZIO 0.00.014552F #64	+Alt+Delete ☐ Open in new ta Icon Hegartends, thc: out growt som deren Hent + A Choose the System default Innpusge	b
		Actio Setup Utili Noin Advanced Flat Bios Information Bios Version Other Version Project Version Build Date and Time Access Level Platform Information	4 Send Ctri- va - Copy Lpht (0) 2000 Alex var configuration - Social C Reer Lcan Regarrends 5:14 UET Los PT 14 Var Los PT 14 Or 2002020 15:46:55 Administrator	+Alt+Delete C Open in new ta Lican Megatrends, Trc. on Facura San Gerver Mart + defrault Language	b
		Antio Setup Utili Point Advanced Alla BDD Information BDD Information Depuise Projet Version Build bereind Time Access Level Platform Platform Point Com Longenuion	 Send Ctrl- vy - Copyright (C) 2020 Aver con Continguation Social G Sub- Restican Registerids 5:14 UET 20, 35 PT 1.4 HE1210, 01465057 364 0.06, 01	+Alt+Delete (*) Open in new ta Loan Medatrends, Inc. out/guration derver Met + Control to derver Met + Control to derver Met + Met Select Surgeon Met Select Sur	b
		Acto Setup UTII RAIN (Advanced State BDG Information BDG Information Core Version Core Version Core Version Build Once and Time Access Level Platform Processor Pros RC Revision Nearry Information Total Memory	Send Ctri Y - Copyright (0) 2020 Area Sold Contiguent (0) 2020 Area Sold Rear Loan Megatrends Sold UET 2 .65 PT 1.4 ME120 Sold Reininistrator ME1210 Sold Proc Mark Sold	+Alt+Delete C Open in new ta	b
		Actio Settin Utili Rain Assumets Plat 800 Information 800 Windon Come Version Come Jancy Project Version 8010 Dare and Take Access Level Platform Information Platform Revision RC Revision RC Revision RC Revision Neocry Information Total Memory	4. Send Ctri y - CopyLight (0) 2020 Amer Sum Configuration Booker (0 Send Configuration Booker (0 UEF 2.0.6 PF 3.4 HE1210/RE210 D00.0 + RE257 MA C7720/RE20 Lef48:55 HE1210 S00.64 - SR0 MD S00.64 - SR0	+Alt-Delete C Open in new ta	b
		Actio Setup Utili Rain Advances Plat BDS Information DDS Wradow ComeLarvy Project Version ComeLarvy Project Version Rocess Level Platform Information Processor Pol Rc Revision Memory Information Total Memory	4 Send Ctri (x - Copylight (0) 2000 Ameri Continue Regatendo Continue Regatendo Continue Regatendo Continue Regatendo Continue Regatendo Continue Regatendo Continue Regatendo Continue Regatendo Continue Regatendo Continue Regatendo Relizio Social - Sito No Social - Si	+Alt-Delete C Open in new ta	b

Accessing the UEFI or BIOS using Serial over SSH

Prerequisites

1	The BMC IP address is known.
2	The remote computer has access to the management network subnet.
З	An SSH client tool is installed on the remote computer. NOTE: PuTTY is recommended for Windows environments and SSH is recommended for Linux environments.
Rele	evant sections:

Discovering platform IP addresse Common software installation Accessing a BMC

Access procedure

NOTE: When using Serial over SSH, to quit the session press ${\it Enter}\,$ followed by ~ .

Step_1	Using an SSH client tool, open an SSH session with the following parameters • BMC IP address • Server port number: 2200	5:
Step_2	 Perform a server reboot using your preferred method. The following are examples: Log into the BMC Web UI and perform the reboot. If the server is currently running an installed operating system, log in and issue the appropriate reboot command. If the server is currently running the integrated UEFI shell, issue the "reset" command. NOTE: When a server reset command is sent, it may take a few seconds for the UEFI/BIOS sign on screen to display. 	<pre>[ME1210][172.16.220.79][-]# jpmi[0K] Started Show Plymouth Power Off Screen. [oK] Stopped Oynamic System Message Bus [oK] Stopped target Basic System, [oK] Stopped target Basic System, [oK] Stopped target Socket. [oK] Stopped target Paths. [oK] Stopped target Paths. [oK] Stopped target Socket. [oK] Closed ARCbind Server Activation Socket. [oK] Stopped target System Initialization. [oK] Stopped supped System Initialization.</pre>
Step_3	The UEFI/BIOS sign on screen should display "Entering Setup". P ress the specified key to enter the UEFI/BIOS setup menu. NOTE: It will take several seconds to display and enter the UEFI/BIOS setup menu.	Version 2.20.1271. Copyright (C) 2020 American Megatrends, Inc. BIOS Date: 08/05/2020 11:07:21 Version 0.16.0946D3C7 MEI210 Firmware Version 0.16.0946D3C7 Press or <f2> to enter setup. Press <f7> for boot menu.</f7></f2>
Step_4	The UEFI/BIOS setup menu should be displayed.	Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc. Main Advanced Platform Configuration Socket Configuration Server Mgmt > BIOS Information SIOS Vendor Compliancy UEFI 2.6; PI 1.4 Project Version Suid Date and Time Obstrom Platform Information Platform Information Pccessor Soc Pc4 CR Rvision OGD51 Wemory Information Total Memory S192 MB Version 2.20.1271. Copyright (C) 2020 American Megatrends, Inc. Access Level Administrator Pit form Information PC4 Soc Pc4 (D5/PRQ - B2-D) Reneral Help +F2: Optimized Defaults Version 2.20.1271. Copyright (C) 2020 American Megatrends, Inc.

Accessing the UEFI or BIOS using Serial over LAN using IPMI

Prerequisites

1	An OS is installed.
2	The BMC IP address is known.
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.
Rel	evant sections:

Discovering platform IP addresses 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] -C 17 sol deactivate	\$ ipmitool -I lanplus -H 172.16.182.31 -U admin -P ready2go -C 17 sol deactivate
Step_2	Activate an SOL session. RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -C 17 sol activate NOTE: It may be required to press the Enter key for the operating system's screen to be displayed.	<pre>\$ ipmitool -I lamplus -H 172.16.182.31 -U admin -P ready2go -C 17 sol activate [SOL Session operational. Use -? for help] CentOS Linux 7 (Corce) Kernel 2.10.0-693.21.1.e17.x86_64 on an x86_64 localhost login:</pre>
Step_3	From another command-line window. Make the platform enter the UEFI/BIOS automatically on the next reboot using the following command. RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -C 17 chassis bootdev bios	\$ ipmitool -I lanplus -H 172.16.182.31 -U admin -P ready2go -C 17 chassis bootdev bios Set Boot Device to bios
Step_4	From the same command-line window, perform a server reset. RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI p assword] -C 17 chassis power reset NOTE: When a reset server command is launched, it may take a few seconds for the UEFI/BIOS sign on screen to display.	<pre>[ME1210][172.16.220.79][-]# ipmi[0K] Started Show Plymouth Power Off Screen. [0K] Stopped Dynamic System Tuning Daemon.</pre>
Step_5	The UEFI/BIOS sign on screen should display "Entering Setup". NOTE : It will take several seconds to display and enter the UEFI/BIOS setup menu.	<pre>Version 2.20.1271. Copyright (C) 2020 American Megatrends, Inc. BIOS Date: 08/05/2020 11:07:21 Version 0.16.0946D3c7 MEL210 Firmware Version 0.16.0946D3c7 Press or <f2> to enter setup. Press <f7> for boot menu.</f7></f2></pre>
Step_6	The UEFI/BIOS setup menu should be displayed.	Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc. Main Advanced Platform Configuration Socket Configuration Server Mgmt > BIOS Information BIOS Vendor Compliancy UEF1 2.5; PI 1.4 Project Version NEL210 0.16.09460327 Kada and Time 08/05/2020 11:07:21 Access Level Administrator Platform Information ME1210 Processor SoC PCH QS/PRQ - B2-D RC Revision 06051 Memory Information + F1: General Help Memory Information + F3: Optimized Defaults Version 2.20.1271. Copyright (C) 2020 American Megatrends, Inc. AB

Accessing the UEFI or BIOS using Redfish

The UEFI/BIOS options can be configured using Redfish. R efer to <u>Configuring UEFI/BIOS options via the BMC using Redfish</u> to proceed.

Accessing the UEFI or BIOS using a serial console through a 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.
Releva	ant sections:
Comm	on software installation
<u>Sendin</u>	g a BREAK signal over a serial connection


Access procedure

Step_1	From a computer with a physical connection to the serial port, open a serial console and the port to which the device is connected.	console tool and start the communication between the
Step_2	 Perform a server reset using one of the following options: If the server is currently running an installed operating system, log in and issue the appropriate reboot command. If the server is currently running the integrated UEFI shell, issue the "reset" command. Send a "BREAK" signal over the serial connection using the method provided in the terminal emulator. Disconnect all the input power connections for 30 seconds and reconnect them. NOTE: If an operating system is installed on the device, a method based on a 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 UEFI/BIOS sign on screen to display. 	<pre>ME1210 System starting 0.11a presence is Initialization. 0.15 presence is Initialization.</pre>
Step_3	When the UEFI/BIOS sign on screen is displayed, press the specified key to enter the UEFI/BIOS setup menu. NOTE : It may take a few seconds for the UEFI/BIOS sign on screen to display confirmation message "Entering Setup".	Version 2.20.1271. Copyright (C) 2020 American Megatrends, Inc. BIOS Date: 07/20/2020 15:46:55 Version 0.08.0146552F MEI210/RSI210 Firmware Version 0.08.0146552F Press dELS or dF2> to enter setup. Press dF7> for boot menu.
Step_4	The UEFI/BIOS sign on screen displays "Entering Setup". NOTE: It will take several seconds to display and enter the UEFI/BIOS setup menu.	Version 2.20.1271. Copyright (C) 2020 American Megatrends, Inc. EIOS Date: 07/20/2020 15:46:55 Version 0.08.024552F FreeSA (EUS) or -former version 0.08.02457 FreeSA (EUS) or -former version
Step_5	The UEFI/BIOS setup menu is displayed.	Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc. Main Advanced Platform Configuration Socket Configuration Server Mgmt > BIOS Information SIDS Vendor Comp Version Sub Vendor Comp Version Sub Vendor Vendor Sub Vendor Sub Vendor

Accessing the switch NOS

Table of contents

- <u>Accessing the switch NOS using the Web UI</u>
 - <u>Prerequisites</u>
 - Browser considerations
 - Access procedure
- <u>Accessing the switch NOS CLI using BMC Web UI Serial over LAN console</u>
 - <u>Prerequisites</u>
 - <u>Browser considerations</u>
 - <u>Access procedure</u>
 - <u>Accessing the BMC of the server for which you want to access the NOS</u>
 - Launching the Web UI SOL console
- <u>Accessing the switch NOS CLI using Serial over SSH from a remote computer</u>
 - <u>Prerequisites</u>
 - <u>Access procedure</u>
- Accessing the switch NOS CLI using SSH from a remote computer
 - Prerequisites
 - <u>Access procedure</u>
- <u>Accessing the switch NOS CLI using SSH from the integrated server</u>
 - <u>Prerequisites</u>
 - <u>Access procedure</u>

The information presented in this section is only for platforms with the Ethernet switch IO module.

- The switch NOS can be accessed through various methods:
 - Using the switch NOS Web UI
 - Using <u>Serial over SSH from a remote computer</u>
 - Using <u>SSH from a remote computer</u>
 - Using <u>SSH from the integrated server</u>
 - Using the <u>BMC Web UI SOL console</u>

Refer to Description of system access methods for more information on the various paths.

Accessing the switch NOS using the Web UI

Prerequisites

1	One of the switch IP addresses is known.
2	The remote computer has access to the switch network subnet.
Relevant section:	
Discove	ring platform IP addresses

Browser considerations

HTML5	To connect to the Web UI, a Web browser supporting HTML5 is required.
HTTPS self- signed certificate	Upon connection to the Web UI, it is mandatory to accept the HTTPS self-signed certificate. For further information about accepting HTTPS self-signed certificates, please refer to your Web browser's documentation.
File download permission	File download from the site needs to be permitted. For further information about file download permission, please refer to your Web browser's documentation.
Cookies	Cookies must be enabled in order to access the website. For further information about enabling cookies, please refer to your Web browser's documentation.

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

Access procedure

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

Step_1	From a remote computer that has access to the switch network, open a browser	🚱 kontron	Ко	ntron Ethe	rnet Switch
	window and enter the IP address discovered for the switch.	Configuration Monitor	Port State Overview		,
	<i>http://[SWITCH_IP]</i>	Hondier Synate Unverset Synate Unverset Toermal Protection Ports Outs Status Outs Outs Status Outs Status	Port State Overview Port Description 1 SFP_PORT_SW1 3 SFP_PORT_SW1 2 SFP_PORT_SW3 3 SFP_PORT_SW3 4 SFP_PORT_SW5 6 SFP_PORT_SW5 5 SFP_PORT_SW5 6 SFP_PORT_SW5 9 SFP_PORT_SW5 1 SFP_PORT_SW5 1 SFP_PORT_SW5 1 SFP_PORT_SW5 1 SFP_PORT_SW1 1 SFP_PORT_SW1 1 SFP_PORT_SW1 1 SFP_PORT_SW1 1 SFP_PORT_SW1 2 SFP_PORT_SW1 1 SFP_PORT_SW1 1 SFP_PORT_SW1 1 SFP_PORT_SW1 2 SFP_PORT_SW1	Link Currer 1 Gidx Down Down Down Down Down Down Down Down	2 Speed 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gfdx 10Gf
		MAC Table VLANs VLANs MVRP SFlow DOMI UDLD TSN Diagnostics Maintenance	16 INTERNAL_PORT_SRV4 Note: ports with no configured spi	eed are disabled o	10Gfdx lue to the selected

Accessing the switch NOS CLI using BMC Web UI Serial over LAN console

Prerequisites

1	The BMC IP address is known.		
2	The remote computer has access to the management network subnet.		
Relevant sections:			
Access	Accessing a BMC		

Accessing a BMC Discovering platform IP addresses Platform power management

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 NOS

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.	Your connection is not secure. The mean of 12,161,10,10 has configured their website improperly. To protect your information from being contractive to this website. The mean Improve the mean of the theorem the theorem the mean 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.	Al Security Exception Image: Control	
Step_4	Log in to the BMC Web UI using the appropriate credentials.	Vername S&T Group S&T Group OpenBMC	
Step_5	You now have access to the management Web UI of the BMC. You can use the interface.	Owner Overview Event logs Overview POST code logs Image: Code logs Operations Image: Code logs Operations Server information Security and access Vertified logs Resource management Nondexturg Dies Nondexturg Dies Servier information Nondexturg Dies	

Launching the Web UI SOL console

Step_1	From the BMC Web UI, click on the Operations menu and then on the SOL console button.	Conversion Conversion Logs ~ Hardware status ~ Operations ~ KVM Firmware Reboot BMC Solic console Server power operations Virtual media Settings ~ Security and access ~ Besource management ~	Keatak Over view Machine Zazi-11-23 16:14:31 Urc Crewer information Medel Manufacture Medel Manufacture Manuf	Rower Chartesh (2) admin + Server LD ● Off off Solt console → Product information Name Manufacturer PRODUCT_NAME Kontron Soil anumber Part subber 9017064072 1057-2338 Asset Tag Wanis
Step_2 Step_3	Change the dropdown menu value to Switch Console . The NOS screen should be displayed.	Sol. console redirects the server's set Sol. console redirects the server's set Status: Connected Password:	N (SOL) CONSOL rerial port output to this window. Switch Console	e

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

Accessing the switch NOS CLI using Serial over SSH from a remote computer

Prerequisites

1	The BMC IP address is known.
2	The remote computer has access to the management network subnet.
З	An SSH client tool is installed on the remote computer. NOTE: PuTTY is recommended for Windows environments and SSH is recommended for Linux environments.
Rele	evant section:
Disc	overing platform IP addresses

Access procedure

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

Step_1	 1 Using an SSH client tool, open an SSH session with the following parameters: • BMC IP address • Port number: 2201 (the BMC will automatically redirect communication to the switch NOS serial console) 	
Step_2	Log in the BMC using the appropriate credentials. Upon successful login, press Enter to get a response from the switch NOS CLI.	IStaX - Kontron 0.02.014833d3 2022-01-08T11:19:1304:00 Press ENTER to get started
		Username: admin Password: #

Accessing the switch NOS CLI using SSH from a remote computer

Prerequisites

1	The network switch IP address is known.
2	The remote computer has access to the switch network subnet.
3	An SSH client tool is installed on the remote computer. NOTE: PuTTY is recommended for Windows environments and SSH is recommended for Linux environments.
Relevant section:	

Discovering platform IP addresses

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, open an SSH client tool and connect with the NOS IP address.	
Step_2	Log in the switch NOS CLI using the appropriate credentials.	IStaX - Kontron 0.02.014833d3 2022-01-08T11:19:1304:00 Press ENTER to get started Username: admin Password: #

Accessing the switch NOS CLI using SSH from the integrated server

Prerequisites

1	An OS is installed on the integrated server.
2	The remote computer has access to the integrated server OS.
З	One of the switch IP addresses is known.
4	The integrated server has access to the switch network subnet.
5	An SSH client tool is installed on the remote computer. NOTE: PuTTY is recommended for Windows environments and SSH is recommended for Linux environments.
Rele	vant sections:

Discovering platform IP addresses Accessing the operating system of a server

Access procedure

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

Step_1	Access the integrated server operating system using the prefer	red method.
Step_2	Using an SSH client tool, open an SSH session with the following parameter: • Switch NOS IP address Log in the switch NOS CLI using the appropriate credentials.	IStaX - Kontron 0.02.014833d3 2022-01-08T11:19:1304:00 Press ENTER to get started Username: admin Password: #

Discovering platform IP addresses

Table of contents

- <u>Discovering the BMC IP address</u>
 - Discovering the platform BMC IP address with DHCP Dynamic DNS update
 - <u>Prerequisites</u>
 - <u>Procedure</u>
 - Discovering the platform BMC IP address using the UEFI or BIOS
 - <u>Accessing the UEFI/BIOS using a serial console (physical connection)</u>
 - <u>Prerequisites</u>
 - Port location
 - <u>Accessing the UEFI/BIOS setup menu</u>
 - <u>Accessing the BMC network configuration menu</u>
 - Discovering the platform BMC IP address using DHCP server logs
 - Prerequisites
 - <u>Procedure</u>
- Discovering the switch NOS IP address
 - Discovering the switch NOS IP address through the switch NOS serial console CLI
 - <u>Prerequisites</u>
 - <u>Procedure</u>

Discovering the BMC IP address

The BMC IP address is the minimum required to access the BMC Web user interface of the platform. It is also used to access the monitoring interface and the KVM/VM to install an operating system.

- The BMC IP address can be discovered:
 - Using <u>DHCP Dynamic DNS update</u>
 - Using the UEFI/BIOS via a serial console (physical connection) device with no OS installed and no known IP address
 - Using the <u>DHCP server logs</u>

Discovering the platform BMC IP address with DHCP Dynamic DNS update

Prerequisites

3	The first assigned MAC address of the BMC is known.
2	A remote computer configured with the same DNS server is available.
1	A DHCP server with active Dynamic DNS update feature is available.

Relevant section:

MAC addresses

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 "BMC" prefix and the first BMC MAC address. For example, if we use the first BMC MAC address (00:a0:a5:d2:e9:0a), the host name would be: BMC 00A0A5D2E90A. Note that this is the default configuration, but that the parameter is user configurable. The method described here only works if the default hostname is still in effect. 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 BMC00A0A5D2E90A	Pinging BOARD NAME_00A0A5D2E90A[172.16.211.126] with 32 bytes of data: Reply from 172.16.211.126: bytes=32 time<1ms TTL=60 Reply from 172.16.211.126: bytes=32 time<1ms TTL=60 Reply from 172.16.211.126: bytes=32 time<1ms TTL=60 Reply from 172.16.211.126: bytes=32 time<1ms TTL=60
		<pre>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</pre>

Discovering the platform BMC IP address using the UEFI or BIOS

Accessing the UEFI/BIOS using a s erial console (physical connection)

Prerequisites

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

Port location



Accessing the UEFI/BIOS setup menu

Step_1	From a computer with a physical connection to the serial port, open a serial console and the port to which the device is connected.	console tool and start the communication between the
Step_2	 Perform a server reset using one of the following options: If the server is currently running an installed operating system, log in and issue the appropriate reboot command. If the server is currently running the integrated UEFI shell, issue the "reset" command. Send a "BREAK" signal over the serial connection using the method provided in the terminal emulator. Disconnect all the input power connections for 30 seconds and reconnect them. NOTE: If an operating system is installed on the device, a method based on a 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 UEFI/BIOS sign on screen to display. 	<pre>ME120 System starting 0:12 = refrequences initialization. %E120 System BIOS version: 0.08.0146552F Date: "07/20/2020" Intel RC Version: 06051, CPU Info: Intel(R) Xeon(R) D-2187NT CPU @ 2.00GHz Processors: 1, Cores: 16, Stepping: N0 Memory Info: Memory Size: 16, Stepping: N0 Memory Size: 16, Stepping: 16, Stepping:</pre>
Step_3	When the UEFI/BIOS sign on screen is displayed, press the specified key to enter the UEFI/BIOS setup menu. NOTE : It may take a few seconds for the UEFI/BIOS sign on screen to display confirmation message "Entering Setup".	Versian 2.20.1271. Copyright (c) 2020 American Megatrends, Inc. BIOS Date: 07/20/2020 16:40:55 Version 0.08 0146552r MEL210/ASI210 Firmware version 0.08 0146552r Press dBELs or <f2> to enter setup. Press <f7> for boot menu.</f7></f2>
Step_4	The UEFI/BIOS sign on screen displays "Entering Setup". NOTE: It will take several seconds to display and enter the UEFI/BIOS setup menu.	Version 2.20.1271. Copyright (C) 2020 American Megatrends, Inc. BIOS Date: 07/20/2020 16:46:53 Version 0.08.024552F MEL100ACLID Firmare variant 0.08.0246532F FALLOR 472- to enter setup. Press 47> for boot menu. Entering Setup
Step_5	The UEFI/BIOS setup menu is displayed.	Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc. Main Advanced Platform Configuration Socket Configuration Server Mgmt > EIOS Information Configuration Socket Configuration Server Mgmt > BIOS Vendor Anchoos the system Core Version S.14 Alchoos the system Core Version UEI 2.6; PT 1.4 * Project Version 07/20/2020 15:46:5 * Build Date and Time 07/20/2020 15:46:5 * Platform Information Flatform Socket Soc FLQS/PRQ - B2-D * Processor Soc FLQS/PRQ - B2-D * Processor Information Total Memory 16384 MB Version 2.20.1271. Copyright (C) 2020 American Megatrends, Inc.

Accessing the BMC network configuration menu

In an ME1210 platform with a pass-through IO module, the BMC is accessible via two network connections. Depending on the configuration interface used, the names for the network connections change.

IPMI and UEFI/BIOS	Redfish and Web UI	Network connectivity
LAN channel 1	eth0	Front panel Srv 5
LAN channel 2	eth1	Front panel Srv 4

In an ME1210 platform with an Ethernet switch IO module, the BMC is accessible via two network connections. Depending on the configuration interface used, the names for the network connections change.

IPMI and UEFI/BIOS	Redfish and Web UI	Network connectivity
LAN channel 1	eth0	Front panel Srv 5
LAN channel 2	eth1	Internal server port 4 \rightarrow switch port 16 *

* The BMC can then communicate through SFP ports Sw 1 to 12, depending on switch configuration.

Stop 1	From the LIFEL/BIOS menu, pavigate to tab Server Mant	Aptio Setup Utilit	y - Copyright (C) 2019 Am	erican Megatrends, Inc.
Jtep_1		Ani Advanced Inter DICS Information DICS Version Compliancy Project Version Build Date and Time Access Level FPGA Version Memory Information Total Hemoty System Language System Date System Time Version 2.20.1271	American Negatrands 5.14 UEFI 2.6: PI 1.4 06/26/2019 09:12:28 Administrator 2.02.0800AD12 32766 HB [English] [Ved 07/10/2019] [13:47:54]	<pre>intry sole Arch dops [Choose the system [default language]</pre>
Step_2	Select BMC network configuration .	Aptio Setup Utilit Main Advanced Intel Main Advanced Intel Mait For BHC FRB-2 Timer Follow FRB-2 Timer Follow GS Watchdog Timer OS Wat Timer Follow	y - Copyright (C) 2019 Am RCSetup Server Ngmt Sec KCS, USB [Disabled] [Enabled] [Foure Cycle] [Poure Cycle] [Disabled] [Disabled] [Reset]	AB erican Megatrends, Inc. urity Boot Event Logs ~ Press <enter> to enable + or disable Serial Mux + configuration. + * * * * * * </enter>
		Serial Hax > System Event Log > View FRU information > BHC network configurat > View System Event Log > BHC Warm Reset 	[Disabled] ion . Copyright (C) 2019 Amer	<pre>"!>: Select Screen "!"v: Select Icem "Enter: Select "Enter: Select "If: General Help "IF: Pervious Values "IF: Pervious Values "IF: Pervious Values "IF: Pervious Values "IF: Select Screen Version Version" "If: Pervious Values "If: Select Screen Version" "If: Select Screen Vers</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 Utilit BRC network configur Configure IPV4 support Configure IPV4 support Configure IPV4 support Course Coursen Configuration Address source Station IP address Subnet mask Station IMAC address Router IP address Router IP address Router IP address Router MAC address Lan channel 2 	<pre>y - Copyright (C) 2019 Am Server Hunt ation (Unspecified) DynamicAddressBmcDhop 172.16.005.245 255.25.0.00 00-40-52-5.0.01 00-05-64-27-10-57 . Copyright (C) 2019 Amer</pre>	arican Megatrends, Inc. ()Select to configure LAN ()Channel parameters ()atarically or ()atarically of ()atarically of

Discovering the platform BMC IP address using DHCP server logs

Prerequisites

2	The first assigned MAC address of the BMC is known.
1	Access to the DHCP server logs is required.

Relevant section:

MAC addresses

Procedure

DHCP IP assignment is specific to the network infrastructure to which the platform is being integrated. The assistance of the network administrator may therefore be necessary to obtain the BMC IP address.

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

The following example illustrates a command prompt method for use with a Linux based DHCP server. This may need to be adjusted to reflect a specific DHCP infrastructure (this action can generally also be done through a DHCP server Web interface).

```
DHCP_Server:~$ cat /var/log/messages * | grep -i 00:a0:a5:d2:e9:0a
Mar 1 13:44:15 DHCP_Server dhcpd: DHCPDISCOVER from 00:a0:a5:d2:e9:0a via ens192
Mar 1 13:44:16 DHCP_Server dhcpd: DHCPOFFER on 172.16.211.126 to 00:a0:a5:d2:e9:0a via ens192
Mar 1 13:44:16 DHCP_Server dhcpd: DHCPREQUEST for 172.16.211.126 (172.16.0.10) from 00:a0:a5:d2:e9:0a via ens192
Mar 1 13:44:16 DHCP_Server dhcpd: DHCPACK on 172.16.211.126 to 00:a0:a5:d2:e9:0a via ens192
```

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

Discovering the switch NOS IP address

The switch NOS IP address can be discovered :

• Through the switch NOS serial console CLI

Discovering the switch NOS IP address through the switch NOS serial console CLI

Prerequisites

2	The remote computer has access to the management network subnet.
З	An SSH client tool is installed on the remote computer. NOTE: PuTTY is recommended for Windows environments and SSH is recommended for Linux environments.
Rele	evant sections:

Default user names and passwords Accessing the switch NOS

Procedure

NOTE: When using Serial over SSH, to quit the session press ${\it Enter}$ followed by ~ .

Step_1	 Using an SSH client tool, open an SSH session with the following parameters: BMC IP address Port number: 2201 (the BMC will automatically redirect communication to the switch NOS serial console) 	login as: admin admin@172.16.220.94's password:
Step_2	Log in the BMC using the appropriate credentials. Upon successful login, press Enter to get a response from the switch NOS CLI.	IStax - Kontron 1.02.014833d3 2021-09-18T11:19:13-4:00 Press ENTER to get started #
Step_3	Use the following command to discover the switch NOS IP address. LocalSwitchNOS_OSPrompt:~# show ip interface brief	<pre># show ip interface brief Interface Address Method Status</pre>

Default user names and passwords

Table of contents

- <u>Management interface (BMC)</u>
- Switch network operating system (NOS)
- <u>Operating system</u>
- <u>UEFI/BIOS</u>

NOTE: For security reasons, it is important to change the default user names and passwords as soon as possible. Refer to <u>Configuring and managing users</u>.

Management interface (BMC)

The BMC is accessible via:

- Web UI
- Redfish
- IPMI

All the access methods share the same users.

User name	Password
admin	ready2go

Switch network operating system (NOS)

User name	Password
admin	ready2go

Operating system

The user name and password are application-specific.

However, if Kontron provided an operating system, the credentials will be the following:

User name	Password
root	kontron

UEFI/BIOS

No default password is set.

Software installation and deployment

- <u>Preparing for operating system installation</u>
- Installing an operating system on a server
- <u>Verifying operating system installation</u>
- Platform resources for customer application
- <u>Common software installation</u>

Preparing for operating system installation

Step_1Choose the operating system needed based on the requirements of your application. It is recommended to choose one from the list of
validated operating systems.Step_2Confirm the OS version to be installed includes or has divers supporting the platform components listed in the PCI mapping.Step_3If 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

Table of contents

- Installing an OS on a server using the KVM
 - Launching the KVM
 - Mounting the operating system image via virtual media
 - <u>Accessing the UEFI/BIOS setup menu</u>
 - <u>Selecting the boot order from boot override</u>
 - Completing operating system installation
- Installing an OS on a server using PXE (Boot from LAN)
- Installing an OS on a server using a USB storage device

The operating system can be installed using the following methods :

- The <u>KVM</u>
- PXE (Boot from LAN)
- A <u>USB storage device</u>

Installing an OS on a server using the KVM

Relevant section: Accessing a BMC using the Web UI

Launching the KVM



Mounting the operating system image via virtual media

Step_1	From the Operations menu, select Virtual media .	Image: Server LED Event logs POST code logs Event logs POST code logs Event logs Inventory and LEDs Sensers BMC information Server lab Operations KVM Firmware Reboot BMC Sol console Server power operations Model Model Server power operations Power consumption
Step_2	Click on Add file to browse for the ISO file.	Windamedia Bxc000AASE10e20 Poer consumption Poer consumption Besturings Padness 172:16:182:33 Poer consumption Disabled Virtual media Load image from web browser Virtual media device Add file Virtual file State State State State State State State
Step_3	Click on Start to access virtual media from the OS.	Virtual media Load image from web browser Virtual media device Indef file OS.iso ×

Accessing the UEFI/BIOS setup menu

Step_1	From the BMC Web UI, click on the Power button.	Skontron	S Refresh 🛞 admin -
		E Overview E Logs ∨ B Hardware status ∧ Inventory and LEDs Sensors Z Operations ∨ ® Settings ∨ ✓ Security and access ∨	Overview Server LD B221-11-20 163358 UTC Off Dit network settings Off Server information Server LD Nodel PRODUCT,NAME Manufacturer Robuct, NAME Manufacturer Network Manufacturer Diracionaria Server information
Step_2	From the Reboot server section, select Orderly and then click on Reboot .	Operations Reboot server O Orderly – opera Immediate – Sei shutting down; Reboot	ting system shuts down, then server reboots rver reboots without operating system may cause data corruption
Step_3	From the Operations menu, click on KVM .	E Cverview E Logs Hardware status ~ Coperations ^ KVM * Firmware Reboot BMC	Image: Note of the expension of the

		SQL console Server power operations Virtual media Serve Security and access Calculation Security and access Security and
Step_4	When the UEFI/BIOS sign on screen is displayed, press the specified key to enter the UEFI/BIOS setup menu. NOTE: When a reset server command is launched, it may take a few seconds for the UEFI/BIOS sign on screen to display. NOTE: It may take a few seconds for the UEFI/BIOS sign on screen to display the confirmation message "Entering Setup".	<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></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>
Step_5	The UEFI/BIOS sign on screen displays "Entering Setup". NOTE : It may take several seconds to display and enter the UEFI/BIOS setup menu.	<page-header><image/><image/><image/><image/><image/><image/><image/><image/><image/><image/><image/><image/><image/><image/><image/><image/><image/><image/><image/><image/><image/></page-header>
Step_6	The UEFI/BIOS setup menu will be displayed.	Exercite

Selecting the boot order from boot override

Step_1	From the UEFI/BIOS setup menu and using the keyboard arrows, select the Save & Exit menu. In the Boot Override section, select UEFI: Linux File-Stor Gadgetxxxx and press Enter. The server will report and the media installation process will start.	KVM Statuz: ⊘ Connected ↓ Send Ctri+Alt+Delete [2] Open in new tab
		Add 5 detup utility - Logy ight (c) 2021 Averican regatrends, inc. • Sound's and a bar a

Completing operating system installation

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

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

Relevant sections:

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

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

Step_1	From the UEFI/BIOS setup menu, select the Advanced tab and then the Network Stack Configuration submenu.	Main Edvanced Platform Configuration Server Wgmt 2 Avoid Study Utility - Copyright (C) 2020 American Megatends, Inc. > Trusted Computing Alkimork Stack Settings > ACPT Settings Alkimork Stack Settings > Sorting Utility - Copyright (C) 2020 American Megatends, Inc. > ACPT Settings Alkimork Stack Settings > SID Configuration * > PCT Subsystem Settings * > Network Stack Configuration * > Network Stack Configuration * > Note Configuration * > SISC Configuration * > Intel(R) Virtual RAID on CPU * > Intel(R) Virtual RAID on CPU * > Intel(R) 1210 Gigabit Network Connection * 00:A0:AS:DD:4A:10 * Shell] VFH: Save & Exit Shell] VFH: Save & Statt
Step_2	Set Network Stack to Enabled . Set IPv4 PXE Support or IPv6 PXE Support , depending on the application, to Enabled .	Advanced Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc. Instruction starts Investment starts Investment starts Investment starts Investment starts Investment starts Investment starts Investment starts Investment starts Investment starts PXE boot wait time 0 Media detect count 1
Step_3	Reboot the system and access the UEFI/BIOS setup menu again.	
Step_4	Navigate to the Save & Exit menu and then to the Boot Override section.	Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc. < Store Changes and Reset Discard Changes and Reset Discard Changes and Reset Discard Changes Default Options Restore Defaults Restore Defaults Restore User Defaults Restore User Defaults Restore Isen Defaults Restore Isen Defaults Restore Isen Defaults Restore Isen Defaults Restore Isen Defaults Restore Isen Defaults Restore User Defaults Restore Isen Defaults Restore User Defaults Save as User Defaults Restore User Defaults Save As User Defaults Restore User Defaults Save As User Defaults Version State Streen * >>: Select Streen * Select Streen * Select Streen * >>: Select Stre
Step_5	Choose the PXE option desired.	Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc. Security Boot Save & Exit Save changes and Reset A Discard Changes and Reset + Discard Changes + Discard Changes + Discard Changes + Discard Changes + Default Options * Restore Defaults * Restore User Defaults * Boot Override + UEFI: Pit Ard Intel(A) IZ10 Grgabit Network * UEFI: Suilt-in EFI Shell * Save a D: Mark Sol 3046 *

Installing an OS on a server using a USB storage device

Relevant sections:

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

Step_1	Create a bootable USB key using the appropriate software. NOTE : RUFUS is recommended.	
Step_2	Open the USB directory in a remote computer.	
Step_3	Navigate to EFI then BOOT (e.g.: E:/EFI/BOOT/).	
Step_4	Open the grub.cfg file with any text editor.	
Step_5	Edit the file and add the following line on the top to activate the serial installation: <i>serialspeed=115200</i> <i>terminal_input serial</i> <i>terminal_output serial</i>	<pre>serialspeed=115200 terminal_input serial terminal_output serial set default="1" function load_video { insmod efi_gop insmod efi_gop insmod efi_uqa insmod video_bochs insmod video_cirrus insmod all_video i } </pre>
Step_6	 Scroll down the file and edit the menu used to start the OS installation. Edit as follows: Remove the quiet argument, if present. Add the console=ttyS0,115200n8 argument. An example is provided in the image for CentOS 7. 	<pre>2 ### EXCENT /Activated/10.11cms ### 2 ### EXCENT /Activated/10.11cms ### 2 #### EXCENT /Activated/10.11cms /### 3 Intradif /Image/geodor/Introd.img 3 Intradif /Image/geodor/Introd.img 4 Intradif /Image/geodor/Introd.img 4 Intradif /Image/geodor/Introd.img 4 Intradif /Image/geodor/Introd.img 4 Intradif /Image/geodor/Introd.img 5 Introdif /Image/geodor/Introd.img 5</pre>
Step_7	Save the file and eject the USB key.	
Step_8	Insert the USB key into one of the USB ports of the front panel.	
Step_9	Power on the platform and access the UEFI/BIOS setup menu	1.
Step_10	Navigate to the Save & Exit menu and then to the Boot Override section.	Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc. < Security Bot
Step_11	Choose the USB option desired.	

Verifying operating system installation

Relevant sections:

- Product architecture
- <u>PCI mapping</u>
- Accessing the operating system of a server
- <u>Common software installation</u>

Verifying support for devices

All the results and commands may vary depending on the operating system and the devices added.

Step_1	Reboot the OS as recommended, then access the OS command prompt.	
Step_2	Install ethtool , ipmitool and pciutils using the package manager, and update the operating system packages. The ipmitool version recommended is 1.8.18. Example for CentOS: LocalServer_OSPrompt:~# yum update LocalServer_OSPrompt:~# yum install pciutils LocalServer_OSPrompt:~# yum install ethtool LocalServer_OSPrompt:~# yum install ipmitool	
Step_3	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_4	Verify that the DIMMs are detected. LocalServer_OSPrompt:~# free - h	[-]# free -h Hem: total used free shared buff/cache available Hem: 156 211M 146 17M 191M 146 Swap: 08 08 08
Step_5	Verify that all the storage devices are detected. LocalServer_OSPrompt:~# lsblk	[-]#]sblk NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT sda 8:0 0 29.8g 0 disk -sdal 8:1 0 512M 0 part -sda2 8:2 0 29.3g 0 part sdb 8:16 0 29.8g 0 disk
Step_6	Confirm the control plane network interface controller is loaded by the igb driver. LocalServer_OSPrompt:~# lspci -s 04:00 -v NOTE: You should discover one 1GbE NIC.	[-]Hingci = 5 0400 Structure controller: Intel Componetion III Gigabit Herwork Connection (rev 03) Structure matter develop 14400 (1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 1400 - 14
Step_7	Confirm the data plane network interface controllers are loaded by the i40e driver. LocalServer_OSPrompt:~# lspci -s b8:00 -v NOTE: You should discover up to four 10GbE NIC.	[-[flagels.Bi(0) -v B0(0). Theorem: unrecolar investigation Reherence Connection 3722 for 10% headplane (rev 0) 30(0). Theorem: unrecolar investigation (rev 0), TG 34, SEM hold 0 Box (rev 0), TG 30(0),
Step_8	Confirm that all the network interfaces are detected and get the list of device names. The following script requires Bash shell. Enter the following block of commands at the LocalServer_OSPrompt:~# ETH_NAMES=\$(grep PCI_SLOT_NAME /sys/class/net/*/device/uevent cut -d '/' -f 5) for ETH_NAME in \$ETH_NAMES; \ do echo -e "\$ETH_NAME: \$(ethtool -i \$ETH_NAME grep -E 'driver bus-info')\n"; \ done	<pre>[-]#ETH NAMES=8(grep FCI_SLOT NAME /sys/class/net/*/device/uevent cut -d '/' -f 5) [-]#for ETH_NAME in %ETH_NAMES; \ > > do echo -e "%ETH_NAME ! %(ethtool -i %ETH_NAME) grep -E 'driver/bus-info')\n"; \ > > done ethl: driver: 140e bus-info: 0000:b8:00.0 eth2: driver: iqb bus-info: 0000:b8:00.1 eth4: driver: 140e bus-info: 0000:b8:00.2 eth5: driver: 140e bus-info: 0000:b8:00.3</pre>
	NOTE: You should discover one 1GbE NIC and up to four 10GbE NIC.	
Step_9	Configure network interface controllers based on your requirements and network topology.	

 NOTE: Interface names may change depending on the OS installed. However, parameters Bus:Device.Function stay the same for the

 Version 2.0 (June 2022)
 www.kontron.com
 // 129

	interface regardless of the operating system.	
Step_10	(Optional) If one or two PCIe add-in cards are installed, verify that the cards are detected. LocalServer_OSPrompt:~# lspci	(c)# lepci (c)# lep
Step_11	Verify communication between the operating system and the BMC. LocalServer_OSPrompt:~# ipmitool mc info	<pre>[-]# ipmitool mc info Device ID : 0 Device Revision : 0 Pirmware Revision : 0.00 IPMI Version : 2.00 Manufacturer ID : 15000 Manufacturer Name : Kontron Product ID : 10027 (0x272b) Product Name : Unknown (0x272b) Devide SDRs : yes Provides Device SDRs : yes Additional Device Chassis Device FRU Inventory Device Chassis Device Aux Firmware Rev Info : 0 0x46 0x44 0x4b</pre>

Operating system power management states

The ME1210 platform does not support power management states. Please refer to <u>Disabling sleep states in Linux</u> for more information.

Platform resources for customer application

Table of contents

- <u>Application ready indication via the power LED</u>
 - <u>Prerequisites</u>
 - <u>Script example</u>
- <u>Customer-specific temperature sensors</u>
 - <u>Prerequisites</u>
 - <u>Script example</u>
 - Additional low level information
 - Port address offset
 - <u>Converting a temperature to hexadecimal</u>
- <u>Configuring the virtual FRU for a PCIe add-on card</u>
 - Listing the available FRUs
 - Adding a virtual FRU
 - <u>Removing a virtual FRU</u>

This section describes platform resources to be coded into the customer application to benefit from all the platform functionalities.

Application ready indication via the power LED

The green power LED can be configured to indicate that the application is ready. **NOTES:**

- The action will be necessary at every power up.
- The LED cannot return to blinking state. A power cycle action will be required.
- The action is harmless if done multiple times.

Prerequisites

1	An OS is installed.
2	Access to the OS is required.
З	The OS App. Ready Led Control UEFI/BIOS option must be set to Disabled.

Relevant sections:

Accessing the operating system of a server Configuring UEFI/BIOS options

Script example

The script example provided is in C. Value 0x01 must be written to the I/O register 0xA20 (byte wide).

#include <sys/io.h>
int main(void)
{
 iopl(3);
 outb(0x01, 0xa20);
 iopl(0);
 return 0;
}

Customer-specific temperature sensors

Some temperature sensors can be manually set from the operating system of the server. Once a value is set, it must be sent periodically within 5 seconds so the fan algorithm does not increase fans to maximum. This is to insure that if the operating system becomes unresponsive, the fans will still cool the system adequately. The valid temperature range is -127 °C to 127 °C. If the value is not updated within 5 seconds, the sensor will be set to maximum value at 128, which will trigger an Upper critical event with maximum fan speed.

The sensors that can be updated in this way are:

- Temp PCIe 1 mbox
- Temp PCIe 2 mbox

By modifying the scripts provided below, the sensors can be renamed.



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.

Prerequisites

1	An OS is installed.
2	Access to the OS is required.
Relevant sections:	

Accessing the operating system of a server Configuring sensors and thermal parameters Sensor list

Script example

The following example uses 2 scripts.

The first script (daemon.sh) is a daemon that monitors a file for new sensor values. It will convert human readable sensor information and write it to the correct port. This script should be launched at boot. To start the script, type "./daemon.sh start"

daemon.sh

#!/usr/bin/env bash

```
sensor_daemon_pipe=/tmp/sensor_daemon_pipe
 sensor_names=("Temp PCIe 1 mbox" "Temp PCIe 2 mbox" "" "" "" "" "" "")
 get_sensor_index() {
   name=$1
   for i in "${!sensor_names[@]}"; do
    if [[ "${sensor_names[$i]}" = "${name}" ]]; then
      echo "${i}";
     fi
  done
 }
 start() {
  trap "rm $sensor_daemon_pipe" EXIT
  if [[ ! -p $sensor_daemon_pipe ]]; then
    mkfifo $sensor_daemon_pipe
   fi
   echo "Daemon started"
   while read data < $sensor_daemon_pipe; do
    sensor_name=$(echo $data | cut -f1 -d=)
    sensor_value=$(echo $data | cut -f2 -d=)
    index=$(get_sensor_index "$sensor_name")
    let TEMP_PORT=0xa28+$index
    hexa=$(printf '%02x\n' $sensor_value)
    printf "\\x$hexa" | dd of=/dev/port bs=1 count=1 seek=$(($TEMP_PORT)) status=none
   done
 }
 case "$1" in
   'start')
     start
    ;;
   *)
     echo
     echo "Usage: $0 { start }"
     echo
     exit 1
    ;;
 esac
The other script sends new sensor values to the file monitored using the following syntax:
```

<Sensor Name>=<Sensor Value>

client.sh
#!/usr/bin/env bash
sensor_daemon_pipe=/tmp/sensor_daemon_pipe
echo "Client Started"
while true; do
echo "Temp PCle 2 mbox=50" > \$sensor_daemon_pipe
sleep 2
echo "Temp PCle 2 mbox=30" > \$sensor_daemon_pipe
sleep 2
echo "Temp PCIe 2 mbox=60" > \$sensor_daemon_pipe
sleep 2
done

NOTE: The scripts were tested with Ubuntu 20.04. They should work on any Linux system that supports Bash version 4.x+.

Additional low level information

The information in this is section is only needed if you are writing directly in the memory port associated with the sensors.

Port address offset

The address offset gives access to the register of the desired sensor.

Sensor	Address offset
Temp PCIe 1 mbox	0xa28
Temp PCIe 2 mbox	0xa29

Converting a temperature to hexadecimal

Positive values are represented by hexadecimal numbers from 0x00 to 0x7F.

- 0°C is the smallest positive value available and corresponds to 0x00.
- 127°C is the largest positive value and corresponds to 0x7F.

Negative values are represented by hexadecimal numbers from 0x81 to 0xFF.

• -1°C is the smallest negative value available and corresponds to 0xFF.

• -127°C is the largest negative value and corresponds to 0x81.

Value 0x80 is marked as n/a, which means no reading.

Configuring the virtual FRU for a PCIe add-on card

In order to automatically report their temperatures to the BMC, some PCIe add-in cards need to be registered into the BMC virtual FRU. **Relevant sections**:

Hardware compatibility list Sensor list Accessing a BMC using Redfish Configuring sensors and thermal parameters

Listing the available FRUs



Adding a virtual FRU



Removing a virtual FRU

Step_1	To unregister a PCIe add-in card from the virtual FRU, use the following command. PCIE_SLOT can either be PCIe1 or PCIe2. RemoteComputer_OSPrompt:~# curl -k -srequest PATCHurl [ROOT_URL]/redfish/v1/Managers/bmcheader "'Content-Type: application/json'"data '{"Oem": {"Kontron": {"VirtualPcieFru": {"[PCIE_SLOT]": ""} } } } ' jq
	<pre>\$ curl -k -srequest PATCHurl https://admin:ready2go@172.16.182.31/redfish/ vl/Managers/bmcheader "'Content-Type: application/json'"data '{"Oem": {"Ko ntron": {"VirtualPcieFru": {"PCIel": ""}}}' jq { "Oem": { "Kontron": { "VirtualPcieFru": { "VirtualPcieFru": { "PCIel": "" } } }</pre>
Step_2	Reboot the BMC to apply the changes. RemoteComputer_OSPrompt:~\$ curl -k -srequest POSTurl [ROOT_URL] /redfish/v1/ Managers /bmc/Actions/Manager.Resetheader "Content-Type: application/json"data '{"ResetType":"GracefulRestart"}' jq
	<pre>\$ curl -k -srequest POSTurl https://admin:ready2go@172.16.182.31/redfish/ 1/Managers/bmc/Actions/Manager.Resetheader 'Content-Type: application/json' -data ''{"ResetType":"GracefulRestart"}" jq { "@Message.ExtendedInfo": [{ "@odata.type": "#Message.v1_1_1.Message", "Message": "Successfully Completed Request", "MessageArgs": [], "MessageArgs": [], "MessageId": "Base.1.8.1.Success", "MessageSeverity": "OK", "Resolution": "None" } } }</pre>

Common software installation

Table of contents

- <u>Required software tools</u>
- <u>Recommended software tools</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.

Required software tools

Tool	Description
ipmitool	IPMI utility for controlling and monitoring the devices through the IPMI interfaces of the platform.
ethtool	Network driver tool used in the documentation.
pciutils	Tool used to manage PCIe add-in cards connected to the platform.
hdparm	Command line program for Linux.
nvme-cli	Userspace tooling to control NVMe drives.

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.

Configuring

- <u>Configuring system access methods</u>
- <u>Configuring date and time</u>
 - Configuring BMC date and time
 - Configuring switch NOS date and time
- <u>Configuring networking</u>
 - Configuring the BMC networking
 - Configuring UEFI network boot
 - Configuring switch NOS networking
- <u>Configuring the switch</u>
- <u>Configuring synchronization</u>
- <u>Configuring UEFI/BIOS options</u>
- <u>Configuring and managing users</u>
 - Configuring and managing BMC users
 - Configuring and managing switch NOS users
- <u>Configuring sensors and thermal parameters</u>

Configuring system access methods

Table of contents

- <u>General considerations and warnings about network configuration</u>
- <u>Configuring IPMI access methods</u>
 - LAN channels
 - <u>Configuring IPMI over LAN</u>
 - <u>Configuring Serial over LAN parameters</u>

General considerations and warnings about network configuration

The architecture of the ME1210 platform offers many entry points, including two LAN channels 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 BMC LAN channel 2 is disabled and 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 both LAN channels will now be disabled.

Relevant sections:

- <u>Default user names and passwords</u>
- Configuring and managing users
- <u>Product architecture</u>
- <u>Configuring the BMC networking</u>

For any configuration related to the Ethernet switch IO module, refer to Configuring the switch.

Configuring IPMI access methods

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

The following procedures will be executed using the <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] -C 17.

LAN channels

For more information, refer to Product architecture.

Ethernet switch IO module BMC LAN channels

In an ME1210 platform with an Ethernet switch IO module, the BMC is accessible via two network connections. Depending on the configuration interface used, the names for the network connections change.

IPMI and UEFI/BIOS	Redfish and Web UI	Network connectivity
LAN channel 1	eth0	Front panel Srv 5
LAN channel 2	eth1	Internal server port 4 \rightarrow switch port 16 *

* The BMC can then communicate through SFP ports Sw 1 to 12, depending on switch configuration.

Pass-through IO module BMC LAN channels

In an ME1210 platform with a pass-through IO module, the BMC is accessible via two network connections. Depending on the configuration interface used, the names for the network connections change.

IPMI and UEFI/BIOS	Redfish and Web UI	Network connectivity
LAN channel 1	eth0	Front panel Srv 5
LAN channel 2	eth1	Front panel Srv 4

Configuring IPMI over LAN

Disabling IOL on a LAN channel

```
      Step_1
      Disable the LAN access.
      [root@localhost ~]# =

      LocalServer_OSPrompt:~# ipmitool lan set [LAN_CHANNEL]
      Set Channel Access for

      access off
      Image: Set Channel Access for
```

root@localhost ~]# ipmitool lan set 1 access off et Channel Access for channel 1 was successful.

Enabling IOL on a LAN channel

 Step_1
 Enable the LAN access.

 LocalServer_OSPrompt:~# ipmitool lan set [LAN_CHANNEL] access on

[root@localhost ~]# ipmitool lan set 1 access on Set Channel Access for channel 1 was successful.

Configuring Serial over LAN parameters

Viewing and configuring SOL parameters

Step_1	Display SOL parameters. LocalServer_OSPrompt:~# ipmitool sol info	<pre>\$ ipmitool sol info Set in progress : true Groce Encryption : false Force Authentication : false Privilage Level : ADMINISTRATOR Character Accumulate Level (ms) : 60 Character Send Threshold : 96 Retry Count : 7 Retry Interval (ms) : 500 Volatile Bit Aate (kbps) : 115.2 Non-Volatile Bit Kate (kbps) : 115.2 Payload Channel : 1 (Ost) Payload Port : 623</pre>
Step_2	Display SOL parameters available for configuration. LocalServer_OSPrompt:~# ipmitool sol set	<pre>\$ ipmitool sol set SOL set parameters and values: set-in-progress set-complete set-in-progress commit-write enabled force-enabledic cation true false force-enabledic cation true false privilege-level user operator admin oem character-accoundate-level <in 5="" increments="" ms=""> character-sed-thresbold N retry-rount N non-valatilebit-irate serial 9.6 19.2 38.4 57.6 115.2 volatile-bit-rate</in></pre>
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

Configuring date and time

- <u>Configuring BMC date and time</u>
- <u>Configuring switch NOS date and time</u>

Configuring BMC date and time

Table of contents

- <u>General information on platform date and time</u>
- Configuring the BMC date and time
 - <u>Configuring the BMC date and time using the Web UI</u>
 - Manually configuring the BMC date and time using the Web UI
 - Configuring the BMC date and time based on the NTP using the Web UI
 - <u>Configuring the BMC date and time using Redfish</u>
 - <u>Manually configuring the BMC date and time using Redfish</u>
 - <u>Configuring the BMC date and time based on the NTP using Redfish</u>
 - Configuring the BMC date and time using IPMI
 - Manually configuring the BMC date and time using IPMI

General information on platform date and time

The date and time need to be set for both the BMC and the switch NOS. This information will be used by the system event logging when recording events. The UEFI/BIOS automatically obtains the date and time from the BMC during boot.

Configuring the BMC date and time

The BMC date and time can be set using:

- The BMC Web UI
- Redfish
- IPMI

Configuring the BMC date and time using the Web UI

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

Manually configuring the BMC date and time using the Web UI

Step_1	From the left-side menu, select Settings and then Date and time .	🚱 kontron 🛛 🔗 Health 🔮 Power 💲 Refresh 🛞 admin-
		Cverview Overview
		Hardware status V BMC time Server LED Operations 2021-11-20 163558 UTC
		We settings A Date and time BMC information Power restore policy BMC information Security and access Security and access
Step_2	Select Manual and configure the date and time.	Date and time
Step_3	Click on the Save settings button.	To change how date and time are displayed (either UTC or browser offset) throughout the application, visit Profile Settings
		- 24-hour time 2021-12-22 20:10:21 UTC
		Configure settings
		Date 24-hour time (UTC) YYYY-MM-DD HHEMM 2021-12-22 20:10
		NTP Server 2 Server 3 10.2.20.1 pool.ntp.org
		Save settings

Configuring the BMC date and time based on the NTP using the Web UI

Step_1	From the left-side menu, select Settings and then Date and time .	Image: Security and access Image: Security and access <td< th=""></td<>
Step_2	Select NTP.	Date and time
Step_3	Enter one or multiple NTP server addresses.	To change how date and time are displayed (either UTC or however, offer) throughout the anolication with throfile dations
Step_4	Click on the Save settings button.	Date 24-hour time 2021-12-22 20:10:21 UTC Configure settings Manual De 24-hour time (UTC) YYYY-MM-DD HetMM 2021-12-22 20:10 2021 20:10 Server 1 Server 2 10:220.1 pool.ntp.org Server settings
Step_5	A success message should appear upon successful configuration.	Image: Non-training line Date 24-hour to Health M Image: Non-training line Image: Non-training line Image: Non-training line Image: NP Server 1 Server 2 10.2.20.1 Image: Non-training line Save settings

Configuring the BMC date and time using Redfish

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

Manually configuring the BMC date and time using Redfish

Step_1	If NTP is enabled, disable it. RemoteComputer_OSPrompt:~\$ curl -k -srequest PATCHurl [ROOT_URL]/redfish/v1/ Managers/bmc /NetworkProtocolheader 'Content-Type: application/json'data '"{"NTP": {"ProtocolEnabled": false}}"' jq	
	<pre>\$ curl -k -srequest PATCHurl https://admin:ready2go@172.16.182.31/redfish/v1/Manager s/bmc/NetworkProtocolheader 'Content-Type: application/json'data '"{"NTP": {"Protoco lEnabled": false}}"' jq</pre>	
Step_2	Set the date and time manually using the following command. RemoteComputer_OSPrompt:~\$ curl -k -srequest PATCHurl [ROOT_URL]/redfish/v1/ Managers/bmcheader 'Content-Type: application/json'data '"{"DateTime": "[DATE_TIME]"}"' jq	
	<pre>\$ curl -k -srequest PATCHurl https://admin:ready2go@172.16.182.31/redfish/v1/Manager s/bmcheader 'Content-Type: application/json'data '"{"DateTime": "2021-12-21T18:36:59 +00:00"}"' jq { "DateTime": "2021-12-21T18:36:59+00:00" }</pre>	
Step_3	Verify BMC current date and time. RemoteComputer_OSPrompt:~\$ curl -k -srequest GETurl [ROOT_URL]/redfish/v1/ Managers/bmc jq .DateTime	
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc jq .DateTime { "DateTime": "2021-12-21T18:39:59+00:00", } }</pre>	

Configuring the BMC date and time based on the NTP using Redfish

Step_1	Add the NTP server(s) and enable the protocol. RemoteComputer_OSPrompt:~\$ curl -k -srequest PATCHurl [ROOT_URL]/redfish/v1/ Managers/bmc/NetworkProtocolheader 'Content-Type: application/json'data '"{"NTP": {"NTPServers": [[NTP_SERVERS]],"ProtocolEnabled": true}]"' jq
	<pre>\$ curl -k -srequest PATCHurl https://admin:ready2go@172.16.182.31/redfish/v1/Manager s/bmc/NetworkProtocolheader 'Content-Type: application/json'data '"{"NTPP": {"NTPServ ers": ["pool.ntp.org", "10.2.20.1"],"ProtocolEnabled": true}}" jq</pre>
Step_2	Verify BMC current date and time. RemoteComputer_OSPrompt:~\$ curl -k -srequest GETurl [ROOT_URL]/redfish/v1/ Managers/bmc jq .DateTime
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc jq .DateTime { "DateTime": "2021-12-21T18:39:59+00:00", }</pre>

Configuring the BMC date and time using IPMI

It is only possible to set time manually using IPMI.

Manually configuring the BMC date and time using IPMI

The following procedures will be executed using the Accessing a BMC using IPMI (KCS) method, but some configurations can also be performed using IOL (Accessing a BMC using IPMI over LAN (IOL)). To use IOL, add the IOL parameters to the command: -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -C 17.

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

Known limitation

Problem

When setting the system event log time with $ipmitool$, multiple repeated	ipmitool sel list. - 1 11/14/2018 17:07:10 Event Logging Disabled #0x07 Log area reset/cleared Asserted
System Event entries will be present in the SEL list.	2 11/14/2018 17:07:13 System Event #0x08 Timestamp Clock Sync Asserted 3 11/14/2018 17:06:57 System Event #0x08 Timestamp Clock Sync Asserted
	4 11/14/2018 17:00:38 System Event #0x08 Timestamp Clock Sync Asserted 5 11/14/2018 17:06:57 System Event #0x08 Timestamp Clock Sync Asserted

Solution

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.

Refer to the following procedure to get the latest unreleased version. NOTE: Some commands may vary depending on the operating system.

Step_1	Download the latest version from its repository. LocalServer_OSPrompt:~# git clone <u>https://github.com/ipmitool/ipmitool.git</u>
Step_2	Once the files have been downloaded, change the directory to the ipmitool directory. LocalServer_OSPrompt:~# cd ipmitool
Step_3	Install ipmitool on the platform (or the remote computer). LocalServer_OSPrompt:~# . /bootstrap && ./configure && make && make install
Step_4	After the installation of ipmitool , set the "-N 5" flag using ipmitool sel set time. This flag sets the command timeout to prevent multiple duplicated entry errors to be logged. LocalServer_OSPrompt:~# ipmitool sel time set "[MM/DD/YYYY HH:MM:SS]" -N 5

Configuring switch NOS date and time

Table of contents

- <u>Configuring the switch NOS date and time using the Web UI</u>
 - Configuring the switch NOS date and time based on the NTP using the Web UI
 - Manually configuring the switch NOS time zone using the Web UI
- <u>Configuring the switch NOS date and time using the CLI</u>
 - <u>Configuring the switch NOS date and time based on the NTP using the CLI</u>
 - Manually configuring the switch NOS time zone using the CLI
 - Manually configuring the switch NOS date and time using the CLI



Changes to the switch configuration are not persistent after rebooting the switch.

To preserve configurations, the current configuration needs to be saved to startup-config. From the switch Web UI:

- Select Maintenance, Configuration and then Save startup-config. Click on Save Configuration to confirm the change. From the switch CLI:
- LocalSwitchNOS_OSPrompt:~(config-if)# end
- LocalSwitchNOS_OSPrompt:~# copy running-config startup-config

The switch NOS date and time can be set using:

- The switch NOS Web UI
- The switch NOS CLI

Configuring the switch NOS date and time using the Web UI

There are three options to proceed:

- Using the NTP recommended practice (if no NTP server is present on the network, the customer's OS on the integrated server could act as an NTP server)
- Manual configuration (time zone only)
- Using the PTP for information on using PTP as source for date and time, refer to Configuring synchronization.



Only the time zone can be manually set from the switch Web UI. It is not possible to manually configure the date and time from the Web UI.

Configuring the switch NOS date and time based on the NTP using the Web UI

Access the switch NOS Web UI. Refer to <u>Accessing the switch NOS using the switch NOS Web UI</u> for access instructions. To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the Web</u> <u>UI</u>.

Step_1	From the left-side menu, select ${\bf Configuration,System,}$ and then ${\bf NTP}$.	🚱 kontron	a 🗗 🛛
Step_2	Enable the NTP service by changing the value from the Mode dropdown menu to Enabled .	Configuration System Formation Formation	
Step_3	Enter the NTP server's address or hostname. NOTE: To enter a server hostname, a DNS service must be configured.	kontron Configuration System NTP Configuration	A 🗗 0
Step_4	Repeat the previous step to add multiple NTP servers if needed.	Information Informat	
Step_5	Click on the Save button.	• Configuration • System • Information • Information • Information • Information • Information • Information • Orgen • Configuration • Information • Orgen • Configuration •	A 🗗 🖌
Step_6	(Optional) To make the change persistent, save running-config to startup-config.		

Manually configuring the switch NOS time zone using the Web UI

Access the switch NOS Web UI. Refer to <u>Accessing the switch NOS using the switch NOS Web UI</u> for access instructions. To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the Web</u> <u>UI</u>.

Step_1	From the left-side menu, select Configuration, System and then Time .	• Configuration • system • orget • Orders Ethernet • Orders Eth
Step_2	Configure the time zone by selecting it from the Time Zone dropdown menu.	Time Zone Configuration Time Zone Configuration Time Zone [(UTC-06:00) Central Time (US and Canada) V Hours -6 V Minutes 0 V Acronym (0 - 16 characters)
Step_3	Configure the Daylight Saving Time .	Daylight Saving Time Mode Daylight Saving Time (Recurring v) Start Time settings Week Day Sun v Month Mar v Hours 2 v Minutes 0 v Day Sun v Month Mar v Hours 2 v Minutes 0 v Bay Sun v Month Nov v Hours 2 v Offset 60 (1-1439) Minutes
Step_4	Click on Save .	Time Zone Configuration Time Zone (UTC-06.00) Central Time (US and Canada) Hours 0 • Acronym (0 - 16 characters) Daylight Saving Time Configuration Daylight Saving Time Configuration Start Time settings Minutes • Daylight Saving Time Disabled • Nonth 1 • Year 2014 • Minutes 0 • Month 1 • Year 2017 • Minutes 0 • Gifset 1 (1 - 1439) Minutes Save Reset
Step_5	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring the switch NOS date and time using the CLI

There are three options to proceed:

- Using the NTP recommended practice (if no NTP server is present on the network, the customer's OS on the integrated server could act as an NTP server)
- Manual configuration
 - Time zone
 - Date and time (the configuration will be lost if a reset occurs)
- Using the PTP for information on using PTP as a source for date and time, refer to Configuring synchronization

The time zone and the date and time can be **manually set from the switch** CLI . However, when a date and a time are configured manually, **the configuration will be lost if a reset occurs** .
Configuring the switch NOS date and time based on the NTP using the CLI

Access the switch NOS CLI using one of the SSH methods described in section <u>Accessing the switch NOS</u>. To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the CLI</u>.

Step_1	Enter configuration mode. LocalSwitchNOS_OSPrompt:~# configure terminal	# configure terminal
Step_2	Enable the NTP. LocalSwitchNOS_OSPrompt:~(config)# ntp NOTE: To disable NTP, use no ntp .	(config)# ntp
Step_3	Configure the NTP server. LocalSwitchNOS_OSPrompt:~(config) # ntp server [SERVER_ID] ip- address [IP_ADDRESS_OR_HOSTNAME] NOTE: To enter a server hostname, a DNS service must be configured.	<pre>(config)# ntp server 1 ip-address 132.163.96.5 <u>OR</u> (config)# ntp server 1 ip-address pool.ntp.org</pre>
Step_4	Exit configuration mode. LocalSwitchNOS_OSPrompt:~(config)# exit	(config)# exit
Step_5	Verify the NTP configuration by displaying the list of NTP servers. LocalSwitchNOS_OSPrompt:~ # show ntp status	<pre># show ntp status NTP Mode : enabled Idx Server IP host address (a.b.c.d) or a host name string</pre>
Step_6	(Optional) To make the change persistent, save running-config to startup-config.	

Manually configuring the switch NOS time zone using the CLI

Access the switch NOS CLI using one of the SSH methods described in section <u>Accessing the switch NOS</u>. To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the CLI</u>.

Step_1	Enter configuration mode. LocalSwitchNOS_OSPrompt:~# configure terminal
	# configure terminal
Step_2	Manually set the hour and minute offsets. LocalSwitchNOS_OSPrompt:~(config)# clock timezone [TIME_ZONE_ACRONYM] [HOUR_OFFSET] [MINUTE_OFFSET]
	(config)# clock timezone CST -6 0
Step_3	Configure the daylight saving time. LocalSwitchNOS_OSPrompt:~(config)# clock summer-time [TIME_ZONE_ACRONYM] date [STARTING_MONTH] [STARTING_DAY] [STARTING_YEAR] [STARTING_HH:MM] [ENDING_MONTH] [ENDING_DAY] [ENDING_YEAR] [ENDING_HH:MM] [OFFSET] NOTE: This command sets the parameters for one year only. They will have to be reprogrammed the following year. or LocalSwitchNOS_OSPrompt:~(config)# clock summer-time [TIME_ZONE_ACRONYM] recurring [STARTING_WEEK] [STARTING_MONTH] [STARTING_DAY 1=Sunday] [STARTING_HH:MM] [ENDING_WEEK] [ENDING_MONTH] [ENDING_DAY] [ENDING_HH:MM] [MINUTE_OFFSET] NOTE: This command sets the parameters for every year. No reprogramming needed.
	clock summer-time CDT recurring 2 1 3 2:00 1 1 11 2:00 60
Step_4	Verify the time zone configuration. LocalSwitchNOS_OSPrompt:~(config)# exit LocalSwitchNOS_OSPrompt:~# show clock detail
	<pre>(config)# exit # show clock detail System Time : 1969-12-31T19:02:43-06:00 Timezone : Timezone Offset : -3600 (-360 minutes) Timezone Acronym : CST Daylight Saving Time Mode : Recurring. Daylight Saving Time Start Time Settings : * Week: 2 * Day: 1 * Month: 3 Date: 0 Year: 0 * Hour: 2 * Minute: 0 Daylight Saving Time End Time Settings : * Week: 1 * Day: 1 * Month: 11 Date: 0 Year: 0 * Hour: 2 * Minute: 6 Daylight Saving Time Offset : 60 (minutes)</pre>
Step_5	(Optional) To make the change persistent, save running-config to startup-config.

Manually configuring the switch NOS date and time using the CLI



The the date and time can be **manually set from the switch CLI**. However, when a date and a time are configured manually, **the configuration will be lost if a reset occurs**.

Access the switch NOS CLI using one of the SSH methods described in section <u>Accessing the switch NOS</u>. To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the CLI</u>.

Step_1	Enter debug mode. LocalSwitchNOS_OSPrompt:~# platform debug allow
	# platform debug allow
Step_2	Manually set the date and time. LocalSwitchNOS_OSPrompt:~(config)# debug time set [DATE] [TIME] Where: • [DATE] = yyyy/mm/dd, yyyy=1970-2037, mm=1-12, dd=1-31 • [TIME] = HH:mm:ss, HH=0-23, mm=0-59, ss=0-59
	# debug time set 2022/01/03 12:34:56
Step_3	Get current date and time. LocalSwitchNOS_OSPrompt:~(config)# debug time get
	2022-02-09T14:04:30-05:00
Step_4	(Optional) To make the change persistent, save running-config to startup-config.

Configuring networking

- Configuring the BMC networking
- <u>Configuring UEFI network boot</u>
- <u>Configuring switch NOS networking</u>

Configuring the BMC networking

Table of contents

- <u>Selecting an access method for BMC networking configuration</u>
- BMC network architecture
 - Ethernet switch IO module option
 - Pass-through IO module option
- Enabling or disabling a BMC network interface
 - Enabling or disabling a BMC network interface using Redfish
 - Enabling or disabling a BMC network interface using BMC Web UL
 - Enabling or disabling a BMC network interface using IPMI
- <u>Configuring a static IP address</u>
 - Configuring a static IP address using Redfish
 - <u>Configuring a static IP address using the BMC Web UI</u>
 - <u>Configuring a static IP address using the UEFI/BIOS setup menu</u>
 - Accessing the BMC network configuration menu
 - <u>Configuring a static IP address using the UEFI/BIOS setup menu</u>
 - <u>Configuring a static IP address using IPMI</u>
 - <u>Configuring a static IP address</u>
- <u>Configuring a dynamic IP address using DHCP</u>
 - <u>Configuring a dynamic IP address using Redfish</u>
 - <u>Configuring a dynamic IP address using the BMC Web UI</u>
 - <u>Configuring a dynamic IP address</u>
 - Configuring a dynamic IP address using the UEFI/BIOS setup menu
 - Accessing the BMC network configuration menu
 - <u>Configuring a dynamic IP address using DHCP</u>
 - <u>Configuring a dynamic IP address using IPMI</u>
- <u>Configuring a VLAN for a BMC network interface</u>
 - <u>Assigning a VLAN</u>
 - Assigning a VLAN using Redfish
 - Assigning a VLAN using the BMC Web UI
 - <u>Assigning a VLAN using IPMI</u>
 - <u>Removing a VLAN</u>
 - <u>Removing a VLAN using Redfish</u>
 - Removing a VLAN using the BMC Web UI
 - <u>Removing a VLAN using IPMI</u>

To configure the BMC networking IP address, a schema must be selected and configured:

- A static IP address
- A dynamic IP address using DHCP

By default, the IP addresses of the network interfaces of the BMC are obtained through the DHCP protocol.

NOTE: The procedures described below must be performed for one interface at a time. If the application requires multiple interfaces, configure them separately.

Relevant sections:

- <u>Discovering platform IP addresses</u>
- <u>Product architecture</u>

Selecting an access method for BMC networking configuration

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 UEFI/BIOS setup menu. Refer to <u>Accessing the UEFI/BIOS using a serial console (physical connection)</u> for access instructions.
 If the BMC IP address is unknown and an OS is installed :
 - Use IPMI via KCS. Refer to Accessing a BMC using IPMI via KCS for access instructions.
 - Use the UEFI/ BIOS setup menu. Refer to Accessing the UEFI/BIOS using a serial console (physical connection) for access instructions.
- If the BMC IP address is known and an OS is installed :
 - Use Redfish. Refer to <u>Accessing a BMC using Redfish</u> for access instructions.
 - Use the Web UI. Refer to Accessing a BMC using the Web UI for access instructions.
 - Use IPMI (via KCS or IOL). Refer to <u>Accessing a BMC using IPMI over LAN (IOL)</u> or <u>Accessing a BMC using IPMI via KCS</u> for access in instructions.
 - Use the UEFI/ BIOS setup menu. Refer to <u>Accessing the UEFI or BIOS</u> for access instructions.

BMC network architecture

Ethernet switch IO module option



In an ME1210 platform with an Ethernet switch IO module, the BMC is accessible via two network connections. Depending on the configuration interface used, the names for the network connections change.

IPMI and UEFI/BIOS	Redfish and Web UI	Network connectivity
LAN channel 1	eth0	Front panel Srv 5
LAN channel 2	eth1	Internal server port 4 \rightarrow switch port 16 *

* The BMC can then communicate through SFP ports Sw 1 to 12, depending on switch configuration.

Pass-through IO module option



In an ME1210 platform with a pass-through IO module, the BMC is accessible via two network connections. Depending on the configuration interface used, the names for the network connections change.

IPMI and UEFI/BIOS	Redfish and Web UI	Network connectivity
LAN channel 1	eth0	Front panel Srv 5
LAN channel 2	eth1	Front panel Srv 4

Enabling or disabling a BMC network interface

This can be achieved:

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

Enabling or disabling a BMC network interface using Redfish

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

Step_1	List the BMC network interfaces and take note of the URL of the interface to be enabled or disabled. RemoteComputer_OSPrompt:~# curl -k -srequest GET url [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces/ jq
	<pre>\$ curl -k -srequest GBTurl https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/Et hernetInterfaces jq { "@odata.id": "/redfish/v1/Managers/bmc/EthernetInterfaces", "@odata.itppe": "#EthernetInterfaceCollection.EthernetInterfaceCollection", "Description": "Collection of EthernetInterfaces for this Manager", "Members": [{</pre>
Step_2	Set the InterfaceEnabled attribute to true to enable the network interface or set it to false to disable the network interface. RemoteComputer_OSPrompt:~# curl -k -srequest PATCHurl [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces/[INTERFACE_NAME]header 'Content-Type: application/json'data '{"InterfaceEnabled":[VALUE]}' jq
	<pre>\$ curl -k -srequest PATCHurl https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/ EthernetInterfaces/eth1header 'Content-Type:application/json'data '{"InterfaceEnabled": tr ue}' jq</pre>

Enabling or disabling a BMC network interface using BMC Web UI

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

Step_1	From the left-side menu of the BMC Web UI, select Settings and then Network .	🚱 konttron 📀 Health 💿 Power 🖓 Refresh 🛞 admin •		
		Cverview Coverview Coverview Audware status Server(LD)		
		Contractions ✓ 2021-11-20 feasses UTC ● Diff Settings Edit network settings → SOL concole Date and time BMC information Server information Power restore policy Firmware version Model Manufacturer 2200/05/666 IPRODUCT_VAMEE Konton		
		Senial number UER version 9017064072 1.02.09579455		
Step_2	From the dropdown menu of the Interface section, select a network interface to configure.	Network Configure network settings for the BMC Interface		
Step_3	Click on the NIC enable button to enable or disable the network interface.			
Step_4	Click on Save settings .	eth1 \Rightarrow NIC enable		
		Save settings		

Enabling or disabling a BMC network interface using IPMI

Step_1	Enable or disable the BMC network interface. LocalServer_OSPrompt:~# ipmitool lan set [LAN_CHANNEL] access [VALUE] Where [VALUE] can be on or off.	[root@localhost ~]# ipmitool lan set 1 access on Set Channel Access for channel 1 was successful.
--------	-------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------

Configuring a static IP address

This can be achieved :

Using <u>Redfish</u>

- Using the <u>BMC Web UI</u>
- Using the <u>UEFI/BIOS setup menu</u>
- Using <u>IPMI</u>

If a VLAN needs to be configured, refer to <u>Configuring VLAN for a BMC network interface</u>.

Configuring a static IP address using Redfish

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

Step_1	To change a static IP address using Redfish, the IPv4StaticAddresses object of a network interface needs to be modified:
	RemoteComputer_OSPrompt:~# curl -k -srequest PATCHurl [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces/[INTERFACE_NAME]header 'Content-Type: application/json'data '{"IPv4StaticAddresses": [{"Address": "[IP_ADDRESS]","SubnetMask": "[MASK]","Gateway": " [GATEWAY]"}]}' jq
	<pre>\$ curl -k -srequest PATCHurl https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/ EthernetInterfaces/eth1header 'Content-Type:application/json'data '{"IPv4StaticAddresses": [{"Address": "172.16.182.32", "SubnetMask": "255.255.0.0", "Gateway": "172.16.0.1"}]}' jq</pre>

Configuring a static IP address using the BMC Web UI

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

Step_1	From the left-side menu of the BMC Web UI, select Settings and then Network .	Example Overview Image: Cogs Image: Cogs Image: Cogs Image: Cogs <th> ♦ Health Overview EMC time 2021-11-20 163558 UTC Edit network settings → BMC information Firmwark settion 200015976c6 </th> <th>Server LED Ciff Sol: console Server information Model Manufactu [PRODUCT_NAME] Kontoo Serial number UEI versio Serial number UEI versio Serial number UEI versio</th> <th>⊗ admin = → πε 9455</th>	 ♦ Health Overview EMC time 2021-11-20 163558 UTC Edit network settings → BMC information Firmwark settion 200015976c6 	Server LED Ciff Sol: console Server information Model Manufactu [PRODUCT_NAME] Kontoo Serial number UEI versio Serial number UEI versio Serial number UEI versio	⊗ admin = → πε 9455
Step_2	Select the network interface to configure from the dropdown menu.	Interface Network interface eth0 eth1 System	↓ ◆	NIC enable On	
Step_3	From the IPV4 section, select Static .	IPV4 IPV4 configuration DHCP Static Static			
Step_4	From the Static section, configure the desired IP address and Subnet mask .	Static IP address 172.16.33.88	Subnet mask 255.255.00		
Step_5	From the System section, configure the Default gateway.	System Default gateway 172.16.0.1			
Step_6	Click on Save settings.	Static			
		IP address	Subnet ma	sk	
		172.16.33.88	255.255.0	.0	
		⊕ Add static IP Static DNS			
		IP address			
		 Add DNS serv Save settings 	ver		

Configuring a static IP address using the UEFI/BIOS setup menu

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

Accessing the BMC network configuration menu

Sten 1	From the UEEL/BIOS menu, navigate to tab Server Memt	Aptio Setup Utility	7 - Copyright (C) 2019 Am	erican Megatrends, Inc.
2106-1		BIOS Information BIOS Vendor Core Version Compliancy Project Version Build Date and Time Access Level	American Megatrends 5.14 UEFI 2.6; PI 1.4 06/26/2019 09:12:28 Administrator	Chooge the system default language
		FFGA Version Hemory Information Total Hemory System Date System Date System Time Version 2,20,1271	2.02.0800AD12 32768 HB (English) (Ued 07/10/2019) (13:47:54) Copyright (C) 2019 Amer	<pre>>>: Select Screen 'v: Select Icm Enter: Select !/: Change Opt. !/: General Help !7: Previous Values !7: Optimied Defaults !F3: optimied Defaults !F4: Save 4 Exit !ESC: Exit ! Exam Megattends, Inc. AB</pre>
Step_2	Select BMC network configuration .	Aprio Setup Utili: Rain Advanced Intel DHC Interface(s) Wait For BHC FRB-2 Timer Dimer FRB-2 Timer Diloy OS Watchdog Timer OS Watchdog Timer Setting DHC Warn Setting DHC Warn Reset Version 2.20.1271	<pre>- Copyright (C) 2019 Am KCSetup Server Mymt Sec KCS, USB [Disabled] [Fambled] [Fower Cycle] [Disabled] [10 minutes] [Reset] [Reset] [Fambled] [Disabled] [Disabled] [Copyright (C) 2019 Amer</pre>	erican Megatrends, Inc. writy Bool Event Logs ^/Press <enter> to enable +lor disable Serial Mux +configuration. +l ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;</enter>
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 Vilit SMC network configure SMC network configure Configure IPV4 support 	<pre>> Copyright (C) 2019 Am Server Mynt Server Mynt tion [Unspecified] DynamicAddressBmcDhep 172.16.205.245 255.255.0.0 00-AD-X5-D6-33-2A 172.16.0.1 00-05-64-2F-10-SF Copyright (C) 2019 Amer</pre>	rican Megattends, Inc. 'Select to configure LN 'Iselect to configure LN 'Ishanet parameters I statically or I dynamically (by BIOS or I BPC). Unapecified + option will not modify + any BNC network + parameters during BIOS + +

Configuring a static IP address using the UEFI/BIOS setup menu

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).	-BBC network configuration- -BBC network configuration- (channel parameters) (channel parameters) (channel parameters) (channel parameters) (channel parameters) (configuration Address [Unspecified] (configuration Address [Unspecified] (current Configuration DynamicAddressBmcDhep (datess Source Station IP address 172.16.205.245 Station IP address 172.16.01 Station IA address (configuration) Station IA address (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (configuration) (con			
Step_2	Select Static .	/ Configuration Address source\ Unspecified <mark>Static</mark> DynamicBmcDhcp DynamicBmcNonDhcp \/			
Step_3	Change the Station IP address . NOTE : This is the BMC IP address (BMC MNGMT_IP).	Lan channel 1 Configuration Address [Static] source /Station IP address			
Step_4	Change the Subnet mask .	Lan channel 1 Configuration Address [Static] source /Subnet mask Station IP address 1 Station MAC address 00- Router IP address 0.0.0.0 Router MAC address 00-00-00-00-00			
Step_5	Change the Router IP address .	Lan channel 1 Configuration Address [Static] Source (Router IP address			
Step_6	Confirm the configuration has changed and exit BMC network configuration using the ESC key.	Lan channel 1 Configuration Address [Static] source Station IP address 172.16.205.245 Subnet mack 255.255.0.0 Station MAC address 00-A0-A5-D6-33-2A Router IP address 172.16.0.1 Router MAC address 00-05-64-2F-10-5F			

Configuring a static IP address using IPMI

The following procedures will be executed using the <u>Accessing a BMC using IPMI via KCS</u> 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] -C 17.

Configuring a static IP address

Step_1	Set the IP source to static. LocalServer_OSPrompt:~# ipmitool lan set [LAN_CHANNE	EL] 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.	<pre>[root@localhost ~]# ipmitool lan set 1 ipaddr 172.16.205.245 Setting LAN IP &ddress to 172.16.205.245</pre>
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.	[root@localhost ~]# ipmitool lan set 1 defgw 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]	[rootBlocalhost -]# ipmitool lan set 1 defgw macaddress 00:05:64:2f:10:5f Setting LAN befault Gateway KAC to 00:05:64:2f:10:5f
Step_6	Verify that the configuration has changed. LocalServer_OSPrompt:~# ipmitool lan print [LAN_CHANNEL]	<pre>[root@localhost ~]# ipmitool lan print 1 Set in Progress : Set Complete Auth Type Support : NOWE PASSWORD Auth Type Enable : Callback :</pre>

Configuring a dynamic IP address using DHCP

This can be achieved:

- Using <u>Redfish</u>
- Using the <u>BMC Web UI</u>
- Using the <u>UEFI/BIOS setup menu</u>
- Using IPMI

NOTE: If a VLAN needs to be configured, refer to Configuring VLAN for a BMC network interface.

Configuring a dynamic IP address using Redfish

Refer to Accessing a BMC using Redfish for access instructions.



Configuring a dynamic IP address using the BMC Web UI

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

Configuring a dynamic IP address

Step_1	From the left-side menu of the BMC Web UI, select Settings and then Network .	Image: Security and access Image: Security and access
Step_2	Select the network interface to configure from the dropdown menu.	Interface Network interface NIC enable C On eth0 eth1 System
Step_3	From the IPV4 section, select DHCP.	IPV4
Step_4	Click on Save settings.	PP4 configuration PLCP Static DHCP

Configuring a dynamic IP address using the UEFI/BIOS setup menu

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

Accessing the BMC network configuration menu

Step 1	From the LIFFL/BIOS menu navigate to tab Server Mgmt	Aptio Setup Utility - Copyright (C) 2019 American Hegatrends, Inc.
Step_1		Bits Anterioration Ichose the system Bits Information Ichose the system Bits Vendor American Megatrends Compliancy UEFI2.6; PI1.4 Project Version 60/26/2019 09:12:28 Access Level Administrator Excl. Version 2.02.0000032
		Memory Information >>: Select Screen Total Memory 32768 MB Total Memory 32768 MB System Language [English] System Date [Wed 07/10/2019] System Time [13:47:54] Last [Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.
Step_2	Select BMC network configuration .	Aptio Setup Ucility - Copyright (C) 2019 American Megatrends, Inc. Rain Advanced IntelRCSetup Server Runt Security Book Event Logs BRC Interface(s) CC3, USB 'Press CEnter> Press CEnter> to adhed Security Book Event Logs BRC Interface(s) CC3, USB 'Press CEnter> to adhed Security Book Event Logs Wait For BRC [Disabled] +lor disable Security How Event Logs FRB-2 Timer [Enabled] +lor disable Security Event Logs FRB-2 Timer time voltey [Power Cycle] +lor disable Security Event Logs OS Watchdog Timer [Disabled] +lor disable Security Event Logs OS Wat Timer Timeout [Disabled] +lor disable Security Event Log S Watchdog Timer [Disabled] +lor disable Security Event Log S Watch Event Log +lor disable Security Event Log > Wate Reset +fr: Operions Values BMC Warm Reset +fr: Security Found Event Log > MC Warm Reset +fr: Security Found Version 2.30.1271. Copyright (C) 2019 American Megatrends, Inc.
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 Vility - Copyright (C) 2019 American Megatrends, Inc. Server Mgnt BMC network configuration- BMC network configuration- Configure IPV4 support

Configuring a dynamic IP address using DHCP

Step_1	From the BMC network configuration menu, select the Configuration Address source option of the LAN interface to configure (LAN channel 1 in this example).	Aptio Secup Utility - Copyright (C) 2019 American Megatrends, Inc. Berver Ngmt BRC network configuration
Step_2	Select DynamicBmcDhcp.	/ Configuration Address source> Unspecified Static DynamicBmcDhep DynamicBmcNonDhep >/
Step_3	Navigate to Save & Exit .	Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Save 4 Ex10 Save A Ex10 Save Changes and Reset Jiscard Changes and Reset H Save Changes Discard Changes H Discard Changes H Discard Changes H Save as User Defaults H Restore User Defaults H AMIFUNDate AMIFUNDate AMI Virtual CDROM 1.00 H Virtual CDROM 1.00 Virtual CDROM 1.00 H Virtual CDROM 1.00 Virtual CDRO
Step_4	Select Save Changes and Exit . This will perform a server reset.	Aptro Setup Utility - Copyright (C) 2019 American Megatrends, inc. Save 6 Exit Save Options Save Continges and Exit Discard Changes and Exit Save Changes and Exit Save Changes and Exit Discard Changes Default Options Restore Defaults Vec No Sale Change Default Options Restore Defaults + [F1: Pervious Viulues + [F2: Pervious Viulues + [F2: Pervious Viulues AMIFRUpdate AMI Virtual CORONO 1.00 Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.
Step_5	When the UEFI/ BIOS sign on screen is displayed, press the spec	cified key to enter the UEFI/ BIOS setup menu. Then, access the Server

Configuring a dynamic IP address using IPMI

The following procedures will be executed using the <u>Accessing a BMC using IPMI via KCS</u> 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] -C 17.

Mgmt menu and select BMC network configuration . The address displayed is your BMC IP address (BMC MNGMT_IP).

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).	<pre>[root8localhost ~]# ip Set in Progress Auch Type Support Auth Type Enable IP Address Source IP Address Subnet Nack MAC Address SNDP Community String IP Reader BMC APC Control Oratituous ARP Intrv1 Default Gateway IP Default Gateway IP Backup Gateway IP Backup Gateway IP Backup Gateway IP Backup Gateway IP Backup Gateway IP S02.14 VLAN Priority RNCP+ Cipher Suites Cipher Suite Priv Max Backup Gateway MAC 802.14 VLAN Priority RNCP+ Cipher Suites Cipher Suite Priv Max</pre>	<pre>mitool lan print 1 : Set Complete : NOWE PASSWORD : Callback : User :: NOWE PASSWORD : Operator : PASSWORD : Operator : PASSWORD : OTM : : Operator : PASSWORD : OTM : : Callback : : Operator : PASSWORD : Oth : : Operator : PASSWORD : Oth : : Operator : PASSWORD : Operator : Operator : PASSWORD : Operator : Operat</pre>	

Configuring a VLAN for a BMC network interface

i

Given the ME1210 architecture, if a VLAN is assigned to the **eth1** BMC network interface, the 1/16 switch port should reflect the configuration. Ensure that the 1/16 port is a member of the assigned VLAN. Refer to Internal connections and Configuring switch VLANs

Assigning a VLAN

This can be achieved:

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

Assigning a VLAN using Redfish

Refer to Accessing a BMC using Redfish for access instructions.



Assigning a VLAN using the BMC Web UI

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

Step_1	From the left-side menu of the BMC Web UI, select Settings and then Network .	Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provides Image: Second provid
		Network BMC information Server information Power restore policy Femare version Model Manufacturer Security and access 200.0159fce6 IPRODUCT_NAME Kontron Sets in under 9017064072 1.02.095794555
Step_2	From the dropdown menu of the Interface section, select a network interface to configure.	Network Interface Network interface teh1 Save settings
Step_3	To assign a VLAN, check the box in the VLAN section and enter the VLAN ID to be affected to the network interface.	VLAN Vlan Id I
Step_4	Click on Save settings .	Static DNS IP address
		No items available • Add DNS server
		Save settings

Assigning a VLAN using IPMI

The following procedures will be executed using the <u>Accessing a BMC using IPMI via KCS</u> 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] -C 17.

Step_1	Associate a pre-configured VLAN to an interface. LocalServer_OSPrompt:~# ipmitool lan set [LAN_CHANNEL] vlan id [VLAN_ID]	<pre>\$ipmitool lan set 1 vla \$ipmitool lan print Set in Progress Auth Type Support Auth Type Enable IP Address Source IP Address Subnet Mask MAC Address Default Gateway IP Default Gateway MAC 802.1q VLAN ID RMCP+ Cipher Suites Subsection Sector Sector Sector Sector Sector Sector Sector Sector Sector S</pre>	an id 1000 : Set Complete : : Callback : : User : : Operator : : Admin : : OEM : : Static Address : 172.16.218.79 : 255.255.0.0 : 00:a0:a5:ca:bb:11 : 172.16.0.1 : 00:00:00:00:00:00 : 1000 : 3,17
		802.1q VLAN ID RMCP+ Cipher Suites Cipher Suite Priv Max Bad Password Threshold	: 1000 : 3,17 : Not Available : Not Available

Removing a VLAN

This can be achieved:

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

Removing a VLAN using Redfish

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

Step_1	Select a BMC network interface and take note of its URL. RemoteComputer_OSPrompt:~# curl -k -srequest GETurl [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces jq
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/vl/Managers/bmc/Et hernetInterfaces jq { "@odata.id": "/redfish/vl/Managers/bmc/EthernetInterfaces", "@odata.type": "#EthernetInterfaceCollection.EthernetInterfaceCollection", "@odata.type": "EthernetInterfaces for this Manager", "Members": [{ {</pre>
Step_2	List the VLANs of a selected BMC network interface and take note of desired VLAN's URL. RemoteComputer_OSPrompt:~# curl -k -srequest GETurl [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces /[INTERFACE_NAME]/VLANs jq
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/Et hernetInterfaces/eth1/VLANs jq {</pre>
Step_3	Access the VLAN information in order to collect its ID. RemoteComputer_OSPrompt:~# curl -k -srequest GETurl [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces/[INTERFACE_NAME]/VLANs/ [VLAN_URL] jq .VLANId
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/Et hernetInterfaces/eth1/VLANs/eth1_1 jq .VLANId [1]</pre>
Step_4	Delete the VLAN for the selected BMC network interface using the following command. RemoteComputer_OSPrompt:-# curl -k -srequest PATCHurl [ROOT_URL]/redfish/v1/Managers/bmc/EthernetInterfaces/[INTERFACE_NAME]/VLANs/ [VLAN_URL]header 'Content-Type: application/json'data '{"VLANEnable": false, "VLANId": [VLAN_ID] }' jq
	<pre>\$ curl -k -srequest PATCHurl https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/ EthernetInterfaces/eth1/VLANs/eth1_1header 'Content-Type:application/json'data '{"VLANEnab le": false,"VLANId": 1}' jq</pre>

Removing a VLAN using the BMC Web UI

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

Step_1	From the left-side menu of the BMC Web UI, select Settings and then Network .	Image: Security and access Very construction Image: Security and access <t< th=""></t<>
Step_2	From the dropdown menu of the Interface section, select a network interface to configure.	Network Interface Network interface eth1 Consistent of the BMC NIC enable Consistent of the BMC
Step_3	To remove a VLAN, uncheck the box in the VLAN section.	VLAN Vlan Id 1
Step_4	Click on Save settings .	Save settings

Removing a VLAN using IPMI

The following procedures will be executed using the <u>Accessing a BMC using IPMI via KCS</u> 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] -C 17.

Step_1	Set the VLAN ID associated with an interface to off. LocalServer_OSPrompt:~# ipmitool lan set [LAN_CHANNEL] vlan id off	<pre>\$ipmitool lan set 1 vla \$ipmitool lan print Set in Progress Auth Type Support Auth Type Enable IP Address Subnet Mask MAC Address Default Gateway IP Default Gateway MAC 802.1q VLAN ID RMCP+ Cipher Suites Cipher Suite Priv Max Bad Password Threshold</pre>	an id off : Set Complete : : Callback : : User : : Operator : : Admin : : OEM : : Static Address : 0.0.0.0 : 255.255.255.255 : 00:a0:a5:ca:bb:11 : 0.0.0.0 : 00:00:00:00:00:00 : Disabled : 3,17 : Not Available : Not Available
		Bad Password Threshold \$: Not Available

Configuring UEFI network boot

Table of contents

- <u>Configuring the network boot</u>
- <u>Configuring VLANs for UEFI network boot</u>
 - Configuring VLANs for UEFI network boot using the UEFI/BIOS menu
 - <u>Creating VLANs</u>

•

- -
- <u>Removing VLANs</u>

Configuring the network boot

IP addresses used for the network boot functionality must be configured. By default they are obtained via DHCP, but they can be configured as static IP addresses.

Configuring VLANs for UEFI network boot

On a platform with the Ethernet switch IO module, VLANs must be configured for any VLAN-tagged traffic coming from the server X722 10GbE interface.

Refer to Configuring the switch for procedures to configure VLANs with the switch network operating system.

The UEFI/BIOS setup menu provides options to create/configure/remove VLANs on each of the server's four X722 NIC 10GbE interfaces as well as on the I210 NIC 1GbE interface. Refer to <u>Product architecture</u> for information on network interfaces. However, the UEFI/BIOS setup menus to configure VLANs are available only when the UEFI network services are active (they are not available when the Compatibility Support Module (CSM) legacy support is activated).

Configuring VLANs for UEFI network boot using the UEFI/BIOS menu

Relevant sections:

- <u>Accessing the UEFI or BIOS</u>
- MAC addresses

Creating VLANs

Step_1	From the UEFI/BIOS setup menu, select the Advanced menu and select one VLAN Configuration (MAC:xxxxxxxxxxxxxx) section.	Aptio Setup – American Megatrends International, LLC. Main <mark>Advanced</mark> Platform Configuration Socket Configuration Server Mgmt ▶		
	Select Enter Configuration Menu . NOTE: The MAC address will be the MAC address of the X722 10GbE or 1210 1GbE interface to configure.	 ISCSI Configuration IISCSI Configuration (MAC:20092A8166C7) VAN Configuration (MAC:20092A8166C7) MAC:20092A8166C7-IPV4 Network Configuration MAC:20092A8166C7-IPV4 Network Configuration Intel(R) Ethernet Connection X722 for 106BASE-T - 00:A0:A5:09:CF:89 VAR Configuration MAC:0000ASD9CFE9V004-IPV4 Network Configuration MAC:0000ASD9CFE9V004-IPV6 Network Configuration Intel(R) Ethernet Connection X722 for 106BASE-T - 00:A0:A5:09:CF:E4 VAR Configuration (MAC:0000ASD9CFEA) VCR CONFIGURATION<		
Step_2	 Create a new VLAN as needed by setting its VLAN ID and Priority: VLAN ID: Value between 0 and 4094 Priority: Value between 0 and 7 The example in the image shows a VLAN with ID 1001 and a 802.1Q Priority 2. 	Aptio Setup - American Megatrends International, LLC. Advanced Create new VLAN VLAN TD 1001 Phionity 2 Add VLAN 2 Add VLAN 2 Configured VLAN List **: Select Screen TL: Select Item Enter: Select Fit: Select Screen 1001 Fit: General Help F2: Previous Values F3: Dotimized Defaults F4: Save & Exit ESC: Exit ESC: Exit		
Sten 3	Select Add VI AN to create the VI AN	Aptio Setup – American Megatrends International, LLC.		
Step_5		Richald Michael R		
		Oreate new VLAN 0 MLAN ID 0 Priority 0 Add VLAN 0 Configured VLAN List (Disabled) Priority:2 Remove VLAN Remove VLAN (Disabled) Priority:2 (Encode) Remove VLAN (Encode) Very 2:21.1277 Copyright (C) 2020 American Megatrends International, LLC.		
Step_5	Add other VLANs as required by repeating steps 2 and 3	Create new VLAN 0 MLAN ID 0 Priority 0 Add VLAN 0 Configured VLAN List (Disabled) MLAN ID:1001, (Disabled) Priority:2 Remove VLAN #t: Select Screen 11: Select Item Enersi Select -/-: Change Opt. F1: General Help F2: Seve 3 Exit Ver. 2.21.1277 Copyright (C) 2020 American Megatrends International, LLC. AB		
Step_4	 Add other VLANs as required by repeating steps 2 and 3. Example: VLAN ID 2002, with 802.10 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. The setting Enabled and Disabled of the VLANs in the list are only used when removing VLANs. 	Create new VLAN M.AN 10 0 Priority 0 Add VLAN Configured VLAN List M.AN 10:1001, Priority:2 Remove VLAN [Disabled] +t: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F3: Optimized Defaults F3: Optimized Defaults F3: Optimized Defaults F3: Optimized Defaults F3: Optimized Defaults F3: Dotimized Defaults F3: Dotimized Defaults F4: Select Screen 11: Select Item Enter: Select Manage Defaults F4: Select Screen F4: Select Screen F4: Select New VLAN Manage Defaults F4: Select Screen F4: Select Defaults F5: Optimized Defaults F5: Optimized Defaults F5: Optimized Defaults F5: Optimized Defaults F4: Select Screen F4: Select Screen F4: Select Screen F4: Select Defaults F5: Optimized Defaults F5: Optimized Defaults F5: Optimized Defaults F5: Selet Screen F4: Select Screen F4: Select Defaults F5: Selet Screen F4: Select Defaults F5: Optimized Defaults F5: Selet Screen F5: Optimized Defaults F5: Selet Screen F5: Selet Screen F5: Selet Screen F4: Select Screen F4: Select Screen F4: Select Screen F4: Select Screen F4: Select Screen F4: Select Screen F5: Optimized Defaults F5: Selet Screen F4: Select Screen F4: Sel		
Step_4	 Add other VLANs as required by repeating steps 2 and 3. Example: VLAN ID 2002, with 802.1Q Priority 4. NOTES: The VLANs shown below the Configured VLAN List are active whether they have the setting Enabled or Disabled . In this example, VLAN ID 1001 and 2002 are active. The setting Enabled and Disabled of the VLANs in the list are only used when removing VLANs. 	Create new VLAN N.AN 10 0 Priority 0 Add VLAN Configured VLAN List VLAN 10:1001, Priority:2 Remove VLAN [Disabled] ++: Select Screen 11: Select Item Enter: Select +/-: Change Ont. Fi: General Help F3: Optimized Defaults F3: Optimized Defaults F3: Optimized Defaults F3: Optimized Defaults F3: Sove & Exit ESC: Exit Ver. 2.21.1277 Copyright (C) 2020 American Megatrends International, LLC. Advanced Ver. 2.21.1277 Copyright (C) 2020 American Megatrends International, LLC. Advanced Create new VLAN Ver. 10 Near 10 Priority add VLAN D O Configured VLAN List Ver. 2.21.1277 (Disabled] Priority:4 Remove VLAN VLAN ID of new VLAN or VLAN ID of new VLAN or VLAN ID Of new VLAN or VLAN ID Configured VLAN List VER Select Screen 11: Select Item Enter: Select F3: Optimized Defaults F3: Optimized Defaults F3: Optimized Defaults F3: Optimized Defaults F4: Select Screen 11: Select Item Enter: Select F4: Change Opt. F1: General Help F3: Optimized Defaults F3: Optimized Defaults F3: Optimized Defaults F3: Optimized Defaults F4: Select Screen 11: Select Item Enter: Select F4: Select Screen 11: Select Item Enter: Select F4: Select Screen 11: Select Item Enter: Select F5: Optimized Defaults F3: Optimized Defaults F4: Select Screen 11: Select Item Enter: Select F4: Select Screen F5: Optimized Defaults F5: Optimized Defaults F5: Optimized Defaults F5: Select Screen F5: Select Scree		

Removing VLANs

Step_1	Step_1 From the UEFI/BIOS setup menu, select the Advanced menu and select one VLAN Configuration (MAC:xxxxxxxxxx) section. Select Enter Configuration Menu . NOTE: The MAC address will be the one of the X722 10GbE port for which VLANs must be removed.	 ISSII Configuration ISSII Configuration (NRC:ROS2A0166C7) IAC:2A032A016C7-IFV4 Network Configuration Intel(R) Ethernet Connection X722 for 1008ACET - 000400509CFE3) MAC:0A006E09CFE3V0004-IFV6 Network Configuration Intel(R) Ethernet Connection X722 for 1008ACET - 000400509CFE3 MAC:0A006E09CFE3V0004-IFV6 Network Configuration Intel(R) Ethernet Connection X722 for 1008ACET - 00101075191CF1EA MAC:00006E09CFE3V0004-IFV6 Network Configuration Intel(R) Ethernet Connection X722 for 1008ACET - 00101765191CF1EA MAC:00006E09CFEA-IFV6 Network Configuration 		
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, VLAN ID 2002 will be removed and VLAN ID 1001 will be kept.	Antio Setup - American Megatrends International, LLC. Advanced Create new VLAN VLAN 10 0 Priority 0 Add VLAN Configured VLAN List VLAN 10:1001, Priority:2 VLAN 10:2002, Priority:4 Remove MLAN Priority:5 VLAN 10:2002, Priority:6 V.AN 10:2002, Priority:7 V.AN N Priority:8 Remove MLAN Ver. 2:21:1277 Copyright (C) 2020 American Megatrends International, LLC. MB		
Step_3	Repeat steps 1 and 2 to remove VLANs in another X722 10GbE interface, as no	eeded.		
Step_4	Press F4 to save changes and exit.			

Configuring switch NOS networking

Table of contents

- Configuring IP addresses to access the switch NOS
- Adding a NOS VLAN interface IP address
 - Adding a NOS VLAN interface IP address using the Web UI
 - Adding a NOS VLAN interface
 - Configuring a static IP address
 - Configuring a dynamic IP address using DHCP
 - Adding a NOS VLAN interface IP address using the CLI
 - Adding a NOS VLAN interface using a static IP address
 - Adding a NOS VLAN interface using DHCP
- <u>Removing a NOS VLAN interface IP address</u>
 - <u>Removing a NOS VLAN interface IP address using the Web UI</u>
 - <u>Removing a NOS VLAN interface IP address using the CLI</u>

 Changes to the switch configuration are not persistent after rebooting the switch. To preserve configurations, the current configuration needs to be saved to startup-config. From the switch Web UI:
 Select Maintenance, Configuration and then Save startup-config. Click on Save Configuration to confirm the change. From the switch CLI:

- LocalSwitchNOS_OSPrompt:~(config-if)# end
- LocalSwitchNOS_OSPrompt:~# copy running-config startup-config

Configuring IP addresses to access the switch NOS

This section is used to configure IP addresses allowing access to the configuration and management interfaces of the network operating system (NOS). This is the application responsible for implementing L2/L3 packet forwarding features.

One such feature is packet forwarding decisions based on VLAN tag. In that context, IP addresses to communicate with the NOS are attached to a VLAN defined in the NOS database. The switch always has at least VLAN1 that can be assigned an interface.

Refer to Configuring switch VLANs for procedures to add VLANs with the network operating system.

Adding a NOS VLAN interface IP address

This can be done using:

- The <u>Web UI</u>
- The <u>CLI</u>

Adding a NOS VLAN interface IP address using the Web UI

Refer to <u>Accessing the switch NOS using the switch NOS Web UI</u> for access instructions.

Adding a NOS VLAN interface

Step_1	From the left-side menu, select ${\sf Configuration}$, ${\sf System}$ and then ${\sf IP}$.	🗞 kontron 🐐 🗭 😧
Step_2	Click on the Add Interface button.	Configuration System System
Step_3	Enter the VLAN numerical ID. NOTE: As explained above, the VLAN must already exist to create the NOS IP address interface.	IP Interfaces
Step_4	Proceed with IP address configuration as explained below.	

There are two options to configure IP addresses:

- Configuring a <u>static IP address</u>
- Configuring a <u>dynamic IP address using DHCP</u>

Configuring a static IP address

To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the Web</u> <u>UI</u>.

Step_1	From the left-side menu, select Configuration , System and then IP .	Configuration Image: Configuration • Configuration • Configuration • Configuration • Configuration • Provide • Configuration • Provide • Configuration • Configuration • Configuration <td< th=""></td<>
Step_2	Manually configure the IP address and the network mask length of the VLAN interface.	DHCPv4 IPv4 HEX Hostname Fallback Current Lease Address Mask Length E 60 172.16.219.119/r 192.168.0.1 24 24
Step_3	Press on the Save button to confirm.	Configuration • Configuration
Step_4	(Optional) To make the change persistent, save running-config to startup-	-config.

Configuring a dynamic IP address using DHCP

Step 1	From the left-side menu select Configuration . System and then IP	Skontron S D
		Configuration Configu
Step_2	Enable the DHCP by checking the checkbox associated with the interface. The Hostname field allows the DHCP client to use a different hostname than the NOS for the DHCP option 12 field. The Fallback is a timeout in seconds after which the interface will be configured using the static IP address in the proper fields if an address cannot be obtained via DHCP.	UP Interfaces DHCPy4 Hostname Fallback Currents O VLAN1 Zero Addr Point IV Fallback Currents O VLAN1 Zero Addr Point IV 60 172 (5215 119) Deletes 101 Zero Addr Point IV 0 0
Step_3	Press on the Save button to confirm.	Image: Control Image:
Step_4	(Optional) To make the change persistent, save running-config to startup-co	nfig.

Adding a NOS VLAN interface IP address using the CLI

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

Adding a NOS VLAN interface using a static IP address

To preserve configurations, the current configuration needs to be saved to startup-config. Refer to Saving the current configuration using the CLL.

Step_1	Enter the VLAN interface configuration mode. LocalSwitchNOS_OSPrompt:~# configure terminal LocalSwitchNOS_OSPrompt:~(config)# interface VLAN [VLAN_ID]	<pre># configure terminal (config)# interface vlan 1</pre>
Step_2	Set the static IP address source. LocalSwitchNOS_OSPrompt:~(config-if-vlan)# ip address [IP_ADDRESS] [MASK]	(config-if-vlan)# ip address 192.168.0.1 255.255.255.0
Step_3	(Optional) To make the change persistent, save running-config to startup-config.	

Adding a NOS VLAN interface using DHCP

To preserve configurations, the current configuration needs to be saved to startup-config. Refer to Saving the current configuration using the CLL.

Step_1	Enter the VLAN interface configuration mode. LocalSwitchNOS_OSPrompt:~# configure terminal LocalSwitchNOS_OSPrompt:~(config)# interface VLAN [VLAN_ID]	# configure terminal (config)# interface vlan 1
Step_2	Set the IP address source to DHCP. LocalSwitchNOS_OSPrompt:~(config-if-vlan)# ip address dhcp NOTE: To view the IP address assigned, use command do show ip interface .	(config-if-vlan)# ip address dhcp
Step_3	(Optional) To make the change persistent, save running-config to startup-config.	

Removing a NOS VLAN interface IP address

• The <u>Web UI</u>

The <u>CLI</u>

Removing a NOS VLAN interface IP address using the Web UI

Refer to Accessing the switch NOS using the switch NOS Web UI for access instructions.

To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the Web</u> <u>UI</u>.

Step_1	From the left-side menu, select ${\bf Configuration}$, ${\bf System}$ and then ${\rm IP}$.	Skontron AD
Step_2	Select the VLAN interface to delete.	Configuration System System
Step_3	Press on the Save button to confirm.	Image: Secure in the secure in th
Step_4	(Optional) To make the change persistent, save running-config to startup	-config.

Removing a NOS VLAN interface IP address using the CLI

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

Step_1	Enter configuration mode. LocalSwitchNOS_OSPrompt:~# configure terminal	# configure terminal
Step_2	Remove the VLAN. LocalSwitchNOS_OSPrompt:~(config)# no interface vlan [VLAN_ID]	(config)# no interface vlan 101
Step_3	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring the switch

Table of contents

- <u>Help tools</u>
 - <u>Switch Web user interface help</u>
 - Switch CLI help
- Port map configuration
 - <u>Switch NOS port mapping</u>
 - <u>Selecting a port map configuration</u>
 - Description of available port maps
 - Listing port map configurations
 - Selecting a port map configuration
- <u>Verifying link status</u>
 - <u>Verifying link status using the CLI</u>
 - Verifying link status using the Web UI
- Enabling a switch port
 - Enabling a switch port using the CLI
 - Enabling a switch port using the Web UI
- Disabling a switch port
 - Disabling a switch port using the CLI
 - Disabling a switch port using the Web UI
- <u>Changing link speed</u>
 - <u>Changing link speed using the CLI</u>
 - <u>Changing link speed using the Web UI</u>
- <u>Configuring switch VLANs</u>
 - <u>Displaying VLANs</u>
 - Displaying VLANs using the CLI
 - Displaying VLANs using the Web UI
 - Creating a VLAN
 - <u>Creating a VLAN using the CLI</u>
 - <u>Creating a VLAN using the Web UI</u>
 - <u>Removing a VLAN</u>
 - <u>Removing a VLAN using the CLI</u>
 - Removing a VLAN using the Web UI
 - <u>Configuring VLAN port membership</u>
 - Configuring port membership using the CLI
 - Configuring port membership using the Web UI
- <u>Configuring static routing</u>
 - <u>Configuring static routing using the CLI</u>
 - Configuring static routing using the Web UI
- <u>Managing the switch configuration</u>
 - Managing the switch configuration using the CLI
 - Displaying the running configuration using the CLI
 - Saving the current configuration using the CLI
 - Restoring the default configuration using the CLI
 - Managing the switch configuration using the Web UI
 - Saving the current configuration using the Web UI
 - <u>Restoring the default configuration using the Web UI</u>

Relevant sections:

- Accessing the switch NOS
- Accessing the operating system of a server
- Configuring and managing users

1

Changes to the switch configuration are not persistent after rebooting the switch.

To preserve configurations, the current configuration needs to be saved to startup-config.

- From the switch Web UI:
- Select Maintenance, Configuration and then Save startup-config. Click on Save Configuration to confirm the change.

From the switch CLI:

- LocalSwitchNOS_OSPrompt:~(config-if)# end
- LocalSwitchNOS_OSPrompt:~# copy running-config startup-config

Help tools

Switch Web user interface help

The Help menu of the switch Web user interface is comprehensive. It should be used to configure the system. Version 2.0 (June 2022) www.kontron.com

Switch CLI help

The switch CLI contains a context-sensitive help feature. Use the ? symbol to display the next possible parameters or commands and their descriptions.

Almost all configuration commands have a corresponding 'no' form. The 'no' form is syntactically similar (but not necessarily identical) to the configuration command; however, it either resets the parameters to default values for the configurable item or disables the item altogether.

NOS00A0A5E01CF4# show	interface * ?
<port_type_list></port_type_list>	Port list for all port types
capabilities	Display capabilities.
description	Description of interface
statistics	Display statistics
status	Display status.
switchport	Show interface switchport information
transceiver	Show SFP transceiver properties
veriphy	Display the latest cable diagnostic results.
NOS00A0A5E01CF4# show	interface *

Port map configuration

Switch NOS port mapping

The following table lists the physical ports of the Ethernet switch of an ME1210 with the appropriate IO module. Note that, in the switch NOS, physical ports are a category of interfaces. The port designation is used in CLI commands, denoted by **[INTERFACE_ID]** below, to monitor or configure the corresponding port.

As shown below, the switch NOS has a configurable port map. Active ports from the table below differ from the selected port map.

NOS port designation	Connection device	Integrated server PCIe bus
Ethernet 1/1	SFP Sw 1	N/A
Ethernet 1/2	SFP Sw 2	N/A
Ethernet 1/3	SFP Sw 3	N/A
Ethernet 1/4	SFP Sw 4	N/A
Ethernet 1/5	SFP Sw 5	N/A
Ethernet 1/6	SFP Sw 6	N/A
Ethernet 1/7	SFP Sw 7	N/A
Ethernet 1/8	SFP Sw 8	N/A
Ethernet 1/9	SFP Sw 9	N/A
Ethernet 1/10	SFP Sw 10	N/A
Ethernet 1/11	SFP Sw 11	N/A
Ethernet 1/12	SFP Sw 12	N/A
Ethernet 1/13	enol *	00:b8:00.3
Ethernet 1/14	eno2 *	00:b8:00.2
Ethernet 1/15	eno3 *	00:b8:00.1
Ethernet 1/16	eno4 *	00:b8:00.0

* eno1-4 is the typical Linux nomenclature as seen in the integrated server operating system.

Selecting a port map configuration

Unlike other configuration elements, a port map configuration change cannot be applied immediately and requires rebooting the switch. As such, it has no impact on running-config, and there is therefore no need to copy running-config to startup-config to make the change permanent.

For the same reason, reloading the switch default configuration does not affect port map selection as default settings are reloaded to running-config and are volatile until copied to startup-config. Default port map configuration must be manually selected by running **portmap cfg 0** in configuration mode, then rebooting the switch.

Description of available port maps

Port map	Active front panel SFP ports		Internal server ports
0	12x SFP+ 10GbE	SFP1-12	4x 10GBASE-KR
1	7x SFP+ 10GbE	SFP1-7	4x 10GBASE-KR
	2x SFP28 25GbE	SFP9-10	
2	2x SFP+ 10GbE	SFP1-2	4x 10GBASE-KR
	4x SFP28 25GbE	SFP9-12	



SFP ports not in the active list cannot be used or configured. CLI configuration commands will respond with a message explaining this. Web UI elements will not offer the unavailable selections. The port map can only be configured using the CLI.

Access the switch NOS CLI. Refer to <u>Accessing the switch NOS</u> for access instructions.

Listing port map configurations

Different port map configurations are available, allowing for combinations of 10GbE and 25GbE ports without exceeding the switch total bandwidth allocation limit.

There are two methods to list the possible port map configurations and report the currently active one:

From EXEC mode

Step_1	Show available port map configuration options and currently active port map configuration. LocalSwitchNOS_OSPrompt:~# show portmap	# show portmap ID 10G ports 25G ports Unused ports
		Active port map configuration: 0

From Configuration mode

Step_1	Access the configuration setup menu. LocalSwitchNOS_OSPrompt:~# configure terminal	# configure terminal
Step_2	Show available port map configuration options and currently active port map configuration. LocalSwitchNOS_OSPrompt:~(config)# portmap list NOTE: The ID is the value of parameter [PORTMAP_ID] used in the commands.	(config)# portmap list ID 10G ports 25G ports Unused ports None 0 1/1-16 None None 1 1/1-7,13-16 1/9-10 1/8,11-12 2 1/1-2.13-16 1/9-12 1/3-8 Active port map configuration: 0

In both cases, if a port map configuration different than the active one is selected but not yet applied as switch has not been rebooted yet, it will be indicated as follows:

ID	10G ports	25G ports	Unused ports
0	1/1-16	None	None
1	1/1-7,13-16	1/9-10	1/8,11-12
2	1/1-2,13-16	1/9-12	1/3-8
Act	ive port map c	onfiguration:	0
Sel	ected port map	configuration	: 1
(Se	lected port ma	p will take ef	fect following switch reboot)

Selecting a port map configuration

Step_1	Access the configuration setup menu. LocalSwitchNOS_OSPrompt:~# configure terminal	<pre># configure terminal</pre>
Step_2	Select the desired port map configuration ID based on port map list. LocalSwitchNOS_OSPrompt:~(config)# portmap cfg [PORTMAP_ID]	(config)# portmap cfg 2 Switch must be rebooted for new port map to take effect
Step_3	Exit configuration mode and reboot the switch NOS to make the new configuration effective. LocalSwitchNOS_OSPrompt:~(config)# end LocalSwitchNOS_OSPrompt:~# reload cold	(config)# end # reload cold % Cold reload in progress, please stand by.

Verifying link status

Link status can be verified using:

- The CLI
- The switch Web UI

Verifying link status using the CLI

Access the switch NOS CLI. Refer to <u>Accessing the switch NOS</u> for access instructions.

Step_1	Verify every link status. LocalSwitchNOS_OSPrompt:~# show interface * status							
	NOS00A0A5DEE242# show Interface	interface Mode	* status Speed/Duplex	Media Type	Flow Control	Max Frame	Excessive	Link
	Ethernet 1/1	enabled	10Gfdx	sfp	disabled	10240	Discard	1Gfdx (CuSFP)
	Ethernet 1/2	enabled	10Gfdx	stp	disabled	10240	Discard	Down
	Ethernet 1/3	enabled	10Gtdx	stp	disabled	10240	Discard	Down
	Ethernet 1/4	enabled	10Gtdx	stp	disabled	10240	Discard	Down
	Ethernet 1/5	enabled	LUGTOX	stp	disabled	10240	Discard	Down
	Ethernet 1/6	enabled	LUGTOX	stp	disabled	10240	Discard	Down
	Ethernet 1/2	enabled	10GTdX	stp	disabled	10240	Discard	Down
	Ethernet 1/8	enabled	10cfdx	sip	disabled	10240	Discard	Down
	Ethernet 1/9	enabled	10cfdx	sip	disabled	10240	Discard	Down
	Ethernet 1/10	enabled	10cfdv	stp	disabled	10240	Discard	Down
	Ethernet 1/11	enabled	10cfdx	sip	disabled	10240	Discard	Down
	Ethernet 1/12	enabled	10cfdx	sip	disabled	10240	Discard	
	Ethernet 1/15	enabled	10cfdx	sip	disabled	10240	Discard	10cfdy Fiber
	Ethernet 1/14	enabled	10cfdx	sip	disabled	10240	Discard	10cfdy Fiber
	Ethernet 1/15	enabled		sip	disabled	10240	Discard	10cfdy Fiber
	Ethernet 1/10	enabred	TOGLAX	sip	ursabiled	10240	Discard	TOGLOX FIDER

Verifying link status using the Web UI

Access the switch NOS Web UI. Refer to Accessing the switch NOS for access instructions.

Step_1 From the left-side menu, select Configuration and then Ports . The Port Configuration should display the status of the links. Step_1 Image: Step_2 Image: Step_2 Image: Step_2	
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

kontron figuration Port Configuration en Ethe Speed Link Configured 10Gbps FDX 10Gbps FDX ~ 10Gbps FDX 10Gbps FDX 10Gbps FDX 10Gbps FDX ~ Gfdx 10Gbps FDX Gfdx 10Gbps FDX ~ 10Gbps FDX Gfdx 10Gbps FDX ~ fdx Save Re

Enabling a switch port

Switch ports can be enabled using:

- The CLI
- The switch Web UI

Enabling a switch port using the CLI

Access the switch NOS CLI. Refer to <u>Accessing the switch NOS</u> for access instructions. To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the CLI</u>.

Step_1	Access the interface setup menu. LocalSwitchNOS_OSPrompt:~# configure terminal LocalSwitchNOS_OSPrompt:~(config)# interface [INTERFACE_ID]	# configure terminal (config)# interface Ethernet 1/6 (config-if)#
Step_2	Enable the interface. LocalSwitchNOS_OSPrompt:~(config-if)# no shutdown	(config-if)# no shutdown
Step_3	(Optional) To make the change persistent, save running-config to startup-config	

Enabling a switch port using the Web UI

Access the switch NOS Web UI. Refer to <u>Accessing the switch NOS</u> for access instructions.

To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the Web</u> <u>UI</u>.

Step_1	From the left-side menu, select ${\bf Configuration}$ and then ${\bf Ports}$.	🔇 kontron						
Step_2	Enable a switch port by selecting its speed configuration.	Configuration System	Port C	onfig	uration			
				1 Jack		Speed		ole
Step_3	Press on the Save button to confirm.	Pons CFM ADS	Ροπ	LINK	Current	Configured	ty	e
		• ERPS				○ ¥	\diamond	~
		► DHCPv4	1		1Gfdx	Disabled V	Auto	~
		► Security	2		Down	Disabled	Auto	~
		 Aggregation 	3		Down	100Mbps FDX	Auto	<u> </u>
		 Link OAM Loop Protection 	4		Down	1Gbps FDX	Auto	~
		Spanning Tree	5		Down	5Gbps FDX	Auto	~
		 IPMC Profile MVR 	6		Down	10Gbps FDX	Auto	~
		► IPMC ► LLDP ■ SyncE ■ MAC Table			Down	10Gbps FDX V	Auto	¥
			0		Down	10Gbps FDX V	Auto	¥
			10		Down	10Gbps FDX V	Auto	· ·
			11		Down	10Gbps FDX ¥	Auto	¥
		 Private VLANs VCL VCL 	12		Down	10Gbps FDX V	Auto	~
			13	-	10Gfdx	10Gbps FDX 🗸	Auto	~
			14	ŏ	10Gfdx	10Gbps FDX 🗸	Auto	~
		Mirroring	15	•	10Gfdx	10Gbps FDX 🗸	Auto	~
		• UPnP • PTP	16	۲	10Gfdx	10Gbps FDX 🗸	Auto	~
		MRP GVRP SFlow DDMI UDLD Monitor Diagnostics Maintenance	Save	Rese	t			
Step_4	(Optional) To make the change persistent, save running-config to startup-	config.						

Disabling a switch port

Switch ports can be disabled using:

- The CLI
- The switch Web UI

Disabling a switch port using the CLI

Access the switch NOS CLI. Refer to <u>Accessing the switch NOS</u> for access instructions. To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the CLI</u>.

Step_1	Access the interface setup menu. LocalSwitchNOS_OSPrompt:~# configure terminal LocalSwitchNOS_OSPrompt:~(config)# interface [INTERFACE_ID]	# configure terminal (config)# interface Ethernet 1/6 (config-1f)#
Step_2	Disable the interface. LocalSwitchNOS_OSPrompt:~(config-if)# shutdown	(config-if)# shutdown
Step_3	(Optional) To make the change persistent, save running-config to startup-config	·

Disabling a switch port using the Web UI

Access the switch NOS Web UI. Refer to <u>Accessing the switch NOS</u> for access instructions.

Step_1	From the left-side menu, select ${\bf Configuration}$ and then ${\bf Ports}$.	🚱 kontron							l
Step_2	Disable a switch port by changing its speed configuration to Disabled .	Configuration System Green Ethernet	Port 0	Config	uration				
					Speed			Cal	
Step_3	Press on the Save button to confirm.	Ports CFM	Port	Link	Current	Configured		ty	ł
		APS FRPS				0	~	0	
		► DHCPv4	1		1Gfdx	10Gbps FDX	~	Auto	Ì
		► DHCPv6	2		Down	Disabled		Auto	
		 Aggregation 	3	Ö	Down	Autonegotiation	e l	Auto	
		► Link OAM	4	ŏ	Down	1Gbps FDX	- 1	Auto	
		Loop Protection Spapping Tree	5	ě	Down	2.5Gbps FDX	- 1	Auto	,
		► IPMC Profile	6	ŏ	Down	5Gbps FDX	- 1	Auto	
		• MVR	7	ĕ	Down	10Gbps FDX 10Gbps FDX	~	Auto	
			8	ě	Down	10Gbps FDX	~	Auto	
		- SyncE	9	ě	Down	10Gbps FDX	~	Auto	
		 MAC Table 	10	ě	Down	10Gbps FDX	~	Auto	
		VLANS VLAN Translation	11	ě	Down	10Gbps FDX	~	Auto	,
		Private VLANs	12	ě	Down	10Gbps FDX	-	Auto	,
		► VCL	13		10Gfdx	10Gbps EDX	~	Auto	,
		TSN	14		10Gfdx	10Gbps EDX	~	Auto	,
		 Mirroring 	15		10Gfdx	10Gbps FDX	~	Auto	,
		• UPnP	16	ŏ	10Gfdx	10Gbps FDX	~	Auto	,
		MRP GVRP GVRP GVRP ODN DDM UDLD Monitor Diagnostics Maintenance	Save	Rese	t				-
Step_4	(Optional) To make the change persistent, save running-config to startup-c	onfig.							

Changing link speed

Link speed can be changed using:

- The CLI
- The switch Web UI

Changing link speed using the CLI

Access the switch NOS CLI. Refer to <u>Accessing the switch NOS</u> for access instructions.

To preserve configurations, the current configuration needs to be saved to startup-config. Refer to Saving the current configuration using the CU.

Step_1	Enter the configuration terminal. LocalSwitchNOS_OSPrompt:~# configure terminal	# configure terminal
Step_2	Enter the interface configuration menu. LocalSwitchNOS_OSPrompt:~(config)# interface [INTERFACE]	(config)# interface Eth 1/8
Step_3	Change the speed. LocalSwitchNOS_OSPrompt:~(config-if)# speed [SPEED] NOTE: For interfaces 2.5GbE (Eth 1/7) and 10GbE (Eth 1/8), the speeds currently supported are "auto 10g" (10GbE only), "auto 2.5g" , "auto 1000" or "auto" .	(config-if)# speed auto 1000
Step_4	(Optional) To make the change persistent, save running-config to startup-config.	

Changing link speed using the Web UI

Access the switch NOS Web UI. Refer to <u>Accessing the switch NOS</u> for access instructions.

Step_1	From the left-side menu, select $\ensuremath{Configuration}$, and then \ensuremath{Ports} .	🚱 kontron							
Step_2	Select a value from the Speed dropdown menu.	✓ Configuration ▶ System	Port Configuration						
Step_3	Press on the Save button to confirm.	Green Ethernet Thermal Protection Ports	Port	Link		Speed			
		► CFM	FOR	LINK	Current	Configured			
		• ERPS				\diamond	~		
		► DHCPv4	1		1Gfdx	1Gbps FDX	~		
		► DHCPV6 ► Security	2		Down	Disabled			
		► Aggregation	3		Down	Autonegotiation 100Mbps EDX			
		► Link OAM	4		Down	1Gbps FDX			
		 Spanning Tree 	5		Down	2.5Gbps FDX	NS		
		▶ IPMC Profile	6		Down	5Gbps FDX 10Gbps FDX			
		= MVR	7	Ö	Down	10Gbps FDX	~		
		► I I DP	8	ŏ	Down	10Gbps FDX	~		
		SyncE	9	ĕ	Down	10Gbps FDX	~		
		MAC Table	10	ŏ	Down	10Gbps FDX	~		
		VLANS	11	ĕ	Down	10Gbps FDX	~		
		Private VLANs	12	ŏ	Down	10Gbps FDX	~		
		► VCL	13		10Gfdx	10Gbps FDX	~		
		► TSN	14		10Gfdx	10Gbps FDX	~		
		 Mirroring 	15		10Gfdx	10Gbps FDX	v		
		• UPnP • PTP	16		10Gfdx	10Gbps FDX	~		
		MRP GVRP SFlow DDMI UDLD Monitor Diagnostics Maintenance	Save	Rese	t				
Step_4	(Optional) To make the change persistent, save running-config to startu	o-config.							

Configuring switch VLANs

Several VLAN configurations can be performed using the CLI or the switch Web UI:

- Displaying a VLAN
- Creating a VLAN
- Removing a VLAN
- Configuring the port membership

Displaying VLANs

Displaying VLANs using the CLI

Access the switch NOS CLI. Refer to <u>Accessing the switch NOS</u> for access instructions.

Step_1	Display the VLAN status for every switch port. LocalSwitchNOS_OSPrompt:~# show vlan	# show vlan VLAN Name 1 default 2 VLAN0002 101 VLAN0101	Interfaces Eth 1/1-16	
--------	-----------------------------------------------------------------------------------------------	-------------------------------------------------------------------------	--------------------------	--

Displaying VLANs using the Web UI

Access the switch NOS Web UI. Refer to Accessing the switch NOS for access instructions.

Step_1	From the left-side menu, select $\operatorname{\textbf{Monitor}}$, $\operatorname{\textbf{VLANs}}$ and then $\operatorname{\textbf{Membership}}$.	🕞 kontron						
	The VLAN port membership should be displayed.	Configuration Monitor System Green Ethernel Thermal Protection Ports CFLS CFLS CFLS ERPS Ent COM DHCPv4 DHCPv4 DHCPv6 Security Aggregation Loop Protection Spanning Tree	VLAN Membership Status for Combined users Start from VLAN 1 with 20 entries per page. [<< >> VLAN ID 1 2 3 4 5 6 7 6 9 10 11 13 14 15 16 1 2 2 2 2 2 2 2 2 101 2 3 4 5 6 7 6 10 11 2 10					

Creating a VLAN

Creating a VLAN using the CLI

Access the switch NOS CLI. Refer to <u>Accessing the switch NOS</u> for access instructions. To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the CLI</u>.

Step_1	Enter configuration mode. LocalSwitchNOS_OSPrompt:~# configure terminal	# configure terminal
Step_2	Create a new VLAN. LocalSwitchNOS_OSPrompt:~(config)# vlan [VLAN_ID]	(config)# vlan 9 (config-vlan)#
Step_3	(Optional) To make the change persistent, save running-config to startup-config.	

Creating a VLAN using the Web UI

Access the switch NOS Web UI. Refer to <u>Accessing the switch NOS</u> for access instructions.

To preserve configurations, the current configuration needs to be saved to startup-config. Refer to Saving the current configuration using the Web

U	l	

Step_1	From the left-side menu, select Configuration , VLANs and then Configuration .	
Step_2	From the Global VLAN Configuration , add the desired VLAN(s) to the Allowed Access VLANs list. NOTE : The list of VLANs needs to be delimited by commas between each interface ID.	• • • • • • • • • • • • • • • • • • •
Step_3	Click on the Save button.	
Step_4	(Optional) To make the change persistent, save running-config to startup-co	onfig.

Removing a VLAN

Removing a VLAN using the CLI

Access the switch NOS CLI. Refer to <u>Accessing the switch NOS</u> for access instructions. To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the CLI</u>.

Step_1	Enter configuration mode. LocalSwitchNOS_OSPrompt:~# configure terminal	# configure terminal
Step_2	Remove a VLAN using the following command. LocalSwitchNOS_OSPrompt:~(config)# no vlan [VLAN_ID]	(config)# no vlan 9 (config)#
Step_3	(Optional) To make the change persistent, save running-config to startup-config.	

Removing a VLAN using the Web UI

Access the switch NOS Web UI. Refer to <u>Accessing the switch NOS</u> for access instructions.

Step_1	From the left-side menu, navigate to Configuration , VLANs , and then Configuration .	<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	From the Global VLAN Configuration , remove the desired VLANs from the Allowed Access VLANs list.	Global VLAN Configuration Allowed Access VLANs Ethertype for Custom S ports B8A8 Global VLAN Configuration Allowed Access VLANs Ethertype for Custom S ports B8A8
Step_3	Click on the Save button.	
Step_4	(Optional) To make the change persistent, save running-config to startup-co	onfig.

Configuring VLAN port membership

i Th

The default configuration for the ME1210 NOS switch port mode is "hybrid". Therefore the documentation does not detail commands related to "access" or "trunk".

Configuring port membership using the CLI

Access the switch NOS CLI. Refer to <u>Accessing the switch NOS</u> for access instructions. To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the CLI</u>.

Step_1	Access the desired interface configuration menu. LocalSwitchNOS_OSPrompt:~# configure terminal LocalSwitchNOS_OSPrompt:~(config)# interface [INTERFACE_ID]	# configure terminal (config)# interface Ethernet 1/3
Step_2	 Proceed with port membership configuration. Use the built-in help feature using "? " to see the possible configurations. VLAN membership configuration command descriptions: Adding one or multiple VLANs using the add command. Adding all currently defined VLANs using the all command. Excluding one or multiple VLANs using the except command. Excluding all currently defined VLANs using the none command. Removing one or multiple VLANs using the remove command. LocalSwitchNOS_OSPrompt:~(config-if)# switchport hybrid allowed vlan add [VLAN_ID] 	(config-if)# switchport hybrid allowed vlan <vlan_list> add all except none remove (config-if)# switchport hybrid allowed vlan add 1</vlan_list>
Step_3	(Optional) To make the change persistent, save running-config to startup-con	nfig.

Configuring port membership using the Web UI

Access the switch NOS Web UI. Refer to <u>Accessing the switch NOS</u> for access instructions.

Step_1	From the left-side menu, navigate to Configuration , VLANs and then Configuration .	
Step_2	Proceed with port membership configuration using the last two columns. The list of VLANs is constructed using a comma to separate elements or a hyphen to describe a range. Example: 1,101-103,4093 Which is equivalent to: 1,101,102,103,4093	Port VLAN Configuration Port Type Port Type </td
Step_3	Press on the Save button to confirm.	Global VLAN Configuration Marging of configuration Marging of configuration Prot VLAN Configuration Prot VLAN Configuration Prot VLAN Configuration Prot Type To Ty
Step_4	(Optional) To make the change persistent, save running-config to start	up-config.

Configuring static routing

Static routing can be configured using:

- The CLI
- The switch Web UI

Configuring static routing using the CLI

Access the switch NOS CLI. Refer to <u>Accessing the switch NOS</u> for access instructions.

To preserve configurations, the current configuration needs to be saved to startup-config. Refer to Saving the current configuration using the CLL.

Step_1	Enter configuration mode. LocalSwitchNOS_OSPrompt:~# configure terminal	<pre># configure terminal</pre>
Step_2	Configure static routing. LocalSwitchNOS_OSPrompt:~(config)# ip route [HOST_ADDRESS] [NETWORK_MASK] [GATEWAY_ADDRESS]	(config)# ip route 192.168.3.0 255.255.255.0 172.16.0.3
Step_3	Exit the configuration menu. LocalSwitchNOS_OSPrompt:~(config)# exit	
Step_4	Display the list of routes to confirm the static route was added. LocalSwitchNOS_OSPrompt:~# show ip route	<pre># show ip route Codes: C - connected, S - static</pre>
Step_5	(Optional) To make the change persistent, save running-config to startup-co	nfig.

Configuring static routing using the Web UI

Access the switch NOS Web UI. Refer to <u>Accessing the switch NOS</u> for access instructions.
Step_1	From the left-side menu, select ${\bf Configuration}$, ${\bf System}$ and then ${\rm IP}$.	Skontron A 🕑 Ø	
Step_2	Click on the Add Route button.	Configuration System System	
Step_3	 Proceed with configuration: Enter host address in the Network column. Enter network mask in number of bits in the Mask Length column. Enter the gateway address in the Gateway column. Configure the Next Hop VLAN (IPv6) and Distance parameters, if needed. 	IP Routes Delete Network Mask Length Gateway Next Hop VLAN (IPv6) Distance 192.168.3.0 24 172.16.0.3 0 1 Add Route Save Reset	
Step_4	Press on the Save button to confirm.		
Step_5	(Optional) To make the change persistent, save running-config to startup-co	nfig.	

Managing the switch configuration

Managing the switch configuration using the CLI

Access the switch NOS CLI. Refer to <u>Accessing the switch NOS</u> for access instructions.

Displaying the running configuration using the CLI

Step_1 Display the current configuration. LocalSwitchNOS_OSPrompt:~# show running-config	NOS00A0ASE10E54# show running-config Building configuration username admin privilege 15 password encrypted 4114dc09c554cbc78c5d5916ca7d0267a 66c020fbfabbeac88b9085591dea74e127c29e0f5fdf14e100c62f46d2410c830045931f03770adda c2c9f1bf89d4227 ! vlan 1 ! spanning-tree mst name 00-a0-a5-e1-0e-54 revision 0 ! spanning-tree mst name 00-a0-a5-e1-0e-54 revision 0 ! ptp ext output auto ptp rs422 main-auto ser proto rmc ! more, next page: Space, continue: g, quit: ^C
---------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Saving the current configuration using the CLI

Changes to the switch configuration are not persistent after rebooting the switch. To preserve custom configurations, use the following command.

Step_1	Save the current configuration. LocalSwitchNOS_OSPrompt:~# copy running-config startup-config	<pre># copy running-config startup-config Building configuration % Saving 1555 bytes to flash:startup-config #</pre>
		#

Restoring the default configuration using the CLI

NOTE: This procedure is equivalent to a factory reset for switch configuration. All configuration changes will be lost.

Step_1	Restore the default configuration. LocalSwitchNOS_OSPrompt:~# reload defaults	<pre># reload defaults % Reloading defaults. Please stand by.</pre>
Step_2	To make the revert to default values permanent, use the following command. LocalSwitchNOS_OSPrompt:~# copy running-config startup-config	<pre># copy running-config startup-config Building configuration % Saving 1555 bytes to flash:startup-config</pre>

Managing the switch configuration using the Web UI

Access the switch NOS Web UI. Refer to <u>Accessing the switch NOS</u> for access instructions.

Saving the current configuration using the Web UI

Changes to the switch configuration are not persistent after rebooting the switch. To preserve custom configurations, use the following

Step_1	From the left-side menu, select Maintenance , Configuration , and then Save startup-config .	Configuration	Save Running Configuration to startup-config
Step_2	Press on the Save Configuration button.	Diagnostics Maintenance Restart Device Factory Defaults Software Configuration Save starture.configuration Uptoad Activate Delete	Please note: The generation of the configuration file may be time consuming, depending on the amount of non- default configuration. Seve Configuration

Restoring the default configuration using the Web UI

Step_1	From the left-side menu, select Maintenance and then Factory	🔇 kontron		ñ 🕩 🛛
	Defaults .	Configuration Monitor	Factory Defaults	
Step_2	Press on the Yes button to confirm the choice.	Diagnostics Maintenance Restart Device Restart Device Factory Defaults Software Upoad Image Select Configuration Save startup-config Downbad Liptoad Liptoad Loptoat Detete	Are you sure you want to reset the configuration to Factory Defaults? Yes No	

Configuring synchronization

Table of contents

- <u>GNSS</u>
 - <u>Factory configuration</u>
 - Configuring the antenna cable delay
 - Verifying the status of the USB port connecting the GNSS receiver to the internal server
 - Configuring the antenna delay
- <u>PTP based on IEEE 1588</u>
 - <u>PPS output</u>
 - <u>Switch NOS PTP External Clock Mode configuration</u>
 - <u>Creating a switch NOS PTP instance</u>
 - Configuring the switch as a telecom grandmaster as per ITU-T G.8275.1
 - <u>Prerequisite</u>
 - <u>Procedure</u>
 - Configuring the switch as a telecom boundary clock as per ITU-T G.8275.1
 - <u>Prerequisite</u>
 - <u>Procedure</u>
 - Configuring the internal server as a telecom time slave clock as per ITU-T G.8275.1
 - <u>Synchronizing the X722 PTP hardware clock</u>
 - <u>Prerequisite</u>
 - <u>Procedure</u>
 - <u>Synchronizing the integrated server system time</u>
 - Prerequisite
 - <u>Procedure</u>
- <u>Configuring synchronous Ethernet</u>
 - <u>Prerequisite</u>
 - <u>Procedure</u>

This section only applies to platforms with the Ethernet switch IO module.

Platform synchronization must be configured for all components to communicate effectively. On this platform, the Time of Day (ToD) and phase synchronization can be obtained from the integrated GNSS receiver or a PTP grandmaster (GM) accessible by the NOS via a switch network connection.

- When the GNSS is used, it transfers the information to the NOS, which can become a PTP grandmaster if configured accordingly .
- When a PTP grandmaster accessible via a network connection is used, it transfers the information to the NOS to synchronize its boundary clock instance.

The switch can then source synchronization to other components using combinations of Precision Time Protocol (PTP) and Synchronous Ethernet (SyncE).

The following components can also be synchronized:

- PTP/SyncE slave devices connected to the platform switch ports
- Platform integrated server's X722 Ethernet controller PTP hardware clock
- NOS system time (using PTP)

This section will describe how to configure synchronization for the various components involved.

Relevant sections:

Accessing the switch NOS Accessing the operating system of a server Configuring and managing users

GNSS

Factory configuration

The NEO-M9N GNSS receiver is configured during platform manufacturing. The following minimal configurations are performed to ensure it operates properly with the Ethernet switch NOS.

Item	Description	Default value	Value in this platform
CFG-NAVSPG-DYNMODEL	Dynamic platform model	0 (Portable)	2 (Stationary)
CFG-UART1-BAUDRATE	Baud rate for UART1	38400	115200

Configuring the antenna cable delay

Configuring compensation of the antenna cable delay is highly recommended to get precise synchronization.

Item	Description	Default value	Value in this platform
CFG-TP-ANT_CABLEDELAY	Antenna cable delay	50 ns	User-defined

To change the GNSS receiver (NEO-M9N) settings, use **ubxtool** from the **gpsd** software package for Linux running on the integrated server.

1	Version 3.22 of the gpsd software package is required. Please refer to <u>https://gpsd.gitlab.io/gpsd/index.html</u> for more information.
	Changes to any other settings are not supported. For example, if a change is made to the baud rate, this will prevent the switch NOS from receiving the Time of Day from the GNSS receiver.

Verifying the status of the USB port connecting the GNSS receiver to the internal server

Log in to the UEFI/BIOS setup menu. Refer to <u>Accessing the UEFI or BIOS</u> for access instructions.

Step_1	From the UEFI/BIOS setup menu, navigate to the Platform	Aptio Setup Utility - Copyright (C) 2021 American Megatrends, Inc. Main Advanced Platform Configuration Socket Configuration Server Mgmt >			
	Configuration tab and select PCH Configuration .	> PCH Configuration > Miscellaneous Configuration > Server ME Configuration > Runtime Error Logging > Reserve Nemory > Non-Silicon Specific Items Setting items on this Screen to incorrect values may cause system to malfunction! Yersion 2,20,1271. Copyright (C) 2021 American Megatrends, Inc.			
Step_2	Select USB Configuration .	Aptio Setup Utility - Copyright (C) 2021 American Megatrends, Inc. Platform Configuration PCH Configuration > PCH Express Configuration > PCH Express Configuration > PCH SATA Configuration > PCH SATA Configuration > PCH SATA Configuration > PCH SATA Configuration > PCH DEVICES > PCH SATA Configuration > PCH SATA Configuration > PCH DEVICES > Security Configuration > PCH DEVICES > PCH DEVICES > Security Configuration > PCH DEVICES > PCH DEV			
Step_3	Select USB HS (10 Board USB2) and ensure its status is set to Enable .	Aptio Setup Utility - Copyright (C) 2021 American Megatrends, Inc. Platform Configuration VISB Precondition [Disable] VSB Precondition [Disable] YHCH Manual Mode [Disable] USB Per-Connector [Enable] USB Per-Connector [Enable] USB Per-Connector [Enable] USB HS (142: Front IO [Enable] VISB HS (142: Front II [Disable Plate, Top USB2)			

Configuring the antenna delay

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

Step_1	Configure the antenna cable delay. In this example, the value will be set to 145 ns. Server_OSPrompt:~# ubxtool -f /dev/ttyACM0 -P32 -z CFG-TP- ANT_CABLEDELAY,[CABLE_DELAY]	root@ubuntu:~# ubxtool -f /dev/ttyACM0 -P32 -z CFG-TP-ANT_CABLEDELAY,145 sent: UBX-CFG-VALSET: version 0 layer 0x7 transaction 0x0 reserved 0 layers (ram bbr flash) transacion (Transactionless) item CFG-TP-ANT_CABLEDELAY/0x30050001 val 145	
Step_2	Save the configuration to flash. Server_OSPrompt:~# ubxtool -f /dev/ttyACM0 -P32 -p SAVE	rootĝubuntu:⊶# ubxtool -f /dev/ttyACM0 -P32 -p SAVE ubxtool: poll SAVE sent: UBX-CFG-CFG: clearMask: 0x0 () saveMask: 0x1f (ioPort msgConf infMsg navConf rxmConf senConf rinvConf antConf logConf) loadMask: 0xf1f (ioPort msgConf infMsg navConf rxmConf senConf rinvConf antConf logConf) deviceMask: 0x17 (devBBR devFlash devEPROM devSpiFlash)	
i	With the default configuration, the GNSS records becomes the timing synchronization source v	eiver is automatically available to be used by the Ethernet switch NOS. The GNSS receiver when a PTP instance 0 is configured for master only mode. This is described below.	
1	The information given by the GNSS receiver can be used concurrently by the internal server through the USB interface if needed. This is mostly interesting for positioning or monitoring information for the user application. Using this interface for timing is not recommended since its accuracy is very limited. For tight timing requirements on the integrated server application, configure the Ethernet switch for PTP on one or more of ports 1/12 to 1/16 and use LinuxPTP to synchronize time with the integrated server's X722 Ethernet controller. This is described below .		
i	Linux applications can alter the configuration of the GNSS receiver. As such, usage of the USB connection to the GNSS receiver is not supported in the event that it causes issues in the Ethernet switch PTP operations.		

PTP based on IEEE 1588

PPS output

Relevant section: <u>SMA PPS output</u>

The PPS output is always enabled and outputs a 100 ms pulse whose rising edge is aligned with the PTP domain 0 ToD counter rollover. The PPS output has less than 10 ns offset from the integrated switch PTP phase at the SMA connector. Any external cable length must be compensated when doing timing measurements.

Switch NOS PTP External Clock Mode configuration

Note that changes to the PTP External Clock Mode configuration parameters are not supported. These parameters are the ones shown below.

NOS Web UI			NOS CLI	
🔇 kontron				NOS00A0A5E05346(config)# ptp ext
 Configuration	PTP External Clo	ock Mode		
 Green Ethernet Thermal Protection 	One_PPS_Mode	Output v		
Ports	External Enable	False v		
► CFM	Adjust Method	Auto 🗸		
● APS ● ERPS	Clock Frequency	1		

Creating a switch NOS PTP instance

The following information is based on the ITU-T G.8275.1 Telecom profile. However, other PTP profiles are available, and the commands can easily be adapted.

Configuring the switch as a telecom grandmaster as per ITU-T G.8275.1

The switch can be configured as a telecom grandmaster (T-GM) (primary reference clock) using the switch NOS CLI or Web UI. The following example will use the CLI and shows minimum configurations using default values for most parameters. Only critical values are included in the exam ple. However, additional configurations are likely to be required.

Prerequisite

1 To obtain meaningful results, the integrated GNSS receiver must acquire timing information. An appropriate antenna must be connected to the chassis GNSS input. Please refer to <u>SMA GNSS RF input pinout and electrical characteristics</u>.

Procedure

Log in to the switch NOS CLI. Refer to <u>Accessing the switch NOS</u> for access instructions.

Step_1	Enter configuration mode. LocalSwitchNOS_OSPrompt:~# configure terminal	NOS00A0A5DEE114# configure terminal NOS00A0A5DEE114(config)#
Step_2	Create the PTP instance. Specifying the filter type in this configuration is required since the default is for 16 timestamp per second, whereas the GNSS receiver 1PPS is 1 Hz. Then add the required interface(s) to "ptp 0", the clock instance created Copy the following lines to the NOS terminal: LocalSwitchNOS_OSPrompt:~# ptp 0 mode master twoway profile g8275.1 ptp 0 filter-type aci-basic-phase-low ptp 0 time-property utc-offset 37 valid ptptimescale Notes : • twoway is recommended to obtain better performance from the ME1210 NOS PTP implementation in this configuration • the utc-offset value changes in time and should be chosen according to the current value	NOS00A0A5DEE114(config)# ptp 0 mode master twoway profile g8275.1 NOS00A0A5DEE114(config)# ptp 0 filter.type aci.basic.phase.low NOS00A0A5DEE114(config)# ptp 0 time-property utc-offset 37 valid ptptimescale
Step_3	(Optional) The following items configure the PTP dataset communicated by the instance. The values here are valid when the instance has achieved PHASE_LOCKED state. ME1210 NOS does not dynamically adjust these settings. If required by the deployment infrastructure, the customer's application will need to monitor the PTP instance state and adjust the values accordingly LocalSwitchNOS_OSPrompt:~# ptp 0 time-property freq-traceable time-traceable time-source 32 ptp 0 virtual-port class 6 ptp 0 virtual-port accuracy 33 ptp 0 virtual-port variance 20061	NOSO0A0A5DEE114# ptp 0 time-property freq-traceable time-traceable time-source 32 NOSO0A0A5DEE114# ptp 0 virtual-port class 6 NOSO0A0A5DEE114# ptp 0 virtual-port accuracy 33 NOSO0A0A5DEE114# ptp 0 virtual-port variance 20061
Step_4	(Optional) Set the NOS system time from the PTP instance LocalSwitchNOS_OSPrompt:~# ptp system-time set	NOSO0A0A5DEE114(config) # ptp system-time set System clock synch mode (Set System time from PTP time)
Step_5	Add interfaces to the PTP instance LocalSwitchNOS_OSPrompt:~# interface Ethernet 1/1,9,12 ptp 0	NOS00A0A5DEE114(config)# interface Ethernet 1/1,9,12 NOS00A0A5DEE114(config-if)# ptp 0
Step_6	End configuration. LocalSwitchNOS_OSPrompt:~# end	NOS00A0A5DEE114(config-if)# end NOS00A0A5DEE114#
Step_7	Verify the current ptp 0 status. LocalSwitchNOS_OSPrompt:~# show ptp 0 slave NOTE: The desired status to be attained is PHASE_LOCKED . Interim steps that can be displayed are FREQ_LOCKING , FREQ_LOCKED , PHASE_LOCKING , HOLDOVER . The time to reach PHASE_LOCKED varies depending on many factors including the status of the GNSS receiver. Twenty minutes is expected for example.	NOS00A0A5DEE114# show ptp 0 slave Slave port Slave state Holdover(ppb)
Step_8	Verify the current offset from the master (which is the GNSS receiver). LocalSwitchNOS_OSPrompt:~# show ptp 0 current	NOSNOS00A0A5DEE114# show ptp 0 current stpRm OffsetFromMaster MeanPathDelay 0 -0.000,000,003,621 0.000,000,000,000
Step_9	(Optional) To make the change persistent, save running-config to startup-config. LocalSwitchNOS_OSPrompt:~# copy running-config startup-config	NOSNOS00A0A5DEE114# copy running-config startup-config

Configuring the switch as a telecom boundary clock as per ITU-T G.8275.1

The switch can be configured as a telecom boundary clock (T-BC) using the switch NOS CLI or Web UI. The following example will use the CLI.

Prerequisite

1 A G.8275.1 telecom grandmaster must be connected to the platform via an integrated switch SFP port to get meaningful results.

Procedure

Log in to the switch NOS CLI. Refer to <u>Accessing the switch NOS</u> for access instructions.

Step_1	Enter configuration mode. LocalSwitchNOS_OSPrompt:~# configure terminal	NOS00A0A5E05346# configure terminal NOS00A0A5E05346(config)#
Step_2	Create the PTP clock instance "0". Then add the desired interface(s) to "ptp 0", the clock instance created. LocalSwitchNOS_OSPrompt:~# ptp 0 mode boundary profile g8275.1 NOTE : Changing the default filter-type is not supported in this configuration.	NOS00A0A5E05346(config)# ptp 0 mode boundary profile g8275.1 NOS00A0A5E05346(config)#
Step_3	(Optional) Set the NOS system time from the PTP instance. LocalSwitchNOS_OSPrompt:~# ptp system-time set	NOS00A0A5E24FC2(config)# ptp system-time set System clock synch mode (Set System time from PTP time)
Step_4	Add interfaces to the PTP instance. LocalSwitchNOS_OSPrompt:~# interface Ethernet 1/1,9,12 LocalSwitchNOS_OSPrompt:~# ptp 0	NOS00A0A5E24FC2(config)# interface Ethernet 1/1,9,12 NOS00A0A5E24FC2(config-if)# ptp 0 NOS00A0A5E24FC2(config-if)#
Step_5	End configuration. LocalSwitchNOS_OSPrompt:~# end	NOS00A0A5E24FC2(config-if)# end NOS00A0A5E24FC2#
Step_6	Verify the current ptp 0 status. LocalSwitchNOS_OSPrompt:~# show ptp 0 slave NOTE: The desired status to be attained is PHASE_LOCKED . Interim steps that can be displayed are FREQ_LOCKING , FREQ_LOCKED , PHASE_LOCKING , HOLDOVER . The time to reach PHASE_LOCKED varies depending on many factors. As a reference, a 20-minute delay can be expected.	NOS00A0A5DEE29C# show ptp 0 slave Slave port Slave state Holdover(ppb)
Step_7	Verify the current offset from the PTP grandmaster. LocalSwitchNOS_OSPrompt:~# show ptp 0 current	NOS00A0A5DEE29C# show ptp 0 current stpRm OffsetFromMaster MeanPathDelay 1 -0.000,000,000,314 0.000,000,013,382 NOS00A0A5DEE29C#
Step_8	(Optional) To make the change persistent, save running-config to startup-config. LocalSwitchNOS_OSPrompt:~# copy running-config startup-config	NOS00A0A5DEE242# configure terminal NOS00A0A5DEE242(config)# end NOS00A0A5DEE242# copy running-config startup-config Building configuration % Saving 2888 bytes to flash:startup-config NOS00A0A5DEE242#

Configuring the internal server as a telecom time slave clock as per ITU-T G.8275.1

To synchronize the internal server's network interfaces and system time precisely, use LinuxPTP.

NOTE: A recent version of LinuxPTP is required for G.8275.1 support, version 3.1 is used here. It must be downloaded and compiled since Linux distributions may only offer older versions in package repositories.

NOTE: Examples are provided for demonstration purposes only. Refer to your Linux distribution documentation to properly configure the PTP services through the OS initialization system.

1

The masterOnly and slaveOnly options below are renamed clientOnly and serverOnly in the current LinuxPTP source tree. If a version more recent than 3.1 is used, the configuration below has to be adapted.

Synchronizing the X722 PTP hardware clock

Prerequisite

1 The switch must be configured as a T-GM or a T-BC as explained above. In the example below, port 1/13 of the integrated switch is used and must be configured for the proper PTP clock instance. This connects to the integrated server **eno1** network connection.

Procedure

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

Step_1	Make sure the network interface is up. Server_OSPrompt:~# ifconfig eno1 up	root@ubuntu:~/linuxptp# ifconfig eno1 up root@ubuntu:~/linuxptp#	
Step_2	Create a configuration file named g8275_client.conf with the following content. Server_OSPrompt:~# cat g8275_client.conf [global] verbose 1 dataset_comparison G.8275.x G.8275.defaultDS.localPriority 128 maxStepsRemoved 255 logAnnounceInterval -3 logSyncInterval -4 logMinDelayReqInterval -4 masterOnly 0 slaveOnly 1 G.8275.portDS.localPriority 128 network_transport L2 domainNumber 24 [eno1]	<pre>root@ubuntu:~/linuxptp# cat g8275_client.conf [global] verbose 1 dataset_comparison G.8275.x G.8275.defaultDS.localPriority 128 max5tepsRemoved 255 logAnnounceInterval -3 logSyncInterval -4 logMinDelayReqInterval -4 serverOnly 0 clientDolly 1 G.8275.portDS.localPriority 128 network_transport L2 domainNumber 24 [eno1] root@ubuntu:~/linuxptp#</pre>	
Step_3	Run ptp4l. Server_OSPrompt:~#./linuxptp/ptp4l -f g8275_client.conf	<pre>root@ubuntu:~/linuxptp# ./linuxptp/ptp41 -f g8275_client.conf ptp41[7789.057]: selected /dev/ptp4 as PTP clock ptp41[7789.059]: port 1: INITIALIZING to LISIENING on INIT_COMPLETE ptp41[7789.059]: port 1: intriALIZING to LISIENING on INIT_COMPLETE ptp41[7780.58]: selected local clock 00a083.fffe.dd41c as best master ptp41[7790.0790.032]: updating UTC offset to 37 ptp41[7790.262]: updating UTC offset to 37 ptp41[7790.263]: nms 598 max 423 freq -7661 +/. 8910 delay -19 /- 168 ptp41[7790.363]: nms 598 max 423 freq -365 +/ -542 delay 151 +/- 13 ptp41[7790.336]: nms 598 max 423 freq -365 +/ -542 delay 151 +/- 13 ptp41[7796.336]: nms 180 max 312 freq -7661 +/- 45 delay 178 +/- 2 ptp41[7796.336]: nms 19 max 27 freq -22 +/- 4 delay 178 +/- 2 ptp41[7796.336]: nms 1 max 2 freq -17 +/- 1 delay 171 +/- 0 ptp41[780.343]: nms 2 max 3 freq -2 +/- 1 delay 171 +/- 0 ptp41[780.343]: nms 2 max 3 freq -2 +/- 1 delay 171 +/- 0 ptp41[780.343]: nms 1 max 2 freq -1 +/- 1 delay 171 +/- 0 ptp41[780.343]: nms 0 max 1 freq -2 +/- 1 delay 171 +/- 0 ptp41[780.343]: nms 0 max 1 freq -2 +/- 1 delay 171 +/- 0 ptp41[780.343]: nms 0 max 1 freq -2 +/- 1 delay 171 +/- 0 ptp41[780.343]: nms 0 max 1 freq -2 +/- 1 delay 171 +/- 0 ptp41[780.343]: nms 0 max 1 freq -2 +/- 1 delay 171 +/- 0 ptp41[780.343]: nms 0 max 1 freq -2 +/- 1 delay 171 +/- 0 ptp41[780.343]: nms 0 max 1 freq -2 +/- 1 delay 171 +/- 0 ptp41[780.343]: nms 0 max 1 freq -2 +/- 1 delay 171 +/- 0 ptp41[780.343]: nms 0 max 1 freq -2 +/- 1 delay 171 +/- 0 ptp41[780.343]: nms 0 max 1 freq -2 +/- 1 delay 171 +/- 0 ptp41[780.344]: nms 1 max 1 freq -2 +/- 1 delay 171 +/- 0 ptp41[780.344]: nms 1 max 1 freq -2 +/- 1 delay 171 +/- 0 ptp41[780.544]: nms 1 ma</pre>	

Synchronizing the integrated server system time

Prerequisite



Procedure

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

Step_1	Verify the running ptp4l status. Server_OSPrompt:~# ./linuxptp/pmc -u -d24 'GET CURRENT_DATA_SET'	<pre>root@ubuntu:~/linuxptp# ./linuxptp/pmc -u -d24 'GET CURRENT_DATA_SET' sending: GET CURRENT_DATA_SET 000005.fffe.dd4a1c-0 seq 0 RESPONSE MANAGEMENT CURRENT_DATA_SET stepsRemoved 1 offsetFromMaster 0.0 meanPathDelay 171.0 root@ubuntu:~/linuxptp#</pre>		
Step_2	Synchronize the physical hardware clock (PHC) with the system clock. Server_OSPrompt:~# ./linuxptp/phc2sys -arm -f g8275_client.conf	<pre>rootQubuntu:-/linuxptp//hlc2sys -arm -f g8275_client.conf phC2sys[10534.84]: reconfiguring after point state change phC2sys[10534.84]: reconfiguring after point state change phC2sys[1053.84]: rotCXE_thering citeConfiguring after point state change phC2sys[1053.84]: rotCXE_textITHE phr offset 33308136708 s0 free +100000000 delay 743 phC2sys[1053.843]: rotCXE_textITHE phr offset 33308136708 s0 free +100000000 delay 743 phC2sys[1053.843]: rotCXE_textITHE phr offset -212 s2 free -2548 delay 830 phC2sys[1053.843]: rotCXE_textITHE phr offset 2022 s2 free -2548 delay 830 phC2sys[1053.843]: rotCXE_textITHE phr offset 2022 s2 free -3560 delay 832 phC2sys[1053.843]: rotCXE_textITHE phr offset 2028 s2 free +360 delay 838 phC2sys[1053.843]: rotCXE_textITHE phr offset 2028 s2 free +2127 delay 834 phC2sys[1053.843]: rotCXE_textITHE phr offset 2012 s2 free +1217 delay 834 phC2sys[1053.843]: rotCXE_textITHE phr offset 2012 s2 free +2127 delay 838 phC2sys[1054.845]: rotCXE_textITHE phr offset 213 s2 free +1217 delay 838 phC2sys[1054.845]: rotCXE_textITHE phr offset 213 s2 free +767 delay 838 phC2sys[1054.845]: rotCXE_textITHE phr offset 213 s2 free +358 delay 828 phC2sys[1054.845]: rotCXE_textITHE phr offset 213 s2 free +358 delay 828 phC2sys[1054.845]: rotCXE_textITHE phr offset 25 s2 free +368 delay 828 phC2sys[1054.845]: rotCXE_textITHE phr offset -25 s2 free +358 delay 828 phC2sys[1054.845]: rotCXE_textITHE phr offset -25 s2 free +358 delay 828 phC2sys[1054.845]: rotCXE_textITHE phr offset -25 s2 free +358 delay 838 phC2sys[1054.845]: rotCXE_textITHE phr offset -25 s2 free +358 delay 838 phC2sys[1054.845]: rotCXE_textITHE phr offset -25 s2 free +358 delay 838 phC2sys[1055.847]: rotCXE_textITHE phr offset -25 s2 free +358 delay 838 phC2sys[1055.847]: rotCXE_textITHE phr offset -25 s2 free +358 delay 838 phC2sys[1055.847]: rotCXE_textITHE phr offset -25 s2 free +358 delay 838 phC2sys[1055.847]: rotCXE_textITHE phr offset -25 s2 free +358 delay 838 phC2sys[1055.847]: rotCXE_textITHE phr offset -25 s2 free +358 delay 838 p</pre>		

Configuring synchronous Ethernet

Synchronous Ethernet (SyncE) (ITU-T G.8262) is supported along with the synchronization status message (SSM) over Ethernet Synchronization Message Channel (ESMC) as defined in ITU-T G.8264. To enable distribution of frequency to some or all ports, two ports should be chosen as SyncE sources. In this example, ports 1/1 and 1/2 will be used.

Prerequisite

1 A valid SyncE clock source from an external network equipment is needed.

Procedure

Log in to the switch NOS CLI. Refer to <u>Accessing the switch NOS</u> for access instructions.

Step_1	Enter configuration mode. LocalSwitchNOS_OSPrompt:~# configure terminal	NOS00A0A5DEE15C# configure terminal NOS00A0A5DEE15C(config)#
Step_2	Nominate ports 1/1 and 1/2 as clock synchronization sources and enable SSM on all ports to distribute status to other network elements. LocalSwitchNOS_OSPrompt:~# network-clock clk- source 1 nominate interface Ethernet 1/1 network-clock clk-source 2 nominate interface Ethernet 1/2 interface Ethernet 1/1-12 network-clock synchronization ssm	<pre>NOS00A0ASDEE15C(config)# net\$clk-source 1 nominate interface Ethernet 1/1 NOS00A0ASDEE15C(config)# net\$cck clk-source 2 nominate interface Ethernet 1/2 NOS00AAASDEE15C(config)# interface Ethernet 1/1-12 NOS00AAASDEE15C(config-if)# network-clock synchronization ssm NOS00AAASDEE15C(config-if)# </pre>
Step_3	End configuration. LocalSwitchNOS_OSPrompt:~# end	NOS00A0A5DEE15C(config-if)# end NOS00A0A5DEE15C#
Step_4	Verify the port status. LocalSwitchNOS_OSPrompt:~# show network- clock	NOS00A0A5DEE15C# show network-clock Selector State is: Locked to 1 Alarm State is: Clk: 1 2 3 LOCS: FALSE TRUE TRUE SSM: FALSE FALSE FALSE FALSE WTR: FALSE FALSE FALSE LOL: FALSE DHOLD: FALSE SSM State is: Interface Tx SSM Rx SSM Mode Ethernet 1/1 QL_DNU QL_PRC Master Ethernet 1/2 QL_LINK QL_LINK Master Ethernet 1/3 QL_PRC QL_FAIL Master Ethernet 1/4 QL_LINK QL_LINK Master Ethernet 1/6 QL_LINK QL_LINK Master Ethernet 1/7 QL_LINK QL_LINK Master Ethernet 1/6 QL_LINK QL_LINK Master Ethernet 1/7 QL_LINK QL_LINK Master Ethernet 1/8 QL_LINK QL_LINK Master Ethernet 1/9 QL_PRC QL_FAIL Master Ethernet 1/10 QL_LINK QL_LINK Master Ethernet 1/11 QL_LINK QL_LINK Master Ethernet 1/12 QL_LINK QL_LINK Master

Configuring UEFI/BIOS options

Table of contents

- <u>Configuring UEFI/BIOS options via the UEFI/BIOS menu</u>
 - <u>Changing the boot order</u>
 - Overriding the boot order
 - Enabling Secure Boot
 - Performing an HDD Security Freeze Lock
 - <u>Configuring the TPM</u>
 - <u>Configuring the server Power Control Policy</u>
 - <u>Configuring option Application Ready LED</u>
 - Disabling server access to the I210 Ethernet controller
- <u>Configuring UEFI/BIOS options via the BMC using Redfish</u>
 - Using the UEFI/BIOS attributes registry to modify configuration
 - <u>Specifying the next boot device</u>

Relevant section:

<u>Platform power management</u>

Options can be configured:

- Using the <u>UEFI/BIOS menu</u>
- Via the BMC using Redfish

Configuring UEFI/BIOS options via the UEFI/BIOS menu

Access the UEFI/BIOS. Refer to Accessing the UEFI or BIOS for access instructions.

Changing the boot order

Step_1	From the UEFI/BIOS setup menu, navigate to the ${\bf Boot}$ menu. Configure the	Aptio Setup Utility - Copyright (C) 2021 American Megatrends, Inc. < Security Boot Save & Exit			
	boot order as desired.	Boot Configuration Betup Fromp: Timeout Bootup NumLock State Control Control Outer Boot Optimized Boot Disabled Disabled Boot Option #1 Boot Option #2 Boot Option #2 CUEFI OS (NDC PC SNE2D SDAFTW-5126) Boot Option #2 CUEFI CS (NDC PC SNE2D SDAFTW-5126) Boot Option #2 CUEFI CS (NDC PC SNE2D SDAFTW-5126) Boot Option #2 CUEFI CS (NDC PC SNE2D SDAFTW-5126) File Control State File Control State Version 2.20.1271, Copyright (C) 2021 American Megatrends, Inc. AB			
Step_2	Select the Save & Exit menu, go to Save Changes and Reset and press Enter to confirm and save the new boot order.	<pre>< Security Boot Save & Exit Aptio Setup Utility - Copyright (c) 2020 American Megatrends, Inc. Save Ohanges and Exit Discard Changes and Exit Save changes Discard Changes and Reset Discard Changes and Reset Discard Changes Default Options Restore Defaults Restore Defaults Restore User Defaults UEFI: Previous Values UEFI: Prev Intel(R) I210 Gigabit Network Shell] Vific Save & Exit UFS: Restore Exit Connection Shell] Vific Save & Exit ESC: Exit</pre>			

Overriding the boot order

This is a non-persistent option to allow booting to a specific device while maintaining the normal boot order.

Step_1	Reboot the platform and access the UEFI/BIOS setup menu.		
Step_2	Navigate to the Save & Exit menu and then to the Boot Override section.	Aptio Setup Utility - Copyright (C) 2020 Ar < Security Boot Save & Exit Save Changes and Reset Discard Changes Default Options Restore Defaults Save as User Defaults Save as User Defaults Boot Override UEFI: PXE IP4 Intel(R) I210 Gigabit Network Connection UEFI: Built-in EFI Shell SSATA P2: M.2 (S80) 3WE4 USATA P2: M.2 (S80) 3WE4 USATA P2: M.2 (S80) 3WE4 USATA P2: M.2 (S80) 3WE4 Version 2.20.1271. Copyright (C) 2020 American Version 2.20.1271. Copyright (C) 2020 American Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean Sourcean	A A A A A A A A A A A A A A

Enabling Secure Boot

The following application notes are required to generate secure boot keys and configure them: <u>Generating custom secure boot keys</u> and <u>Provisioning custom secure boot keys</u>.

Step_1	Navigate to the Security tab and access the Secure Boot submenu.	Aptio Setup - American Megatrends International, LLC.
		The password length must be ' Secure Boot in the following range: + configuration Minimum length 3 + Maximum length 20 + Administrator Password + User Password + HDD Security Freeze [Enabled] + >: Select Screen Lock + >: Select Item HDD Security Configuration: + Fit General Help PONACCON_5200 MTFDDAK3TSTDC + Fit General Help Secure Boot + Fit General Help VFit Save 4 Exit ESC: Exit
Step_2	Select the Secure Boot option and change it to Enabled .	Aptio Setup - American Megatrends International, LLC. Security Secure Soct feature is System Mode User Secure Boot International, LLC. Key Management International, LLC. Secure Secure International, LLC.
Step_3	Use the application notes mentioned above as reference to generate and cor	nfigure secure boot keys.
Step_4	Navigate to the Save & Exit menu, go to Save Changes and Exit and press Enter to confirm.	Actio Setup Utility - Dopyright (C) 2019 American Megatrends, Inc. 4 Security Boot Save & Exit Save Changes and Exit Discard Changes and Reset Discard Changes Discard Changes Discard Changes Discard Changes Discard Changes Discard Changes Discard Changes Save Balics Save Befaults Save as User Defaults Restore User Defaults Restore User Defaults Boot Override UEFI: PNE IP4 Intel(R) Ethernet Connection X722 for 100BASE-T Version 2.20.1276. Copyright (C) 2019 American Megatrends, Inc. AB

Performing an HDD Security Freeze Lock

Step 1	Navigate to the Security tab, and enable or disable the HDD Security Freeze	Aptio Setup Utility - Copyright (C) 2021 American Megatrends, Inc.
5.0021	Lock .	have Administrator rights. The password length must be in the following range: Minimum length 3 Maximum length 20 + ito Dis needs Power Cycle Administrator Password User Password Doser Password MD Security Freese [Enabled] HDD Security Configuration: HDD Security Configuration: HDD Security Configuration: P2:ML2(S0) 3ME WDC PC SNS0 SDAFUW-5126 + iff: General Reip > Secure Boot > Secure Boot > Secure Flash Dyate Version 2.20.1571. Copyright (C) 2021 American Megatrends, Inc.
Step_2	Navigate to the Save & Exit menu, go to Save Changes and Exit and press Enter to confirm.	Actio Setuo Utility - Copyright (C) 2019 American Negatrends, Inc.

Configuring the TPM

Step_1	Navigate to the Advanced menu, go to Trusted Computing and then Security Device Support. Verify that it is set to Enable . Possible values: [<u>Enable</u> /Disable] NOTE: The TPM has to be inserted to see the menu.	Aptio Setup - American Megatrends International, LLC. Advanced TREGO Device Found Firmwate Version: 7,62 Vendor: IFX Support Advanced Available PCR banks SHA-1, STRA-1, STRA-1, STRA-56 SHA-1, STRA-1, STRA-1, STRA-56 STRA-1, STRA-1, STRA-1, STRA-1, STRA-1, STRA-56 STRA-1, STRA-1, STRA-1, STRA-1, STRA-56 STRA-1, STRA-1,
Step_2	From the Advanced menu and the Trusted Computing section, select TPM2.0 UEFI Spec Version and set the applicable spec. Possible values: [TCG_1_2 / <u>TCG_2</u>] NOTE: The TPM has to be inserted to see the menu.	Aptio Setup - American Megatrends International, LLC. Advanced Active FCR banks SHA-1,SH3256 ()Select the TGG2 Spec () Available FCR banks SHA-1,SH3256 ()Select the TGG2 Spec () SHA-1 FCR Bank [Enabled] + TGG 1.2: the Compatible * SHA-1 FCR Bank [Enabled] + TGG 1.2: the Compatible * SHA-1 FCR Bank [Enabled] + TGG 2: Support net TGG2 + Pending operation [None] + TGG 2: Support net TGG2 + Flatform Hierarchy [Enabled] + TGG 2: Support net TGG2 + Storage Hierarchy [Enabled] + TGG 2: Support net TGG2 + Todate Metric Select (Internet to the term of the term of the term of term of term of the term of term
Step_3	From the Advanced menu and the Trusted Computing section, select Device Select and set the applicable device. Possible values: [TPM 1.2 / TPM 2.0 / <u>Auto</u>] NOTE: The TPM has to be inserted to see the menu.	Aptio Setup - Aserican Megatends International, LLC. Advanced Active FCR banks SHA-1,SHA256 'ITPM 1.2 will restrict ' Available FCR banks SHA-1,SHA256 'I support to TFM 1.2 will restrict ' SHA-1 FCR Bank [Enabled] '12.0 devices, THM 2.0 will ' SHA-1 FCR Bank [Enabled] '12.0 devices, Auto will ' Patient's support both with the ' Patient's migrachy [Enabled] '12.0 devices, Auto will ' Patient's both with the ' Patient's both with ' Patient's both with the ' Patient's both with ' Pat
Step_4	Navigate to the Save & Exit menu, go to Save Changes and Exit and press Enter to confirm.	Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc. Image: Sever & EXIT Save Changes and Exit Discard Changes and Exit Save Changes and Reset Discard Changes and Reset Discard Changes Default Options Restore Defaults Restore Defaults Boot Override UEF1: PXE IP4 Intel(R) Ethernet Connection VT22 for JOBRSE-T Vtrsion 2.20,1276. Copyright (C) 2019 American Megatrends, Inc.

Configuring the server Power Control Policy

This option is used to configure the system's response to a system input power loss.



Configuring option Application Ready LED

This option changes the behavior of the green power LED. Refer to <u>Platform components</u> for behavior information. Refer to <u>Platform resources for</u> <u>customer application</u> for information on how to control this behavior from your application.

Step_1	Navigate to the Boot menu, and enable or disable the OS App. Ready Led	Aptio Setup Utility - Copyright (C) 2021 American Megatrends, Inc. < Security Boot Save & Exit			
	Control given to the UEFI/BIOS.	Beet Configuration Secure Frage Timbot Bootay Numbook State Ontaria Quiet Boot Optimized Boot Deable Foot USB Boot Boot Option #1 Boot Option #2 Not Option #2	1 [On] [Cambled] [Diamled] [Diamled] [Diamled] [OEFI OS (MOC PC SH500 SSAFTON-5120]) [CEFI F RS: TM Intel(R) I110 Gigabit Network Connection]	<pre>* Sender/Dischle the * control of the 05 App * Ready Control by BIOS. * * * * * * * * * * * * * * * * * * *</pre>	

Disabling server access to the I210 Ethernet controller

Ctor 1	Noviente te the Distform Configuration tob and so to item DCU Devices	Platform Configuration	
Step_1		PCH Configuration > PCH Soft Devices > PCI Express Configuration > PCH SATA Configuration > PCH SATA Configuration > VSS Configuration > Security Configuration > Tracethy Configuration > PLatform Thermal Configuration > PCH DRA Configuration	Enable/Disable Intel(R) 10 Controller Hub devices ><: Select Screen Tv: Select Item Enter: Select Item Enter: Select Item F2: Previous Values F2: Optimized Defaults F3: Optimized Defaults
Step_2	Navigate to device I210 Enable/Disable and select Disable . This will effectively disconnect the I210 Ethernet controller from the server.	Aptio Setup Dility - Copyright (C) 2021 American Setup Dility (DeepSs) Board Capability (DeepSs) DeepS Power Folic (Disable) (C27 Wake From DeepSu (Disable) (D-APIC 24-119 KTE (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disable) (Disabl	TION Repairends, Inc. TIDE Enable/Disable TIDE Enable/Disable TIDE Enable/Disable TIDE Enable/Disable TIDE Enable TIDE Enable TI

Configuring UEFI/BIOS options via the BMC using Redfish

Most of the UEFI/BIOS options available in the UEFI/BIOS menu can be modified using the Redfish interface. To perform these operations, some understanding of the Redfish schema and process is required.

- UEFI/BIOS Redfish resources might not be present after a BMC reboot or update. If so, reboot or power on the platform in order to fill the registries.
- All changes made using Redfish are pending until the next platform resets. Reset the platform in order to apply the changes.

Relevant sections: Accessing a BMC using Redfish Platform power management

Using the UEFI/BIOS attributes registry to modify configuration

This section describes how to use the UEFI/BIOS attributes registry to modify the configuration using the BMC as an intermediate. The UEFI/BIOS registry is used as a guide to get all the details about the UEFI/BIOS configuration attributes.

There are two steps to changing a UEFI/BIOS option:

- 1. Collect the option information
- 2. Change the option

Obtaining the UEFI/BIOS attributes registry

Step_1	<pre>Find the value of the PRODUCT_ID and UEFI_VERSION attributes required for the command in step_2. RemoteComputer_OSPrompt:~# curl -k -srequest GETurl [ROOT_URL] /redfish/v1/Registries/ jq In this example: PRODUCT_ID = 10027 UEFI_VERSION = 1.2.0</pre>
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1/Registrie { "@odata.id": "/redfish/v1/Registries", "Description": "Collection of MessageRegistryFileCollection", "Description": "Collection of MessageRegistryFileS", "Members": [</pre>
Step_2	Get the attributes registry. RemoteComputer_OSPrompt:~# curl -k -srequest GETurl [ROOT_URL] /redfish/v1/Registries/BiosAttributeRegistry[PRODUCT_ID].[UEFI_VERSION].json jq \$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1/Registrie s/BiosAttributeRegistry10027.1.2.0.json jq [] NOTE: The output of this command is quite large and may be more useful directed into a local file. The curl option -o,output [FILE_NAME] can be used to do this.

Here is an example of a UEFI/BIOS attribute configuration definition in the registry.

{
"AttributeName": "TCG003",
"DefaultValue": "Enable",
"DisplayName": " Security Device Support",
"HelpText": "Enables or Disables BIOS support for security device. 0.5. will not show Security Device. TCG EFI protocol and INT1A interface will
not be available.",
"ReadOnly": false,
"ResetRequired": true,
"Type": "Enumeration",
"UefiNamespaceId": "x-UEFI-AMI",
"Value": [
{
"ValueDisplayName": "Disable",
"ValueName": "Disable"
},
{
"ValueDisplayName": "Enable",
"ValueName": "Enable"
}
]
}.

Where:

AttributeName is the UEFI/BIOS internal name of the configuration attribute. This is a unique identifier used to read or modify this specific attribute (see below).

DefaultValue is the default value of the attribute.

HelpText is the text describing the attribute. It is the exact same help text found in the UEFI/BIOS menu.

ReadOnly indicates if the attribute is read only.

ResetRequired specifies if a CPU reset is required to apply this attribute.

Type specifies the type of the attribute. Available types are: Enumeration, Boolean, String, Integer .

Value is optional and is used for the Enumeration attribute type. It contains a list of values available for the attribute.

Obtaining the current UEFI/BIOS configuration

At each boot, the UEFI/BIOS firmware sends its current UEFI/BIOS configuration to the BMC. If the UEFI/BIOS is configured from another source (for example, the UEFI/BIOS menu), the updated UEFI/BIOS options are sent automatically to the BMC.



Provisioning new UEFI/BIOS configuration

To modify the current UEFI/BIOS configuration, a pending configuration object needs to be created in Redfish. This pending configuration will be applied at next boot and then deleted.

Step_1	Make sure the server has been booted at least once. This is to ensure that the UEFI/BIOS configuration is synchronized between the BMC and the UEFI/BIOS .				
Step_2	Send new UEFI/BIOS attribute(s). RemoteComputer_OSPrompt:~# curl -k -srequest POSTurl [ROOT_URL] /redfish/v1/Systems/ system /Bios/SD header 'Content-Type:application/json'data '{ "[ATTRIBUTE_NAME]": [NEW_SETTING], "[ATTRIBUTE_NAME]": [NEW_SETTING] }' jq NOTE: All the attributes available can be modified in the same command. In this example, two UEFI/BIOS settings are changed. NOTE: The values for [NEW_SETTING] must be a taken from the possible values specified in the registry according to the type of the attribute (Enumeration, Boolean, String, Integer).				
	<pre>\$ curl -k -srequest POSTurl https://admin:ready2go@172.16.182.31/redfish/v1/Systems/ system/Bios/SDheader 'Content-Type:application/json'data '{"ACPI003": true,"ACPI004" ; true)' jq { "@Message.ExtendedInfo": [{ "@odata.type": "#Message.v1_1 1.Message", "MessageArgs": [], "MessageId": "Base.1.8.1.Success", "MessageId": "Base.1.8.1.Success", "MessageSeverity": "OK", "Resolution": "None" } } } </pre>				
Step_3	Reboot the server and wait for the reboot to be completed. This will synchronize the new pending UEFI/BIOS configurations with the UEFI/BIOS.				
Step_4 Validate the UEFI/BIOS attributes are properly modified by viewing the current UEFI/BIOS settings. RemoteComputer_OSPrompt:~# curl -k-srequest GETurl [ROOT_URL] /redfish/v1/Systems/system/list					
	NOTE: The pending configuration at /redfish/v1/Systems/ system /Bios/SD will be removed at the end of the configuration process.				
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1/Systems/s yetem/Bios [jq</pre>				

Specifying the next boot device



Configuring and managing users

- <u>Configuring and managing BMC users</u>
- Configuring and managing switch NOS users

Configuring and managing BMC users

Table of contents

- Privilege levels
- <u>Configuring user names and passwords</u>
 - Using the Web UI
 - Using Redfish
 - Using IPMI
- <u>Adding a user</u>
 - Using the Web UI
 - <u>Using Redfish</u>
 - Using IPMI
- Deleting a user
 - Using the Web UI
 - <u>Using Redfish</u>

 - <u>Using IPMI</u>
- Configuring privilege level
 - Using the Web UI
 - Using Redfish
 - Using IPMI



It is recommended to change the administrator password immediately after accessing the Web UI.

Privilege levels

This section describes the permissions associated with the different privilege levels in the BMC Web UI and Redfish.

Roles		Description					
BMC Web UI and Redfish	IPMI						
Admin	0x4 - Administrator	Users are allowed to configure everything regarding the BMC (including user management and network configuration). Users will have full administrative access.					
Operator	0x3 - Operator	Users are allowed to view and control basic operations. This includes rebooting of the host. Users are not allowed to change anything regarding user management and network configuration. Users can change their own passwords.					
User	0x1 - Callback	Users only have read access and can't change any behavior of the system. Users can change their own passwords.					
No-Access	0xF - No Access	Users with this privilege level will not have access to the BMC.					

Configuring user names and passwords

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.

Using the Web UI

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

Step_1	From the left-side menu, click on Security and access and then on User management .	€ kontron III Overview E Logs III Hardware status Coperations	Health ● Power			
		Settings Citl network setting Setsions LDAP User management Policies Certificates	ps → SOL console → tion Server information Mosel Manufacturer ME1210 Kontron Seral number UEF version 9017064072 1.02.09579455			
Step_2	Select the user to manage from the User management section.	User management				
		Username Privilege	Status			
		admin Administrator	Enabled 🖉 🔟			
		myuser Administrator	Enabled			
		✓ View privilege role descriptions				
Step_3	Change the username and/or the password and confirm modifications by clicking on Save .	Edit user	×			
	NOTE: The password needs to be updated to update any other parameter.	Account status Enabled Disabled Username Cannot start with a number No special characters except underscore Myuser Privilege	User password Password must be between 8 – 20 characters Confirm user password			
		Administrator \$	Cancel Save			

Using Redfish

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

Step_1	List the users available. RemoteComputer_OSPrompt:~# curl -k -srequest GETurl [ROOT_URL]/redfish/v1/AccountService/Accounts jq
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1/AccountSe rvice/Accounts jq { "@odata.id": "/redfish/v1/AccountService/AccountCollection", "Description": "BMC User Accounts", "Members": [{</pre>
Step_2	Change the password.
	RemoteComputer_OSPrompt:~# curl -k -srequest PATCHurl [ROOT_URL] /redfish/v1/ AccountService/Accounts/ [USERNAME]header 'Content-type: application/json'data '"{"Password":" [NEW_ PASSWORD] ", "UserName":" [NEW_USERNAME] "}"' jq
	<pre>\$ curl -k -srequest PATCHurl https://admin:ready2go@172.16.182.31/redfish/v1/Account Service/Accounts/myuserheader 'Content-Type: application/json'data '"{"Password": "P assword7890!", "UserName": "myuser2"}" jq</pre>

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] -C 17.

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]	<pre>[root@localhost ~]# ID Name 1 2 admin 3 user 4 5 6 7 8 9 10</pre>	ipmitoo Callin false false true true true true true true true	l user list Link Auth false false false false false false false false false false	1 IPMI Msg true true 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	Identify the ID number of the user to be changed.	[root0localhost ~]# ID Name admin admin user 4 5 6 7 8 9 10	ipmitoo Callin false false true true true true true true true	l user list Link Auth false false false false false false false false false false	1 IPMI Msg true true 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_3	Change the user name. LocalServer_OSPrompt: ~# ipmitool user set name [IPMI user ID] NOTE: The first and second user names of the user list are reserved f	[new IPMI use ields and therefo	r nam ore car	e] ''t be mo	dified.		
Step_4	Verify that the user name has updated correctly by printing the user list. LocalServer_OSPrompt:~# ipmitool user list [LAN_CHANNEL]	<pre>[rootBlocalhost ~]# ID Name 1 2 admin 3 operator 4 5 6 7 8 9 9 10</pre>	ipmitool Callin false false true true true true true true true tru	user list 1 Link Auth 1 false 1 false 1 false 1 false 1 false 2 false 2 false 2 false 2 false 2 false 2 false 3	IPNI Nag Drue Drue 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	
Step_5	Change the password. LocalServer_OSPrompt: ~# ipmitool user set password [IPMI user ID] [new IPMI password]	[rootθlocalhost Set User Passwor	~]# ipm d comma	itool use: nd succes:	r set pas sful (use	sword 3 newpassword r 3)	

Adding a user

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.**

Using the Web UI

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

Char 1	Event the left eide menu elisters Committee and	Rentron I Dated	admin
step_1	access and then on User management .		y deman *
		E togs	
		Coperations Coperatio	
		Settings ∨ Edit network settings → SOL console →	
		Sessions BMC information Server information	
		LDAP Firmware version Model Manufact User management	rer
		Policies Serial number UEF vers 9017064072 1.02.095 Certificates	in 9455
Step_2	Click on Add user .	User management	
		🕄 Account policy settings 🖉 Ad	Luser
		Username Privilege Status	user
		🗌 admin Administrator Enabled 🖉	Ū
		myuser Administrator Enabled	Ū
Stop 3	Fill the required fields and click on Add user		
preh_p		Add user	×
		Account status User password	
		Enabled Password must be between 8 20 characters	-
		Uisabled	0
		Username	
		Cannot start with a number No special characters excent Confirm user password	
		underscore	
		myuser	
		Privilege	
		Administrator 🗢	
		Cancel Add us	er

Using Redfish

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



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] -C 17.

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@iocalhost ~]# 1 2 admin 4 5 6 7 8 9 10	ipmitoo: Callin false false true true true true true true true tru	user list Link Auth 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			
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 pas	swor	1]					
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 a user

Using the Web UI

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

Step_1 From the left-side menu, click on Security and access and then on User management .	E Cverview E Logs Hardware status ************************************	Overview BAC time 2021-11-23 172400 UTC Toft network settings BMC information Formary version 2000159fce6	 e Health e Power Server LED Off off SOL console Server infor Model M61219 Serial number 9017064072 	Refresh ® admin → → mation Mandeturer Konteen UEF version 1.02.09579455
Step_2 Select the user to delete from the User management section.	User mana Username admin myuser	Agement Privilege Administrator Administrator descriptions	Account policy settings Status Enabled Enabled	Add user

Using Redfish

Refer to Accessing a BMC using Redfish for access instructions.

Step_1	List the privilege levels available. RemoteComputer_OSPrompt:~# curl -k -srequest GETurl [ROOT_URL]/redfish/v1/AccountService/Roles jq
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1/AccountSe rvice/Roles jq { "@odata.id": "/redfish/v1/AccountService/Roles", "@odata.id": "SoleCollection.RoleCollection", "members": [{</pre>
Step_2	Change the privilege level. RemoteComputer_OSPrompt:~# curl -k -srequest PATCHurl [ROOT_URL]/redfish/v1/AccountService/Accounts/ [USER_ID]header 'Content-type: application/json'data '"{"RoleId":" [ROLE] "}" jq
	<pre>\$ curl -k -srequest PATCHurl https://admin:ready2go@172.16.182.31/redfish/v1/Account Service/Accounts/myuserheader 'Content-Type: application/json'data '"{"RoleId": "Adm inistrator"}** jq { "@Message.ExtendedInfo": [{ "@Message.trgs": I]. "Message: "Successfully Completed Request", "Message: "Successfully Completed Request", "Message: "Successfully Completed Request", "MessageSeverity": "OK", "Resolution": "None" } }</pre>

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] -C 17.

Users can't be deleted using ipmitool . However, they can disabled.

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@localhost ~]# ID Name 1 2 admin 3 4 5 6 7 8 9 10	ipmitool Callin false false true true true true true true true tru	user list Link Auth false false false false false false false false false false	1 IPMI Msg true 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 fie	elds and therefore	can't b	e disablec	Ι.	

Configuring privilege level

Using the Web UI

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

Step_1	From the left-side menu, click on Security and access and then on User management .	Skontron Image: Health Power C Refresh Image: Admin - Image: Overview Overview
		Logi v
		BMC time Server LED Coperations 2021-11-23 17:24:00 UTC Off
		Settings ∨ Edit network settings → SOL cansole →
		Security and access
		Sessions BMC information Server information
		User management
		Policies Serial number UEF version 9017064072 1.02.09579455
		Letinicare
Step_2	Select the user to manage from the User management section.	User management
		Add user
		Username Privilege Status
		admin Administrator Enabled 🖉 📋
		nyuser Administrator Enabled
		\sim View privilege role descriptions
Step_3	Change the privilege level fields as well as the password and confirm the configuration by clicking on the Save button.	Edit user ×
		Account status
		Enabled Password must be between 8 –
		Disabled 20 characters
		0
		Username
		Cannot start with a number
		No special characters except
		(Multiscole)
		myuser
		Privilege
		Administrator 🗢
		Cancel Save

Using Redfish

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



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] -C 17.

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 ~]f TD Name 1 admin 3 4 5 5 7 8 9	<pre>ipmitool Callin false false true true true true true true true</pre>	Luser list Link Auth false false false false false false false false false	1 IPMI Msg true 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
Step_2	List the privilege levels available. LocalServer_OSPrompt:~# ipmitool channel help	Channel Commandas authoap (c) getaccess (c) setaccess (c) getaccess (c) getky (c) getky (c) setky (c) setky (c) setky (c) defined (c) defi	Urue mannel number> mannel number> mannel number> mannel number} mani skey> [chan	<pre>idise (max privilege> (use: id) (use: id> [callin= annel] nel]</pre>	on off] [ipmi-on	NG RULESS
Step_3	Set the privilege level for each channel.	ואבו 1 (ווכבס וס)	معادينا م	~~_{000		בעבו

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 and managing switch NOS users

Table of contents

- Configuring switch NOS users using the switch NOS command-line interface
- <u>Configuring switch NOS users using the switch NOS Web UI</u>
 - <u>Changing the password of a user</u>
 - <u>Adding a user</u>
 - Deleting a user
 - <u>Configuring privilege level</u>

i

Changes to the switch configuration are not persistent after rebooting the switch.

- To preserve configurations, the current configuration needs to be saved to startup-config.
 - From the switch Web UI:
 - Select Maintenance, Configuration and then Save startup-config. Click on Save Configuration to confirm the change. From the switch CLI:
 - LocalSwitchNOS_OSPrompt:~(config-if)# end
 - LocalSwitchNOS_OSPrompt:~# copy running-config startup-config

Configuring switch NOS users using the switch NOS command-line interface

Refer to Accessing the switch NOS for access instructions.

To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the CLI</u>. **NOTE:** If the switch NOS configuration is restored to default, the administrator password will be reset.

Step_1	Access the configuration setup menu. LocalSwitchNOS_OSPrompt:~# configure terminal	# configure terminal
Step_2	Configure the user. LocalSwitchNOS_OSPrompt:~(config)# username [USERNAME] privilege [PRIVILEGE_LEVEL] password unencrypted [PASSWORD] NOTE: The username is only used to identify the user and therefore can't be changed.	(config)# username user privilege 15 password unencrypted newPassword
Step_3	(Optional) To make the change persistent, save running-config to startup-config.	

Configuring switch NOS users using the switch NOS Web UI

Refer to Accessing the switch NOS using the Web UI for access instructions.

Changing the password of a user

To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the Web</u> <u>UI</u>.

Step_1	From the left-side menu, select Configuration , Security , Switch and then Users .	
Step_2	Click on the desired user.	> System Users Configuration • Green Ethemet • Thermal Protection • Ports • CFM • APS • APS • ERPS • DHCPv4 • DHCPv4 • DHCPv4 • DHCPv6 • Switch • Switch • Users • Privilege Levels • Auth Method • SH • HTTPS • Access Management • SMMP • RMON • Network • AAA
Step_3	Change the value of the Change Password dropdown menu to yes .	Edit User User Settings User Name myuser
Step_4	Enter the password in both fields (Password and Password (again)).	Change Password Yes Password Password Password Password Pivilege Level 15 V
Step_5	Click on the Save button to confirm.	Save Reset Cancel Delete User
Step_6	(Optional) To make the change persistent, save running	-config to startup-config.

Adding a user

To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the Web</u> <u>UI</u>.

Step_1	From the left-side menu, select Configuration , Security , Switch and then Users .	
Step_2	Click on the Add New User button.	 System Green Ethernet Thermal Protection Ports CFM APS ERPS DHCPv4 DHCPv4 DHCPv6 Security Switch Users Auth Method SSH HTTPS Access Management SNMP RMON Network AAA
Step_3	Fill the required fields: User Name , Password , Password (again) and Privilege Level . NOTE: For more information on the different privilege levels, click on the help button located at the top-right corner of the switch Web UI page.	Add User User Name myuser Password Password (again) Privilege Level 15 Save Reset Cancel
Step_4	Click on the Save button to add the user.	
Step_5	A new user should be displayed in the user list.	Users Configuration User Name Privilege Level admin 15 mysseg 15 Add New User
Step_6	(Optional) To make the change persistent, save running	-config to startup-config.

Deleting a user

To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the Web</u> <u>UI</u>.

Step_1	From the left-side menu, select Configuration , Security , Switch and then Users .	
Step_2	Click on the desired user.	> System > Green Ethernet - Thermal Protection > Ports > CFM - APS - APS > DHCPv4 > DHCPv6 > Security ▼ Switch - Number of State - Auth Method - SSH - HTTPS - Access Management > SNMP - RMON > Network
Step_3	Click on the Delete User button.	Edit User User Settings User Name myuSer Change Password No Privilege Level 15 Save Reset Cancel Delete User
Step_4	The user should be removed from the user list.	Users Configuration User Name Privilege Level admin 15 Add New User
Step_5	(Optional) To make the change persistent, save running	g-config to startup-config.

Configuring privilege level

To preserve configurations, the current configuration needs to be saved to startup-config. Refer to <u>Saving the current configuration using the Web</u> <u>UI</u>.

Step_1	From the left-side menu, select Configuration , Security , Switch and then Users .	
Step_2	Click on the desired user.	 System Green Ethernet Thermal Protection Ports CFM APS ERPS DHCPv4 DHCPv4 DHCPv4 DHCPv6 Security Switch Users Add New User
Step_3	Change the privilege level using the dedicated dropdown menu. NOTE: For more information on the different privilege levels, click on the help button located at the top-right corner of the switch Web UI page.	Edit User User Name myuser Change Password No V Privilege Level 15 V Save Reset Cancel Delete User
Step_4	Click on the Save button to confirm.	
Step_5	(Optional) To make the change persistent, save running	-config to startup-config.

Configuring sensors and thermal parameters

Table of contents

- Performing configurations using Redfish
 - <u>Configuring sensor thresholds</u>
 - Configuring minimum fan speed
 - Configuring maximum fan speed
 - Configuring a threshold offset
 - <u>Configuring a start point offset from threshold</u>
 - <u>Configuring the minimum ambient temperature</u>
- Performing configurations using IPMI
 - <u>Configuring thresholds</u>

NOT	CE	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.
	Chang	es made to thermal parameters will be lost when the BMC is upgraded. However, they are persistent upon rebooting the BMC.
	The inf should • Tem • Tem • Tem • Tem • Tem	Formation provided in this section is to configure sensors related to the end user PCIe add-in cards. Only the following sensors I be configured by the end user: np PCIe 1 mbox np PCIe 1 np PCIe 2 np PCIe 2 np Chassis
Rofor to	Installir	og a thermal probe for the PCIe add-in card for installation information and to Platform resources for customer application for

Refer to Installing a thermal probe for the PCIe add-in card for installation information and to <u>Platform resources for customer application</u> for code to integrate into the application to communicate customer-specific sensor information to the BMC. For more information on sensors, refer to the <u>Sensor list</u>. For event data interpretation instructions, refer to <u>Interpreting sensor data</u>.

There are several methods to configure platform sensors, including:

- Using Redfish
- Using <u>IPMI</u>

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



Performing configurations using Redfish

Relevant sections:

Accessing the BMC using Redfish

Creating URLs and Sensor list (for the URLs required to change thresholds and the SENSOR_NAME)

Configuring sensor thresholds

Refer to <u>Accessing a BMC using Redfish</u> for access instructions. **NOTE:** Sensor thresholds that are not populated by default can neither be populated nor configured.

Step_1	Identify the URL to use in order to change the thresholds and the sensor name.
Step_2	Change the threshold value of the desired sensor. RemoteComputer_OSPrompt:~# curl -k -srequest PATCHurl [ROOT_URL]/redfish/v1/[SENSOR_URL]header 'Content-Type: application/json'data '{ "[RESOURCE]": [{"MemberId": "[SENSOR_NAME]", "[THRESHOLD]": [VALUE]}] }' jq Supported values for parameter [THRESHOLD] are: • LowerThresholdCritical • LowerThresholdNonCritical • UpperThresholdNonCritical • UpperThresholdNonCritical To modify customer-specific PCIe add-in card related sensors, the value for parameter [RESOURCE] is: • Temperatures
	<pre>\$ curl -k -srequest PATCHurl https://admin:ready2go@172.16.182.31/redfish/v1/Chassis/ME121 0 Baseboard/Thermalheader 'Content-Type:application/json'data '{"Temperatures": [{"MemberI d": "TempPOIe_1", "UpperThresholdNonCritical": 77}]}' jq { "@odata.id": "/redfish/v1/Chassis/ME1210 Baseboard/Thermal", "@odata.type*: "#Thermal.v1_4_0.Thermal", "Frans": [], "Idd: "Thermal", "Temperatures": [] }</pre>

Configuring minimum fan speed



Minimum fan speed should never be under 30%.

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

Step_1	Set minimum fan speed. RemoteComputer_OSPrompt:~# curl -k -srequest PATCHurl [ROOT_URL]/redfish/v1/Managers/bmcheader 'Content-Type: application/json'data '{ "Oem": { "OpenBmc": {"Fan": {"FanControllers": {"Fan_Controller": {"OutLimitMin": [MINIMUM_FAN_SPEED]}}}) jq
	<pre>\$ curl -k -srequest PATCHurl https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc header 'Content-Type:application/json'data '{"Oem": {"OpenBmc": {"Fan": {"FanControllers": {"Fan_Controller": {"OutLimitMin": 30.0}}}}) jq</pre>

Configuring maximum fan speed

The maximum fan speed cannot be set over 100%. A value of less than 100% can affect system performance and operating temperature range.

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

Step_1	Set maximum fan speed. RemoteComputer_OSPrompt:~# curl -k -srequest PATCHurl [ROOT_URL]/redfish/v1/Managers/bmcheader 'Content-Type: application/json'data '{ "Oem": { "OpenBmc": {"Fan": {"FanControllers": {"Fan_Controller": {"OutLimitMax": [MAXIMUM_FAN_SPEED]}}}}) jq
	<pre>\$ curl -k -srequest PATCHurl https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc header 'Content-Type:application/json'data '{"Oem": {"OpenBmc": {"Fan": {"FanControllers": {"Fan_Controller": {"OutLimitMax": 90.0}}}}} / jq</pre>

Configuring a threshold offset

A threshold offset is an offset applied to the Upper non-critical and Upper critical thresholds to start the fans before getting to the actual threshold. This ensures events are not send for nothing near threshold values. Refer to <u>Accessing a BMC using Redfish</u> for access instructions.

Step_1	Set a threshold offset. RemoteComputer_OSPrompt:~# curl -k -srequest PATCHurl [ROOT_URL]/redfish/v1/Managers/bmcheader 'Content-Type: application/json'data '{"Oem": {"OpenBmc": {"Fan": {"LinearControllers": {" [SENSOR_ID] ": {"ThresholdOffset": [VALUE] }}}}) ' jq NOTE: The ThresholdOffset value must be negative.
	<pre>\$ curl -k -srequest PATCHurl https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc header 'Content-Type:application/json'data '{"Oem*: {"OpenBmc": {"Fan*: {"LinearControllers ": {"Temp_PCIe_1": {"ThresholdOffset":-3}}}}); jq</pre>

Configuring a start point offset from threshold

A start point offset from threshold is an offset applied to the "Upper non-critical + Threshold offset" to start the fans at a lower temperature value. This ensures a smoother curve from minimal fan speed before getting to the Upper non-critical threshold.

Step_1	Set a start point offset from the threshold. RemoteComputer_OSPrompt:~# curl -k -srequest PATCHurl [ROOT_URL]/redfish/v1/Managers/bmcheader 'Content-Type: application/json'data '{"Oem": {"OpenBmc": {"Fan": {"LinearControllers": {"[SENSOR_ID]": {"StartPointOffsetFromThreshold": [VALUE]}}}}) NOTE: The StartPointOffsetFromThreshold value must be negative.
	<pre>\$ curl -k -srequest PATCHurl https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc header 'Content-Type:application/json'data '{"0em": {"OpenBmc": {"Fan": {"LinearControllers ": {"Temp_PCIe_1": {"StartPointOffsetFromThreshold": -9}}}}}' jq</pre>

Configuring the minimum ambient temperature

For information on the functionalities linked to the minimum ambient temperature, refer to <u>Platform cooling and thermal management</u>. The minimum ambient temperature is the Temp Inlet sensor value at which fans will start running at minimum speed. Below this value, fans are stopped so the heater can do its work in a cold environment. Refer to <u>Accessing a BMC using Redfish</u> for access instructions.

 Step_1
 Set the minimum ambient temperature.

 RemoteComputer_OSPrompt:~# curl -k -s --request PATCH --url [ROOT_URL]/redfish/v1/ Managers/bmc --header

 'Content-Type: application/json' --data '{ "Oem": {"OpenBmc": {"Fan": {"FanControllers": {"Fan_Controllers": {"Fan_Controll

Performing configurations 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] -C 17.

Configuring thresholds

Step_1	From a remote computer that has access to the server OS through SSH, RDP or the platform serial port, c hange the threshold value of the desired sensor. LocalServer_OSPrompt:-# ipmitool sensor thresh " [SENSOR_ID]" [THRESH_TYPE] [VALUE] Supported THRESHOLDS are: • unr = upper non-recoverable • ucr = upper non-recoverable • ucr = upper non-critical • lnc = lower non-critical • lcr = lower critical	\$ ipmitool sensor thresh "Temp BMC" ucr 180 Locating sensor record 'Temp BMC' Setting sensor "Temp BMC" Upper Critical threshold to 180,000
	 lcr = lower critical lnr = lower non-recoverable 	

Operating

- Platform power management
- <u>Monitoring</u>
 - <u>Monitoring sensors</u>
 - <u>Sensor list</u>
- <u>Maintenance</u>
 - <u>System event log</u>
 - Interpreting sensor data
 - <u>Component replacement</u>
 - <u>Backup and restore</u>
 - <u>Upgrading</u>
- Platform cooling and thermal management

Platform power management

Table of contents

- Power management using the BMC Web UI
- Power management using Redfish
- Power management using IPMI over LAN (IOL)
- Rebooting the BMC using the Web UI
- <u>Rebooting the BMC using Redfish</u>
- <u>Rebooting the switch NOS</u>

A power action command can be executed using:

- The <u>BMC Web UI</u>
- <u>Redfish</u>
- IPMI over LAN

Power management using the BMC Web UI

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

Step_1	List every power action command. RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -C 17 chassis power	<pre>\$ ipmitool -I lamplus -H 172.16.182.31 -U admin -P ready2go -C 17 chassis power Chassis Commands: status power.policy, restart_cause poh, identify, selftest, bootdev, bootparam, bootmbox</pre>
Step_2	Execute the power action command from the commands listed. RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -C 17 chassis power [POWER_ACTION]	\$ ipmitool -I lanplus -H 172.16.182.31 -U admin -P ready2go -C 17 chassis power off Chassis Fower Control: Down/Off
Step_3	Verify the power status. RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -C 17 chassis power status	\$ ipmitool -I lanplus -H 172.16.182.31 -U admin -P ready2go -C 17 chassis power status Chassis Power is off

Power management using Redfish

Refer to Accessing a BMC using Redfish for access instructions.

Step_1	<pre>Execute the following command to manage platform power. RemoteComputer_OSPrompt:~\$curl -k -srequest POSTurl [ROOT_URL]/redfish/v1/ Systems/system/Actions/ComputerSystem.Resetheader 'Content-Type: application/json'data '{"ResetType":"[POWER_ACTION]"}' jq Supported values for parameter [POWER_ACTION] are: • On • ForceOff • ForceOn • ForceRestart • GracefulRestart • GracefulRestart • GracefulShutdown • PowerCycle \$ curl -k -srequest POSTurl https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system /Actions/ComputerSystem.Resetheader 'Content-Type:application/json'data '{"ResetType":"GracefulFestart"} </pre>
	<pre>{ "@odata.type": "#Message.vl l l.Message", "Message": "Successfully Completed Request", "MessageId": "Base.l.8.l.Success", "MessageSeverity": "OK", "Resolution": "None" } }</pre>
Step_2	Verify the current power state.
	RemoteComputer_OSPrompt:~\$ curl -k -srequest GETurl [ROOT_URL]/redfish/v1/Systems/system jq .PowerState
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system</pre>

Power management using IPMI over LAN (IOL)

Refer to <u>Accessing a BMC using IPMI over LAN (IOL)</u> for access instructions.

Step_1	List every power action command. RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -C 17 chassis power	<pre>\$ ipmitool -I lanplus -H 172.16.182.31 -U admin -P ready2go -C 17 chassis power Chassis Commands:</pre>
Step_2	Execute the power action command from the commands listed. RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -C 17 chassis power [POWER_ACTION]	\$ ipmitool -I lanplus -H 172.16.182.31 -U admin -P ready2go -C 17 chassis power off Chassis Power Control: Down/Off
Step_3	Verify the power status. RemoteComputer_OSPrompt:~# ipmitool -I lanplus -H [BMC MNGMT_IP] -U [IPMI user name] -P [IPMI password] -C 17 chassis power status	\$ ipmitool -I lanplus -N 172.16.182.31 -U admin -P ready2go -C 17 chassis power status Chassis Power is off

NOTE: IPMI power command **reset** will not perform a hardware reset. It will perform a simple server power down and then will power up the server automatically.

Rebooting the BMC using the Web UI

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

NOTE: Rebooting the BMC using the Web UI might terminate the current user session.

Step_1	From the left-side menu, click on $\ensuremath{Operations}$ and then $\ensuremath{Reboot}\xspace$.	Skontron Skefeeh @ admin -
		🗈 overview 🛛 🖉
		Hardware status Constraints C
		Kum East Refloot settings Sub Concol Reboot BMC Server information Product information SOL concole Manufacture Name Server power operations Manufacture Name Virtual media 2021-04-06 - 9017064072
Step_2	Click on the Reboot BMC button and then confirm.	Image: Server power operations Virtual media
Step_3	Wait for the BMC to boot. It may take a moment.	

Rebooting the BMC using Redfish

Refer to <u>Accessing a BMC using Redfish</u> for access instructions.
Step_1	Execute the following command to reboot BMC. RemoteComputer_OSPrompt:~\$curl -k -srequest POSTurl [ROOT_URL] /redfish/v1/ Managers /bmc/Actions/Manager.Resetheader 'Content-Type: application/json'data '{"ResetType":"GracefulRestart"}' jq
	<pre>\$ curl -k -srequest POSTurl https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc/A ctions/Manager.Resetheader 'Content-Type:application/json'data '{"ResetType":"GracefulRest art"}' jq { "@Message.ExtendedInfo": [{ "@Odata.type": "#Message.vl_l l.Message", "MessageArge": [], "MessageArge": [], "MessageArge": [], "MessageSverity": "OK", "Resolution": "None" } }</pre>
Step_2	Wait for the BMC to reboot. It may take a moment.

Rebooting the switch NOS

NOTE: This procedure applies only to a platform equipped with the Ethernet switch IO module. **NOTE:** Make sure all changes to the configuration are saved prior to rebooting the switch NOS. Refer to <u>Configuring the switch</u>.

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

Step_1	LocalSwitchNOS_OSPrompt:~# reload cold
	NOTE: If you press a key during reset, the process will momentarily stop and then resume.
	NOTE: Rebooting the switch NOS may take several seconds.

Monitoring

- Monitoring sensors
- <u>Sensor list</u>

Monitoring sensors

Table of contents

- <u>General monitoring procedure for unit-based sensors</u>
 - <u>Monitoring using the BMC Web UI</u>
 - Monitoring using Redfish
 - <u>Creating URL extensions</u>
 - <u>Viewing sensor details</u>
 - Monitoring using IPMI
- Discrete sensor monitoring procedure
 - Board Reset
 - Possible values (IPMI only)
 - <u>Monitoring Board Reset using IPMI</u>
 - <u>Monitoring last reset time</u>
 - <u>Heaters</u>
 - Possible values
 - Monitoring heaters using Redfish
 - Monitoring heaters using IPMI
 - Intrusion
 - Event assertion
 - Event deassertion
 - IPMIWatchdog
 - <u>Jumpers Status</u>
 - Monitoring Jumpers Status sensor using Redfish
 - Monitoring Jumpers Status sensor using IPMI
 - <u>TelcoAlarms</u>
 - Monitoring TelcoAlarms using Redfish
 - Monitoring TelcoAlarms using IPMI
 - Event assertion
 - Event deassertion

The platform has many sensors, you can refer to the <u>Sensor list</u> for details and to determine the sensor ID. Sensors can be separated in two categories and both types are described in the Sensor list:

- Unit-based sensors use the general monitoring procedure
- Discrete sensors use the discrete sensor monitoring procedure

General monitoring procedure for unit-based sensors

There are several methods to monitor platform unit-based sensors, including:

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

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

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

Monitoring using the BMC Web UI

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 Hardware status and then Sensors .	Kontron Prover Refresh @ admin- ID Overview Overview Overview IZ togs Verview
		Inventory and LEDs source time Sensors Ldit network settings © Operations ∧ KVM BMC information
		Firmware Firmware version Model Manufacturer Reboot BMC 2.00.0159fce6 ME1210 Kontron SOL contole Server power operations UEF version UEF version Virtual media V Hordmann Power consumption Security and access V MAC address Power consumption Resource management Proteins Nat available Power consumption
Step_3	The sensor list will be displayed. Scroll down to see the list of sensors or use the dedicated search bar to filter the sensors.	Sensors Source Sensors Sensors Sensors Source
		Coperations Control Contro Control Control Control
		Rebot BMC D L P30 O K V V V V SOL console D C PSU O K V V V V V Server power operations D C PSU O K V V V V V
		V 12V O K 11.04 V 12.091 V 12.972 S Seturity and access ~ V 1V8 O K V V V V V Resource management ~ PCH AUX O K 1.654 V 1.789 V V 1.346

Monitoring using Redfish

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

Creating URL extensions

Relevant section:

<u>Sensor list</u>

Туре	URL extensions	Parser arguments
Fan sensors	Chassis/ ME1210_Baseboard /Thermal	jq ".Fans"
Temperature sensors (including PSU sensors)	Chassis/ ME1210_Baseboard /Thermal	jq ".Temperatures"
Voltage sensors (including PSU sensors)	Chassis/ ME1210_Baseboard /Power	jq ".Voltages"
Power sensors (including PSU sensors)	Chassis/ ME1210_Baseboard /Sensors	jq
Other unit-based sensors	Chassis/ ME1210_Baseboard /Sensors	jq
Discrete sensors	Managers/bmc	jq ".0em.Kontron.Discrete"
Pass-through IO module sens ors	Chassis /IOBoard/Thermal	jq ".Temperatures"
Ethernet switch IO module sensors	Chassis /Switchboard/Thermal	jq ".Temperatures"

NOTE: Power supply sensors do not have a dedicated URL in Redfish. They will appear along with the ME1210 sensors according to their reading unit type.

Viewing sensor details



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 langlus -H [BMC MNGMT_IP] - U [IPMI user name] -P [IPMI password] -C 17.

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	\$ ipnitool sensor Fan 1 10600.000 EPM ok na na na Fan 1 10544.000 RFM ok na na na na Fan 3 10518.000 RFM ok na na na na Fan 3 10518.000 RFM ok na na na Fan 4 11318.000 RFM ok na na na Fan 5 10454.000 RFM ok na na na Fan 6 10454.000 RFM ok na na na Fan 7 10518.000 RFM ok na na na Fan 8 10600.000 RFM ok na na na Temp CFU 28.000 degrees C ok na -41.000 na Temp CFU Area 30.000 degrees C ok na -41.000 na
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 "Temp CPU" Sensor ID : Temp CPU (0x16) Entity ID : 0.1 (Unspecified) Sensor Type (Threshold) : Temperature (0x01) Sensor Reading : 27 (+/-0) degrees C Status Hysteresis : Unspecified Negative Hysteresis : Unspecified Minimum sensor range : Unspecified Maximum sensor range : Unspecified Event Message Control : Per-threshold Readable Thresholds : 1cr unc ucr Settable Thresholds : 1cr unc ucr Assertion Events : Event Enable : Event Messages Disabled Assertions Enabled : 1cr+ unc- ucr-</pre>

Discrete sensor monitoring procedure

This section describes the specific behaviors and monitoring methods for the platform's discrete sensors. The platform comes equipped with the following discrete sensors:

- Board Reset
- Heater CPU, Heater PCIe1, Heater PCIe2
- Intrusion
- IPMIWatchdog
- Jumpers Status
- TelcoAlarm1, TelcoAlarm2, TelcoAlarm3, TelcoAlarm4

Board Reset

The Board Reset sensor will report the last reset cause in the system event log.

Relevant sections: Sensor list System event log

Possible values (IPMI only)

The cause of the last board reset can only be found in the system event log entries.

Event offset	Description
0×01	Unexpected power loss
0x02	Power cycle or serial port reset
0x06	Cold reset
0×07	Power reset from IPMI command

Monitoring Board Reset 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] -C 17.

Step_1	Access the system event log and identify the ID of the desired event from the first column. LocalServer_OSPrompt:~# ipmitool sel list	<pre>\$ ipmitool sel list 1 2022-04-29 13:12:54 EDT Board Reset #0x01 Unknown Asserted 2 2022-04-29 13:13:02 EDT Board Reset #0x01 Cold Reset Asserted 3 2022-04-29 13:14:22 EDT Board Reset #0x01 Unknown Asserted</pre>
Step_2	Display the details of the system event log entry. LocalServer_OSPrompt:~# ipmitool get [ID] The value is represented by the most significant byte of the Event Data (RAW) value. Note that bit 7 of the most significant byte is reserved and always equal to 1 (or 0x8 in hexadecimal). Refer to the list of possible values.	<pre>\$ ipmitool get 3 SEL Record ID : 0003 Record Type : 02 Timestamp : 2022-04-29 2022-04-29 Generator ID : 0020 EvM Revision : 04 Sensor Type : Board Reset Sensor Number : 01 Event Type : Sensor-specific Discrete Event Direction : Assertion Event Event Data (RAW) : S2ffff Event Interpretation : Missing Description : Unknown Sensor ID : BoardReset (0x1) Entity ID : 0.1 (Unspecified) Sensor Type : Board Reset (0xc4)</pre>

Monitoring last reset time

The last reset time can be found using the BMC Web UI and Redfish.

Monitoring the last reset time using the BMC Web UI

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

Step_1	From the left-side menu, click on Operations and then Server power operations , or simply click on the Power button at the top of the page.	Image: Security and access Image: Security and access Image: Security and access Image: Security and acces Image: Security and access Image: Security and acces Image: Security and acces Image: Security and acces
Step_2	The last power operation time will be displayed.	Server power operations Current status Server status On Last power operation 2022-03-18 18:45:58 UTC

Monitoring the last reset time using Redfish

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

Step_1	RemoteComputer_OSPrompt:~\$ curl -k -srequest GETurl [ROOT_URL]/redfish/v1/ Systems/system jq .LastResetTime
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1 /Systems/system jq .LastResetTime "2022-03-18T18:45:58+00:00"</pre>

Heaters

The BMC will register events indicating a heater status change. There are three heater sensors present in the platform:

- Heater CPU
- Heater PCIe1 (optional)
- Heater PCIe2 (optional)

For information about the PCIe heaters, contact the Kontron support team. Refer to Support information.

Relevant sections:

Platform cooling and thermal management - Behavior upon startup at temperatures below 0°C Sensor list

Possible values

Value	Description
0	Device disabled
1	Device enabled

Monitoring heaters using Redfish

Refer to <u>Accessing a BMC using Redfish</u> for access instructions. **NOTE:** Redfish will not report the presence of heaters.

Step_1		Display the heaters' statuses using the following command. RemoteComputer_OSPrompt:~\$ curl -k -srequest GETurl [ROOT_URL]/redfish/v1/ Managers/bmc jq .Oem.Kontron.Discrete
		<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1 /Managers/bmc jq .Oem.Kontron.Discrete { "Heater_PCIel": "0", "Heater_PCIel": "0", "Heater_PCIel": "0", "JMP1 (JPx p1-2)": "?", "JMP2 (JPx p3-4)": "0UT", "JMP3 (JPx p5-6)": "0UT", "JMP4 (JPx p7-8)": "0UT", "JMP5 (JPx p9-10)": "0UT", "JMP5 (JPx p1-12)": "0UT", "JMP7 (JPx p13-14)": "0UT", "JMP7 (JPx p13-14)": "0UT", "TelcoAlarm1": "1", "TelcoAlarm4": "1", "TelcoAlar</pre>

Monitoring heaters 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] -C 17.

Intrusion

The chassis intrusion sensor will register an event if the chassis is opened. This sensor needs manual deassertion.

Relevant sections:

Event assertion

The chassis intrusion sensor will register an event in the following circumstances:

- When the chassis is opened the BMC will register a critical chassis intrusion event in the system event log.
- When the chassis intrusion sensor is manually deasserted the BMC will register a chassis intrusion reset event in the system event log.

Event deassertion

This sensor needs manual deassertion. If a chassis intrusion occurs, the sensor's state needs to be manually reset. Redfish is the only supported way for event deassertion.

Refer to Accessing a BMC using Redfish for access instructions.

NOTE: As of the current BMC firmware version, the BMC health status will be in a critical state as long as there are critical events in the system event log. Currently, the only supported way of restoring the BMC health status is by clearing the system event log. Refer to <u>System event log</u> for further instructions. It is recommended to export all system event log entries beforehand.

IPMIWatchdog

The IPMIWatchdog sensor will report a critical event in the system event log when it expires because an error prevents the platform from booting correctly.

Relevant sections: Sensor list

System event log

Jumpers Status



Jumpers Status sensor values are reserved and should never differ from the default values shown below. Otherwise, it could render the platform inoperable.

Relevant section: Sensor list

Monitoring Jumpers Status sensor using Redfish

Refer to Accessing a BMC using Redfish for access instructions.



Monitoring Jumpers Status sensor 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] -C 17.

Step_1	Display the Jumpers Status sensor value using the following command.	\$ ipmitool sensor grep "Jumpers status" Jumpers Status 0x0 discrete 0x00fe na na na
	LocalServer_OSPrompt:~# ipmitool sensor grep	
	"Jumpers Status"	
	The value is represented by bytes in the fourth column.	
	The value should always be $0 \times 000 fe$.	

TelcoAlarms

TelcoAlarm sensors are normally-closed dry contacts between an **Alarm Input** signal and the **Alarm Common** signal. Those signals are located on the front panel Alarm Port RJ45 connector. The BMC will register an event indicating a status change. Refer to <u>Connector pinouts and electrical</u> <u>characteristics</u> for pinout.

NOTE: If no normally-closed contacts are connected to the front panel, the BMC will register a critical event in the system event log each time it reboots because it will assume it detects faulty hardware or a cut wire. Refer to <u>System event log</u> for a description of what happens in the SEL upon reboot with regards to TelcoAlarms.

There are four TelcoAlarm sensors present in the platform:

- TelcoAlarm1
- TelcoAlarm2
- TelcoAlarm3
- TelcoAlarm4

Relevant sections:

<u>Sensor list</u> System event log

Monitoring TelcoAlarms using Redfish

Refer to Accessing a BMC using Redfish for access instructions.

Step_	 Display the TelcoAlarm statuses using the following command. RemoteComputer_OSPrompt:~\$curl -k -srequest GETurl [ROOT_URL]/redfish/v1/ Managers/bmc jq .0em.Kontron.Discrete Possible values are: 0 for a closed contact 1 for an open contact
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1 /Managers/bmc jq .Oem.Kontron.Discrete { "Heater_CPU": "0", "Heater_PCIe1": "0", "Heater_PCIe2": "0", "JMPI (JPx pl-2)": "?", "JMP2 (JPx pl-2)": "?", "JMP2 (JPx p3-4)": "0UT", "JMP3 (JPx p5-6)": "0UT", "JMP4 (JPx p7-8)": "0UT", "JMP4 (JPx p7-8)": "0UT", "JMP6 (JPx p1-12)": "0UT", "JMP6 (JPx p1-2)": "0UT", "JMP7 (JPx p13-14)": "0UT", "TelcoAlarm1": "1", "TelcoAlarm3": "1", "TelcoAlarm3": "1", "TelcoAlarm3": "1", "TelcoAlarm3": "1", "TelcoAlarm3": "1", "TelcoAlarm4": "1",</pre>

Monitoring TelcoAlarms 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] -C 17.

Step_1	Display the TelcoAlarm statuses using the following command. LocalServer_OSPrompt:~# ipmitool sensor grep TelcoAlarm The value is represented by the second byte from the left in the fourth column. Possible values are: • 0x0080 for a closed contact • 0x0180 for an open contact	<pre>\$ ipmitool sensor TelcoAlarm1 TelcoAlarm2 TelcoAlarm3 TelcoAlarm4</pre>	grep 0x0 0x0 0x0 0x0 0x0	TelcoAlarm discrete discrete discrete discrete	0x0180 0x0180 0x0180 0x0180	na na na na	na na na na	na na na
--------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------	-----------------------------------------	--------------------------------------------------------------------	--------------------------------------	----------------------	----------------------	----------------

Event assertion

The TelcoAlarm sensors will register an event in the following circumstances:

- When a TelcoAlarm input changes from closed to open the BMC will register a critical TelcoAlarm event in the system event log.
- When a TelcoAlarm input changes from open to closed the BMC will register a TelcoAlarm restoration event in the system event log, but note that a restoration event does not deassert a critical TelcoAlarm event.

Event deassertion

This event cannot be deasserted.

NOTE: As of the current BMC firmware version, the BMC health status will be in a critical state as long as there are critical events in the system event log. Currently, the only supported way of restoring the BMC health status is by clearing the system event log. Refer to <u>System event log</u> for further instructions. It is recommended to export all system event log entries beforehand.

Sensor list

Table of contents

- <u>ME1210 sensors</u>
 - <u>Unit-based sensors</u>
 - Fan sensors
 - <u>Temperature sensors</u>
 - <u>Voltage sensors</u>
 - Power sensors
 - <u>Other unit-based sensors</u>
 - Discrete sensors
- Power supply sensors
 - DC PSU sensors
 - <u>AC PSU sensors</u>
- <u>10 module sensors</u>
 - Ethernet switch IO module sensors
 - Pass-through IO module sensors
- <u>Application-specific sensors</u>
 - <u>Silicom P3iMB sensors</u>

Refer to Monitoring sensors for monitoring instructions.

For Redfish URL extensions, refer to <u>Monitoring sensors using Redfish - Creating URL extensions</u>. For information about **Sensor type code** and **Event/Reading type code**, refer to <u>Interpreting sensor data</u>.

ME1210 sensors

ME1210 sensors are always present regardless of the platform hardware configuration.

Unit-based sensors

Fan sensors

Sensor name [SENSOR_ID]	Description	Sensor type code	Event/Reading type code
Fan 1	FAN 1 Speed (RPM)	Fan (0x04)	0x01 (Threshold Based)
Fan 2	FAN 2 Speed (RPM)	Fan (0x04)	0x01 (Threshold Based)
Fan 3	FAN 3 Speed (RPM)	Fan (0x04)	0x01 (Threshold Based)
Fan 4	FAN 4 Speed (RPM)	Fan (0x04)	0x01 (Threshold Based)
Fan 5	FAN 5 Speed (RPM)	Fan (0x04)	0x01 (Threshold Based)
Fan 6	FAN 6 Speed (RPM)	Fan (0x04)	0x01 (Threshold Based)
Fan 7	FAN 7 Speed (RPM)	Fan (0x04)	0x01 (Threshold Based)
Fan 8	FAN 8 Speed (RPM)	Fan (0x04)	0x01 (Threshold Based)

Temperature sensors

Sensor name [SENSOR_ID]	Description	Sensor type code	Event/Reading type code
Temp	Temperature of DIMM 1 on channel A	Temperature	0x01 (Threshold
DIMMA1		(0x01)	Based)
Temp	Temperature of DIMM 2 on channel A	Temperature	0x01 (Threshold
DIMMA2		(0x01)	Based)
Temp	Temperature of DIMM 1 on channel B	Temperature	0x01 (Threshold
DIMMB1		(0x01)	Based)
Temp	Temperature of DIMM 2 on channel B	Temperature	0x01 (Threshold
DIMMB2		(0x01)	Based)
Temp	Temperature of DIMM 1 on channel D	Temperature	0x01 (Threshold
DIMMD1		(0x01)	Based)
Temp	Temperature of DIMM 2 on channel D	Temperature	0x01 (Threshold
DIMMD2		(0x01)	Based)
Temp DIMME1	Temperature of DIMM 1 on channel E	Temperature (0x01)	0x01 (Threshold Based)
Temp	Temperature of DIMM 2 on channel E	Temperature	0x01 (Threshold
DIMME2		(0x01)	Based)
Temp CPU	Internal CPU temperature	Temperature (0x01)	0x01 (Threshold Based)
Temp BMC	Temperature under BMC	Temperature (0x01)	0x01 (Threshold Based)
Temp CPU	Temperature under CPU	Temperature	0x01 (Threshold
Area		(0x01)	Based)
Temp Chassis	Temperature from chassis thermistor	Temperature	0x01 (Threshold
	Refer to <u>Installing a thermal probe for the PCIe add-in card</u> for thermal probe location.	(0x01)	Based)
Temp FPGA	Temperature under FPGA	Temperature (0x01)	0x01 (Threshold Based)
Temp Inlet	Temperature of fresh air inlet	Temperature (0x01)	0x01 (Threshold Based)
Temp M2	Temperature near M.2 A and B	Temperature	0x01 (Threshold
Area		(0x01)	Based)
Temp PCIe 1	Temperature from PCIe slot 1 thermistor	Temperature	0x01 (Threshold
	Refer to <u>Installing a thermal probe for the PCIe add-in card</u> for thermal probe location.	(0x01)	Based)
Temp PCle 1 mbox	Temperature from PCIe slot 1 reported via mailbox Refer to <u>Platform resources for customer application - Customer-specific temperature</u> <u>sensors</u> for reporting instructions.	Temperature (0x01)	0x01 (Threshold Based)
Temp PCIe 2	Temperature from PCIe slot 2 thermistor	Temperature	0x01(Threshold
	Refer to <u>Installing a thermal probe for the PCIe add-in card</u> for thermal probe location.	(0x01)	Based)
Temp PCIe 2 mbox	Temperature from PCIe slot 2 reported via mailbox Refer to <u>Platform resources for customer application - Customer-specific temperature</u> <u>sensors</u> for reporting instructions.	Temperature (0x01)	0x01 (Threshold Based)
Temp PSU	Temperature of system PSU outlet	Temperature	0x01 (Threshold
Outlet		(0x01)	Based)
Temp VCCIN	Temperature near VCCIN switcher	Temperature (0x01)	0x01 (Threshold Based)
Temp	Temperature near VDDQ_AB switcher	Temperature	0x01 (Threshold
VDDQ_AB		(0x01)	Based)
Temp	Temperature near VDDQ_DE switcher	Temperature	0x01 (Threshold
VDDQ_DE		(0x01)	Based)
Temp	Temperature near V_3V3_SUS switcher	Temperature	0x01 (Threshold
V_3V3_SUS		(0x01)	Based)

Voltage sensors

Sensor name [SENSOR_ID]	Description	Sensor type code	Event/Reading type code
VBAT	RTC battery voltage	Voltage (0x02)	0x01 (Threshold Based)
V_1V8_PCH_AUX	V 1V8 PCH AUX voltage	Voltage (0x02)	0x01 (Threshold Based)
V_3V3_M2	V_3V3_M2 voltage	Voltage (0x02)	0x01 (Threshold Based)
V_3V3_PCH_AUX	V_3V3_PCH_AUX voltage	Voltage (0x02)	0x01 (Threshold Based)
V_3V3_SLOT	V_3V3_SLOT voltage	Voltage (0x02)	0x01 (Threshold Based)
V_12V_SLOT1	V_12V_SLOT1 voltage	Voltage (0x02)	0x01 (Threshold Based)
V_12V_SLOT2	V_12V_SLOT2 voltage	Voltage (0x02)	0x01 (Threshold Based)
V_12V_SUS	V_12V_SUS voltage	Voltage (0x02)	0x01 (Threshold Based)
V_VTT_AB	V_VTT_AB voltage	Voltage (0x02)	0x01 (Threshold Based)
V_VTT_DE	V_VTT_DE voltage	Voltage (0x02)	0x01 (Threshold Based)

Power sensors

Sensor name [SENSOR_ID]	Description	Sensor type code	Event/Reading type code
P_12V_SLOT1	V_12V_SLOT1 power consumption	Power Supply (0x08)	0x01 (Threshold Based)
P_12V_SLOT2	V_12V_SLOT2 power consumption	Power Supply (0x08)	0x01 (Threshold Based)

Other unit-based sensors

Sensor name [SENSOR_ID]	Description	Sensor type code	Event/Reading type code
Humidity	Relative humidity at air inlet	Other Units-based sensor (0x0B)	0x01 (Threshold Based)

Discrete sensors

For information about discrete sensors, refer to Discrete sensor monitoring procedure.

Sensor name [SENSOR_ID]	Description	Sensor type code	Event/Reading type code
Heater CPU	Heater status indicator for CPU	Chassis (0x18)	0x9 ('digital' Discrete - Device Disabled/Device Enabled)
Heater PCIe1	Heater status indicator for PCIe1	Chassis (0x18)	0x9 ('digital' Discrete - Device Disabled/Device Enabled)
Heater PCIe2	Heater status indicator for PCIe2	Chassis (0x18)	0x9 ('digital' Discrete - Device Disabled/Device Enabled)
Intrusion	Alarm status from front panel connector	Platform Alert (0x24)	0x3 ('digital' Discrete - Assert/Deassert)
TelcoAlarm1	Status from front panel alarm connector	Platform Alert (0x24)	0x3 ('digital' Discrete - Assert/Deassert)
TelcoAlarm2	Status from front panel alarm connector	Platform Alert (0x24)	0x3 ('digital' Discrete - Assert/Deassert)
TelcoAlarm3	Status from front panel alarm connector	Platform Alert (0x24)	0x3 ('digital' Discrete - Assert/Deassert)
TelcoAlarm4	Status from front panel alarm connector	Platform Alert (0x24)	0x3 ('digital' Discrete - Assert/Deassert)
IPMIWatchdog	IPMI Watchdog action reporting	Watchdog 2 (0x23)	0x6f (Sensor Specific)
Board Reset	Reports the last reset source	Board Reset (Kontron OEM) (0xCA)	0x6f (Sensor Specific)
Jumpers Status	Reserved – event-based sensor	Jumpers Status - Kontron OEM (0xD3)	0x6f (Sensor Specific)

Power supply sensors

The power supply sensors will differ according to the power supply unit configuration of the platform. The ME1210 comes equipped with either a DC or an AC power supply unit.

DC PSU sensors

NOTE: The DC PSU sensors are only present when a DC PSU is connected.

Sensor name [SENSOR_ID]	Description	Sensor type code	Event/Reading type code
DC PSU Pout	Output power from PSU	Power Supply (0x08)	0x01 (Threshold Based)
DC PSU Vout	DC PSU 48V to 12V regulator o utput voltage	Voltage (0x02)	0x01 (Threshold Based)
DC PSU lout	DC PSU 48V to 12V regulator o utput current	Current (0x03)	0x01 (Threshold Based)
DC PSU Regulator	Temperature in the DC PSU 48V to 12V regulator	Temperature (0x01)	0x01 (Threshold Based)
DC PSU HoldUp	Temperature in the DC PSU HoldUp generation regulator	Temperature (0x01)	0x01 (Threshold Based)
DC PSU Inlet	Temperature in the DC PSU feed ORing circuit	Temperature (0x01)	0x01 (Threshold Based)
DC PSU HUVout	DC PSU hold up voltage	Voltage (0x02)	0x01 (Threshold Based)
DC PSU Vin	DC PSU QBrick input voltage	Voltage (0x02)	0x01 (Threshold Based)
DC PSU Feed A	DC PSU FPGA Feed A reading	Voltage (0x02)	0x01 (Threshold Based)
DC PSU Feed B	DC PSU FPGA Feed A reading	Voltage (0x02)	0x01 (Threshold Based)

AC PSU sensors

NOTE: The AC PSU sensors are only present when an AC PSU is connected.

Sensor name [SENSOR_ID]	Description	Sensor type code	Event/Reading type code
AC PSU Vout	Output voltage from PSU	Voltage (0x02)	0x01 (Threshold Based)
AC PSU Pout	Output power from PSU	Power Supply (0x08)	0x01 (Threshold Based)
AC PSU Vin	Input voltage from PSU	Voltage (0x02)	0x01(Threshold Based)
AC PSU Pin	Input power from PSU	Power Supply (0x08)	0x01(Threshold Based)
AC PSU Temp1	Temperature from PSU	Temperature (0x01)	0x01(Threshold Based)

10 module sensors

The IO module sensors will differ according to the IO module configuration of the platform. The ME1210 comes equipped with either a p assthrough or an Ethernet switch IO module .

Ethernet switch IO module sensors

NOTE: The Ethernet switch IO module sensors are only present if the platform is equipped with an Ethernet switch IO module.

Sensor name [SENSOR_ID]	Description	Sensor type code	Event/Reading type code
Temp SWB Clk	Temperature under ZL30772 DPLL on Ethernet switch IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB Inlet	Temperature at air inlet on Ethernet switch IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB OCXO	Temperature under OCXO on Ethernet switch IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP1	Temperature from SFP1 module on Ethernet switch IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP2	Temperature from SFP2 module on Ethernet switch IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP3	Temperature from SFP3 module on Ethernet switch IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP4	Temperature from SFP4 module on Ethernet switch IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP5	Temperature from SFP5 module on Ethernet switch IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP6	Temperature from SFP6 module on Ethernet switch IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP7	Temperature from SFP7 module on Ethernet switch IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP8	Temperature from SFP8 module on Ethernet switch IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP9	Temperature from SFP9 module on Ethernet switch IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP10	Temperature from SFP10 module on Ethernet switch IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP11	Temperature from SFP11 module on Ethernet switch IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB SFP12	Temperature from SFP12 module on Ethernet switch IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp SWB Switch	Temperature from switch die on Ethernet switch IO module	Temperature (0x01)	0x01 (Threshold Based)

Pass-through IO module sens ors

NOTE: The pass-through IO module sensors are only present if the platform is equipped with a pass-through IO module.

Sensor name [SENSOR_ID]	Description	Sensor type code	Event/Reading type code
Temp IOB Inlet	Temperature at air inlet on pass-through IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp IOB LAN1	Temperature under LAN1 controller on pass-through IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp IOB LAN2	Temperature under LAN2 controller on pass-through IO module	Temperature (0x01)	0x01 (Threshold Based)
Temp IOB PHY	Temperature under Cortina PHY on pass-through IO module	Temperature (0x01)	0x01 (Threshold Based)

Application-specific sensors

Silicom P3iMB sensors

Silicom P3iMB sensors are only present when Virtual PCIe FRU is configured for a P3iMB PCIe add-in card.

Sensor name [SENSOR_ID]	Description	Sensor type code	Event/Reading type code
T P3iMB Local S <x></x>	Local temperature for Silicom P3iMB (Pomona Lake) PCIe add-in card Where <x> is the PCIe slot ID. Silicom-BMC interface (Index 0).</x>	Temperature (0x01)	0x01 (Threshold Based)
T ACC100 TSDE S <x></x>	eASIC TSD1 East temperature for Silicom P3iMB (Pomona Lake) PCIe add- in card Where <x> is the PCIe slot ID. Silicom-BMC interface (Index 1).</x>	Temperature (0x01)	0x01 (Threshold Based)
T ACC100 TSDW S <x></x>	eASIC TSD2 West temperature for Silicom P3iMB (Pomona Lake) PCIe add-in card Where <x> is the PCIe slot ID. Silicom-BMC interface (Index 2).</x>	Temperature (0x01)	0x01 (Threshold Based)

Maintenance

- <u>System event log</u>
- Interpreting sensor data
- <u>Component replacement</u>
- Backup and restore
- <u>Upgrading</u>

System event log

Table of contents

- <u>Relationship between the system event logs</u>
- TelcoAlarms registered in the SEL upon BMC reboot
- <u>Accessing the SEL using the BMC Web UI</u>
 - <u>Accessing the system event log</u>
 - <u>Clearing the system event log</u>
 - Exporting the system event log
- Accessing the SEL using Redfish
 - <u>Accessing the system event log</u>
 - <u>Clearing the system event log</u>
 - <u>Redfish supported event types</u>
- <u>Accessing the SEL using IPMI</u>
 - <u>Accessing the system event log</u>
 - <u>Clearing the system event log</u>
- Exporting the system event log

System event logs can be accessed:

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

Relationship between the system event logs

System event logs accessed via the BMC Web UI and Redfish are managed independently. This has two implications:

- The Web UI and Redfish logs may display events that are not supported by the IPMI event log.
- Using either the Web UI or Redfish methods described below to clear the logs will yield an empty log for both these interfaces. But the IPMI event log clear command must be used to clear the IPMI event log.

TelcoAlarms registered in the SEL upon BMC reboot

TelcoAlarms are used to detect s tatuses of the inputs of the front panel alarm connector. If nothing is connected to the Alarm Port, TelcoAlarm events will be registered in the SEL if a BMC reboot occurs. This happens because in order to detect faulty wiring (a cut cable, etc.) the system considers an open loop as an event—and an empty Alarm Port creates an open loop.

If the Alarm Port is not used, a solution would be to install a loop back RJ45 connector assembly into the Alarm Port.

The TelcoAlarms generated will set the BMC health status in a critical state. Currently, the only supported way of restoring the BMC health status is by clearing the system event log. Kontron recommends exporting the SEL before clearing it.

Relevant section: Platform components

Accessing the SEL using the BMC Web UI

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

Accessing the system event log

Step_1	From the left-side menu of the BMC Web UI, select Logs and then Event Logs .	Event logs OVERVIEW Event logs Event logs POST code logs Event logs Event logs Event logs FOST code logs Event logs Event logs Server LD Event logs Server logs Event logs Server logs Event logs Server logs Event logs Server logs Event logs Server information Firmware Reboot BMC SOL console Server information Firmware Sol console Sol console Server information Firmware Server power operations Vintal medie Mit 210					
Step_2	The system event log is displayed. The following information can be collected: 1. Event ID 2. Severity 3. Date 4. Description 5. Status	Konttron Image: Non-State Image: Non-State Event logs Image: Non-State Image: Non-State Image: Non-State </th <th>over C Refresh () admin - Delete all C-Export all Description Status ple (1)</th>	over C Refresh () admin - Delete all C-Export all Description Status ple (1)				

Clearing the system event log

NOTE: This method will clear the events visible via the Web UI and the Redfish interfaces. The IPMI event log must be cleared separately.

Step_1	Click on the Delete all button.	Event logs										
								From date		To date		
		9	Search	logs		4 items		YYYY-MM-DD		YYYY-MM-E	DD 📋	
								≅ Filter		Delete all	Export all	
					∲ ID	Severity	Date	Description	Sta	tus		
			/		1637428849	🛛 ОК	2021-11-20 17:20:49 UT	Host system DC power is on	•) Unresolved	₿ Ö	
			/		1637428843	🛛 ОК	2021-11-20 17:20:43 UT	Host system DC power is off	0) Unresolved	₿ ∅	
		`	/		1637428590	🛛 ОК	2021-11-20 17:16:30 UT	Host system DC power is on) Unresolved	₿ Ū	
		`	/		1637428585	🛛 ОК	2021-11-20 17:16:25 UT	Host system DC power is off	0) Unresolved	₿ Ó	
		20		¢ It	ems per page						< 1 →	
Step_2	Confirm choice by clicking on the Delete button.	10E20		Del Are und	ete all lc you sure y one.	ogs ou want to	o delete a	ll logs? This act	tion c	Hea	lith C	Pc

Exporting the system event log

Step_1	Click on the Export all button to download the system event log.	Εv	rent	logs					
		Q 5	Search log	5	4 items		From date	To date	-DD 📋
					A. A. 1.		Se Filter	🗇 Delete all	Export all
				€ ID	Severity	© Date	Description	Status	
		``````````````````````````````````````	<ul> <li>I</li> </ul>	1637428849	OK OK	17:20:49 UT	C power is on	Unresolved	₿ Ö
			~	1637428843	🖉 ОК	2021-11-20 17:20:43 UT	Host system DC C power is off	Unresolved	₿ Ö
			• 🗆	1637428590	🖉 ОК	2021-11-20 17:16:30 UT	Host system DC C power is on	Unresolved	D 🛈
			× 🗆	1637428585	🛛 ок	2021-11-20 17:16:25 UT	Host system DC C power is off	Unresolved	₿ 0
		20	¢	Items per page					< <u>1</u> >

# Accessing the SEL using Redfish

### Accessing the system event log

**NOTE:** Depending on the event, there may not be an associated sensor attribute. However, if this attribute is present, refer to <u>Interpreting sensor</u> <u>data</u> for further interpretation instructions.



### Clearing the system event log

NOTE: This method will clear the events visible via the Web UI and the Redfish interfaces. The IPMI event log must be cleared separately.

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 -srequest POSTurl [ROOT_URL] /redfish /v1/Systems/system/LogServices/EventLog/Actions/LogService.ClearLog   jq
	<pre>\$ curl -k -srequest POSTurl https://admin:ready2go@172.16.182.31/redfish/v1/Systems/system /LogServices/EventLog/Actions/LogService.ClearLog   jq {     "@Message.ExtendedInfo": [         "@edata.type": "#Message.vl_l 1.Message",         "Message": "Buccessfully Completed Request",         "MessageId": "Base.1.8.1.Success",         "MessageArer": [],         "Resolution": "None"     }     ] }</pre>
Step_2	Verify that the system event log was properly cleared. RemoteComputer_OSPrompt:~# curl -k -srequest GETurl [ROOT_URL] /redfish /v1/Systems/system/LogServices/EventLog/Entries   jq
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/vl/Systems/system/ LogServices/EventLog/Entries   jq { "@odata.id": "/redfish/vl/Systems/system/LogServices/EventLog/Entries", "@odata.type": "#LogEntryCollection.LogEntryCollection", "Description": "Collection of System Event Log Entries", "Members": [], "Members@odata.count": 0, "Name": "System Event Log Entries" } </pre>

### Redfish supported event types

The event format is composed of the OpenBMC event schema version followed by the event type [SCHEMA VERSION].[EVENT TYPE]. The current schema version is **OpenBMC.0.1**.

Event type	Description
InventoryAdded	Indicates that an inventory item with the specified model, type and serial number was installed
InventoryRemoved	Indicates that an inventory item with the specified model, type and serial number was removed
BoardReset	Indicates that the payload was reset
DCPowerOn	Indicates that the system DC power is on
DCPowerOff	Indicates that the system DC power is off
SensorThresholdCriticalLowGoingLow	Indicates that a threshold sensor has crossed a critical low threshold going low
SensorThresholdCriticalLowGoingHigh	Indicates that a threshold sensor has crossed a critical low threshold going high
SensorThresholdCriticalHighGoingLow	Indicates that a threshold sensor has crossed a critical high threshold going low
SensorThresholdCriticalHighGoingHigh	Indicates that a threshold sensor has crossed a critical high threshold going high
SensorThresholdWarningLowGoingLow	Indicates that a threshold sensor has crossed a warning low threshold going low
SensorThresholdWarningLowGoingHigh	Indicates that a threshold sensor has crossed a warning low threshold going high
SensorThresholdWarningHighGoingLow	Indicates that a threshold sensor has crossed a warning high threshold going low
SensorThresholdWarningHighGoingHigh	Indicates that a threshold sensor has crossed a warning high threshold going high
FanRedundancyLost	Indicates that system fan redundancy has been lost
FanRedundancyRegained	Indicates that system fan redundancy has been regained
FanSpeedDeviated	Indicates that fan speed has deviated from target, could indicate a faulty fan
FanSpeedRestored	Indicates that fan speed is now back to normal
IPMIWatchdog	Indicates that IPMI watchdog timed out

# Accessing the SEL 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] -C 17.

# Accessing the system event log

Step_1	List all the events. LocalServer_OSPrompt:~# ipmitool sel list	\$ ipmitool sel list 1 2020-08-05   01:04:10 EDT   Fan #0x04   Lower Critical going low   Asserted 2 2020-08-05   01:04:10 EDT   Fan #0x04   Lower Critical going low   Asserted 3 2020-08-05   01:04:10 EDT   Fan #0x07   Lower Critical going low   Asserted 4 2020-08-05   01:04:10 EDT   Fan #0x07   Lower Critical going low   Asserted 5 2020-08-05   01:04:10 EDT   Fan #0x08   Lower Critical going low   Asserted 6 2020-08-05   01:04:10 EDT   Fan #0x08   Lower Critical going low   Asserted 7 2020-08-05   01:04:10 EDT   Fan #0x08   Lower Critical going low   Asserted 8 2020-08-05   01:04:10 EDT   Fan #0x08   Lower Critical going low   Asserted 9 2020-08-05   01:04:10 EDT   Fan #0x08   Lower Critical going low   Asserted 9 2020-08-05   01:04:10 EDT   Fan #0x08   Lower Critical going low   Asserted 9 2020-08-05   01:04:10 EDT   Fan #0x08   Lower Critical going low   Asserted 9 2020-08-05   01:04:10 EDT   Fan #0x08   Lower Critical going low   Asserted 9 2020-08-05   01:04:10 EDT   Fan #0x08   Lower Critical going low   Asserted 9 2020-08-05   01:04:10 EDT   Fan #0x08   Lower Non-critical going low   Asserted 9 2020-08-05   01:04:10 EDT   Fan #0x08   Lower Critical going low   Asserted 9 2020-08-05   01:04:10 EDT   Fan #0x08   Lower Non-critical going low   Asserted 9 2020-08-05   01:04:10 EDT   Fan #0x08   Lower Non-critical going low   Asserted 9 2020-08-05   01:04:10 EDT   Fan #0x08   Lower Non-critical going low   Asserted 9 2020-08-05   01:04:10 EDT   Fan #0x09   Lower Non-critical going low   Asserted 9 2020-08-05   01:04:10 EDT   Fan #0x09   Lower Non-critical going low   Asserted 9 2020-08-05   01:04:10 EDT   Fan #0x09   Lower Non-critical going low   Asserted 9 2020-08-05   01:04:10 EDT   Fan #0x09   Lower Non-critical going low   Asserted 9 2020-08-05   01:04:10 EDT   Fan #0x09   Lower Non-critical going low   Asserted 9 2020-08-05   01:04:10 EDT   Fan #0x09   Lower Non-critical going low   Asserted 9 2020-08-05   01:04:10 EDT   Fan #0x09   Lower Non-critical going low   Asserted 9 2020-08-05   01:04:10 EDT
Step_2	To obtain more details about a specific event, use the following command. LocalServer_OSPrompt:~# ipmitool sel get [EVENT_ID]	<pre>\$ ipmitool sel get 1 SEL Record ID : 0001 Record Type : 02 Timestamp : 2020-08-05 2020-08-05 Generator ID : 0020 EWM Revision : 04 Sensor Type : Fan Sensor Number : 04 Event Type : Threshold Event Direction : Assertion Event Event Data (RAW) : 520011 Trigger Threshold : 1666,000RPM Description : Lower Critical going low Sensor ID : Fan 1 (0x4) Entity ID : 0.1 Sensor Type (Threshold) : Fan Sensor Reading : 7252 (+/- 0) RPM Status : ok Lower Kon-Recoverable : na Lower Critical : 1666,000 Upper Non-Critical : 1666,000 Upper Non-Critical : na Upper Non-Critical : na Upper Non-Critical : na Upper Non-Recoverable : na Event Enable : Event Messages Disabled Assertions Enabled : Inc- lcr- Deassertions Enabled : lnc+ lcr+</pre>

# Clearing the system event log

Version 2.0 (June 2022)

NOTE: This method will only clear the IPMI event log. The Web UI and Redfish event logs must be cleared separately.

Step_1 Use the following command to clear the system event log. LocalServer_OSPrompt:~# ipmitool sel clear \$ ipmitool sel clear Clearing SEL. Please allow a few seconds to erase.

## Exporting the system event log

# Interpreting sensor data

#### Table of contents

- Interpretation procedure
- Interpretation information
  - <u>Sensor type</u>
  - <u>Sensor event/reading type</u>
    - <u>Threshold-based event/reading type</u>

# Interpretation procedure

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

- Event ID
- Associated sensor
- Description

Refer to System event log for instructions.

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

Step_1	<ul> <li>In ipmitool , the sensor command returns a table.</li> <li>LocalServer_OSPrompt:~# ipmitool sensor</li> <li>The columns are defined as:</li> <li>Name</li> <li>Numerical reading</li> <li>Event/reading type/unit</li> <li>Unit-based sensors status/discrete sensors reading</li> <li>Lower non-recoverable threshold value</li> <li>Lower critical threshold value</li> <li>Upper noncritical threshold value</li> <li>Upper critical threshold value</li> <li>Upper non-recoverable threshold value</li> </ul>	f.jmilcol.semaor         s.000         Jappa         OK         Da         na         na<
Step_2	The numerical reading value is shown in the second column. LocalServer_OSPrompt:~# ipmitool sensor	\$ ipmitool sensor       Amps       ok       na       na       na         DC PSU lout       5,000       Amps       ok       na       na       na       na         Heater PCIel       na       discrete       0x0080       na       na       na       na         Heater PCIel       na       discrete       na       na       na       na       na         Hatter PCIel       na       discrete       na       na       na       na       na         Jumpers Status       0x0       discrete       0x0166       na       na       na       na         TelcoAlarn1       0x0       discrete       0x0180       na       na       na       na         TelcoAlarn3       0x0       discrete       0x0180       na       na       na       na         Fan 1       10388,000       RPM       ok       na       na       na       na         Fam 2       10388,000       RPM       ok       na       na       na       na         Temp CPU       28,000       degrees C       ok       na       -41,000       na         Temp CPU Area       28,000       degrees C       ok
Step_3	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 <b>OK</b> . Otherwise, the last threshold reached is displayed. Refer to <u>Threshold-based event/reading type</u> for the definitions of threshold states.	\$ ipmitool sensor         Amps         ok         na         na         na         na           DC PSU Jout         5,000         discrete         0x00 k         na         na
Step_4	An event will be created according to the assertion enabled for the specified sensor. LocalServer_OSPrompt:~# ipmitool sensor get " [SENSOR_ID]"	<pre>\$ ipmitool sensor get "Temp BMC" Locating sensor record Sensor ID : Temp BMC (0x1b) Entity ID : 0.1 Sensor Type (Threshold) : Temperature Sensor Reading : 26 (+/- 0) degrees C Status : ok Lower Non-Recoverable : na Lower Critical : -41,000 Lower Non-Critical : na Upper Non-Critical : 76,000 Upper Critical : 86,000 Upper Non-Recoverable : na Positive Hysteresis : Unspecified Negative Hysteresis : Unspecified Negative Hysteresis : Unspecified Assertion Events : Event Enable : Event Messages Disabled Assertions Enabled : lcr- unc+ ucr+ Deassertions Enabled : lcr+ unc- ucr-</pre>

# Interpretation information

cach sensor has a <u>sensor type</u> attribute and a <u>sensor event/reduing type</u> attribute. For more information about HWI sensors refer to the HWI documentation.

### 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)	Report the temperature of a platform component.
02h (Voltage)	Report a voltage present either on the power supply or the platform.
03h (Current)	Report a current output of a platform component.
04h (Fan)	General information about the fan(s) of the platform (e.g. speed, presence, failure).
08h (Power supply)	General information about the power supply (e.g. presence, failure, health status).
0Bh (Other Unit-based sensor)	Report a sensor-specific unit.
18h (Chassis)	Report the presence of an item in the chassis.
CAh (Board Reset - Kontron OEM)	Report the last restart/reboot source.
D3h (Jumpers status - Kontron OEM)	Reserved.
23h (Watchdog 2)	General information about the IPMI watchdog.
24h (Platform alert)	Report information about alerts generated by the BMC.

### 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.

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	Unit-based sensors, meaning it has a numerical reading and event triggers	Offsets are standard and defined in the <u>Threshold-based</u> <u>event/reading type</u> 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, a fan speed or a discrete state.

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	

# **Component replacement**

Refer to <u>Components installation and assembly</u> for component replacement procedures.

# **Backup and restore**

### Table of contents

- <u>UEFI/BIOS</u>
  - <u>Backing up the UEFI/BIOS</u>
  - <u>Restoring the UEFI/BIOS</u>
  - <u>Getting information on the latest UEFI/BIOS backup</u>
  - Description of creation and restoration steps
- <u>Switch NOS configuration</u>
  - Backing up and restoring the switch NOS configuration using SCP
  - Backing up and restoring the switch NOS configuration using the switch NOS Web UI

On an ME1210 platform, UEFI/BIOS and switch NOS configurations can be backed up and restored.

# **UEFI/BIOS**

This section describes how to create a UEFI/BIOS backup that includes the current UEFI/BIOS settings and perform a restore from the backup created.

Access the BMC. 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] -C 17.

## Backing up the UEFI/BIOS

For information on [BYTE1], refer to Description of creation and restoration steps.

Step_1	<ul> <li>Back up the UEFI/BIOS. This action saves the UEFI/BIOS and the configuration.</li> <li>LocalServer_OSPrompt: ~# ipmitool raw 0x3c 0x07 0x00</li> <li>Completion code: <ul> <li>0x00: Recovery process started successfully</li> <li>0xd5: Recovery process cannot be started</li> </ul> </li> </ul>	\$ ipmitool raw 0x3c 0x07 0x00
Step_2	<ul> <li>Verify the UEFI/BIOS backup status.</li> <li>LocalServer_OSPrompt: ~# ipmitool raw 0x3c 0x07 0x01</li> <li>The completion code is always 0x00.</li> <li>[BYTE0] Status: <ul> <li>0x00: Success/Idle</li> <li>0x01: In-progress</li> <li>0x02: Failure</li> <li>[BYTE1] Current step:</li> <li>Refer to the table in section Description of creation and restoration steps.</li> <li>In the image to the right, the status of the backup creation is In-progress and the current step is Set Server to Power Off state.</li> </ul> </li> </ul>	\$ ipmitool raw 0x3c 0x07 0x01 01 02

### **Restoring the UEFI/BIOS**

For information on [BYTE1], refer to <u>Description of creation and restoration steps</u>.

Step_1	<ul> <li>Restore the UEFI/BIOS. This action restores the UEFI/BIOS and the configuration.</li> <li>LocalServer_OSPrompt: ~# ipmitool raw 0x3c 0x07 0x02</li> <li>Completion code: <ul> <li>0x00: Recovery process started successfully</li> <li>0xd5: Recovery process cannot be started</li> </ul> </li> </ul>	\$ ipmitool raw 0x3c 0x07 0x02
Step_2	Verify the status of the restoration. LocalServer_OSPrompt: ~# ipmitool raw 0x3c 0x07 0x01 The completion code is always 0x00. [BYTE0] Status: • 0x00: Success/Idle • 0x01: In-progress • 0x02: Failure [BYTE1] Current step: • Refer to the table in section Description of creation and restoration steps. In the image to the right, the status of the restoration is In-progress and the current step is Set Server to Power Off state.	\$ ipmitool raw 0x3c 0x07 0x01 01 02

### Getting information on the latest UEFI/BIOS backup

Step_1	Get information on the backed up UEFI/BIOS. LocalServer_OSPrompt: ~# ipmitool raw 0x3c 0x07 0x03 Completion code: • 0x00: Backup is valid • 0xff: Backup is invalid [BYTE0-BYTE5] Version: • [1B] Major • [1B] Minor • [4B] Aux [BYTE6] Status [BYTE7-BYTE10] Unix timestamp In the image to the right, the version is 0.57.095125C7, the status is 0x00 and the timestamp is 1613153548.	\$ ipmitool raw 0x3c 0x07 0x03 00 00 39 09 51 25 c7 0c c5 26 60
--------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------

### Description of creation and restoration steps

Step description	Step value (BYTE1)	Details
No step	0×00	Nothing is currently going on, no failure to report.
Get UEFI/BIOS version	0×01	Retrieve UEFI/BIOS version over DBUS.
Server Power Off	0x02	Set server to Power Off state.
Force Intel ME Recovery mode	0x03	Force Intel ME to recovery mode.
MTD partition detect	0x04	Check flash device and partition are detected.
MTD Flash erase	0×05	Target flash being erased. Target depends on whether action is CREATE or RESTORE.
MTD Flash write	0×06	Target flash being written. Target depends on whether action is CREATE or RESTORE.
MTD Flash verify	0×07	Target flash being verified. Target depends on whether action is CREATE or RESTORE.
Reset Intel ME to Normal mode	0×08	Reset Intel ME to return to normal mode.
Server Power On	0×09	Set server to Power On state.

# Switch NOS configuration

This section describes how to backup and restore the switch NOS configuration. These operations can be achieved:

- Using <u>SCP</u>
- Using the switch NOS Web UI

### Backing up and restoring the switch NOS configuration using SCP

### Prerequisites

1	A server configured for the desired protocol is available and accessible from the switch NOS.
2	If restoring a configuration, the corresponding configuration file is present on the server.

The URL following the server IP address is a path relative to the user home folder provided ("~/"). To specify an absolute path, use a double slash after the IP address (e.g. scp://<SERVER_USERNAME>:<SERVER_PASSWORD>@<SERVER_IP>//<path/to/configfile>).

Refer to <u>Accessing the switch network operating system</u> for access instructions.

### Backing up the switch configuration

Step_1	Access the switch network operating system using SSH or a serial connection.
Step_2	<ul> <li>Copy the desired configuration to the remote server.</li> <li>running-config : configuration currently active (may differ from startup-config if changes were made since the last boot, but not saved).</li> <li>startup-config : saved configuration applied at switch boot.</li> <li>LocalSwitchNO5_OSPrompt:~# copy <running-config startup-config> scp://<server_username>:</server_username></running-config startup-config></li> <li><server_password>@<server_ip>/<file_path> save-host-key</file_path></server_ip></server_password></li> </ul>
	# copy startup-config scp://user:password@192.168.0.10/ startup-config save-host-key % Saving 1506 bytes to server 192.168.0.10: startup-config

# Restoring the switch configuration

Step_1	_1 Access the switch network operating system using SSH or a serial connection.	
Step_2	<ul> <li>Copy the configuration file from the remote server as one of the following:</li> <li>running-config : configuration currently active (volatile until saved as startup-config).</li> <li>startup-config : saved configuration applied at switch boot.</li> <li>LocalSwitchNOS_OSPrompt:~# copy scp://<server_username>:</server_username></li> <li><server_password>@ <server_ip>/<file_path> <running-config startup-config> save-host-key</running-config startup-config></file_path></server_ip></server_password></li> </ul>	# copy scp://user:password@192.168.0.10/startup-config startup-config save-host-key % Saving 1506 bytes to flash:startup-config
Step_3	If the configuration was written to the startup-config, the switch NOS must be rebooted for the changes to take effect. LocalSwitchNOS_OSPrompt:~# <b>reload cold</b>	# reload cold % Cold reload in progress, please stand by.

## Backing up and restoring the switch NOS configuration using the switch NOS Web UI

Access the switch NOS Web UI. Refer to <u>Accessing the switch NOS</u> for access instructions.

# Backing up the switch configuration

Step_1	<ul> <li>From the left-side menu of the switch NOS Web UI, select Maintenance , then Configuration , and then Download . Choose the configuration to back up:</li> <li>running-config : configuration currently active (may differ from startup-config if changes were made since the last boot, but not saved).</li> <li>default-config : configuration applied when the default configuration is reloaded.</li> <li>startup-config : saved configuration applied at switch boot.</li> </ul>	Configuration         Montor         Dagnostics         Maintenance         Resider Device         Resider Device         Vignad         Uptade         Image Select         Configuration         Select configuration file to save.         Presider Device         Select configuration file to save.         Configuration         Select configuration         Device do Configuration
Step_2	Click <b>Download Configuration</b> , then select where to save configuration file.	Configuration         Monitor         Diagnostics         Manitenance         Restart Device         Restart Device         Raditory Octanuts         Software         Configuration file to save.         Pactory Octanuts         Software         Control Configuration         Software         Software         Control Configuration         Software         Software         Software         Software         Software         Control Configuration         Software         Soft

# Restoring the switch configuration

Step_1	From the left-side menu of the switch NOS Web UI, select ${\bf Maintenance}$ , then	🚱 kontron
	<b>Configuration</b> , and then <b>Upload</b> . Click <b>Choose file</b> . Then, using the pop-up file browser, select the desired configuration file to restore.	<ul> <li>Configuration</li> <li>Monitor</li> <li>Diagnostics</li> <li>Maintenance</li> <li>Restar Device</li> <li>Factory Defaults</li> <li>Software</li> <li>Upload</li> <li>Image Select</li> <li>Configuration</li> <li>Save statup-config</li> <li>Device</li> <li>File Name</li> <li>Parameters</li> <li>Create new file</li> <li>Upload</li> <li>Upload</li> <li>Upload</li> <li>Upload</li> <li>Upload</li> <li>Upload</li> <li>Upload</li> <li>Choose file No file chosen</li> <li>Destination File</li> <li>Upload</li> </ul>
Step_2	<ul> <li>Choose the configuration to restore:</li> <li>running-config : configuration currently active (volatile until saved as the startup-config). This selection allows fully replacing or merging on top of the current running-config.</li> <li>startup-config : saved configuration applied at switch boot.</li> <li>Create new file : creates a new configuration entry that can be subsequently activated using the Maintenance → Configuration → Activate path of the menu.</li> <li>NOTE: A default-config cannot be written to, but a previously backed up default-config can be written to as one of these options.</li> </ul>	<ul> <li>Configuration</li> <li>Nonitor</li> <li>Diagnostics</li> <li>Maintenance</li> <li>Restart Device</li> <li>Factory Defaults</li> <li>Software</li> <li>Upload</li> <li>Configuration</li> <li>Sweaturp.config</li> <li>Restartup-config</li> <li>Restartup-config</li> <li>Restartup-config</li> <li>Startup-config</li> <li>Startup-config</li> <li>Create new file</li> <li>Create new file</li> <li>Upload Configuration</li> </ul>
Step_3	Click Upload Configuration .	<ul> <li>Configuration</li> <li>Monitor</li> <li>Diagnostics</li> <li>Maintenance</li> <li>Restart Device</li> <li>Factory Defaults</li> <li>Software</li> <li>Upload</li> <li>Image Select</li> <li>Configuration</li> <li>Destination File</li> <li>Deteite</li> </ul>
Step_4	If the configuration was written to as startup-config, the switch NOS must be rebooted for changes to take effect. This can be achieved by selecting <b>Maintenance</b> , then <b>Restart Device</b> from the left-side menu. Then, confirm that a restart is to be performed by clicking <b>Yes</b> .	<ul> <li>Configuration</li> <li>Nointor</li> <li>Diagnostics</li> <li>Maintenance</li> <li>Restart Device</li> <li>Factory Derivation</li> <li>Software</li> <li>Upload</li> <li>Ingestett</li> <li>Configuration</li> <li>Sestartp-configuration</li> <li>Ses</li></ul>

# Upgrading

### Table of contents

- <u>Upgrading BMC and FPGA firmware</u>
  - Upgrading the firmware of the BMC and the FPGA using Redfish
    - <u>Prerequisites</u>
    - <u>Procedure</u>
  - Upgrading the firmware of the BMC and the FPGA using the Web UI
    - Prerequisites
    - <u>Procedure</u>
- <u>Upgrading UEFI/BIOS firmware</u>
  - <u>Upgrading UEFI/BIOS firmware using the built-in UEFI shell and a USB storage device</u>
    - <u>Prerequisites</u>
    - <u>Procedure</u>
  - Upgrading UEFI/BIOS firmware using the built-in UEFI shell and a UEFI-compatible operating system
    - <u>Prerequisites</u>
    - <u>Procedure</u>
  - <u>Upgrading UEFI/BIOS firmware from the server operating system</u>
    - Prerequisites
    - <u>Procedure</u>
- Upgrading switch firmware
  - <u>Upgrading switch firmware using SCP</u>
    - <u>Prerequisites</u>
    - <u>Procedure</u>
  - Upgrading the switch firmware using the switch NOS Web UI

# **Upgrading BMC and FPGA firmware**

BMC and FPGA firmware is upgraded using the same methods. Only the content of the archive provided by Kontron will differ depending on the component(s) to upgrade. The following examples document a BMC firmware upgrade.

**NOTE:** For the upgrade to work, the upgrade image version must be different from the one running on the BMC. In other words, it is not possible to upgrade with the same version.

Relevant sections:

Description of system access methods Accessing a BMC

BMC and FPGA firmware can be upgraded:

- Using <u>Redfish</u>
- Using the Web UI

### Upgrading the firmware of the BMC and the FPGA using Redfish

Redfish is the preferred interface for upgrading BMC and FPGA firmware.

### Prerequisites

Releva	ant section:
2	Access to the BMC Redfish interface is required.
1	The .tar file provided by Kontron was downloaded on the remote computer.

Accessing a BMC using Redfish

### Procedure

The following procedure is for upgrading the firmware of a BMC and can be applied to upgrade the firmware of an FPGA.

Step_1	From the BMC Redfish interface, verify the current firmware version. RemoteComputer_OSPrompt:~\$curl-k-srequest GETurl [ROOT_URL]/redfish/v1/Managers/bmc   jq .FirmwareVersion \$ curl-k-srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc   jq
Step_2	Verify that the new firmware isn't already uploaded to the platform using the URL returned by this command. Otherwise, the BMC
	RemoteComputer_OSPrompt:~\$curl -k -srequest GETurl

	[ROOT_URL]/redfish/v1/UpdateService/FirmwareInventory jq		
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1/UpdateService/F irmwareInventory   jq</pre>		
	<pre>{     "Godata.id": "/redfish/v1/UpdateService/FirmwareInventory",     "@odata.type": "#SoftwareInventoryCollection.SoftwareInventoryCollection",     "Mombare".</pre>		
	<pre>-venubis's t {     "@odata.id": "/redfish/vl/UpdateService/FirmwareInventory/8c50fd55" }.</pre>		
	<pre>"@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/c172d3d8" }.</pre>		
	<pre>{     "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/d6bcd2a6" }; </pre>		
	<pre>{     @odata.id": "/redfish/v1/UpdateService/FirmwareInventory/ebbd5d7b" }</pre>		
	]; "Members@odata.count": 4, "Name": "Software Inventory Collection"		
Step_3	Verify that the new firmware version doesn't match the version of a firmware inventory entry. If necessary, repeat for all firmware inventory entries.		
	RemoteComputer_OSPrompt:~\$curl -k -srequest GETurl		
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1/UpdateService/F</pre>		
	irmwareInventory/d6bcd2a6   jq .Version [ "1.02.09579455"		
Step_4	Set the apply time of the firmware update to UnReset . RemoteComputer_OSPrompt:~\$ curl -k -srequest PATCHurl [ROOT_URL] /redfish/v1/UpdateServiceheader		
	'Content-Type: application/json'data '{"HttpPushUriOptions": {"HttpPushUriApplyTime": {"ApplyTime": "OnReset"}}}'		
	\$ curl -k -srequest PATCHurl https://admin:ready2go@172.16.182.31/redfish/v1/UpdateService		
	feader 'Content-Type: application/json'data '{"HttpPushorloptions": {"HttpPushorlApplyTime": "OnReset"}}}'   jq		
Step_5	Upload the BMC firmware by executing the following command. The BMC should return a TaskService URL.		
	'Content-Type: application/octet-stream'upload-file ' [FILE_PATH]'   jq		
	<pre>\$ curl -k -srequest POSTurl https://admin:ready2go@172.16.182.31/redfish/v1/UpdateService header 'Content-Type: application/octet-stream'upload-file 'update.tar'   jq</pre>		
	<pre>"@odata.id": "/redfish/v1/TaskService/Tasks/1", "@odata.type": "#Task.v1_4_3.Task", "rd#. =1"</pre>		
	"TaskState": "Running", "TaskStatus": "OK" }		
Step_6	Using the URL returned by the previous step, ensure that the task is completed. <b>PercentComplete</b> value should be 100 before		
	proceeding with the next steps. It may take several seconds.		
	.PercentComplete		
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1/TaskService/Tas ks/1   jq .PercentComplete</pre>		
	1 100 1		
Step_7	Reboot the BMC and wait for the BMC to power on.		
	RemoteComputer_OSPrompt:~\$ curl -k -srequest POSTurl [ROOT_URL] /redfish/v1/Managers/bmc/Actions/Manager.Resetbeader 'Content-Type: application/ison'data '{"ResetType":		
	"GracefulRestart"}' jq		
	NOTE: When upgrading the FPGA firmware, the firmware activation process will automatically reboot the BMC.		
	ctions/Manager.Resetheader 'Content-Type:application/json'data '{"ResetType":"GracefulRest art}'   jq {		
	"@Message.ExtendedInfo": [ { "@odata.type": "#Message.vl_1_1.Message",		
	<pre>"Message": "Successfully Completed Request", "MessageArgs": [], "MessageId": "Base.1.8.1.Success",</pre>		
	"MessageSeverity": "OK", "Resolution": "None" }		
Step_8	Once the BMC becomes available again, verify that the firmware version has changed. RemoteComputer_OSPrompt:~% curl _k _srequest GETurl [ROOT_URL]/redfish/v1/Managers/hmc Lin		
	.FirmwareVersion		
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go@172.16.182.31/redfish/v1/Managers/bmc   jq .FirmwareVersion "2.00.015afd1b"</pre>		
	*2.00.015afd1b*		

# Upgrading the firmware of the BMC and the FPGA using the Web $\ensuremath{\mathsf{UI}}$

## Prerequisites

– Releva	ant section:
2	Access to the BMC Web UI is required.
1	The .tar file provided by Kontron was downloaded on the remote computer.

Accessing a BMC using the Web UI

# Procedure

The following procedure is for upgrading the firmware of a BMC and can be applied to upgrade the firmware of an FPGA.

Step_1	From the left-side menu of the BMC Web UI, click on <b>Operations</b> and then on <b>Firmware</b> .	Cverview	Overview	ම Health ම Power € Refresh ® admin -
		KVM	BMC time 2021-11-20 16:35:58 UTC	Server LED
		Firmware	Edit network settings	$\rightarrow$ SOL console $\rightarrow$
		<ul> <li>Operations</li> <li>Settings</li> </ul>	RMC information	Server information
		Security and access	Firmware version 2.00.0159fce6	Set Vet III.0111141UOTI Model Mandaturer (PRODUCT_NAME] Konton Serial number UET venion 9017064072 1.02.09579455
Step_2	Verify the current firmware version. Make sure that the new firmware is more recent	Firmware		
		BMC		
		Running image	Back	kup image
		Version	Versi	on
		2.00.01603cd7	2.00.	.0159fce6
			2	Switch to running
Step_3	From the <b>Update firmware</b> section, choose a <b>.tar</b> file to upload for the BMC by clicking on <b>Select file</b> .	Update firm	nware	
Step_4	Click on Start update . Image file			
		Start update		
Step_5	When the file has successfully been uploaded, a success message should appear in the top right corner.		orner.	
Step_6	Wait for the BMC to update. The page should refresh automat	ically once the update	e succeeded.	
Step_7	Once the BMC becomes available again, verify that the	Firmerica		
	firmware version has changed.	BMC		
		Running image	Back	cup image
		Version 2.00.016054c2	Versic 2.00: ₹	on 01603cd7 Switch to running

# Upgrading UEFI/BIOS firmware

UEFI/BIOS firmware can be upgraded:

- Using the built-in UEFI shell and a USB storage device
- Using the built-in UEFI shell and a UEFI-compatible operating system
- From a <u>Linux-based operating system</u>

### Upgrading UEFI/BIOS firmware using the built-in UEFI shell and a USB storage device

### Prerequisites

1	The .zip archive provided by Kontron has been downloaded.	
2	Access to the UEFI/BIOS menu is required.	
З	The USB storage device was formatted using fat32 .	
Relevant section:		

## Accessing the UEFI or BIOS

#### Procedure

Step_1	From another computer, extract the archive content provided by Kontron to a USB storage device. The <b>startup.nsh</b> file should be located directly in the root folder of the USB storage device. <b>NOTE:</b> Some of the archive content can change depending on the upgrade version.	• > UNTITLED 2 (D:) • C efi firmware lan startup.nsh
Step_2	Insert the USB storage device in one of the USB ports of the front panel.	
Step_3	Power on the platform and access the UEFI/BIOS setup menu.	
Step_4	Navigate to the <b>Save &amp; Exit</b> menu and then to the <b>Boot Override</b> section. Select the option that represents the USB storage device and press <b>Enter</b> . The built-in EFI Shell should launch.	Aptio Setup Utility - Copyright (C) 2021 American Megatrends, Inc.         < Security Boot Save & Exit
Step_5	Press any key other than ' <b>q</b> ' to continue. The UEFI/BIOS upgrade should start.	FS0: FS1: BIOS UPDATE STARTING Enter 'q' to quit, any other key to continue: AMI Firmware Update Utility Manufacture v5.13.00.05 for Kontron (64 Bits) Copyright (c) 1955-2820, American Megatrends International LLC. All rights reserved. Subject to AMI licensing agreement. Reading flash Done Reading flash Done Pass - System Secure Flash Pass - Check RomLayout Pass - Check RomLayout Done Erasing Main Block Bx000A33000 (B8%)
Step_6	Once completed, the BMC and the platform will automatically reset. It may ta remote connection might be lost.	ake several seconds to complete the power cycle and the

### Upgrading UEFI/BIOS firmware using the built-in UEFI shell and a UEFI-compatible operating system

### Prerequisites

4	Access to the OS is required.
3	A Linux UEFI-compatible operating system is installed on the platform.
2	Access to the UEFI/BIOS menu is required.
1	The .zip archive provided by Kontron has been downloaded.

### Relevant sections: Accessing the UEFI or BIOS Accessing the operating system of a server

### Procedure

Step_1	P ower on the platform and access the operating system.		
Step_2	Once the archive is downloaded to the platform, decompress the .tar.gz arc LocalServer_OSPrompt:~# tar -xfv [FILE_NAME].tar.gz	hive on the Linux OS installed on the platform .	
Step_3	Copy the content of the archive to the /boot/efi directory. LocalServer_OSPrompt:~# cp -a [PATH_TO_ARCHIVE]/. /boot/efi/	<pre>[root@localhost ~]# cp -a /home/archive/. /boot/efi/</pre>	
Step_4	Verify that the <b>startup.nsh</b> script can be found directly in the <b>/boot/efi</b> directory. LocalServer_OSPrompt:~# <b>ls /boot/efi</b> <b>NOTE</b> : Some of the content of the archive could change depending on the version.	<pre>[root@localhost ~]# ls /boot/efi EFI firmware lan startup.nsh</pre>	
Step_5	Reboot the platform and access the UEFI/BIOS setup menu.		
Step_6	Navigate to the <b>Save &amp; Exit</b> menu and then to the <b>Boot Override</b> section. Select the option that corresponds to the <b>UEFI: Built-in EFI Shell</b> and press <b>Enter</b> . The built-in EFI Shell should launch.	Aptio Setup Utility - Copyright (C) 2021 American Megatrends, Inc.         < Security Boot Save & Exit	
Step_7	Press any key other than ' <b>q</b> ' to continue. The UEFI/BIOS upgrade should start.	FS0: FS0: FS1: BIOS UPDATE STARTING Enter'q'to quit, any other key to continue: AMI Firmware Update Utility Manufacture v5.13.00.05 for Kontron (64 Bits) Copyright (c) 1985-2020, American Megatrends International LLC. All rights reserved. Subject to AMI licensing agreement. Reading flash	
Step_8	Once completed, the BMC and the platform will automatically reset. It may t remote connection might be lost.	ake several seconds to complete the power cycle and the	

# Upgrading UEFI/BIOS firmware from the server operating system

## Prerequisites

1	The .tar.gz archive provided by Kontron has been decompressed on a Linux OS installed on the platform .	
2	A Linux-based OS is installed on the platform.	
Relevant section: Accessing the operating system of a server		

Step_1	Access the operating system and open a command line interface.
Step_2	Uncompress the .tar.gz archive on the Linux OS installed on the platform . LocalServer_OSPrompt:~# tar -xfv [FILE_NAME].tar.gz
Step_3	Access the folder created by the archive. LocalServer_OSPrompt:~# cd [FILE_NAME]
Step_4	E xecute the upgrade script. LocalServer_OSPrompt:~# ./update.sh NOTE: It may take a moment for the UEFI/BIOS firmware upgrade to complete.

# Upgrading switch firmware

Switch firmware can be upgraded using:

- <u>SCP</u>
- The switch NOS Web UI

### Upgrading switch firmware using SCP

### Prerequisites

1	A server configured for the desired protocol is available and accessible from the switch NOS.
2	The . itb upgrade file provided by Kontron was downloaded on the server.

# Accessing the switch NOS

Relevant section:

### Procedure

1	The URL following the server IP address is a path relative to the user home folder provided ("~/"). To specify an absolute path use a double slash after the IP address (e.g. scp://[SERVER_USERNAME]: [SERVER_PASSWORD]@[SERVER_IP]//[path/to/filename.itb]).	
ΝΟΤΙΟ	It is imperative that the file that will be uploaded to the switch has the .itb extension. If a file with another extension is uploaded, a complex recovery procedure would have to be performed. Should this situation occur, contact customer support.	
Step_1	Access the switch NOS using SSH or a serial connection.	
Step_2	Initiate firmware download and upgrade. LocalSwitchNOS_OSPrompt:~# firmware upgrade scp://[SERVER_USERNAME]: [SERVER_PASSWORD]@[SERVER_IP]/[FILE_PATH] save-host-key	
	<pre># firmware upgrade scp://user:password@192.168.0.1/ istax_kci0.09.01494556.itb save-host-key Downloading Got 18510664 bytes Starting flash update - do not power off device!</pre>	
Step_3	Wait for the switch NOS to reboot after the upgrade completes.	
Step_4	Confirm the upgrade was successful by checking the firmware version. LocalSwitchNOS_OSPrompt:~# <b>show version</b> In the results, look for the version in the Primary Image section. In the image, the version is 1.01.0161bc08.	
	Primary Image              Image         : linux (&ctive)           Version         : Kontron S1901 NOS IStaX 1.01.0161bc08           Date         : 2022-02-24T11:08:01-05:00	

# Upgrading the switch firmware using the switch NOS Web UI

NOTE: While being functional, this method is currently not preferred since it is subject to change.

#### Relevant section:

Accessing the switch NOS using the switch NOS Web UI

Step_1	From the left-side menu of the switch NOS Web UI, select Maintenance , Software and then Upload .	Software Upload
Step_2	Click the <b>Select File</b> button and then choose the desired. <b>itb</b> file.	System     Secret File o     If selected     Start Upgrade     Upload status: Idle
Step_3	After selecting the file for the upgrade, click on <b>Start Upgrade</b> .	Software Upload         Software Upload         System         Green Elternet         Thermal Protection         Ports
Step_4	Wait for the upload and upgrade process to complete.	<ul> <li>Configuration</li> <li>System</li> <li>Green Einenet</li> <li>Thermal Protection</li> <li>Ports</li> <li>CFM</li> <li>APS</li> <li>ERPS</li> <li>Link OAM</li> <li>DHCPV4</li> <li>DHCPv4</li> <li>Security</li> </ul>
Step_5	Once the upgrade is done, from the left-side menu, select <b>Monitor</b> , <b>System</b> and then <b>Information</b> . Confirm that the <b>Software Version</b> corresponds to that of the .itb file.	Kontron     Configuration     Configuration     Monitor     System     System     Contact     System     Contact     NoStonADA5E02722     Location     Contact     Name     NOStonADA5E02722     Location     Contact     Name     NOStonADA5E02722     Location     Hardware     MacAddress     Orea-s5-s0-27-22     Chip ID     VSCRee     System Date     System     System Date     System Vol-047HS22.48+00:00     System Date     System Orl-047HS22.48+00:00     System Date     System Date     Software     Softwa
### Platform cooling and thermal management

#### Table of contents

- Behavior upon startup at temperatures below 0°C
- <u>Behavior at temperatures below or above 10°C</u>
- Cooling management
  - <u>Cooling management characteristics</u>
- Fan fault detection method
- Default temperature thresholds

#### Relevant sections:

Environmental considerations Sensor list

Configuring sensors and thermal parameters

The ME1210 platform can operate within an ambient temperature range of:

- -40°C to +65°C when using a DC PSU
- -5°C to +50°C when using an AC PSU



Fans may not be running when the ambient temperature is below 10°C.

### Behavior upon startup at temperatures below 0°C

The system is designed to operate in a cold environment, but for all components to run in their specified temperature ranges, the system needs to be heated before startup. Heating elements are built in for the CPU and, optionally, for the PCIe add-in cards.

- When the platform is started at temperatures below 0°C, an internal heating element preheats the components sensitive to cold prior to the board power on.
- Once the temperature of these components exceeds 0°C, the server is powered on.
- This behavior is communicated through platform LEDs. For more information, refer to General platform LEDs.

### Behavior at temperatures below or above 10°C

The ambient temperature is measured by sensor Temp Inlet.

- When the **ambient temperature is below 10°C** and no sensor has exceeded its temperature thresholds, the fans will be on standby (not running and making no sound).
- When the ambient temperature is above 10°C, the fans will be started and run at 8% of their maximum capacity.
- If, at any ambient temperature, it is detected that a sensor reaches its Upper non-critical threshold, fan cooling will engage to ensure that no component is overheating.



### **Cooling management**

The cooling management of the platform is handled by an 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. For each sensor, the temperature reading is compared against corresponding configured thresholds to determine the required fan speed. The resulting duty cycle is based on cooling parameters, such as minimum and maximum fan speed, and gets linearly increased when a temperature reading gets between the Upper non-critical and Upper critical thresholds for that sensor. The fan control behavior can be fine-tuned by configuring these thresholds to match the target environment.

In addition to the sensors read by the BMC, other sensors can be read by a customer application, if available, running under the server's OS and

then reported to the BMC. As such, PCIe add-in card temperatures, as well as M.2 and SFP temperatures, can be reported to the BMC by the customer application and considered by the fan speed regulator in its computation for thermal management function. Thresholds for these sensors can be configured as well.

#### **Cooling management characteristics**

- Minimum fan speeds are set to 8%.
- Minimum ambient temperature is set to 10°C. Above this temperature, fans will be running. Below this temperature, fans will be stopped but ready to start if a component requires cooling.
- Fans are started before reaching their threshold value using a threshold offset parameter.
- Fan speed deviation is monitored for failure.
- A watchdog timer sets fans to 100% if the BMC does not issue control commands. This will normally occur while the BMC reboots, for example, during a firmware upgrade.
- A BMC firmware upgrade failsafe sets fan speed to 100% during a BMC firmware upgrade or reboot.
- A small negative slew rate applies on fan speed to ensure a slow decrease in fan speed and prevent fan oscillation.
- Fast response to temperature rise.
- Fan redundancy.

#### Fan fault detection method

To detect faulty fans, the speed of each fan is continuously monitored and compared to the target value sent by the fan controller. If the fan speed is out of range by  $\pm 15\%$  for 30 seconds, the fan is marked as faulty and a Redfish event is sent. The fan can later be restored if the speed comes back within the deviation range for a steady period of 5 seconds.

All the fans are redundant. This means that when a fan is faulty, all the other healthy fans will be set to maximum speed. To access the SEL using Redfish to see the events, refer to <u>System event log</u>.

```
{
 "@odata.context": "/redfish/v1/$metadata#LogEntry.LogEntry",
 "@odata.id": "/redfish/v1/$ystems/system/LogServices/EventLog/Entries/#1614699759_4",
 "@odata.type": "#LogEntry.v1 4 0.LogEntry",
 "Created": "2021-03-02115:42:39+00:00",
 "EntryType": "Event",
 "Id": "1614699759_4",
 "Message1": "Fan_1"
],
 "Message1": "OpenBMC.0.1.FanSpeedDeviated",
 "Name": "System Event Log Entry",
 "Godata.tod": "/redfish/v1/$metadata#LogEntry.LogEntry",
 "Godata.type": "/redfish/v1/$metadata#LogEntry.LogEntry",
 "Godata.type": "/redfish/v1/$metadata#LogEntry.LogEntry",
 "Godata.type": "#LogEntry.v1_4 0.LogEntry",
 "Godata.type": "#LogEntry.v1_4 0.LogEntry",
 "Godata.type": "#LogEntry.v1_4 0.LogEntry",
 "Created": "2021-03-02115:42:44+00:00",
 "EntryType": "Event",
 "Id": "1614699764_4",
 "MessageF: "Fan_1"
],
 "MessageF: "Fan_1"
],
 "MessageF: "Fent",
 "Id": "1614699764_4",
 "MessageF: "Fent",
 "MessageI: "GonenBMC.0.1.FanSpeedRestored",
 "Mame": "System Event Log Entry",
 "Severity": "0K"
},
```

### **Default temperature thresholds**

To see temperature thresholds, refer to the instructions provide d in Monitoring sensors and Configuring sensors and thermal parameters.

# Troubleshooting

- <u>Collecting diagnostics</u>
- <u>Factory default</u>
- Support information

## **Collecting diagnostics**

#### Table of contents

- <u>Collecting the FRU information</u>
  - <u>Collecting the FRU information using the BMC Web UI</u>
  - <u>Collecting the FRU information using IPMI</u>
- <u>Collecting the BMC firmware version</u>
  - <u>Collecting the BMC firmware version using the BMC Web UI</u>
  - <u>Collecting the BMC firmware version using Redfish</u>
- <u>Collecting the BMC event log</u>
- <u>Collecting hardware configuration information</u>
  - <u>Collecting power supply type (AC or DC)</u>
    - <u>Collecting power supply type using the BMC Web UI</u>
    - <u>Collecting power supply type using Redfish</u>
    - <u>Collecting power supply type using IPMI</u>
  - <u>Collecting product IO module information</u>
    - <u>Collecting product IO module information using the BMC Web UI</u>
    - <u>Collecting product IO module information using Redfish</u>
  - <u>Collecting product IO module information using IPMI</u>
     <u>Collecting memory device configuration</u>
    - <u>Collecting memory device configuration</u>
    - Collecting memory device configuration using Redfish
  - Collecting the Ethernet switch running configuration
- <u>Collecting the Ethernet switch event log</u>

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

- The FRU information
- The BMC firmware version
- The BMC event log

٠

- Hardware configuration
- The Ethernet switch running configuration (optional)
- The Ethernet switch event log (optional)

Collecting all this data beforehand can accelerate the process.

## **Collecting the FRU information**

Collecting the FRU information can be performed using the following methods:

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

#### Collecting the FRU information using the BMC Web UI

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



#### Collecting the 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 (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] -C 17.

Step_1	Use the following command to collect the FRU information. LocalServer_OSPrompt:~# ipmitool fru print	<pre># ipmitool fru print FRU Device Description : Builtin FRU Device (ID 0) Chassis Type : Main Server Chassis Chassis Part Number : XXXX-XXXX Chassis Serial : XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</pre>
	Take note this command wil return all detected FRU devices including PCIe addons card with FRU EEPROM (Intel N3000 in this example).	Chassis Serial : XXXXXXXX Chassis Extra : MEI210 Board Mfg Date : Wed Apr 7 13:30:00 2021 Board Mfg C : Kontron Board Product : ME1210 Board Serial : 9017064072 Board Part Number : 1067-2338 Board Extra : MAC=00:A0:A5:E1:0E:20/07 Product Mane : ME1210 Product Name : ME1210 Product Part Number : 1067-2338 Product Version : Product Serial : 9017064072 Product Serial : 901706775 Board Mfg C : Kontron Board Product : ME1210-PSU-DC Board Serial : 9017067765 Board Part Number : 1067-4309 FRU Device Description : ME1210-SW-X (ID 212) Board Mfg C : Kontron Board Product : ME1210-SW-X (ID 212) Board Mfg C : Kontron Board Product : ME1210-SW-X Board Serial : XXXXXXXXX Board Part Number : MAC=CC:CC:CC:CC:CC:CC/DD

### Collecting the BMC firmware version

Collecting the BMC firmware version can be performed using the following methods:

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

#### Collecting the BMC firmware version using the BMC Web UI

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

Step_1	From the left-side menu of the BMC Web	<b>&amp;</b> kontron		🥝 Health	Over	C Refresh	(admin +	
	UI, select <b>Operations</b> and then <b>Firmware</b>	⊡     Overview       Image: Example of the second s	Overvie	W				
		➡         Hardware status         ∨           ⇒         Operations         ∧	BMC time 2021-11-20 16:35:5	a UTC	Server LED			
		KVM Firmware	Edit network sett	tings →	SOL console		→	
		Reboot BMC       SOL console       Server power operations       Virtual media       Stettings     ~       Security and access     ~	BMC inform Firmware version 2.00.0159fce6	nation	Server ir Model [PRODUCT_N. Serial number 9017064072	formatio Manufa AME] Kontro UEFI ve 1.02.09	N nn rsion 9579455	
Step_2	The BMC, UEFI/BIOS and FPGA firmware versions will be displayed.	Firmware BMC						
		Running image		Backup image				
		Version 2.00.015afd1b		Version 2.00.0159fce6				
		UEFI						
		Running image						
		Version 1.02.09579455						
		FPGA						
		Running image						
		Version 1.02.080051ee						

#### Collecting the BMC firmware version using Redfish

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



## Collecting the BMC event log

To collect the BMC event log please refer to the System event log section.

### **Collecting hardware configuration information**

Hardware configuration information might be required to make the proper board health diagnostics. The following list contains basic examples of information that could help the Kontron support team.

- Power supply type (AC or DC)
- Product IO board configuration
- Memory device configuration

#### Collecting power supply type (AC or DC)

Collecting the power supply type can be performed using the following methods:

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

#### Collecting power supply type using the BMC Web UI

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

Step_1	From the left-side menu of the BMC Web UI, select Hardware status and then Inventory and LEDs .	Image: Sensors       Image: Sensors         Image: Sensors       Sensors         Image: Sensors       Sensors         Image: Sensors       Sensors         Image: Sensors       Solution         Sensors       Solution         Sensors       Solution         Sensors       Solution         Image: Sensors       Solution         Sensors       Solution         Sensors       Solution         Image: Sensention       Solution <td< th=""></td<>
Step_2	From the <b>Power supplies</b> section, collect the power supply type.	Power supplies Q Search 1 items ↓ ID ↓ Health ↓ Location number Identify LED ↓ DC_PSU OK

#### Collecting power supply type using Redfish

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



#### Collecting power supply type 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] -C 17.

Step_1	Use the following command to collect the FRU information. LocalServer_OSPrompt:~# ipmitool fru print	<pre># ipmitool fru print FRU Device Description : Builtin FRU Device (ID 0) Chassis Type : Main Server Chassis Chassis Part Number : XXXX-XXXX</pre>
	Power supply types: AC PSU: M1877 DC PSU: ME1210-PSU-DC	Chassis Serial : XXXXXXXXX Chassis Extra : MEL210 Board Mfg Date : Wed Apr 7 13:30:00 2021 Board Mfg : Kontron Board Product : MEL210 Board Serial : 9017064072 Board Part Number : 1067-2338 Board Extra : MAC=00:A0:A5:E1:0E:20/07 Product Manufacturer : Kontron Product Name : MEL210 Product Varsion : Product Version : Product Serial : 9017064072 Product Serial :
		FRU Device Description : ME1210-PSU-DC (ID 74)Board Mfg Date : Mon Jun 1 04:00:00 2020Board Mfg : KontronBoard Product : ME1210-PSU-DCBoard Serial : 9017067765Board Part Number : 1067-4309
		FRU Device Description : ME1210-SW-X (ID 212)Board Mfg Date : Mon Aug 12 11:55:00 2019Board Mfg : KontronBoard Product : ME1210-SW-XBoard Serial : XXXXXXXXXBoard Part Number :Board Extra : MAC=CC:CC:CC:CC:CDD

#### Collecting product IO module information

Collecting the product IO module information can be performed using the following methods:

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

#### Collecting p roduct IO module information using t he BMC Web UI

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

Step_1 From the left-side menu of the BMC Web UI, select Hardware status and then Inventory and LEDs .	Nontread       Overview       Logs       Hardware stat       Inventory ar       Sensors       Operations       Settings       Security and	access	Overvi BMC time 2021-11-20 1633 Edit network s BMC infor Firmware version 2.00.0159Fc66	Health     (     eW     sseurc     stings     →     ss mation     S	Power      Refresh     @ adr      wr LED     off      OI. console     →      console     //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //      //
Step_2       From the Chassis section, collect the IO module information. If needed, expand the IO module board information by using the left-side arrow.	Chass ~	ID Baseboard Switchboard Part number: Serial number: X Model: Asset tag: Manufacturer: Ki Chassis type: Rai	Health OK OK OK A A A A A A A A A A A A A	Location number	Identify LED  Off

#### Collecting product IO module information using Redfish

Refer to Accessing a BMC using Redfish for access instructions.



#### Collecting product IO module 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 (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] -C 17.

Step_1	Use the following command to collect the FRU information. LocalServer_OSPrompt:~# ipmitool fru print IO module type: Switchboard = ME1210-SW-X IOBoard = ME1210-IOS	<pre># ipmitool fru print FRU Device Description Chassis Type Chassis Part Number Chassis Serial Chassis Extra Board Mfg Date Board Product Board Product Board Part Number Board Extra Product Manufacturer Product Name Product Version Product Version Product Version Product Version Product Serial Product Asset Tag FRU Device Description Board Mfg Board Product Board Serial Board Product Board Serial Board Part Number</pre>	<pre>: Builtin FRU Device (ID 0) : Main Server Chassis : XXX-XXXX : XXXXXXXXXX : ME1210 : Wed Apr 7 13:30:00 2021 : Kontron : ME1210 : 9017064072 : 1067-2338 : MAC=00:A0:A5:E1:0E:20/07 : Kontron : ME1210 : 1067-2338 : : 9017064072 : : ME1210-PSU-DC (ID 74) : Mon Jun 1 04:00:00 2020 : Kontron : ME1210-PSU-DC : 9017067765 : 1067-4309</pre>	
		FRU Device Description Board Mfg Date Board Product Board Serial Board Part Number Board Extra	: ME1210-SW-X (ID 212) : Mon Aug 12 11:55:00 2019 : Kontron : ME1210-SW-X : XXXXXXXXXX : : MAC=CC:CC:CC:CC:CC/DD	

#### Collecting memory device configuration

Collecting the memory device configuration can be performed using the following method:

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

#### Collecting memory device configuration using the BMC Web UI

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

Logs       ↓         Imathy and LEDs       BMC information         Sensors       ↓         Operations       ↓         Settings       ↓         Security and access       ↓         BMC information       ↓         JOURD Security and access       ↓	ver LED Off SOL controle → Server information Maski Mandatume PRODUCT_NAME Kontron S017064072 UFF1version 1.02.09579455
Step_2     From the DIMM slot section, collect the memory configuration information.     DIMM slot	
♦ ID	\$ Serial number
✓ DevType2_DIMM0 OK 18A5F2G72PD8Z-3G2E1	28358324
✓ DevType2_DIMM2 OK 18A5F2G72PD8Z-3G2E1	28358246
✓ DevType2_DIMM4 OK 18ASF2G72PD8Z-3G2E1	2B3577A3
✓ DevTypeZ_DIMM6	2B357E65
✓ Devīype2_DIMM1 ● NO DIMM	NO DIMM
✓ DevType2_DIMM3	NO DIMM
✓ Der/lyps2_DIMM5	NO DIMM
✓ DevType2_DIMM7 ● NO DIMM	NO DIMM

### Collecting memory device configuration using Redfish

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

Step_1	List all the memory devices using the following command. RemoteComputer_OSPrompt:~\$ curl -k -srequest GETurl [ROOT_URL] /redfish/v1/Systems/system/Memory   jq
	<pre>\$ curl -k -srequest GRTurl https://admin:ready2go@12.16.182.31/redfish/v1/Systems/s **Gatas.id*: */redfish/v1/Systems/system/MemoryCollection.MemoryCollection*, **Gatas.id*: */redfish/v1/Systems/system/Memory/DevType2_DIMM0* **Gatas.id*: */redfish/v1/Systems/system/Memory/DevType2_DIMM1* *Godata.id*: */redfish/v1/Systems/system/Memory/DevType2_DIMM2* **Godata.id*: */redfish/v1/Systems/system/Memory/DevType2_DIMM2* *Godata.id*: */redfish/v1/Systems/system/Memory/DevType2_DIMM2* *Godata.id*: */redfish/v1/Systems/system/Memory/DevType2_DIMM2* *Godata.id*: */redfish/v1/Systems/system/Memory/DevType2_DIMM2* *Godata.id*: */redfish/v1/Systems/system/Memory/DevType2_DIMM2* *Godata.id*: */redfish/v1/Systems/system/Memory/DevType2_DIMM2* *Godata.id*: */redfish/v1/Systems/system/Memory/DevType2_DIMM4* *Godata.id*: */redfish/v1/Systems/system/Memory/DevType2_DIMM5* *Godata.id*: */re</pre>
Step_2	Collect m emory device information using the following command. RemoteComputer_OSPrompt:~\$ curl -k -srequest GETurl [ROOT_URL] /redfish/v1/Systems/system/Memory/[DEVICE_URL]   jq
	<pre>\$ curl -k -srequest GETurl https://admin:ready2go0172.16.182.31/redfish/v1/Systems/s {     context: -: /redfish/v1/Systems/system/Memory/.     eodata.10*: - /redfish/v1/Systems/system/Memory/DevTyps2_DIM00*,     #Odata.10*: - /redfish/v1/Systems/systems/systems/systems/systems/systems/systems/systems/systems/</pre>

# Collecting the Ethernet switch running configuration

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



## Collecting the Ethernet switch event log

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

Step_1	Display the switch event log. LocalSwitchNOS_OSPrompt:~# <b>show logging</b>	switch logging host mode is enabled switch logging level is notice Number of entries on Switch 1: Grand is a set of the set of the set of the set of the set Notice is notice National is not set of the set of t
		ID Level Time & Message
		1 Informational 1969-12-31T19:00:23-05:00 SYS-BOOTING: Switch just made a cool boot.
		2 Notice 1969-12-31T19:00:32-05:00 LINK-UPDOWN: IP Interface VLAN 1 changed state to up.
		3 Notice 1969-12-31T19:00:32-05:00 LINK-UPDOWN: IP Interface VLAN 1 changed state to up.
		4 Notice 1969-12-31T19:00:32-05:00 LINK-UPDOWN: IP Interface VLAN 2 changed state to do
		5 Notice 1969-12-31T19:00:32-05:00 LINK-UPDOWN: IP Interface VLAN 2 changed state to do

### Factory default

#### Table of contents

- <u>Restoring default UEFI/BIOS settings</u>
- <u>Restoring default switch NOS settings</u>
  - <u>Restoring default switch NOS settings using the CLI</u>
  - Restoring default switch NOS settings using the Web UI
- <u>Restoring a BMC password</u>

## **Restoring default UEFI/BIOS settings**

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

Step_1	From the UEFI/BIOS setup menu, navigate to the <b>Save &amp; Exit</b> menu and select <b>Restore Defaults</b> .	Save 6 Exit Save Changes and Exit Discard Changes and Exit Save Changes and Rest Discard Changes and Reset Save Changes Discard Changes	<pre>^ Restore/Load Default</pre>
Step_2	Select Save Changes and Reset .	Save C Exit Save Changes and Exit Discard Changes and Exit Discard Changes and Rest Save Changes Discard Changes Default Options Perfore Defaults Save as User Defaults Restore User Defaults	<pre>^ Restore/Load Default * Values for all the * setup options. * * * * * * * * * * * * * * * * * * *</pre>

Step_3 Wait for the system to reset. The UEFI/ BIOS settings should have been reset to default values.

### **Restoring default switch NOS settings**

Use caution when restoring default settings. Y our access to system components could be interrupted because of networking configuration changes. Refer to <u>Description of system access methods</u> to select an appropriate path to access the platform components.

#### Restoring default switch NOS settings using the CLI

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

NOTE: This procedure is equivalent to a factory reset for switch configuration. All configuration changes will be lost.

Step_1	Restore the default configuration. LocalSwitchNOS_OSPrompt:~# <b>reload defaults</b>	<pre># reload defaults % Reloading defaults. Please stand by.</pre>
Step_2	To make the revert to default values permanent, use the following command. LocalSwitchNOS_OSPrompt:~# copy running-config startup-config	<pre># copy running-config startup-config Building configuration % Saving 1555 bytes to flash:startup-config</pre>

#### Restoring default switch NOS settings using the Web UI

Refer to Accessing the switch NOS for access instructions.

To preserve configurations, the current configuration needs to be saved to startup-config. Refer to Saving the current configuration using the Web UI.

NOTE: This procedure is equivalent to a factory reset for switch configuration. All configuration changes will be lost.

Step_1	From the left-side menu, select Maintenance, Configuration and then Activate .	🔇 kontron	<b>* 9</b>
Step_2	Click on the <b>default-config</b> radio button.	Honitor     Diagnostics     Maintenance	Activate Configuration Select configuration file to activate. The previous
Step_3	Press on the Activate Configuration button to confirm.	Restart Device     Factory Defaults     Software     Configuration     Save startup-config     Download     Upload     Activate     Delete	leading to loss of management connectivity. Please note: The activated configuration file will <u>not</u> be saved to startup-config automatically. File Name @ default-config startup-config Activate Configuration
Step_4	(Optional) To make the change persistent, save running-config	to startup-config.	

### **Restoring a BMC password**

A BMC administrator password can be restored using the <u>Accessing a BMC using IPMI (KCS)</u> method.

Step_1	Identify the ID of the user with the password to restore. LocalServer_OSPrompt:~# ipmitool user list [CHANNEL]	# ipmitool user list ID Name 1 admin 2 mynewuser 3 4	1 Callin false false true true	Link Auth true true false false	IPMI Msg true true false false	Channel Priv Limit ADMINISTRATOR ADMINISTRATOR NO ACCESS NO ACCESS
Step_2	Reset the password. LocalServer_OSPrompt:~# ipmitool user set password [USER_ID] [NEW_PASSWORD]	# ipmitool user se	t passw	ord 1 "new	password12	23456"

# Support information

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

- Sending a BREAK signal over a serial connection
- Disabling sleep states in Linux

### Sending a BREAK signal over a serial connection

The documentation refers to the possibility of resetting a Kontron server using a special signal called **BREAK**. Wikipedia describes a break condition as something that "occurs when the receiver input is at the 'space' (logic low, i.e., '0') level for longer than some duration of time."

Here are methods to send a BREAK signal for various terminal emulators and other serial connection implementations.

# PuTTY

PuTTY accepts the keyboard combination of the CTRL key with the PAUSE/BREAK (modern keyboard often indicate only PAUSE). The signal can also be sent via the application menu. An example is shown in the image below.



## Minicom

A BREAK signal can be sent from the minicom Linux utility's help.

Minicom Command Summary	
Commands can be called by CTRL-A <	key>
Main Functions	1
send breakF	

#### Picocom

A BREAK signal can be sent from the picocom Linux utility's help.

*** Picocom commands (all prefixed by [C-a])
*** [C- ] : Send break

### Serial console servers

There are also dedicated servers that implement many physical serial connections which are then accessible via a network using telnet or SSH clients for example. These serial console servers typically allow the configuration of a key combination or sequence for each port that will send a **BREAK** signal to the connected device. Refer to your device manual for more information.

## Disabling sleep states in Linux

In Linux, sleep states are not controlled exclusively with definitions in the ACPI tables. They are also controlled by the operating system. Refer to accessing <u>Accessing the operating system of a server</u> for access instructions.

## Verifying enabled sleep states

Step_1	Verify enabled sleep states.	<pre>[root@localhost ~]# cat /sys/power/state freeze disk</pre>		
	LocalServer_OSPrompt:~# cat /sys/power/state	Treeze arsk		

### **Disabling sleep states**

Step_1	Disable sleep states using systemd.	<pre>[root@localhost ~] # sudo systemctl mask sleep.target suspend.target hibernate.ta rmst hubrid_sleep target</pre>		
	LocalServer_OSPrompt:~# sudo systemctl mask	Created symlink from /etc/systemd/system/sleep.target to /dev/null.		
	sleep.target suspend.target hibernate.target	Created symlink from /etc/systemd/system/suspend.target to /dev/null.		
	hybrid-sleep.target	Created symlink from /etc/system/system/hybrid-sleep.target to /dev/null.		

# **Application notes**

- <u>Generating custom secure boot keys</u>
- <u>Provisioning custom secure boot keys</u>

## 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.

### Provisioning custom secure boot keys

Table of contents

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

## Introduction

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

Secure Boot is a UEFI-defined feature used to authenticate a UEFI executable, such as an OS loader, using digital signing mechanisms based on the Public Key Infrastructure process, reducing the risks of pre-boot malware attacks. The feature uses a database of authorized signatures to confirm the UEFI executable integrity prior to execution.

Boards will typically have a pre-loaded set of Platform Key (PK), Key Exchange Keys (KEK), authorized signature database (db) and blacklisted / revoked signature database (dbx) as defined by the OEM, as well as some industry-standard certificates issued by Microsoft that allow booting Windows or well-known Linux distributions such as Ubuntu. It may be desirable for an end customer to update these keys with their own set for security reasons.

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

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

## Updating secure boot keys from the UEFI setup utility

#### Prerequisites

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 <u>Ger</u>	evant section: Ierating 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

Refer to Accessing the UEFI or BIOS for access instructions.

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><text></text></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 <b>Secure Boot</b> submenu from the <b>Security</b> tab.	Antia Setup Utility - Copyright (C) 2020 American Megatrends, Inc.

		If DNLY the Administrator's password is set, then this only limits access to Setup and is only asked for when entering Setup. If DNLY the User's password is set, then this is a power on password and must be entered to boot or enter Setup. In Setup the User will have Administrator rights. The password length must be in the following range: Minimum length 20 Administrator Password User Password User Password User Password Secure Boot Configuration
Step_3	Access the Key Management page by selecting the <b>Key</b> <b>Management</b> menu item.	Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc. Security System Mode User Secure Boot (Disabled) Not Active Secure Boot Hode (Custom) Restore Factory Keys Restor Factory Keys Restory
Step_4	Default Factory Keys should already be provisioned, as identified by the "Factory" attribute in the Key Source column in the Secure Boot variable table. To replace the default Platform Key with your own, select <b>Platform</b> <b>Key(PK)</b> .	Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc. Security Factory Key Provision [Enabled] Factory Key Formate Boot variables Factory Key Formate Boot variables Factory Key Formate Boot variables Factory Key Formate Boot variable State Key Source Factory Key Formate State Key Source Factory Key Schange Keys [F1] Factory Factory Key Schange Keys [F2] Factory Factory Key Schange State [F7] Factory Factory Signatures [F7] Factory [F7] Factory Factory Signatures [F7] Factory [F7] Factory Factory Factory Factory Factory [F7] Factory [F7] Factory [F7] Factory [F7] Factory [F7
Step_5	Select <b>Update</b> from the pop-up window.	Actio Setup Utility - Copyright (C) 2020 American Megatrends, Inc. Security Fractory Key Provision Fractory Fractory Fractory Signatures Size Si Fractory Fractory Signatures Size Size Size Key Fractory Signatures Size Size Size Size Size Key Fractory Signatures Size Size Size Size Size Size Size Size
Step_6	Select <b>No</b> to load a key from an external media.	Actio Setup Utility - Copyright (c) 2020 American Megatrends, Inc. Security Factory Key Frovision [Enabled] Factory Key Frovision File for a file: Factory Key Frovision [Enabled] Fress 'Yes' to load factory default 'FK' Factory Key Frovision [Enabled] Fress 'Yes' to load factory default 'FK' Factory Key Frovision [Enabled] Fress 'Yes' to load factory default 'FK' Factory Key Frovision [Enabled] Fress 'Yes' to load factory default 'FK' Factory Key Frovision [Enabled] Fress 'Yes' to load factory default 'FK' Factory Key Factory [File General Help Fortiden Signatures] 4269] 3] Factory [File General Help Freview Values]

		▶ OsRecovery Signatures] 0  0  No Keys ▼ F4: Save & Exit ESC: Exit Version 2.20.1276. Copyright (C) 2020 American Megatrends, Inc. AB
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.	Aptio Setup Utility - Copyright (C) 2020 American Megarends, Inc. Security Factory Key Provision [Enabled] Pactory Keys Provision [Enabled] Pacetro Factory Keys Reset To Setup Mode Export Secure Boot variables Select a file system Media/Softado, OVPCI(10)OVPCIC/0)Vev/C2PAth(Npce 3, Subtype 23)H0(Parti Repla/Softado, OVPCI(10)OVPCIC/0)Vev/C2PAth(Npce 3, Subtype 23)H0(Parti Repla/Softado, OVPCI(10)OVPCIC/0)Vev/C2PAth(Npce 3, Subtype 23)H0(Parti Repla/Softado, OVPCI(10)OVPCIC/0)Vev/C2PAth(Npce 3, Subtype 23)H0(Parti Repla/Softado, Signatures] 42051 & 2   Factory Pathonicad Signatures] 42051 & 2   Factory Pathonicad Signatures] 42051 & 2   Factory Pathonicad Signatures] 42051 & 0   No Keys B dSRecovery Signatures] 0 & 0   No Keys B dSRecovery Signatures] 0 & 0   No Keys Version 2.20,1276. Copyright (C) 2020 American Megatrends, Inc.
Step_8	From the list of files, select the Public Certificate file for the Platform Key (PK.cer in this example).	Actio Setup Utility - Copyright (C) 2020 American Megatrends, Inc. Security Factory Key Provision [Enabled] Factory Key Provision [Enabled] Restore Factory Legs Reset To Setup Mode Expont Secure Boot variable [Size] Keys Succe Period Garange Keys [205] 2 Factory Net Select Screen Factory Keys Schange Keys [205] 2 Factory Net Select Screen Factory Keys Schange Keys [205] 2 Factory Net Schange Keys [205] 2 Facto
Step_9	Specify that the file format is <b>Public Key Certificate</b> .	Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc. Security Factory Key Provision Restore Factory Keys Restore Factory Keys Restore Boot variables Enroil Efi Image Device Guard Ready Renowe 'UEFI Ca' from I Renowe 'UEFI Ca' from I Renowe 'UEFI Ca' from I Renowe 'UEFI Ca' from I Renowe 'UEFI Ca' from I Renowe'UEFI Ca' from I Re
Step_10	Select <b>Yes</b> to confirm Platform Key update.	Actio Setue Utility - Copyright (C) 2020 American Megatrends, Inc. Security Fractory Key Provision Enabled] Restore Factory Keys Restore Factory Keys Restore Boture Boot variables Update Update Update Device Guard R Confirm update of 'PK' with content from Restore Bot Ve Restore Bot Ve Restore Bot Ve No Restore Bot Ve Restore Restore Ve Restore Bot Ve Restore Bot Ve Restore Bot Ve Restore Bot Ve Restore Restore Restore Restore Ve Restore Restore R
Step_11	Confirm that the update completed successfully. The table should now show that a key was added from an "External" Key Source.	Aptio Setup Utility – Copyright (C) 2020 American Megatrends, Inc. Security

		<ul> <li>Factory Key Provision [Enabled]</li> <li>Resterne Factory Key</li> <li>Reset To Setup Mode</li> <li>Expont Secure Boot variables</li> <li>Erroil I fi Image</li> <li>Device Guand Ready</li> <li>Renowe "UEFI CA" from B</li> <li>Resterne Boot variable   Size  Keys Key Source</li> <li>Platform Key(RX) = 841  1 External</li> <li>Key Exchange Keys   2405  2 Factory</li> <li>Anthorized Signatures   3724  77] Factory</li> <li>Anthorized Signatures   3724  77] Factory</li> <li>Anthorized Signatures   3724  77] Factory</li> <li>Acthorized TimeStampi 0  0  No Keys</li> <li>Secure 8xit</li> <li>Escience 1 Rest Instance</li> <li>Secure 8xit</li> <li>Secure</li></ul>
Step_12	<ul> <li>Select Key Exchange Keys to update or append the KEK database with your own. In this case:</li> <li>Selecting Update from the pop-up window will erase the preprovisioned KEK entries and add a new KEK as a single entry;</li> <li>Selecting Append will add the new KEK to the database.</li> </ul>	Aptio Setup Utility - Copyright (c) 2020 American Megatrends, Inc. Security Factory Key Provision Restore Factory Key Provision Enabled Factory Key Provision Enabled Factory Key Provision Enabled Factory Key Provision Enabled Factory Key Provision Enabled Factory Key Froutic Key Enable Device Guard Ready Remove 'UEF 104' from Becure Boot variable Platform Key(Kk) Asthenized Signatures   324  77  Factory Anthonized Signatures   324  77  Factory Secure Solutions   0   0 No Keys Secure Solutions   0   0 No Keys Mathonized Signatures   0   0   No Keys Secure Solutions   0   0   No Keys Fat Save 8 Exit ESC: Exit
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".	Aptio Setup Utility - Copyright (C) 2020 American Hegatrends, Inc. Security Factory Key Provision [Enabled] Fastore Factory Keys Fastore Boat variables Expond Secure Boat variables Expond Secure Boat variables Enroil Efi Image Device Guand Ready Fastore UB defaults Secure Boat variable   Size  Keys Key Source Platform Key(FK)   481   1   External Fastore Keys   2020   31 Katory Fachdden Signatures   3724   77 Factory Fachdden Signatures   30   0   No Keys Signatures   0   0   No Keys Fachdden Signatures   570   0   No Keys Fachden Signatures   570   0   No K
Step_14	<ul> <li>Select Authorized Signatures to add an authorized Public Key certi</li> <li>Selecting Update from the pop-up window will erase the pre-provement of Selecting Append will add the new certificate to the database.</li> <li>Follow steps 4 to 11 to add a new db entry. If the certificate was appended</li> </ul>	ficate to the db. As for KEK: visioned db entries and add a new certificate as a single entry; ended to the database, the Key Source will be "Mixed".
Step_15	Select Save Changes and Exit from the Setup Utility.	Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc. Security Boot Save & Bait Save Changes and Reset Discard Changes and Reset Discard Changes and Reset Save Changes Discard Changes Discard Changes Discard Changes Discard Changes Default Options Restore Defaults Restore Defaults Restore User Defaults Boot Override ubuntu (INTEL SDPEDKF51208) Version 2,20,1276, Copyright (C) 2020 American Megatrends, Inc. Boot Default (C) 2020 American Megatrends, Inc.



# **Reference** guides

- Supported Redfish commands
- <u>Supported IPMI commands</u>

### **Supported Redfish commands**

Table of contents

- <u>Systems URLs</u>
- <u>Managers URLs</u>
- <u>Registries URLs</u>
- <u>Session Service URLs</u>
- <u>Task Service URLs</u>
- <u>Telemetry Service URLs</u>
- <u>Chassis URLs</u>
- <u>Account Service URLs</u>
- <u>Certificate Service URLs</u>
- <u>Update Service URLs</u>
- Event Service URLs
- <u>Miscellaneous URLs</u>

The information is presented in the following format:

• Description | URL | Type

Schema definition Schema definition for a specific type can be retrieve from <u>https://redfish.dmtf.org</u>

## Systems URLs

- Collection of computer systems | /redfish/v1/Systems | ComputerSystemCollection
- Information about a specified system | /redfish/v1/Systems/[SYSTEM_INSTANCE] | ComputerSystem.v1_15_0
- Computer system reset action | /redfish/v1/Systems/[SYSTEM_INSTANCE]/ResetActionInfo | ActionInfo.v1_1_2
- Collection of memory devices for this system | /redfish/v1/Systems/[SYSTEM_INSTANCE]/Memory | MemoryCollection
- Collection of processors | /redfish/v1/Systems/[SYSTEM_INSTANCE]/Processors | ProcessorCollection
- Collection of storage devices for this system | /redfish/v1/Systems/[SYSTEM_INSTANCE]/Storage | StorageCollection
- Collection of log services for this system | /redfish/v1/Systems/[SYSTEM_INSTANCE]/LogServices | LogServiceCollection
- EventLog service | /redfish/v1/Systems/[SYSTEM_INSTANCE]/LogServices/EventLog | LogService.v1_1_0
- Collection of EventLog entries | /redfish/v1/Systems/[SYSTEM_INSTANCE]/LogServices/EventLog/Entries | LogEntryCollection
- PostCodes services | /redfish/v1/Systems/[SYSTEM_INSTANCE]/LogServices/PostCodes | LogService.v1_1_0
- Collection of PostCodes entries | /redfish/v1/Systems/[SYSTEM_INSTANCE]/LogServices/PostCodes/Entries | LogEntryCollection
- Information about BIOS Configuration Service | /redfish/v1/Systems/system/Bios | Bios.v1_1_0

### **Managers URLs**

- Collection of managers | /redfish/v1/Managers | ManagerCollection
- Information about a specified manager | /redfish/v1/[MANAGER_INSTANCE] | Manager.v1_11_0
- Collection of Ethernet interfaces for a specified manager | /redfish/v1/Managers/[MANAGER_INSTANCE]/EthernetInterfaces | EthernetInterfaceCollection
- Information about a specified Ethernet interface | /redfish/v1/Managers/[MANAGER_INSTANCE]/EthernetInterfaces/[ETHERNET_INTERFACE_INSTANCE] | EthernetInterface.v1_4_1
- Cold reset action for this manager | /redfish/v1/Managers/[MANAGER_INSTANCE]/ResetActionInfo | ActionInfo.v1_1_2
- Collection of network protocol information | /redfish/v1/Managers/[MANAGER_INSTANCE]/NetworkProtocol | ManagerNetworkProtocol.v1_5_0
- Collection of HTTPS Certificates | /redfish/v1/Managers/bmc/NetworkProtocol/HTTPS/Certificates | CertificateCollection
- Collection of Trustore certificates | /redfish/v1/Managers/bmc/Truststore/Certificates | CertificateCollection

## **Registries URLs**

- Registry repository | /redfish/v1/Registries | MessageRegistryFileCollection
- Summary of a specified registry | /redfish/v1/Registries/[REGISTRY_INSTANCE] | MessageRegistryFile.v1_1_0
- Detailed information about a specified registry | /redfish/v1/Registries/[REGISTRY_INSTANCE.JSON] | MessageRegistryFile.v1_1_0

### **Session Service URLs**

- Session service | /redfish/v1/SessionService | SessionService.v1_0_2
- Collection of sessions | /redfish/v1/SessionService/Sessions | SessionCollection
- Information about a specified session | /redfish/v1/SessionService/Sessions/[SESSION_ID] | Session.v1_3_0

# Task Service URLs

- Task service | /redfish/v1/TaskService | TaskService.v1_1_4
- Task collection | /redfish/v1/TaskService/Tasks | TaskCollection

## **Telemetry Service URLs**

- Information about the telemetry service | /redfish/v1/TelemetryService | TelemetryService.v1_2_1
- Collection of metric definitions | /redfish/v1/TelemetryService/MetricReportDefinitions | MetricReportDefinitionCollection
- Information about a specified metric definition | /redfish/v1/TelemetryService/MetricReportDefinitions/[METRIC_REPORT_DEF] | MetricReportDefinition.v1_3_0
- Collection of metric reports | /redfish/v1/TelemetryService/MetricReports | MetricReportCollection
- Information about a specified metric report instance | /redfish/v1/TelemetryService/MetricReports/[METRIC_REPORT_INSTANCE] | MetricReport.v1_3_0

# Chassis URLs

- Chassis collection | /redfish/v1/Chassis | ChassisCollection
- Information about a specified chassis instance | /redfish/v1/Chassis/[CHASSIS_INSTANCE] | Chassis.v1_14_0
- Resets the chassis | /redfish/v1/Chassis/[CHASSIS_INSTANCE]/ResetActionInfo | ActionInfo.v1_1_2
- Collection of voltage sensors | /redfish/v1/Chassis/[CHASSIS_INSTANCE]/Power | Power.v1_5_2

# Account Service URLs

- Redfish account service | /redfish/v1/AccountService | AccountService.v1_5_0
- Collection of Redfish user accounts | /redfish/v1/AccountService/Accounts | ManagerAccountCollection
- Information about a specified Redfish account | /redfish/v1/AccountService/Accounts/[ACCOUNT_INSTANCE] | ManagerAccount.v1_4_0
- Collection of available roles | /redfish/v1/AccountService/Roles | RoleCollection
- Information about a specified role | /redfish/v1/AccountService/Roles/[ROLE_INSTANCE] | Role.v1_2_2
- Collection of account LDAP Certificates | /redfish/v1/AccountService/LDAP/Certificates | CertificateCollection

# **Certificate Service URLs**

- Certificate service | /redfish/v1/CertificateService | CertificateService.v1_0_0
- Certificate service locations | /redfish/v1/CertificateService/CertificateLocations | CertificateLocations.v1_0_0

# Update Service URLs

- Redfish update service | /redfish/v1/UpdateService | UpdateService.v1_5_0
- Collection of firmware images | /redfish/v1/UpdateService/FirmwareInventory | SoftwareInventoryCollection

# **Event Service URLs**

- Event service | /redfish/v1/EventService | EventService.v1_5_0

## **Miscellaneous URLs**

- List of OEM JSON schemas and extensions | /redfish/v1/JsonSchemas
- Information about a specified JSON schema | /redfish/v1/JsonSchemas/[JSON_SCHEMA_NAME]

### Supported IPMI commands

#### Table of contents

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

### **Application commands**

#### IPM device commands

Net function	Command	Command name	Supported / Unsupported
0x06	0×01	Get Device ID	Supported
0x06	0x02	Cold Reset	Supported
0x06	0x03	Warm Reset	Unsupported
0x06	0x04	Get Self Test Results	Supported
0x06	0x05	Manufacturing Test On	Unsupported
0x06	0x06	Set ACPI Power State	Supported
0x06	0×07	Get ACPI Power State	Unsupported*
0x06	0x08	Get Device GUID	Supported
0x06	0x09	Get NetFn Support	Unsupported
0x06	0x0A	Get Command Support	Unsupported
0x06	0x0C	Get Configurable Commands	Unsupported
0×06	0x60	Set Command Enables	Unsupported
0x06	0x61	Get Command Enables	Unsupported
0x06	0x64	Get OEM NetFn IANA Support	Unsupported
0x06	0x0B	Get Command Sub-function Support	Unsupported
0×06	0x0D	Get Configurable Command Sub-functions	Unsupported
0×06	0x62	Set Command Sub-function Enables	Unsupported
0×06	0x63	Get Command Sub-function Enables	Unsupported
0x06	0x52	Master Write-Read	Unsupported

* Commands are not rejected and can cause unpredictable behavior.

#### Watchdog timer commands

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

### BMC device and messaging commands

Net function	Command	Command name	Supported / Unsupported
0×06	0x2E	Set BMC Global Enables	Supported
0×06	0x2F	Get BMC Global Enables	Supported
0×06	0x30	Clear Message Flags	Supported
0×06	0x31	Get Message Flags	Supported
0×06	0x32	Enable Message Channel Receive	Unsupported
0×06	0x33	Get Message	Supported
0×06	0x34	Send Message	Supported
0×06	0x35	Read Event Message Buffer	Supported
0×06	0x36	Get BT Interface Capabilities	Supported
0×06	0x37	Get System GUID	Supported
0×06	0x38	Get Channel Authentication Capabilities	Supported
0×06	0x39	Get Session Challenge	Unsupported
0×06	0x3A	Activate Session	Unsupported
0×06	0x3B	Set Session Privilege Level	Supported
0x06	0x3C	Close Session	Supported
0x06	0x3D	Get Session Info	Supported
0x06	0x3F	Get AuthCode	Unsupported
0x06	0x40	Set Channel Access	Supported
0x06	0x41	Get Channel Access	Supported
0x06	0x42	Get Channel Info Command	Supported
0x06	0x43	Set User Access Command	Supported
0x06	0x44	Get User Access Command	Supported
0x06	0x45	Set User Name	Supported
0x06	0x46	Get User Name Command	Supported
0x06	0x47	Set User Password Command	Supported
0x06	0x52	Master Write-Read	Unsupported
0x06	0x58	Set System Info Parameters	Supported
0x06	0x59	Get System Info Parameters	Supported

#### IPMI 2.0 specific commands

Net function	Command	Command name	Supported / Unsupported
0x06	0x48	Activate Payload	Supported
0×06	0x49	Deactivate Payload	Supported
0x06	0x4A	Get Payload Activation Status	Supported
0×06	0x4B	Get Payload Instance Info	Supported
0×06	0x4C	Set User Payload Access	Supported
0×06	0x4D	Get User Payload Access	Supported
0×06	0x4E	Get Channel Payload Support	Supported
0×06	0x4F	Get Channel Payload Version	Supported
0×06	0x50	Get Channel OEM Payload Info	Unsupported
0×06	0x54	Get Channel Cipher Suites	Supported
0×06	0x55	Suspend/Resume Payload Encryption	Unsupported
0x06	0x56	Set Channel Security Keys	Unsupported
0x06	0x57	Get System Interface Capabilities	Unsupported

## **Chassis commands**

#### Chassis device commands

Net function	Command	Command name	Supported / Unsupported
0×00	0×00	Get Chassis Capabilities	Supported
0×00	0×01	Get Chassis Status	Supported
0×00	0x02	Chassis Control	Supported
0×00	0x04	Chassis Identify	Supported
0×00	0x05	Set Chassis Capabilities	Supported
0×00	0x06	Set Power Restore Policy	Supported
0×00	0×07	Get System Restart Cause	Unsupported*
0×00	0×08	Set System Boot Options	Supported
0×00	0x09	Get System Boot Options	Supported
0×00	0×0A	Set Front Panel Button Enables	Unsupported*
0×00	0×0B	Set Power Cycle Interval	Unsupported
0×00	0x0F	Get POH Counter	Unsupported*

* Commands are not rejected and can cause unpredictable behavior.

# Bridge commands

Bridge management commands

Net function	Command	Command name	Supported / Unsupported
0x02	0×00	Get Bridge State	Unsupported
0x02	0x01	Set Bridge State	Unsupported
0x02	0x02	Get ICMB Address	Unsupported
0x02	0х03	Set ICMB Address	Unsupported
0x02	0x04	Set Bridge Proxy Address	Unsupported
0x02	0x05	Get Bridge Statistics	Unsupported
0x02	0×06	Get ICMB Capabilities	Unsupported
0x02	0×08	Clear Bridge Statistics	Unsupported
0×02	0x09	Get Bridge Proxy Address	Unsupported
0x02	0×0A	Get ICMB Connector Info	Unsupported

### Bridge discovery commands

Net function	Command	Command name	Supported / Unsupported
0×02	0x10	Prepare For Discovery	Unsupported
0x02	0x11	Get Addresses	Unsupported
0x02	0x12	Set Discovered	Unsupported
0x02	0x13	Get Chassis Device Id	Unsupported
0x02	0x14	Set Chassis Device Id	Unsupported

#### Bridging commands

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

#### Bridge event commands

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

### Sensor event commands

Net function	Command	Command name	Supported / Unsupported
0x04	0x16	Alert Immediate	Unsupported
0x04	0x11	Arm PEF Postpone Timer	Unsupported
0x04	0x01	Get Event Receiver	Unsupported
0x04	0x10	Get PEF Capabilities	Unsupported
0x04	0x13	Get PEF Configuration Parameters	Unsupported
0x04	0x15	Get Last Processed Event ID	Unsupported
0x04	0x20	Get Device SDR Info	Supported
0x04	0x21	Get Device SDR	Supported
0x04	0x23	Get Sensor Reading Factors	Unsupported
0x04	0x25	Get Sensor Hysteresis	Unsupported
0x04	0x27	Get Sensor Threshold	Supported
0x04	0x29	Get Sensor Event Enable	Supported
0x04	0x2B	Get Sensor Event Status	Supported
0x04	0x2D	Get Sensor Reading	Supported
0x04	0x2F	Get Sensor Type	Supported
0x04	0x17	PET Acknowledge	Unsupported
0x04	0x02	Platform Event	Supported
0x04	0x2A	Re-arm Sensor Events	Unsupported
0x04	0x22	Reserve Device SDR Repository	Supported
0x04	0x00	Set Event Receiver	Unsupported
0x04	0x12	Set PEF Configuration Parameters	Unsupported
0x04	0x14	Set Last Processed Event ID	Unsupported
0x04	0x24	Set Sensor Hysteresis	Unsupported
0×04	0x26	Set Sensor Threshold	Supported
0×04	0x28	Set Sensor Event Enable	Unsupported
0x04	0x2E	Set Sensor Type	Unsupported
0x04	0x30	Set Sensor Reading And Event Status	Supported

# Storage commands

### FRU information commands

Net function	Command	Command name	Supported / Unsupported
0x0a	0×10	Get FRU Inventory Area Info	Supported
0x0a	0x11	Read FRU Data	Supported
0x0a	0x12	Write FRU Data	Supported

### SDR repository commands

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

#### SEL device commands

Net function	Command	Command name	Supported / Unsupported
0x0a	0x40	Get SEL Info	Supported
0x0a	0x41	Get SEL Allocation Info	Unsupported
0x0a	0x42	Reserve SEL	Supported
0x0a	0x43	Get SEL Entry	Supported
0x0a	0x44	Add SEL Entry	Supported
0x0a	0x45	Partial Add SEL Entry	Unsupported
0x0a	0x46	Delete SEL Entry	Supported
0x0a	0x47	Clear SEL	Supported
0x0a	0x48	Get SEL Time	Supported
0x0a	0x49	Set SEL Time	Supported
0x0a	0x5C	Get SEL Time UTC Offset	Unsupported
0x0a	0x5D	Set SEL Time UTC Offset	Unsupported

### **Transport commands**

#### LAN device commands

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

#### Serial over LAN commands

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

## Kontron OEM commands

Net function	Command	Command name	Supported / Unsupported
0x3C	0×07	UEFI Recovery	Supported

### 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.
<b>A</b> WARNING	WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.
<b>A</b> CAUTION	CAUTION indicates a hazardous situation which, if not avoided, may result in minor or moderate injury.
NOTICE	NOTICE indicates a property damage message.



#### Electric Shock!

This symbol and title warn of hazards due to electrical shocks (> 60 V) when touching products or parts of them. Failure to observe the precautions indicated and/or prescribed by the law may endanger your life/health and/or result in damage to your material. Please also refer to the "High-Voltage Safety Instructions" portion below in this section.



### ESD Sensitive Device!

This symbol and title inform that the electronic boards and their components are sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this product in order to ensure product integrity at all times.

HOT Surface! Do NOT touch! Allow to cool before servicing.



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

This symbol precedes helpful hints and tips for daily use.

### Acronyms

ACPI	Advanced Configuration and Power Interface
AI	Artificial Intelligence
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
BIOS	Basic Input/Output System
BMC	Baseboard Management Controller
BSP	Board Support Package
СВІТ	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
DTS	Digital Thermal Sensor
----------------	-----------------------------------------------------
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
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

LPL		Low Pin Lount
LVDS		Low Voltage Differential SCSI
MAT		Maximum Ambient Temperature
MB, Mbyte		Megabyte – 1024 KB
MCU		Microcontroller
MEC		Multi-Access Edge Computing
МХМ		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
ОСХО		Oven-Controlled Crystal Oscillator
OS		Operating System
OTP		Over-Temperature Protection
OVP		Over-Voltage Protection
PBIT		Power On Built-In Test
PCH		Platform Controller Hub
PCI		Peripheral Component Interconnect
PCIe		Peripheral Component Interconnect Express
PECI		Platform Environment Control Interface
PIRQ		PCI Interrupt Request Line
PMbus		Power Management Bus
РММ		POST Memory Manager
PnP		Plug and Play
POST	Power-On Self Test	
PSU	Power Supply Unit	
PTP	Precision Time Protocol	
PXE	Preboot eXecution Environment	
RAID	Redundant Array of Independent Disks	
RAN	Radio Access Network	
RAS	Reliability, Availability, and Serviceability	
RDIMM	Registered Dual In-Line Memory Module	
RDP	Remote Desktop	
RMM	Remote Management Module	
RoHS	Restriction of Hazardous Substances	
SAS	Serial Attached SCSI (Small Computer System Interface)	
SATA	Serial Advanced Technology Attachment	
SCSI	Small Computer Systems Interface	
SDRAM	Synchronous Dynamic RAM	
SEL	System Event Log	
SFP+	Small Form-	factor Pluggable that supports data rates up to 10.0 Gbps

SMS	Server Management Software
SNMP	Simple Network Management Protocol
SOC	System on a Chip
SOL	Serial over LAN
SSD	Solid State Drive
SSH	Secure Shell
THOL	Tested Hardware and Operating System List
TPM	Trusted Platform Module
TUV	Technischer Uberwachungs-Verein (A safety testing laboratory with headquarters in Germany)
UART	Universal Asynchronous Receiver Transmitter
UEFI	Unified Extensible Firmware Interface
UL	Underwriter's Laboratory
USB	Universal Serial Bus
UV	Under-Voltage
V	Volt
VA	Volt-Ampere (volts multiplied by amps)
Vac	Volts Alternating Current
Vdc	Volts Direct Current
VDE	Verband Deutscher Electrotechniker (German Institute of Electrical Engineers)
VGA	Video Graphics Array
vRAN	Virtualized Radio Access Network
VSB	Voltage Standby
W	Watt
WEEE	Waste Electrical and Electronic Equipment
Ω	Ohm